

Bir Sayı Tut...

Malcolm E. Lines



BİR SAYI TUT...

Malcolm E. Lines

Bir Sayı Tut... - Think of a Number

Malcolm E. Lines

Çeviri: Nermin Arık

© IOP Publishing Ltd. 1990

© Türkiye Bilimsel ve Teknik Araştırma Kurumu, 1997

Bu yapıtın bütün hakları saklıdır. Yazılar ve görsel malzemeler,
izin alınmadan tümüyle veya kısmen yayımlanamaz.
Türkçe yayın hakları Kesim Ajans aracılığı ile alınmıştır.

*TÜBİTAK Popüler Bilim Kitapları'nın seçimi ve değerlendirilmesi
TÜBİTAK Yayın Komisyonu tarafından yapılmaktadır.*

ISBN 975 - 403 - 139 - 8

İlk basımı Aralık 1998'de yapılan
Bir Sayı Tut...
bugüne kadar 22.500 adet basılmıştır.

10. Basım Şubat 2004 (2500 adet)

Yayınlar ve Tanıtım Daire Başkanı

Şefik Kahramankaptan

İşletme Müdürü

M. Kemal Bostancıoğlu

Yayıma Hazırlayan: Gökçe Bayrakçıken

Kapak Tasarımı: Aytaç Kaya

Sayfa Düzeni: Seval Özgöl

Dizgi: Birsan Kızıldağ

TÜBİTAK

Atatürk Bulvarı No: 221 Kavaklıdere 06100 Ankara

Tel: (312) 427 33 21 Faks: (312) 427 13 36

e-posta: kitap@tubitak.gov.tr

İnternet: kitap.tubitak.gov.tr

Semih Ofset - Ankara

Bir Sayı Tut...

Malcolm E. Lines

ÇEVİRİ

Nermin Arık

TÜBİTAK POPÜLER BİLİM KİTAPLARI

İçindekiler

Önsöz	I
I. Bölüm	1
<i>Giriş</i>	
II. Bölüm	9
<i>Fibonacci Ailesi ve Dostları</i>	
III. Bölüm	29
<i>Dolu Tanesi Sayılarıyla İnip Çıkma</i>	
IV. Bölüm	41
<i>Yalanlar, Kahrolası Yalanlar ve İstatistik</i>	
V. Bölüm	57
<i>En Kusursuz Kare</i>	
VI. Bölüm	69
<i>Eukleides'in Beşincisindeki Sorun!</i>	
VII. Bölüm	85
<i>Saat Sayıları</i>	
VIII. Bölüm	101
<i>Kriptografi: Gizli Yazışma Sanatı</i>	
IX. Bölüm	115
<i>Sayılar ve Ulusal Güvenlik</i>	
X. Bölüm	129
<i>Dört Renk Yeterli midir?</i>	
XI. Bölüm	143
<i>Cetveller, Ominolar ve Profesör Golomb</i>	
XII. Bölüm	155
<i>NP Problemi de Nedir?</i>	

XIII. Bölüm	169
<i>Bir Teneke Kutunun İçinde</i>	
<i>Kaç Top Sallayabilirsiniz?</i>	
XIV. Bölüm	185
<i>Ara Boyutlar</i>	
XV. Bölüm	197
<i>Kaosa Giden Yol</i>	
XVI. Bölüm	209
<i>Süper Matematik ve Canavar</i>	
<i>Ek Okumalar</i>	223
<i>Dizin</i>	225

Önsöz

1961 baharında bir sabah kendimi Oxford'daki Magdelen College'ın yazlık oturma odasında, gerçekten etkileyici bir meşe masada otururken buldum; araştırma asistanlığı sınavlarının sözlü bölümünde, araştırmalarımı öğretim üyelerine karşı savunuyordum. Matematiğe bir ölçüde yatkın bir fizikçi olduğum için soruların çoğu orada bulunan bilimcilerden ve matematikçilerden geliyordu. Sorular bir süre, "Green fonksiyonları" olarak bilinen, biraz da gizemli havaları olan matematiksel nesneler üzerine yoğunlaştı. Bunlar o zamanlar benim kendi teorik araştırma alanımda çok modaydı; ancak uzman olmayanlar için bilimciler de dahil pek fazla bir şey ifade etmiyorlardı. Doğrusunu söylemek gerekirse, o günkü bilimcilerin çoğu bu fonksiyonları belki de hiç duymamışlardı. Ancak o ara onlar benim için önemliydiler, ben de soruları başarıyla göğüslediğim kanısındayım.

Artık soru sorma sırası salondaki dinleyicilere gelmişti. (ben de kendimi biraz daha güvende hissetmeye başlamıştım). Salondakilerin çoğu kendi alanlarında ünlü kişilerdi ancak bu alanlar bilimin dışındaydı; büyük olasılıkla da geçen kırk dakikalık matematik sohbeti boyunca uyanık kalmak için çok çabalamışlardı. Bunlardan birisi, görkemli akademik giysiler içinde bir üye, etkileyici bir bakışla bana bakarak ayağa kalktı. Anlaşılan, kendisi için (ve herhalde orada bulunanların çoğu için) kavranması mümkün olmayan bu söyleşiden sıkılmıştı. Beni bugün bile huzursuz eden şu soruyu sordu: "Şu çok söz ettiğiniz Green fonksiyonlarına dönelim; bunlardan birini bir Ortaçağ tarihçisine nasıl açıklarsınız?" Soruyu bugün bile her sözcüğüyle anımsadığım halde yanıtlımın ne olduğu hakkında hiçbir şey hatırlamıyor olmam yanıtlımın niteliği konusunda iyi bir fikir verebilir.

Birkaç yıl sonra, ABD'nin New Jersey eyaletindeki Belle Araştırma Laboratuvarı'nda katı durum fizikçisi olarak çalışmaya başladım. Bu bilgisayar devrimi dönemi idi. Şirket birkaç yılda bir, daha büyük ve daha hızlı "sayı-öğütücü" satın alarak daha az düşünüp daha çok işlem yapmayı giderek kolaylaştırıyordu. Ancak arada bir, denklemlerin *kesin* çözümünün (veya matematikçilerin deyişiyle *analitik* çözümün) var olduğunu hissettiğim bir matematiksel problem söz konusu olduğunda, bilgisayardaki sayısal çözüme bakmaya direnip, daha yaşlı bir meslektaşına, düşünmeyi önlemenin bu kadar kolay olmadığı dönemlerde bilimsel olgunluğa ulaşma şansına erişmiş, nazik bir meslektaşın ofisine giderdim. "Bu denklemlerin analitik çözümü olduğundan eminim; ama bulamıyorum. Aptallık mı ediyorum?" derdim. Çoğu kez anlayışlı bir şekilde yarı-gülümseyerek "Belki biraz." diye yanıtlar; sonra beni nazik bir biçimde gereken çözümlere doğru yöneltirdi.

1980 yazında bir öğleden sonra, böyle bir ziyarete gittiğimde onu olağanüstü heyecanlı buldum. Ayağa fırladı ve daha ben alışılmış sorumu soramadan elime bazı kâğıtlar tutuşturdu. "Bunu oku," dedi, "şimdiye kadar gördüğüm en ilginç çalışmalardan biri; harikulade derin, ama zarif biçimde basit." Onun amaçlamadığı sonucu dile getirmekten kendimi alıkoydum; o kadar basitti ki ben (ya da bir Ortaçağ tarihçisi diyebilir miyim?) bile ana hatlarını anlayabilirdim. Gerçekte bu, elinizdeki kitabı okumayı sürdürmeye karar verirsiniz, ileride ele alacağımız, kaosun başlangıcı teorisi konusunda yapılmış ilk çalışmalardan biriydi.

O sıralar, ben ve eşim, bizden birkaç ev uzakta oturan genç bir çiftle ayda bir kez görüşür, konuşurduk. Adam inşaat işlerinde çalışıyordu, kadın ise ev hanımıydı; yarı-zamanlı olarak da moda evlerinin giysilerinin dağıtım işinde çalışıyordu. Akşamlarımız hep dinlendirici olur hoşça vakit geçirirdik, sohbetler pek akademik sayılmazdı. Hatta vaktimizin çoğunu Makjonng (1920'lerde çok revaçta olduğu söylenen çini parçalarla oynanan bir Çin oyunu) oynamakla, son görüşmemizden beri dağarcığımızda birikmiş fıkra ve deneyimleri

anlatmakla geçirirdik. Derken bir akşam, konuşmanın akışı içinde, ev sahibesi beni şaşırtan şu sözleri söyledi: “Sayılar hakkında bir kitap yazmayı düşündüğünü duydum. Fibonacci hakkında da bir şeyler söyleyecek misin?”

Geçmişteki bu “söz şip-şak”larını anlatmaktaki amacım hiç kuşkusuz, bazı tarihçilerin Green fonksiyonları konusunda bilgi edinmek için gizlice yanıp tutuştuklarını, ya da kaotik hareketin yeni ve büyüleyici alanının, ona tümüyle yabancı olan kişilerce bütün ayrıntılarıyla anlaşılabilir olduğunu öne sürmek değil. Ancak üç farklı noktayı vurgulamak istiyorum. Birincisi, bilimin herhangi bir yönünü (ve evet, hatta matematiği) anladığını söyleyen ve ondan coşku duyan bir kimse, bu bilginin özünü ve heyecanını, normal ölçüde zekâsı olan, ilgi duyan, sıradan kişilere aktarabilmelidir. İkincisi, bu türden heyecan verici gelişmelerin çoğunun böyle bir açıklamaya elverişli olduğudur.

Son ve belki en önemli olarak da “oralarda bir yerde” herkesin düşündüğünden çok daha geniş bir ilgi potansiyeli olabileceğidir: Tabii, eğer yazarlar bilim dergilerinin çetrefil uzman dili ile toplumun normal konuşma dili arasındaki dil uçurumunu birleştirici bir köprü kurmak için ciddi bir çaba gösterirlerse... İşte bu kitap, böyle bir eğilimi yüreklendirmeyi amaçlayan alçakgönüllü bir çabadan ibaret.

Malcolm E. Lines
Ağustos 1989

Giriş

Çağlar boyu, insanoğlunun saymaya ve ölçmeye karşı ilk kez ilgi duymasından bu yana, “sayı” kavramı insanı büyüleyen, ama bazen de ona işkence eden bir gelişme sergilemiştir. Bildiğimiz 1, 2, 3 sayıları hakkındaki en basit kavramlarla başlayıp, negatif sayılara, kesirlere, ondalıklara ve daha da ötesine uzanan “sayı”nın en genel anlamıyla ne ifade etmesi gerektiği konusundaki temel anlayış sürekli genişlemiştir. Buna paralel olarak, bu sayısal kavramların alışılmadık ve harikulade özellikleri hakkında acımasızca artan bir dizi büyüleyici soru ve spekülasyon ortaya çıkmış; bunlarla ilgili problemlerin bazıları kısa sürede, dönemin uzmanlarını hoşnut edecek biçimde “temizlenmiştir”. Bazıları içinse daha uzun süreli çaba gerekmiştir; bazen onlarca, bazen yüzlerce yıl süren çabalar... Birkaçı da, inatla, yaşamayı sürdürmekte ve dünyanın en ünlü matematikçilerini (son dönemlerdeki işbirlikçileri olan elektronik dijital bilgisayarların yardımı ile veya onlarsız) şaşırtmaya, onların yaratıcılığını ve zihinsel dengesini sınamaya devam etmektedirler.

Bu kitabın konusu, başlığından da anlaşılacağı gibi, bir anlamda sayılardır. Ancak kitap, sayıların özellikleriyle ilgili olmaktan çok (bu, daha önce yayınladığım, *A Number for Your Thoughts* adlı kitapta ele alınmıştır) sayıların “doğa” ile, çok genel bir anlamda, karşılıklı etkileşimi konusuy- la ilgilidir. Örneklerin bir bölümü, en azından ilk bakışta daha hafif mizaçlı gibi görünebilirler; dolu fırtınaları, taksiler, teras dekorasyonu, çam kozalakları, bisiklet fabrikaları ve boya kitaplarıyla ilgili olanlar gibi (isterseniz sayılar eğlencede diyebilirsiniz). Diğer bazıları daha ağırlıklı görünen konularla; gizli şifreler ve ulusal güvenlik, simetri ve atom

fiziği, meteoroloji, uzayın, dördüncü (hatta 3,5'nci) boyutta bükülmesi ve bilgi ağı sistemleri gibi konularla ilgilidirler. Bu örneklerde, sayılarla gerçek dünya sorunları arasındaki etkileşimin daha önemli sonuçları olduğu görünümü var; yani bir anlamda işe daha yakın bir şey. Gerçekten de, bir ara kitaba *İşte ve Oyunda Sayılar* başlığını vermeyi düşündüm. Ancak okul öncesi çocuklar için yazılan elementer bir aritmetik kitabını çağrıştırdığı, ama hiç de öyle olmadığı için vazgeçtim. Bu kitapta anlatılan her öykü, benim deyişimle, sayıyı iş yaparken veya oyun sırasında betimlese de (eğlendirici olduğunu umduğum bir biçimde) çoğu kez çok önemli sonuçları olan, çok derin matematiksel kavramlar içeren problemler hakkında bir kavrayışa yol açmaktadır. Birçoğu, gelişmesi yüzyıllar alan fikirleri izliyor, diğer bazıları çok yakın dönemde ortaya çıkmışlardır. Bazıları artık tam olarak çözülmüşlerdir, diğer bazıları gelişimlerinin henüz başlangıcındadırlar. Bazıları gizlerini açıklamak için günümüzün en güçlü “sayı öğretici” bilgisayarlarına gerek duymuşlar, bazıları da kuramsal düşüncenin esinli bir anına teslim olmuşlardır.

Birçok yerde öykülerimiz bizi, günümüz araştırmalarının “sivri ucuna” getirse de onları anlamamız fazla matematik gerektirmiyor. Gerçekte lisenin ilk yılındaki cebirin yarısını anımsayan bir kimse bu giriş bölümünün gerisini atlayarak doğrudan II. Bölüm'deki “Fibonacci Destanı”na geçebilir. Bunun dışında olanlar için, metinde açıklanmayan bazı sözcüklerin anlamlarını tekrarlamak, bu sözcükler yakın dönemlerdeki matematiksel sohbetlerinizin düzenli bir parçası olsunlar veya olmasınlar, iyi bir fikir olabilir.

İlk olarak, sayma sayılarına (yani 1, 2, 3, 4 vb. sayılara) *tamsayı* denilir. Yalnızca 1 ve kendileri ile tam olarak (yani kalan bırakmadan) bölünebilen tamsayılara *asal sayılar* denilir. Örnek olarak 3, 11 veya 29'u verebiliriz. Bunların dışında kalan bütün tamsayılara *bileşik* diyoruz. Bu demek oluyor ki, bütün bileşik sayılar kendilerinden daha küçük tamsayıların çarpımlarından elde edilebilirler; örneğin $32 = 4 \times 8$. Daha küçük olan bu tamsayılara, büyük sayının çarpanları

denilir. Bunlar arasında daha özel olan çarpanlar bulunur; *asal çarpanlar*. Yukardaki örnekte verilen 4 ve 8'in her ikisi de asal olmadığından onların her biri tekrar "çarpanlara ayrılabilir" (ve belki de tekrar tekrar) ve bu, sadece asal çarpanlar kalana kadar sürdürülebilir. Bileşik sayı olan 32 için işlem

$$32 = 2 \times 2 \times 2 \times 2 \times 2$$

ifadesine varana kadar sürdürülmüştür. Bu beş tane iki, 32'nin asal çarpanlarıdır. Asal çarpanlar özeldir; çünkü her bileşik sayı için bir tane ve sadece bir tane asal çarpanlar takımı vardır. Bu nedenle asal sayılar, bütün öteki sayıların çarpım yoluyla elde edildiği atomlardır (veya en küçük parçalar). Bütün tamsayıların asal çarpanların bir *çarpımı* olduğunu söyleriz. Bu nedenle çarpım, çarpma işleminin sonucu demek oluyor. Otuz iki, hem 8 ve 4'ün, hem de beş tane ikinin çarpımıdır. Toplama işlemi için buna eşdeğer olan terim *toplamdır*; 32'nin 28 ve 4'ün toplamı olduğu gibi.

Yukarıdaki denklemlerde dikkatimizi çeken bir başka şey de sağ taraftaki bütün o ikilerin pek hoş görünmediğidir. Ayrıca bileşik sayı, beş tane iki yerine 50 tane iki gerektirirse başımız dertte olabilir. Bunu halletmek için matematik bir çeşit kısa-yazış icadetmiştir. Bunu kullanarak yukardaki denklem

$$32 = 2^5$$

şeklinde yazılabilir. Bu yazış biçimindeki üst takısı olan 5'e *üs* veya *kuvvet* denilir ve size kaç tane ikiyi birbiriyle çarpacağınızı söyler. Başka bir örnek de

$$8 = 2^3$$

olabilir. 32 ile 8'in çarpımını yaparak (yani $32 \times 8 = 256$) ve sonucu $256 = 2^8$ şeklinde çarpanlara ayırarak şunu yazabiliriz:

$$2^5 \times 2^3 = 2^8$$

Burada önemli bir şey dikkatimizi çeker. Bu da böyle yazılmış sayıları birbirleriyle çarparken üslerini topluyor olduğumuzdur ($5 + 3 = 8$).

Bu kısa yazış biçimi, başka şeyler yanında, çok büyük sayılar içeren ifadeleri yazmamıza olanak sağlar; ayrıca da yazdıklarımızın doğru olduklarını biliriz, halbuki bu sayılar açıkça yazıldıklarında (ya da matematikçilerin deyişiyle ondalık notasyonda), hesap makineleri (hatta büyük bilgisayarlar) onların neye benzediklerini bilemezler. Örneğin $317^{12} \times 317^{12} = 317^{24}$ olduğunu biliyoruz, sağdaki sayının ondalık ifadesi 61 rakamlı olduğu halde. Dahası, 317^{12} bütün öteki sayılar gibi bir sayı olduğundan, kendisiyle çarpıldığı zaman, yeniden kısa-yazışı kullanarak, $(317^{12})^2$ şeklinde yazılabilir. Bunun sonucu olarak

$$(317^{12})^2 = 317^{24}$$

yazabiliriz, bundan da, bir kuvvete yükseltilen bir kuvvetin, bu iki kuvvetin çarpımı olan bir kuvvet olacağı kuralını öğreniyoruz (yani; $12 \times 2 = 24$).

317^{12} , on iki tane 317 'nin birbiriyle çarpımı demek olduğundan, n bir pozitif tamsayı olduğu sürece 317^n 'nin anlamı da açıktır. 317^1 'in sözcük anlamı olan "bir tane 317 'nin birbiriyle çarpımı" biraz tuhaf kaçıyor ancak onun değerinin 317 olması gerekiyor, çünkü ancak bu şekilde, kuvvetleri toplama kuralı ($1 + 1 = 2$) anlamh olur:

$$317^1 \times 317^1 = 317^2$$

317 'nin sıfırcı kuvveti için ne diyebiliriz? Bunun sözcük ifadesi "hiçbir 317 'nin birbirleriyle çarpımı" şeklindedir. Eğer sıfıra eşit olan tek bir şey varsa, o da ancak bu olabilir demek akla yakın. Ancak öyle değil!

Bunu da yine güvendiğimiz, kuvvetlerin toplamı kuralımızla öğreniyoruz:

$$317^0 \times 317^1 = 317^1$$

olmalıdır, çünkü üsler veya kuvvetler $0 + 1 = 1$ sonucunu veriyor. 317^1 de 317 olduğundan bu denklem şu şekli alır.

$$317^0 \times 317 = 317$$

ama bu ancak, eğer 317'nin sıfırıncı kuvveti bir olursa doğru olur. Doğal olarak burada 317 sayısı özel bir önem taşıyor, onun yerine başka herhangi bir sayı kullanarak da aynı sonuca varabilirdim. Öyleyse her sayının sıfırıncı kuvveti 1'dir. Herhangi bir sayı mı dedim? "Hemen hemen" herhangi bir sayı demek daha doğru olur. Hiçbir güçlük çıkarmayacak gibi görünen bir sayıyla, 0^0 ile durum oldukça farklı; ancak buna az sonra döneceğim.

Daha önce, bir sayının kesirli bir kuvvetinin ne anlama geldiği sorusu üzerinde duralım. Burada da kuvvetlerin toplamı kuralı yardıma yetişiyor. Onu kullanarak,

$$2^{1/2} \times 2^{1/2} = 2^1 = 2$$

ve

$$2^{1/3} \times 2^{1/3} \times 2^{1/3} = 2^1 = 2$$

olması gerek; çünkü her ikisinde de kuvvetler doğru olarak toplanmıştır. Böylece 2'nin bir bölü ikinci kuvveti, kendisiyle çarpıldığında 2 olan sayı demek oluyor (yani, 2'nin *karekökü* veya bilgisayarıma göre 1,414213562...dir.) Aynı şekilde 2'nin bir bölü üçüncü kuvveti, kendisiyle çarpılıp, sonra kendisiyle tekrar çarpıldığında 2 olan sayıdır; bu, 2'nin *küpkökü* veya 1,259921050...dir. Aynı kolaylıkla $2^{1/10}$ veya $2^{0.1}$, 2'nin onuncu kökü olur vb. Yukarıdaki rakam 1'den farklı olsa da bu, ilke olarak, bir sıkıntı yaratmaz. Örneğin:

$$3^{2/3} \times 3^{2/3} \times 3^{2/3} = 3^2 = 9$$

olması bize $3^{2/3}$ 'ün, 9'un küpkökü olduğunu söyler.

Negatif kuvvetler de

$$2^1 \times 2^{-1} = 2^0 = 1$$

türü eşitlikler yolu ile açıklanabilirler; bundan 2^{-1} 'in $1/2$ 'ye eşit olması gerektiğini görürüz. Gerçekte, herhangi bir n için $2^{-n} = 1/(2^n)$ dir. Hesap makineleri kullanırken negatif sayılarla arada bazı sıkıntılar olur. Örneğin, makinenizde y^x için bir anahtar varsa ve $y = -1$, $x = 0,5$ tuşlarına basarsanız (yani -1 sayısının karekökünü isterseniz) yanıt VERİ HATASI gibi bir şey olacaktır. Çaresizlik içeren bu mesaj bize, yanıtın $1,8$ veya $-2,7$ gibi, makinelerin anlayabildiği “gündelik sayılar” cinsinden verilemeyeceğini söylemektedir. “Kompleks sayılar” denilen sayılara gerek vardır ve şükürler olsun ki bu kitabı okurken ne sizin ne de makinenizin, bunları dert etmesine gerek yoktur.

Bu kez de “ 0^0 ” problemini halletmek durumundayız. Benim güvenilir Hewlett-Packard’ıma y^x düğmesi yoluyla $y = 0$ ve $x = 0$ girişini yaparsam yine çaresizlik çığlığı olan VERİ HATASI yanıtı gelir. Hiçbir negatif sayı işe girmedeği için sorun kompleks sayılarla ilgili olamaz.

Öyleyse makine neden bana bir yanıt veremiyor? Bu kitapta tartışılan konularla doğrudan bir ilgisi olmasa da, yanıtı bulmak üslerle ilgili yararlı bir alıştırma olabilir. Önce $y = x = n$ olarak aldığımızı ve n 'yi giderek küçülttüğümü varsayalım; $0,001$; $0,00001$, vb. y^x tuşunu kullanarak giderek 1 'e yaklaşan yanıtlar ($0.9931...$, $0.9998...$, vb.) elde ederim. Öyleyse 0^0 neden 1 'e eşit değildir? Yanıt, en kolay, x ve y 'yi bir grafik kâğıdı üzerindeki eksenler olarak düşünerek ve $x = y = 0$ 'ı merkez (veya başlangıç noktası) olarak anlaşılabilir. Şimdiye kadar başlangıç noktasına $x = y$ doğrusu boyunca yaklaştığımızı düşündük. Başka doğrultulardan da yaklaşabiliriz (örneğin, $y = 0$ olduğu, x 'in sıfır olmadığı ancak x -ekseni boyunca giderek küçüldüğü) ve başka yanıtlar buluruz (sıfır gibi). Öyleyse 0^0 sayısının, ona nasıl yaklaşıldığına bağımlı olan bir limit değeri var. Bu limit değeri, x ve y giderek küçülürken aralarında nasıl bir ilişki

olduğuna bağımlı olarak, bu limit değeri 0 ile 1 arasında herhangi bir sayı olabiliyor. Ancak çok özel yaklaşım biçimleri bu limit için 1'den farklı olan yanıtlara yol açarlar. Bu nedenle, bir anlamda 0^0 , eğer şanssız değilseniz, 1'dir! Bu ifade doğrudur ancak ifade biçimi hiç de matematiksel değildir. Kesin ifade şöyledir: 0^0 için 1'den farklı bir limit değeri elde etmek istiyorsanız, grafik kâğıdı üstünde, başlangıç noktasına yaklaşırken, x-eksenine çok yakın olan x'in herhangi bir kuvvetinden daha yakın olarak, (uzman deyişle) logaritmik olarak yaklaşmanız gerekir.

II. Bölüm

Fibonacci Ailesi ve Dostları

Hint-Arap sayılar sistemindeki sayısal simgeler (1, 2, 3, 4,... sayıları) Avrupa'ya, bu konuda yazılmış bazı kitapların basılmasıyla birlikte yayılmıştır. Bu kitaplar arasında en önemli olan *Liber Abaci* ("Abaküs Konusunda Bir Kitap" olarak çevrilebilir) adında bir kitaptı. Yazarı Leonardo Fibonacci isminde ilginç bir İtalyan matematikçisiydi. Fibonacci'nin (bu soyadının sözcük anlamı "Bonacci'nin oğlu"dur) 1202'de, 27 yaşındayken yazdığı bu kitap, günümüze kadar var olmayı, 1228'deki ikinci baskısıyla sürdürmüştür.

Liber Abaci oldukça büyük boyutlu bir kitaptır ve kapakları arasında o dönemde bilinen matematiğin büyük bölümünün kayıtlarını içerir. Cebirin kullanımı, farklı önem ve zorluk derecesinde bir çok örnek de verilerek, çok özel bir yer tutmaktadır. Ne tuhaftır ki bunların arasından bir tanesi ve yalnız bir tanesi diğerlerinin çok ötesinde ünlü olmuştur: Günümüze erişen 1228 yılındaki ikinci baskının 123-124 sayfalarında yer almaktadır ve tavşan üretmek gibi pek olası sayılamayacak bir konuyla ilgilidir. Temelde sorulan şu sorudur; eğer bir çift tavşan her ay yeni bir çift tavşan doğurursa ve her yeni tavşan çifti kendi doğumlarından iki ay sonra yavru lamaya başlarsa, bir çift tavşandan bir yılda kaç çift tavşan üretilebilir? Burada galiba dile getirilmemiş bir varsayım içermektedir, her tavşan çiftinin bir dişi bir erkek tavşandan oluştuğu varsayımı yer almaktadır (olasılık yasalarını ciddi biçimde zorlayan bir koşul); ancak bunu matematikten çok biyolojinin konusu olarak bir yana bırakırsak geriye kalan hesap işi zor değildir. Biraz düşünerek tavşan toplumunun nasıl oluştuğunu saptadıktan sonra aşağıdaki sayı dizisini elde

ederiz. Dizideki sayılar Ocak (ilk yavru çiftin ortaya çıktığı ay) ile Aralık arasındaki takvim aylarının her birinde kıştır kıştır yem yiyen tavşan çiftlerinin sayısını vermektedir:

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144

Bu diziye baktığımızda onun çok basit bir biçimde oluştuğunu hemen görebiliriz. Sözcüklerle bu şöyle ifade edilebilir; her sayı (doğal olarak ilk ikisi dışında) kendinden evvel gelen iki sayının toplamından oluşmuştur. Böylece, örneğin, dizinin sonundaki Aralık ayı sayısı, Ekim ve Kasım sayıları olan 55 ve 89 sayılarını toplayarak kolayca bulunabilir.

Sanırım, buraya kadar bir sorun yoktur, ancak matematikçiler arasında bile (onların heyecan eşiği sıradan insan için akıl almazdır) bu kadar heyecana yol açan nedir? Eğer kitabın bu bölümü amacını yerine getirebilirse, bu “Fibonacci sayıları”nın gizemli ve harikulade özelliklerinden hiç olmazsa birkaçı onların neden bu kadar ilginç olduğunu anlaşılır kılacaktır. Ancak önce diziyi genelleyelim. Tavşanların ölümlü olduklarını ve doğurganlıklarının saat gibi dakik düzeninde bir azalma olabileceğini yok sayarsak yukarıda verilen sayı dizisi, istenildiği kadar, çok daha büyük sayılara sürdürülebilir. Hatta tavşanları tümünden bir yana bırakıp, n 'inci sayıyı F_n olarak yazarak (Fibonacci'nin anısına F harfi kullanıyoruz) ve F_n 'nin kendinden önce gelen F_{n-2} ve F_{n-1} sayılarının toplamı olduğunu hatırlayarak sonsuz bir sayı dizisi tanımlayabiliriz. Fibonacci sayılarının dizisi bu şekilde,

$$F_1, F_2, F_3, F_4, F_5, \dots, F_n, \dots$$

olarak yazılabilir. Burada noktalar *ad infinitum* (sonsuzadek) bir sürekliliğe işaret etmektedir. Bu notasyonu kullanarak $F_1 = 1$ ve $F_2 = 1$ verildiğinde daha sonra gelen bütün sayıları sırasıyla bulmamızı sağlayan basit denklem şudur:

$$F_n = F_{n-1} + F_{n-2}$$

Eğer $n = 3$ ise $F_3 = F_2 + F_1 = 1 + 1 = 2$ 'dir. Benzer şekilde $F_4 = 3$, $F_5 = 5$ vb. buluruz. Tanımlayıcı denklem n 'nin üçten büyük ve üçe eşit her değeri için geçerlidir.

Fibonacci sayıları ilk verilen tavşan probleminde en büyük sayı olan $F_{12} = 144$ 'ün ötesine devam ettirildiklerinde çok büyük bir hızla büyürler. Örneğin dizinin 25'inci sayısı 75.025 olmuş, 100'üncü sayısı olan F_{100} 'de kocaman bir 21 basamaklı

354.224.848.179.261.915.075

sayısı olmuştur. Dahası, sayılar büyüdükçe onları tanımlayan denklemden ilk bakışta beklenenden, bir anlamda, çok daha basit bir düzen benimserler. Eğer her Fibonacci sayısını bir sonraki komşusuyla bölerek bulunan oran yazılırsa, bu düzen kolayca görülebilir. Böylece ilk iki oranla yola çıkarak, $F_1 / F_2 = 2$, $F_2 / F_3 = 1/2$ (veya ondalık olarak 0,5) ve dizi boyunca ilerleyerek aşağıdaki sayıları elde ederiz.

1,000000
0,500000
0,666666
0,600000
0,625000
0,615385
0,619048
0,617647
0,618182
0,617978
0,618056
0,618026
0,618037
0,618033
0,618034
0,618034

Bu sayılar beklenmedik bir 0,618034... sayısına doğru gidiyorlar. Buradaki noktalar, yukardaki sayılar, eğer verilen

altı ondalık haneden öte bir hassasiyetle hesaplanırlarsa daha fazla ondalık hanesinin var olabileceğine işaret etmektedirler. Gerçekte, bu “Fibonacci oranları”nı almayı sonsuza kadar sürdürme sonucunda bulunan sayılar $(\sqrt{5} - 1) / 2$ sayısına giderek daha yaklaşırlar, bu sayının ondalık ifadesi de cep bilgisayarımızın verdiği hassasiyetle

0,618033989’dur.

Ancak daha doğru olarak, bu sayı, ondalık açılımı hiç tekrarlamadan sonsuza kadar süren bir sayıdır. Bu tür bir sayıya *irrasyonel* deriz. Bunun nedeni sayının akli dengesinin bozuk olması değildir (bundan kuşkulanmış olmanız hoşgörülebilir); matematiksel bir anlamda, onun hiçbir zaman iki tamsayının *oranı* olarak ifade edilemeyeceği ile ilgilidir.

Fibonacci sayıları ailesi, üç ayrı nedenle yüzyıllardan bu yana yoğun bir ilgi odağı olmuştur: Birincisi, dizinin daha küçük üyelerinin doğada, beklenmedik yerlerde tekrar tekrar karşımıza çıkmasıdır; bitkiler böcekler, çiçekler ve benzer şeylerle ilgili olarak. İkinci neden, oranların limit değeri olan 0,618033989 sayısının çok önemli bir sayı olmasıdır; çoğu kez “altın oran” olarak adlandırılan bu sayının, oyun kartlarının biçiminden Eski Yunan sanatı ve mimarisine kadar birçok şeyin matematiksel temelini oluşturduğu görülmektedir. Üçüncüsü daha çok, sayıların kendilerinin, sayılar teorisinde beklenmedik biçimde farklı birçok kullanımı olan ilginç özellikleriyle ilgilidir. Gerçekte Fibonacci sayıları üzerine yapılan yayınlar o denli artmıştır ki, üç ayda bir yayınlanan *The Fibonacci Quarterly* dergisi tümüyle onların özelliklerine adanmıştır ve bu konuda her yıl birkaç yüz sayfalık araştırma yayımlanması dışında, arada uluslararası konferanslar da düzenlenmektedir.

Önce doğada, daha küçük Fibonacci sayılarıyla ne şekilde karşılaşıldığına bir bakalım. İlk olarak, bir bitkinin sapındaki yaprakların, bir ağacın dallarının düzeninde hemen her zaman Fibonacci sayılarını bulursunuz. Eğer yapraklardan biri başlangıç noktası olarak alınmışsa ve bundan başlaya-

rak, aşığıya veya yukarıya doğru, başlangıç noktasının tam olarak altında veya üstünde olan bir yaprak bulunana kadar yapraklar sayılırsa (sap çevresinde birden fazla dönmeye gerek olabilir) bulunan yaprak sayısı farklı bitkiler, fidanlar ve ağaçlar için farklıdır, ancak her zaman bir Fibonacci sayısıdır. Dahası, yaprak sayma töreni sırasında süreç kendini tekrarlamadan önce yapılan tam devir sayısı da bir Fibonacci sayısıdır. Böylece, örneğin bir kayın ağacı bir tam devir için üç yaprak gerektirir. Halbuki püsküllü söğüt ağacına beş devir için on üç yaprak gerekir.

Genel olarak, Fibonacci sayıları için bitki bilimi botanik tam bir altın madeni gibidir. Papatyaların normal olarak bir Fibonacci sayısı kadar taç yaprağı vardır, bu nedenle bir eleştirmenin daha önce söylediği gibi, “seviyor, sevmiyor” falının olumlu sonuç vermesi “talih perisi”nin araya girmesinden çok Fibonacci sayılarının dağılımının istatistiğine bağlıdır. Papatyalar bağlamında hangi Fibonacci sayısının en sık görüldüğünü bilmiyorum (bu kitabı yazdığım şu ara ne yazık ki kış; yoksa gereken araştırmayı ben şahsen yaptım). Ancak 21, 34, 55 ve hatta 89 sayıları bildirilmiştir.

Doğada Fibonacci sayılarıyla karşılaşmanın en ünlü örneği ayçiçekleriyle ilgilidir. Ayçiçeğinin çiçek kısmında, baklava biçimindeki ufak bölmelerde tohumlar vardır. Bu bölümlerin sınırları şekilde görüldüğü gibi merkezden başlayıp çiçeğin dış kenarına giden sarmal eğriler şeklindedir. Eğer şekildeki modelde, saat yönünde olan ve saat yönünde olmayan sarmalları sayarsanız hemen her zaman Fibonacci dizisinde art arda gelen sayılarla ödüllendirilirsiniz. Şekil 1’de saat yönünde 13, ters yönde 21 sarmal var (onları sayın). Bu sayılar doğada genel olarak rastlananlara kıyasla küçük olsalar da resim çizerken büyük kolaylık sağlıyorlar. Gerçek ayçiçeğinin başında, çoğunlukla, 34 ve 55 sarmal bulunur, ancak daha küçük olan bazılarında 21 ve 34, daha büyüklerinde ise çoğu kez 55 ve 89 sarmal vardır; hatta 89 ve 144 sarmalın bulunduğu bildirildiği olmuştur. Ayçiçeklerinin hiçbir özel durumu yoktur, sadece tohumları büyük olduğundan sarmalların ayırt edilmesi ve sayılması daha kolay olmaktadır. Birçok

çiçeğin, tohum başı, bir kıvrıncığın yaprakları, bir soğanın katmanları, ananas ve kozalakların kat kat kabukları gibi bitkisel şekillerin birçoğu Fibonacci sarmalları içerirler.

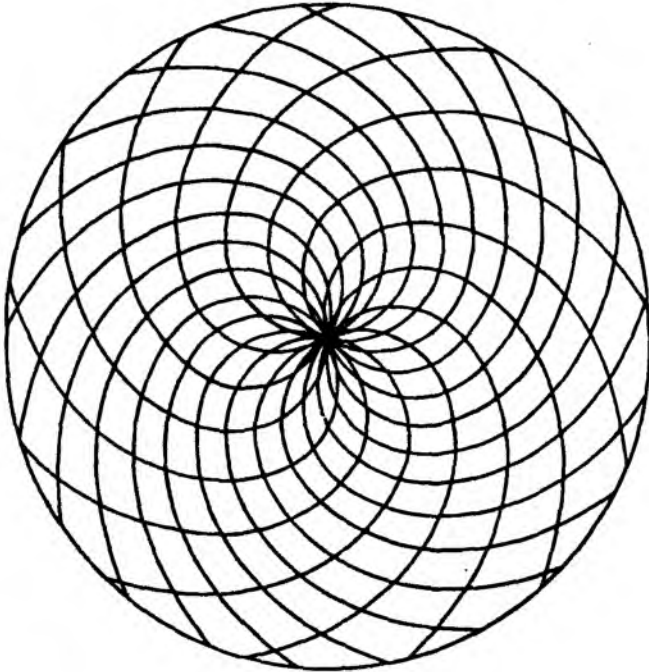
Değişik çam ağacı kozalakları üstünde çok dikkatli bazı incelemeler yapılmıştır. Kozalaklar henüz kapalıyken yani taze ve yeşilken sarmal sayımı çok kolayca yapılabilir. Daha yaşlı, açık kozalaklar da suda ıslatılarak tekrar kapanmaları sağlanabilir (bu durumda sarmallar çok daha kolayca görülebilirler). O zaman ilginç bazı sorular daha sorulabilir; örneğin, kozalakların sarmallarının sağdan sola doğru mu, soldan sağa doğru mu olduğu yoksa bazen bir yönlü, bazen de başka yönlü mü oldukları gibi. Bundan kastedilen, sayısı daha büyük olan sarmalların hep saat yönünde mi, saate ters yönde mi, yoksa bazen bir yönde bazen öbür yönde mi gittiğidir. Yanıt olarak belki de, “sarmalları, sağdan sola doğru giden kozalaklar olduğu kadar soldan sağa doğru giden kozalaklar da vardır; ancak bazı ağaçlarda bir tek yön baskındır.” denilebilir. Tek bir özel çam türü için bile bazı ağaçlarda sarmalları sağdan sola doğru giden kozalaklar çoğunluktayken, komşusunda tam tersinin söz konusu olması şaşırtıcıdır. Bildiğim kadarıyla bunun nedeni tam bir sırdır. Ancak yine de neredeyse bütün ağaçlar, her iki türden kozalak veriyorlar.

“Fibonacci olmayan herhangi bir kozalak bulunmuş mudur?” diye sorabilirsiniz. Yamt “Evet ama çok az sayıda.” şeklindedir. Yüzde bir veya iki oranında “serseri” kozalakları olan (çoğu zaman birkaç belirli çam türünden) bazı çam ağaçları var. Bunlar bile sık sık Fibonacci kozalaklarıyla, yakından ilişkili, örneğin, normal olan 5 ve 3 sayıları yerine belki de bir çift-Fibonacci sarmalının 10 ve 6 sayı çiftine sahipler.

Bu bölümün başlığı “Fibonacci Ailesi ve Dostları” olduğuna göre bu dostların bazılarının kimliklerini sorma vakti geldi sanırım.

Eğer Fibonacci sayılarının nasıl oluştuğunu, yani n’inci sayının, daha küçük iki komşusundan

$$F_n = F_{n-1} + F_{n-2}$$



Şekil 1.

denklemini kullanarak hesaplandığını hatırlarsak ilk iki sayı seçilmeden bütün dizinin tümüyle saptanmış olmayacağı açıkça görülür. Fibonacci dizisi, $F_1 = 1$ ve $F_2 = 1$ ile başlar, öbürlerini de yukardaki denkleme göre daha sonra saptarız. Ancak bu iki başlangıç sayısının özel hiçbir yanı olmadığından, başlangıç için başka değerler de seçebilir ve aynı tanımlayıcı denklemi kullanarak tümüyle farklı bir sayı dizisi elde edebilirsiniz.

Bu akraba sayı ailelerinden en ünlüsü Fransız matematikçisi Edvard Lucas'ın adıyla anılan Lucas Sayıları dizisidir. Başlangıç sayıları için seçilebilecek ikinci en basit sayıları seçerek $F_1 = 1$ ve $F_2 = 3$ olarak almıştır. $F_1 = 1$ ve $F_2 = 2$ koyarsak (ki daha basitmiş gibi görünüyor) Fibonacci dizisi-

ni çok ufak bazı düzensizliklerle tekrarlayan bir dizi oluştuğuna ve yeni hiçbir şey elde edilemediğine dikkatinizi çekirim. Halbuki Lucas sayıları Fibonacci akrabalarından çok farklı bir dizi oluşturlar ve şöyle başlarlar:

1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322,...

Genellikle L_n , sembolüyle gösterilirler, L sembolü Lucas'ı onurlandırmak için seçilmiştir.

Daha önce söylenenler ışığında Lucas dizisinin birçok ak-raba dizisinden sadece birisi olduğu aşikâr olmakla beraber, konumuz bakımından, bu sayıların da bazen doğada görül-meleri ilginçtir. Örneğin Lucas ayçiçekleri olduğu bildiril-miştir. Onlara Fibonacci yoldaşlarından daha az rastlanıyor; ancak 123 sağ sarmalı ve 76 sol sarmalı olan örnekler görül-müş ve dikkatle sınıflandırılmışlardır.

Doğa'da Fibonacci modelinin ve daha ender de olsa, Lucas modelinin neden bulunduğunu kimse gerçekten bilmiyor. Yapılan farklı açıklamaların sayısının, bir tahmin yürütme-ye gönüllü olan bilimcilerin sayısına neredeyse eşit olduğu görülüyor. Bunlar arasında, biraz daha akla yakın bir açık-lama, bir Sap çevresindeki yaprakların Fibonacci sarmalla-rına göre sıralanmakla yüzeylerinin güneşi en verimli biçim-de almalarının sağlandığı yolundadır. Bu matematiksel ola-rak belki de kontrol edilebilir; ancak henüz kimsenin böyle bir hesaplama yapma zahmetine girip girmediğini bilmiyo-rum. Daha az olası (ve kesinlikle daha az doğrulanabilir) bir açıklama da polen taşıyan böceklerin "sayısal düzenleri" ter-cih ettikleri varsayımına dayanmaktadır. Bu tercih, evrim süreciyle, Fibonacci geometrilerinin baskın çıkmasına yol açmıştır. Gerçeği söylemek gerekirse sizin tahmininiz de belki başka herhangi birininki kadar geçerli olabilir.

Şimdi biraz da, Fibonacci ve Lucas sayı dizilerinin her i-kisinin hiç yılmadan, düzgün adımlarla sonsuza doğru git-meleri sonucu ortaya çıkan ve altın oran denilen limit oranı 0,618033989, üzerinde duralım. Bu sayıya duyulan ilgi 2000 yıl öncesinden de geriye uzanır. "Atalarımız" belki de,

onun matematiksel temelini bizim açıkladığımız biçimde bilmiyorlardı; ancak altın oranı temel alan sanat ve mimarının göze olağanüstü güzel göründüğünü bildikleri kesin. Bu nedenle geometriyi altın orana göre tanımladılar; Özellikle de bir düz doğru parçasını ikiye ayıran nokta olarak. Öyle ki, küçük parçanın büyüğe oranı, büyüğün bütüne olan oranına tam olarak eşittir.

Okulda öğrendiği cebirin birazını hatırlayanlarınız için, küçük bölümü x , büyük bölümü 1 ile göstererek yukardaki geometrik ifadeyi

$$x / 1 = 1 / (1 + x)$$

şeklinde yazabiliriz; buradaki (/) işareti “ile bölünür” anlamına gelir; $1 + x$ ise, doğal olarak doğru parçasının bütünü-nün uzunluğudur. Bu denklemin altın oran tarafından gerçekten sağlandığı, cep bilgisayarı kullanılarak doğrudan kontrol edilebilir. 1 sayısı 1,618033989... sayısıyla bölündüğünde 0,618033989’a eşit olduğu doğrulanabilir. Ancak okul cebirinden birazını daha hatırlarsanız daha da iyi bir yöntem bulabilirsiniz. Yukarıdaki ifadeyi

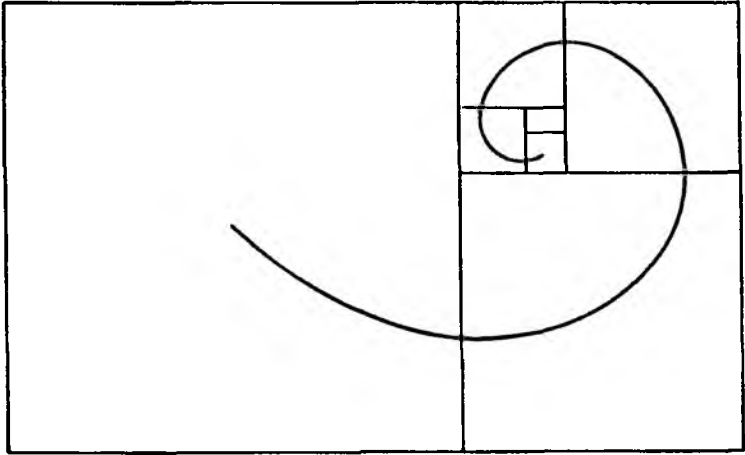
$$x^2 + x - 1 = 0$$

biçimindeki ikinci derece ifadeye dönüştürerek $x = (\sqrt{5} - 1) / 2$ tam çözümünü elde edersiniz.

Kısa kenarının uzun kenarına olan oranı altın oran kadar olan bir dikdörtgen çizerseniz son derece ünlü bir sanat eseri elde edersiniz, ona altın dikdörtgen denir. Eski Yunan’da ona, onu daha da saygıdeğer kılan Kutsal Kesit adını vermişlerdi. Bunu Şekil 2’de görüyorsunuz. İlk bakışta o kadar övgüye değer bir özellik göze çarpmasa da birçok yönden ilginç bir yapıdır. Bunun nedeni günümüze kadar uzanan sayısız nesiller boyunca insanların çoğunun onu bütün dikdörtgenler içinde göze en hoş görünen dikdörtgen olarak görmesidir. Bunun sonucunda günlük yaşamımızda karşılaştığımız binlerce dikdörtgenin büyük bölümünün boyutları, altın dik-

dörtgeninkine yakındır. Parçalar, paketler, kitap sayfaları, fotoğraflar, kibrit kutuları, bavullar, oyun kâğıtları, bayraklar, yazı kâğıtları, gazeteler ve sayısız başka örnek bu sınıftandır. Nedenini bilmeden desinatörler bilinçdışında Kutsal Kesit'e yakın olan dikdörtgen şekillerini tercih ederler. Bunu neden yaparlar? Altın dikdörtgen, her nasılsa, “doğru görünür”, ötekiler ya çok kısa ve şişman veya çok uzun ve incedir. Sanatçıların ve psikologların tam anlayamadıkları bir nedenle altın dikdörtgenin estetik bir çekiciliği var.

Yunan mimarisinde ve Yunan çömlekçiliğinde altın oran ve Kutsal Kesit'e çok sık rastlanır; aynı şey heykel, resim sanatları, mobilya ve sanatsal tasarımlar için de doğrudur. Parthenon'un ön bölümü, eksiksiz olduğu dönemde, bir altın dikdörtgen içine neredeyse tıpatıp girebilirdi. Altın orana



Şekil 2.

Mısır piramitlerinin bazılarının boyutlarında da rastlanır. Leonardo da Vinci de altın dikdörtgenlerden çok etkilenmiş, hatta bu konuda hazırlanan bir kitaba yazılarıyla katılmıştır.

Büyük ressamların birçoğu tuval boyutlarını, altın oranı titizlikle dikkate alarak düzenlediler. Sanatsal bakımdan “kutsal oran”la ilgili olarak farklı iki geometrik simetri kul-

lanılmıştır. Birisi, daha aşikâr olan, altın oran ve dikdörtgenler yoluyla 0,61803..., sayısını içeren statik ilişkidir, ancak ikincisi hareketle (veya en azından hayal edilen bir hareketle) ilgilidir. Olası görünmeyen bu ikinci etkinin kökeninde altın dikdörtgenin sahip olduğu çok özel bir başka özellik yatar. Bu dikdörtgen Şekil 2’de gösterildiği gibi bir kare ile daha küçük bir dikdörtgene bölünürse, küçük dikdörtgenin de “altın” olduğu görülür. Dahası aynı şekilde devam edersek, küçük olan dik dörtgen de bir başka ve daha da küçük bir dik dörtgene bölünebilir ve bu dikdörtgen de altındır. İlke olarak bu süreç *ad infinitum* sürdürülebilir ve giderek küçülen sayısız kareler ve altın dikdörtgenler ortaya çıkar. Bunlar içeriye doğru bir sarmal oluşturarak sonuçta bir noktaya yönelirler. Eğer, giderek küçülen bu karelerin (veya dikdörtgenlerin, hiç fark etmez) köşelerini veya merkezlerini şekilde görüldüğü gibi, düzgün bir eğriyle birleştirirsek genel olarak altın sarmal olarak bilinen bir sarmal elde ederiz.

Şekil 2’ye bir ressamın gözüyle bakarsak “fır dönen karelerin” bir resmini görürüz. Bu ilke, sanat eserlerine incelikli biçimde uygulanırsa hareket izlenimi elde edilir. Bunu betimlemek için “dinamik simetri” deyiimi kullanılmıştır. Birçok ressam, özellikle de 20. yüzyıl başlarında Amerikalı ressam George Bellows dönen karelerin yarattığı bu izlenimi büyük ölçüde kullanmıştır. Ancak bu üslubun kökeni yine Eski Yunan’a uzanır.

Şekil 2’de oluşan sarmal, herhangi bir sarmal değildir, gerçekte çok özeldir ve Şekil 1’deki ayçiçeği sarmalının aynısidir. Onun tam matematiksel adı eşit açılı sarmal veya logaritmik sarmaldır. Ona “logaritmik” denilmesi onu en basit biçimde ifade eden cebirsel denklemin logaritmalar kullanılarak yazılması nedeniyledir. Ancak günlük yaşamı algoritmalarla sıkça karşılaşmadan geçen çoğunluk için altın sarmalın özel yapısı “eşit açılı” özelliğini kullanarak daha kolay kavranabilir. Bu özellik şudur: Sarmalın merkezinden çizilen bir düz doğru, sarmalı hep aynı açıyla keser; bu şekilde çizilen başka herhangi bir doğru da aynı şeyi yapar; şekilleri kullanarak bunu doğrulayabilirsiniz.

Bu çok özel sarmalın, bir nedenle, doğada aşırı tercih görmesi çok şaşırtıcıdır. Deniz kabukluları, salyangozlar, doğanın boynuzları, pençeleri ve uzun azı dişleri, daha önce değindiğimiz Fibonacci-ilişkili kozalaklar, çiçekler; bunların hepsinin eşit açılı sarmalın bölümleri olduğu anlaşılıyor. Fibonacci'nin firdöneren kareleri bir eğri çiziyor, bir nedenle doğanın özellikle tercih ettiği de bu eğri oluyor. Uzayın derinliklerindeki büyük galaksilerin bile dışa doğru dönen yıldızlardan oluşmuş dev boyutlu eşit açılı sarmal kolları var. Belki de doğada her yerde Fibonacci'nin sayılarının, oranının ve sarmalının bulunması, bu oranları sanat içinde göze hoş görünür yapmaktadır.

Ancak Fibonacci sayılarının ve altın oranın doğa ve sanattan ayrı olarak tümüyle matematiksel olan ilginç yönleri de var, şimdi bu olası görünmeyen özelliklerin bazılarını ele alacağız.

Matematikçilerin hayal ürünleri olan kavramlar arasında hayal edilmesi daha zor olanlardan birisi de sürekli kesir denilen kavramdır. Herkes (en azından bunun gibi bir kitabı seçme eğilimi olan herkes) bir kesrin ne olduğu konusunda oldukça iyi bir fikir sahibidir. Özellikle, en basit türden olan bir adi kesir, bir tamsayının bir başkasıyla bölünmesinden başka bir şey değildir. En basit örnek, belki de, yarım veya $1/2$ 'dir. Yürekli bir çabayla, basit bir şeyi daha karmaşık yaparak onu şöyle yazabiliriz:

$$\frac{1}{1+1}$$

Şimdi biraz daha gayrete gelerek bu basit biçimi temel alan ancak işi bir adım öteye götüren bir kesir icad edelim:

$$\frac{1}{1+\frac{1}{1+1}}$$

Kesirleri toplama kurallarını hatırlayanlar yukardaki sayıyı hesapladıklarına $2/3$ yanıtını bulurlar. Benzer şekilde, aynı biçimde bir adım daha atarak;

$$\frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}}$$

yazarız ve yine kuralları bilenler bu garip nesnenin hangi adi kesire eşit olduğunu bulabilirler; yanıt $3/5$ 'tir. Artık bildiğimiz yolla devam ederek kesir yapılamayı bir adım daha sürdürürsek $5/8$ gibi basit bir kesiri ifade etmek için çok karmaşık bir yol bulduğumuzu anlarız.

Şimdi sıra, kavram bakımından atılacak büyük adımda. Kesir aynı adımları izleyerek hiç durmadan sürüp gider, *ad infinitum* devam etme anlamında bir "sürekli kesir" olur-

$$\begin{array}{c} \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}}}}}}} \end{array}$$

sa ne olur? Bu sayı ne olabilir? İnsan bunu nasıl hesaplayabilir? İpuçlarından birisi hesaplamış olduğumuz ilk dört katın yapı taşlarıdır. Onlar için $1/2$, $2/3$, $3/5$ ve $5/8$ sayılarını bulmuştuk. Bunlar da Fibonacci kesirleri F_2/F_3 , F_3/F_4 , F_4/F_5 ve F_5/F_6 ...nin kendileridirler. Bu bir rastlantı mı, yoksa daha fazla kat eklemeyi sürdürsek bu garip görünümlü kesrin giderek altın oran olan $0,618033989\dots$ sayısına yaklaşacağı anlamına mı geliyor? Yukarıya yazdığımız sürekli kesir, sonsuz limitte, gerçekten altın orana mı eşit olur? Bunu anlamak için sonsuza nasıl gidilebilir?

Sonsuz limitle ilgili soruyu yanıtlamanın 10'uncu kattaki veya 20'nci kattaki kesirin değerini hesaplamaktan ko-

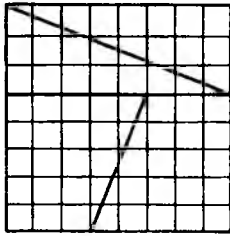
lay olması şaşırtıcıdır. Bunun sırrı, sonsuz kesirin en yukardaki satırına bakıp “1 bölü (duraksama) 1 artı bir şey” diyerek düşünmekten geçiyor. Şimdi “Bu bir şey nedir?” diye sorarız. Genelde yanıt “korkunç bir şey”dir. Ancak sonsuz limitte ve sadece sonsuz limitte, yanıt kolaydır; bu “bir şey” başlangıçta karşımızda olan sonsuz sürekli kesrin ta kendisidir. Onun değerine x dersek, x ’in “1 bölü (duraksama) 1 artı x ” olduğu aşikârdır. Bir denklem şeklinde yazarsak,

$$x = 1 / (1 + x)$$

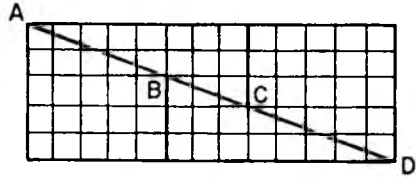
olur. Bu denklem daha önce altın kesiti tanımlarken bulduğumuz denklemdir ve çözümü $x = (\sqrt{5} - 1) / 2$, yani gerçekten de altın orandır. Öyleyse sonsuz sürekli kesirlerin en basiti (yani, sadece birlerden oluşan) yine bizi o çok özel 0,618033989... sayısına götürüyor. Bu sayıyı bulmak için kesiri sonsuza kadar sürdürmenin gerekli olması, altın oranının irrasyonel olduğunun bir başka doğrulamasıdır.

Fibonacci sayılarının bir başka tuhaf özelliği daha vardır. Bu özelliği ilginç yapan ilk defa (bildiğim kadarıyla) *Alice Harikalar Diyarında* adlı kitabın yazarı Lewis Carroll tarafından fark edilmiş olmasıdır. Lewis Carroll’un bu tür şeylerle ilgilenme nedeni onun gerçek yaşamda usta matematikçi Charles L. Dodgson olmasıdır. On dokuzuncu yüzyılın ikinci yarısının büyük bölümünde, Oxford Üniversitesi’ndeki Christ Church College’de matematik hocalığı yapmıştır. Christ Church’ün dekanının kızı olan gerçek Alice’le burada karşılaşmıştı; ancak bu öykü konumuz dışındadır. Onun Fibonacci bulmacası genellikle, geometrik bir paradoks (veya çelişki) olarak takdim edilir ve en basit şekliyle, 65’in 64’e eşit olduğunu “kanıtlama” yöntemi olarak kullanılır.

Şekil 3’e bakalım. Önce, 8×8 büyüklüğündeki bir kareyi Şekil 3 (a)’da görüldüğü gibi dört parçaya keselim. Birbirinin aynı olan iki üçgen ile, iki dörtgenden oluşan bu dört parçayı ayırıp Şekil 3 (b)’de görüldüğü gibi bir araya getirelim. Bu



(a)



(b)

Şekil 3.

yeni düzenlemede parçalar bir dikdörtgen oluşturur; ancak şaşılacak olan şey bu yeni dikdörtgenin kenar uzunluklarının 5×13 olmasıdır. Bu nedenle alanı 5×13 yani 65'tir, halbuki ilk alan 8×8 yani, 64'tür. Ne oldu? Her iki alanı oluşturan parçaların kenar uzunluklarının kontrolü hiçbir aldatmaca olmadığını gösteriyor. Öyleyse Şekil 3 (a)dan Şekil 3 (b)ye gitmekle ortaya çıkan birim alan fazlalığı nereden geldi? Okumayı sürdürmeden önce biraz düşünün. Yanılığının ne olduğunu görebilir misiniz?

Eğer şekli bir grafik kâğıdı üzerine tam ölçeğe göre çizip, Şekil 3 (a)da verildiği gibi kesip Şekil 3 (b)deki modele göre birleştirmeye çalışırsanız, sırrı keşfedersiniz. Bu işe girişmeyenler veya günlük yaşamları bilim dışında olduğu için hazırda bir grafik kâğıdı bulamayanlar için açıklıyorum. Şekiller çok inandırıcı görünmekle beraber gerçekte Şekil 3 (a)daki dört parçanın, Şekil 3 (b)deki gibi bir araya gelerek tam bir dikdörtgen oluşturmaları imkânsızdır.

Şekilde A, B, C ve D olarak işaretlenmiş noktalar, çizim dikkatle yapılırsa, bir doğru üstünde olmayacaklar (gördükleri gibi) çok uzun ve ince bir dörtgen alanın (paralel kenar denilen) köşelerinde olacaklardır; bu alan da aranılan birim alandır.

“Güzel de, bunun Fibonacci ile ne ilgisi var?” diyebilirsiniz. Eğer şekle bir daha bakarsanız, şekli oluşturan dört parçanın kenar uzunlukları 3, 5 ve 8'dir; bunlar art arda gelen üç Fibonacci sayısıdır. Önemli olan nokta bu üç sayının hiçbir özelliğinin olmadığı, onların ölçülmesi kolay olan kü-

çük sayılar oldukları için kullanıldığıdır. Art arda gelen farklı üç “Fibonacci” olarak da benzer bir paradoks oluşturulabilirdik. Örneğin 13×13 ’lük bir kare ile başlar, kenarlar için 5 ve 8 tamsayılarını alarak küçük modeli kestiğimiz gibi, keserek ve parçaları 8×21 dikdörtgen şeklinde birleştirsek 13×13 ’ün, 8×21 ’e eşit olduğunu veya daha açık olarak $169 = 168$ olduğunu sözcük kullanmadan “kanıtlarız”. Ancak daha büyük Fibonacci sayılarını kullandıkça, paradoksu açıklayan geometrik “uyumsuzluk” daha zor fark edilir, çünkü bir “birim”lik eksik alan bütün resmin giderek küçülen bir bölümünü oluşturur, örneğin, eğer kenar uzunluğu 8,9 cm olan kare biçiminde bir kâğıt alıp onu Lewis Carroll’un yaptığı gibi kenarları 5,5 ve 14,5 cm olan (55, 89 ve 144 art arda gelen üç Fibonacci sayısıdır) bir dikdörtgene çevirirsek uyumsuz paralel kenarı tamamlayan açıklığın en geniş yeri, yaklaşık onda bir cm kadardır ve gözle fark edilmesi çok zordur.

Fibonacciyle, aşağıdaki gibi garip toplamalar düzenliyerek farklı matematiksel eğlenceler bulunabilir:

0,1
1
2
3
5
8
13
21
34
55
89
144
233
...

0,112359550561...

Burada Fibonacci sayıları, sırayla bir hane kaydırılarak yazılmış ve toplanmıştır. Bu akıl almaz toplama işlemi sonsuza dek sürdürüldüğünde toplamın tam olarak $10/89$ basit kesrine eşit olduğunun ispat edilmiş olması inanılmazdır. Benim dokuz haneli hesap makinesi $10/89 = 0,112259551$, olduğunu söylüyor. Son ondalık haneyi “yuvarladığı” anlaşıyor. Yine de $10/89$ rasyonel bir kesir olduğu için ve bu tür kesirler eninde sonunda tekrarlayan ondalık kesirlere dönüştüğü için yukarıdaki ondalık sayılar sonunda tekrar etmeli, bunu yapıyorlar da; ancak 44 ondalık haneden sonra. Fibonacci yerine Lucas sayılarını kullanarak aynı toplama modeli yazılırsa bir başka basit kesir, $12/89$ elde edilir. Bu sayının da; 44 basamak sonra tekrarlayan bir ondalık açılımı vardır.

Eğer Fibonacci sayılarını sağa doğru bir rakam yerine iki rakam kaydırarak benzer toplama işlemleri yapılırsa 0,010102030508... olarak başlayan bir ondalık sayı elde ederiz. Bunun da sonsuza kadar olan tam değeri bilinmektedir ve tam olarak rasyonel $10/9899$ sayısındır. Benzer şekilde her aşamada üç rakam sağa kaymak, yine bir başka “rasyonel” sayı, $10/998.999$ sayısını veriyor. Lucas sayıları kullanarak benzer işlemler yapıldığında da toplamların basit kesir olarak değerleri bilinmektedir. Bunlardan başka Fibonacci veya Lucas sayılarını dönüşümlü olarak toplayıp çıkaran, veya dizinin sadece her ikinci sayısını (veya üçüncüsünü) toplayan benzer birçok toplamlar için de eşdeğer olan rasyonel sayılar bilinmektedir. Bütün bu sonsuz toplamların sonucu neden rasyonel bir sayı olmaktadır yani tekrarlayan ondalık sayı? Ondalık sayılar arasında tekrarlayanlardan sonsuz kat daha fazla irrasyonel (tekrarlamayan ondalık) sayı olduğu bilinmektedir. Bunu boş zamanlarda düşünmeniz için size bırakıyorum. Geceleri uykusu kaçan neden sadece ben olmalıyım?

Aklınıza başka bir şey de gelmiş olabilir. Bu bölümün başında altın oranın bir sonsuz sürekli kesir sonucu elde edildiği için irrasyonel olduğunu söylemiştim. Halbuki yukardaki bütün bu sonsuz toplamlar rasyonel sayıyla sonuçlanıyor. Kuşkulandırmakta haklısınız.

Şansızından altın oranın irrasyonel olduğunu kanıtlamak ilk cebir kitabının ilk bölümünü öğrenmiş bir öğrenci için bile çok kolaydır. Yapacağımız, onu tanımlayan denklemi alıp, p ve q tamsayılar olmak koşuluyla, denklemin p/q şeklinde bir çözümü olduğunu varsaymaktır. Bu kesrin üstünü ve altını, eğer mümkünse, aynı sayı ile bölerek onu en yalın biçimine getirelim. Örneğin

$$\frac{164}{64} = \frac{82}{32} = \frac{41}{16}$$

ve p ve q'nün hiçbir tamsayı'yla (1 dışında) bölünmediğinden emin olalım. $x = p/q$ yazarsak tanımlayıcı denklem

$$(p/q)^2 + (p/q) - 1 = 0$$

şeklini alır. q^2 ile çarpıp terimleri düzenleyerek $p^2 + pq = p(p + q) = q^2$ veya buna denk olan

$$p + q = q^{2/p}$$

elde edilir. Sol taraf tamsayı olduğundan denklem bize p'nin $q^{2/p}$ 'yi tam olarak böldüğünü (yani, kalan olmadan) söylemektedir. Ancak, p ve q'yu aynı zamanda bölen bir sayı olmadığına göre (matematik lisaniyla, p ve q'nun ortak çarpanı olmadığına göre) bunun olanaksız olduğu aşikârdır. Bu nedenle altın oran x, eğer p ve q tamsayılarsa, p/q şeklinde yazılmaz; başka deyişle x irrasyoneldir.

Görüyoruz ki, Fibonacci sayıları ve onlardan türeyen çeşitli sayılar doğada, sanatta ve matematikte çok olağandışı bir rol oynuyorlar. Yeni matematiksel genellemeler (genel terimin, daha önce gelen üç terimi toplamakla elde edildiği "Tribonacci sayıları"

$$1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504, \dots$$

gibi) *Fibonacci Quarterly*'nin her yeni sayısında görülmektedir. Uygulamalar da son derece boldur, ancak sanat konu-

sundaki bazı yorumlamaların güvenilir olmaktan çok romantik olduđu tartışılabilir. Fibonacci tiryakilerinin, neredeyse her gözlemi bu sayılarla ilgili yaklaşık bir biçime dönüştürme alışkanlıklarını (bazıları Cod Burnu kıyısında bir altın sarmal görmüş, diğer bazıları çiçeklerin üstündeki böceklerin büyüklüklerinde ayların gezegenlerinden olan uzaklıklarında ve periyodik tablodaki elementlerin atomlarının yarıçaplarında yaklaşık Fibonacci dizileri bulmuşlar) hesaba katsak da kanıtların toplamı gerçekten ikna edici. Fibonacci dizileri ve altın sarmal bazı tekrarlanan büyüme modellerinin önemli bir parçası; ancak “nasıl” ve “neden” olduğu tam bir sır. Ve bütün bunlar, bir 13. yüzyıl delikanlısının yarattığı teorik “abrakadabra” tavşanlar ailesinden çıkmıştır. Kayıtlara göre, komşularının bu delikanlıya karşı takındıkları tavır için saygılı sözcüğü uygun düşmüyor; ona, biraz küçümseyerek, “Bigollone” yani “mankafa” derlermiş.

III. Bölüm

Dolu Tanesi Sayılarıyla İnip Çıkma

“Dolu tanesi sayısı” problemi konusunda gerçekten bilinen tek şey onun kökeninin sırla örtülü olduğudur. Bildiğim kadarıyla, tarihi bir yayınla veya matematikçiler arasında bilinen herhangi bir mektuplaşmayla başlamadığı kesin. Çok eski de değilmiş gibi. Sanki son elli yıl içinde dünyanın her yanındaki öğrenim merkezlerinde rasgele biçimde ortaya çıkmış gibi görünüyor. Ağızdan ağıza mı yoksa son elli yılda birbirlerinden bağımsız olarak tekrar tekrar, “yeniden mi keşfedildiği” belli değil. Hatta problemin genel kabul görmüş bir ismi bile yok. Bazıları ona $3N+1$ problemi diyor, başkaları Collatz problemi (1930’larda bir öğrenci olan ve bazılarınca problemin yaratıcısı olduğu söylenen Lothar Collatz’a atfen). Dolu tanesi sayıları olarak betimlenmesi oldukça yenidir. Ancak az sonra göreceğiniz gibi, olgunun tümünün görsel algılanması bakımından özellikle uygun bir betimlemeye benziyor. 1950 yılına kadar problem hakkında yayınlanmış olan önemli herhangi bir kayıt yoktu. Fakat o günden bu yana, özellikle de 1970’den sonra hızla artan ilginin odağı oldu. Çözümü için ödüller konuldu ve yanlış bir sürü kanıt boşuna ödül parasının peşine düştü.

Öyleyse bu dolu tanesi sayıları nedir ve bütün bu ilgi neden? Kısa ve az bilinen geçmişleri göz önüne alındığında onlara verilen önem belki de gereğinden fazla olmuştur. Diğer yandan, tanımlanmalarının inanılmaz ölçüde kolay olmasına karşın hem çözülmemiş bir probleme yol açmışlar, hem de bu problemin (günümüzdeki en iyi matematik beyinlerine göre) uzun yıllar çözülmeden kalması olasılığı var. Konunun uzmanlarından hiç olmazsa birisinin “matematik henüz

bu tür problemlere hazır değil” dediği bilinmektedir. Sanırım biz de dikkatimizi bu gizemli sayılardan esirgemeyerek, kendilerine özgü sırlarını öğrenmeye çalışsak iyi olacak.

Dolu tanesi sayıları çok basit bir yolla, aşağıda verilen kurallar uyarınca elde edilirler. Bir sayı düşünün, sayı tek ise üçle çarpıp bir ekleyin, çift ise ikiye bölün. Ve elde edilen her yeni sayı için bu kuralı tekrar tekrar uygulayın, dizi ilerledikçe de ne olduğuna bir bakın. Önce, başlangıç sayısı olarak 1, 2, 3 sayılarını alarak en basit durumları inceleyelim. Kuralları uygulayarak bu sayılar için elde edilen diziler şöyledir:

1, 4, 2, 1, 4, 2, 1, 4, 2
 2, 1, 4, 2, 1, 4, 2, 1, 4, 2
 3, 10, 5, 16, 8, 4, 2, 1, 4, 2,

Bunların hepsi kısa sürede aynı 1, 4, 2, 1, 4, 2 döngüsüne giriyorlar. Biraz daha büyük bir başlangıç sayısıyla, örneğin 7'yle tekrar deneyelim.

7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1...

Bu sefer biraz daha uzuyor ve 52 gibi görkemli bir sayıya yükseliyor, ancak sonra tekrar aşağı düşüyor ve sonuç öncekiler gibi, sonu gelmeyen 142142142 döngüsüne giriş.

Yanıtlanacak basit soru şudur: “Bütün bu tür diziler, başlangıç sayıları ne olursa olsun, bu şekilde mi sonuçlanırlar?” Yukarıda değindiğim gibi, bunları yazdığım sırada bu sorunun yanıtı bulunmuş değil. Ancak yine de genel durumu için hiç olmazsa “çok kesin olmayan” bir şeyler söyleyebiliriz. Örneğin şu şekilde akıl yürütülebilir: Tamsayıların, engin denizinde tek ve çift sayı gelme olasılığı aynı olduğu için dizinin herhangi bir noktasındaki sayının tek veya çift olma olasılığı da aynıdır; kurala göre tek sayı bir sonraki adımda üç katından büyük bir değere giderken çift sayı yarıya iniyor, öyleyse “genel” dizi (eğer bundan kastettiğimiz “talihsiz” bazı özel durumlar dışındaki genel durum ise) sürekli artmalı-

dır. Aldığımız ilk birkaç özel örnekte belki de, şansımız ya-ver gitmemiş olamaz mı?

Denemeyi biraz daha sürdürmek gerekiyor. Ancak bir da-kika düşünelim; sırayla bütün başlangıç sayılarını denemek gerekmiyor. Yukardaki dizilerde görülen sayıların hepsinin aynı sonuca yol açacakları hemen görülebilir. Ayrıca, her çift sayı ilk adımda ikiye bölüneceğinden bunları da bırakabiliriz, daha küçük bir tek sayı nasıl olsa aynı diziyi üretecektir (ya-ni, çift sayılı dizideki ilk tek sayı). Bu sürdürme işlemlerimizi 9, 15, 19, ... vb. sayılarını başlangıç sayısı olarak almaya in-dirgemektedir. Denediğinizde kolayca göreceğiniz gibi bunla-rın hiçbirisi uzun ömürlü olmuyor (hepsi kısa sürede 142142 döngüsüne giriyor). Ta ki başlangıç sayısı olarak 27'ye varana kadar. O zaman, nihayet, bizi biraz serüven bekliyor:

27, 82, 41, 124, 62, 31, 94, 47, 142, 71, 214,
107, 322, 161, 484, 242, 121, 364, 182, 91, 274,
137, 412, 206, 103, 310, 155, 466, 233, 700, 350,
175, 526, 263, 790, 395, 1186, 593, 1780, ...

Dizinin bu noktasında (39'uncu sayıda, veya üretiminin 38'inci adımında) 1000 engelini güvenle aştık ve tam yol ilerliyoruz. Dizi daha ileriye sürdürülürse daha da güçleniyor ve 77'nci adımda 9232 "yüksekliğine" erişiyor. Ancak bu noktada felaket başlıyor ve "çöküş"e geçiliyor;

9232, 4616, 2308, 1154, 577, 1732, 866, 433, ...,

ve sonunda 111'inci adımda (112'inci sayı) 1'e iniyoruz, yo-lun sonu, veya daha doğrusu tekrar 142142 döngüsüne gi-riş. Ancak bu sefer hiç olmazsa emeğimizin karşılığını biraz aldık. Bu serüvenin bütün öyküsü Şekil 4'deki resimde gös-terilmiştir.

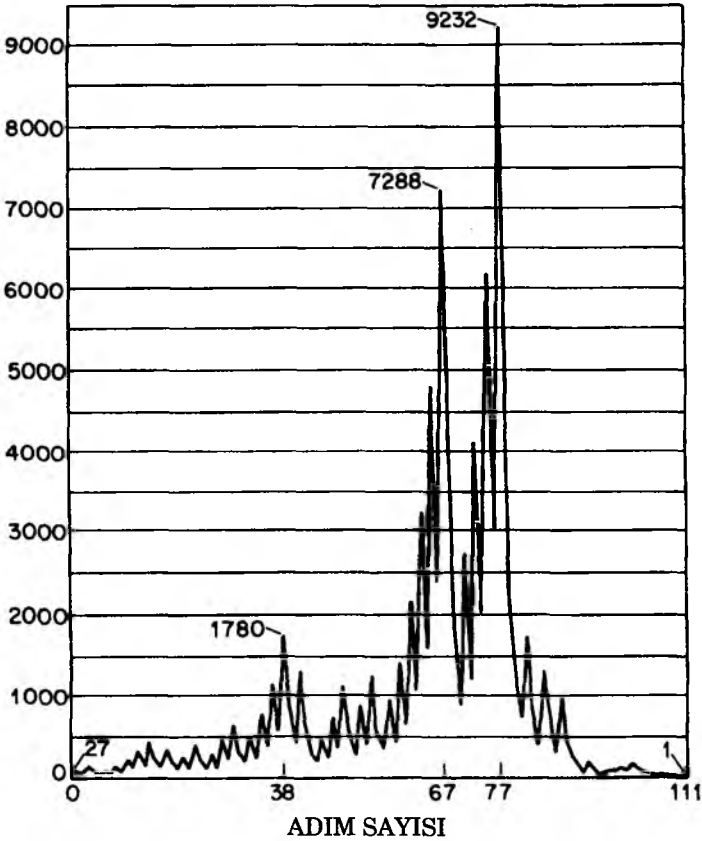
"Dolu tanesi sayıları" adı bu tür resimlerden esinlenmiş-tir. Sayıların iniş çıkışı bir fırtına bulutunda oluşan dolu ta-nelerinin hareketinden farklı değildir; önce yukarı doğru bir hava akımına yakalanıp çok yükseklerle çıkarlar, sonra onla-

rı taşıyan hava akımından çıkar kendi ağırlıklarıyla düşmeye başlarlar, ama yeniden, hem de daha güçlü bir akımla döngü tekrarlar. Ancak, gerçek dolu tanesi fırtına bulutunun içinde sürekli büyür bu da onun kaderini belirler; er veya geç, ağırlığı onu yukarı taşıyan en güçlü akımı bile aşar ve toprağa düşer. Bu, dolu tanesi sayılarının da değişmez kaderi midir?

Biraz önce yaptığımız usavurumda yanlış bir şey olduğu belli. Bütün dolu tanesi sayılarının sonunda “dünyaya düşmesi” doğru olsun veya olmasın, çok büyük bir bölümünün düştüğü kesin. İleri sürdüğümüz argümandaki zayıf nokta 27 ile başlayan dizinin incelenmesiyle hemen görülebilir. Bir tek sayıdan sonra gelen sayı her zaman çift olduğu halde, bir çift sayıdan sonra gelen sayının tek olması gerekmiyor. Bu nedenle, daha önce varsaydığımız, dizide tek ve çift sayıların görünme olasılıklarının aynı olduğu doğru *değil*. Sonunda çift sayıların sayısı teklerinkini aşacak ve bu nedenle “oyunun kuralları”nın, ilk bakışta, tek sayılara vermiş olduğu varsayılan 3’e karşı 2 avantajı dengelemeye yöneleceklerdir. Gerçekte, bir dolu tanesi dizisinde, yanyana olan üç tür sayı çifti olabilir: Tek-çift, çift-tek ve çift-çift.

Şimdi “Dizide bu farklı üç çiftin bulunma olasılıkları eşit olduğunda ne olur?” diye sordüğümüzü düşünelim. Birincisinde (tek ardından çift) dolu tanesi sayısı üçle çarpılarak artıyor (kuralın “1 ekle” bölümü, daha çok büyük sayıları içeren genel hesaplamalarda ihmal edilebilir), ikinci ve üçüncü olasılıklarda sayı ikiye bölünerek azalıyor. Her adım için *ortalama* sonuç: 3 çarpı $1/2$ çarpı $1/2$ yani $3/4$ ’tür. Şimdi şu ileri sürülebilir: Dolu tanesi eğrilerindeki bütün sivrilikler düzgün duruma geldiğinde, çok büyük başlangıç sayıları örneğin, bir trilyon veya 10^{12} , her adımda yaklaşık % 25 azalır ve bu nedenle sonunda 1’e inmesi kaçınılmazdır (verdiğimiz örnek için bu, 90 ila 100 adımdır).

Bir trilyonla başlayan bir dolu tanesi dizisini bir sayısına indirmek için gerçekte kaç adım gerektiğini bilmiyorum (anlaşılan bu bilgisayarla araştırılmış ve sonunda 142142 döngüsüne gerçekten indiği bilinmektedir); ancak 27 başlan-



Şekil 4. 27 ile başlayan dolu tanesi sayı dizisi.

gıç sayısı için gereken adım sayısı yüzden fazla olduğuna göre bu tür başlangıç sayıları için, yukarıda ileri sürülenler nitelik bakımından aşağı yukarı doğru olsalar bile, gerekli adım sayısında çok büyük iniş çıkışlar olacaktır. Gerçekte bu irdelemeler bazı başlangıç sayıları için dolu tanesinin bir daha aşağı inmeyecek ölçüde yukarı sapma yapabileceği olasılığını dışlamıyor. Düşünülebilecek en güçlü bilgisayar bile sadece sonlu sayıda adım sınavabileceğine göre bu tür bir dolu tanesinin kuşku götürmeyecek biçimde var olduğu bil-

gisayarla saptanamaz. Ancak “sayı-öğütme” yoluyla dolu tanesi dizilerini, olanaklı en büyük başlangıç sayılarıyla üreterek incelemek eğitici olacaktır. Böyle bir bilgisayar programını yazmak çok kolaydır ve ayrıca çalışmaya başlayınca bir süre için düşünmemize de gerek olmayacaktır, sadece oturup dolu tanelerinin hareketlerini seyredeceğiz.

Bu kitabın yazıldığı dönemde (1989) bu konuda, bildiğim en büyük girişim Tokyo Üniversitesi’nde yapılmıştır. Anlaşıldığına göre bir trilyona kadar olan bütün sayılar denenmiş ve hepsi de sonunda 142142 döngüsüne inmiştir. Görülen o ki, her çıkışın bir inişi gerçekten var! Ancak yine de dolu tanelerinin birçoğu için “fırtına bulutunda yolculuk” hayli olaylı geçmiştir ve çok yükseklerle çıkmıştır. İlk 100.000 başlangıç sayısı için bulunanların bir kaçına göz atalım.

İlk 50 tamsayı içinde bire dönmek için en uzun yolu kat eden 27’dir. Bu 111 adım (başlangıç sayısını da katarsak 112 sayı) içeriyor. Şekil 4’te görüldüğü gibi 67’nci adımda 7288 gibi azametli bir yüksekliğe çıkıyor, sonra çarpıcı biçimde 911’e düşüyor, yeni bir hava akımıyla karşılaşp daha da yukarılara (77’nci adımda 9232’ye) çıkıyor, sonra bir başka düşüş ve en sonunda birkaç uzayan çarpımın ardından, 111’inci adımda en aşağıya, 1’e düşüyor.

İlk 50 başlangıç sayısından sonra 9232 zirvesinin oldukça büyük bir engel olduğu görülüyor, 255’e gelinmeden de geçilemiyor. Bu dizi, 27 ile başlayan diziden daha kısa fakat hızla 13.120’ye yükseliyor ve yine hızla tekrar yere iniyor. Gerçekte 9232 zirvesi en uzun dizilerin hepsi için sonun başlangıcı oluyor, ta ki 703 başlangıç sayısına gelinsin. Bu dizi 170 adım sürüyor ve 250.504 zirvesine çıkıyor. 703 başlangıç sayısı, 27’den büyük (ve 100.000’den küçük) olan ve yeni uzunluk ve yükseklik rekorlarının her ikisini de kıran iki sayıdan birisi. Öbürü 26.623; 307 adım sürüyor ve 106.358.020 zirvesine erişiyor.

Yukarıda verilen sayısal bilgi parçacıklarından anlaşılan odur ki, adım sayısı, büyüyen başlangıç sayısına göre daha yavaş artış göstermektedir. 27 başlangıç sayısında 111 adım

olduğu halde 77.031 başlangıç sayısında (100.000'den küçük başlangıç sayıları içinde en büyük diziye yol açan sayı) sadece 350'ye ulaşmış. Diğer taraftan, zirve değerleri çok daha hızlı artıyor; 77.671 başlangıç sayısında (100.000'in altındaki sayılar içinde en büyük zirveye yol açan sayı) 1.570.824.736'ya çıkıyor. Bunun üstünde biraz düşünelim. Demek oluyor ki, araştırmamızın bu aşamasında dolu tanesinin çıktığı en büyük değer başlangıç değerinin 20.000 katından daha büyük. Dahası, zirve yüksekliğinin başlangıç değerine oranı, başlangıç sayısının artmasıyla artıyormuş gibi görünüyor. Yukarı doğru olan hava akımları ve ani düşmeler kısa sürede, giderek daha çarpıcı oluyorlar.

Çok büyük başlangıç sayıları N için (örneğin birkaç yüz veya daha fazla basamaklı) dizinin uzunluğunun oldukça "iyi davrandığı", ortalama olarak $24, 64D - 101$ (D , başlangıç sayısı olan N 'deki basamak sayısı) değerine yerleştiği ileri sürülmüştür. Bu formülün önemli bir teorik temeli yoktur; rasgele seçilmiş çok sayıda büyük başlangıç sayılarıyla elde edilen verilere dayanmaktadır. Örneğin, ister inanın ister inanmayın, başlangıç sayısı olarak $N = 1... (998 \text{ sıfır})....1$, bilgisayarla izlenmiş ve 142142 döngüsüne 23.069 adımda indiği saptanmıştır. $D = 1000$ basamaklı sayı için formül 24.539 adım öngörmektedir; % 10 civarında bir hata.

Bir dolu tanesi sayısının eriştiği zirve değerinin hep çift sayı olması gerektiğini görmek kolaydır. Yeni bir zirve rekorunun yalnızca tek olan bir başlangıç sayısı ile kırılabileceği de kanıtlanmıştır. Ancak dizi uzunluğu rekorunu kıracak başlangıç sayıları konusunda teorik herhangi bir tek veya çift kısıtlaması olmadığı görülmektedir. Görülen odur ki, uzunluk rekoru kıranların çoğunluğu tek sayıdır: 100.000'in altındaki istisnalar 6 (dizi uzunluğu 8), 18 (dizi uzunluğu 20) ve 54'tür (dizi uzunluğu 112).

Eğer, örneğin ilk yüz başlangıç sayısı için bütün dizi uzunlukları ve zirve yüksekliklerinin bir listesi yapılırsa ilginç bir dağılım elde edilir; kesinlikle rasgele olmayan ancak anlaşılması da kolay olmayan bir dağılım.

İşleri hızlandırmak için bir cep hesap makinesi kullanarak bunu siz de kolayca yapabilirsiniz. Yüz tane başlangıç sayısı çok fazlaymış gibi görünüyor ancak hepsini tek tek yapmanız gerekmez. Daha önce ürettiğimiz, başlangıç sayısı 7 olan diziyi düşünün:

7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1....

Bu dizi bize sadece uzunluğunun 16, zirve değerinin 52 olduğunu söylemiyor, aynı zamanda (ikinci sayı 22 olduğu için) 22 için dizi uzunluğunun 15, zirve değerinin 52 olduğunu ve (üçüncü sayı 11 olduğu için) 11 için uzunluğun 14, zirve değerinin 52 olduğunu vb. söylüyor. Bu bir tek “dolu tanesi” bize tam 16 başlangıç sayısı için gereken bütün bilgiyi veriyor. Ayrıca bizi, farklı birçok başlangıç sayısı için aynı zirve değerinin elde edildiği konusunda biraz aydınlatıyor; örneğin 52, yalnızca başlangıç sayısı 7 için bir zirve değil, aynı zamanda 22, 11, 34 ve 17 için de zirvedir. Bunun en çarpıcı örneği 27 ile başlayan dizinin zirve değeri olan 9232’dir. Bu 77’nci adımda ortaya çıktığından, ondan önce gelen 76 sayının dizilerinin zirve değeri de aynıdır. Gerçekte ilk 1000 başlangıç sayının üçte birinden fazlası için de zirve değeri aynı sayıdır.

Artık zirve değerinin neden rasgele olmadığını görüyoruz; dizi uzunlukları için ne diyebiliriz? Olanaklı her uzunluk gerçekleşebilir (bunu, ikinin kuvvetleri olan 2, 4, 8, 16, 32, 64, sayılarını başlangıç sayıları olarak kanıtlamak kolaydır; bunlar uzunlukları 1, 2, 3, 5, 6 ... vb. olan diziler üretirler) ancak burada da bazı uzunluklarla diğerlerinden daha sık karşılaşılır. Gerçekte bunlar kümelenmeye yönelirler. 1976 yılında aynı dizi uzunluğunu veren art arda gelen 52 başlangıç sayısından oluşan bir zincir yayınlandı. Bütün bunlar ne anlama geliyor? Daha küçük başlangıç sayıları içeren, 386’dan 391’e kadar olan daha küçük bir zincir vardır. Bu grup özellikle ilginçtir, nedeni de şudur: Bunun üyeleri sadece eşit uzunlukta olmakla kalmayıp hepsi de aynı zirve değere (doğal olarak 9232 değerine) sahipler. Bunu siz de kanıtlayabilirsiniz.

“Dolu tanesi konusunda” nereye geldiğimizi saptayalım. 1.000.000.000.000’a (yani bir trilyona) kadar olan her başlangıç sayısının, kuşku götürmez biçimde bire inip sonu gelmeyen 142142 döngüsüne düştüğü bilindiğine göre bütün sayılar için de böyle olduğu olası görünüyor. Bunun basit bir kanıtının olup olmadığı ve eğer varsa bizim yaşam süremizde bulunup bulunmayacağını bilmiyoruz. Bu problem ciddi araştırmacıların dikkatini çekecek ölçüde önemli değil, ancak yine de birçok matematikçi bu konuya şöyle bir göz atmanın ötesinde ilgi göstermiştir. Gerçekte bu o ölçüde yaygındır ki bir ara bunun ABD’de yapılan ciddi matematik araştırmalarını baltalamayı amaçlayan yabancı örgütün işi olduğu yolunda bir nükte moda olmuştur.

Bu bir trilyon sayı dizilerini düşünürken bana şaşırtıcı gelen bir şey var. O da şudur: Bunların hiçbirisi, ne kadar uzun olursa olsun aynı sayıyı iki defa içermiyor. Bir dizinin dolu taneleri aşağı yukarı giderken sayı uzayının hep aynı bölgelerinden geçiyor olmaları bunu daha da şaşırtıcı yapıyor. Bir sayının tekrarlanmadığını nereden biliyoruz? Tekrarlansaydı sayıların düzenleri hiç bitmeyen bir döngüyle (isterseniz halka deyin) tekrarlar ve hiçbir zaman, (söylendiğine göre) hepsinin yaptığı gibi 1’e inmezdi. Az önce söylediklerimiz, dolu tanesi dizisinin her adımda ortalama $3/4$ çarpanı kadar azaldığına kendimizi inandırmak için kullandığımıza benzer basit bir olasılık argümanı ile sonunda böyle rastlantıların olacağını söyleyebiliriz. Böyle bir trilyon dizi içinde bu tür tek bir rastlantının olmama ihtimali inanılmaz ölçüde küçüktür. Bir düşünün! Art arda gelen çift sayılardan sonra dizimiz bir tek sayıya her geldiğinde, daha önce bulunduğu sayı bölgesine giriyor ve bunu şimdiye kadar kontrol edilmiş olan nerdeyse bir trilyon dolu tanesi dizisinin hepsinde, tekrar tekrar yapıyor ama yine de bir tek sayının tekrarladığı görünmüyor.

Bu kadar şanslı (veya şanssız, bakış açımıza göre) olabileceğimiz düşünülemez. Dolu tanesi dizilerinde üretilen sayıların (görünümler bir yana) rasgele olmadığı sonucuna zorlanıyoruz. Bu sayıların içlerinde saklı, kesin olarak be-

lirlenmiş bazı matematiksel sınırlamalar var olsa gerek; belki de biz bunlardan birine tesadüfen çarptık. Eğer bunlar rastlantısal değillerse o zaman benim bu konudaki olasılık argümanım da başarısızlığa mahkumdur. Bu, aynı zamanda, bir dolu tanesi sayısının “sonsuz kadar uçma”ya gücü olmadığına işaret eden tek sonucu, $3/4$ argümanımızı da beraberinde götürür.

Öyleyse, belki de bir kuşku payı bırakmalıyız. Konu kapanmamıştır. Bazı dolu tanesi sayıları, belki de, sınırlanmadan sürekli daha yükseklerle, uçabiliyordur; eğer böyle değilse, en azından 142142 son durağından daha saygın bir yerde döngüye giriyordur. Periyodu 400.000’den küçük olan başka hiçbir döngünün olmadığı ileri sürüldüğüne göre bu saygın konumdaki döngü, eğer varsa, gerçekten çok etkileyici olmalı.

Bütün bunları okumanın oldukça eğlendirici olduğunu, normal bir hesap makinesiyle (eğer varsa) donanmış olarak sizin katkınızın ne olabileceğini düşünüyor olabilirsiniz. Yukarıda verilen dolu tanesi problemi için gerçekten yapabileceğiniz hiçbir şey yoktur, çünkü onların üstüne güçlü bilgisayarlarla bile gidilmiştir. Diğer yünden, bütün dolu taneleri aynı değildirler, çok çeşitli görünümlemlerle ortaya çıkabilirler. Gerçekte sayılamayacak kadar dolu tanesi vardır ve onların çoğuna (kullanmaktan hoşlandığım metafor karışımıyla) insan eli ayak basmamıştır. Örneğin, bir tek sayıyı 3’le çarpıp 1 eklemek yerine 3’le çarpıp belirlediğiniz herhangi bir tek sayıyı, 3, 5, 7 hatta, daha büyük bir sayıyı ekleyebilirsiniz. Bütün bu “dolu fırtınaları” için, daha önce vermiş olduğumuz $3/4$ argümanı (sizce herhangi bir güvenilirliği kalmışsa eğer) geçerlidir; bu tür herhangi bir dizi sürekli artamaz. Ancak bunlarla, en azından bazı durumlarda, başka döngüler üretilebilir.

Örneğin, tek sayı için “3’le çarpı 7 ekle”, çift sayı için de her zamanki “2’ye böl” kuralıyla üretilen dolu tanesini ele alalım. Başlangıç sayısı 1 olan dizi şöyledir:

1, 10, 5, 22, 11, 40, 20, 10, 5, 22, 11,...

kısa sürede sonu gelmeyen 5, 22, 11, 40, 20, 10, 5 halkasına girmiştir. Başlangıç sayısı olarak 7 alındığında,

7, 28, 14, 7, 28, 14, 7...

biçiminde bir döngü görürüz; ancak başlangıç sayısı olarak 9 alındığında dizi 25 adımlık bir yolculuk sonunda 1'e iner:

9, 34, 17, 58, 29, 94, 47, 148, 74, 37, 118, 59, 184, 92, 46, 23,
76, 38, 19, 64, 32, 16, 8, 4, 2, 1,...

Gördüğümüz gibi bu dizi, ikinin bir kuvvetine (yani, 2^6 olan 64) rastladığı için "bir taş gibi" ta 1'e kadar düşmüştür. Bu sonuç bir başka olasılık argümanını (zayıf da olsa) akla getirmektedir. Döngüye girmeden yeterince uzayan her dolu tanesi dizisinin (2 'nin kuvvetleri olan sonsuz sayıda sayı var olduğu için) sonunda bunlardan birine rastlayarak, takla atarak yere düşeceği ileri sürülebilir. Bu argüman, eğer bir değeri varsa, gerçekte, tek sayıları 5, 7 veya 9 ile çarpıp, örneğin 1 ekleyerek, çift sayıları da (her zaman olduğu gibi) 2 ile bölerek elde edilen bütün dolu taneleri için de geçerlidir. Bu yeni diziler için önceki $3/4$ argümanı artık geçerli değildir; (kontrol edin) artık $5/4$, $7/4$ veya $9/4$ argümanlarına dönüşmüşlerdir. Bunlar, her sayının (ortalama olarak) bir önceki sayıdan $5/4$, $7/4$ veya $9/4$, vb. çarpanı kadar büyük olacağını öngörürler. Bunun mantıksal sonucu, yeni dolu tanesi dizileri, eğer şanssız değillerse, sınırsız olarak büyüyerek sürüp gidecekleridir.

Bu nedenle, burada, özellikle ilginç olan bir durum ortaya çıkıyor. İki olasılık argümanı arasında bir çelişki olduğu görülüyor. Örneğin, sayıları 5'le çarpıp 1 eklediğimiz "dolu fırınası"nda argümanlardan biri şunu söylüyor: "Her terim, ortalama olarak, bir evvelkinden onun $5/4$ kat fazla olmalı ve bunun sonucunda dizi hiç durmadan büyümelidir." 2 'nin kuvvetleriyle ilgili öteki argüman ise sonsuza gittiğini iddia eden bu tür her dizinin ($5/4$ kuralına rağmen) "şanssız" olmaya mahkum olduğunu ve oraya varamayacak olduğunu söylüyor. Hangisine inanıyorsunuz?

Bildiğim kadarıyla bu dolu fırtınası hakkında pek fazla araştırma yapılmamıştır. Öyleyse yolunuz açık olsun. Size sadece kısa bir süre için eşlik edeceğim. Böylece, başlangıç sayısı 1 olduğunda;

1, 6, 3, 16, 8, 4, 2, 1

buluyoruz. Bu örnekte kazanan ikinin kuvvetleri argümanı oldu! Başlangıç sayısı olarak 2, 3 ve 4 alındığında bunlar yukardaki dizide zaten var olduklarından, oluşturdukları diziler de sonunda 1'e düşmeye (veya, eğer tercih ederseniz, bir 1, 6, 3, 16, 8, 4, 2, 1... halkasına) mahkumlar. Öyleyse başlangıç olarak ilgileneceğimiz bir sonraki sayı 5 olacak. Diziyi oluşturduğunuzda

5, 26, 13, 66, 33, 166, 83, 416, 208, 104, 52, 26, 13,

buluruz. Bu dizideki döngü "önemsiz olmayan" (bundan kastettiğimiz 1 sayısını içermemesidir) türdendir; 13'ten 416'ya yükselmekte ve sonra tekrar 13'e inmektedir. Başlangıç için 7 sayısını aldığımızda ne olduğu konusunda tek söyleyeceğim bunun iyi bir serüven olacağıdır. Araştırmaya başlayın. Başlangıç için başka sayılar deneyin. Daha sonra, nerdeyse sınırsız sayıdaki farklı türden dolu fırtınalarının herhangi birisini deneyin; belki de kendi "tahminlerinizi" ortaya koyarsınız. Eğer "ciddi" matematiği baltalamak için kurulan uluslararası örgütün bir parçası olmaktan korkuyorsanız o başka!

IV. Bölüm

Yalanlar, Kahrolası Yalanlar ve İstatistik

“Yalanlar var, kahrolası yalanlar ve istatistikler var.” diyerek bir zamanlar parlamentodaki meslektaşlarını uyaran kişi İngiliz Başbakanı Benjamin Disraeli’dir. İstatistik biliminin bu kadar kötü bir ünü nasıl kazandığı bilinmiyorsa da, söylenmek istenen şudur: Normal bir “sıradan insan”, zeki olsun veya olmasın, bu bilim hakkında o kadar az şey bilmektedir ki, kötü niyetli veya yanlış bilgi sahibi olduklarının farkında olmayan insanların vardıkları aslı olmayan sonuçları tümüyle kabul etmeye kolayca ikna edilebilir. Temel problem, olasılık konularında sağ duyu veya sezginin çok yetersiz bir rehber olmasındadır. Gerçekten bu olguya işaret eden pek çok basit örnek vardır. İyi bir vatandaşın bir jüri üyeliği görevini yerine getirirken karşılaşılabileceği küçük bir örnekle başlamak yerinde olur sanırım.

Söz konusu dava bir görgü tanığı bulunan bir çarpıp kaçma davasıdır. Bu tanık kazayı yapanın bir taksi olduğunu ve renginin mavi olduğunu söylüyor. Kazanın olduğu kentte sadece iki taksi şirketi var; bunlardan biri yeşil, öbürü mavi renkli arabalar kullanıyor. Dava, yeterince açık gibi görünüyor: Her olasılığa göre çarpıp kaçan şoförün “mavi taksi” şirketinin şoförleri arasından aranması gerekir, (şu anda, söz konusu arabanın, çalıntı olabileceğini hesaba katmıyoruz, bu pek olası değil).

Şimdi biraz duralım; ufak bir sorun var. Kaza olduğunda hava kararıyordu ve testler gösteriyor ki tanık yeşil veya mavi arabaları sadece % 80 oranında doğru olarak ayırt edebiliyor. Şöyle diyebilirsiniz; Pekala bu kanıtı biraz daha az

kesin yapıyor; ancak en büyük olasılık hâlâ (hiç kuşku yok) olayla ilgili taksinin mavi olması yolunda. Sorumluluk duygusu taşıyan bir jüri üyesi başka hangi sonuca varabilir? Öyleyse, bu kanıt da adil bir karara varmak için yararlanılan bütün öteki bilgilerin yanında yerini almalıdır. Bu değerlendirmeye karşı çıkanınız var mı? Sanmıyorum; ancak yine de bu özel dava konusunda böyle bir değerlendirme (aşağıda açıklanacağı gibi) tamamen temelden yoksundur.

Nedenine gelince: Şimdiye dek toparladığımız bilgileri yarsız kılacak çok önemli bir soru, bu kentteki taksilerin yüzde kaçının mavi, yüzde kaçının yeşil şirkete ait olduğu sorusu henüz sorulmamıştır. Davamız bakımından yanıt, yeşil-taksi şirketinin mavi-taksi şirketinden çok daha büyük olduğu ve kentteki taksilerin en az % 85'ini çalıştırdığı yolundadır. Eğer tanık, taksilerin % 20'sinin rengini yanlış olarak saptıyorsa durum çok değişir. Şimdi neden böyle olduğunu görelim.

Karmaşık matematik ve olasılık formüllerinin ayrıntılarına girmeden, tanığın bir tek kaza değil de böyle bir çok (örneğin 100) kaza gördüğünü ve hepsinde kaza yapan arabanın rengini söylediğini düşünelim. Böylece istatistiğin özüne çabucak girebiliriz. Olasılık yasalarına göre bu kazaların 85'ini yeşil arabaların, 15'ini de mavi arabaların yapması beklenebilir. Tanık, yeşil arabaların % 20'sini yani 17'sini yanlışlıkla mavi olarak tanımlıyor. Mavi arabaların yer aldığı 15 kazanın % 80'ini, yani 12'sini doğru olarak mavi diye teşhis edecektir. Demek ki mavi arabaların yaptığını söylediği 29 kazanın 17'sinde tanık hata yapmıştır; hemen hemen % 60'lık bir hata oranı. Tanığın kazayı yapan arabanın mavi olduğu yolundaki ifadesi, büyük olasılıkla, yeşil bir taksinin yanlış teşhisidir.

Bu durumda, ortaya konan kanıtlardan çıkarılacak doğru sonuç, kaza yapan taksinin büyük olasılıkla yeşil olduğudur; ancak olasılıklar birbirlerine yakın oldukları için jüri üyelerinin bu kanıtı hiç olmazsa dikkate almaması belki de en iyisidir. Şimdi Disraeli'nin istatistik hakkındaki samimi kuşkusunu anlamaya başlıyoruz. Olasılık teorisinin vardığı

çoğu sonuç gerçekten de “eski dostumuz sağduyu”ya aykırı düşmektedir.

İstatistik teorisinin, matematiksel yönden oldukça sağlam olmasına karşın, inanılması güç sonuçlarla karşımıza çıkma şeklindeki bu can sıkıcı eğilimi yüzyıllar öncesine gider. En ilginç eski örneklerden biri bir şans oyunuyla ilgili olan ve ilk olarak 1730’larda İsviçreli matematikçi Daniel Bernoulli tarafından dile getirilen problemdir. Oyun “yazı” gelinceye kadar yazı tura atmaktan ibarettir. Eğer ilk atmada yazı gelirse “kazanç” 2 (yani ikinin birinci kuvveti olan 2’nin kendisi) fiştir; fişin değerini istediğiniz gibi saptayabilirsiniz, söz gelimi ona 1 dolar diyelim. Eğer yazı ancak ikinci atışta gelirse kazanç 2^2 (yani 4) dolar oluyor. Eğer üçüncü atışta gelirse kazanç 2^3 (yani 8) dolardır ve böylece sürüyor. Yanıtlanması gereken soru şudur: Yazı tura atanın bu oyuna girebilmesi için “kasaya” ödemesi gereken adil para miktarı ne olmalıdır? Buradaki adil sözcüğü eğer oyun hiç durmadan tekrarlansaydı kasa ve oyuncunun “fit olma”ları anlamına gelmektedir.

Matematik bakımından yanıtı bulmak zor değildir. Sorun, yamta inanmanın, olanaksız değilse bile, zor olmasıdır. Nedeni şu şekilde açıklanabilir. İlk atmada yazı gelme şansı ikide bir olduğundan ilk atışta 2 dolar kazanma şansı, ikide birdir. Kazanmanın “tek” olanağı bu olsaydı oyuna giriş ücreti olarak 1 dolar ödemek “adil” olurdu. Ancak oyunun iki atışta bitme ve 4 dolar kazandırma şansının $1/4$ olduğu da düşünülebilir. Oyun bu elde “biterse”, “adil” ücretin yine 1 dolar olacağı aşikârdır. Gerçekte, bu düşünme yolu genellenabilir; eğer “yazı” ancak n’inci (buradan n seçeceğiniz herhangi bir tamsayıdır) atışta gelirse kazanacağım oyun için adil görüş ücreti ne olmalıdır diye sorarsam yanıt yine 1 dolardır. Ancak gerçek oyunda, yazı ne zaman gelirse gelsin hep benim kazanmama yol açmaktadır; yani her n değeri için. Öyleyse, “adil” giriş ücreti her bitiş olanağı için ödenecek 1 dolarların toplamına eşit olmalıdır, yani

$$1 + 1 + 1 + 1 + 1 + 1 + \dots$$

Burada noktalar işlemin hiç bitmeden süreceğini göstermektedir. Ne var ki bu sonsuz miktarda para demektir, toplam sonsuzdur ve tüm dünyadaki paraların tümünün “adil” bir oyun için yeterli olmadığı anlamına gelmektedir. Başka bir deyişle, oyuna girmek için bir milyar dolar istense de oyuncu kazançlıdır. Bütün servetinizi (bu, bir “milyar”dan az da olsa) bu oyunu bir kerecik oynamak için gözden çıkarırmıydınız? Matematik, hiç duraksamadan bu fırsatın üstüne atlamanız gerektiğini söylemektedir. Yanlış olan nedir?

Bir sorun şudur ki, gerçek yaşamdaki oyunlarda kasada, kazananlara ödemek üzere sadece sonlu miktarda para vardır. Örneğin, bizim kasamızda, 2^{20} dolara (bir milyon dolar-dan biraz fazlası) kadar ödeme yapacak para bulunduğunu düşünelim. O zaman yazı gelmesi için 20’den fazla atış gerektiren bütün oyunlar geçersiz ve yok sayılacaklardır. Böyle bir sıralama durumunda “bir kumar oyunu”na giriş için ödenmesi gereken adil ücret ne olmalıdır? Önceki argümanları kullanırsak daha önceki sonsuz toplamdaki ilk yirmi tane biri toplamak yeterlidir; bu da 20 dolar eder. Bu durumda ancak eğer ilk dört atış sırasında bir yazı gelirse siz kaybedersiniz, eğer beşinci veya daha sonraki ellerde yazı gelirse siz kazanırsınız ve bir milyon dolar kazanmanız bile olasıdır. Buna göre bu oyun fena da görünmüyor, değil mi? Sez-gimiz bizi yine yanıltıyor mu? Belki öyle, ancak şu sonsuz toplamı algılamak hâlâ biraz zor görünüyor. Bernoulli’nin zamanında da öyleydi. O dönem, bu sonsuz kavramı için sağlam bir matematiksel anlayış olmadığı bir dönemdi ve sonuç bir çok tartışmaya konu olmuştu.

Bunun ötesinde, bir başka karmaşa daha vardı. Şöyle ki, gerçek yaşamda aklımız, sonsuz küçük olasılıkla sonsuz miktarda para kazanma şansını, fazla çekici bulmuyor, matematik bu kazanma olasılığı konusunda ne derse desin. Eğer oyuna giriş ayrıcalığı pahalı ise, bu daha da geçerli oluyor. Örneğin, bir milyon dolar kazanma şansının milyonda bir olduğu bir piyangoyu ele alalım. Katılım için 1 dolar “adil” bir bedeldir ve çoğu insan katılmaktan mutludur (çok daha düşük olasılıkla çalışan Eyalet Şans Oyunları siste-

minde bu, inandırıcı biçimde görülmektedir). Şimdi de bir milyar (10^9) dolar kazanma şansının milyonda bir olduğunu varsayalım. Bilet için adil bedel şimdi 1000 dolardır. Bu pi-yango da matematiksel olasılığa göre, bir evvelki ile aynı ölçüde “adil”dir. Ancak şimdi önemli miktarda para kaybetmenin hemen hemen kesin olması (1.000.000’da 999.999) olası alıcıların çok daha büyük bölümünü bu riske girmekten alı-koyacaktır. Para miktarı büyüdükçe bu etki daha da güçlenir. Örneğin milyonda bir şansla bir milyar dolar kazanmak için kim 100.000 doları (borç alabildiğini varsayarsak bile) tehlikeye atar? Halbuki bu son kumar, sırf matematiksel kazanma olasılıkları açısından son derece çekicidir.

Gördüğümüz gibi akıl bunları farklı yorumlamaktadır. Her türlü lüks ve kötü alışkanlığa yönelseniz de çok ufak bir bölümünden fazlasını harcayamayacağınız bir parayı, çok uzak bir ihtimalle kazanma şansı için bütün bir yaşam boyu sağlanabilecek parayı kaybetmek ödenecek çok ama çok pahalı bir bedeldir. Gerçek yaşamda hedefler yalnızca matematiksel kazanma olasılıklarının olumlu veya olumsuz olmalarına göre saptanmazlar. Eğer enflasyon başını alıp gitmezse 10^{90} dolar kazanma ile 10^9 dolar kazanma arasında pratik bakımdan hiçbir fark yoktur.

Para terazisinin öbür kefesinde, olasılıklar olabildiğince küçük olsa da, kumarda küçük bir miktar parayı tehlikeye atmaya hazır insanlar vardır. Buradaki düşünme tarzı şöyle olsa gerek: “Oyuna girmek için gereken az bir para bizi fazla etkilemez. Ama sonunda birisi kazanacaktır, bizim de herkes kadar, şansımız var!” Örneğin, eğer siz de bilinen reklam posta listesindeyseniz, geçmiş yıllar boyunca “100.000 dolar kazanmış olabilirsiniz!” türü birkaç mektup almışsınızdır. Bu şu demektir; bir şirket listesindeki her aileye bir numara göndermiş, kazanan sayıyı da önceden seçmiştir; bu belki de sizin zarfınızdan çıkan numaradır, ancak ikramiye-yi almak için mutlaka yanıt vermeniz gerekmektedir. Yanıt vermeye değer mi?

ABD’de bu tür “bedava” işlerle ilgili olan daha büyük girişimler ülkenin büyük bir bölümündeki evlere -10 milyon

ılımlı bir sayı olabilir- bu tür teklifleri kolayca postalayabilirler. Bu on milyon rakamını kabul edersek, o zaman sizin kazanma şansınız on milyonda birdir. Öyleyse ortalama olarak 100.000 dolar, bölü on milyon kazanma şansınız var demektir. O da tam 1 cent'tir. Bu para ise, oyuna katılmak için reklamcıya göndereceğiniz yanıtı yapıştıracağınız posta pulu masrafından çok daha azdır. Akli başında istatistikler her oynadığınızda (ortalama) 20 cent'ten fazlasını kaybettiğinizi, sadece aptalların böyle bir oyuna geleceğini bağırıp dururlar. Ancak siz bunu bir de kazanana sorun! Gerçekte, başvuru- rulan kişilerin ağırlıklı bir bölümü, bir hiç karşılığında bir şeyler verildiğine ve bunun da bütün kumarlar içinde en iyisi olduğuna inanarak, bu "bedava"lara şevkle katılırlar.

Verdiğimiz senaryo pratik yaklaşımın matematiksel bildirimlere tümüyle mantıksal nedenlerle üstün geldiği durumlardan birisidir. Bazı insanlar için günlük yaşamın sıkıcı tekrarından kurtulmak ve (genellikle kısa ömürlü olan) beklentisinin heyecanını yaşamak, gerçekten, bir posta pulu bedeli ödemeye değer. Öte yandan istatistik alanına giren konularda sağ duyunun hatalı sonuçlara vardığı ve bu hataların düzeltilecek yanının olmadığı durumlara da kolayca rastlanabilir. Bu tür yanlış anlamalardan en sık rastlanana, istatistikçilerin gururla "ortalamaya dönüş ilkesi" dedikleri ilkeyle ilgilidir. Bu ilke ilk olarak 19. yüzyılda, bir İngiliz beyefendisi olan bilimci Sir Francis Galton tarafından ortaya atıldı. Söylediği basit olarak şudur: Bir ortalama değer çevresinde kümelenmiş tümüyle rasgele bir olaylar serisinde bir olağanüstü olayı, büyük olasılıkla, (kura sonucu) sıradan bir olay izler. Böylece, çok uzun boylu babaların oğullarının, ortalama olarak biraz daha kısa boylu, çok kısa boylu babaların bir ölçüde daha uzun boylu çocukları olduğuna dikkat çekilmiştir. Bu doğru olmasaydı, ortalıkta bir sürü 30 metre ve 30 cm boyunda insanlar dolaşırdı.

ABD'de, özellikle spor meraklıları arasında "üniversite ikinci sınıf uğursuzluğu" denilen şey bunun en güçlü tezahürünün örneğidir. İlk sezonda inanılmaz etkileyici bir biçimde ortaya çıkan bir spor kahramanının, çoğu kez, görece düş ki-

rıklığı yaratan bir ikinci yılı olur. Bu olguyu beyzbol terimleriyle açıklarsak daha iyi belirtebiliriz. Bu rasgele bir seçim değildir; çünkü, istatistiksel veriler içinde gömülmüş olan beyzbol, bu tür yanlış anlamalar için ideal bir üreme ortamı sağlar. Bir sezonda maçların, örneğin, ortalama % 60'ını kazanması beklenen ve aynı ölçüde yetenekli top atıcı oyunculardan oluşan bir küme düşünelim. İstatistik, doğası nedeniyle (kuşkusuz) bu ideal durumun gerçek bir sezonda yer almasına izin vermeyecektir. Top atıcıların bazıları yeteneklerine göre saptanmış olan % 60 kazanma oranını haklı çıkaracak ölçüden daha iyi, bazıları da daha kötü bir oyun çıkaracaklardır. Özellikle, biri veya ikisi kazanma yüzdesini % 60'ın oldukça üstüne, % 80'e kadar çıkacaktır; bu, çok normal olan istatistiksel dalgalanmaların nerdeyse önlenemeyen bir sonucudur.

Ancak basın ve beyzbol sevenler buna nasıl bakacaklar? İstatistiksel dalgalanmalara değinecekler mi ? Doğaldır ki hayır! Bu birkaç spor şanslısı (en azından bir sezon için şanslı olan) üstün kahramanlar olarak göklere çıkarılacaktır. Arada bir bu betimleme haklı da olabilir, ancak ertesi sezon geldiğinde genellikle, ortalamaya dönüş ilkesi kendini gösterir. Bunun sonucunda, çok büyük bir olasılıkla bu aynı "süper kahramanlar" belirli ölçüde çok daha kötü sonuçlar alacaktır. "İkinci yıl uğursuzluğu" baş gösterecek ve kaçınılmaz olarak, spor eleştirmenlerinin lügatçesinde yerini alacaktır. Neden olarak da, akla gelebilen her türlü baskı veya süper kahramanlık sonrası yaşamın nimetlerinden aşırı yararlanma ileri sürülecektir. Son derece muhtemel olan "ortalamaya dönüş" açıklaması, fark edilmiş olsa bile, basın için çekici değildir. Bildiğim kadarıyla, ona spor sayfalarında hiç rastlanmamıştır.

Aynı "gerileme" ilkesi, ilerlemeyi yüreklendirmek bakımından övgüden çok daha etkili olduğu şeklinde de yanlış yorumlanır. Bunun nasıl yapıldığını görelim. Örneğin, herhangi bir girişim üstünde çalışan bir grup öğrenciyi ele alalım. Günler ve haftalar geçtikçe, çabalarının sonucunda yetenekleri de gelişecektir. Ancak (yine o korkulan istatistiksel dalgalanma-

lar nedeniyle) bu ilerleme öngörülebilin, düzgün bir biçimde olmayacaktır. Belirli herhangi bir test uygulandığında sadece iyi (veya kötü) şans sonucu, kapasitelerinin üstünde (veya altında) başarı göstereceklerdir. Burada yeteneklerden kastedilen şey, büyük sayıda bu tür testler sonucu alınan ortalama başarı düzeyidir. Testte daha başarılı olanlar, kuşkusuz, övgünün aslan payını alırlar. Artık aşına olduğumuz ortalamaya gerileme denilen istatistik yasası uyarınca da, daha sonraki bir testle kendi gerçek (daha düşük) kapasitelerine daha yakınlaşmış olacaklardır. İlk testte istatistiksel nedenlerle daha az başarılı olanlar ve bu nedenle eleştirilenler için ise tam tersi doğrudur. İstatistiksel dalgalanmaların gerçek doğasına aşına olmayanlar için, bütün veriler, başarının yükselmesini teşvik etmek konusunda eleştirinin övgüden daha etkili olduğuna işaret etmektedir. Disraeli daha kuşkucu olsaydı, kendi bakımından daha iyi olabilirdi.

Bununla yakından bağlantılı olan ve sporla ilgili yanlış bir kavram da “momentum” veya “sıcak dönem”dir. Böyle kavramların mutlaka tümüyle temelden yoksun olmayabilecekleri düşünülse de, bu olguya örnek olarak verilen olaylar, eylemin rasgele olmasından başka bir şey değildir. Daha basit olsun diye, berabere kalmaya izin verilmeyen spor dallarından (beyzbol ve basketbol iki güzel örnektir) birinde tipik bir sezondaki maçlara bir göz atalım. Yine işi basitleşmek için, herhangi bir ligdeki bütün takımların tam olarak aynı kapasiteye sahip olduklarını varsayalım. Bu demektir ki, paranın yazı veya tura gelme şansı nasıl eşitse, herhangi bir maçta A takımının veya B takımının kazanma olasılıkları aynıdır: Sezon boyunca oynanan maçlar için istatistik yönünden ne bekleyebiliriz? Bütün takımların kazanma-kaybetme sayıları birbirinin aynı mı olacaktır? Doğaldır ki hayır! Gerçekte maçların sonuçlarını yazı tura atmak yoluyla belirleyerek bir sezon oynamayı denemek sizin için ilginç olabilir. “Sezon” sonunda bir tane en başarılı takım, bir tane de en başarısız takım olacaktır. Spor yazarları da hiç kuşku yok takımlardan birinin başarısı ötekinin de başarısızlığı için, istatistik dışında, akla gelebilecek her şeyi ileri süre-

ceklerdir. Takımlar arasındaki yetenek farklılıklarının önemli bir etkisi olmadığını savunmuyoruz. Bizim savunduğumuz, en yetenekli takımın çoğu kez “şampiyonluğu” kazanmayı başaramayacağı; bunun nedenin de varsayılan kararlılık veya karakter eksikliği değil, sadece istatistiğin oynadığı kaçınılmaz rol olduğudur.

Yazı tura ligimizin tıpatıp yetenekli takımları arasında, her takım için (örneğin) 100 maç içeren bir sezonda başka ne gibi çarpıcı sonuçlar bekleyebileceğimize bir bakalım. Arka arkaya bir dizi maç kazanılacak veya kaybedilecektir. Momentumun etkisi budur. Örneğin, eğer son maçınızı kaybettiyseniz bundan sonraki n maçınızı, hiçbir suçunuz olmadan kaybetme olasılığınız, istatistiksel bakımdan 2^n ’de birdir. Eğer $n = 6$ ise, art arda yedi maç zincirinin hepsini sadece şans nedeniyle kaybetme veya kazanma olasılığı altmış dörde bir olur ve 100 maçlık bir sezonda böyle bir zincirin gerçekleşme olasılığı oldukça kuvvetlidir. Eğer maçlar kaybedilmişse takım “bir çöküntü içindedir” ve bundan nasıl çıkacağı konusunda endişelidir. Ama eğer maçlar kazanılmışsa takımın “arkasında momentum vardır” ve hatta bir “kazanma formülü keşfettiği” bile ileri sürülecektir. Ne var ki, sonunda, gerileme yasasının işe el atması ve bu çöküntü veya mutluluk dönemlerinin sona ermesi kaçınılmazdır.

Kuşkusuz bütün bunlarda istatistiksel dalgalanmalar dışında başka etkilerin rol oynayıp oynamadığını saptama olanakları vardır; ancak spor analizi yapanlar çoğu kez bunu pek dikkate almazlar. “Momentum”un güvenilirliğini saptamak için bir çalışma yapıldığında oyuncuların kendileri bile tümüyle yanlış sonuçlar çıkarırlar. Profesyonel basketbol oyuncuları arasında, yakın zamanda, çok aydınlatıcı bir istatistiksel araştırma yapılmıştır. Hem oyuncular hem de sporseverler, oyuncuların isabetli atışlarını kısa süreler içinde yaptıklarına; bir maç sırasında oyuncuların “sıcak” olduğu, attıkları her şutun bir sayı yaptığı bir dönemin olduğuna inanma eğilimindedir. Bu inanç o denli yer etmiştir ki, takımındaki oyuncular topu “eli sıcak” oyuncuya geçirerek bu etkiden gerçekten yararlanmaya çalışırlar.

Böyle bir etki gerçekten var mıdır? Cornell Üniversitesi'ndeki araştırmacılar bir profesyonel basketbol takımının 50 maçının ayrıntılı kayıtlarını incelediler. Oyuncuların kendileri, basket yapma olasılıklarının başarılı bir atış sonrasında, başarısız bir atış sonrasında göre % 25 fazla olduğunu düşündükleri halde, araştırmacılar tersinin doğru olduğunu saptadılar. Gerçekten de bir oyuncunun başarısız bir atıştan sonra basket yapma olasılığı başarılı bir atıştan sonrakine göre % 6'ya varan ölçüde daha fazlaydı. Demek oluyor ki istatistiksel dalgalanmalar uyarınca kaçınılmaz olan sıcak ve soğuk dönemler yalnızca tesadüflerin yarattığı duruma kıyasla biraz daha az etkileyici olmuşlardır. Ortada momentum denilen şey var olmadığı gibi, onun hayal edilen varlığı takımın genel başarısını belki de gerçekten olumsuz etkiliyordu. Bunun en olası açıklaması şöyle olabilir; tesadüfen art arda birkaç basket atan bir oyuncu kendisinin "sıcak" dönemde olduğunu düşünerek ya başka durumda girişmeyeceği daha zor atışlara kalkışıyor, ya da savunma oyuncuları tarafından daha dikkatli bir korunma altına alınıyor. Öte yandan birkaç başarısız atış yapan bir oyuncu ise yeniden güven kazanmak için, daha sakıncasız atış arayışında oluyor veya belki de, savunma oyuncularınca fazla yakın izlemeye alınmıyor.

Takımların kazanma ve kaybetme dönemleri için benzer bir durumun (aşırı güvenli hissetme bakımından) var olup olmadığı, bildiğim kadarıyla incelenmemiştir. Ancak buna karşın akla gelebilecek her istatistiksel dalgalanma karşısında spor yazarlarını bir açıklama bulmaya çalışmaktan hiçbir şey alıkoyamaz. Uzun süre rastlantısal süreçlerle karşı karşıya olmak daha çok kişinin bunların rastlantısal olduğunu fark etmelerine yol açmıyor. Okuyucu (veya yazar) onlara değer verse bile, istatistiksel incelikleri tartışmanın spor yazarı için bir satış potansiyeli yoktur.

İnsanlara, bazı olayların olası sonuçlarına dayanarak seçim yapmaları ile ilgili sorular sorulduğunda, mantığı nasıl bir yana bıraktıklarını göstermek genellikle çok kolaydır. Bu bağlamda, matematiksel yönden birbirinin aynı olan durum-

larda, sorunun soruluş biçimine göre, inanılmaz ölçüde farklı yanıtlar alınabilir. Örneğin, insanlara 3200 dolarlık kesin kazanma şansı ile kazanma şansı % 80, hiçbir şey kazanma şansı % 20 olan 4000 dolar arasında bir seçim yapmaları istendiğinde, araştırma görevlileri onların büyük çoğunluğunun emin kazanç olan 3200 doları seçtiklerini saptadılar. Eğer durum ters çevrilir ve seçimin 3200 dolarlık kesin kayıp ile % 80 olasılıkla 4000 dolar kaybetmek, %20 olasılıkla hiçbir şey kaybetmemek arasında yapılması istenirse yanıt neredeyse tümüyle terstir; yanıtlayanların % 90'ı bu durumda kumar oynamayı seçiyor ve bu yolla kaybetmeyi önleyeceğini umuyor. Tamamen metamatiksel bakış açısından, her iki durumda, iki seçim arasında fark olmamalıdır. Ancak anlaşılan odur ki gerçek dünyada istatistik pek önemli değil. Burada çarpıcı bir tablo ortaya çıkmaktadır: İnsanlar kazanç peşinde koşarken kaybetme riskini azaltmaya yöneliyorlar; ama kayba uğramamak için, matematiğin emirlerine kulak asmadan riske giriyorlar.

Disraeli'den yapılan alıntıyı en çok haklı çıkaran istatistikler "karmaşıklık faktörü" denilen şeyleri içeren istatistik türleridir. Bunlar genellikle belirlenmemiş karmaşıklıklar (genellikle fark edilmemiş, çoğu zaman da hiç bilinmeyen) içerirler ve matematiksel bakımdan doğru olan sonuçlara varmayı olanaksız kılarlar. Bunlar daha çok örnekleme hataları olarak düşündüğümüz şeylerde görülürler. Örneğin, bir bakımdan birbirleriyle kıyaslanacak iki grup insanın, sonucu çarpıcı biçimde etkileyecek başka özellikler bakımından "rasgele" olduklarından nasıl emin olabiliriz? Bu "yanıltıcı etkenleri" yok saymanın acı sonuçları bir iki örnekle aydınlatılabilir. Önce, her ikisinin de nüfusu 100.000 olan İşkent ve Uykukent gibi iki hayali kentteki yaşam ve ölümü ele alalım. Ölüm oranları kıyaslandığında, Uykukent'de yılda 1500 ölüm olduğu halde yılda 1000 ölümün olduğu İşkent'de cenaze işlerine bakanların daha az çalıştığı saptanıyor. Aşıkâr görünen sonuç, İşkent'in (bir nedenle) yaşamak için Uykukent'ten daha sağlıklı bir yer olduğudur. Başka ne olabilir? İstatistikler yalan söylemezler! Bu sırada, biraz da-

ha gayretli iki istatistikçi tuhaf bir şey fark ederler. Yukarıda verilen sayılara karşın, her yaş grubunda (yani 0-10 yaş arası çocuklar, 10-19 yaş arası gençler, yirmili yaşlarda olanlardan 100 yaşın üstündeki en yaşlı vatandaşlara kadar) her yıl İşkent'te Uykukent'ten daha fazla ölüm var. Bu da (aynı ölçüde aşikâr mı?) aynı verilerden, öncekinin tam tersi olan bir sonuç ortaya koyuyor.

Bilgisayar hatası mı var? Biri rakamları mı karıştırdı? Belli ki hayır; yeniden kontroller yapılıyor, bütün veriler doğru. Öyleyse sorun ancak bulguların yorumundan kaynaklanabilir. Yorumlardan birinin yanlış olduğu kesin. Kentlerin isimleri bize ipucu veriyor. İşkent yeni iş olanakları bol olan bir kent; bu nedenle daha çok genç ailelerin oturduğu bir yer. Buna karşılık Uykukent gençler için iş olanağı pek olmayan, daha çok emeklilerin oturduğu bir kent. Buradaki yanıltıcı etkenin yaş olduğuna şaşmamak gerek. İki kentteki yaş dağılımı çok farklı. Hemşehrilerinin çoğu emekli olan Uykukent'te ölüm oranının daha yüksek olması çok doğal; çevre sağlığı ne olursa olsun bu sonuç beklenir. Önemli olan nokta şudur: Karşılıklı yaş dağılımları hakkında bilgi yoksa toplam ölüm rakamlarından, çevresel sağlık etkenleri kapsamında hiçbir sonuç çıkarılamaz. Doğru yorumlama (eğer ortalıkta gözden kaçmış başka yanıltıcı etken yoksa), toplam ölüm oranı yanında yaşı da dikkate alarak yapılan yorumdur. Uykukent yaşamın tadını çıkarmak için, İşkent'ten daha sağlıklı bir kenttir.

"Yaş"ın yanıltıcı etken olduğu hakkında daha abes (ama daha komik) bir başka örnek de gayretli bir amatör istatistikçinin öyküsüdür. Bu kişi, okul derslerindeki başarıyı akla gelebilecek her tür etkenle karşılaştırarak sonunda başarı ile ayakkabı numarası arasında çok çarpıcı bir karşılıklı ilişki buldu. Bir dizi ilkokuldaki bütün çocukları standard bir testten geçirerek yadsınması olanaksız bir sonuca vardı: En büyük ayakkabı numarası olan çocuklar en yüksek notları alıyorlardı. Ancak daha sonra, ayakkabı numaralarının daha çok, yaşla karşılıklı ilişki içinde olduğunu keşfedince oldukça utandı. Çıkarılacak doğru sonuç hiç de

şaşırtıcı değildi: Daha büyük çocuklar, hem bilgi birikimi hem de ayakkabı numarası bakımından küçüklerden daha ilerdeydiler.

Bu oldukça aşikâr örneklerin işaret ettiği genel problem yine de çok ciddidir. Bir istatistikçinin belki de en zor işi test edilen örnekleme grupları arasında gizlenip gözden kaçmış yanıltıcı hiçbir etkenin olmadığından emin olmasıdır. Ashında böyle bir etkenin var olmadığından *kesinlikle* emin olmak genelde, olanaksızdır. Bunun en iyi örneği, akciğer kanserindeki ölüm oranları konusunda, sigara içmenin bir etken olabileceği düşünülmeden önceki dönemlerde yapılan araştırmalardır. O yıllarda araştırılan gruplarda çok farklı sayıda sigara tiryakisi bulunmasından kaynaklanan tümüyle yanlış birçok istatistiksel ilişkiler ve sonuçlar bulunmuştu. O dönemde, sigara içmenin sonuçları herhangi bir şekilde etkilemesinden kuşkulanmak söz konusu değildi. Şimdi geriye baktığımızda bütün o dönemin çalışmalarını önyargılı buluyoruz ve “yanıltıcı sigara içme etkeni”nden dolayı, tümüyle asılsız olduklarını söyleyerek reddediyoruz. Çok farklı ancak aynı ölçüde sakıncalı sonuçlara yol açan bir başka durum daha vardır; istatistik uzmanlığı olmayan kişilerin istatistiksel olayları bilmeden yanlış yorumlamaları. Bu tehlike, daha çok yapılan hatalar rastlantısal değil de sistematik olduğu zaman ortaya çıkar. Böyle bir durumda, örneğin, bir komitenin bazı üyeleri (yanlarında bir uzman istatistik danışmanı bulundurmada) hep birden aynı sonuca, verilerden çıkarılmayacak ortak bir sonuca varabilirler; bu nedenle de bir bilirkişiye danışmaya gerek duymazlar. Politik bağlamda bu, eski zaman vergi mükellefinin parasının yerinde harcanmamasından da kötüdür. Buna bir örnek (neyse ki politik sonuçları bulunmuyor) çoğu kez sorulan şöyle bir sorudur: “Bir odada bulunan insanların en az ikisinin doğum gününün aynı olması için oda da en az kaç kişi olmalıdır? Doğru yanıt 23’tür; ama istatistikçi olmayan sıradan kişilerin çok büyük bir çoğunluğu bu sayının inanılmaz ölçüde küçük bir sayı olduğu kanısındadırlar (50 ila 70 arasındaki tahminler çoğunluktadır).

Bu türden öznel sistematik hatalar, bazen, kamuyu ilgilendiren politikalarda ciddi sonuçlara yol açarlar. Bu konuda yakın zamanda yer alan bir örnek, küçük topluluklarda ortaya çıkan ender görülen hastalıklarla ilgilidir. Bu sorunun iki ayrı yönü vardır. İlk olarak hastalığa yakalanma olasılığı farklı bölgeler için eşit olsa bile, az sayıdaki ender hastalık vakalarının, yaklaşık olarak aynı nüfusa sahip kent ve kasabalarda eşit olarak dağılması beklenemez. “Poisson dağılımı” olarak bilinen yasanın bir sonucu olan doğal istatistiksel dalgalanmalar bazı bölgelerde olayların kümelenmelerine yol açar, bazılarında ise hiçbir vaka görülmez. Örneğin, belirli bir hastalıkta, toplum başına, yılda ortalama iki ölüm düşüyorsa, Poisson dağılımı bize (belirli bir yılda) toplulukların % 13’ünde hiçbir ölüm olmayacağını, % 5’inde beş veya altı kadar ölüm olacağını söyler. Bu, yalnızca istatistiksel nedenlerden dolayı böyledir. Ancak işe karışan bir başka şey vardır; eğer birden fazla hastalık hakkında istatistiksel veri toplanmışsa, o zaman, aynı doğum günü yanlış kavramı buraya da el atarak, durumun doğru değerlendirilme olasılığını azaltır. Bununla kastedilen şudur; çok sayıda ve çeşitli türden hastalık vakalarının görüldüğü bir toplum; tamamen rastlantısal olarak da, “akıllı sıradan insan”ın beklediğinden çok daha sık ortaya çıkabilir. Bu durum çok tehlikelidir; çünkü insanlar risk değerlendirmesinde yanılırlarsa, hatalar birbirlerini götürmeye yönelirler ve fazla zarar vermezler. Ancak eğer hatalar, ortak doğum günü ve Poisson dağılımı olgularında olduğu gibi, büyük ölçüde, sistemli önyargı hataları ise o zaman kısıtlı olan kaynaklar bizi yanlış yönlendirilmiş, tümü hayal ürünü olan tehlikelerden korumak için harcanır, bu da ciddi kayıplara yol açar.

Yeni bir bölüme geçmeden önce, son olarak istatistiğin en çarpıcı yanlış kullanımına, bazen gizli mesaj olgusu denilen yönüne de değinmeliyim. Şu tür bir şey: Çok çok eski bir yapıda uzaylılar bizim gibi sonradan gelecek nesillere, çözülmeyi bekleyen gizli bir mesaj bırakmıştır. Giza’daki Büyük Piramit bu tür “mesajlar” için en gözde avlanma yeridir. Ak-

lınıza gelebilen her türlü uzunluk ve açı ölçülecek sonra da bu ölçümlerle başka dikkate değer sayılar arasında, örneğin, pi veya dünyanın çapını veya ayın uzaklığını (veya güneşin veya yıldızların, hiç fark etmez) bu uygun birime göre ifade ederek bulduğumuz sayılar arasında ilişki kurulacak. Ondalık noktasını kaydırmaya, doğal olarak, izin vardır. Çünkü bu, uzaylıların gizemli doğalarını daha iyi değerlendirmemize olanak sağladığı gibi gerçekten rastlantısal olan olaylar arasında çok çarpıcı “rastlantılar” bulmak için de daha iyi olanaklar sağlar.

Böyle bir rastlantı bulduktan sonra, “Bu sütunun yüksekliğinin şu baklava biçimindeki odanın boyutuna oranı, pi’nin kareköküne hemen hemen eşit. Giza’nın yapıldığı dönemde Mısırlılar pi’yi bu kadar dakik olarak bilmiyorlardı. Bu bilgiyi nereden almış olabilirler?” şeklinde fikirler yürütmeye koyulursunuz. Burada ima edilen uzaylılardır ve fazla üstelemeye gerek kalmadan işe basın da el atınca arkadan sansasyon gelir.

İstatistiğin yanlış kullanımının bu türünde başarının sırrı önce gerçek bir “anamlı” sayılar üretme bahçesi oluşturmaktır. Bunlardan binlercesini üretmek için Güneş Sistemi’ne bakmak yeterlidir: Gezegenlerin boyutları, kütleleri, yoğunlukları ve bunlar arasındaki akla gelebilecek her türlü oranlar. Arada bir de pi ile veya onun basit kuvvetleri veya kökleriyle bir çarpım karıştırın, artık hazır sayılırsınız. Gizli mesaj oyununun kuralları ondalık noktasını değiştirmenize izin verdiği için ne de olsa belirli bir anlamı olan sayının 100 kat büyüğünü veya küçüğünü bulmak sayının kendisine eşit bir sayı bulmak kadar etkileyicidir. Kendi evinizdeki boyutlar arasında bile gerçekten etkileyici bir rastlantı bulmamız garanti edilir; evinizin yapılmasında uzaylıların bir parmağı olduğu fikrine basın kolayca katılmasa da son bir sır daha (reklam bakımından): Gidip kendinize eski çağlardan kalma uygun bir anıt bulun, ne kadar eski olursa o kadar daha etkileyici olur. Şansınız açık olsun!

Bu sayısal rastlantıların sokaktaki insanı, sık sık, doğa üstü bir şeylerin var olduğuna ikna etmesinin nedeni, bin-

lerce “anlamalı sayılar” listesinin hiçbir zaman açıklanmamış olmasıdır. Bütün dikkatler, keşfedilmemiş olan rastlantı üzerinde yoğunlaşır sanki eldeki tek aday odur. Olanakların sonu yoktur. Örneğin, Şikago’daki Sears Tower’ın boyunu (dünyanın en yüksek binasıdır) New York’daki Woolworth binasının (yapıldığı 1913 yılında dünyanın en yüksek binasıydı) boyuna bölerseniz sonuç 1,836’dır. Bu bir protonun kütlesini bir elektronun kütlesine bölerek elde edeceğiniz sayının binde birinin ta kendisidir. Bunu da bir düşünün!

V. Bölüm

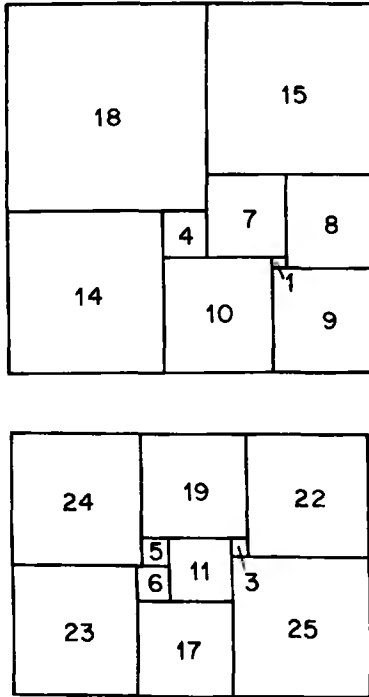
En Kusursuz Kare

Terasınızı mahallenizde, belki de bütün dünyada görülmemiş biçimde, sadece görülmemiş değil yakın zamana kadar bilinmeyen bir biçimde karo taşlarıyla döşeyen ilk siz olun. Konuklarınızla konuşacak şey bulamadığınız bir günde çok ilginç konuşma konusu olur (tabii, eğer onun büyüleyici öyküsü hakkında en azından biraz bilginiz varsa). Nedir bu öykü? Bu taş döşeme düzeni nasıl bir şey? Bu kadar heyecan niye? Bu soruları yanıtlamak için, en azından 1920'lere belki de daha öncesine gitmemiz gerekir.

Bir dikdörtgeni hepsi farklı boyutlarda olan karelere bölme sorusunun matematik literatüründe ilk kez 1925 yazında görüldü. Hatta o zaman iki belirli örnek de verilmişti. Bunlar Şekil 5'te, kenar uzunlukları tamsayılarla işaretlenmiş elementer karelerle gösterilmiştir. Büyük dikdörtgenleri küçük *dikdörtgenlere* bölme probleminin bir kaç yıl önce söz konusu olduğu doğrudur, ancak kareye bölmeyle ilgili bilinen ilk referans budur ve kareler biraz daha özeldirler, bir anlamda nihai dikdörtgendirler. Öyleyse bu türden nihai problem de, herhalde büyük bir kareyi hepsi farklı büyüklükteki karelere bölmek olmalıdır. Bütün oluşturan karelerin hepsinin farklı olmasını gerektiren sınırlama çok önemlidir. Bu olmasaydı problem önemsiz olurdu; ben bile bir kareyi dört eşit kareye bölebilirim, ancak konumuz bu değildir.

"Kareyi karelemek" de denilen bu nihai problemin kökeni biraz bilinmezlik içerir. Bu yüzyılın başlarında İsviçreli ünlü bulmaca ustası Sam Lloyd bir yama-işi yorgan problemi ortaya attı, çözüm bir kareyi daha küçük karelere bölmeyi

gerektiriyordu ancak karelerin *hepsinin farklı* olması gerekli değildi. Hepsinin farklı olmasının gerekliliği “kareyi kareleme” probleminin can alıcı noktasıdır; çünkü Sam Lloyd’un yorgan bulmacası döneminde hepsi farklı karelere ayırmanın mümkün olup olmadığı bile bilinmiyordu (küçük karelerin sayısı konusunda bir kısıtlama olmadığı halde). Gerçekte, 1930’da çıkan ve problemin yayınlanmış ilk referanslarından birisinde bir öneri ileri sürülüyordu (Moskova Üniversitesi’nden Profesör N. N. Lusin göndermişti), bir kareyi, her biri diğerlerinden farklı boyutta olan, sonlu sayıda kareye bölmenin olanaksız olduğunu söylüyordu.



Şekil 5.

Bu nedenle “kareyi kareleme” problemini çözme girişiminde vurgulanacak ilk şey bir çözümün var olup olmadığı-

nın genel bir kanıtını vermeye çalışmak olmalıdır. Gerçekte böyle bir kanıtlama hiçbir zaman yapılamadı. Bu yönde ilk adım Cambridge Üniversitesi'nden dört matematikçinin gerçek bir örnek vermesiyle atılmıştır. Kareyi kareleme probleminin çözümü olan ve giderek ünlenen bu ilk "kusursuz" kare 1938'de bulunmuştu ve daha küçük 69 kareye bölünmüştü. Bu örneği ertesi yıl bir ikincisi izlemişti (bir Alman grubu tarafından bulunmuştu) ve bu örnek, gerçekte daha önce yayınlanmış olan ilk örnekten, Cambridge örneğinden, daha küçüktü; yani daha az sayıdaki küçük karelere, tam olarak 55 kareye, bölünmüştü.

Bu dönemde kusursuz kareler üretecek iyice tanımlanmış hiçbir yöntem yoktu, bu nedenle girişim büyük ölçüde emek ve "birazcık da şans" gerektiriyordu. Bu problemle ilişkili ama daha basit olan "dikdörtgen kareleme" yani dikdörtgenleri eşit olmayan karelere bölme probleminde, daha çok yöntemle dönük ilerleme kaydediliyordu. Bu bağlamda, verilen herhangi bir mertebedeki bütün dikdörtgenleri çizmek için genel bir yöntem bulunmuştu; burada "mertebe" dikdörtgenin bölündüğü karelerin sayısıdır; Yöntemi ayrıntılarıyla anlayamasak bile, problemi c-net denilen özel bir elektrik devresiyle ilgili olan eşdeğer bir probleme dönüştürmekten ibaret olduğunu söyleyebiliriz. Karelennen her dikdörtgenin bir c-netten, önceden saptanmış oldukça sıkıcı bir yöntemle elde edilebileceği gösterilmiştir. Bu yolla, olası en küçük kareli dikdörtgenlerin dokuzuncu mertebeden olacağı (yani dokuz kare içereceği) bunlardan da sadece iki tane olduğu gösterilmişti. Bu iki dikdörtgenin de eşit kenarlı olmaması (yani kare olmaması) ve bu nedenle de en kusursuz diyeceğimiz en küçük kusursuz karenin mertebesinin en az on olması büyük talihsizlikti.

Bu demektir ki 1925'te bilinen karelenmiş iki dikdörtgen-den birisi (Şekil 5'te, yukarda olan) olanaklı en küçük mertebeden bir karelenmiş dikdörtgendir. Kendisi her ne kadar kare değilse de (ancak 32 ve 33 kenar uzunluklarıyla kareye, baştan çıkaracak kadar yakın) en kusursuz kareyi aramak için genel ama oldukça verimsiz bir yol bulmuş oluyo-

ruz. Her mertebeten *bütün* dikdörtgenleri bulup, onların bir kare olup olmadıklarını kontrol etmek. Bu kulağa hoş geliyor, ancak bir sorun, hem de büyük bir sorun var. Herhangi bir mertebeden olan bütün dikdörtgenleri bulmak için gereken zaman ve çaba, mertebenin sayısı arttıkça, çok büyük bir hızla artmaktadır, 9, 10, 11, 12...vb. Bilgisayar öncesi 1940'lı yıllarda sadece 13'üncü mertebeye kadar olan kareli dikdörtgenlerin bütün takımı biliniyordu ve (ne yazık ki!) bunların hiçbirisinin kenarları eşit değildi. Bu nedenle en kusursuz kare 14 ve 55'inci mertebeler arasında bilinmeyen bir yerdedi.

1950'lerde elektronik bilgisayarların ilerlemesiyle c-netlerini inceleme işlemleri (ve bu yolla kareli dikdörtgenlerin bütün takımlarını bulma işi) doğal olarak, makinelere bırakıldı. 1960 yılına gelindiğinde Hollandalı bir grup, bilgisayar hızından yararlanarak 15'inci mertebeye kadar (yani en fazla 15 kareden oluşmuş) olan kareli dikdörtgenleri listelemeyi başardı, ama yine de bunların hiçbirisi kusursuz kare değildi. Yapılan işin boyutları konusunda bir fikir vermek için, 15'inci mertebeden basit kareli dikdörtgenlerin sayısının 2609 olduğunu söylemek yeterlidir. Burada kullanılan "basit" sözcüğü dikdörtgenin içinde, karelerden oluşmuş başka bir dikdörtgen olmadığı anlamına gelmektedir. Eğer karelerden oluşmuş bir dikdörtgen varsa o zaman kareli büyük dikdörtgene "bileşik" diyoruz. Tanım uyarınca, Şekil 5'teki küçük dikdörtgen basittir. Ancak, eğer biraz düşünürseniz, en küçük kareli karenin (yani en kusursuz karenin) basit olması gerekmez, ama olabilir de.

"Basit" kareli dikdörtgenler üzerinde durma nedenimiz şudur: Her basit kareli dikdörtgenden, onunla ilişkili sonsuz sayıda bileşik dikdörtgenler ailesi elde edilebilir, bu nedenle de önemli herhangi bir entellektüel probleme yol açmazlar. Örneğin, verilen herhangi bir kareli dikdörtgenden, basit veya bileşik olsun, daha büyük bir bileşik dikdörtgen oluşturulabilir. Ona, kenarı ilk dikdörtgenin kenarlarından birine eşit bir kare eklemek yeterlidir. Dahası, yeni bileşik dikdörtgen oluşturmak için kullanılan bu yöntemin istenildiği ka-

dar sürdürebileceği açıktır. Ancak bu bileşik dikdörtgenlerin hiçbirinin kare olamayacağı da aynı ölçüde açıktır (çünkü bunlar var olan bir dikdörtgene kareler eklemekle elde edilmişlerdir). Bu, en kusursuz kareyi ararken bileşik dikdörtgenleri unutabileceğimiz anlamına mı gelmektedir? Ne yazık ki hayır! Çünkü *bütün* kareli dikdörtgenler yukardaki türden değildir ve bileşik kusursuz kareler mümkündür. Bu, arayışımıza yeni bir sorun eklemektedir. Genel c-net yöntemi sadece bütün basit kareli dikdörtgenleri oluşturmaktadır, “düşük mertebeli” bir bileşik en kusursuz kare c-net’in gözünden kaçabilir. Bu pek olası görünmese de (bir kanıt olmadığı halde en kusursuz karenin basit olacağı izlenimi yaygındı) zamanı geldiğinde düşünülmesi gerekecektir.

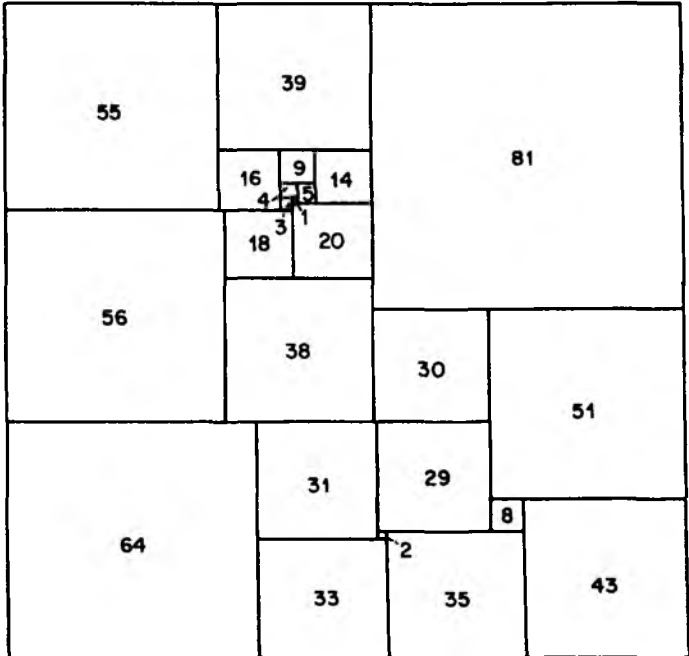
Giderek artan bilgisayar hızını ve c-net yöntemini kullanarak 1960’ların başında 18’inci mertebeye kadar olan bütün basit kareli dikdörtgenler üretilmişti. Basit kareli dikdörtgenlerin sayısının tam listesi aşağıda verilmiştir:

Mertebe	Sayı	Mertebe	Sayı
9	2	14	744
10	6	15	2609
11	22	16	9016
12	67	17	31427
13	213	18	110384

150.000’den fazla kareli dikdörtgen var ve bunların bir tanesinin bile kenarları eşit değil! 1962’de liste 19’uncu mertebeye yükseltildi; aralarında tek bir kusursuz kare yine yoktu. Bu nedenle artık en kusursuz karenin (eğer beklendiği gibi basitse) daha küçük en az 20 kare içereceği açıkça görülüyordu.

Gerçekte bundan biraz daha fazlası da biliniyordu; çünkü İkinci Dünya Savaşından sonra, savaş öncesinin 69 ve 55 mertebelerinden cesaret alan hevesli amatörler daha az metodik olan çalışmalarla bu işe el attılar. Bu sistemli bir şekilde yapılmadığı halde ve belki de bir bilim olduğu kadar

bir sanat olarak yapıldığı halde, başarılı da oldu, bu başarı giderek (gerçek kusursuz karenin keşfi ile) en kusursuz karenin sahip olabileceği olanaklı en büyük mertebeyi aşağı çekti. Bu bağlamda en dikkate değer keşif 1948'de T. H. Willcocks tarafından yapıldı. Kendisi İngiltere'nin Bristol kentinde, bir Bank of England çalışanıydı. Satranç meraklısı bir amatör matematikçi olduğu için eğlence türü matematikle de etkin biçimde ilgileniyordu. "Kareyi kareleme" problemi ve bu konuda daha önce başarılmış sonuçlar hakkındaki bilgisini bu ilgiye borçluydu. Ancak giderek artan karelenmiş dikdörtgenlerin listesiyle ilgilenmek yerine kendi çizimlerini üretip depoladı. Bunlardan, kendi icadettiği çeşitli teknikleri kullanarak sonunda birkaç kusursuz kare keşfetmeyi başardı; bu karelerin en küçüğü 24'üncü merte-



Şekil 6. En küçük bileşik kusursuz kare.

beden bir bileşik kusursuz kareydi. Bu başarının boyutu ancak şimdi geriye dönüp iyice baktığımızda tam olarak değerlendirilebilir. Willcocks'un 24'üncü mertebeden bileşik kusursuz karesi günümüzde bilinen en küçük mertebeden bileşik kusursuz bir karedir. Bundan başka, en kusursuz karenin, sonunda keşfedildiği 1978 yılına kadar bilinen en küçük mertebeli tam kare, yine bu kareydi. Bu nedenlerle burada gösterilmeyi gerçekten hak etmektedir ve aşağıda gösterilmiştir.

Ancak şimdi, 1964 yılına dönelim ve nihai en küçük mertebeli tam kare arayışını sürdürelim. Daha küçük en az 20 kare içeriyor ve Willcocks'un inanılmaz keşfi uyarınca da, 24 kareden daha fazlasını içeremiyor. Fakat neredeydi ve neye benziyordu? Dikdörtgenleri kareleme konusunda yapılan genel çalışmalar bir durma noktasına gelmişti, çünkü 1964'te var olan bilgisayarlar 20'li mertebeler için bütün çözümleri, süre ve masraf bakımından kabul edilebilir ölçüde üretecek kapasitede değillerdi. Tam kareler arayışında yepyeni bir yöntemin keşfi önemli bir adım atılmasına neden oldu.

Yeni yöntem, "eksik karelenmiş kareler" denilen, tek bir dikdörtgen dışında, eşit olmayan karelere bölünmüş kareler hazırlamayı içeriyordu. Bu eksik kareler elektrik devrelerine benzetme yoluyla geliştirilen genel bir yöntemle kolayca çizilebiliyorlardı. Bu eksik kareleri hazırladıktan sonra hızla büyüyen karelenmiş dikdörtgenler listesi taranarak eksik karedeki "delik"le kenar uzunlukları oranı aynı olan bir dikdörtgenin var olup olmadığı araştırılıyordu. Var ise yeni bir tam kare bulunmuş demektir. Bu yolla bulunan tam karelerin, oluşma yöntemleri nedeniyle, basit olmayıp bileşik olduklarına dikkatinizi çekerim. Bu yeni yöntem, böylece, daha önceki basit tam kareleri bulma yöntemini de tamamlamış oluyordu.

İlk olarak 1963'te uygulanan bu yöntem en küçüğü 25 olmak üzere 20'den fazla küçük mertebeli (29'dan küçük) yeni bileşik tam karenin bulgulanmasına yol açtı. Yöntem bilgisayar için programlanmıştı ve Şekil 6'da görülen kareyi aşacak kareyi bulmak için çok uzun bilgisayar saatleri harcan-

dı. Yine de bütün bu çabalara karşın mertebesi 24'ten küçük (Wilcocks'un kâğıt kalem kullanarak bulduğu) olan bir kare bulunamadı. Ancak bu yöntem sayesinde orta ve yüksek mertebeli bileşik tam kareler oldukça kolay (hatta kâğıt kalemle) bulunur oldular.

Bunun sonucunda, daha öncekileri var olup olmadıkları bile sorgulanan daha yüksek mertebeli tam karelere artık pek önem verilmiyordu. Onlardan on binlercesini üretebiliyorduk; 33 veya daha küçük mertebede 2000'den fazla bu tür kare üretilmiş bulunuyor. Yine de Willcocks'un ki en küçük olmayı sürdürüyor, ondan sonra 25'inci mertebeden iki kare ve 26'dan 13 kare geliyor.

1960'ların sonuna doğru ilgi tekrar basit tam karelere yöneldi. Bunlar, bildiğiniz gibi, daha küçük bir karenenmiş dikdörtgen içermiyorlar. O döneme gelindiğinde birkaç tane basit tam kare (31'e kadar inen mertebelerde) keşfedilmişti ancak kullanılan yöntemler, genişletilerek daha genel bir yöntem bulmaya uygun değillerdi. 1967'de Kanada'daki Ontario kentindeki Waterloo Üniversitesi'nde John C. Wilson doktora tezinde basit kareli kareler üretmek için kullanılacak ilk genel yöntemi ortaya koydu. Bu yöntem herhangi bir mertebede olanaklı olan *bütün* kareli kareleri ürettiğini söylemiyordu, ancak bu tür karelerin sayısında kısa sürede büyük artışa yol açtı. Gerçekte, Wilson'un grafik çizimler içeren teknikleri bilinen en küçük basit tam karenin mertebesini 25'e indirdi. Tam olarak söylemek gerekirse, mertebesi 25 olan 51 ve 26 olan 24 farklı basit tam kare buldu. Ancak Willcocks'un 24'üncü mertebeden karesi inatla yenilmezliğini koruyordu. En kusursuz kare bu olabilir miydi?

1978'e gelindiğinde durum pek değişmemişti ve çalışmalarda bir durgunluk var gibiydi. Bilinen en düşük mertebeli tam kare hâlâ T. H. Willcocks'un bileşik karesiydi. 25'inci mertebeden 10 kadar tam kare biliniyordu (8 basit, 2 bileşik) ve 26'ncı mertebeden 41 (28 basit, 13 bileşik). Bu 26'ncı mertebeden 13 bileşik kareden birinin içinde iki ayrı küçük karenenmiş dikdörtgen vardı ve bunun bilinen bu tür en küçük kare olduğu sanılmaktadır. Bu arada, bilgisayarların

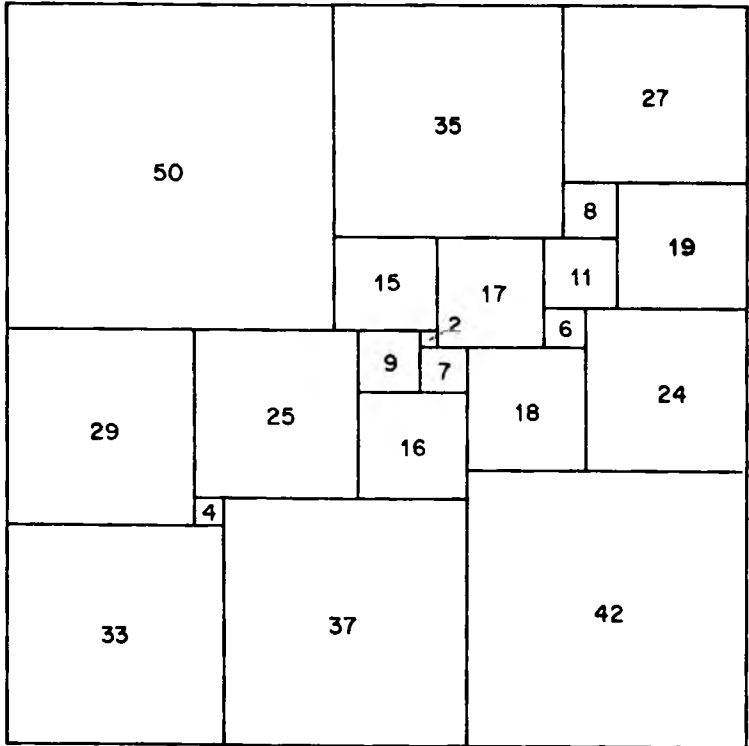
verimliliği artmış ve 20'nci mertebeden tam dikdörtgenlerin hepsi bulunmuştu; ancak kenarları eşit olana yine rastlanmamıştı. Bütün bunlar 21 ila 23'üncü mertebeden tam kare olup olmadığı sorusuna bir yanıt getirmemişti.

Yanıt sonunda, 22 Mart 1978 gecesinde bir yıldırım çarpmışcasına bilgisayar ekranında parladı. Yer ise Hollanda'nın Enschede kentindeki Twente University of Technology idi. Dr. A. J. Duijvestijn, yeni ve çok gelişkin bir bilgisayar programı aracılığıyla "kaba kuvvet" yöntemini zorlayarak, olanaklı bütün basit tam kareli 21'inci mertebe dikdörtgenleri bulup kenarlarının eşit olup olmadığını araştırıyordu. 21'inci mertebeden binlerce dikdörtgen bulunmuştu; kenarlarının eşit olup olmadığının test edilmesi sürüp giderken birden ortaya çıktı!; 21 elementli o güzel tam kare! Şekil 7'de verdiği-miz bu karenin kenar uzunluğu. 112 birim; en büyük bileşeni 50×50 bir kare, en küçük ise 2×2 . Kırk yıl süren çalışmalar sonucunda en küçük tam kare bulunmuştu.

Ancak problem tam olarak çözülmüş değildi. İlk olarak, tek çözüm bu muydu? Yani, bilgisayarın bulup çıkarmayı sürdürdüğü binlerce tam dikdörtgen içinde 21'inci mertebeden başka tam kare var mıydı? Uzun saatler boyu süren dikkatli incelemeler sonunda soru yanıtlandı. Bütün 21'inci mertebeden kareli dikdörtgenlerin elde edilmesinden sonra basit bir tam kare olanın sadece bu olduğu ortaya çıktı. Gerçekten de tekti. Ancak, aynı zamanda da en kusursuz kare miydi? Duijvestijn sadece basit tam kareleri saptayan bir teknik uyguluyordu. Bu konuda bir fikri olan herkes en kusursuz karenin basit olduğu kanısında olsa da, hep bir kuşku vardı. Acaba daha küçük bir bileşik tam kare olabilir miydi? Neyse ki, bu kuşku uzun sürmedi. Aynı yıl içinde daha sonra en küçük bileşik karenin en az 22 bileşeni olması gerektiğinin bir kanıtı bulundu. Şekil 7'deki Duijvestijn'in karesi gerçekten de en-kusursuz karedir. Geometri dünyasında gerçekten benzersiz bir konumu vardır. Aynı sayıda veya daha az sayıda karelerden oluşan başka hiçbir kare, hiçbir zaman bulunamayacaktır. Sonunda, 1982'de, mertebesi 24'ten küçük olan bileşik tam kare olmadığı ve 24 bile-

şeni olan bir ve yalnızca bir bileşik tam kare, yani Şekil 6'daki Wilcocks'un karesi, olduğu kanıtlandı.

Daha küçük mertebeli tam kareleri sınıflandırma işi, bu kitabın yazıldığı dönemde henüz tamamlanmış değildi. Özellikle, basit tam karelerin tam listesi tamamlanmamış, bu süreci hızlandırıcı verimli bir yöntem bulunmamıştır. Bileşik tam karelerin üretilmesi daha düzenli olarak ilerlemekte, ancak bunda bile, 24, 25, 26 gibi birkaç küçük mertebeden daha büyük herhangi bir mertebede, olanaklı bütün örnekleri bulmak için gereken bilgisayar süresi hâlâ çok uzundur.

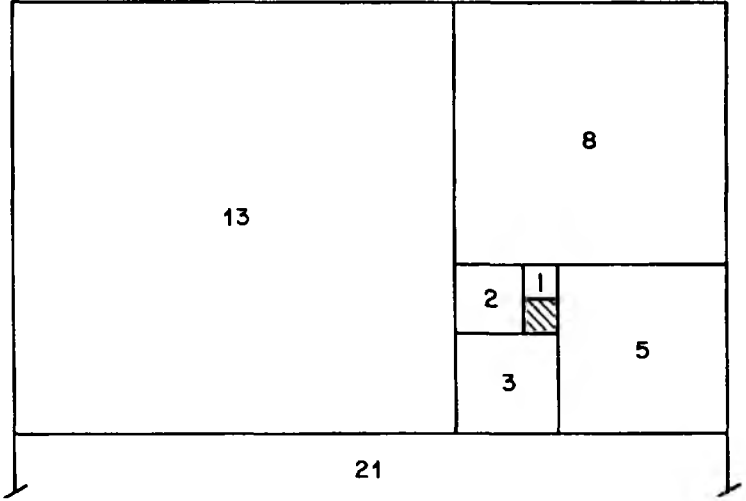


Şekil 7. En kusursuz kare.

Bizim bakımımızdan öykü tamamlanmıştır. Hem en küçük basit tam kare olan 21'inci mertebe kare (Şekil 7) hem de en küçük bileşik tam kare olan 24'üncü mertebe kare (Şekil 6) bilinmektedir. Her ikisi de, o mertebelerdeki yegane örnek olmak anlamında, tektir. Bu şekillerden birinden çıkarılan bir kalıp bir teras zeminini düzenlemekte kullanılabilir. Dünyanın en yetenekli metamatikçilerinin (amatör veya profesyonel) 40 yıllık ortak çalışmalarının sonucu, sizin yapacağınız bir anma girişimini, kuşkusuz, hak etmektedir. Teras düzenlemesi başlasın!

En kusursuz karelerle vedalaşmadan önce bu karelerin var oluşlarının, ilgili bir başka problem için çok basit bir çözüm bulunmasına da yol açtığını bilmek ilginç olacak. Bu problem, sonsuz bir düzlemi, hiçbirini diğerine eşit olmayan karelerle döşemenin mümkün olup olmadığını soruyor. Problem, kenar uzunlukları, 1, 2, 3, 5, 8, 13... olan, firdönen Fibonacci karelerinden oluşmuş bir sarmal yoluyla, Şekil 8'de görüldüğü gibi hemen hemen çözülmüş gibidir. Sarmal durmadan sürdürülürse sonsuz düzlem, sonunda, daha önceki bir bölümde tartıştığımız Fibonacci dizisinin elementlerini kenar uzunluğu olarak alan karelerle kaplanacaktır. Ancak bir sorun vardır. Fibonacci dizisi iki tane birle başlamaktadır. Bu demektir ki döşeme düzeni birbirinin aynı olan iki kare (Şekil 8'de 1 ile gösterilen ortadaki en küçük kare) içermektedir, ancak problem birbirlerinden farklı kareler istemektedir. Karelenebilir karelerin var olup olmadığının bilinmediği, 40 yıldan fazla bir süre öncesinde olsaydı, hem çok yakın hem de çok uzak olan bu noktada durdurulurduk. Ancak şimdi bu iki eşit kareden birini, bilinen binlerce tam kareden birisi gibi bölerek parke döşeme problemini çözebiliriz.

Sizi şimdi cesaret kırıcı bir öneriyle başbaşa bırakabilir miyim? Kareyi başarıyla karelere böldükten sonra, "küçük küplendirmeye ne dersiniz? Yani bir küpü, herhangi ikisi aynı boyutta olmayan daha küçük küplere ayırmak. Özellikle en kusursuz küpün görünümü nasıldır? Şansınızdan yanıt bilinmektedir. Bir küpü, boyutları birbirlerinden farklı olan,



Şekil 8.

sonlu sayıda küçük küplere ayırmak olanaksızdır. Bunun ispatı geometrinin en güzel ispatlarından birisidir. Eğer hayal kırıklığına uğradınızsa üzülmeyin. Taş döşeme probleminin üç boyuta uyarlaması, bildiğim kadarıyla henüz çözülmedi. Açıkça ifade edilişi şöyledir: Bütün üç boyutlu uzay, boyutları birbirlerinden farklı olan küplerle doldurulabilir mi? Düşünmekte olabildiğince özgürsünüz.

VI. Bölüm

Eukleides'in Beşincisindeki Sorun!

Doğruyu söylemek gerekirse çok kişi için en popüler yazarlar listesinde Eukleides'in adının yeri yoktur. Biz onu hâlâ lise geometrisindeki sorun ve sıkıntılarımızla ilgili olarak hatırlarız ve bu tür anılar da onu hoşgörmemize pek izin vermezler. Ancak yine de Eukleides'in bilimsel incelemelerini içeren ünlü eseri yaklaşık iki bin yıldır okutulmaktadır. Günümüzde bile onun ilk birkaç bölümü, biraz değiştirilmiş şekliyle bütün okul geometrisinin temelini oluşturmaktadır. Bu nedenle, hem kendisi hem de eseri kısa bir süre için de olsa, sanırım dikkatimizi hak etmektedir.

Eukleides'in geometrinin "baba"sı olduğu, "oyunun kuralları"nı ilk onun belirlediği şu veya bu şekilde herkesce bilinir. Ancak bu kurallar konusunda yüzyıllar boyu süren tartışmalar ise fazla bilinmez. Bu tartışmaların sonunda, yepyeni geometrilerin gelişmesine yol açtığı ise daha da az bilinir. Bu yeni geometriler yirminci yüzyıl fiziğinin, özellikle de genel görecelik olarak bilinen zaman ve uzay biliminin ortaya çıkmasına çok büyük katkısı olmuştur. Bütün bunlar, büyük bir titizlikle beş "aksiyom" (yani doğruluğu aşikâr olan şey) tanımlayarak, uzayın ve ölçmenin özelliklerini bir bilim şekline getirmeye uğraşan eski geometricilerin çalışmalarından çok farklıydı.

Doğruluğu aşikâr olan bu gerçekler tam anlamıyla böylediler, doğru oldukları öyle aşikârdı ki sorgulanmaları söz konusu olamazdı. Onlar "geometrinin kuralları" olarak ifade edilmeden önce herhangi bir şeyi ispat edecek bir referans çerçevesi olmadığı için formal bir anlamda ispat edilemezlerdi. Yine de Eski Yunan geometricileri için onların

birbiriyle çelişmeyen kurallar dizisinden daha fazla bir anlamı vardı; onlar gerçek uzayın gerçek özelliklerini temsil ediyorlardı; uzayın gerçekliği ne ölçüde aşıkârsa onlar da o ölçüde aşikârlardı. Şimdi bu kurallara göz atarak öbürlerinden daha az aşikâr olabilecek bir “gerçeklik” olup olmadığını görmeye çalışalım. Birinci aksiyom farklı herhangi iki noktayı birleştiren sadece bir tek düz doğru olduğunu söylüyordu. İlk sorumuz “Düz doğru ile ne kastediyorsunuz?” olabilir. Doğrunun ne olduğu hakkında hepimizin oldukça iyi bir fikri olduğunu kabul etsek de geometri oyunumuzun kesin olması için yanlış anlaşılmaya açık bir boşluk bırakmaya dikkat etmeliyiz. Bu nedenle doğruyu, söz konusu noktalar arasındaki en kısa uzaklık olarak tanımlarız. Doğruların görece uzunlukları (en azından ilke olarak) her zaman kıyaslanabildiği için bu tanım “düz olma”yı belirlemek için pratik bir yöntem vermektedir.

İkinci aksiyom “Her düz doğru, sonu gelmemecesine uzatılabilir.” der. Burada biraz sorun var, çünkü bunun, içinde yaşadığımız gerçek uzay için doğru olup olmadığını görmek için sonsuza kadar gitmemiz olanaksızdır. Yine de eğer boş uzayın oluşturduğu evreni hayalinizde canlandırmaya çalışırsanız “sonsuz kadar” deyiminin kastettiği şeyi algılamak oldukça kolaylaşır. Boş uzay için ne gibi bir sınır göz önüne getirebilirsiniz? Eukleides'in varsayımını kabullenmek daha sorunsuz bir kavram gibi görünüyor.

Üçüncü aksiyom, merkezi herhangi bir nokta olan, herhangi bir yarıçaplı çember çizilebileceğini söylüyor. İlk bakışta bu aksiyom biraz tuhaf görünüyor. Uzayın özellikleri konusunda ne söylemek istiyor? Söylemek istediği, uzayın *yöresel* özelliklerinin (örneğin, bir çemberin çevresinin yarıçapına oranı) uzayın bir bölgesinden bir başkasına gitmekle değişmediğidir. Bunun da deneyimle uyumlu olduğu izlenimi var. Çin'deki çemberler (ve büyük olasılıkla aydakiler de) ABD'dekilerle aynı özellikleri taşırlar.

Dördüncü aksiyom şudur: “Bütün dik açılar birbirlerine eşittirler.” “Dik açı”nın, tümüyle geometrik olan bir anlamda, ne olduğunu tam olarak belirtmeden bu ifade fazla bir

anlam taşıyor; şimdi bunu yapalım. İki doğru karşılaştığında keşisme noktasında dört açı (iki çift eşit açı) tanımlar. Eğer doğrular, bu dört açı eşit olacak doğrultuda olurlarsa o zaman açılarının her birine “dik açı” denir. Böylece aksiyom, hangi iki doğru alınır alınsın veya keşisme uzayın hangi noktasında olursa olsun bu eşit kesme açılarının büyüklüğünün aynı olacağını söylemektedir. Burada da varsayımda bir hata bulmak çok zor.

Bu bizi elimizdeki öykünün ana teması olan beşinci aksiyoma getiriyor. Bu aksiyom için Eukleides’in vermiş olduğu orijinal ifade oldukça çapraşık olduğu halde biz yine de önce onu vereceğiz. Bu ifade şöyledir: Eğer bir düzlem üzerinde bulunan iki düz doğru, başka bir doğru tarafından kesilirse ve eğer bir taraftaki iç açılarının toplamı iki dik açıdan küçükse, o zaman doğrular, açılarının toplamının iki dik açıdan az olduğu tarafta yeterince uzatılırlarsa birbirlerini keserler. İfade uzun olmakla beraber, bir resim çizerek kolayca anlaşılabilir. Bu, aynı zamanda, özellikle şu sonucu vermektedir: Eğer iki doğru (bu bağlamda doğru, düz doğru demektir) bir başka doğru tarafından her biriyle dik açılar oluşturacak şekilde kesilirse o zaman başlangıçtaki iki doğru hiçbir zaman birbirlerini kesmez.

Birbirlerini kesmeyen doğrular “paralel” olarak tanımlanırlar. Buna göre Eukleides’in beşinci aksiyomu ya da genellikle anıldığı gibi, Eukleides’in beşincisi (ABD Anayasasının değişikliklerine dostane bir kinaye olarak sanırım) “paralel” kavramını kullanarak tekrar ifade edilebilir. İskoçyalı matematikçi ve fizikçi John Playfair’a (1748-1819) atfedilen ve bazen Eukleides’in Paralellik Aksiyomu olarak da söz edilen bu basit ifade “verilen bir noktadan verilen bir doğruya yalnızca bir tek paralel doğru çizilebilir” şeklindedir. Bunu kullanarak okul geometrisinden hatırladığımız birçok tanıdık şey ispatlanabilir; örneğin, “Bir üçgenin açılarının toplamı 180 derecedir” (Eukleides buna daha uygun bir deyişle, iki dik açı derdi). Ancak bu aksiyom, içinde yaşadığımız uzay için gerçekten doğru mu? Eukleides’in beşinci aksiyomu, ikinci aksiyomu gibi sonsuz hakkında bir beyanda bulun-

yor. Eğer paralel doğrular *hiçbir zaman* kesişmiyorsa, bu bizim uzayın sonsuz uzakta nasıl davrandığı konusunda bir şeyler bildiğimiz sonucunu verir. Ancak, uzayın hiç bitmeden sürdüğünü söyleyen ikinci aksiyomun tersine, beşinci aksiyom, bizim deneysel olarak kontrol edebileceğimiz herhangi bir bölgenin dışında kalan uzayın bir özelliği hakkında kesin bir bilgimiz olduğunu içermektedir.

Bu ikileme çağdaş yaklaşım, "Bu aksiyomların bizim geometri oyunu oynayacağımız uzayı tanımladığını düşünürsek sorun yoktur." şeklindedir. Kuralları ilk koyan Eukleides'in anısına ona Eukleides uzayı diyoruz. Ancak şimdi, aşağıda belirteceğimiz gibi olanaklı başka "uzaylar" konusunda edindiğimiz kavramlardan yararlanma ayrıcalığımız var. Eski Yunan'da bunlar yoktu. Onlar "gerçek uzay"ı; bizim, yıldızların ve galaksilerin bulunduğu uzayı ölçmekle ilgileniyorlardı. Önemli soru "Evrendeki bütün maddelerin içinde bulunduğu uzay boşluğu için beşinci aksiyom geçerli midir?" şeklindeydi. Bu şekilde sorulduğunda soruyu inandırıcı biçimde yanıtlamak hiç kolay değildi. Uzayın ufak bir bölgesinde paralel doğruların yakınlaşma veya uzaklaşma eğilimlerinin olduğu gerçekten fark edilmiyor. Ancak doğruları yeterince uzağa izlediğimizde böyle bir şeyin yavaş yavaş başlamayacağından nasıl emin olabiliriz?

Kuşkulanmak için pratik bir neden var gibi görünüyor. Yine de Eukleides'den yüzyıllar sonra, genel kanı, beşinci aksiyomun doğru olması gerektiği yolundaydı. İki türlü görüş öne sürülüyordu. Birincisi dinsel. Tanrının bütün yaratılarının içinde bulunduğu boş uzayın, onun gözünde kutsalsuz olması gerekirdi. Böyle olunca da düzensiz biçimde yaklaşan, uzaklaşan doğrular karmaşasını içermesi olası değildi. Eukleides'in beşincisi, olabilecek en basit ve en düzgün uzayı tanımlamaktadır. Bu nedenle, yaradılışın kutsal güzelliği onun "gerçek uzay" olmasını gerektirir: Tanrının kendisi, eserinin bozulmasına izin vermezdi. On sekizinci yüzyılda büyük destek kazanan ikinci argüman ise, sonsuz uzay kavramının kendisinin aklın bir eseri olduğunu söylüyordu. Akıl, Eukleides-dışı bir uzay düşünemeyeceğine göre beşinci

aksiyom doğru olmaktaydı. Bu çok ilginç bir bakış açısı, ancak az sonra göreceğimiz gibi, artık onu desteklememiz olanaklı değil; çünkü hayalimizde Eukleides-dışı bir evren canlandırmamız hiç de zor değil.

Ancak Eukleides'in beşincisinin öyküsünden çok uzaklaşmayalım. Önceki yıllarda, matematikçiler ve geometriciler arasında, çoğunluğun katıldığı daha az felsefi olan bir görüş açısı vardı. Buna göre beşinci aksiyom bağımsız bir ifade değildi, ilk dört aksiyomdan bir yolla çıkarılabilir olmalıydı. Bu doğru çıkarsa evrenin uzak bölgelerindeki uzayın geometrisi konusundaki kuşklar tümünden ortadan kalkardı. Yıllar boyu, birçok hatalı ispat ortaya atıldı ve bunlar dikkatli incelemeler sonucu ortadan kalktı. Dünyanın en büyük matematikçilerinden bazıları da, sonunda Eukleides'in beşincisini ispatladıklarına kendilerini inandırmışlardı. Örneğin, ünlü 18. yüzyıl Fransız geometri ustası Joseph Louis Lagrange hakkında bir öykü anlatılır; mesleğinin bir döneminde sadece ilk dört aksiyomu kullanarak bir üçgenin açılarının toplamının iki dik açı olduğunu ispatladığına inanıyordu. Söylendiğine göre Fransız Akademi'sine "İspatını" açıklayan bir konferansın ortasında, birden durmuş, "Bunu tekrar düşünmeliyim." diye mırıldanmış ve hemen salonu terk etmiştir.

Tersine olan bütün iddialara karşın sonunda, kuşku götürmez biçimde, Eukleides'in beşincisinin öteki aksiyomlardan çıkartılmayacağı ispatlanmıştır. O, tümüyle bağımsız bir aksiyomdur. Bu kanıt 1868 yılında verildiği halde, paralellik aksiyomunun "ispatları" yirminci yüzyılın bir bölümüne kadar görünmeyi sürdürdüler. Gerçekte Eukleides'in beşincisine olan tutku o denli büyüktü ki, Eukleides dışı bazı çok iyi geometri sistemleri geliştirildiği halde Eukleides idealine inatçı bir tapınmanın sürdürülmesi nedeniyle bunlar hiçbir zaman dikkate alınmadılar. Öte yandan, "Eukleides yanlılarını" anlayışla karşılamak zor değildir, çünkü geometri kurallarından beşincinin çıkarılması "hazmetmesi çok güç" olan sonuçlara yol açmaktadır. Örneğin, bir düz doğrunun aynı tarafından aynı uzunlukta iki dik

doğru çizer ve uçlarını birleştirerek bir dikdörtgen oluştursanız, Eukleides'in beşincisi olmadan, sadece iki dik açının var olduğunu söyleyebilirsiniz. Öteki iki açı için söyleyebileceğiniz yalnızca, onların eşit olduklarıdır; onların dik açıdan küçük, büyük veya ona eşit olması aynı ölçüde olasıdır. Sizin, "Ama bu saçma. Böyle bir çizim dik açılardan başka ne verebilir? Sağ duyumuzu kullanmalıyız." dediğinizi duyar gibiyim.

Sağ duyunun bizi nerelere götürebileceği Düzdiyar'a yapılacak bir yolculukla kolayca gösterilebilir. Düzdiyar, bizim alıştığımız gibi üç boyutlu değil iki boyutlu bir evrendir. Düzdiyarlılar Düzdiyar'da otururlar ve doğal olarak onlar da iki boyutludurlar ve bizim dördüncü boyuttan habersiz olduğumuz gibi onlar da üçüncü boyuttan habersizdirler. Dünyaları sadece doğu-batı ve kuzey-güney koordinatlarıyla ölçülür.

Düzdiyarda yaşam normal biçimde sürer ve Düzdiyarın geometricileri, içinde yaşadıkları uzayın özelliklerini ölçmek için kendi geometri kurallarını geliştirmişlerdir. Gerçekte, Eukleides'in beş aksiyomu, bize olduğu gibi onlara da yeterlidir. Bu nedenle onlar da "Eukleides'in beşincisi" problemiyle yüzyüzedirler. Ancak arada büyük bir fark vardır. Üç boyutlu bizlerin Düzdiyar'dakilere göre tanrısal bir avantajımız bulunuyor: Biz üçüncü boyutun varlığını hayal edebiliriz. Böyle bir şeyin olasılığını bile akıllarına getirmemiş olan zavallı Düzdiyarlılar için, üçüncü boyut kavranması tümüyle olanaksız olan bir şeydir. Halbuki bizler onların evrenlerinin üç boyutlu biçimini gerçekten görebiliriz.

Düzdiyar evreninin gerçekte, örneğin, büyük bir kürenin yüzeyi, dünya yüzeyinin tamamen düzeltilmiş yüzeyi gibi olduğunu varsayalım. Onlar için belirli bir bölgede geometri yapmak sorun değildir. Her şey Eukleides'le uyumlu görünür. Özellikle de, bir düz doğrunun aynı yanından, aynı uzunlukta iki dik doğru çizip, uçlarını birleştirmek, bizde olduğu gibi, onlara da "dört dik açısı olan" güzel bir dikdörtgen vermektedir. Ancak bizler, (Düzdiyarlılara göre) onların deneyimi dışında olan tanrısal bir yetiye, bir başka boyut düşünebilme yetisine sahibiz. *Onların* uzayında bir düz doğ-

runun (yani küre üstündeki iki nokta arasındaki en kısa uzaklığın) onların evreni olarak gördüğümüz kürenin “büyük çemberi”nin ufak bir yayı olduğunu biliyoruz.

Düzdiyarlıların evreninin bir tanrısı olarak siz (okuyucu) onların dikdörtgen çizme deneyini, onlar için düşünülemez olan bir ölçüde, gerçekleştirebilirsiniz. Bir top bulun. Onun yüzeyi Düzdiyar evrenidir. Bu size çok küçük görünebilir unutmayın ki siz artık bir tanrısınız. Düzdiyarlılar için bu top belki de, milyarlarca Düzdiyar ışık yılı çapındadır. Bir kalemle top üstünde bir “düz” doğru (yani Düzdiyarlılar anlamında düz-top yüzeyinde hareket ederken iki nokta arasındaki en kısa yol) çizin ve doğrunun aynı yanından eşit uzunluklu iki dik doğru yükseltin. Düzdiyar dikdörtgenini oluşturmak için de bunların uçlarını birleştirin, şimdi ne görüyorsunuz? Oluşan açılar eşit ama dik değil. Gerçekte onlar dik açıdan daha büyükler. Eukleides’in beşincisinin Düzdiyar’da geçerli olmadığı anlaşıyor. Gerçekte Düzdiyar’daki *bütün* doğruların sonunda birbirlerini kestiği görülür. Paralel doğru diye bir şey yoktur. Küçük ölçekte paralel gibi görülen doğrular, dünyadaki boylam çizgilerine benzerler; sonunda kutuplarda birleşirler. “Enlem çizgileri için ne diyebiliriz, onlar birbirlerini hiç kesmiyorlar.” diye düşünebilirsiniz. Doğru, ancak onlar Düzdiyar’da, düz doğru değildir. Ekvator dışındaki bir enlem üzerinde bulunan iki nokta arasında, her zaman, enlem çizgisinden farklı olan, daha kısa bir uzaklık vardır.

Biz, üç boyutlu yaratıklar, Düzdiyar’da görülen bu Eukleides-dışı davranışı şaşırtıcı bulmuyoruz. Düzdiyarlılara “Sizin evreniniz gerçekten düz değil, bir kürenin yüzeyi, ancak çapı o kadar büyük ki sizin bulduğunuz bölgedeki eğilmesi sizin ölçebileceğinizden çok daha küçük olduğu için size düz görünüyor.” diyebiliriz. Onların yanıtı, büyük olasılıkla, “Küre mi? Düzdiyarda küre nedir?” şeklinde olacaktır. Biz de, belli etmemeğe çalıştığımız bilgece bir tebessümle, kendimize, “Üç boyut kavramı tümüyle onların hayalgücü dışında bir şey.” deriz sanırım. Şimdi de tartışma boyutunu bir yükselterek kendi zihinsel sınırlamalarımızın farkına

varalım. Kendi evrenimizde hayal edilemeyen uzaklıklar içeren geometrik şekiller çizebilseydik Düzdiyar deneyine çok benzer şeylerin olmayacağını kim söyleyebilir? Açılarının toplamı dört dik açıdan fazla olan bir dikdörtgen elde edemez miyiz? Peki o zaman ne olur? Nedeni, evrenimizin dördüncü boyutta kavisli olması mıdır acaba? Yoksa gerçekte dört boyutlu bir kürenin “yüzeyi” olan bir uzayda mı yaşıyoruz? Ancak dört boyutlu bir küre ne demek oluyor? Bu sorular biraz Düzdiyarlıları anımsatmıyor mu, şimdi biz zihinsel olarak daha az yetenekli olan türlerin problemlerini mi yaşıyoruz?

Tekrar Düzdiyar'a dönersek, artık Eukleides geometrisinin geçerli olması için ne gerektiği hakkında bir fikir edinebiliriz. Üç boyutlu yaratıkların bakış açısına göre Düzdiyar, eğer düz (yani düzlem) olsaydı, Eukleides-vari olabilirdi. Eğer Düzdiyarlılar Eukleides'in bütün aksiyomlarını sadece uzaylarını “tanımlamak” için benimsedilerse o zaman evrenlerinin üçüncü boyutunda hiçbir bükülmenin olmadığını varsaymaktadırlar; bu ifadenin ne anlam taşıdığını gerçekten anlamaları, zaten söz konusu değildir. Aynı şekilde eğer biz de üç boyutlu dünyamızda, sadece Eukleides'in bütün aksiyomlarını kabul edersek biz de uzayımızın dördüncü boyutunda hiçbir bükülme olmadığını varsayıyoruz demektir. Bu ifadeyi fiziksel herhangi bir anlamda kavramakta biz de zorlanıyoruz.

Eğer uzayımız dördüncü boyutta herhangi bir şekilde bükülüyorsa o zaman Eukleides'in beşincisi geçerli olmayacaktır. Paralel oldukları varsayılan doğruları sonsuza kadar izlememiz, gerçekte mümkün olmadığı için Eukleides'e uyup uymadıklarını saptamak için başka olanaklar bulmamız gerekiyor. Bunlar ne olabilir? Eğer yaşadığımız bölgede uzay küçük bir eğrilme yapıyorsa o zaman (en azından ilkel olarak) çember ve üçgen gibi bazı geometrik şekilleri titizlikle inceleyerek bunu saptayabilmemiz gerekir. Bir üçgenin açılarının toplamının iki dik açıya eşit olduğunu ve bir çemberin çevresinin çapına oranının irrasyonel sayıların en ünlüsü olan pi sayısına (veya 3,1415926535897932...;

noktalar ondalık hanelerinin sonsuza kadar sürdüğünü söylüyorlar) eşit olduğunu okul günlerinizden hatırlıyor olabilirsiniz. Okul kitaplarının büyük olasılıkla size söylemediği şey ise, bu iki ifadenin de ancak Eukleides'in sorunu beşincisine sadık kalmak koşuluyla doğru olacaktır. Bu nedenle çevremizdeki üçgenlere ve çemberlere çok dikkatle bakmak zorundayız.

Çok küçük ölçüde Eukleides-dışı olan bir uzayda üçgenin açılarının toplamı iki dik açıdan biraz daha küçük veya biraz daha büyük olacak, çemberin çevresinin çapına oranı da π 'den biraz daha büyük veya biraz daha küçük olacaktır. Düzdiyarlıların evreni olan şu topu tekrar ele alarak bir Düzdiyar üçgeni veya bir Düzdiyar çemberi çizin ve kontrol edin. Düzdiyardaki bir üçgenin açılarının toplamının iki dik açıdan fazla, bir çemberin çevresinin çapına oranının ise π 'den az olduğunu görürüz. Eğer evrenin nerdeyse kendi büyüklüğünde üçgenler ve çemberler çizersek sapmalar da büyür, fakat yöresel ölçülerde çok küçülür. Ayrıca Pythagoras'ın kenar uzunlukları a , b ve c olan bir üçgen hakkındaki ünlü teoremi ($a^2 + b^2 = c^2$) de artık geçerli değildir. Bizim yöremiz yakınındaki üç boyutlu uzayda bu tuhaf olayların hiçbirisi gözlenmemiş olduğu için (ölçümlerin günümüzde olanaklı olan hassasiyet derecelerine göre) uzayımızın dördüncü boyutunda, olabilecek eğrilğin en azından yöresel ölçüde, çok küçük olduğunu kabul etmek durumundayız. Ancak biz de, galaksinin veya daha da ileri giderek görülebilen evrenin boyutuyla kıyaslandığımızda çok küçük kalıyoruz. Boş uzayın yeterince uzağında, "ta oralarda" ne olup bittiğini kim söyleyebilir?

Eğrilmiş veya Eukleides-dışı bir evrene sahip olma düşüncesinin, özellikle ilginç olan bir sonucu var: Sonsuzluk kavramıyla yüzleşmeyi gerektirmeden sınırsız bir uzayın kolayca düşünülmesine olanak sağlıyor. Bu düşünceyi kavramak için tekrar Düzdiyara dönmek iyi olacak, çünkü orada bizler tanrılar gibiyiz.

Sonsuz bir uzay, Düzdiyarlılar için de, bizim için olduğu kadar şaşırtıcı bir kavramdır. O, böyle bir evrende yaşadığını düşünür, ama bizim için yaşadığı evren bir topun yüze-

yinden ibarettir ve üç boyutlu deney bakımından bunda şaşırtıcı veya sonsuz olan bir şey yoktur.

Düzdiyarın gerçekte, üç boyutlu küresel bir yüzey olduğunu bildiğimiz halde Düzdiyar sakinlerine bu üçüncü boyut kavramını aktarabileceğimiz fiziksel hiçbir yol yok. Onlar için toprakları yöresel olarak Eukleides-vari (yani düzlemsel bir yüzey). Arka bahçelerindeki ağırlığı saptayabilen yeterince hassas araçlara sahip değiller. Onlar için evrenleri bir düzlemdir ve onun büyüklüğünün sonsuz olmaması durumunda başka ne olabileceğini düşünmek temelde olanaksızdır. “Başka nasıl olabilir?” diye soruyorlar. “Evrenin sonu nasıl bir engelle işaretlenebilir ve onun ötesinde ne olabilirdi?”

Şimdi, güçlü ve atak bir Düzdiyarlının bu teoriyi test etmek için yola çıkmaya karar verdiğini varsayalım. Ne olabilir? Üç boyutlu bakış açısından sonuç bellidir. Düzdiyarda düz bir doğru boyunca yola çıkan yolcumuz kendisinin çıkış noktasından sürekli uzaklaştığını, evrenin kenarına doğru yürüdüğünü düşünecektir. Ancak üç boyutta olan bizler onun, Düzdiyarın Ferdinand Magellan'ı olarak yavaş yavaş küresel evreninin çevresinde gittiğini görürüz. Eğer yola yeterince uzun bir süre devam ederse, bir gün, *bizim* beklentimize uygun olsa da onun için hiç beklenmedik bir şey olacak ve kendini yola çıktığı yerde bulacaktır. “Bu çok saçma, bir düz doğru boyunca sürekli gittim, sürekli evden uzaklaştım. Evrenin gerçekten sonsuza uzandığından tam emin olmaya başlamıştım, geri dönüp o yollara tekrar koyulup evdekilere bu haberi götürmeyi düşünürken, kendimi *evde* buluverdim! Pusulayı şaşırmış olmalıyım; siste kaybolmuş bir insan gibi dönüp durmuşum.” Ama biz onu temin ediyoruz, gittiği yol Düzdiyarda dümdüz giden sağa veya sola sapmayan düz bir doğrudur. Yolculuğun böyle bitmesinin nedeninin, Düzdiyar evreninin üçüncü boyutta bükülmüş olması, böylece hiçbir sınır veya “kenar” olmadığı halde sonlu büyüklükte olması ve büyüklüğünün (onlara göre) inanılmaz, dev boyutlu bir kürenin yüzeyi kadar olduğunu açıklıyoruz. Bizim Düzdiyarlı yolcu için bütün bunların fazla bir anlamı yoktur. O,

yalnızca uzayın bir üçüncü boyutu diye bir şeyin olmadığını söyler, bu durumda “onun içinde bir şey nasıl bükülebilir?”

Şimdi, resmin bütününe bir boyut ekleyelim. Gelecekte bir gün neredeyse ışık hızında giden uzaygemisi Enterprise’la evrenimizin çok uzak bölgelerini araştırmanın mümkün olduğunu varsayalım. Enterprise mürettebatının kaderinin de Düzdiyar yolcusunun kaderi gibi olacağını düşünebilir miyiz? Dünyadan düz bir doğru boyunca uzayın en uzak bölgesine yol alırken onlar da civarda görünenlerin tanıdık gelmeye başladığını mı fark edecekler? Dünya gezegeni “ta oralarda” da olabilir mi? Eğer bizim evrenimiz, gerçekten dört boyutlu bir kürenin “yüzeyi” ise, böyle bir şeyin gerçekleşmesi kesin olurdu. Dört boyutlu bir gözlemci, “Bunda şaşılacak bir şey yok, Enterprise uzaygemisinin izlediği yol üç boyut için gerçekten düz bir doğrudur, ama dört boyut için eğri bir çizgidir.” diyecektir. Bizim yanıtımız ise, “Ne demek istiyorsun, uzayın dördüncü boyutu diye bir şey yoktur ki, onun içinde bir şey nasıl eğri olabilir?” Eğer boyutunuz, problemin boyutundan bir fazlaysa bunu anlamak çok kolaydır!

Bizim “gerçek” üç boyutlu evrenimizin, dördüncü bir boyutta, bir şekilde bükülmüş olabileceği düşüncesi bir bilimkurgu değildir; gerçek bir olasılıktır. Bu durumu anlatmak için gereken geometri de Eukleides geometrisinin ta kendisidir; ancak beşinci aksiyomu değiştirilmiş olarak. Eukleides-dışı geometriyi ciddiye alan ilk kişi, bütün Alman matematikçilerinin en ünlüsü olan Karl Friedrich Gauss’dur (1777-1855). Gauss’un “Eukleides’in beşincisi”ni içermeyen, tümüyle tutarlı bir geometriyi ilk ne zaman geliştirdiği kesin olarak bilinmiyor, çünkü onu hiç yayınlamadı. Ancak Rus Nikolai Lobachevski (1793-1856) veya Macar Janos Bolyai (1802-1860) 1820’lerin sonlarında ve 1830’ların başlarında tamamlanmış teorilerini yayınlamadan önce, Gauss’un temel sonuçların birçoğuna sahip olduğu kesindir. Bu düşünce deliliğin sınırında gibiydi. Hatta Bolyai’nin babası ona yazdığı bir mektupta, “Tanrı aşkına onlar, seni sağlığından, huzurundan ve mutluluğundan yoksun bırak-

madan önce sen bu düşünceleri bırak” diyerek yalvarıyordu. Daha sonra (1854’te), kavramsal bakımdan daha basit olan, iki boyutlu küresel bir yüzey için geçerli olan ve hiçbir iki doğrunun paralel olamayacağı bir geometrinin yayınlanması ve bunun da, bir başka Alman matematikçiye, Georg Bernhard Riemann’a (1826-1866) ait olması ilginçtir.

Geometrinin, Eukleides’in beşincisinin mutlak egemenliğinden kurtulması birçok kişi tarafından bütün düşünce devrimlerinin en büyüğü olarak betimlenmiştir. Özellikle, 20. yüzyıl başlarında Albert Einstein’ın dehasının, uzay ve zamanın Eukleides-dışı bir fizik teorisi oluşturmaya olanak sağlamıştır. Einstein, maddesel cisimlerin (taş, sopa benzeri şeylerin) hareketleriyle ilgileniyordu ve başka cisimlere görece sabit hızla hareket eden cisimler için bir teori geliştirmişti. Buna “özel görecelik” teorisi deniliyordu ve 1906 yılında gün ışığına çıkmıştı. Bu teoriyi hızdaki (veya ivme-deki) değişiklikleri de içerecek biçimde genişletmeye çalışırken, yerçekiminin, benzersiz bir fiziksel kuvvet olduğunu fark etti. Bunun nedeni, yerçekimi etkisiyle özgürce düşen bütün cisimlerin (uzayda) ağırlıklarından ve bileşimlerinden bağımsız olarak, aynı yolu izlemeleriydi. Bu, yerçekiminin gerçekte uzayın kendisinin (daha doğrusu, uzay ve zamanın her ikisinin) bir özelliği olduğu anlamına geliyordu.

“Genel görecelik teorisi” denilen bu yeni teoride, yerçekimi Eukleides biçimi bir uzaydan ayrılır; yani uzaya bir “eğrilik”, bir bükülme ekler. Bu bakış açısına göre gezegenler güneş çevresinde yerçekimi kuvvetine uyarak dönmüyorlar (daha önceki Isaac Newton’un Eukleides-yanlı teorisinin varsaydığı gibi), yerçekiminin, gerçekte uzayın kendisini çarpıttığı için dönüyorlar. O zaman gezegenlerin hareketi bükülmüş bir uzayda tamamen özgür bir hareket olarak görülebilir. Ayrıca, Newton ve Einstein’a dayanan betimlemeler arasındaki fark sadece “aynı şeye farklı iki bakış” değildir. Bu iki betimlemenin gezegenler için *özdeş* olmayan yörüngeler öngörmeleri ilginçtir, ancak galaksimizimizin bizim bulunduğumuz bölgesinde, görece küçük olan yerçekimi alanlarında, bu farklar küçüktür. Ama yine de, daha önceki

Eukleides-yanlı resimde, Einstein'ın Eukleides-dışı yaklaşımı nedeniyle yapılan ufak düzeltmeler ölçülebilir düzeydedirler. Bunlar ilk olarak, güneşin çekim etkisinin en güçlü olduğu Merkür gezegeninin yörüngesinin çok dikkatli incelenmesi sonucunda saptanmıştır.

Bu nedenle, içinde yaşadığımız gerçek uzayın bizim bulunduğumuz bölgesinde biraz eğrilmiş (veya Eukleides-dışı) olduğu konusunda inandırıcı kanıtlar bulunmaktadır. Bu eğrilmenin, güneşin ışınlarını da etkilemesi son derece ilginçtir. Işık çok büyük bir hızla yol aldığı için onun üzerindeki yerçekimi etkisi maddesel nesnelerin çoğundan daha azdır. Ayrıca Newton'un Eukleides-yanlı uzayında bu etkiler hiç yoktur. Bunun sonucunda, ışığın yerçekimi nedeniyle bükülmesinin doğrudan gözlenmesi, bizim "üç boyutlu" uzayın Eukleides-dışı özelliğini de doğrulamış olur. Bu tür etkiler gözlenmiş bulunuyor. Özellikle, güneş tutulması sırasında hassas araçlar kullanarak böyle bükülme gözlemlenebilir; bu dönemlerde yıldızların güneşin kenarına yakın olan doğrultulardaki imgelerinin kaydığı gözlenir. Bu tür bir gözlem, Einstein'ın bu Eukleides-dışı olayı öngörmesinden birkaç yıl sonra, 1919'da yapılmış ve genel göreceliğin ilk zaferlerinden birisi gerçekleşmişti.

Evren daha çok boş görünse de, çok çok büyük olduğu için içerdiği madde de (toz, gezegenler, yıldızlar, hatta karadelikler) çok çok büyüktür. Einstein 1915'te, uzayda yerçekiminin neden olduğu sayısız hafif eğilmelerin, uzayın derinliklerine gitmekle sıfır ortalamasına indirgenmediğini fark etmişti. Böyle olsaydı sonunda bu, Düzdiyarlıların kendi iki boyutlu küresel uzaylarına benzer şekilde "kapalı" bir uzaya yol açabilecek ölçüde üst üste eklenirdi. O zaman, içinde yaşadığımız gerçek evren, Düzdiyar gibi sonlu ama sınırsız olurdu, yani sonlu bir üç boyutlu hacime sahip olurdu, tıpkı Düzdiyarlıların sonlu bir iki boyutlu alana sahip oldukları gibi.

Böyle bir evren, hiç olmazsa ilke bakımından, yeterince serüven tutkusu olan bir Enterprise ekibi tarafından çepçevre dolaşılabilir. Hatta yeterince güçlü bir teleskoptan bakarak insanın, kendi ensesini görmesi mümkün olabilir! Fazla gülme-

yin, bu tuhaf görünebilir ama bazı astronomlar, gökyüzünde, çapın karşılıklı iki ucunda radyo yıldızlarının bulunma olasılığının “rastlantı”dan daha büyük olduğunu iddia ediyorlar. Bu yıldız çiftleri gerçekte aynı yıldızın, birbirine karşıt yönlerdeki görüntüleri olabilirler mi? Eğer öyleyse, o zaman, buna göre evrenimizin “çapı” 10^{10} ışık yılı veya dünyasal ölçme birimleri-ne göre yaklaşık 96.540.000.000.000.000.000 m’dir.

Eğer bütün bunlar sizin için yeterince çarpıcı değilse, Düzdیارlıların yüzeyinde yaşayabilecekleri yegane üç boyutlu nesnenin bir küre (veya bir küreyi sürekli gererek veya herhangi bir şekilde çarpıtarak elde edilebilecek bir nesne) olmadığını hatırlamak yerinde olur. Yaşadıkları iki boyutlu evrenin başka türlü bir eğrilmiş yüzey olduğu düşünüldüğünde, daha da şaşırtıcı (en azından Düzdیارlılar için) özellikler elde edilebilir. Örneğin, ince uzun bir kâğıt şeridi, dar uçlarından tutup bir kere bükerek döndürdükten sonra, iki ucu birleştirdiğimizi varsayalım. Eğer kâğıdın her iki yüzeyinin de aynı uzay olduğunu düşünürseniz (sanki kâğıdın kalınlığı veya maddesel varlığı yokmuş gibi) o zaman bu yeni Düzdیار halkası çevresinde yapılacak bir yolculuk sağ ve solu da ters çevirecektir. Bir kâğıt şerit kullanarak bunu siz de görebilirsiniz.

Bu bükülmüş Düzdیار evreninin üç boyuttaki benzeri nasıl bir şey olabilir? Uzayın herhangi bir küçük bölgesinde çevremizde gördüğümüz “Eukleides-yanlı” uzaydan pek farklı görünmez. Ancak “evrenin kenarını” araştırmak için dünyadan yola çıkarak düz bir doğru boyunca giden bir uzay serüvencisi sonunda kendisini hem çok bildik, hem de tuhaf biçimde farklı bir yerde bulur. Her şey bıraktığının ayna görüntüsü gibi olmuştur. Yola çıkarken yanına aldığı kitabı hâlâ okuyabilmektedir, ama dünyadaki öteki kitapları ancak aynaya tutarak okuyabilmektedir. Yolculuğu yapmamış olan topluluğa göre ayna görüntüsü olan kitap bizim yolcunun kitabıdır. Uzay serüvencisi, kendisini bu ikilemden kurtarmak için tek bir şey yapabilir, evren çevresinde bir kere daha dolanmak. O zaman bu çabasının ödülü, her şeyin tekrar normal haline dönmesi olacaktır.

Bildiğim kadarıyla hiçkimse evrenimiz için yukardaki acaip, “bükülmüş evren” modeli gibi bir şey ileri sürmemiştir; Einstein ise, dört-boyutlu biraz pürüzlü bir kürenin yüzeyinden, yani, sonlu bir hacmi olan sınırsız bir evrende oturduğumuza inanmıştır. Vardığı bu sonuç evrendeki madenin her yerde, her zaman aynı olduğu ve aynı olacağı varsayımıyla elde ettiği genel görecelik denklemlerinden kaynaklanmaktadır. Ancak Einstein döneminden bu yana, evrenin tümünün, temelde değişmez bir doğası olduğu düşüncesinin yanlış olduğu yolunda, üst üste gelen güçlü, deneysel kanıtlar elde edilmiştir. Tam tersi, düşünülmektedir. Evrenin bir “big bang” yani, bir büyük patlamayla başladığı ve sonunda da bir “gib gnab” (veya bigbang’ın tersine ne denilirse) son bulabileceği düşünülmektedir. Evrenin çeşitli bölgelerindeki Eukleides-dışı eğriliğin derecesi kütle dağılımına bağımlı olduğu için, evrenin “şekli” de zamanla değişiyor olabilir, sanki yeterince problemimiz yokmuş gibi!

Kesin olan, belki de, tek şey bulunuyor; Eukleides’in beşinciyle sorun olduğu gerçeği. Eğer ölçümler yeterince duyarlılıkla yapılırsa, evrenin yaşadığımız yöresel bölgelerinin, okul geometrisinin kurallarına uymadığı görülür. Bütün bunların anlamı nedir? Anlamı şudur: Matematikte ve bilimde sezgi güçlü bir araçtır, ancak ona her zaman güvenilemez. Evrenin yapısı, kuramsal matematiğin kendisi gibi, en büyük matematikçilerin ve bilimcilerin düşünebildiklerinden bile çok daha tuhaf olma eğilimindedir.

VII. Bölüm

Saat Sayıları

Saat bir sayma makinesinden başka nedir ki? Dakikaları sayar, saatleri sayar, hatta bazen de saniyeleri sayar. Dahası, ona güç veren kaynak, (eski moda veya modern de olsa) var olduğu sürece hemen hemen hiç durmadan saymayı sürdürür. Diğer yandan, saatin saymasında farklı olan bir şey vardır, durmadan (ideal olarak) saydığı halde, sayılar hiçbir zaman çok büyümez. Örneğin, saatlerin sayısı 12'nciye her geldiğinde başa döner. Eğer saat 2 ise ve biz 12 saat veya 24 saat beklersek bize saatin yine 2 olduğunu söyler. Çok dikkatle saydığı halde kaç tane 12 saat geçtiğine hiç alırdır gibidir, sadece 12 saatlerden geriye kalanı "hatırlamayı" tercih eder.

Bütün bunlara alışık olduğumuz için bize hiç tuhaf gelmez. Ancak çok tuhaf görünen bir aritmetiğe yol açtığına kuşku yoktur. Örneğin saatin 8 olduğunu bildiğimizi ve 6 saat "eklersek" saatin kaç olacağını bilmek istediğimizi varsayalım. Bu problemin ileri matematik gerektiren türden olduğu söylenemez, yanıtı kolayca bulabiliriz; saat 2 olacaktır. Öyleyse saatin bakış açısından

$$8 + 6 = 2 \text{ dir.}$$

Bu eşitliğe bir saatin ifadesi olarak değil de aritmetiğin bir ifadesi olarak bakarsak gerçekten olağan dışı görünür.

Yine de bu "saat aritmetiği", kendi içinde tamamen tutarlıdır. $2 - 4 = 10$, $2 + 12 = 2$ ve $6 + 38 = 8$ gibi eşitliklerin doğru olduklarını hemen gösterebiliriz. Yaptığımız, 12'li kümeleri sayarak veya 12'ye bölerek sadece kalanı yazmaktır.

Bütün bunlarda 12 sayısının özel bir marifeti olmadığı açıktır. Saatlerin çoğu dakikaları ve saniyeleri de sayar; onlarda da sadece kalanlara önem verirler, arada kaç tane 60 kümesinin geçtiği önemsizdir. Saniye kolunun bakış açısından, normal aritmetikte olduğu gibi $8 + 6 = 14$ 'tür, ancak $8 + 62 = 10$ 'dur.

Her seferinde ne yaptığımızı açıkça belirtirsek bu eşitliklerin her biri akla yakındır. Bu durumda ne kastettiğimizi belirtecek basit bir yol bulmazsak büyük bir kargaşanın ortaya çıkacağı da açıktır. Örneğin öğretmen Johnny veya Jill'den tahtada yazılı olan $8 + 6 = ?$ eşitliğini tamamlamasını isterse, 2 yanıtına (ki saatin, saat kolu için eşitlik doğrudur) akademisyenlerin kaşları çatılır ve “yanlış” olduğu söylenir. Diğer yandan, normal olarak 14 olması gerektiği düşünülen yanıt saat aritmetiğinde, en azından saat koluna göre saat aritmetiğinde, 2 olmaktadır. Bunu açıklamak için

$$14 = 2 \pmod{12}$$

yazılması benimsenmiştir. Burada (mod 12) 12'li kümeleri çıkarıp sadece kalanın dikkate alındığını anlatmaktadır. Matematikçiler bu ifadeye biraz haşmetli bir şekilde “14, 2 modulo 12'ye denktir” derler ve çoğunlukla = yerine $\equiv$ kullanırlar (nedeni, herhalde basit yazılırsa kimseyi etkilemeyeceği ve daha fenası, herkesin anlayacağı olsa gerek). Biz bunu “14, 12-saatinde 2 ile aynıdır” şeklinde okuyabiliriz ve “12'li kümelerle sayıldığında (ya da bölündüğünde) 14'ün kalanı 2'dir” şeklinde anlarız.

Daha genel birkaç örnekle bu yazış biçimine çabucak alışabiliriz. Böylece $49 = 1 \pmod{8}$ ifadesi bize 49'un sekizle bölündüğünde 1 kalanını verdiğini söyler ki bunun doğru olduğu herkesçe bilinir. Aynı şekilde, $55 = 7 \pmod{8}$ dir; yani 55 sekize bölündüğünde kalan 7'dir. Yeterince basit! Ancak bir adım daha atarak, fazla zorlanmadan, negatif kalan kavramıyla tanışırız. Eğer 55, yukarıda belirtildiği gibi 8'in tam katlarından 7 birim daha fazlaysa, 8'in tam katlarından 1 birim eksik olarak da düşünülebilir veya “saat eşitliği” olarak

$$55 = -1 \pmod{8}$$

yazılabilir. Benzer şekilde;

$$99 = -1 \pmod{10} \text{dur.}$$

İyi güzel de bu ne işe yarar diyebilirsiniz. Güzel bir soru! Bir “saat sayısı” eşitliğinin her iki tarafına sayı ekleyebiliriz, çıkartabiliriz ve onları bir kuvvete yükseltebiliriz ve yine de eşitlik bozulmaz. Başka deyişle, bölme işlemi dışında (bu işlem biraz daha fazla dikkat gerektirir ve bu bölümde daha sonra ele alınacaktır) saat eşitliğinin iki yanı, normal eşitlikler gibi birbirlerine eşittirler ve onlarla da aynı işlemleri yapabiliriz. Örneğin,

$$49 = 1 \pmod{8}$$

eşitliğini ele alalım, iki tarafa da 2 ekleyelim. $51 = 3 \pmod{8}$ olur ve bunun da doğru olduğu aşikârdır. Aynı kolaylıkla her iki taraftan 2 çıkarabiliriz. $47 = -1 \pmod{8}$ de doğrudur. Her iki tarafı aynı sayı ile çarptığımızda elde edilen sonuç pek o kadar basit değildir. 49’la çarparak

$$49^2 = 49 \pmod{8}$$

yazarız. Sekizli-saatte, 49 ile 1 aynı sayıdır ve $49^2 = 2401$ olduğundan yukarıdaki eşitlik

$$2401 = 1 \pmod{8}$$

eşitliğine dönüşür. Bunun doğruluğu da, 2401’i 8’e böldüğümüzde kalanın 1 olduğunu saptayarak kolayca görülür. Ancak bu ifade (doğru da olsa) size fazla şaşırtıcı gelmeyebilir.

Bir saat eşitliğinin iki tarafını da bir kuvvete yükseltmek söz konusu olduğunda aklımız karışmaya başlar. Yine $49 = 1 \pmod{8}$ eşitliğini ele alıp iki tarafı, örneğin 100’üncü kuvvete yükseltelim. 1 sayısı hangi kuvvete yükseltirse yükseltsin de 1’e eşit olacağından, şu sonucu hemen yazabiliriz.

$$49^{100} = 1 \pmod{8}$$

49^{100} sayısı bütün evrendeki atomların toplam sayısından çok daha büyük bir sayıdır. Açık olarak yazıldığında 170 basamaklı, günümüz bilgisayarlarının herhangi birisinin baş edemeyeceği büyüklükte bir sayıdır. Ancak yine de, yukarıdaki saat eşitliğinden, 8'e bölündüğünde kalanın 1 olduğunu hemen biliriz. Her iki taraftan 1 çıkararak da, yine çok büyük bir sayı olan $49^{100} - 1$ 'in 8'e *tam olarak* bölünebildiğini hemen görürüz. Eğer bir aylık bir boş zamanınız varsa ve aritmetik işlemleri yapmaktan hoşlanıyorsanız, aynı sonucu "sayı öğütürük" elde etmeniz de mümkün olabilir. Ancak saat aritmetiği kullanarak, dünyanın en büyük bilgisayarlarının bile doğrudan yöntemlerle hesaplayamayacağı kadar büyük sayılarla da aynı kolaylıkla işlem yapabiliriz.

Yine aynı basit saat denklemi ile başlayarak her iki tarafı 1.000.000'uncu kuvvete yükseltirsek ne olur? Hiçbir sorun yoktur. Hemen,

$$49^{1.000.000} = 1 \pmod{8}$$

yazabiliriz. Sol taraftaki sayı, ondalık şeklinde yazıldığında basamak sayısı 1.500.000'den oldukça büyüktür ve elinizdeki gibi birkaç kitabı doldurur. Ancak yine de 8'e bölündüğünde kalanın 1 olduğunu ve $49^{1.000.000} - 1$ sayısının 8'in tam katı olduğunu biliyoruz.

"Saat eşitliğinin sağ tarafında 1 veya 0 olursa (o zaman herhangi bir n sayısı için 1^n veya 0^n sayılarının değerini hemen biliyoruz) iyi güzel ama bu biraz sınırlayıcı olmuyor mu?" diyebilirsiniz. Şaşıracaksınız ama öyle olmuyor, çünkü biraz akıl kullanarak sağ tarafı 1 veya 0'a indirgemek her zaman olanaklıdır.

Örneğin, en yakın arkadaşınızın size 1 sayısının arkasına 999.999 tane sıfır, sonra da 9 yazarak elde edilen sayının 13'e bölünüp bölünemeyeceğini sorduğunu düşünelim. İlk tepkiniz "Şaka mı yapıyorsun?"dan başlayıp "senin gibi arkadaşın olanın düşmana ne ihtiyacı var"a kadar uzanabilir.

Ancak yine de yeni keşfettiğiniz saat aritmetiğiyle her şey yitirilmiş sayılmaz. Söz konusu sayı $10^{1.000.000} + 9$ şeklinde de yazılabilir. Soru 13'e bölünebilirlik içerdiğine göre (mod 13) saat ile çalışmamız yerinde olur. Yapılabilecek en basit başlangıç da

$$10 = -3 \pmod{13}$$

şeklindedir. Bu ifade, 10 sayısı 13'e bölündüğünde -3 kalanını verir demekten ibarettir. Bu eşitliği kendisiyle çarparak (yani iki tarafın da karesini alarak) ve -3 çarpı -3'ün +9 olduğunu hatırlayarak

$$10^2 = 9 \pmod{13}$$

elde ederiz. Yani, 100, 13'e bölündüğünde kalan 9'dur. Yedi tane 13, 91 olduğuna göre kalan gerçekten 9'dur, yani yukardaki ifade doğrudur.

Sağ tarafta kolayca 1 veya 0 nasıl oluşturabiliriz? Yukardaki iki eşitliği birbirleriyle çarpmaya ne dersiniz? Sağ tarafta 10 çarpı 100, 1000 (ya da 10^3), sol tarafta, -3 çarpı 9 da -27 olduğuna göre sonuç

$$10^3 = -27 \pmod{13}$$

olur. Ancak $-27 = -13 - 13 - 1$ olduğu için, 13'e bölündüğünde kalanı -27 olan sayının aynı zamanda 13'e bölündüğünde kalanı -1 olan sayı olduğunu görürüz.

Bu nedenle

$$10^3 = -1 \pmod{13}$$

yazabiliriz. Bu sayı hâlâ doğrudan kontrol edilebilecek kadar küçüktür 77 tane 13'ün değeri 1001 olduğuna göre, gerçekten de 1000 ile -1, "13'lü saatte" aynı sayıdır.

Burada önemli olan, sağ tarafta artık 1 sayısını görebiliyor olmamızdır. Gerçekte gördüğünüz sayı -1'dir; ancak bu-

nun önemli olmadığını biliyoruz, çünkü -1 sayısı herhangi bir kuvvete (n diyelim) yükseltildiğinde, n tek sayı ise -1 'e, n çift sayı ise $+1$ 'e eşittir. Şimdi bu son saat eşitliğinin iki tarafını $n = 333.333$ kuvvetine yükseltelim

$$(10^3)^{333.333} = -1 \pmod{13}$$

Bir kuvvetin tekrar kuvvetini aldığımızda sadece üsleri çarpmak yeterli olduğundan (örneğin $(10^3)^2 = 10^6$ veya sözcüklerle; bin çarpı bin, bir milyondur) yukardaki ifade

$$10^{999.999} = -1 \pmod{13} \text{ olur.}$$

Artık amacımız olan $10^{1.000.000} + 9$ sayısına yaklaşıyor gibiyiz. Ancak henüz oraya varamadık. Sol tarafta bir 10 sayısına gerek var. Öyleyse başlangıçtaki $10 = -3 \pmod{13}$ ifadesi ile çarpalım. Eksi çarpı eksinin artı olduğunu hatırlayarak

$$10^{1.000.000} = 3 \pmod{13}$$

buluruz. Hedefe varmak için iki tarafa da 9 eklemek yeterlidir ve sonunda

$$10^{1.000.000} + 9 = 12 \pmod{13}$$

elde ederiz. Bu bize verilen sayının 13'e tam bölünmediğini, 13'e bölündüğünde kalanın 12 (veya -1 , çünkü 12 ve -1 sayıları 13'lü saatte aynıdırlar) olduğunu söylemektedir. Öyleyse $10^{1.000.000} + 10$ sayısı 13'e tam bölünür, halbuki onun görünümü böyle bir ayrıcalık için aday olabileceğini hiç akla getirmez. Bu örnekten edindiğiniz yüreklilikle, saat sayılarını kullanarak, akıl almaz büyüklükteki sayıların, herhangi bir sayıyla (işlemleri basitleştirmek için küçük sayılar seçerek) bölünebilirliklerini saptamanız olanaklıdır.

Buraya kadar yaptıklarımızda bölme işlemini ele almadık; çünkü saat sayılarını bölme kuralları ötekilere göre daha sınırlayıcıdır. İlk olarak, bir saat eşitliğinin iki tarafı,

ancak ortaya kesirler çıkmasına yol açmayan bir sayıyla bölünebilir. Örneğin $12 = 2 \pmod{5}$ eşitliğini 2 ile bölebiliriz ve $6 = 1 \pmod{5}$ elde ederiz ki bunun doğru olduğu açıkça görülebilir. Ancak 3'e bölersek $4 = 2/3 \pmod{5}$ olur ve bunun anlamı yoktur, en azından bu kitapta kullanılan en basit notasyon çerçevesinde. İkinci bir sınırlama daha vardır. Eğer böldüğümüz sayı, saat sayısını, yani mod sayısını da tam olarak bölüyorsa, bölme işleminde, bu sayı da bölünmelidir. Örneğin $15 = 6 \pmod{9}$ saat eşitliğini 3'e yalnızca $5 = 2 \pmod{3}$ şeklinde bölebiliriz, $5 = 2 \pmod{9}$ şeklinde bölemeyiz. Bu tür basit bir eşitliğin doğru olmadığı kontrol edilebilir; çünkü $5 = 2 \pmod{9}$ değildir.

Saat aritmetiğinin nerelerde kullanılabileceği konusuna şöyle bir değindiğimiz halde bu yöntemin sayıların özelliklerini incelemek için çok güçlü ve yeni bir yaklaşıma yol açtığı anlaşılmış olsa gerek; ancak daha fazlasına da uygulanabilir. Bu nedenle onu keşfeden insanın yaşamına kısaca bir göz atalım. Karl Friedrich Gauss bir dâhi çocuktur. 1777 yılında Almanya'da bulunan Brunswick'te doğdu. Benzersiz matematik dehasını henüz sekiz yaşındayken kanıtladığı söylenir*. Öğretmen, öğrencileri bir süre oyalamak için onlardan 1'den 100'e kadar olan sayıları toplamalarını ister. Böyle bir problem için bir formül olduğu kuşkusuz. Ancak öğretmen bunu bilse de çocuklar bilmezler. Bu nedenle öğrenciler dikkatle problemle uğraşırken öğretmen de bir saat kadar bir süre huzur ve sükun içinde oturacaktır. Pek olası görünmese de sonunda ancak bir veya iki öğrenci doğru yanıtı bulacaktır. Ancak küçük Karl Gauss'un hemen sınıfın önüne gelerek doğru yanıt olan 5050 sayısını kendisine vermesi onu çok şaşırtır.

Anlaşıldığına göre Gauss da formülü biliyordu ancak öğretmenden bir farkı vardı. Onu daha önce öğrenmemişti; o anda çabucak kendisi çıkarmıştı. Bir kere gördükten sonra oyun çok kolaydır; 1 ile 99'u toplayın (100 eder), sonra 2 ile

* Karl Friedrich Gauss, henüz üç yaşında iken okuma yazma ve aritmetik sembollerinin anlamlarını kendi kendine öğrenmiş ve babasının ücret bordrosunda bir hata olduğunu zihinsel hesaplama ile ortaya çıkararak ailesini şaşırtmıştır. (ç.n.)

98'i (o da 100 eder), 3 ile 97, 4 ile 96 vb. son olarak da 49 ile 51; her aşamada bulunan sayı 100'dür. Bu, 49 tane 100 yapar, şimdi de ortadaki 50'yi ve en sondaki 100'ü ekler ve doğru yanıt olan 5050'yi elde edersiniz. Matematikçinin daha sonraki gelişmesi bakımından öğretmen bu olayla çocuktaki dehayı fark etti ve böylece çoğunlukla gelmiş geçmiş en büyük matematikçi olduğu düşünülen insanın meslek yaşamı başlamış oldu.

On sekiz yaşına geldiğinde düzgün bir yedigenin (yani, kenarları eşit uzunlukta, iç açıları eşit olan yedi kenarlı şekil) sadece cetvel ve pergel kullanarak çizilmesinin olanaksız olduğunu ispatlamıştı. Bu matematikçi ve geometricilerin 2000 yıldır sonuç alamadan uğraştıkları bir problemdi. Doktora tezi olarak cebirsel denklemlerin sahip olabilecekleri çözümlerin sayısı konusunda bir ispat sundu. Bu teorem, günümüzde de "cebirin temel teoremi" olarak anılır. Ayrıca bu da en iyi matematik beyinlerini yüzyıllar boyu işgal etmiş bir problemdi. Boş zamanlarında astronomiye yöneldi ve hatta Göttingen Üniversitesi'nde gözlemevinin müdürü oldu. Aynı zamanda da 1807'den 1855'teki ölümüne kadar aynı üniversitede matematik profesörlüğünü sürdürdü. Ancak yine de temel çalışma alanları matematik ve teorikfizikti. Günümüzde manyetik alan şiddetinin birimi olan "gauss" onun bu alana yaptığı katkıların bir onayıdır. Ve elektrostatik belki de en temel teoremi "gauss teoremi" olarak bilinir. Çalışmaları istatistik alanını da kapsar ve günümüzde en temel ve en iyi bilinen olasılık dağılımına "gauss dağılımı" denilmektedir; başka ne olabilirdi ki?

Gauss'un sayılar teorisindeki en önemli çalışması 1801'de, henüz 24 yaşındayken yayınladığı *Disquisitiones Arithmeticae* kitabıdır. Gauss, kitabın ilk bölümlerinde denklik teorilerini (yani) o günden bu yana sayılar teorisi alanındaki neredeyse bütün araştırmalara damgasını vuran saat sayılarını ilk defa ortaya koymuştur. Kitabın daha sonraki bölümlerinde, birçok matematik probleminin ilk çözümleri yer alıyordu. Daha önceki nesillerin en ünlü matematikçileri bu problemlerden birçoğu üzerinde çalışmış ve sonuç alınamamıştı. Bu tür problemlerin bazılarında aynı teoremin üç ayrı ispa-

tını vermiş olması dehasının boyutuna bir işarettir. Başka deyişle, daha önce hiç kimsenin ispatlamayı başaramadığı bir şeyi Gauss bir kere ispatlamış, sonra da fazladan iki ayrı ispat daha vermiştir.

Mucit hakkındaki bu kısa “sapak”tan sonra şimdi saat sayılarının gerçek sayılar teorisindeki ispatlamalarda nasıl kullanıldığına bir bakalım. Ciddi görünümlü bu ifade sizi endişelendirmesin; saat denklemleri (daha çok denklikler olarak bilinirler) burada da, daha önce olduğu kadar kolay anlaşılır şeylerdir. Örneğin, onların yardımıyla sayı teoremlerinin en ünlülerinden biri olan Fermat’ın “küçük teoremi”ni açıklayabiliriz (ilk defa Fransız matematikçi Pierre de Fermat (1601–1665) tarafından ileri sürülmüş ve ispatlanmıştır; ancak bu orijinal ispat hiç yayınlanmamıştır). Bu eğlenceli bir teoremdir; çünkü bir sayının *çarpanlarının hiçbirini bilinmediği halde* çarpanların var olduğunu ispatlayan bir yöntemle yol açmaktadır.

Rasgele bir asal sayı ele alalım, örneğin 7. Bu sayıdan küçük olan bütün tamsayıları yazıp (1, 2, 3, 4, 5, 6) sonra her birini iki ile çarpalım. Yeni bir dizi elde ederiz: 2, 4, 6, 8, 10, 12. Bu sayıları 7’li saate (daha doğru deyişle modulo 7’ye) göre yazınca da dizi; 2, 4, 6, 1, 3, 5 olur ki bu, ilk dizinin sırası değişmiş biçimidir. Öyleyse modulo 7 ile sayıldıklarında, 1’den 6’ya kadar olan sayıların çarpımı (kısaca yazıyla bu, genel olarak 6! şeklinde yazılır ve ona “6 faktoriyel” denir) ile 2, 4, 6, 8, 10, 12 sayılarının çarpımı birbirine eşittir.

Ancak bu ikinci dizinin her üyesi, birinci dizide ona karşılık olan sayının iki katıdır. Dizide altı üye olduğuna göre, 2, 4, 6, 8, 10, 12 sayılarının çarpımı da 2^6 çarpı 6! olmalıdır. Öyleyse şu sonuca varmış oluyoruz.

$$2^6 \times 6! = 6! \pmod{7}$$

6! sayısında (tanım gereği) modulo sayısı olan 7 ile tam bölünen bir çarpan yoktur, öyleyse daha önce verdiğimiz bölme kuralına göre iki tarafı 6! ile bölerek

$$2^6 = 1 \pmod{7}$$

buluruz. 2^6 , 64 olduğuna göre, 64'te 9 tane 7 artı, “kalan” 1 olduğu için, doğrudan hesaplama ile sonucu kolayca doğrulayabiliriz ve bu nedenle de övgüye değer bir şey yapmış sayılırız. Burada önemli olan bu yöntemin genellemeye açık oluşudur. Örneğin, eğer ilk dizideki 1'den 6'ya kadar olan sayıları 3 ile çarparak (2 yerine) elde edilen sayılar 3, 6, 9, 12, 15, 18, $\pmod{7}$ de, 3, 6, 2, 5, 1, 4 $\pmod{7}$ sayılarına eşittirler ki, bunlar da ilk sayıların karışmış bir dizisidir.

Aynı çarpma işlemleriyle elde edilen denklik

$$3^6 = 1 \pmod{7}$$

dir. Benzer şekilde 4, 5, 6 ile çarparak yine

$$4^6 = 1 \pmod{7}$$

$$5^6 = 1 \pmod{7}$$

$$6^6 = 1 \pmod{7}$$

buluruz. Ancak “saat sayısının” kendisine geldiğimizde (örneğinizde yedi) bu model değişir, çünkü 7^6 (altı tane 7 sayısının çarpımı) 7 ile tam olarak bölünebilir ve $7^6 = 0 \pmod{7}$ 'dir.

p bir asal sayı olmak koşuluyla 1'den $p - 1$ 'e kadar olan tamsayıların, 2, 3 veya $p - 1$ 'e kadar olan tamsayılarla çarpıldıktan sonra $\pmod{p}$ 'ye göre sayıldıklarında tekrar kendilerine dönüşeceklerini ispatlamak zor değildir. Diğer yandan eğer p asal değilse bu her zaman yer almaz. Örneğin, $p = 6$ için, 1, 2, 3, 4, 5 sayıları 2 ile çarpıldıklarında 2, 4, 0, 2, 4, 0 $\pmod{6}$ olurlar; 3 ile çarpıldıklarında ise 3, 0, 3, 0, 3, 0. Hem 2 hem de 3 sayıları 6'yı tam olarak böldükleri için bu örnekte ortaya sıfırlar çıkmaktadır. Asal ve asal olmayan birkaç sayı ile denemeler yaparak kısa sürede ne olup bittiğini daha iyi anlayabilirsiniz.

Demek oluyor ki son keşfimiz, herhangi bir asal p sayısı için ve p 'ye eşit olmayan (veya p 'nin bir tam katı olmayan) n sayısı için,

$$n^{p-1} = 1 \pmod{p}$$

veya her iki taraftan 1 çıkararak,

$$n^{p-1} - 1 = 0 \pmod{p}$$

olduğudur. Sözcüklerle ifade edildiğinde bunun anlamı şudur: Eğer n sayısı p 'ye bölünebilir değilse, $n^{p-1} - 1$ sayısı her zaman asal olan p sayısı ile tam olarak bölünür. Bunun nasıl işlediğini birkaç örnekle görelim. Kolaylık olması için ilk önce n 'nin ikiye eşit olduğu örneklerle başlayacağız: O zaman, $2^2 - 1 = 3$ gerçekten 3'e (asaldır) bölünebilmektedir, 4'e ise (asal değildir) bölünebilir değildir. $2^4 - 1 = 15$, 5'e (asaldır) bölünebilir; $2^5 - 1 = 31$, 6'ya (asal değildir) bölünmez; $2^6 - 1 = 63$, 7'ye (asaldır) bölünebilir vb.

İlk bakışta asal sayıları test edecek bir yöntemimiz var gibi görünüyor. Gerçekte M.Ö. 500 yıllarında Çinliler $2^{p-1} - 1$ sayısının, eğer p asal ise, her zaman p ile bölünebilir olduğunu; p asal değilse (veya doğru sözcükle "bileşik" ise) hiçbir zaman bölünebilir olmadığını ifade etmişlerdi. Ancak bu doğru mudur? Dikkatli olmamız gerek. İspatımız p 'nin asal olduğu durum için verilmişti. Genel olarak $n^{p-1} - 1$, özel olarak da $2^{p-1} - 1$ sayılarının asal olmayan rastlantısal bir p sayısı ile bölünebilir olabileceği reddedilmişti. $2^{p-1} - 1$ için Çinliler böyle bir sayı bulmayı başaramamışlardı, gerçekten 1819 yılına kadar hiçkimse böyle bir sayı bulamamıştı. 1819 yılında $2^{340} - 1$ sayısının 341 ile bölünebildiği ve 341'in (11 çarpı 31 olduğu için) asal olmadığı fark edildi.

Yukarıda verilen denklik ifadesini sağlayan asal olmayan sayılar, görece çok azdırlar. Ancak yine de sayıları sonsuzdur ve onlara "sahte-asal" denilen p sayılarını tanımlarlar. Bu sayılar $n = 2$ için etraflıca incelenmişlerdir. Bu durumda, 1010 sayısından küçük 455.052.512 gerçek asal sayı olmasına karşın, sahte asalların sayısı 14.884'tür. Öyleyse,

$$2^{p-1} = 1 \pmod{p}$$

testini geçen p sayılarından, yaklaşık yüzde üç binde biri gerçek asal değildirler. Bu “sahtekarlar”ın çoğu, yani $n = 2$ için bulunan sahte-asalların çoğu tek sayıdır. Gerçekte çift olan sahte-asal sayının bulunması ancak 1950’de başarılı olmuştur (161.038) ve bulunmaları hâlâ aynı ölçüde zordur. $n = 2$ için bulunan sahte-asal sayılar dışında $n = 3, 4, 5, \dots$ vs için de benzer çalışmalar yapılabilir. $n = 2$ ile $n = 10$ için bilinen en küçük sahte-asallar, sırasıyla şunlardır: 341, 91, 15, 124, 35, 25, 9, 28 ve 33. Gerçekte $n = 2$ için bulunan 341, $n = 100$ ’e kadar bulunan “en küçük sahte-asal” sayıların en büyüğüdür (ancak 341 değeri yalnız $n = 2$ için değil $n = 15, 60, 63$ ve 78 içinde en küçük sahte-asaldır). Bu, Çinlilerin onu neden bulamadıklarını da açıklamaktadır. Çünkü $2^{340} - 1$, ondalık şeklinde yazıldığında 103 basamaklı, oldukça büyük bir sayıdır. Bu şekildeki ifadesini hesaplayıp, 341’le bölünebilir olup olmadığını test etmek kolay değildir. Eğer saat aritmetiğini biliyorsanız (ki Çinliler bilmiyordu) durum farklıdır. Bu bölümün başında verilen kuralları uygulayarak $2^{340} - 1$ sayısının 341 ile bölünebilir olduğu, yani

$$2^{340} = 1 \pmod{341}$$

olduğu, birkaç satırla hemen doğrulanabilir. Deneyin!

Sahte-asallar kavramının ardından “süper-sahte asallar” geldi. Bunlar, $n^{p-1} - 1$ sayısının, p ile karşılıklı olarak asal olan *bütün* n sayıları tarafından tam olarak bölünebildiği p sayılarıdır. Bunlara “Carmichael sayıları” denir ve kesin olarak bilinmese de, sonsuz sayıda oldukları düşünülmektedir. En küçüğü $3 \times 11 \times 17$ olan 561’dir ve bu sayıların en az üç asal sayının çarpımı olduğu bilinmektedir. Böylece, $2^{560} - 1$ sayısı 561’le bölünebilir; aynı şekilde $4^{560} - 1, 5^{560} - 1, 7^{560} - 1$ vb. gibi, 3, 11 veya 17 ile bölünemeyen *bütün* n sayıları için de 561 ile bölünebilirler. Bundan sonra gelen Carmichael sayıları, sırasıyla 1105, 1729, 2465, 2821, 6601 ve 8911’dir ve 10.000’den küçük olan yegane sayılardır. 1010’dan küçük olan 1547 Carmichael sayısı olmasına karşın, bu sınırın altında 455 milyondan fazla gerçek asal sayı bulunmaktadır.

Fermat'nın küçük teoremi (ne yazık ki!) asal sayıları bulmak için "su geçirmez" bir tarife sağlamıyor, çünkü asal maskesi altında gizlenen sahte-asal sayılar da (az sayıda olsa da) üretme olanağı bulunuyor. Ancak aynı ölçüde etkileyici bir şey sağlıyor; Fermat'nın küçük teoremini sağlamayan her hangi bir tek sayı asal olamayacağına göre bazı (belki de çok büyük) tek sayıların çarpanlarının olması *gerektiğini* söylüyor (bu çarpanların ne oldukları hakkında hiçbir fikrimiz olmadığı halde). Gerçekte matematikçiler için özel önemi olan birçok büyük sayı vardır; bu ve bazı benzer yöntemlerle bunların bileşik sayı olduğu bilinmektedir; ancak hiçbir çarpan bulunamamıştır.

Gauss ve onun saat sayıları hakkında son bir öyküyle bu bölümü kapatacağız. Fermat'nın küçük teoreminin ispatında p asal olmak üzere, 1, 2, 3, ..., $p - 1$ sayılarıyla karşılaştık. Bu sayıların hepsini çarparak faktoriyel ifade ile, $(p - 1)!$ elde ettiğimizi düşünelim. Eğer $(\text{mod } p)$ saati ile sayarsak bu sayı neye denk olur? Önce en küçük asalları kullanarak bunu görmeye çalışalım. $p = 2$ için, $(p - 1)! = 1$ ve $1 = -1 \pmod{2}$ dir. $p = 3$ için $(p - 1)! = 2$ ve $2 = -1 \pmod{3}$ tür. $p = 5$ için $(p - 1)! = 24$ ve $24 = -1 \pmod{5}$ tir. $p = 7$ için $(p - 1)! = 720$ ve $720 = -1 \pmod{7}$ dir: Sanki $(p - 1)!$ sayısının "p saati" ile sayıldığında -1 olma eğilimi var gibi görünüyor. Bu kuralın gerçekten, genel durum için de geçerli olduğunu gösterebilirsiniz. Bunun için $(p - 1)!$ çarpımını oluşturan çarpanları ikişer ikişer alarak 1 çarpı $p - 1$ 'in $-1 \pmod{p}$ olduğunu, bütün ötekilerin ise $+1 \pmod{p}$ olduğunu fark ederiz. Örneğin, $p = 11$ için, 2 çarpı 6, 3 çarpı 4, 5 çarpı 9 ve 7 çarpı 8 çarpımlarının hepsi $+1 \pmod{11}$ e eşittir; bunu ikili çarpımların sonuncusu olan 1 çarpı 10 yani $-1 \pmod{11}$ ile çarparak sonuca varırız. Öyleyse bütün p asal sayıları için

$$(p - 1)! = -1 \pmod{p}$$

dir. Eğer p asal değilse $(p - 1)!$ deki sayıların ikisinin çarpımı p olmalıdır, yani $0 \pmod{p}$ 'ye eşittir. Sıfırın her sayıyla çarpımı sıfır olduğu için, eğer p bileşik bir sayıysa

$$(p - 1)! = 0 \pmod{p}$$

olur. İşte burada asallığı saptamak için gerçekten “su geçirmez” bir test var. $(p - 1)!$ sayısı p ile bölündüğünde, eğer p asalda kalan -1 oluyor; p asal değilse kalan 0 oluyor. Ancak bir de kötü haberimiz var. Faktoriyel şeklindeki sayılar, kuvvetlerin tersine, saat aritmetiğini kullanmaya kolayca uygulanamazlar bu nedenle de testin pratik bir değeri yoktur. Başka deyişle, $(p - 1)!$ sayısı p ile bölündüğünde kalanın ne olduğunu bulmak, doğrudan p ’nin çarpanlarını bulmaktan daha fazla zaman alır. Ancak yine de genel sonuç ilginçtir; çünkü bize sayıların asal olup olmadıklarını saptamak için olası bütün çarpanları denemek dışında da yöntemler olduğunu söylemektedir.

Asal sayılar hakkındaki bu teorem Wilson teoremi olarak bilinir ve ilginç bir tarihi vardır: Wilson veya resmi ünvanıyla Sir John Wilson, pek tanınmamış bir İngiliz hakimdi; bu kadar az bir nedenle ölümsüzleşen çok az insan vardır. Teoremi ilk ortaya atan da, ilk ispatlayan da o değildi. Gerçekte onu hiç kanıtlayamamış ve onun hakkında hiçbir şey yayınlamamıştı. Eğer Cambridge Üniversitesi’nde matematik profesörü olan bir arkadaşıyla bir öğle yemeği sırasında probleminden, tesadüfen, bahsetmeseydi böyle bir sonuca da erişemezdi herhalde. O zaman, profesör bunu bir “spekülasyon” olarak yayınlamış ve onu ortaya atanın da Sir John olduğunu söylemişti. Matematik topluluğunun dikkatini çeken bu yayın sonucunda teorem Wilson’un adıyla anılmaya başladı. Daha sonra bu sonucun, bütün bunlardan 100 yıl kadar önce, Baron Gottfried von Leibnitz (Alman filozofu ve matematikçisi, 1646-1716) tarafından bilindiğine değin birçok kanıt olduğu halde Wilson adı sürdü ve sayılar teorisi konusundaki bütün kitaplarda sonsuza dek kutsallaştı.

Bununla ilgili “Gauss öyküsü” daha da hoştur. “Wilson Teoremi” nin 1770’de ilk yayınlanmasının yanı sıra, anlaşılan, bu “varyasyon” (o zaman kanıtlanmamıştı) hakkında bir de tahmin yürütülmüştü: Bunu ispatlanma olasılığı yoktu; çünkü asal sayıları ifade eden bir notasyon bilinmiyordu.

Bu Gauss'a iletiildiğinde, beş dakika içinde, “saat sayılarını kullanarak ispatlamaya girişti ve gerekçenin notasyon değil nosyon olduğunu söyledi. Ancak gerçekte ilk yayınlanan ispat Gauss'unki değildir. Bu şeref, “varsayımın ilk yayınlanmasından bir yıl sonra ispatı veren Fransız matematikçisi ve astronom Joseph Louis Lagrange'a (1736-1813) aittir.

Sayılara meraklı olanlar için Wilson'un teoremi hakkında son bir açıklama verelim. Orijinal teorem $(p - 1)! + 1$ sayısının, ancak ve ancak p asal ise p ile tam bölündüğünü söyler. Aynı ifade daha ender olarak, sadece p ile değil, p^2 ile de tam bölünebilir. Bunu sağlayan 105'ten küçük olan asal sayılar, yalnızca 5, 13 ve 563'tür.

VIII. Bölüm

Kriptografi: Gizli Yazışma Sanatı

Çocukluğumuzda hepimiz ara sıra şifreli bir mesaj, “gizli” bir mesaj yazmaya girişmişizdir sanırım. Onun sadece şifrenin “anahtarının” önceden verildiği kişi tarafından anlaşılabilceği (daha doğrusu çözülebileceği) umulur. Belki de çoğumuz bütün şifreleme (uzmanlarının deyimiyle “kripto” çekmek) sistemleri içinde en basit olanını, alfabenin bir harfini bir başkasıyla değiştirmeyi kullanmışızdır. Örneğin A yerine B, B yerine C, C yerine D, vb., en sonunda da Z yerine A harfini koyduğumuzu düşünelim. O zaman hiçbir ilginç yanı olmayan “BİR SİYAH KALEMİM VAR” mesajı şifrelendiğinde

CJSSJZBILBMFNJNYBS

şeklini alır ve ilk bakışta yeterince gizemli görünür.

Alfabenin herhangi bir harfi yerine herhangi bir başka harf koyabileceğimiz için, bu basit değiştirme yöntemini kullanan çok çeşitli düzenler bulunabilir. Tam olarak söylemek gerekirse $29!$ (29^* faktoriyel) sayıda; bu sayının değeri ise yaklaşık 9 çarpı 10^{30} dur. Şifrelemek için böyle akıl almaz büyüklükte seçme olanağı varken, birilerinin anahtarı bulma (ya da “şifreyi kırma”) olasılığının çok uzak olduğu düşünülebilir. Eğer yalnızca çok kısa bir mesaj (yukarıdaki, “siyah kalem incisi” gibi) iletmek istiyorsak, bu yargı doğru olabilir de; yeter ki yukarıdaki paragrafta verilen A yerine B, B yerine C, C yerine D, vb. örneğindeki gibi aşırı basit bir düzen seçmeyelim.

* 29 sayısı Türkçe alfabesindeki harf sayısıdır. (ç.n.)

Eğer aynı şifre çok sayıda bilgiyi iletmek için kullanılmak istenirse, ne yazık ki 9×10^{30} gibi büyük sayılara karşın, onu “kırmak” çok kolaydır. Burada yakayı ele veren, belli bir dildeki harf ve harf bileşimlerinin rasgele olmamasıdır. Örneğin Türkçede “a, e, de, da, ki, ve, ile, bir, vb., ne” çok sık kullanılır; buna karşın art arda üç sessiz harfe, ğ ile başlayan sözcüklere pek raslanmaz. Dilin bu “parmak izleri”ni ve de ortaya çıkan farklı harf bileşimleri hakkında sayısız başka istatistiksel ipuçlarını kullanarak, bir “şifre çözücüsü”nün harfleri değiştirmeye dayanan böyle basit bir sistemi çabucak çözme olanağı vardır. Harfler yerine bir dizi anlamsız işaret konulsa bile fark etmez; yine de dilin kendi düzeni, sonunda, onları ortaya çıkarır ve gizli mesajımız kısa sürede herkese mal olur. Akla gelen ikinci bir şifreleme planı da, harfleri birbirleriyle değiştirmek yerine, “yer değiştirme” ya da karıştırma yöntemidir. Örneğin, “anahtar” olarak 3, 1, 5, 2, 6, 4 sayı dizisini aldığımızı düşünelim ve “BİR SİYAH KALEMİM VAR” mesajını bu diziye göre şu şekilde şifreleyelim: Birinci harfi üçüncü konuma, ikinci harfi birinci konuma, üçüncüyü beşinciye, son alarak da altıncı harfi dördüncü konuma getirelim. İlk altı harfi bu şekilde yer değiştirdikten sonra, daha sonra gelen altı harfe de aym şeyi uygulayalım ve bunu mesaj bitinceye kadar yineleriz. Böylece orijinal mesajın ilk altı harfi İSBYRİ olur; ikinci altı harfi ise HAAEKL. Böyle devam ederek şifreyi tamamlarsak

İSBYRİHAAEKLİVMRMA

elde ederiz. Bu sistemi kullanan çok kısa mesajlar çoğu kez tek bir şekilde kırılmazlar (örneğin kodlanmış mesaj, ya da “şifre” olan mesaj ADKİR, 31254 anahtarıyla KADİR, ya da 31245 anahtarıyla KADRI olur); daha uzun mesajlar da yine oldukça güvensizdir. Ayrıca bunların İngilizce metinler için genel “çözüm” yöntemleri, anahtardaki sayı dizisinin uzunluğu hakkında hiçbir bilgi olmadığı durumlar için bile, ta 1878’de yayınlanmıştır. Böylece, yer değiştirmeye dayanan en basit şifreleme sistemi, harf değiştirme sisteminde olduğu gibi, ancak çok sınırlı ölçüde güvenlik sağlamaktadır.

Şifreleri kırmayı biraz daha zorlaştırmak için ne yapılabilir? Bir kere, yerine koyma sistemini, orjinal metindeki her harfi hep aynı harfle değiştirmeyerek, güçlendirmek düşünülebilir. Bunu gerçekleştirmenin bir yolu bir sözcük seçip (örneğin KADİFE) bunu şifrelenecek mesajın altına tekrar tekrar aşağıda görüldüğü gibi yazmaktır:

BİR SİYAH KALEMİM VAR KAD İFEKA DİFEKAD İFE

B harfi Türkçe alfabenin 2. harfi, onun altındaki k de 14. harfi olduğu için mesajın ilk harfini alfabenin, 2 ve 14'ün toplamı olan 16. harfi olan "M" ile kodlarız. Benzer şekilde, mesajın ikinci harfinin yerine, İ (12) ile A (1)'yı "toplayarak" bulduğumuz J (13) koyarız. Bu toplama sürecinde 29'dan büyük bir sayı çıkarsa yapacağımız şey yeniden alfabenin başına dönmek, "A" için 30, "B" için 31, vb. sürdürmekten ibarettir. Bu örnekteki anahtar kullanarak yukarıdaki mesajın tümü, çözümü zorlaştırmak için aralıkları da kapatarak

MJÜDÖDLİÖJSİAJRHGV

haline dönüşür.

Genellikle Vigenere şifresi denilen bu tür bir kodlama sisteminde, orijinal mesajın belirli bir harfinin yerine hep aynı harfi koymak gerekmiyor. Görüldüğü gibi, mesajdaki ilk "İ" harfi "A" ile kodlanıyor; ikinci "İ" ise "F" harfiyle kodlanıyor. Şifreyi kırmaya çalışan birisini şaşırtmak için bunun yardımcı olacağı ve daha önceki iki sistemden daha güvenli olduğu düşünülebilir. Ne var ki, bu doğru olsa bile, yukarıda verilen türden Vigenere şifreleri yine de kolayca deşifre edilebilir. Gerçekten, bu yöntem için de 100 yılı aşkın bir zaman öncesinde, oldukça genel bir çözüm yöntemi geliştirilmiştir Buradaki zaaf anahtar sözcüğün art arda yazıldığı satırdadır (örneğin yukarıdaki KADİFEKADİFEKADİFE...). Bunun gibi altı harfli bir anahtar sözcük, sıkça kullanılan "bir" ve "ile" gibi sözcükleri hep üç harfin altı kombinasyonlarından belir-

li birisi ile değiştiriyor. Buna benzer ipuçları, sonunda anahtarı ele verir ve şifre çözülür. Sorun yine herhangi bir dilde harf ve sözcüklerin rastlantısal olmayan bir biçimde ortaya çıkmasından kaynaklanıyor.

Ancak anahtar olarak kendini hiç yinelenmeyen bir metin kullanırsak ne olur? Bu “koşan-anahtarlı Vigenere şifreleri”nde çok rastlanan ele verici harfler ve sözcükler şifrelenediklerinde hiç yinelenmezler ve nihayet kırılmayan bir şifre elde etmemize yol açarlar. Gerçekten de, ilk icat edildiklerinden nerdeyse üç yüzyıl sonra bile, bu koşan-anahtar şifrelerinin tamamen güvenli oldukları düşünülüyordu. Ancak, 1883’te bu tür şifreleri bile kırabilecek bir yöntem açıklandı. Çözümlerine yol açan ipucu yine harflerin ve sözcüklerin, bu defa hem mesajda hem de anahtarda rastlantısal olmayan sıklıkta görülmeleriyle ilgilidir. Örneğin “E” harfinin yine “E” harfiyle değiştirilme olasılığı % 1,69 kadardır; başka herhangi belirli bir harfle değiştirilme olasılığı daha da küçüktür (ama o da bellidir). Açıkça görüldüğü gibi, bu tür şifre kırma, yukarıda anlatılanlardan çok daha güçtür ve ipucu verici ilişkilerin ortaya çıkması için oldukça uzun bir şifre gerektirmektedir. Ancak bunlar eninde sonunda ortaya çıkmakta ve şifre kırılabilir. 1950’lerden bu yana hızla gelişen bilgisayar teknikleri bu koşan-anahtar şifresini her zamandan daha zayıf duruma getirmiştir.

Ne yapılabilir? Anlaşılan şifrenin kusuru, koşan-anahtar için bir metin kullanılmasında yatmaktadır. Koşan-anahtar için tümüyle rasgele ve hiç tekrarlanmayan bir dizi harf kullanıldığını düşünelim. Bu durumda, mesajın metnindeki *her harfin*, ister en olası “A” ister en az olası “Ğ” ya da “J” olsun şifredeki *herhangi başka* bir harfle değiştirilme olasılığı *aynıdır*. Böyle bir sistemde şifre kırmanın dayandığı semboller arası ilişkiler ve sıklıklar tamamen giderilmiş olmaktadır. Nihayet tam güvenceli bir sistem bulunmuştur. Ancak ne yazık ki bu sistem de oldukça kullanışsızdır; çünkü metnin her harfi ve sembolü için ayrı bir sembol ya da anahtar gerekmektedir (gönderenden alıcıya ulaştırılacak). Bu sakıncanın, rasgele olsun olmasın, herhangi bir koşan-anahtarlı Vi-

genere şifresi için de geçerli olduğu ileri sürülebilir. Ancak önemli bir fark vardır; rasgele olmayan anahtar için uygun bir yerden, örneğin tanınmış (ya da pek tanınmamış) kitapların belirli bölümlerinden bir metin alınabilir. Halbuki rasgele anahtar, amaçlanan alıcının üzerinde veya sakladığı bir yerde olacaktır ve “düşman”ın eline geçtiğinde onun olağandışı görünüşü hemen kuşku uyandıracaktır. Önceleri, bu sorunu aşmak için yine uygun olan ancak tekrarlayan rasgele anahtarın ezberlenebileceği düşünülmüştü. Ancak, harf seçimindeki sıklık bakımından rasgele olsa da yeterince uzun bir mesaj için anahtarın tekrarlanıyor olmasının şifreyi kırmak için yeterli olduğu anlaşılmıştır.

Burada kaçınılmaz bir sonuç ortaya çıkıyor; tam güvence için anahtar rasgele olmalı, hiç tekrarlanmamalı ve bu nedenle de şifrelenecek mesajların toplam uzunluğunda olmalıdır. Bu ifadeye bile son bir koşul eklemeye gerek vardır. İfade ancak, şifrenin kendisi de en azından mesaj kadar karmaşıklık (bunun için bazen kullanılan sözcük “entropi”dir) içeriyorsa doğrudur. Bunun için temelde, anahtarın en azından alfabedeki sayı kadar değişik semboller içermesi gereklidir. O halde, eğer anahtar alfabedeki 29 harfin hepsinin rasgele seçilmesine dayanıyorsa mesaj güvencedir. Öte yandan, tamamen rasgele olan, hiç tekrarlanmayan ve mesajdan daha kısa olan; ancak güvenceli olmayan bir “entropi” dizisi oluşturmak da olanaklıdır.

Buna abartılı bir örnek olarak, aşağıdaki gibi, birlerden ve ikilerden oluşmuş tümüyle rasgele bir sayı dizisini alalım:

11212222212122212121111

Gerçekte bu dizi masamda yazı-tura atarak (tura için 1, yazı için 2) elde edilmiştir. Eğer 1 sayısını “mesajdaki bu harfi alfabenin bir sonraki harfiyle değiştir” (yani A’yı B ile, B’yi C ile vb.) ve 2’yi “mesajdaki bu harfi alfabedeki iki sonraki harfle değiştir” (yani A’yı C ile, B’yi Ç ile vb.) şeklinde yorumlarsak kırmızı kalem kutusuyla ilgili mesajımız şu şekilde şifrelenir:

CJSSKACİLCMGOKNZBS

Eğer “bir ve iki kaydırma” anahtarından kuşku duyuluyorsa, deşifre etmenin çok büyük sıkıntı çekmeden başarılabileceğine sanırım siz de katılırsınız.

Her harf yerine rasgele bir başka harf koyarak elde edilen bir kullanımlık alfabetik anahtarın, kırılmayacak şifre probleminin çözümü olduğu anlaşılmaktadır. Güvenli olması nedeniyle uygulanan bu tür bir kullanımlık anahtarlar yakalanan yabancı gizli ajanlar üzerinde defalarca ele geçmiştir. Bunun iyi bilinen bir örneği 1957 yılında New York’da yakalanan Sovyet ajanı Albay Rudolph Abel’dir. Washington ile Moskova arasındaki “kırmızı hat”ın da aynı tür bir sistemi (kuşkusuz tümüyle otomatik hale getirilmiş olarak) bir defalık anahtarla kullandığı bildirilmiştir.

Kesin güvenli olmalarına karşın bu bir kerelik anahtar sistemlerinin, örneğin savaş dönemlerinde olduğu gibi, çok miktarda gizli bilgi aktarmak gerektiği durumlar için hiç elverişli olmadığı açıktır. Gerçekten de İkinci Dünya Savaşı sırasında sürekli iletişim için kullanılan sistem, çok uzun, ama pratik olarak, sonuçta, tekrarlayan, harf-yerine-harf koyma anahtarlı sistemdi. Savaş döneminin ünlü şifreleri, Almanların ENIGMA, İngilizlerin TYP EX, Amerikalıların SIGABA ve Japonların RED and PURPLE adlı makine şifreleri bu türdendi. Bu nedenle hepsinin geliştirilmiş istatistiksel yöntemlerle “kırılma” olasılıkları vardı. O dönem belki de şifre kırmanın altın çağıydı ve bu, çoğu zaman korkunç derecede güç bir işti. Gerçekten de, Amerikalılar, Japon şifresi PURPLE’ı kırmayı, deneyimli bir şifre-kırma ordusunun bir yıldan daha uzun süren “şifre analizi” uğraşları sonucu nihayet 1940 yazında başarabildiler.

Genel olarak şifreler, şifre çözücüyü istatistiksel kanıtlardan yoksun bıraktıkları ölçüde zor kırılırlar. Hiç bitmeyen ve hiç tekrarlanmayan, rasgele anahtar kullanma dışında harf değiştirme sistemlerine, her seferinde, tek harf yerine iki ya da üç harf koyarak da şaşırtmaca eklenebilir. Bu, dil kalıplarının istatistiksel kanıtlarını tümüyle orta-

dan kaldırmasa da, çok basit anahtarlar elde etmeyi sağlayabilir; olası şifre kırıcısının istatistik sularını bulandırdığı da kesindir.

Böyle bir yöntem için düşünülebilecek en basit sistem alfabenin harflerini bir beş-harf çarpı beş-harf kare şeklinde düzenlemek olabilir. (Türkçede Ç, Ğ, İ, Ö harfleri yerine C, G, I, O kullanılmasının mesajları pek bozmayacağı düşünüldükçe Ç, Ğ, İ, Ö harfleri atlanmıştır). Harfler bu kare içine rasgele bir biçimde yerleştirilir. Örneğin

TZRME
KOAYP
FVDBN
UHGJS
CLÜŞİ

ve basit bir kural uyarınca, bir harf ikilisi yerine bir başka harf ikilisi konur. Örneğin, eğer iki harf aynı sırada ya da aynı sütunda değilse, basit değişim kuralını açıklamak için, TO ile KZ, PR ile EA ve RS ile GE'nin yer değiştireceğini söylemek yeterlidir. Aynı sırada olan harfler için "bir sıra yukarı" gibi bir kural kullanılabilir. Öyle ki, örneğin GH, DV'ye, TE de CI'ya gider (kare anahtarının "kenarları olmayan" bir duvar kâğıdı motifi gibi kendini yinelediği düşünüldükçe). Bunun gibi, aynı sütundaki harfleri, diyelim ki, bir sağ sütuna taşıyabiliriz; örneğin ÜA'yı ŞY'ye, PI'yı KC'ye götürebiliriz. Bu sistemi kullanırsak

BIRSIYAHKALEMIMVAR

şeklindeki siyah kalem mesajımız şimdi

ŞNGEPŞGOTRZİEŞBZYM

olur. Bunun doğruluğu, kare anahtarını ve yukarıda verilen kuralları kullanarak kolayca saptanabilir.

Bu tür yöntemler giderek daha karmaşıklaştırılabilir ve harfleri üçlü, dördü, hatta beşli gruplar halinde değiştirilerek bulunan sistemler, kırılması aynı ölçüde zorlaşan şifrelere yol açarlar; bu yolla şifre-kırıcı için son derece güç hale getirilebilirler. Anahtarın olağanüstü kısa ve özlü olması (harfleri değiştirme yöntemleri ezberlenecekse) onlara bir üstünlük sağlar. Başlıca kusurları ise, şifreleme ve deşifre etme süreçlerinin görece güç ve zaman alıcı olması; daha büyük güvence için süreçler daha karmaşık duruma getirildikçe hata yapma olasılığının giderek artmasıdır.

Buraya kadar tartışılan bütün şifre sistemleri, her ne kadar biçim ve güvenlik bakımından birbirlerinden farklıysalar da, hepsinin ortak bir yanı vardır: Bunlar, herhangi bir bilgi iletilmeden önce, hem şifreleyen hem de amaçlanan alıcının şifrenin anahtarına sahip olması anlamında *simetrik*tirler. Bu, uygulama bakımından kolay olmadığı gibi güvenlik bakımından da çok sakıncalıdır. Çünkü bir yandan bilginin verilmesi gerekebilecek *her* kişinin ya da kurumun önceden saptanmasını, öte yandan onların her birine anahtarın verilmesini (bu yüzden de gizliliği korunmalarını) zorunlu kılmaktadır. Eğer amaçlanan bu alıcıların herhangi birisi anahtarlarla birlikte “düşman”ın eline düşerse sistem çöker; hiçbir işe yaramaz.

Yakın zamana kadar buna verilen genel tepki “Çok fena, ama ne yapalım ki çaresi yok!” biçimindeydi. İnanması güç ama öyle olmadı. Bu şaşırtıcı gerçek ilk kez 1970 ortalarında fark edildi. Eğer bu bölümün sayılarla ne ilgisi olduğunu (iş ya da eğlence bakımından) anlamadığınızı düşünmekteyseniz yanıt işte “tam burada”, *asimetrik* şifrededir. Bu görüş ilk olarak 1976’da, Kaliforniya’da Stanford Üniversitesi’ndeki bir grup araştırmacı tarafından yayınlandı. Ona, “açık anahtar” şifreleme sistemi adını verdiler; çünkü, onu kullanan kişi, (aşağıda açıklanacağı gibi) bütün dünyaya, kendisine gizli mesaj göndermek isteyenlerin nasıl bir şifre kulanmaları gerektiğini ilan edebiliyor. Bu, örneğin bir genel katalogla yapılabilir. İnanılması güç ama, herkes ona şifreli bir mesaj gönderebilir; ancak, onu deşifre edebilecek tek kişi

kendisidir. Bunun sonucunda, iletişim kurmak isteyen olası iki kişinin önceden aynı anahtarlara sahip olması ve onu yaşamı pahasına korumasına hiç gerek kalmamaktadır. Her alıcı kendi şifre çözme sırrını biliyor, onu koruyacak tek kişi de yine kendisi oluyor. Örnek olarak, düşman saflarını araştırmaya giden bir keşif kolunun başı olan bir komutanı ele alalım. Gözcülerin her biri haberleri düşmandan gizli olacak biçimde geriye, ona gönderebilmelidir. Artık düşmanın şifreleme makinelerinden birini ele geçirmesinin ve şifre “anahtarı”nı keşfetmesinin zerre kadar önemi yoktur; çünkü onlar aynı anahtarı taşıyan başka şifreler ele geçirdiklerinde bu bilginin şifreyi çözmede hiçbir yardımı olmayacaktır. Sistem güvencededir; deşifre etme sırrına (ya da uygulama da, deşifre makinesine) yalnızca komutan sahiptir.

Kodlama talimatını yayınlayarak onları herkesin eline veren olası alıcı kriptografik sırrın yarısını, bilerek, açıklamış oluyor. Bunu yapmaktaki amacı, herkesin (gerekli beceriye sahip olan herkesin) hatta varlığından haberdar olmadığı kişilerin, ona bilgi kodlamalarını sağlamaktır; ancak yine de şifreyi çözmek için bilinmesi kesinlikle gereken anahtarın öteki yarısını dünyada bilen tek kişi kendisi olacaktır. Bütün bunlar biraz da büyücülüğü çağrıştırıyor gibi. Bu sürecin nasıl işlediğini anlamak için durumu biraz basitleştirmemiz gerekiyor; çünkü bunun makinelerde bilfiil uygulamasında çok büyük sayılar söz konusu olmaktadır. Biz bu yöntemi, büyük-lüklerin yol açtığı karmaşa ile şifre kırıcıyı başarısız kılan büyük sayılar yerine, kâğıt kalemin (ya da en çok bir cep hesap makinesinin) yeterli olacağı küçük sayılarla açıklayacağız.

İki asal sayının çarpımı olan bir sayı düşünün. Açıklama için ben (ikisi de asal sayı olan) 2×7 olan 14 sayısını seçiyorum. Asal sayıların her ikisinden 1 çıkarın, 1 ve 6 elde edersiniz. Şimdi de bu son iki sayıyı çarpın. “Niçin?” diye sormayın; bana güvenin... şimdilik bana güvenin. Bu yeni sayıyı yani $1 \times 6 = 6$ 'yı Yunan alfabesindeki ϕ harfi ile gösterelim. Bu sayının hem şifreleme hem de deşifre etme sistemlerinde, ileride göreceğimiz gibi, çok özel bir önemi vardır. Şimdi ϕ ile ortak çarpanı olmayan başka bir sayı seçiyorum. $\phi = 6$ 'nın çar-

panları 2 ve 3 olduğundan 2 veya 3 ile tam olarak bölünmeyen *herhangi* bir sayıyı seçebilirim. Bu özellikleri taşıyan en küçük sayı olduğu için 5'i seçiyorum; çünkü bu "basit" örnek için sayıların olabildiğince küçük olmasını istiyorum.

Genel katalogda yayınlayarak açıkladığım sayılar ilk seçtiğim 14 ile bu 5 sayısıdır. Bana bir mesaj kodlamak için şunları yapacaksınız: önce alfabedeki harfleri $A = 1$, $B = 2$, $C = 3$, vb. sayılarıyla değiştireceksiniz. Şifrelemek için, herhangi belirli bir harfe karşılık gelen sayının beşinci kuvvetini (5 benim katalog sayılarının birincisidir) alacaksınız ve bulduğunuz sayıyı 14'e (katalogdaki ikinci sayıya) böldükten sonra sadece kalan sayıyı not edeceksiniz. Bu son işlem, bir önceki bölümdeki dili kullanırsak, 14'lü saate veya (mod 14)e göre saymak anlamına geliyor.

Çok kısa ve kolay bir sözcüğü kodlayarak bunun nasıl yapıldığını açıkça görelim. Sözcük ÇABA olsun. Önce harfleri sayılara dönüştürerek $A = 1$, $B = 2$, $C = 3$, $Ç = 4$... kuralı ile sözcük 4121 olur. Bunu şifrelerken

$$4^5 = 1024 = 73 \times 14 + 2$$

$$1^5 = 1 = 0 \times 14 + 1$$

$$2^5 = 32 = 2 \times 14 + 4$$

$$1^5 = 1 = 0 \times 14 + 1$$

$$5^5 = 3125 = 223 \times 14 + 3$$

ya da buna denk olarak, saat diliyle

$$4^5 = 2 \pmod{14}$$

$$1^5 = 1 \pmod{14}$$

$$2^5 = 4 \pmod{14}$$

$$1^5 = 1 \pmod{14}$$

olduğunu hatırlayarak, kalan dizisi olan 2141 elde ederiz. Öyleyse 2141, bu özel sistemde ÇABA sözcüğünün şifrelenmiş halidir. Onu deşifre etmek için, 2141'yi 4121'e ya da onun alfabetik ifadesi olan ÇABA sözcüğüne gidecek "anahtar"ı bilmek gerekiyor. O anahtar nedir? Anahtar aslında,

yalnız şifrenin alıcısının bildiği bir sayıdır. Onu elde etmek için de Φ sayısının bilinmesi gerekir. Açıkça ifade edersek, bu sayı katalogdaki birinci sayıyla çarpıldığında (örneğinizde 5), Φ 'li gruplarla (örneğinizde 6'lı gruplar) sayıldığında 1 kalanını veren sayıdır. Öyleyse, basit örneğimizde “şifre kıran” gizli sayı 11'dir; çünkü

$$5 \times 11 = 55 = 9 \times 6 + 1$$

ya da, saat sayısıyla

$$5 \times 11 = 1 \pmod{6}$$

Şimdi, deşifre etmek için, şifrelediğimiz yolu izleriz; ancak, şifre sayılarının yükseltilecekleri kuvvet olarak gizli 11 sayısını kullanırız. 2141 şifresini ele alarak, kalanları hesaplarız.

$$2^{11} = 4 \pmod{14}$$

$$1^{11} = 1 \pmod{14}$$

$$4^{11} = 2 \pmod{14}$$

$$1^{11} = 1 \pmod{14}$$

Bu harikalar harikası bir şey; şifrelenmemiş orijinal 4121 sayısı, ya da ÇABA elde edildi. Φ sayısını içeren bu kuralla yukarıda görüldüğü gibi şifrenin nasıl tam olarak çözüldüğü sorusunun yanıtı ileri matematik ve saat sayılarının gizemlerinde yatmaktadır. Sayılar ne kadar büyük olursa olsun yöntem geçerlidir. Bu önemli bir noktadır; çünkü eğer çok büyük sayılara uygulayamazsak (kuşkusuz, şifreleme ve şifre çözme için bilgisayar kullanılarak) yeni herhangi bir şey başarmış sayılmayız.

Örneğin, yukarıda verilen basit örnek, harfleri harflerle değiştirmeyi daha karmaşık biçimde yapmaktan farklı bir şey değil. Gerçekte bunda bile başarılı değil; çünkü $\pmod{14}$ e göre saydığından, sadece 13 tane farklı kalan olabilir, ama, noktalama işaretlerini, aralıkları vb. kodlamasak bile, alfabede 29 tane harf var. Ayrıca, $4121 = \text{ÇABA}$ ile bir

başka olanak, 4121 = ÇAR (R, alfabenin 21. harfi), arasında ayırım yapmıyor. Bu son sorun alfabenin her harfi için iki rakam kullanarak kolayca aşılabılır; yani, A = 01, B = 02, C = 03,..., V = 27, Y = 28, Z = 29. Bu sistemde ÇABA sözcüğünün sayısal şekli 04010201 olur, ama ÇAR artık tamamen farklıdır: 040121. Bu sistemin bir başka yararı daha var, 30'dan 99'a kadar olan sayılar başka kullanımlara açıktır; ! @, #, *, (,), \$, &, ?, ve başka birçok farklı sembol için kullanılabilirler.

Asimetrik kodlamanın ne kadar güçlü olduğu, büyük sayılar kullanıldığında, iki şekilde ortaya çıkar. Örneğin, başlangıç sayısı olarak (basit örnekteki 14 yerine) her biri, 30 basamaklı iki asal sayının çarpımı olan 60 basamaklı bir sayı aldığımızı varsayalım. Şimdi, bir seferinde art arda, gelen 30 harf ve sembolden oluşan (her sembol için 2 rakam) şifre artık bire bir (harf) koyma değil otuza otuz koyma şeklinde çok değişik bir şekle dönüşmüştür. Bir örnekle açıklayalım. Otuz "harfli" orijinal metindeki tek bir harfin, örneğin 14 sayılı harfin değiştirilmesi, aynı 30'lu takımın şifrelenmiş durumdaki iki rakamlı otuz "harf"inin hepsini birden değiştirebilir. Bu nedenle, şifre kırıcı gizli şifre çözme sayısını (basit örnekte 11) bulmadıkça şifrenin kırılması söz konusu değildir. *Ben o sayıyı bulabilirim*, çünkü ilk seçilen iki asal sayının kimliklerini tam olarak biliyorum. Öyleyse Φ hesaplanabilir ve onu kullanarak şifreleme ve şifre çözme için gereken kuvvetler, basit örnekte yapıldığı gibi; tam olarak seçilebilir. Şifre kırıcı da, ancak eğer benim 60 basamaklı sayımı iki tane 30 basamaklı asal çarpana ayırabilirse, aynı şeyi yapabilir.

Yukarıda anlatılan asimetrik kodlama sisteminin başarısının sırrı, 30 basamaklı sayıların asal olup olmadıklarının saptanmasının (günümüz bilgisayarlarıyla) görece kolay olması; buna karşın 60 basamaklı bir sayıyı, 30 basamaklı iki asal çarpana ayırmanın ise çok zor olmasıdır. Bu nedenle seçtiğim 60 basamaklı sayıyı genel katalogda yayınlayabilirim, çünkü herkes onu bilse bile hiçkimsenin onu çarpanlara ayırarak şifreyi kırmayı başaramıyacağına güvenirim. An-

cak asimetrik kodları “kıırma” probleminin bu meydan okuyuşu ile harekete geen arpanlara ayırma yntemleri, gnmzde (bir sonraki blmde ele alınacaėı gibi) ok byk hamlelerle geliřmeye bařlamıřtır. Bunun sonucunda, 60 basamaklı kodlama sayıları gvenlik bakımından řimdiden “sallanmaya” bařlamıřlardır. řimdilerde, uzunluėu yz veya daha fazla basamaklı olan sayılar tercih edilmektedir.

Bu, gvenli asimetrik kodlama sistemlerinin keřfi, kriptografi bilimini yakın gelecekte tmyle deėiřtirecek gibi grnyor. Ancak sorunlar da var olmayı srdryor. Bunların belki de en nemlisi, grece gvenli olan simetrik sistemlere kıyasla (en azından řimdilik) ok fazla bilgisayar sresi gerektiren karmařık řifreleme ve řifre zme sistemlerini kullanmasıdır. Eėer bu fark kaınılmaz ise, simetrik ve asimetrik olan řifreleme sistemlerinin her ikisi de var olmayı srdrecek ve belirli uygulamaların gereklerine uygun olarak her ikisi de kullanılacak demektir. Uygulamada kullanıldıkları biimleriyle bunların her ikisi de kırılmaz deėildir (1970’lerin sonlarında asimetrik řifrelemenin keřfini hal-ka aıklayan gazete manřetlerinin iddialarına raėmen). Nasıl ki simetrik harf deėiřtirme sistemleri hibir zaman tek-rarlanmayan, yeterince “entropi” ieren rasgele anahtar sınırına geldiklerinde ancak kırılmaz duruma geldiler; asimetrik sistemler de, ancak sonsuz uzunlukta sayılar kullanmakla, soyut sınırlar iinde kırılmazlıėa ulařabilirler. Asimetrik sistemlerin temel stnlė tm anahtara sadece olası alıcının sahip olmasını gerektirmesindedir. Bu nedenle, fiziksel bakıř aısından (teknolojik bakıř aısının tersine) olaėanst gvenlidir.

IX. Bölüm

Sayılar ve Ulusal Güvenlik

$2^{193} - 1$ sayısının asal çarpanları nelerdir ve bu kimin umurundadır? Hatırlayacağınız gibi çarpanlar, birbirleriyle çarpıldıklarında söz konusu sayıyı oluşturan sayılardır. Bu tanımlamayla, sorumuzun ilk bölümünün yanıtı 13.821.503, 61.654.440.233.248.340.616.559 ve daha da büyük olan 14.732.265.321.145.317.331.353.282.383'tür ve hepsi de asal sayılardır. Sorunun ikinci bölümünün yanıtı, inanması zor da olsa, ABD Hükümeti'dir. Sizin "Şaka mı yapıyorsun?" dediğinizi duyar gibiyim; ancak bu kesinlikle bir şaka konusu değildir. Söz konusunu olan, bilgisayar güvenliği ve hızla artan, bilgisayar hileleri, hırsızlığı ve casusluğu konularıdır.

Büyük bilgisayar sistemleri yeterli düzeyde koruma gerektirir ve bu tür bilgisayarlar ortaya çıkalı fazla zaman geçmediğinden, şirket yöneticileri ve hükümet görevlileri korumayı nasıl sağlayacaklarını yeni yeni anlamaya başlamışlardır. Geçmişte, duyarlık gerektiren yazıların kilitlenmesi gerektiğinde herkes hem fikirdi. Ancak tellerden akan elektroniklerin, saç inceliğindeki cam liflerden geçen ışık atımlarının nasıl güvenceye alınacağını kavramak kolay değil. Bilgisayar sistemleri, kapısını kilitleyerek kolayca güvence altına alınabilen bir odaya konulmuş büyük metal kabineler ve dönen manyetik diskler çağından, hızla, bütün bir binada, bir şehirde hatta bütün dünyada terminaller içeren sistemlere dönüşmüşlerdir.

Bu iletişim ağları çok şaşırtıcı ve beklenmedik biçimlerde tehlikeye açıktırlar. Sistemin fiziksel yöntemlerle korunması artık mümkün değildir ve bilgisayar programlarının ken-

dilerine yazılmış korumalara yoğunlaşmaktadır; son bölümde tartıştığımız gizli şifrelerin kullanımı gibi. Bununla ilişkili durumlar, bankalar arası para transferlerini (örneğin büyük bankalar müşterileri için günde *milyarlarca* dolar para içeren elektronik işlemler yapar) veya ulusal güvenlik işlerini bile içerebilmektedir. Ayrıca, ABD ve Avrupa'da sürekli birbirleriyle konuşan (para transferleri yapan ve önemli bilgi aktaran) 100.000'den fazla bilgisayar merkezi olduğu gerçeği ile birleştiren problem boyutu ortaya çıkmaktadır. Bilgisayar destekli suçlara atfedilen kayıpların şimdiden yılda *milyarlarca* dolara vardığı tahmin edilmektedir. Bütün bunların, sayıların çarpanlara ayrılmasıyla ne ilgisi olabilir? Son bölümdeki gezintilerimizi sonuna kadar izleyenler bunu şimdiden biliyor. Geriye kalanlar (yazıklar olsun!) için kısaca açıklayacağım.

Bundan on yıl kadar önce, bilgisayar güvenliği sorunu ilk gündeme geldiğinde, iki büyük asal sayının çarpımından oluşan çok büyük sayılara dayanan bir şifreleme yöntemi içeren bir koruyucu sistem önerildi. Bunun anlamı, çarpım olan sayı verildiğinde şifrelemenin, ancak onun iki asal çarpanının saptanması halinde kırılabileceğiydi. Sistem temelde, büyük asal sayıların bilgisayar yoluyla saptanması kolay olduğu halde (çarpımları bulmak daha da kolaydır), ters problemin, yani büyük sayıların asal çarpanlarını bulmanın çok zor olmasına dayanıyordu. Örneğin, birçok modern bilgisayar algoritmalarını kullanarak, 40 basamaklı asal sayıları bulmak ve birbirleriyle çarparak 80 basamaklı bir sayı oluşturmak sadece birkaç dakika alır. Ters problem olan 80 basamaklı bu bileşik sayıyı çarpanlara ayırmak ise, günümüzde (bu sayıyı dikkatle hazırlayanlar dışında herkesin) araştırma kapasitesinin en uç sınırındadır. Bu nedenle böyle bir sayıyı temel alan şifreleme sistemi oldukça güvenilirdir. Ancak ne kadar zaman için? Bir zamanlar matematiğin en ilgi görmeyen alanlarından birisi olan çarpanlara ayırma araştırmaları, şifreleme ve bilgisayar güvenliğiyle ilgili olduğu için artık en faal alanlarından birisidir. Bu nedenle sayılar ve çarpanları üzerinde biraz duracağız.

Her tamsayı çok özel bir şekilde, kendine özgü bir kişiliği olacak şekilde, asal sayılardan oluşur. Bunun nedeni, her tamsayının bir ve sadece belirli bir asal sayılar kümesinin çarpımı olmasıdır. Örneğin, 60 sayısı, 2 çarpı 2 çarpı 3 çarpı 5'tir. Bu 2, 2, 3, 5 sayılarına, 60 sayısının asal çarpanları denilir. 60 sayısı verildiğinde, 2, 3, 5, 7, 11,... asal sayılarının her birisinin en küçükten başlarayarak, 60 sayısını tam olarak bölüp bölmedikleri test edilir, ta ki en küçük "çarpan" bulunsun. 60, bu sayıyla bölünür, aynı süreç tekrarlanarak daha büyük asal çarpanlar bulunur. Sayı büyüdükçe çarpan bulma işi daha da sıkıcı olur; ancak bu, en azından ilke olarak her tamsayıya uygulanabilen bir yöntemdir. Eğer sayının kareköküne kadar olan bütün asal sayılar denenmiş ve bir çarpan bulunamamışsa o zaman sayının kendisinden ve birden başka çarpanı yok demektir; öyleyse asal bir sayıdır.

Bu demektir ki, kıyaslanabilir büyüklükteki sayıları (örneğin 10 basamaklı sayıları) çarpanlara ayırmak hepsi için aynı ölçüde zor değildir. Birçok küçük asal çarpan olan sayılar, çarpanlara ayrılmış son durumlarına, küçük çarpanları olmayan sayılardan daha kolay ayrışırlar. Basamak uzunlukları aynı olan sayılardan birinci gruptakilere çarpanlara ayırması "kolay sayılar" ikinci gruptakilere de "zor sayılar" denir. Yukarıda verilen kaba kuvvete dayanan çarpanlara ayırma yönteminin "zor sayılara" uygulanması basamak sayısı arttıkça daha da zorlaşır. Böylece, örneğin bu bölümün başında değinilen zor sayının ondalık ifadesinde 58 basamak vardır. Günümüzde, her nano saniyede (*mil-yarda* bir saniye) bir bölme işlemi yapabilen en hızlı bilgisayarlar kullanıldığında bile, gösterilen yöntemle çarpanları bulmak 35.000 yıllık bir bilgisayar süresi gerektirir. Çarpanların bu yöntemle elde edilmediği aşikârdır. Onlar 1983 yılında Albuquerque, New Mexico'daki Sandia Ulusal Laboratuvarında çalışan bir grup tarafından 100 dakikadan biraz daha az bir sürede saptanmışlardı. Güçlü bir bilgisayara yanında, çok daha hızlı bir çarpanlara ayırma yöntemi uygulanmışlardı.

Bu yeni yöntem, çarpanlara ayırma konusunda en son gerçekleştirilen, büyük bir atılımdı ve Hollandalı matematikçi Hendrik Lestra tarafından bulunmuştu. Yöntem hem basitliği hem de yaratıcılığı bakımından matematik toplumunda sürpriz ve memnuniyetle karşılandı. Ancak ne yazık ki (ama bir kriptograf iseniz, şansınızdan) bir zayıf noktası vardır. Birbirinden önemli ölçüde farklı asal çarpanlar olduğu durumlarda verimliydi. Asal Çarpanları yaklaşık aynı büyüklükte olan sayılar için ise ancak önce bilinen en iyi yöntemler kadar hızlı olabiliyordu. Lenstra'nın yöntemi sayı "teorisyenleri" için çok önemlidir. Çünkü sayıların çoğunluğu bu ikinci türden değildirler. Fakat, bir önceki bölümde tartıştığımız gibi, asimetrik kriptografide kullanılan büyük sayılar, özellikle, sadece birbirine yakın iki asal çarpanı olacak şekilde oluşturulur. Bu nedenle çarpanlara ayırma konusundaki bu son gelişmeye karşı dokunulmazlıkları sürmektedir. Ancak bu ne kadar sürebilir?

Lenstra'nın yöntemi, çarpanlarla ilgilenen topluluğu, kısa vadede ikiye bölebilir; sayıcılar ve şifre kırıcılar. Sayıcılar sayıları, çarpanları olduğu için çarpanlara ayırırlar. Onların pul koleksiyoncularına benzedikleri söylenmiştir; sayı koleksiyonlarındaki boş yerleri doldurmaya çalışırlar. "Aranılan" ve "en çok aranan" sayıların listelerini oluştururlar; bunlar uzun süredir çarpanlara ayrılmaya karşı koyan sayılardır. Daha sonra, yavaş yavaş ve teker teker, onları listeden silerler. Şifre kırıcıların yaklaşımı daha militaristtir. Ulusal Güvenlik Örgütü ve Savunma Bakanlığı'nca desteklenirler, özel bir tercihleri yoktur, amaçları sadece, her sayıyı dize getirmektir. Yanıtlamaya çalıştıkları soru, çarpanlara ayırmanın "zor" bir problem olmasının gerekli olup olmadığıdır. Çarpanlara ayırma problemlerinin birçoğunu daha önce düşünüldüğünden daha kolay duruma getiren Lenstra'nın yöntemi, bu konuda 20. yüzyıl matematiğini gerçekten kullanan ilk girişimdir. Önceki yöntemler 18. yüzyıl kavramlarını (daha çok Gauss'un) kullanmışlardı. Lenstra'nın çalışmaları bir başlangıç, matematiğin "büyük topları"nın, yakın döneme kadar ihmal ettikleri bu uğraşa yönelmeleri-

nin başlangıcı olabilir mi? Çarpanlara ayırma konusundaki büyük atılım, belki de, henüz gerçekleşmemiştir. Birisi çıkıp “zor sayılar”ın kesin bir anlamda gerçekten zor olduğunu ispatlayana kadar bunu merak etmeyi sürdüreceğiz. Eğer bu problem Federal para ile çözülebiliyorsa o zaman onun çözüleceğini varsayabiliriz. Belki bundan 10 veya 20 yıl sonra insanlar artık çarpanlara ayırma konusundan söz etmeyecektir; çünkü artık kolayca yapılabilir olmuştur. O zaman, asimetrik kriptografi konusundan da söz edilmeyecektir; çünkü artık güvenilirliği kalmamıştır.

Sayıları çarpanlara ayıranların günümüzde mazhar oldukları ayrıcalık ve medya ilgisi karşısında, geriye bakıp bu problemle uğraşmanın hiçbir kazanç sağlamadığı dönemlerde büyük çaba harcayan akademisyen ve amatörler hak ettikleri krediyi vermek yerinde olur sanırım. En başından başlayalım. Son birkaç yıla gelene kadar, çarpanlarla uğraşma daha çok eksantrik olarak tanınan kişilerin oyun alanı sayılmış olsa da bununla ilgilenen matematikçiler ve amatörler her zaman olmuştur. En eski çarpan tabloları, asal sayılar konusundaki araştırmalarla ilgili olarak yapılmışlardı. 17. yüzyıl başlarında 24.000’e kadar olan sayılar için düzenlenmiş böyle bir tablo mevcuttu ve bu 1668’de 100.000’e kadar genişletilmişti. Bu tür sonuçların yayınlanmasının kolay olmamasına şaşkınmamak gerekir; çünkü toplumun genelinde böyle çalışmalara fazla ilgi (talep bir yana) yoktu. Bu bağlamda, belki de en talihsiz olanı, Viyanalı öğretmen Antonio Felkel’in tablosu olsa gerek. Büyük emeklerle hazırladığı tablosunu, o dönemin tanınmış bir Alman matematikçisinin yardımıyla Avusturya İmparatorluk Hazinesi’nin desteğini sağlamış ve 1776’da yayınlamayı başarmıştı. Tablo 400.000’e kadar olan bütün sayıların çarpanlara ayrışımını içeriyordu. Ancak kitaba o kadar az alıcı ilgi gösterdi ki, sonunda Hazine kitabın neredeyse hepsini piyasadan topladı ve kâğıdı Türkler’e karşı savaşta kullanılmak üzere kartuşlara dönüştürdü.

19. yüzyılda matematikçiler Z Dase denilen ve hızlı zihinsel hesap yapabilen insanları kullanarak, çarpanların tablosunu 10.000.000’a çıkardılar. Tarihe baktığımızda, arada bir,

bu gibi çok seri zihinsel hesap yapanlar ortaya çıkmıştır. Bunlar formal matematik konusunda fazla yetenekli değildirler. Hepsinin çok belirli ve olağanüstü tek bir yeteneği vardır; hızlı hesaplama. Bu zihinsel başarılarını herkes gibi kendilerinin de bilmediği yöntemlere borçludurlar. 19. yüzyılın çarpanlara ayırma uğraşının zirvesinde, Prag Üniversitesi profesörlerinden J. P. Kulik'in çalışmaları yer alır. Yirmi yıldan fazla bir süre hobi olarak yürütülen bir çalışmanın yayınlanmamış olan sonucu 100.000.000'a kadar olan bütün sayıları kapsıyordu. Ne yazık ki (belki de şaşırmamak gerekir) birkaç taneden öte hata içerdiği de artık anlaşılmıştır.

Bildiğim kadarıyla şimdiye kadar, buna yaklaşan büyüklükte bir tablo yayınlanmış değildir. Ayrıca ilgimiz 20, 30, 40 veya daha fazla basamaklı sayılara uzandıkça böyle bir tablonun, ilke olarak bile, pek akla yakın olmadığı açıkça görülebilir. İlgi, belirli bir limite kadar olan bütün sayıların çarpanlarını sıralamaktan çok herhangi belirli büyük bir sayının çarpanlarını bulma problemine yönelmiştir. Okuyucunun da artık kavramış olacağı gibi, bu işi başarmak için bilinen etkili basit hiçbir yol yoktur. Bazı belirli tür sayıları çarpanlara ayırmak için yüzyıllar boyu, birçok yöntem geliştirilmiştir, ancak bunların hiçbirisi genel değildir. Konu olan sayı farklı yöntemlerle ve umutlarla test edilir veya günümüzde, kuşkusuz makinelerden yardım istenir.

Bu tür makinelerin ilki Kaliforniya Üniversitesi'nde, Dr. D. H. Lehmen ve babası tarafından yapılmış ve etkileyici bir başarıyla karşılaşmıştı. Bu cihaz 1930'lu yılların başlarında (transistörlerin keşfi elektronik bilgisayar çağına öncülük etmeden çok önce) yapılmıştı ve tümüyle mekanikti. Makinenin içinde her birinde 100 diş bulunan ve birbirinin aynı olan bir dizi çark, hareket edemeyecek biçimde ortak bir dönen şafta monte edilmişti. Bu çarklar, çaplarının bir ucundan her birinde farklı bir asal sayı kadar diş bulunan başka dişlilere geçirilmişlerdi. Asal sayı dişlilerinin her birinde her diş için bir delik vardı ve bu deliklerin hepsi bir doğru boyunca sıralandıkları anda, ancak o anda, onlardan geçen bir ışık demetinin ışıkları görünüyordu. Bu cihazın çalışmasının gerisinde

yatan teori burada ayrıntılarıyla verilemese bile, temel kur-gu öyle düzenlenmişti ki, delikler aynı anda bir doğru boyun-ca sıralandıklarında (bu onlardan geçen ışık demetinin bir foto-dedektör üzerine düşmesiyle fark ediliyordu) bir çarpan-lara ayırmanın başarıldığı saptanmış oluyordu.

Sayıların bilinmeyen dünyasına adım atıp çarpan avına çıkmanın büyük heyecanını mucitlerin kendi kalemlelerinden, *Scripta Mathematica* 1'de (1933) "Hunting Big Game in the Theory of Number" (Sayılar Teorisinde Büyük Safari) adıyla yayınlanan bir makaleden nakledelim: "Laboratuvardaki masanın etrafına toplanmış, kahvelerini yudumlayan bir grup profesör ve eşlerinin bu acaip makinenin gizemli ve akıl almaz gücünü tartışırken yaşadıkları heyecanı görseniz çok şaşırdınız." diyordu baba Dr. Lehmer. "Onu çarpan tabloları gibi şeylerle halledilebilecek küçük sayılar için ça-lıştırmanın sportmenliğe yakışmayacağı, onun normal teles-kopların uzanımı dışında, bizim galaksimizin ötelerinde pu-suya yatmış bekleyen sayılar için kullanılması konusunda anlaşılmaya vardık."

"Uzaktaki sayılar galaksi"sinden makineye verilen ilk gö-rev, $2^{93}+1$ sayısının çarpanı olan yenilmez kahraman 1.537.228.672.093.301.419'un çarpanlarını bulmaktı. Bu sa-yının bileşik olduğu biliniyordu (Bölüm 7'de verilen türden yöntemlerle); ancak tabloların kapsamında olan hiçbir kü-çük çarpanı yoktu. Yaklaşık üç saniye sonra, Dr. Lehmer'in anlatımıyla, makinenin dönen tekerleklerinin yanındaki "göz", işareti verdi ve makine durdu. Araştırıldığında bu 19 basamaklı sayının 529.510.939 ve 2.903.110.321 gibi asal çarpana ayrıştırıldığı anlaşıldı. Nefes kesici bir andı; yıllar-ca çözüme karşı direnmiş bir problem üç saniyede halledil-miştir. Bilinmeyene yönelik bu serüvenin ilk çarpıcı günle-rinde heyecan gerçekten doruktaydı. Tırmanılmamış birçok sayısal yamaç incelenmiş ve sonunda birçok zirve fethedil-miştir. On veya yirmi yıl sonra, çarpanlara ayırma problemlerinin üstüne elektronik işlemlerin gerçek gücüyle gidildi-ğinde bu çabaların, görece, ne kadar zayıf kalacağı kimse-nin aklına gelmiyordu.

Büyük sayıları bilgisayarlarla çarpanlara ayırma dönemi 1971'de, 40 basamaklı bir sayının dize getirilmesiyle, başladı. Bir amatör için herhangi bir büyük sayıya "ünlü" denilmesi yadırganabilir ancak matematikçiler hangi sayıların ayrıştırılmasının zor olduğunu bilirler ve her an size "en çok aranan" numaraların kısa bir listesini verebilirler. Bunlar sadece görünür hiçbir küçük çarpanı olmayan sayılar değildirler. Çoğu kez mühendisler ve matematikçilerin önlerine çıkan cebirsel problemlerde çarpanları önemli olan sayılardır. Tam bu sıralarda Amerikan Matematik Topluluğu (Mathematical Society) matematikçilerin büyük sayıların çarpanlarını araştırma çabasını desteklemeye karar verdi. Amaç, a bir küçük tamsayı, n de büyük bir tamsayı olmak üzere, $a^n + 1$ ve $a^n - 1$ şeklindeki sayılarını bütün çarpanlarının bir listesini çıkarmaktı. Bu sayıların sayılar teoresinde her zaman özel bir önemi olmuştur ayrıca da mühendisler tarafından rasgele sayılar üretmek için kullanılmışlardır. Amerikan Matematik Topluluğu tablosuna yüzyılın dönemecinde bu tür sayıların kısmi bir tablosunu oluşturan İngiliz albayın anısına, Cunningham Projesi Tablosu, denilecekti. "Cunningham sayıları" için böylece başlayan ortak girişim 1970'lerde giderek güçlendi ve yöntemler daha da geliştirildi. Amaçlanan 50 basamağa ulaşan sayılar yanında, Lehmer'in bisiklet dişlileri ve zincirlerinden oluşan mekanizmasına boyun eğen 20 basamaklı sayılar cüce kalıyorlardı.

Günümüzdeki bilgisayarlar son derece hızlı oldukları halde, gördüğümüz gibi, yine de büyük sayıların çarpanlarını doğrudan bulmayı başaramıyorlar. Özel trikler bulunması gerekir; matematikçilerin yaptığı, büyük bir sayının çarpanlara ayrılmasını ele alıp, bunu, daha küçük binlerce sayının çarpanlara ayrılmasına indirgemektir. Bu küçük sayıların hepsinin ayrıştırılmasına gerek yoktur; örneğin bazı belirli asal sayıların, onları tam olarak bölüp bölmediğini bilmek yeterli olabilir. Ancak bu daha küçük sayıların her biri, ilk sayının çarpanları konusunda biraz bilgi verebilir ve bunlar bir araya getirilerek nihai amaç gerçekleştirilebilir.

Bilgisayar işlemlerini giderek daha incelikli duruma getiren çarpan avcıları, 1982'de, o dönemde kullanılabilecek en hızlı bilgisayarı (Cray I) kullanarak yöntemin etkin sınırı olduğunu düşündükleri noktaya varmışlardı. Bu sınır, yaklaşık 50 basamaklı zor sayıları kapsıyordu. Ancak ne yazık ki "en çok aranan" sayıların 1982 listesinde birkaç tane de 60 veya daha fazla basamaklı sayı vardı ve tahminler ise, en iyisinden "ihtiyatlı" şeklindeydi.

1970'ten başlayarak her sonbaharda çarpanlara ayırma problemiyle ilgilenen bir grup matematikçi Kanada'nın Winnipeg kentinde toplanıp ilerlemeleri gözden geçirirdi. Bu nedenle, 1982 toplantısının, o dönemdeki bilgisayarlar bakımından konunun kapanmasıyla sonuçlanacağı beklenir gibiydi. Durumu özetleyen bir makalenin basına verilmesine karar verildi, Dr. D. H. Lehmer'in (orjinal mekanik çarpanlara ayırma makinesinin mucidi) yazarlardan biri olacak ölçüde işin içinde olması çok ilginçti. Winnipeg'deki toplantıya katılanlardan birinin söylediği gibi "Eğer 60 basamaklı zor sayıların gelecek yıl içinde çarpanlara ayrılacağına bahse girseydiniz orada bulunan herkesten para toplayabilirdiniz."

Durumun birdenbire değişmesine yol açan daha hızlı bilgisayarlar değil, bilgisayar donanımının sayısal işlevlerini tam olarak nasıl yaptığının ayrıntılarını araştırmaya yoğunlaşmasıydı. Bu atılım, Winnipeg'deki toplantıda bira içilirken gerçekleşti. Konuşmalarla geçen bir günün sonunda çarpımlarla uğraşan grup, genelde, bilgisayarların özellikle de hızlı Cray bilgisayarların zaman sınırlamalarıyla ilgili temel sorunlar konusunda sohbet ederken bir Cray araştırma mühendisi onlara katıldı. Beyinlerin tesadüfi karşılaşması kısa sürede herkesin heyecanla, hep birlikte konuşmasına yol açtı, çünkü çarpanlara ayırıştırma için gerekli olan belirli tekrarlama işlemleri Cray'in yapısına çok uygundu. Binlerce çok uzun sayının, on binlerce kere değiştirilmesi gerekiyordu, ancak değişiklikler, her seferinde az sayıda ve belirli konumlarda yapıyordu. Cray'in yapısı, bu değişikliklerin, sayıların uzunluklarına değil, yapılan değişiklik sayısına orantılı bir sürede yapmasına olanak sağlıyordu.

Bu haber çarpan meraklarını tekrar Cray'lerinin başına koşturdu mühendisin söyledikleri gerçekten de doğrudur. Bunun yararları çabucak kendini gösterdi. 52, 53 ve 54 basamaklı sayılar birkaç saatte çarpanlara ayrıştırıldı. Bu sayılar daha önceki çabaları boşa çıkarmıştı ve bazıları 100 saatten fazla bilgisayar zamanı kullanmıştı. Bu yeni başarılarından yüreklenerek "en çok aranan"lar listesinin en tepesindeki 58 basamaklı bir sayıya el attılar. Bu sayı, bu bölümün en başında sözü edilen $2^{193} - 1$ sayısıydı. Yaklaşık sekiz saat sonra, sayı yenik düştü, çarpanları bulunmuştu. Sayı uzunluğu her üç basamak arttığında, bu yöntemle çarpan bulma süresi de iki katına çıktığı için, yine bir zaman engeline yaklaşıyorlardı: 60 basamak uygulama sınırına yakın olabilirdi. Ancak teknik bakımından yeni gelişmeler sağlandı ve bunları kullanarak 58 basamaklı gözde $2^{193} - 1$ sayısı iki saatten az bir sürede tekrar ayrıştırıldı (hızda beş katlık bir gelişme). Bundan kısa bir süre sonra da 60 basamaklı bir sayı teslim oldu ve sonra bir başka "en çok aranan" sayı, 63 basamaklı bir sayı, beş saatten biraz uzun bir sürede diz çöktü.

1983'den bu yana teknik gelişmeler aynı hızla sürmektedir. Hem çarpanlara ayırmada kullanılacak algoritmalar, hem de bu algoritmaları en verimli biçimde gerçekleştirecek bilgisayarlar arasında rekabet vardır. Bunlar arasında önemli olan çok yeni bir bilgisayar bulunmaktadır. Bu bir NASA bilgisayarıdır (daha çok uydu verilerini incelemek için kullanılması öngörülmüştür) ve hem yapısı hem de kullandığı lisan türleri bakımından çarpanlara ayırma işi için çok uygundur. Bu sıralarda çarpanlara ayırma için programlanmaktadır ve en zor 70 basamaklı sayıları bile, rutin olarak bir saatten kısa sürede halletmesi beklenmektedir. Çok zor olanlar dışındaki bütün sayılar Lenstra'nın tekniği ile artık çok daha sürede teslim oluyorlar.

Kendi bilgisayarlarını yapmakta olan bir grup araştırmacı belki de bu konudaki nihai çabayı gerçekleştirmektedir. Bu bilgisayar, bulabilecekleri en verimli yolla çarpanlara ayırma işini yapacak ve yalnızca bunu yapacaktır. Bu Purdue Üniversitesi ile Georgia Üniversitesi'nin işbirliği ile ya-

pılan bir girişimdir. Resmi yayınlardaki adı “hassasiyeti artırılmış operand bilgisayar” anlamına gelen “extended precision operand computer”in baş harflerinden oluşan EPOC olacaktır ancak popüler adı Georgia Balyozu’dur. 80 basamak uzunluğuna kadar olan sayıların çoğunun EPOC’un uzamı içinde olması ve bir günden az bir süre gerektirmesi beklenmektedir.

Ancak benim bunları yazdığım şu sırada (1989) çarpanlara ayırmanın zirvesi, tek bir “süper bilgisayar”la değil, birçoğunun ortak çabasıyla başarılmıştır. En son eğilim, çok sayıda farklı bilgisayarın hesaplamalarını bir araya getirme yönündedir, bunların her biri tek bir çarpanlara ayırma probleminin ayrı yönleri üzerinde (genellikle yoğun olmayan gece saatlerinde) çalışıyorlar. Daha sonra yaptıklarını birleştirmek için bunları elektronik posta yoluyla bir işlem merkezine bildiriyorlar. Bu yaklaşımın en başarılı sonucu, birkaç farklı ülkede yüzlerce bilgisayarı bir aya yakın bir süre kullanarak yakın dönemde, 100 basamak engelini ilk defa aşılmasıdır. Ayrıntıları verirsek, “zor” sayı olan $11^{104} + 1$ ’in “kolay” çarpanı $11^8 + 1$ ’den sonra kalan bölümüydü. Onun iki asal çarpana (60 basamaklı ve 41 basamaklı) ayrıldığı haberi 10 Ekim 1988’de sabahın saat 2’sinde ilan edildi; Kaliforniya saatiyle (artık önemli sayıların çarpımlara ayırma süreleri dakikalarla ölçülüyor, tıpkı bir çocuğun doğum haberini verirken yapıldığı gibi). Bu başarı her ne kadar, pek sıradan değilse de, 100 basamaktan küçük olan her sayının tehlikede olduğuna da işarettir. Nitekim 1988’de sadece PC’leri kullanarak 95 basamaklı bir çarpanlara ayırma gerçekleşti. Gerçi bu iş için, üç ayı aşkın bir süre tam bir bilgisayar ordusu kullanıldı!

Bütün bunlardan sonra, ulusal güvenliğin konumu nedir? Hükümet için geliştirilen ilk asimetrik şifre (ona, geliştirenlerin isimlerinin son harfleri kullanılarak RSA denilmişti), hiç kimsenin 80 basamaklı bir sayıyı çarpanlara ayırmayı başarmıyacağı varsayımını temel almıştı. 1970’lerin sonuna doğru şifreyi geliştirme çalışmaları sürerken bu sayının çok güvenli olduğu düşünülüyordu. Ancak artık bu şifrenin güvenilirliği sorgulanmaya başlamıştır. Daha büyük sayılar

kullanarak yeni şifrelerin yapılması gündeme gelmiştir (belki de 200 basamaklı sayılarla, bu gerçekten daha güvenilir olur) hiç olmazsa bir süre için.

Acaba çarpanlara ayrılacak sayı için mutlaka bir sınır olması gerekir mi? Öyle bile olsa öngörebileceğimiz bir gelecek için ne denilebilir? Günümüz teknikleri bakımından sınırlayıcı olan, daha çok, maliyettir. Günümüzde (1989), 140 basamaklı bir sayının, örneğin bir yılda, çarpanlara ayrılmasını “satın alma”nın bedelinin 10 milyar dolar olacağı hesaplanmıştır. 200 basamaklı sayı ne durumdadır? Tahmini hesaplara göre bunun bedeli 100 milyar dolara yaklaşmaktadır; sahiden de astronomik bir fiyat, ama gerçekte bu, ABD’nin yıllık iç borç faizine ödenen paranın yarısı kadardır.

Büyük sayıların çarpanlara ayrılammaması konusu gizli şifre sistemlerinden başka şeyleri de ilgilendirmektedir. Bilgisayar yoluyla yapılan her türlü iş görüşmelerinde dürüstlüğü güvence altına almak için de yöntemler geliştirilmiştir. Problemin ifadesi kolaydır. Bilgisayar terminalleri önünde oturan iki insandan birinin ötekini aldatmasını nasıl önleyebilirsiniz? Örneğin, işle ilgili önemli bir bilgi alışverişi yapacağınızı düşünelim. Bilgiyi önce kim verecektir ve diğerini bilgiyi aldıktan sonra anlaşılmayı bozmaktan, nasıl alıkoyabilirsiniz? Kısacası, iki insanın, güvenilen bir üçüncü kişinin yardımı olmadan gizli bilgiler alıp vermesi olanaklı mıdır? Ayrıca da, bu üçüncü şahsa ne kadar güvenilebilir? Burada yardıma koşan çarpanlara ayırmadır.

Dürüstlikle ilgili olabilecek en basit durumlardan birini ele alalım. Bilgisayarımın terminali önünde oturuyorum, siz de sizinkinin önünde. Gelecek hafta yapılacak bir futbol maçı üzerine bahse gireceğiz; ancak ikimiz de aynı takıma şans veriyoruz. Öyleyse kimin hangi takımı alacağı konusunda yazı tura atalım. Ama parayı kim atacak ve öbür insan paranın hangi yanının geldiğinden nasıl emin olacak? Aldatmayacağımıza inanılabilir mi? Bu sorun, 1981’de Kaliforniya Üniversitesi’nden Manuel Blum ve Harvard Üniversitesi’nden Michael Rabin’in icat ettikleri aşağıda anlatacağımız ilginç yöntemle çözülmüştür.

Asimetrik şifrelemede olduğu gibi; iki büyük asal sayı alıyorum ve bunları çarparak daha da büyük bir sayı elde ediyorum (örneğin 150 basamaklı); uzunluğu nedeniyle bu sayıyı çarpanlara ayırma olanağı yoktur. Bu N sayısını size iletıyorum ve çarpanlara ayırmanızı istiyorum. Doğal olarak, bunu yapamıyorsunuz; ancak verilen sayının asal olmadığını ve bu nedenle de gerçekten çarpanları olduğunu doğrulayabiliyorsunuz, yani sizin bunu yapmanızı sağlayan bilgisayar yöntemleri var. $N/2$ 'den küçük olan herhangi bir sayı seçiyorsunuz ve onu deniyorsunuz. Büyük olasılıkla bir çarpan olmayacaktır. Şimdi bu rasgele seçtiğiniz M sayısının karesini alıyorsunuz ve bu M^2 'yi N gruplarına göre sayarak (bölüm 7'de verilen saat aritmetiğini kullanarak) kalan R sayısını buluyorsunuz. Bana sadece ve sadece R sayısını gönderiyorsunuz. İlk çarpanları kullanarak (ben bunları biliyorum ama siz bilmiyorsunuz) $N/2$ 'den küçük olan ve bu R kalanını verecek bütün sayıları elde edebileceğim bir yöntem var. Genellikle, bu tür sadece iki sayı vardır. Bu nedenle de elimde iki sayı bulunuyor ve bunlardan birisi sizin M sayınızdır, ancak hangisi olduğunu bilmiyorum. Bunlardan birisini seçip size gönderiyorum. Bu benim yazı-tura atma eşdeğeridir. Bunu yaparken, sizin seçmiş olduğunuz M sayısını size gönderme şansım % 50'dir. Eğer bunu başarmışsam size yeni bir bilgi vermiş değilim ve hâlâ benim N sayımı çarpanlara ayıramazsınız. Bu nedenle de, siz kaybetmiş oldunuz. Ancak eğer ben size öbür sayıyı göndermişsem, artık sizin elinizde aynı kalanla ilgili iki sayı var demektir. Bu bilgiyle benim ilk sayımı çarpanlara ayırmanızı sağlayan basit bir yöntem mevcuttur ve siz kazanıyorsunuz.

Bu süreç hakkında dikkatle düşünürseniz, her iki "oyuncu"nun da kazanma şansı % 50'dir ve aldatma olanağı yoktur. Eğer size önemsiz olmayan (yani asal) çarpanları olmayan bir sayı vermişsem; bunu kontrol edebilirsiniz. Aynı şekilde eğer gönderdiğiniz R sayısını kalan olarak vermeyen bir sayı gönderirsem yine benim hile yapma çabamı fark edebilirsiniz. Bu yöntemin dayandığı "bilinmeyen transfer" denilen temel süreç, telefon ve bilgisayar yoluyla yapılan

karşılıklı her tür işte iki tarafın da çıkarlarını korur. Bilinmeyen transfer kavramı genişletilerek, bir bilgisayardan bir diğerine, aracıya gerek kalmadan her türlü onaylanmış belgenin, örneğin kontratların, doğrudan gönderilmesine olanak sağlayabilir. Gönderen mesajın içeriğini doğrulayan alındıyı otomatik olarak alır. Temel süreç, mesajı birkaç sayıdan oluşan bir rakamlar dizisiyle şifreleyip, çarpanlara ayrılmak üzere göndermeye dayanmaktadır. Bu sayıların her birisi için “yazı-tura atma” işlemlerini uyguladıktan sonra bu sayılar sonunda (bazıları için belki birkaç “atma” sonra) alıcı mesajı deşifre eder. Mesajı gönderenin alındısı ise “para atma”nın bilgisayar kaydıdır. Bir anlaşmazlık çıkarsa hakim bu kayıtlardan alıcıya mesajı deşifre etmek için yeterince bilgi verilmiş olduğunu ve bu nedenle de mesajın alınmış olduğunu saptayabilir. Bu süreç biraz daha süslenerek, aynı anda farklı yerlerde kontrat imzalamayı da kapsayabilir. Beklenmeyen şey olur ve ne kadar uzun ve “zor” da olsa, her sayıyı çarpanlara ayırabilen basit bir yöntem keşfedilmezse, bu fikirlerin, çok yeni olmakla beraber gelecek yıllar içinde iş anlaşmalarının önemli bir özelliği olmaları beklenmektedir. Bu, belki de insanlığın, matematiğin başarısından çok başarısızlığından yararlandığı tek durumdur.

X. Bölüm

Dört Renk Yeterli midir?

Boyama kitaplarını boyamak kadar, çocukluğumuzla ilgili anıları çağrıştıran çok az şey vardır. Büyükler boyama kitapları boyamazlar. Bu noktaya dikkat çeken politik bir de fıkra vardır. Rakibinin saflığını ve gelişmemişliğini vurgulamak isteyen bir aday, kısa süre önce, rakibinin evinin ve kütüphanesinin bir yangın sonucu yok olduğunu, “ne yazık ki, yangında kütüphanedeki her iki kitabın da yandığı ve bunlardan birinin henüz boyanmamış bile olduğu”nu söylediğini dile getiriyordu. Anlaşılan, boyamanın ilkel düzeyinin, genel olarak, fazla yetenek gerektirmediği kanısı yaygındır.

Bir boyama kitabındaki bir resmi boyamak için temel ilke, ortak sınır çizgisi olan bölgelerde (bitişik diyeceğiz) farklı renklerin kullanılmasının gerektiğidir. Tek bir kısıtlama olunca da kutudaki bütün renkler, farklı incelik ve estetik beğenilere göre kullanılarak canlı renkli resimler yaratılabilir. Bu kadar zevkli bir uğraştan yalnızca bir matematikçi bir problem çıkarabilir. Bir süre sonra bu işe yaklaşımı artistik olmaktan çok matematiksel olan bir kişinin aklına bir soru gelir; düşünülebilecek herhangi bir resmi tamamen boyamak için en az kaç renk gerekir?

Üç rengin yeterli olmayacağını anlamak için ufak bir deneme yeterlidir. Diğer yandan, beş renk gerektiren bir resim bulmak da oldukça zor görünür. Bu nedenle yanıt, büyük olasılıkla dördttür. Doğru yanıt ne olursa olsun, bunun dünyanın en ağırlıklı matematiksel konularından birisi olmadığına katılacağınızdan eminim. Ancak ilk izlenimler çok yanıltıcı olabilirler. Bu, dünyanın en iyi matematik beyinlerini yüz yılı aşkın bir süredir yenilgiye uğratan “dört renk prob-

lemi”dir. Günümüzde bile bu problem “eski ekol” matematikçileri için bir huzursuzluk kaynağıdır, çünkü sonunda, 1976 yılında bulunan ispat çok fazla bilgisayar hesaplaması gerektirmişti. Doğruluğu yalnızca, güçlü bilgisayar elektronikliğini kullanma olanağına sahip olan uzmanlarca kanıtlanabilmektedir. Bu ne biçim matematiksel ispattır? Ve insanlar bilgisayara neden inansınlar?

Böyle bir çatışma çıkmasının nedeni, bir bilgisayarın ilk defa önemli bir matematiksel ispat için temel bir katkıda bulunmuş olmasıdır. Kuşkusuz çok daha kısa ve basit bir ispatın “oralarda bir yerlerde”, yeni bir kuşağın doğurgan matematiksel beyinlerince hâlâ keşfedilmeyi beklediği ümit edilebilir. Ancak daha kolay bir ispatın var olmaması da aynı ölçüde olasıdır.

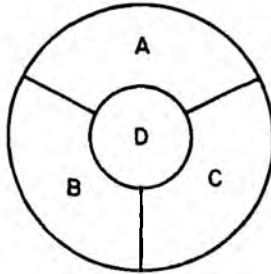
Eğer böyleyse, dört renk problemi (ünlü olma yolundaki başka iddialar yanında) yeni tür bir matematiksel ispatın doğmasına da yol açmıştır; temelinde var olan karmaşıklık nedeniyle, bilgisayar kullanımı *gerektiren* ispatlar. Bütün bunlar bir “masumiyetin yitimi”ni hissedenler için ürkütücü olsa da geleceğin gidişatı bu yönde olabilir.

Nihai çözümün bir kuvvet gösterim yönü olmasına karşın kökeni çok daha alçak gönüllüdür. Kısa süre önce Londra’da bir öğrenci olan Francis Guthrie kardeşi Frederick’e yazdığı bir mektupta bir haritayı, bitişik ülkelerin renkleri farklı olacak şekilde boyamak için sadece dört rengin, her zaman yeterli olacağından söz ettiğinde yıl 1852’ydi. Bitişik ülkelerle, kastettiği sonlu uzunlukta ortak sınırları olan ülkelerdi; bir noktada değen sınırlar bunun dışında kalıyordu.

Böylece, örneğin, bir satranç tahtası, dört karenin birbirine değdiği birçok nokta olmasına karşın, iki renkle boyanabilir. Ayrıca, ülke sözcüğü ile bir sınırla çevrilmiş tek bir alanı kastediyordu, yani, bölümün başında değindiğimiz boyama kitabı ile aynı kuralları kullanıyordu.

Francis’in erkek kardeşi hâlâ Londra’daki Universty College’da öğrenciydi ve dönemin ünlü matematikçilerinden biri olan bir Profesör De Morgan’ın derslerine giriyordu. Kendisi dört renk iddiasının doğru olup olmadığını saptayacak bir

yöntem bulamadığı için konuyu bu işlerin uzmanı olan hocasına iletti. Dört rengin gerektiği, açıkça görülebilirdi; çünkü birbirine bitişik dört alanı (veya ülkesi) olan bir resim çizmek kolaydı. Bunun bir örneği Şekil 9'da görülmektedir, renkler A, B, C, D olarak gösterilmiştir. Ancak daha sonra ne yapılabilirdi?

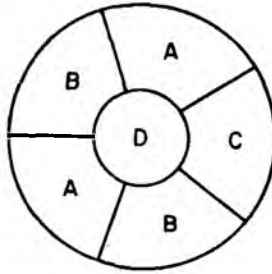


Şekil 9.

Profesör de Morgan bu problemi ele aldı ve her biri diğer dördüyle komşu (yani bitişik) olan beş ülke olasılığını araştırmaya girişti. Eğer böyle bir şekil çizilebilirse o zaman en az beş rengin gerektiği hemen görülebilirdi. Ancak sonunda De Morgan bu şekilde bağlantılı olan bir örnek bulamadıktan başka, bu tür bir beşli bölgenin var olmasının mümkün olmadığını ispatlamayı da başardı. Bu oldukça büyük bir başarıydı ve önceleri problemin çözüldüğünü de sandı. Ancak ne yazık ki problem çözülmemişti. Bunun nedenini anlamak için Şekil 9'a, üçü birbiriyle temas eden dört bölgeye tekrar bakalım.

Şekil 9'daki gibi hiçbir bölge içermeyen bir harita çizdiğimizizi düşünelim. Böyle bir harita, sadece üç renkle boyanabilir mi? Yanıtın "belki de hayır" olduğunu göstermek çok kolaydır. Neden hayır? Şekil 10'da çizilmiş haritayı ele alalım. Altı ülke var ama, her birinin diğer üçüne bitişik olduğu dörtlü bir ülke grubu bulunmuyor. Ancak yine de harita için dört renk gerekiyor; üçü dış halkadaki ülkeler için birisi de ortada olan ülke için. Öyleyse dört renk gerektiren haritaların ille de, her biri diğer üçüyle bitişik olan dörtlü bir grup

içermesi gerekmiyordu. Aynı şekilde, beş renk gerektiren haritaların da Profesör De Morgan'ın olanaksız olduğunu ispatladığı durumu içermesi gerekemeyebilirdi; yani dördü birbirine bitişik olan beşli bir ülke grubu. Bu durumda, bazı haritalar için beş renkten fazlasının gerekli olabileceği ihtimali vardı. Kapı hâlâ aralıktı, ancak bu konuyla ilk uğraşanlardan hiçbirinin kapının kendi yaşamları süresince ve sonradan gelen birkaç nesil boyunca da böyle kalacağına ihtimal vermedikleri kuşkusuz.



Şekil 10.

Öykü şimdi yirmi yıl veya daha sonrasına, 1878'e uzanır. Ünlü İngiliz matematikçisi Arthur Cayley dört renk probleminin doğru veya yanlış olduğunu kendi başına saptayamayınca onu Londra Matematik Topluluğu'na sunmaya karar verdi. Bundan kısa bir süre sonra Topluluğun Arthur Kempe adındaki üyesi (mesleği avukatlıktı) dört rengin yeterli olduğu savını ispatladığını iddia eden bir makale yayınladı.

Bu ispatın ayrıntıları burada verilmese de içerdiği temel aşamalar kolayca açıklanabilir. İlk olarak, "normal" bir harita kavramı tanımlanıyordu. Eğer bir haritada, bir noktada üçten fazla ülke bir arada değilse ve hiçbir ülke bir başkasını *tümüyle* çevrelemiyorsa ona "normal" diyoruz. Bu tanımla (ülkeler yerine devletleri konu edersek) anakaradaki ABD haritası normal sayılamaz; çünkü Utah, Colorado, Arizona ve New Mexico eyaletlerinin hepsi bir noktada birleşiyor. Güney Afrika tarafından tümüyle çevrilmiş olan Lesotho'da normal olmayan ikinci duruma bir örnektir. Gerçek harita-

ların dünyasında bunların ender görülür olmaları kolaylık sağlar. Çünkü normal olmayan herhangi bir harita, en azından, aynı sayıda renk gerektiren, yakından ilişkili normal bir haritaya dönüştürülebilir ve bu nedenle de dikkate alınmaları gerekmez. Örneğin, eğer beş renk gerektiren bir harita varsa, o zaman beş renk gerektiren normal bir harita da var demektir. Böylece, sadece normal haritaları dikkate almak yeterli olur.

Bu basitleştirmeden sonra Kempe, her normal haritanın beş veya daha az komşusu olan, en az bir ülke içermesinin gerektiğini ispatlamaya girişti. Daha sonra da, eğer beş renk gerektiren bir haritada altıdan daha az komşusu olan bir ülke varsa (olması gerektiğini zaten göstermişti), ondan, ülke sayısı daha az olan, beş renkli bir başka harita çizilebileceğini gösterdi. Kullandığı yöntem, iyi bilinen klasik *Reductio ad absurdum* yani durumu abese indirgeme yöntemi idi. Örneğin, daha az ülke içeren beş renkli yeni haritayı alıp süreci tekrarlayarak daha az sayıda ülke içeren bir harita elde ederiz ve bu böylece sonsuza kadar gider. Ancak, eğer sonsuz olmayan sayıda ülke ile başlamışsak, sonunda o kadar az ülke kalmıştır ki, beş renk gerektirmesi olanaksızdır. Bu nedenle argüman bir saçmalığa yol açmıştır, bu da, bizi ilk varsayımın, yani beş renk gerektiren bir haritanın var olduğunun yanlış olduğu sonucuna götürmektedir.

Problem çözülmüş gibi görünüyordu ve “ispat”, on bir yılı aşkın bir süre, 1890 yılına kadar doğru olarak kabul edilmişti. O zaman korkunç bir şey keşfedildi; bir hata, hem de düzeltilmesi kolay olmayan bir hata keşfedildi. Yanlış olan neydi? Kempe’nin ispatı iki bölümden oluşuyordu; birinci bölümde, yani, her normal haritanın beş veya daha az komşusu olan en az bir ülke içermesi gerektiği savının ispatında hata yoktu. Bu nedenle sorun “indirgeme” bölümüyle ilgiliydi. İki veya üç komşusu olan ülkeler için indirgeme yöntemi önemsizdir (tek komşu durumu da önemsizdi ve normal olmayan haritalarla ele alınmıştı), onu doğrudan izleyebiliriz.

Eğer beş renk gerektiren bir harita varsa, o zaman en az ülke ile buna sahip olabilen bir haritanın da var olması ge-

reker. Bu en “küçük” beş renkli haritada, sadece iki komşusu olan bir ülke ele alalım ve bütün dikkatimizi bu üç ülkeli gruba yöneltelim. Komşulardan birisi ile sınırı kaldırarak bu iki ülkeyi “birleştirdiğimizi” varsayalım. Bu yeni haritada, beş renkli en küçük haritadan bir ülke eksilmiştir ve bu nedenle, tanım gereği, artık dört renkle boyanabilir. Onu bu şekilde boyayalım, sonra da sınırı çizelim. Yeniden oluşturulan ülke sadece, başka iki ülkeyle bitişiktir ve bunların renklerinin var olan A, B, C, D arasında A ve B renkleri olduğunu düşünelim. O zaman onu C veya D ile boyayabiliriz. Bu demektir ki ilk harita yalnızca dört renkle boyanabilmektedir. Bu sonuç, ilk beş renk varsayımı ile çelişmektedir. Öyleyse, en küçük beş renk haritalarından hiçbirisi sadece iki komşusu olan bir harita içeremez.

Üç komşusu olan bir ülke için de aynı basit irdeleme yapılabilir çünkü o zaman da, boyama için A, B, C, D renklerinden birisi kalmış olacaktır. Dört komşusu olan bir ülke için problem biraz daha zordur ve bitişik komşular dışında olanları da hesaba katmayı gerektirir. Bu durumda, özellikle bitişik dört komşunun dört *ayrı* renge gerek kalmadan boyanabileceğini ve dördüncü rengin her zaman, söz konusu olan dördüncü ülkeyi boyamak için kalabileceğini göstermek gerekir. Kempe bu durum için de çok basit ve şık, aynı zamanda da doğru olan bir ispat bulmayı başarmıştı. Ancak, Kempe’nin çalışmalarındaki hata, en son ve en karışık bölümde, beş komşusu olan bir ülkeyle ilgili irdelemelerdeydi. Bu durumda, hiç kimse, belirli hiçbir örnek bulamamış da olsa, beş renkli bir haritanın var olma ihtimali hâlâ mevcuttu.

1890 yılının sonunda durum şöyleydi: Genel bir harita (veya boya kitabı için) en az dört renk gerektiği kesindi. Eğer beş renk gerektiren bir harita varsa o zaman bu tür *en küçük* haritanın beş komşusu olan en az bir ülke içermesi ve daha az komşusu olan hiçbir ülke içermemesi gerekiyordu. Bu nedenle, “dört renk” ispatındaki nihai aşama bu beş komşulu ülkeye odaklanmalıydı. Böyle bir ülke ve onun yöresel çevresi her zaman “küçültülebilir” miydi, yani, varsayılan en küçük beş renkli haritadaki bir sınır (yani, bir ülke)

onu boyamak için gerekli renk sayısı azalmayacak şekilde kaldırılabilir miydi? Eğer kaldırılabilirse o zaman beş renkli en küçük harita var olamaz ve dört renk gerçekten yeterli olurdu! Bu bakımdan, son ayrıntılarda hatalı olsa bile, Kempe'nin çalışmaları yolu belirliyordu.

Beş komşu durumuna yaklaşım yöntemi iki bölümden oluşur. İlk önce, bu beş komşulu yapının genel çevresinde var olabilecek ülkelerin olası yöresel konumlarının şekilleri incelenir. Bundan, "kaçınılamaz şekillerin tam listesi" çıkarılır. Bu, en az bir tanesi haritada görünmesi kaçınılmaz olan ülkelerin yöresel düzenlenme şekillerinin tümünü içeren bir listedir. İkinci bölümde ise, bu listedeki her düzenleme şeklinin, öğrenmiş olduğumuz anlamda, yani boyamak için gereken renk sayısını azaltmadan bir ülkeyi yok etme anlamında, küçültülebileceğini göstermektir. Burada karşımıza birbirinden bağımsız olan şekil olasılıkları ortaya çıkmaktadır; bunlardan bazılarının çok az sayıda üyesi vardır, diğer bazılarının ise binlerce üyesi. Kempe, görece az sayıda üyesi olan bir şekil seçti ve bunların her birinin küçültülebileceğini ileri sürdü. Ancak ne yazık ki bunlardan birisi Kempe'nin iddia ettiği gibi küçültülebilir değildi; gerçekte indirgenmesi de olanaksızdı. İspat, bunun dışında, etkileyici, mantıksal bir zincir oluşturduğu halde bu zayıf halka nedeniyle tümüyle çökmüştü.

Kempe'nin ispatı onurlu bir başarısızlıkla sonuçlanmışsa da, onun probleme yaklaşımı, elimizde olan yöntemler arasında en ümit verici olanıydı; sonraki 15-20 yıl boyunca matematikçiler tarafından tekrar tekrar ele alınmıştır. İlk çalışmaların çoğunluğu indirgeme üzerinde duruyordu; yani, sık sık ortaya çıkan şekillere bakıp bunların indirgenebilir olup olmadığını saptıyordu. Bu yolla, yavaş yavaş, indirgenebilir olası şekillerin hepsini içeren bir katalog oluştu. Hiçbir indirgeme yolunun bulunamadığı modeller, kaçınılmayan şekiller listesi düzenlenmesinde dikkate alınmayacaktı. İçinde çok fazla ülke bulunmayan haritalar için bir ölçüde başarı sağlanmıştı, çünkü bunlarda olası konuşlanma modelleri (veya şekilleri) çok daha azdı. 1950 yılına gelindiğin-

de 36'dan az ülke içeren her haritanın sadece dört farklı renkle boyanabileceği saptanmıştı.

Ancak genel problem için durum pek olumlu görünmüyordu. Baş edilebilecek sayıda üyesi olan kaçınılmayan şekiller listesinde her zaman, indirgenemeyen bir üye ortaya çıkıyordu. Bu tür problemlili üyeleri olmayan listelerde ise, her zaman, indirgenir olup olmadığı test edilmesi gereken binlerce üye oluyordu; dört renk problemi çözülmeden önce bunların her birinin indirgenebilir olduğunun gösterilmesi gerekiyordu. Ancak 1950'den sonra yeni bir etken işe karıştı; çok hızlı bilgisayarlar ortaya çıktı ve çalışmalar, problemi, bilgisayarla çözmek için uyarlamaya yöneldi. Doğrudan, elle hesaplama gereği karamsarlığa kapılan daha önceki araştırmacıların çalışmaları tekrar ele alınmalıydı.

İndirgenebilirliği (en azından indirgenebilirliğin daha aşıkâr şekillerini) test etmek için bilgisayar programları geliştirildi ve kısa sürede giderek artan sayıda indirgenebilir konuşlandırma saptanıp kataloglandı; gerçekte, o günden bu yana indirgeme konusunda bazı gelişmeler kaydedilmiş olsa da dört renk probleminin ispatı için gereken bütün kavramlar 1960'ların sonlarında esas itibariyle açıklığa kavuşturulmuştu. Ancak ne yazık ki, problemin öbür yönünde (yani, indirgenebilirliği kanıtlanmamış ve kuşkulu olan türden sorunlu eleman içermediği bilinen kaçınılmaz konuşlandırma listelerini bulmak) aynı ölçüde ilerleme kaydedilmemişti. Ayrıca, en az 18 ülke içeren konuşlandırmaların da içerilmesi gerektiği beklense de bu tür şekiller için bilgisayar süresi bakımından bir dar boğaz vardı. Modele ilave edilen her ülke için gereken bilgisayar testlerinin süresinin dört katına çıkmasıyla ilgili bir sorun vardı. 11 veya 12 ülke içeren şekiller kabul edilebilir süre ve masrafla halledilebilir olsalar da, 1960 sonlarının bilgisayarları için sınıra çok yakındı. 18 ülke içeren bir model için tek bir indirgeme testinin 100 bilgisayar saati alacağı ve o dönemde var olan bellek kapasitesinden fazlasını gerektireceği hesaplanmıştı.

Yeni ilerlemeler için daha hızlı ve daha büyük belleği olan bilgisayarların gelişmesini beklemek gerekiyordu. Hiç kimse

kaçınılmaz ve indirgenebilirler listesinde kaç tane model olacağını tam olarak bilemediği için bilgisayarların daha ne kadar hızlı ve büyük olması gerektiği de bilinemiyordu; ancak listede test edilecek binlerle model olması bekleniyordu. Illinois Üniversitesi'nde, Kenneth Appel ve Wolfgang Haken problemi ele aldıklarında durum böyleydi. Belirli bir sayıdan fazla (örneğin 15 veya 16) ülke içermeyen kaçınılmaz grupları aramakla işe başladılar. Bu listedekilere "iyi şekiller" adını verdiler, yani bunların indirgeme testleri çok uzak olmayan bir zamanda, akla yakın bir sürede, yapılabilirdi.

Bundan sonraki yaklaşık üç yıl boyunca tekniklerini sürekli geliştirdiler ve sonunda, 1975 yazı geldiğinde, dört-renk problemine başarılı bir hücum yapma şanslarının olduğuna karar verdiler. Ocak ile Haziran 1976 arasında, Illinois Üniversitesi'ndeki IBM 360 bilgisayarı kullanılarak, saldırının son ayrıntıları da titizlikle saptanmıştı. En sonunda 1976 yılı Temmuz ayında nihai zafer ilan edildi. İndirgenebilir şekillerin kaçınılmaz olanlar listesi sonunda bulunmuştu. Üç bilgisayar, 100 saatten fazla bir çalışma sonunda onu saptamıştı ve bu iş için, 1500 kadar şeklin indirgenebilir olduğunu göstermek gerekmişti.

O zamandan bu yana hem programlar hem de bilgisayar ispatı başka gruplar tarafından da kontrol edilmiş ve doğrulanmıştır. Illinois'deki görkemli Urbana Postanesi'nin de başarının ilan edildiği günden sonra, postaneden giden bütün posta pullarının üstünde belirttiği gibi; dört renk gerçekten yeterliydi. Öyleyse neden, hâlâ, bütün bunlardan biraz endişeli gibiyiz? Bunun nedeni, hiç kimsenin bu veya başka herhangi bir kitabı okuyarak ispatı ayrıntılarıyla kontrol etme olanağına sahip olmamasıdır.

Bu bilgisayarlı ispatın kabul edilmesinin, normal ispatlarda söz konusu olmayan bir inanç ögesi içerdiği kuşku götürmez. Çünkü, ispatın her satırını okuyup anlasam bile, bilgisayarın yaptığı varsayılan şeyleri doğru olarak yaptığına inanmam gerekiyor. Demek oluyor ki benim, dört-renk probleminin ispatına inanmam, bilgisayarların doğru olarak programlandığına ve bunlarda içerilen hesapları doğru

olarak yaptığına inanmama indirgenmiş oluyor. Bunu ancak (eğer uzmansam) bir başka bilgisayarın yardımına sığınarak kontrol edebilirim. Bu nedenle de kontrol “benim elimden” çıkmıştır.

Bunu, bir matematikçi şöyle açıklıyor: “Dört renk teoreminin ispatlandığını ilk duyduğumda tepkim ‘Harika! Nasıl yaptılar?’ şeklinde olmuştu. Yepyeni, çok parlak bir bakış açısı, güzelliğiyle beni etkileyecek bir düşünce olacağını bekliyordum. Gerçeği öğrendiğimde düş kırıklığına uğradım. Tepkim ‘Bu da onun gerçekten iyi bir problem olmadığını gösteriyor.’ şeklindeydi.” Bir düş kırıklığı olduğu kesindir. Bilgisayar kanıtlarına göre dört renk teoreminin doğruluğunu kabul etsek bile, daha basit, daha zarif bir ispatın “oralarda bir yerlerde” olduğu ve keşfedilmeyi beklediği duygusu var olmayı sürdürmektedir. Bu doğru olabilir ancak ne yazık ki, olmayabilir de. İfade edilmeleri kolay olan matematik problemlerinin ispatlarının mutlaka kolay anlaşılır olması gerekmediği artık bilinmektedir. Bazı durumlarda ise, problemin ileri sürdüğü sav doğru olduğu halde, ispatın *ilke olarak* bile, var olmaması çok şaşırtıcıdır.

Bunlar bizi, bazı basit savların, doğru oldukları halde ya ispatlarının olmadığı ya da, olsa bile, bunların normal anlamda kolay bir ispat olmadığı sonucuna götürüyor. Dört renk probleminin bir ispatı olduğunu biliyoruz; ancak kâğıt-kalemle yapılabilecek türden bir ispatın var olup olmadığını hâlâ bilmiyoruz. Var olsa bile, belki de artık bilgisayar tekniklerine daha yatkın olan problem gruplarının var olabileceği gerçeğini kabul etmenin de zamanı gelmiştir. Bunlar, güçlü teorik araçlar yerine bu yeni türden çözümleri, çok kolay, ancak fazla işlem gerektiren, bunların kâğıt-kalemle tamamlanmalarına insanın hatta evrenin ömrünün yetmeyeceği kadar adım gerektiren problemlerdir.

Ayrıca, bir bilgisayarın sonuçlarının bir başka bilgisayarla kontrol etmenin, yeterince doyurucu olmadığı yolunda, belki de sezgisel bir kuşku hâlâ mevcuttur. Ancak bu pek güçlü bir eleştiri değildir, çünkü çok fazla sayıda doğrudan hesaplama gerektiren işlemlerde bilgisayarlar, insanlara kı-

yasla, çok daha güvenilirlerdir. Buna koşut bir düşünce, var olan bütün ispatların (dört renk dışında) kabul edilebilir uzunlukta ve insanlarca doğrudan kontrol edilebilir olduğu yolundadır; bu da kolayca yanıtlanabilir. Sadece kısa ispatlar üretebilen aletler kullanırsanız, elde edeceğiniz şeyler de bunlarla sınırlı kalır. O zaman sadece bilgisayar tekniğine yanıt verebilen problemler “çözülmemiş” problemler kutusunda sonsuza dek kalmayı sürdürürler.

Bütün bu çabanın, eğer varsa, sonucu ne olmuştur? Bir haritanın dört renk mi yoksa daha fazlasını mı gerektirdiğinin, harita yapanlar için pek önemli olmadığı ortadadır. Ciddi matematiksel herhangi bir sonuç ortaya çıkmış mıdır? Yanıt, çok şükür ki, “evet”! 120 yıllık dört renk probleminin çok önemli bir yan ürünü “Çizge Teorisi” olarak bilinen tümüyle yeni bir matematik dalının gelişmesidir. Noktalar arasındaki izlekleri en verimli biçimde birleştirme konusuyla ilgilenmektedir. Örneğin, insanlara en verimli (yani en az pahalı ve en uygun olan) hizmet götürecek havayolları rotalarını veya telefon hatlarını nasıl saptayabiliriz? Eğer fazla yükleme veya bozulma nedeniyle bir sorun ortaya çıkarsa, sistem içinde yeniden izlenecek en verimli rota hangisidir? Günümüz iletişim ve ulaşım endüstrileri için bunlar çok büyük önem taşıyan sorulardır. Bu konularda yaşamımızı daha kolay hale getirmiş olan bütün ilerlemelerde dört renk probleminin önemli katkısı olmuştur.

Problemin çözümünü sonunda bilgisayarla vermiş olan Dr. Appel ile Dr. Haken’e göre, bundan daha da önemli bir sonuç ümit edilmektedir: Sonunda kuramsal matematiğin geleneksel yöntemleri ile gelişen bilgisayar hesapları tekniğinin karşı karşıya gelmek yerine, işbirliğine girişmelerine yol açacağı. Aynı şeyin geçmişte yaşanmış olduğunu da öne sürüyorlar. Eski Yunan döneminden Ortaçağlara kadar, matematiğin fizikten üstün bir bilim olduğu düşünülürdü. Çünkü matematik, mantığın ve basit, aşıkâr gerçeklerin sağlam temelleri üzerine inşa edilmişti, halbuki fizik, karışık deneyler gerektiriyordu ve ölçüm hataları içeren kesin olmayan yanıtlarla ilgiliydi. Bu tür bir tavır, Galileo Galilei

(1564-1642) gelip, Aristoteles'in yerçekimi etkisiyle cisimlerin serbest düşmesi hakkındaki savlarının yanlışlığını tek bir deneyle ispat edene kadar deneysel fiziğin gelişmesini 2000 yıl geri bırakmıştır. Aristoteles'in bu savları, sadece kuramsal düşünce içeren süreçlerin bir sonucuydu ve bu tür soyut uslamaların varsayılan üstünlüğüne dayanıyordu. Ve 20 yüzyıl boyunca hiç karşı gelinmeden var olmayı sürdürmüşlerdi.

Deney yapmanın önemi kabul edilir edilmez iki bilim alanı (matematik ve deneysel fizik) işbirliği yoluyla, tek başına başarabileceklerinden çok daha fazlasını başarmaya başladı. Appel ve Haken, dört renk problemine verdikleri bilgisayar ispatının, geleneksel matematiksel ispat yaklaşımının sınırlamalarını öne çıkararak kuramsal matematik çerçevesi içinde insan ve bilgisayarın başarılı bir işbirliğine yol açacağını umut etmektedirler.

Bütün bunlar konusunda söyleyeceğimiz sonsöz, dört renk sınırlamasının yalnızca bir düzlem ya da küresel bir yüzey (veya bunlardan sürekli bir deformasyon yoluyla elde edilmiş bir yüzey) üzerine çizilen haritalar için geçerli olduğuyla ilgilidir. Temelde daha çapraşık olan, kulpların, bükülmelerin olduğu yüzeyler için daha fazla renk gerekir. Geçmişte, ta 1890'larda Percy Heawood (Kempe'nin "ispat"ındaki hataya ilk dikkat çeken kişi) bu can simidi benzeri genellemelerin bazılarını araştırmıştı. Bir kürenin içinden, birbirlerini kesmeyen n tünel geçirilirse "cins (genus) n " yüzeyi denilen bir yüzey şekillenir. Öyleyse küre, genus 0 yüzeyidir, bir simit veya bir can simidi cins 1'dir. Heawood şaşırtıcı bir sonuca vardı; cins 1, 2, 3, 4.... yüzeyleri için boyama problemleri orijinal dört renk probleminden daha basitti ve bu, çok daha karmaşık görünen yüzeyler için genel çözümü de verdi.

Böylece can simidi yüzeyine çizilmiş herhangi bir haritayı boyamak için gereken farklı renk sayısı, aynı problemin düz veya küresel yüzey için olan eşdeğerinden 80 yıl önce biliniyordu. Bunu not edelim; yanıt yedidir. Yedi rengin hepsinin de gerektiğini gösteren örnekler verilmişse de bunları bul-

mak hiç de kolay değildir. Uykunuzun kaçtığı bir gece bir iç-lastiği şişirerek şansınızı denemek isteyebilirsiniz. Bunun bir yolu, verilen bir rengin her bölgesinin farklı altı renkli bölgeye dokunacak şekilde çizmektir. Diğer yandan, bu bölümün başında gösterildiği gibi, daha incelikli bir düzenleme bulmak da mümkün olabilir, (Şekil 10'da dört renk problemi için verilmiş olana benzer). Gerçekten meraklı olanlar her iki türden örnekler bulmadan yetinmeyeceklerdir. İç lastiğinizi daha iyi tanımak için gerçekten ilginç bir yol.

Cins 1 (can simidi yüzeyi) dışındaki yüzeyler için Heawood'un verdiği bütün yanıtlar doğru olduğu halde ispatların tam olmaması ilginçtir. Gerçekte, cins n yüzeyi üzerindeki bir haritayı boyamak için gereken en fazla renk sayısını veren bir $c(n)$ formülü vermiştir ve bu formül sıfırdan büyük her n değeri için geçerlidir. Böylece, örneğin, $c(1) = 7$, $c(2) = 8$, $c(3) = 9$, ... (hayır, ilk üç terimin akla getirdiği gibi dizi sonsuza kadar sürmüyor). Heawood hiçbir cins n haritasının $c(n)$ 'den fazla renk gerektirmediğini ispatladığı halde, dikkatinden kaçan bir şey vardı; $c(n)$ 'den daha az rengin bazen yeterli olamayacağını ispatını (can simidi dışında) vermemiş olması. Örneğin bir düzlem veya küresel bir yüzey üzerine çizilmiş bir haritayı boyamak için beş renkten fazlasının gerekmediğini ispatlamak çok kolaydır, ancak bu alışlagelmiş haritalar için beş renk teoreminin ispatlandığını göstermiyor. Sonunda Heawood'un verdiği sayıların doğru olduğu anlaşıldı, ancak ispat 1969'da verilebildi. Heawood'un $c(n)$ için verdiği formülde $n = 0$ olduğunda, çok büyük bir şans eseri, $c(0) = 4$ yani dört renk probleminin doğru yanıtının bulunması ilginçtir. Ancak Heawood, formülünün bu en basit görünümlü geometriye, ünlü dört renk problemine yol açan geometriye uygulanabileceği düşüncesini aklından hiç geçirmedi.

XI. Bölüm

Cetveller, Ominolar ve Profesör Golomb

Cetveller kadar aşına olduğumuz az şey vardır. Bize ölçme olanağı sağlarlar, özellikle de, eğer dikkatimizi bir cm aralıklı işaretlerine çevirirsek, bir ve 12 cm arasındaki herhangi bir tamsayı aralığını ölçmemize izin verirler. İçinizden bunda dünyayı yerinden eden bir şey yok diyebilirsiniz; ancak bu belirli sistemin fazla verimli olmadığını hiç düşündünüz mü? Bu on üç işareti 0'dan (sol, uçta, diyelim) 1, 2, 3, ... olmak üzere en sağ uçtaki 12'ye kadar işaretlediğimizde, örneğin, altı cm'lik bir uzunluğu ölçmek için yedi farklı olanak var. Göreceğiniz gibi cm işaretlerinin şu kombinezonlarından herhangi birisini kullanabiliriz: (0,6), (1,7), (2,8), (3,9) (4,10), (5,11) veya (6,12). Daha uzun aralıklar için de durum pek parlak değil, (dokuz cm uzunluğu, dört farklı yolla ölçülebiliyor) ve daha kısımları için ise çok daha fena. Örneğin tek bir cm uzunluğun tam 12 yolla ölçülebildiğini görmek kolaydır.

Pekâlâ, diyeceksiniz, kabul ediyorum! Ama bundan bana ne? Bu noktaya daha sonra döneceğim. Ancak eğer benim daha sonra açıklama yapmamı kabul ediyorsanız, önce bildiğimiz bütün cetvellerdeki bu genel fazlalığın nasıl azaltılabacağı ya da tümünden önleneyeceği konusunu biraz düşünebiliriz. Böyle bir girişim için, olanaklı en basit durumları ele alarak başlamak her zaman en akıllı yaklaşımdır. Bizim konumuzda en basit yaklaşım ise, sadece iki işareti olan (0 ve 1 diyeceğiz) bir cetveldir. Bu "önemli olmayan prototip cetvel"dir; pratik kullanım yönünden gülünç olmasına karşın, yine de kusursuzca verimlidir. Bundan kastedilen, ölçebildiği tek uzunluğu sadece bir şekilde ölçebilmesidir.

Basitlik bakımından bir sonraki aşama, üç işaretli bir cetveldir. Eğer işaretleri 0, 1 ve 2 konumlarına koyarsak (yani, her iki ucunda ve ortasında birer işaret olan 2 cm'lik cetvel) artık verimli olmayan bir ölçü aleti oluşturmuş oluyoruz, çünkü bir cm'lik bir uzunluğu iki yolla, (0,1) ve (1,2) olarak ölçebilmekteyiz. Oyunun daha başında karşılaştığımız bu durum ümit kırıcıdır ama ümitsizliğe düşmeyin, henüz yenilmiş değiliz. Bunun yerine üç işaretin 0, 1 ve 3 konumlarına konulduğunu düşünelim. Bu üç cm uzunluğunda bir cetveldir ve üç işaret içermektedir, oldukça da ustalıklıdır, çünkü bir cm (0,1) iki cm (1,3) ve üç cm (0,3) ölçebilmektedir, ayrıca her birini de tek bir yolla ölçmektedir. Bu nedenle verimlilik bakımından kusursuzdur; eğer "kusursuz" sözcüğüyle kastettiğimiz, N (cm, diyelim) uzunluğunda genel bir cetvelin 1'den N'e kadar olan tam sayı uzunlukların her birinin tek bir yolla ölçülmesine olanak veren bir cetvel ise, demek oluyor ki 1 ve 3 cm uzunluğunda kusursuz cetveller vardır, ancak 2 cm uzunluğunda yoktur.

Dört işaretli cetveller üzerinde, biraz dene ve göz yöntemi kullanarak, kısa sürede, uzunlukları 4 veya 5 olan kusursuz cetvel olmadığını ancak bir sonraki kusursuz cetvelin, işaretlerinin 0, 1, 4, 6 konumlarında olduğu, 6 uzunluktaki cetvel olduğunu saptarız. Bu cetvel, bir cm (0,1), iki cm (4,6), üç cm (1,4), dört cm (0,4), beş cm (1,6), ve altı cm (0,6) ölçebilir; bunlar yine ancak tek bir yolla ölçülebilmektedir. Kusursuz (yani, kusursuzca verimli) cetvel fikri Güney Kaliforniya Üniversitesi'nde matematik profesörü olan Soloman Golomb'un bir icadıdır. Ancak bunların sadece akademik ilgi konusu olmaması şaşırtıcıdır. Bunlar, şimdiye kadar, kodlama teorisi, x-ışınlarıyla kristalleştirme, radyo astronomisi ve biraz daha bilgi edindikten sonra açıklayacağımız başka alanlarda da kullanılmaya başlanmıştır.

Bunlar hakkında öğreneceğimiz bir sonraki bilgi kırıntısı ise tüm konunun ölüm çanlarını çalar gibidir; çünkü Golomb'un verdiği zarif bir ispatla var olan tüm kusursuz cetvellerin, gerçekte yukarıda verilen üç kusursuz cetvel olduğu saptanmıştır. Bu cetvelleri birim işaretlerine göre şu şekilde yazabiliriz:

0, 1
 0, 1, 3
 0, 1, 4, 6

Beş işareti olan bir cetvel (eğer düşünürseniz) 10 uzunluk ölçülebilir. Eğer kusursuz olsaydı, uzunluğu 10 olurdu ve 1, 2, 3, ... 10 birime kadar uzunlukların her birini ancak bir yolla ölçebilirdi. Ancak dörtten fazla işareti olan cetvellerde kusursuzluk olası iki yoldan birisiyle yitilir; ya uzunluklar birden fazla yolla ölçülebilir ya da bazı uzunluklar hiç ölçülemez. Böyle umutsuz bir durumda, Profesör Golomb'un fikirlerinden esinlenen matematikçiler, bir sonraki en iyi şeyi bulmak için işe koyuldular. Örneğin, var olmayan beş işaretli kusursuz cetvelden bir sonraki en iyi şey, ölçülebilen uzunlukları yalnızca bir defa içeren, ama kaçınılmaz olarak da birçok cetvelin uzunluğundan küçük olan her uzunluğu ölçemeyen bir cetvel olabilirdi. Ancak bu, tek başına, yararlı bir tanım değildir; çünkü istenildiği gibi seçilen bu tür birçok sayı bulunmaktadır. Örneğin, sayılarını rasgele seçtiğim, beş işaretli 0, 4, 10, 27, 101 cetvelini ele alalım. Bu cetvel 4 (0,4), 6 (4,10), 10 (0,10), 17 (10,27), 23 (4,27), 27 (0,27), 74 (27,101), 91 (10,101), 97 (4,101) ve 101 (0,101) uzunluklarını tek bir yolla ölçebilir. Aranılan cetvel beş işareti olan ve "fazlalığı" olmayan, yani hiçbir uzunluğu birden fazla yolla ölçmeyen *en kısa* cetveldir.

Gerçekte, en kısa beş işaretli cetvel 11 uzunluğundaki cetveldir; "ümit edilen" kusursuz 10 cetvelinden bir birim daha uzun olan cetvel. İşaretlerin konumları aşağıda verilmiştir.

0, 1, 4, 9, 11

ve 11'e kadar, 6 dışında kalan bütün uzunlukları ölçebilmektedir. Eğer önceden Golomb'un ispatını bilmiyor olsaydık bu biraz düş kırıklığı yaratabilirdi, çünkü bilinen dört işaretli kusursuz, 6 uzunluğundaki cetvelden yola çıkarak ve giderek artan uzunluklar alarak, olası bir kusursuz, beş işaretli 10 uzunluğundaki cetvele doğru olumlu yolda ilerliyoruz gibi görünüyordu. Böylece örneğin beş işaretli, 7 uzunluğunda bir cetvel bulabiliyoruz.

0, 1, 3, 6, 7

Bu cetvelin *üç kat* "fazlalığı" var; üç uzunluğu (yani 1, 3 ve 6'yı) farklı iki yolun her biriyle ölçebiliyor. Daha sonra, sadece *iki kat* fazlalığı olan 5 işaretli, 8 uzunluğunda bir cetvel buluruz:

0, 1, 4, 6, 8.

Bu cetvelin iki kat fazlalığı var, 2 ve 4'ü iki ayrı yolla ölçüyor. Sonra da 5 işaretli 9 uzunluğunda ve yalnızca *tek kat* fazlalığı olan bir cetvel. Bunun işaretleri;

0, 1, 4, 7, 9

ve eğer kontrol ederseniz, 1 ile 9 arasında, 3 dışındaki, bütün uzunlukları, tek bir yolla ölçüyor, sadece (1,4) ve (4,7) olarak 3'ü iki yolla ölçüyor.

Bu eğilim kaçınılmaz gibi görünüyor. Bir sonraki adımın, sapkınlık göstermeden, beş işaretli kusursuz bir, 10 uzunluğunda cetvel olması gerekiyor. Ancak ne kadar uğraşsak da onu bulamıyoruz, çünkü öyle bir cetvel yok! Ah! Ne acımasız bir dünya! Birden 10'a kadar olan bütün uzunlukları *ölçecek* 10 uzunluğunda bir cetvel bulmak için altıncı bir işaret gerekiyor. Örneğin:

0, 1, 3, 6, 8, 10.

Ancak, o zaman da cetvel utanç verici biçimde verimsiz, çünkü 3, 5 ve 7'yi iki yolla, 2'yi ise tam üç yolla ölçmekle, beş kat fazlalığı var. Bu akıl almaz bir israf. Sayılar, bundan daha dikkatli davranmalı. Deneyimin bu acı ilacını içtikten sonra altı işaretli cetvellere ilerleyebiliriz. İlk önce dört kat fazla olan bir cetvel buluyoruz. Örneğin uzunluğu 11 olan

0, 1, 4, 7, 9, 11

ve daha sonra üç kat fazla olan 12 uzunluktaki

0, 1, 4, 7, 10, 12.

Yine kusursuz bir altı işaretli 15 uzunluğunda cetvele doğru, yüreklenmiş, şaşmadan ilerliyoruz; ama bu cetvel de yok. Ancak bu noktada hiç olmazsa pratik önemi olan bir şey yanıtlamış *olduğumuza* dikkatinizi çekerim. O da, şudur: On iki cm uzunluğundaki bir cetvelin üstündeki on üç işaretten, (cm aralıklarıyla işaretlenmiş), uzunluğu bir ile 12 cm arasında olan bütün tamsayı uzunluklarını ölçme özelliğini yitirmeden, kaç silinebilir? Yanıt, yedisini silerek altı işaret bırakabileceğimiz, yolundadır; örneğin, yukarıda verilen 0, 1, 4, 7, 10, 12 işaretleriyle. Bu durumda 3 cm üç ayrı yolla, (1,4), (4,7), (7,10); 6 cm iki yolla, (1,7), (4,10) ve bütün ötekiler tek yolla ölçülebiliyorlar.

Genel durumda, n işareti olan en kısa cetvele, mucidinin anısına, “ n işaretli Golomb cetveli” denilmektedir. 6 işaretli Golomb cetvelinin uzunluğu ümit edildiği gibi, kusursuz 15 değil, 17’dir. 15 işarete kadar olan bütün Golomb cetvelleri artık bilinmektedirler. 15 işaretin ötesinde, bunu yazdığım şu sırada, henüz bilinmeyen Golomb cetvelleri üzerinde etkin araştırmaların yapıldığı bölgeye gireriz. Aşağıdaki listede bilinen bütün Golomb cetvelleri gösterilmiştir.

İşaretlerin Sayısı	Golomb uzunluğu
2	1
3	3
4	6
5	11
6	17
7	25
8	34
9	44
10	55
11	72
12	85
13	106
14	127
15	151

Bilinen en büyük (15 işaretli) Golomb cetvelinin işaret konumları aşağıdaki gibidir:

0, 6, 7, 15, 28, 40, 51, 75, 89, 92, 94, 121, 131, 147, 151

İşaretlerin sayısı arttıkça Golomb cetvellerinin boyu da oldukça düzgün bir şekilde, artmaktadır; ancak fark edilebilen bir artış modeli yoktur. Örneğin, bir Golomb cetvelinden bir sonraki en büyük cetvele gidildiğinde uzunluklardaki artış aşağıdaki dizide gösterilmiştir:

2, 3, 4, 5, 6, 8, 9, 10, 11, 17, 13, 21, 21, 24, ?

ve modelin “düzgünlüğü” bozulmaya başlamıştır bile. Örneğin, 17 ile 21 arasındaki 13’ün önceden tahmin edilmesi olanaksızdır. Bundan sonra ilk keşfedilecek (16 işaretli) Golomb cetvelinin uzunluğu ne olacaktır? Farklardaki düzene bakarak 173 ile 178 arasında bir değer tahmin edilebilir. 16 işaretli, fazlalığı olmayan 179 boyunda bir cetvel bilinmektedir. Bundan sonra ki “Golomb” bu olabilir, ancak bilgisayarlar bu soruya henüz kesin bir yanıt vermediler.

“Araştırma bölgesi”ne geçerek, bilinen (1989), en kısa 16 ila 24 işaretli, fazlalığı olmayan cetvellerin listesini veriyoruz.

İşaret sayısı	Bilinen en kısa	Alt sınır
16	179	154
17	199	177
18	216	201
19	246	227
20	283	254
21	333	283
22	358	314
23	372	346
24	425	380

Bu tabloda “alt sınır” olarak adlandırılmış bir sütun bulunmaktadır. Bu sütun, belirli sayıda işareti olan bir Golomb cetvelinin en kısa uzunluğunu saptayan bilinen bir formülün sonuçlarından oluşmuştur. 16 işaretli cetvel için bu sayı 154’tür; demek oluyor ki, bunlar yazılırken, 16 işaretli Golomb cetvelinin uzunluğu 154 ile 179 arasında bir yerde olabilir.

Ayrıca, araştırma bölgesinde, fazlalığı olmayan, bilinen en kısa cetveller ve alt limitler arasındaki farkın (bu iki sayının oranı olarak ifade edildiğinde) yaklaşık, 1,075 ve 1,177 sınırları arasında değiştiğini görüyoruz. Bu oranlara göre, araştırma bölgesinde “en iyi” (en küçük oran) tahmin, 18 işaretli ve 23 işaretli cetveller için, “en kötü” (en büyük oran) tahmin ise 21 işaretli cetvel için yapılmış olandır. Bu kitabı okuduğunuz dönemde araştırmanın daha öteye ilerlemiş olacağı hemen hemen kesindir; ancak yine de burada amatörler için bir fırsat vardır. Bir PC yardımıyla, gerçekten meraklı bir kişinin yukarıdaki tablolarda verilen “en kısa” cetvelleri biraz daha kısaltmaları çok olasıdır; ancak gerçek Golomb cetvelinin bulunduğunu göstermek, belki de, günümüzdeki en güçlü bilgisayarlar dışında, hiç kimsenin eriminde değildir. Birisi çıkıp da, günümüzde uygulanan her olası adayı üretip kontrol etme şeklindeki basmakalıp süreçten daha verimli bir test geliştirirse, kuşkusuz durum değişir.

Bütün bunların, bir bilgisayar alıştırması olarak eğlenceli olmak dışında, inanmayabilirsiniz ama, pratik bilimsel kullanımları da vardır. Sayıların ilginç özelliklerini araştırırken, yararlı olma gibi bir gerekçe geleneksel olarak, akla bile gelmez. Gerçek “sayı-meraklısı” için eğlence sayıları, her bakımdan çalışan sayılar kadar ilginçtirler. Bu bağlamda yararlılık, pastanın üstüne sürülen krema gibidir. Son dönemlerdeki uygulamalardan birisi radyo astronomisi alanındadır. Bu bilim, uzayın derinliklerindeki “radyo kaynaklarından” dünyaya gelen uzun dalga boylu elektromanyetik ışıınımı araştırılmaktadır. Bu kaynaklar o kadar uzaktırlar ki, Dünya’dan gözlem yapanlar için onlar uzaydaki “nokta kaynaklar” veya ölçülebilen alanları olmayan nesneler için en iyi yaklaşım sayılırlar. Eğer bilimciler böyle bir ışıınının uzaydaki doğrultu-

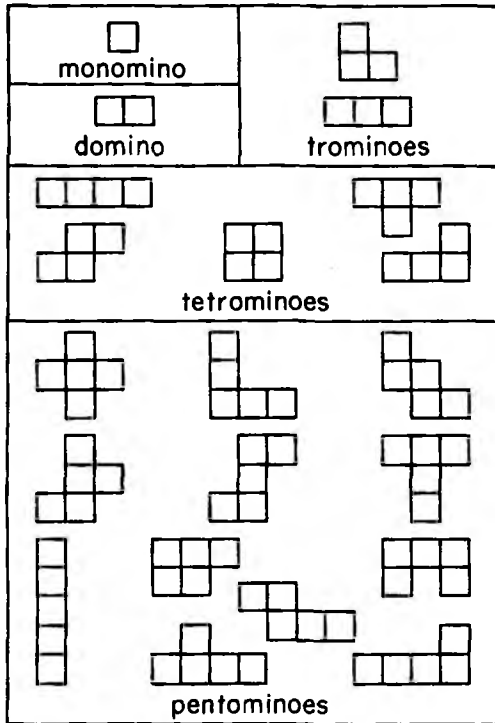
sunu dakik olarak saptayabilirlerse o zaman, Dünya'daki uzaklıkları (New York'taki Empire State Building'in tepesi ile Paris'teki Eiffel Kulesi'nin tepesi arasındaki uzaklık gibi) birkaç cm'lik bir hata payı ile saptayabilirler.

Işınım, sayısız ışık yılı boyunca uzayda yol aldıktan sonra Dünya'ya vardığında (bizim ölçümlerimiz bakımından) *tam olarak*, paralel bir dalga sınırı şeklinde, kıyıya bir açıdan çarpan paralel dalgalar biçimindedirler. Uzaydan geldikleri açıyı ölçmek (deneyin yapıldığı yöredeki yer düzeyine göre) için birkaç km uzunluğunda düz bir doğru boyunca antenler yerleştirilir. Gelen sinyaldeki her dalganın her antene vardığı an, olanaklı en büyük hassasiyetle saptanır. Daha basit olsun diye her antenin, dalga tepesinin ulaştığı anı kaydettiğini varsayalım. Ayrı antenlerde bulunan iki bilimcinin karşılaştığı sorun şudur: Gözledikleri "aynı dalga tepesi miydi, yoksa farklı iki tepe miydi?" Kıyının farklı noktalarında ellerinde kronometre olan iki insan dalga üzerinde aynı deneyi daha kabaca yaptıklarında yanıtı bulmaları kolaydır; çünkü onlar kıyı boyunca bütün dalga sınırını görebilirler. Radyo dalgası deneyinde durum daha zordur. Ancak, bir Golomb cetveli "işaretleri" boyunca yerleştirilen antenlerle yanıtı bulmanın mümkün olduğu anlaşılmıştır. Eğer iki anten arasındaki uzaklık, farklı başka iki çift anten arasındaki uzaklığa eşitse, o zaman bu iki çift anten yeterli bilgi vermektedir. Bu nedenle belirli sayıdaki antenler için açı hesaplamadaki en büyük hassasiyet, antenler Golomb cetveli işaretlerine göre konuşlandırıldıkları zaman elde edilmektedir.

Bu pahalı deneylerin nihai sonucu Dünya üzerindeki uzaklıkları ve açısal yönleri daha önce erişilememiş bir hassasiyetle ölçebilme olanağıdır. Örneğin dünyanın çapı, çevresinde döndüğü eksenin eğimi ya da bir günün uzunluğu vb. gibi temel nicelikler sırasıyla, santimetre, açısal bir yayın saniyelik kesri ve zamanın mikrosaniye hassasiyetiyle ölçülebilmektedirler. Bu hassas ölçümler de bu niceliklerdeki yıllık, mevsimlik ve hatta meteorolojik değişimlerin saptanmasına olanak sağlarlar. Bu sonuçlar şimdilik, daha

çok şaşırtıcı ve gizemli olsalar da yakın dönemde, yaşadığımız fiziksel dünyanın anlaşılmasında büyük ilerlemelere yol açabilirler.

Profesör Golomb, Harvard'da öğrenci olduğu gençlik yıllarında, hâlâ çözüme karşı koyan bir zekâ-bulmacasının da sorumlusuydu. Problem *Poliomino* olarak tanımlandığı bir nesneyle ilgilidir. Bir poliomino (ben onu "omino" ailesinin bir genel üyesi olarak düşünürüm) eşit kenarlı kareleri kenarlarından birleştirilerek elde edilen bir şekildir. Öyleyse, bunun en basit üyesi (önemsiz olan ve tek bir kareden ibaret olan "monomino" dışında) bildiğimiz domino'dur ve bütün omino terminolojisi bundan elde edilmiştir.



Şekil 11.

Gerçekte, iki eşit boyutlu (onlara “birim” diyeceğiz) kare-den bir domino oluşturma'nın tek yolu vardır, çünkü burada uzaydaki yönlenmeyle ilgilenmiyoruz. Başka deyişle, *bizim* için “kuzey-güney” dominosu ile “doğu-batı” dominosu, *biçim* yönünden aynıdır. Ancak tromino (üç kareden oluşan şekil; bunun son zamanlarda satışa sunulan tri-ominolarla bir ilgisi olmadığını unutmayın) biçim bakımından birbirinden farklı iki şekilde yapılabilir. Bunlar Şekil 11’de gösterilmiştir. Birisi zincir benzeri bir yaratık, öbürü de büyük L harfi-ne benzer bir şey.

Domino ve tromino kavramlarının 4, 5, 6, 7, ... birim kare-den oluşan giderek artan karmaşıklıkta ominolara genelle-nebileceği açıkça görülmektedir. Dört-kare türü veya tetro-mino, farklı beş şekilde olabilmektedir, beş-kareli tür olan pentominos ise tam 12 şekilde (yine Şekil 11’e bkz.) oluşabil-mektedir. “1, 2, 3, 4, 5, ... birim kareden oluşan, temelden farklı kaç omino bulmaktadır?” sorusunun yanıtı böylece aşağıdaki sayı dizisiyle başlar;

1, 1, 2, 5, 12,

Ancak dizi nasıl devam etmektedir? n birim kareden olu-şan genel poliomino için yanıtı veren formül nedir? Böyle bir formül gerçekten var mıdır? Profesör Golomb bunları soru-yordu ve bu satırların yazıldığı şu anda yanıtlar hâlâ bilin-memektedir.

Diğer yandan artık elimizde büyük ve güçlü hesap yapabi-len makineler bulunduğu için, en az 18 birim kareden oluşan poliomino'lar için belirli sayısal yanıtlar “sayı öğretici” yoluyla elde edilmiştir. Dizi, $n=18$ 'e kadar şu şekilde ilerlemektedir:

1, 1, 2, 5, 12, 35, 108, 369, 1285, 4655,
17.073, 63.600, 238.591, 901.971, 3.426.576,
13.079.255, 50.107.911, 192.622.052

Ayna yansımaları sayılmamıştır; ancak içinde delikler olan şekiller içerilmiştir. Art arda gelen sayılar arasındaki

oran 3,8 ile 3,9 arasında bir bölgeye yöneliyor gibidir, başka deyişle yukardaki dizinin sonuna doğru olan her sayı, kendinden önce gelen sayının dört katından biraz küçük. Ancak genel problem için alt ve üst sınırları veren formüller olduğu halde kesin sayıyı saptayacak bir formül bilinmiyor.

Özdeş eşit kenar üçgenlerin, kenarları boyunca birleştirilmeleriyle şekillenen “ominolar” için de benzer ve çözülmemiş bir problem vardır. İlk birkaç üçgen poliomino gruplarını bulmak ve bunların kare birimli akrabalarından daha büyük sayılara mı, yoksa küçük sayılara mı yol açtığını denebilirsiniz. Daha gayretli olanlarınız düzgün altıgen (yani, eşit açılı ve eşit kenarlı) poliominolar oluşturmaya bile girişebilirler. Bütün bu problemler genel bağlamda çözülmemişlerdir. İşlemler bakımından bir sonraki bölümde açıklandığı anlamda “zor” problemdirler. Ancak bildiğim kadarıyla bunların gerçekten NP-tam (0 bölümün terminolojisiyle) olup olmadıkları henüz kesinleşmemiştir.

XII. Bölüm

NP Problemi de Nedir?

AT&T Bell Laboratuvarından Dr. Ronald Graham, hayali bir bisiklet montaj fabrikasında yaşanan bir planlama problemiyle ilgili, ilginç bir öykü anlatmıştı. Anlaşılan (en azından öyküye göre) bir bisikletin montajı, gövdeyi hazırlamak, tekerlekleri monte etmek, vitesleri takmak vb. gibi 10 ayrı işlem içeriyor. Bu 10 işi harflerle (A'dan J'ye diyelim) adlandırarak, her işi tamamlamak için montaj ustalarına gereken süre, dakika olarak, aşağıdaki tabloda gösterilmiştir:

İş	A	B	C	D	E	F	G	H	I	J
Süre	7	7	7	2	3	2	2	8	8	18

Uzun süre alan J işi, takma ve ayarlama (gidon, sele, frenler gibi) içeren en son işlerle ilgilidir.

Yukarıda verilen süreleri topladığımızda bir montaj ustasının bu işi tek başına tamamlaması için 64 dakika gerektiği ortaya çıkar. Bu fabrikanın montaj atölyesinde yer sorunu olduğu bilinmektedir, şöyle ki, 20 montaj ustasının her birinin tek başına, ayrı bir bisiklet üzerinde çalışması için yeterince geniş yer yoktur. Bu nedenle işler, ustalar ikişer kişilik on ekibe ayrılarak, her ekip bir bisiklet üzerinde çalışacak şekilde düzenlenmiştir.

Bunu yapmakla her ekibin bir bisikleti, tek usta için gerekenin yarısı kadar sürede (yani 32 dakikada) tamamlaması bekleniyordu. Yukarıdaki tabloya bakarsak, işleri örneğin, aşağıdaki biçimde ayırarak bunun sağlanabileceğini görürüz.

Usta 1	İş	A	D	E	F	J
	Süre	7	2	3	2	18
Usta 2	İş	B	C	G	H	I
	Süre	7	7	2	8	8

Ancak, ne yazık ki, bir sorun çıktı, bir bisikletin parçalarını, herhangi bir sırada birleştirme olanağı yoktu. Bazı şeyler, diğer bazıları takılmadan önce monte edilemiyor; örneğin pedallar ancak vites vb. bazı şeylerden sonra takılabiliyor. Bu nedenle, işin pratik gerçekleri göz önüne alınarak montaj sırasında bazı sınırlamalar yapılması gerekiyor. Getirilen kısıtlamaların, bizim harflerle ifadeleri şöyle oluyor.

Bu işler,	bu işlerden önce yapılamaz.
J	A, B, C, D, E
C	D, E, A
E, F	D
H, I	E, F, G
G	F
B	A

Bunun işleri oldukça karıştırdığını söylemeye gerek yok. Özellikle, yukarıda verilen 32 dakika planı hemen suya düşüyor. Çünkü plan, C işinin (Usta 2 tarafından) A ve B işleri tamamlandıktan sonra başlamasını öngörüyor, halbuki kısıtlama tablosu, D, E ve A işleri bitmeden C'nin yapılamayacağını söylüyor. Çalışma planının tekrar gözden geçirilmesi gerektiği aşikâr. Bir çok dene ve gör uygulamasından sonra şirket sonunda “standart” olarak benimsendiği, aşağıdaki tabloda karar kılıyor:

Usta 1		A		B		I		H	
Süre		7		7		8		8	
Usta 2		D F G E		C				J	
Süre2		2 2 2 3		7				18	

Eğer kontrol ederseniz, bütün pratik kısıtlamalara uyulduğunu ancak ne yazık ki, ilk beklenenden 2 dakika daha fazla süre, 34 dakika aldığını görürsünüz.

Buna karşın son derece kabul edilebilir bir plandır; çünkü, zaman israfını önlemek için şirketin benimsediği, aşağıda verilen iki kurala da uymaktadır.

Kural 1. Hiçbir montaj ustası, yapabileceği bir iş varsa, boş kalmaz.

Kural 2. Başlanan her iş en kısa sürede tamamlanmalıdır.

Bu plan bir süre için, yaklaşan Noel zamanı ile birlikte gelen ek siparişler yığılmaya başlayana kadar, çok iyi iş gördü. O zaman şirket, üretimi artırmak amacıyla, zaman-hareket incelemesi yapacak bir verimlilik uzmanı çağırdı. Planlamayı geliştirmek için birkaç başarısız girişimle sayfalarca kâğıt israf ettikten sonra, verimlilik uzmanı üretimde istenilen artış sağlaması için elektrikli aletler kiralamayı önerdi. Bu aletlerin kiralanması hayli pahalı da olsa, her bir iş, el aletlerine kıyasla, bir dakika daha kısa sürede tamamlanıyordu.

Yapılacak 10 ayrı iş olduğu ve her birinden bir dakika kazanıldığı için iki ustadan oluşan her ekip için yaklaşık beş dakikalık bir iyileşme bekleniyordu. Başka deyişle, tek bisikletin montajında 30 dakika engeli aşılmış oluyordu; bu, şirketin Noel telaşını karşılamak için amaçladığı hedefti.

Önce, 34 dakikalık “standard” iş düzenine göre çalışmaya başlandı, ama işler iyi gitmedi. Eğer işçiler çalışabilecekleri bazı sürelerde işsiz kalmayacaklarsa (bu iş verimliliğinin 1. kuralının ihlali olurdu) düzenlemede bazı değişiklikler yapmak kaçınılmazdı. Neler olduğunu görelim. Yukarıda verilen standard plan uygulamasında aşağıdaki noktada bir sorun çıktı:

Usta 1		A	
Süre		6	
Usta 2	D F G E C ?		
Süre	1	1	1 2

Usta 2 standart iş planına göre yapması gereken C işine 5. dakika noktasında başlayamıyordu, çünkü Usta 1 henüz A işini bitirmemişti (ve A tamamlanmadan önce C başlayamazdı.) Usta 1'in A işini bitirmesini beklemek 1. verimlilik kuralının Usta 2 tarafından ihlali demekti. Bu durumda Usta 2 yapabileceği bir başka iş bulmak zorundaydı, yani H veya I. Verimlilik kurallarını harfiyle uygulamak böylece, ikili montaj ekibinin tek bisiklet montaj süresini beklenmedik biçimde 35 dakikaya çıkarmıştı; daha yavaş el aletleri kullanarak yapılan süreden bile uzun bir zaman. Bunun nasıl olduğunu tam olarak görmek için kesin çalışma planını tekrar yazalım:

Usta 1		A		B		H			
Süre		6		6		7			
Usta 2		D		F		G		E	
Süre		1	1	1		2		7	
								6	
									17

Verimlilik uzmanı bunun çok saçma olduğunu düşündü ve daha kısa iş sürelerinin avantajını iyi kullanmak için iş planını tekrar düzenleme üzerinde biraz düşünmenin iyi olacağına karar verdi. Ancak, ne yazık ki, ne kadar düşünse de yukarıdaki 35 dakikadan daha iyi bir plan bulamadı. Eğer şirketin “verimlilik kuralları”na bağlı kalınacaksa, buna şaşırılmamak gerekir.

Ümitsiz bir son atılımla kiralanmış olan aletler geri verildi ve bu iş için daha çok işçi kullanılmasına karar verildi. Böylece yüzde elli daha fazla işçi alınarak her bisiklet üstünde üç montajcının çalışması sağlandı. Şirket bunun maliyet açısından iyi olmadığını fark ediyordu; ancak Noel sırasında bisikletleri acilen piyasaya vermek zorundaydı, bu bir panik dönemi idi. Verimli bir iş düzeni bulmak için biraz düşünmeye gerek olduğu açıktı, ancak şimdi bir bisiklet için ideal süre 64/3 (veya yaklaşık 21) dakika olduğu için, çok verimli olmayan bir planla bile, 30 dakika sınırı sıkıntısızca aşılabiliirdi.

Tam bu noktada gerçek kabus baş gösterdi. İlk olarak, her üç işçinin de aynı anda montaj çalışmasına başlama ola-

nağı yoktu; çünkü, daha önce montaj gerektirmeyen sadece iki iş vardı, A ve D işleri. Yeni işe başlayan Usta 3 bu nedenle göreve, oturup bakmakla başlamak zorundaydı. Umut verici bir durum değildi bu!

Ancak, daha kötüsü gelmek üzere. Verimlilik uzmanının, üç usta kullanarak ve şirket kurallarına uyarak, bulabildiği en iyi düzen, her montaj için 32 dakika gerektiriyordu. Bu, 30 dakika hedefinin dışında olmaktan başka, ilk uygulanan “standart” iki-usta düzenlemesinden sadece 2 dakika daha kısaydı. Bütün kural ve kısıtlamalara uyan en iyi üç-usta düzen şöyleydi:

Usta 1		A		B		I	
Süre		7		7		8	
Usta 2		D		E		G	
Süre		2	3	2		7	
Usta 3			F			H	
Süre		2	2	3		8	

Söylendiğine göre, verimlilik uzmanı, en son, çığlık çığlığa koşarak oralardan uzaklaşırken görülmüştü. Eğer başka bir gerçeği bilseydi, bir uçurumun tepesine doğru koşuyor olabilirdi! Çünkü, ilk verilen “standart düzenden daha da verimli olan bir iki-usta düzeni bulunuyor. Bu, gerçekte, 32 dakika ile sadece üç-usta ekibine verimlilik bakımından eşit olmakla kalmıyor iki-usta ekibi için de kusursuzca verimli. Onu bulabilir misiniz? Onu size söylemeli miyim yoksa işin zorluğunu anlamanız için size mi bırakmalıyım? Vazgeçiyorum (isterseniz kopya çekebilirsiniz!) Kusursuz çözüm şudur:

Usta 1		A		B		J	
Süre		7		7		18	
Usta 2		D		E		F	
Süre		2	3	2		7	
Usta 3		C		G		I	
Süre		2	3	2		8	

Biraz eğlenceli biçimde aktardığımız bu öykünün çok ciddi bir yönü var. Bu tür planlama problemlerinin araştırılmasına ilk yol açan sorun, anti-balistik roket savunma sistemleri için bilgisayar programları düzenleme çalışmalarıdır. Orada, bilgisayarın bireysel öğelerinin bilgisayar verimliliklerini artırarak, çalışma sürelerini azaltmanın, problemin tümünün süre bakımından, otomatik olarak, daha verimli olmasına yol açmadığı anlaşılmıştır. Bu askerler için, endişe verici bir sonuçtu.

Tekrar bisiklet firmasına dönersek, gerçekten ne yanlış yapılmıştı? Yüzeyde her şey, optimum bir program için ayarlanmış gibi görünüyordu. Gerçek suçlu “verimlilik kuralları”ydı. Bunlar, yolun ötesinde, beklenmeden ortaya çıkabilecek, belki de önemli problemleri dikkate almadan, ileriye göremeyen bir aç gözlülük içeriyorlardı. İşçiler ara vermeden çalışma zorunluluğu olan işlerle başlıyorlar ve sonradan daha acil bir iş çıktığında, ara vermelerine olanak olmuyordu. Eğer sadece kiralananmış alet uygulanmasındaki kritik 5 dakika noktasında Usta 2’ye A işinin bitmesine izin verecek 1 dakikalık parmaklarıyla oyalanarak bekleme süresi tanınsaydı. Bu olsaydı daha sonraki planlama düzeni çok farklı olabilirdi. Örneğin:

Usta 1		A		B		I		H	
Süre		6		6		7		7	
Usta 2		D		F		G		E	
Süre	1	1	1	2	1	6		17	

Sonuçta 30 dakika hedefi aşılarak (tam olarak 29 dakika) mutlu sona varılabilirdi. Bütün o panik ve verimlilik uzmanının son delilik nöbeti önlenebilir ve şirket için Noel zamanı parasal bakımdan bir o kadar daha neşeli geçerdi.

Daha genel bir bağlamda, bilgisayarı bir sonraki en verimli adım için programlama, çoğu kez, oldukça kolaydır ancak onu “ileriye görecektir” şekilde veya o kısa vadeli kararın istenmeyen olası bazı sonuçlarını öngörecektir şekilde programlamak ise çok zordur. Bütün problemlerin bu tür

hoş olmayan yönleri yoktur. Bazıları için bir sonraki en verimli adım gerçekten, bütün için de en verimli olan adımdır. Ne yazık ki, daha önemli olan planlama problemlerinin büyük bölümünün artık saç-baş yolduran türden olduğu anlaşılmıştır. Bunlar, mutlak bir anlamda, daha yüksek zorluk derecesindeki problemlerdir; özellikle inatçı olan bu matematiksel bilmece sınıfına *NP problemleri* denilmeye başlanmıştır. Bunlar ilk olarak 1970'li yılların başlarında bir grup bilgisayar bilimcisi tarafından fark edilmiştir ve açıklaması, uğraşmamıza değmeyecek ölçüde karmaşık nedenlerle, gerçekte NP, "gerekirci olmayan polinom" yerine kullanılmaktadır.

Bu problemler, ilke olarak değil sadece uygulamada zor olan problemlerdir. İlke olarak, önce, olanaklı her farklı durum için hesaplanarak (bilgisayarla hesaplama daha olası) sonra da (eğer varsa) verilen koşulları sağlayan en verimli sonuç seçilerek tam olarak çözülebilirler. Bundan daha basit ne olabilir? Ancak sorun, en basit olanlar dışında kalan bütün NP problemlerinde farklı durumların sayısının akıl almaz büyüklükte olmasıdır. Bunlar için günümüzün (hatta belki de yarının) en güçlü bilgisayarları bile o kadar uzun bir süre kullanmaktadır ki, aşikâr görünen bu çözüm yöntemi uygulama bakımından tümüyle elverişsizdir. Gerçekte, günümüz teknoloji dünyasının ilgilendiği, daha önemli NP problemlerinin çoğunun mutlak olarak en verimli olan çözümünü kesinlikle saptamak için bilgisayarları yüzyıllar boyu (hatta bazıları için, evrenin var olduğu süreden de uzun bir zaman) çalıştırmak gerekebilir.

NP problemlerinin hepsi yeni değildir. Bazıları yıllardır biliniyor ve birçok uygulamalı durumda aniden ortaya çıkıyor. Bu birbirleriyle ilişkisiz gibi görünen problemlerin hepsinin, matematiksel bir anlamda, aynı ailenin bireyleri oldukları, ilk olarak Toronto Üniversitesi'nden Stephen Cook tarafından, 1971'de fark edildi. Bu, problemlerden herhangi birisi için iyi bir çözüm bulmaya yarayan etkili, yaklaşık bir yöntemin diğerleri için de geçerli olacağını anlatmaktadır. Daha önce matematikçiler bu problemlerin her birini tek tek

ele alıp, her biri için ayrı bir “iyi” çözüm yöntemi arıyorlardı. Cook’un çalışmalarından sonra bilimciler, daha önce bağlantısız olan planlama problemlerinin kaç tanesinin, kısa süre sonra NP-tam (veya sadece NP) problemleri olarak adlandırılacak problemler içine alınabileceğini görmek için atağa kalktı. Bu satırların yazıldığı sırada bir kaç yüz kadar bu tür problem saptanmıştır. En ünlülerine bir göz atmak eğlenceli olabilir.

Bu problemlerin en ünlüsü ve medyanın ilgisini çekmiş olanı, belki de, gezgin satıcı problemidir. Bir gezgin satıcının ülkeyi baştan başa dolaşıp 10 kente uğradıktan sonra oturduğu kente döneceğini varsayalım. Eğer izleyeceği yol, saate en az km olacak şekilde düzenlenirse bu zaman ve benzin masrafı bakımından onun yararına olacaktır. Tümülle matematiksel olan bir bakış açısından ilk durak olarak bu on kentin herhangi birisi onun emrindedir. Daha sonra, ikinci durak yeri için, dokuz seçim vardır, sonra sekiz vb. Böylece farklı gezi programlarının toplam sayısı $10! = 3.628.800$ ’dür. Ancak bu rotanın yarısı sadece ters yönde, yolun öteki yarısından oluştuğu için doğru sayı $10!$ ’in yarısı veya $1.814.400$ ’dür. Formal olarak bile, bu problem yeterince korkunçtur. Uygulamada, doğal olarak, bu matematiksel olasılıkların bir çoğu “sağ duyu” kullanılarak reddedilecektir. Satıcımız ideal gezi programını, büyük ihtimalle, küçük sayıda daha akla yakın olasılıkları dikkate alarak saptayacaktır.

Eğer kentlerin sayısı daha fazla olursa örneğin, ABD’nin 48 eyalet başkenti söz konusu olursa ne olur? Şimdi problem çok fazla bilgisayar süresi gerektiren, çok zor bir hale gelmiştir; ancak tam çözümü yıllardır bilinmektedir. Satıcının bir başkentten yola çıkıp yol boyunca 47 başkenti dolaşıp ilk başkente, döndüğünü düşünelim. Hiç düşünmeden problemin birbirinden farklı $47!$ ’in yarısı kadar yani $1,3 \times 10^{59}$ rota içerdiğini söyleyebiliriz. Saniye’de bu tür bir milyon işlem yapabilen bir bilgisayar kullanırsak işlemi tamamlamak, yaklaşık 4×10^{45} yıl, veya evrenin yaşının 10^{36} katı kadar zaman alacaktır. Burada sağduyunun büyük

yardımlı olacağı açıktır ve gerçekte ilk olarak 1948'de elde edilen çözüm, bu boyuttaki bir satıcı problemi için *kesin* en iyi yolu saptayabilen özel bir lineer programlama yöntemiyle bulunmuştu; bu sonucun açıklanması gezgin satıcı tarihinin sanki bir dönüm noktası olmuştu. Birkaç yüz konumla ilgileniyorsak ne olur? Başka hiçbir ek kısıtlama getirilmes-e bile problem artık günümüz bilgisayarlarının kesin çözüm kapasitelerini aşmaktadır.

Gezgin satıcımızı birkaç yüz kent dolaşacak şekilde programlamak onun için zor olsa da bu boyutta sayılar içeren benzer problemleri düşünenler için bu zor değildir. Örneğin, paralı telefon kulübelerinden veya satış makinelerinden, hatta parkmetrelerden para toplamak bizim en verimli planlama amacımızı zorlayabilir. Daha teknik bir düzeyde, son derece daha karmaşık olan telefon çağrılarını yönlendirme problemi düşünülebilir. Bu problem günümüzde, milyonlarca konumdan yapılan milyonlarca telefon konuşmasından başka, yoğunluk veya arıza durumlarında, eğer olanak varsa, farklı rotalar planlamayı da içerebilir. Bu tür bir NP probleminin daha iyi bir çözümü telefon şirketi için milyonlarca dolar tasarruf demek olabilir.

Çok ilgi çeken bir başka zor problem ya da NP problemi de, bidon paketleme denilen problemdir. Belirli bir sayıda birbirinin aynı bidon ve oldukça farklı biçimlerde bir yığın paket olduğunu varsayalım. Bütün paketleri, bidonlar içine, dışarı taşmadan, koyabilmek için en az kaç bidona gerek olduğu sorulabilir. Burada da, temel problem, aynı türden büyük bir grup problemin bir örneğidir; bu problemler, farklı uzunluktaki televizyon reklamlarının bir dakikalık zaman aralıklarına göre sıraya konulması veya ev yapımında kullanılan kalasların farklı uzunluklardaki parçalara biçilmesi gibi daha çağdaş problemleri de içermektedir. Başka örnekler bulmak da kolaydır; örneğin, kargo yükleme, ambar depolama ve bütçe planlama.

Bidon doldurma problemleri, gerçekte, daha önceki planlama problemlerinin ters çevirilmiş şeklidirler. Belirli bir sayıdaki işçinin, verilen bir işi, bazı sınırlamalar uyarınca, en

çabuk nasıl tamamlayacaklarını sormak yerine şimdi bir işi, belirli bir sürede bitirmek için en az kaç işçinin gerektiği sorusuna, matematiksel bakımdan yakın olan bir soru sormaktayız. Bunu bidon doldurma lisanına çevirdiğimizde bidonlar işçilerin yerini alır, paketler de tamamlanmış işi oluşturan iş öğeleridirler. Öyleyse bidon doldurma da bir NP problemi ve bu nedenle de, mutlak olarak en iyi düzeni bulma anlamında, çözümü zor olan bir problemdir. Ayrıca, bu konuda aşikâr olan ve genelde çok fazla zaman isteyen, olanaklı bütün düzenlemeleri (en azından ilke olarak) tek tek kontrol etme yöntemi dışında, kesin çözüm veren herhangi bir yöntem de bilinmemektedir. Örneğin, eğer bir milyardan (10^9) küçük olan ve toplamı da 50 milyardan biraz küçük olan rasgele seçilmiş yüz sayı verilirse ve sonra da bunların beş milyar kapasitesi olan 10 bidona yerleştirilip yerleştirilmeyeceğinin saptanması sorulursa bu, günümüz dünyasındaki toplam bilgisayar kapasitesini aşmaktadır. Bu durum inanırlılığı zorluyor gibidir; çünkü sadece 100 sayıdan (veya paketten) söz ediyoruz ve bundan çok daha karmaşık bidon problemleri olduğu kesin. Ancak, gezgin satıcı probleminde sadece birkaç düzine (veya en fazla birkaç yüz) kentten söz ediyorduk.

Bidon paketleme probleminde yanıtı bulmak için denenecek olanaklı düzenleme sayısını bulmak özellikle kolaydır. Örneğin, eğer sadece A ve B bidonlarımız ve iki paketimiz (a ve b) varsa olanaklı düzenleme sayısı dört ya da 2^2 'dir: (1) a'yı A'ya, b'yi B'ye koyabiliriz; (2) b'yi A'ya, a'yı B'ye koyabiliriz; (3) a ve b'yi A'ya koyar, B'ye bir şey koymayız; (4) a ve b'yi B'ye koyar, A'ya bir şey koymayız. Eğer üç paketimiz ve 2 bidonumuz varsa, kombinasyon sayısının sekiz veya 2^3 olduğu hemen bulunabilir, dört paket ile toplam 16 veya 2^4 kombinasyon vardır. Bu sayıların düzeni bir genellemeye işaret ediyor gibi ve bunun gerçekten doğru olduğu ortaya çıkıyor. Yani, n paket iki bidona, 2^n yolla konulabiliyor. Eğer üç bidon varsa bu sayı 3^n oluyor vb. böylece en genel sonuç, n paketi N bidona koymanın N^n sayısı kadar farklı biçimde yapılabileceği şeklindedir.

Bütün evrende toplam 10^{75} atom olduğuna göre, 75 pake-ti 10 bidona koyma probleminin evrendeki atom sayısı ka-dar olanaklı çözümü var demek oluyor. Yukarda verilen, yüz sayıyı 10 bidona koyma probleminin, artık bildiğimiz gibi, 10^{100} (bazıları bu sayıya gogol diyor) olanaklı çözümü var ve şimdi problemin karmaşıklığını daha iyi anlıyoruz. Gogol, katrilyonlarca evrendeki toplam atom sayısından daha büyük bir sayıdır. Bilgisayarların kapasiteleri konu-sunda yukarıda söylenenlerden sonra, hiçbir bilgisayarın, bu problemi hiçbir zaman çözemeyeceği aşikârdır (hatta hayal edilebilecek en hızlı ve verimli, geleceğin bilgisayarı bile). Çok temel ve büyük bir matematiksel gelişme yardı-ma gelirse durum değişebilirse de şimdilik ufukta böyle bir şey görünmüyor.

Öyleyse ne yapılabilir? Vaz mı geçeceğiz? Kesinlikle ha-yır! Sadece biraz daha alçakgönüllü olup, eğer *mutlak* en iyi çözümü bulmak için tutarlı bir yöntem bulamıyorsak, hiç ol-mazsa en iyiye yakın olan bir yanıt verecek daha basit bir yöntem bulmaya çalışacağız, diyoruz. Bize gereken, “algorit-ma” yöntemidir. Bu yöntemde bilgisayar bilimcileri problemi çözmek için makineye, adım adım izlenecek bir dizi talimat verirler. Daha doğrusu, bize gereken “iyi bir algoritma”dır; çünkü olanaklı her çözümü hesaplayıp, hepsini tek tek kont-rol etmek şeklinde bir “kötü algoritma”mız zaten var.

Algoritmalar bakımından “iyi” ile “kötü” arasındaki fark süreyle ilgili bir şeydir. Özellikle n paketle ilgili bir problem-de bilgisiyar süresi üslere göre artıyorsa (yani, bir sayının n 'inci kuvveti gibi artıyorsa) algoritma kötüdür. Eğer paket-lerle ilgili bir problemde, paket sayısı ile ilgili olan süre bu tür, üslere göre artma içermiyorsa algoritma iyidir. Örneğin, eğer gereken süre sadece n 'ye (veya, hatta n 'nin bir kuvveti-ne) orantılı ise o zaman n makul değerlere yükseldiğinde (örneğin, yüzlere veya binlere) çözüm için gereken süre kötü algoritmalarda olduğu gibi, korkunç bir hızla “patlamaz” Böylece iyi algoritmayla n -merdiveninde, akla uygun bir sü-rede (ve daha kabul edilebilir bir masrafla), kötü algorit-mayla çıkabileceğinizden, daha yukarıya çıkabilirsiniz. Bu-

nu, farklı iki algoritmayı kıyaslayarak daha iyi değerlendirebiliriz. Birisinin n^2 gibi değiştiğini (yani tanımımıza göre iyi bir algoritma) diğerinin de 2^n gibi değiştiğini (kötü bir algoritma) varsayalım. Hangi anlamda iyi ve kötü oldukları, 100 paket içeren bir bidon doldurma problemini kıyaslayarak açıkça görülebilir. Bu durumda, bilgisayarın çalışmasını tamamlaması için, kötü algoritma, iyi algoritmanın " 2^{100} bölü 100^2 " katı kadar fazla zaman gerektirir. Bu, 10^{26} kat daha uzun bir süre. Başka deyişle iyi algoritmanın bir saniyede başardığı şeyi, kötü algoritmanın başarması için milyar kere milyar yıldan daha uzun bir süre gerekmektedir.

"İyi" algoritmalar, mutlak en iyi olmasalar da ona yeterince yakın bir "planlama" veya paketleme düzeni bulma bakımından sadece kabul edilebilir bile olsalar, büyük önem taşırlar. Planlama düzeni için sıkça kullanılan iyi algoritmalarından birisi "kritik izlek" denilen yöntemdir. Temel fikir, her adımda bir sonraki adımda yapılacak "en acil" işi seçmeye çalışmaktır. "En acil"den kastedilen ise, yapılmamış işler zincirinde, tahsis edilen sürelerden en fazla süresi kalmış olan zinciri başlatan iştir. Daha ilerde "dar boğazlara" yol açmaya en yatkın olan bu tür işlerdir. Böyle bir kriter, gerçekte bölümün başında vermiş olduğumuz bisiklet montajı örneğinde bizi nihai çözüme götürmektedir. Öte yandan, her zaman nihai çözüme götürme güvencesi de vermez; hatta bazı örneklerde, çok kötü sonuçlara götürür, o ölçüde ki, mutlak en kötü çözümü verdiği bazı örnekler bile oluşturulabilir. Genel olarak, işler arasında zaman sıralaması kısıtlamalarının en az olduğu problemlerde en iyi sonucu verir.

Bidon doldurma bağlamında olanaklı en basit algoritmalarından birisi "ilk sığan" yöntemidir. Bunda önce, bidona konulacak paketleri büyüklüklerine göre sıralarız. Daha sonra paket dizisi boyunca, büyükten başlayarak, sırayla her bidonu alabildiği kadar paketle doldurulup bir sonraki bidona geçeriz; ancak daha sonraki bir aşamada, daha önceki bir bidona sığabilen küçük bir pakete gelindiğinde, bunu, önceki bidona koyarız. Buna örnek olarak, "büyüklükleri" 10, 9, 8, 8, 6, 6, 5, 5, 3 (toplam büyüklük 60) olan paketleri, kapasite-

si 20 olan bidonlara doldurma işini ele alalım. Gereken en az bidon sayısı üç olduğu halde bu ideal minimumla yetinen bir çözümün var olma güvencesi yoktur.

İlk sığan yöntemini uygulayarak, 10 ve 9 paketlerini ilk bidona koyarız. Bundan sonraki paket 8'dir ve ilk bidon için fazla büyüktür, o zaman ikinci bidona gider, bir sonraki 8 de öyle. Birinci 6 paket üçüncü bidona gider ve böylece paket dizisi boyunca ilerleyerek dört bidon gerektiren "çözüm"ü buluruz.

	3	5	
9	8	6	
10	8	6	5
Bidon 1	Bidon 2	Bidon 3	Bidon 4

Fena değil! Acaba 3 bidonlu bir çözüm var mı? Evet, bu problem için var; o da şöyle:

5	3	6
5	8	6
10	9	8
Bidon 1	Bidon 2	Bidon 3

İlk sığan yönteminin olanaklı en iyi düzenlemeyi verdiği olur mu? Yanıt evet'tir. Bunun bir örneği, büyüklükleri 14, 10, 8, 7, 6, 6, 4, 3, 2 (toplam büyüklük yine 60) olan paketleri yine 20'lik bidonlara yerleştirmektir. Bu durumda ilk sığan yöntemi kusursuz doldurmaya yol açmaktadır:

		3
	2	4
6	8	6
14	10	7
Bidon 1	Bidon 2	Bidon 3

Bu yöntem, genellikle, çok sayıda bidon içeren problemlerde en iyi çözümden % 22 kadar fazla bidon gerektirir. Yine de bazı durumlarda, ilk sığan paketlemesinde “bisiklet benzeri” durumlarla sıkıntıya düşülebilir. Örneğin, bu algoritma kullanıldığında bazı paketler probleminden çıkarıldığı halde daha da *fazla* bidon gerektiren örnekler bulunabilir. Bu tür NP-tam problemlerin “iyi” algoritmalarından hoşlanmadıkları ve olanak bulurlarsa onları kızdırmak için işbirliği yaptıkları anlaşılıyor.

NP-tam problemleri için, bilgisayar algoritmaları konusunda, belki de, en büyük ilerleme New Jersey'deki AT&T Bell Laboratuvarları'ndan Narendra Karmarkar tarafından 1984'te açıklanmıştır. Kesin çözüme götürmese de, olanaklı en iyi yaklaşık çözümü bulmak için gereken süreyi önemli ölçüde azaltmaktadır. Ayrıca, daha önceki en iyi algoritmayla (1947'de George Dantzig adında bir matematikçinin geliştirdiği simplex yöntemi) kıyasla, getirdiği iyileştirme, problem büyüdükçe daha da çarpıcı olmaktadır. Bunun sonucunda, Karmarkar'ın aşaması sonrası “ulaşılmaz” gibi görülen bir çok probleme artık ulaşılmaktadır.

Bu çarpıcı gelişme kısa sürede telefon işlerinde uygulamaya konuldu; milyonlarca yerden gelen milyonlarca telefon konuşmalarının rotaları artık bu algoritma yardımıyla saptanmaktadır. Bununla ilgili problemler eski simplex algoritmasının kapasitesinin çok ötesinde karmaşıklık içeriyorlardı. Bu yöntemin telefon şirketine sağladığı parasal tasarruf çok büyüktür. AT&T, Karmarkar'ın algoritmasının farklı uygulamalarının patentini almıştır ve bu başarı Karmarkar'a, şimdiden uluslararası bilim topluluğundan iki önemli ödül getirmiştir. Yöntem hâlâ “cılanmaktadır”; ayrıntıları gidererek daha incelikli hale getirildikçe onun daha da gelişeceği kuşkusuzdur.

XIII. Bölüm

Bir Teneke Kutunun İçinde Kaç Top Sallayabilirsiniz?

Aynı büyüklükte, belirli sayıda birçok topu alıp, küp biçiminde bir teneke kutuya koyun. Onları yavaşça sallayın ve kaptaki düzeylerini ölçün. İşlemi tekrarlayın ve tekrar ölçün, ..., ve tekrar. Eğer sallama tam olarak yapılırsa bu düzeyin hiç değişmediğini hemen fark edersiniz, her ne kadar topların her seferinde kesin olarak aynı düzen içinde olmaları akıl almaz gelse de. Ancak yine de bu, gerçek yaşamda iyi bilinen bir durumdur; yarım kilo kahve içeren bir kutunun hacminin tam belirli olduğuna sadece bakkal değil müşteriler de inanır. Bakkal da, müşteri de bunun nasıl hesaplanacağını bilmezler; ama yolda karşılaştıkları matematikçinin bildiğinden emindirler. Matematikle uğraşanların yeteneklerine duydukları güven övgüye değerdir, ama ne yazık ki yersizdir. Çünkü dünyadaki hiçbir matematikçi de bunun nasıl hesaplanacağını bilmiyor!

Aradığımız, belirli bir hacim içine küreleri en iyi nasıl yerleştireceğimizdir; bu bağlamda en büyük “paketleme oranı”ndan söz ederiz, bu oran topların kutuda kapladıkları nihai hacmin kutunun hacmine oranıdır. Bu orana f dersek toplar arasındaki kaçınılmaz boşluklar da f ’den geriye kalan, $1 - f$ oranıdır, öyle ki bu iki bölümün (dolu ve boş) toplamı 1’dir. Matematikçi için söylediğimiz de, üç boyutlu uzayda kürelerin en yoğun biçimde düzenlenmesi durumunda f sayısının değerinin ne olacağını henüz kimsenin hesaplamayı başaramamış olmasıdır; kürelerin bu durumuna “rasgele yoğun paketleme” diyoruz. Rasgele paketleme için uygun bir matematiksel betimleme bile olmaması daha da üzücü. An-

cak yine de, deneyler, f sayısının var olduğunu, oldukça dakik şekilde hesaplanabilir olduğunu ve yaklaşık $f = 0,64$ olduğunu göstermektedir.

Şimdi, soruyu biraz değiştirdiğimi düşünelim. Topları sallamak yerine onları rasgele değil de tekrarlanan bir düzenle yerleştirsem ne olur? Golf ya da bilardo toplarıyla yapacağınız birkaç dakikalık bir deney üç boyutta, özellikle verimli olan bir düzenli yoğun paketlemenin var olduğuna sizi ikna edecektir. Bu, savaş anıtlarındaki top mermisi yığınlarında veya meyva reyonlarında sıkça görülen düzendir. Önce düz bir yüzey üzerine her biri diğer ikisine değecek şekilde üç küre konulur. Bunların merkezleri bir eşkenar üçgen (kenarları eşit olan, açıları 60° olan üçgen) oluştururlar.

Her yeni küreyi, daha önce konulmuş olan kürelerin en az ikisine değecek şekilde koyarak paketlemeyi sürdürürüz. Bu yolla, bir küre katmanı elde ederiz; bu kürelerin her biri, (vaktimiz veya topumuz veya sabrımız yetmediği için) paketlemeyi durdurduğumuz en “dıştaki” küreler hariç, başka altı küreye değmektedir.

Şimdi bu birinci katın üstüne ikinci bir kat küre yerleştiririz; bu küreleri, ilk kattaki küre üçgenlerinin bıraktıkları çukurluklara koyarız. Bitmiş ikinci kat, birinci katın aynıdır, ancak yatay olarak biraz kaymıştır, yani herhangi iki kürenin merkezleri dikey olarak üst üste değildir. Aynı şekilde, çukurlukların içine yeni küreler koyarak başka katmanlar da inşa ederiz ve sonunda tam bir üç boyutlu, düzenli yığın ortaya çıkar. Buna “ön merkezli kübik” paketleme denir ve biraz cebir ve geometri kullanımı ile bunun paketleme oranı olan f için π bölü 18’in karekökü sayısını buluruz. Bu başı 0,74048... olan irrasyonel bir sayıdır. Öyleyse bu depolamada toplar, var olan boşluğun nerdeyse % 75’ini dolduruyorlar. Bunun, *düzenli* bir paketleme ile elde edilebilecek en yoğun (yani en büyük f değeri) paketleme olduğu bilinmektedir; ispatı da 1831’de Gauss tarafından yapılmıştır.

Bunun rasgele yoğun paketleme için elde edilen deneysel 0,64 değerinden üstünlüğü etkileyicidir; dikkatli planlamanın rasgele bir sallamadan daha başarılı olması da şaşırtıcı

değildir (ancak orijinal problemde $f = 0,74$ 'e varılmasını engelleyen, büyük olasılıkla, kutunun "sınırları"dır; ama bu özenli sıralama için de geçerlidir). Artık, üç boyutta olası en yoğun paketlemenin $f = 0,74048...$ olduğunu kabul etmek nerdeyse dayanılmazdır. Gerçek, matematikçiler dışındaki bilimcilerin bunun doğru olduğunu bildikleri sıkça söylenir. Ancak kesin matematiksel ispat bakımından bu soru yanıtlanmamıştır; çünkü çok zekice oluşturulmuş, düzenli olmayan (yani kendisini düzgün aralıklarla tekrarlamayan) ve daha yoğun bir paketlemeyi başaran bir sistemin var olamayacağı kanıtlanmamıştır. Söz edilen bu yoğun, rasgele paketleme, düzen kendini tekrarlamadığı için rasgeledir, aynı zamanda da şans eseri (yani "sallama" ile) ortaya çıkma olasılığı son derece küçük olduğu için çok özel bir paketlemedir. En iyi matematikçilerin, kuşku ötesinde kanıtlamayı başardıkları tek şey üç boyuttaki küre paketlemesinde, hiçbir paketlemenin yaklaşık $0,7796$ 'dan büyük bir paketleme faktörünün f değerini alamayacağıdır. Ancak bu sonuç, daha verimli, rasgele bir paketleme yapmaya gerçekten uğraşan bir kimseye pek yardımcı değildir, çünkü ispat, bu üst sınıra yaklaşan bir düzenlemenin nasıl yapılacağı konusunda hiçbir ipucu vermiyor.

Bu f için $0,74048$ 'den büyük bir değer öngören özel rasgele paketleme olanağını gerçekten ciddiye almalı mıyız? Bunun tümünden saçma bir düşünce olmadığı en iyi, konumuz bağlamında "öpen sayı" olarak sevgiyle söz edilen sayıya biraz dikkat vermekle görülür. Öpen sayı, merkezi bir küre etrafına birbirlerine ve ortadaki küreye değecek veya öpecek şekilde yerleştirilebilen aynı boyuttaki kürelerin sayısıdır. Daha önce, iki boyutta ön merkezli kübik kafesin ilk katını oluştururken bu sayı altıydı. İki boyutlu öpme problemine yanıt bulmak için golf toplarının veya bilardo toplarının olması gerekli değil, cebinizdeki bozuk paralar da aynı işi yapar. Bir tanesini masanın üstüne koyun ve diğerlerini (aynı boyutta) onun çevresine, hepsi ilk paraya değecek biçimde yerleştirin. Üç boyutta, toplar kullanarak deney yapmak uygulama yönünden bu kadar kolay değildir.

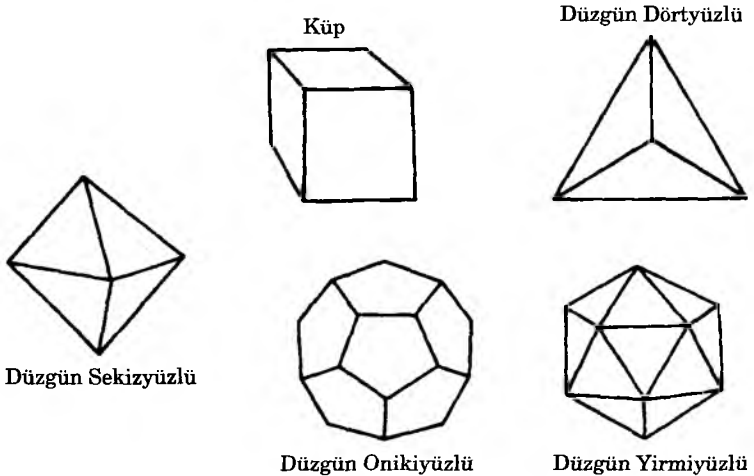
Üç boyutlu öpme probleminin 1649 yılında Sir Isaac Newton ile İskoçyalı bir astronom olan David Gregory arasında ünlü bir çatışmaya konu olması ilginçtir. Newton öpme sayısının 12 olduğunu ileri sürüyordu (ön merkezli kübik düzende bulunan sayı da budur). Halbuki Gregory, kanıtlayamadığı halde, 13'üncü bir kürenin araya sıkıştırılabileceğine inanıyordu. Bunun temelinde yatan düşünce, ön merkezli kübik paketlemede birbirlerine değen kürelerin ortadakinin çevresinde, aradaki açıklıkların hepsi aynı yönde olacak şekilde döndürüldüğünde, ortadaki küreye değebilecek bir fazla küreye, yer açılabileceğine dayanıyordu. Bu yolla açılan aralığın bir fazla kürenin sığmasını sağlayacak kadar büyük olmadığı ancak 1874 yılında kanıtlanabildi. Böylece bu öpme probleminin doğru yanıtı Newton'unkidir; yani 12.

Bu sonuca karşın bir kaç küreyle, ön merkezli kübik paketlemeden daha iyi (paketleme yoğunluğu bakımından) sonuç veren bir küme yapmaya başlamak olanaklıdır. Örneğin, dört küreli, her biri diğer üçüne değen bir tohum ele alalım. Bu dört küre birbirlerine dokunurken merkezleri "düzgün dört yüzlü" olarak bilinen geometrik cismin köşelerinde olacaktır. Bu cisim, birbirinin aynı olan dört üçgen yüzeyden oluşur (yani bu bir çeşit üçgen piramittir); bu yüzeylerin her biri eşit kenarlı ve eşit açılıdır. Her küre, diğer üçüne gerçekten dediğinden, bu, üç boyutta, dört küre için en yoğun düzenleme olmalıdır.

Şimdi bu "dörtüylü" tohuma, birer birer, başka küreler eklediğimizi düşünelim. Aranılan tek şey, bu yolla eklenen her kürenin, başka üç küreye değmesidir. Birbirlerine değen dört bilyardo topu alıp bir beşincisini ilave etmeyi deneyin; bir sorun yoktur (ancak deneyi gerçekten düzenlemek için bir yardımcıya gerek olabilir). Bu çok güzel. Bunu sürdürürsek paketlememin yoğunluğunun maksimum olacağı kesin, daha önce sözünü ettiğimiz gibi en büyük yoğunluk, $f = 0,7796$ 'dır. Öyleyse sorun nedir? Sorun şudur; bunu sürdürdüğünüzde, her zaman bir sonraki topun belirtildiği gibi eklenemeyeceği bir an gelir. "Büyüyen" kümenin belirli

bir aşamasında, yüzey, var olan üç küreye degecek biçimde bir başka küre ilavesine izin vermeyen bir biçim alır. Bu noktaya gelindiğinde felaket başlamıştır, büyük hacimli boşluklar kaçınılmaz olarak ziyan olmaktadır, bu da paketleme yoğunluğunu, çarpıcı biçimde ön merkezli kubik 0,74'ün altına, deneysel sınır olan 0,64 civarına tekrar indirmektedir.

Bizim göstermiş olduğumuz, gerçekte, üç boyutlu uzayın, düzgün dörtyüzlülerle, küplerle (örneğin) doldurulduğu gibi tam olarak doldurulamayacağıdır. Uzayı şekilleri aynı olan blokları yan yana getirerek doldurma, geometrinin çok eski ve zor bir problemidir ve düzgün dörtyüzlü ile karşılaşılan ikilem 2300 yıl öncesine, Aristoteles dönemine uzanır. Onun iddiası (artık onun yanlış olduğunu biliyoruz) var olan düzgün beş cisimden (bunlar bütün kenar uzunlukları ve açıları eşit olan şekillerdir; bkz. Şekil 12) küp ve dörtyüzlü birlikte paketlenliklerinde boşluğun tam olarak dolduğu yolundaydı.



Şekil 12.

Düzgün geometrik cisimlerin keşfedilmesi ve bunların sadece beş tane olduğunun ispatı Eski Yunan'ın en büyük matematiksel başarılarından birisidir. Bunlar Eukleides tarafından ayrıntılarıyla incelenmişlerdir. Bu cisimlerin, bütün maddeleri oluşturan nihai parçacıklar (ya da atomlar) olabileceklerini ilk ileri sürenin Plato olduğu sanılıyor. Aristoteles, Plato'nun argümanının gerçekte bağdaşmadığını, çünkü bu temel üç boyutlu beş şekilden yalnızca ikisinin birleşerek boşluğu, aralık bırakmadan doldurduklarını söyledi. Aristoteles'in düşüncesine göre aralık boşluk demekti ve doğada boşluk olamazdı. Bilmeden, bir kutuya doldurulan toplarla ilgili bir hata yaptığını fark edemedi! Aristoteles bu hatayı yaptıktan sonra ortaya çıkan kargaşanın düzeltilmesi 18 yüzyıl aldı. Ondan sonra bile Aristoteles'in yanlışı, varlığını farklı biçimlerde, uzun zaman sürdürdü, birçok boşluk doldurma probleminde çirkin yüzünü yıllar boyu göstererek kafaları karıştırdı, birçok geometriciyi zor durumda bıraktı.

Peki, küre paketlemede bu bizi nereye götürüyor? Görülen o ki, bir sonraki adımı en verimli yapmaya çalışan (gelecekteki sıkıntıları dikkate almadan) "açgözlü algoritma" bazı bakımlardan, son bölümdeki bisiklet montajı probleminin ilk çözümlerine benzemektedir ve onunla aynı kadere de paylaşıp. Matematikçiler hâlâ (ve yoğun rasgele paketlemeler, sıvıların ve camların atom düzenlemeleri konusunda fiziksel sonuçlara yol açtığı için de bilimciler) küreleri $f = 0,74048$ 'den daha verimli olarak rasgele paketleyecek bilgisayar algoritmaları bulmaya çalışıyorlar ancak, maalesef, henüz başaramadılar. Artık, doğanın, belki de, doğru yanıtı biliyor olabileceğinin kuvvetle olası olduğu düşünülüyor, çünkü doğanın $f = 0,64$ değeri, en gelişmiş bilgisayarla bile elde edebildiğimiz en iyi değer. Ancak yine de bir matematiksel ispatın kesinliği hâlâ yok. Fizikçiler ve kimyacılar yanıtı "biliyorlar" ama matematikçiler kapıyı biraz aralık bırakmak zorundadırlar.

Ayrıca, matematikçiler, doğaları gereği, bundan fazlasını da yapmak istiyorlar. Oyunu neden bir, iki veya üç boyutla sınırlıyoruz? Eğer kendimizi, ona "bakmaya" ayarlayabilirsek,

daha fazla boyutlu bir dünya bizi şaşırtmak ve bizimle oynamak için orada bekliyor. Üç boyutta öpme problemi (yani ortadaki bir topun çevresine, her biri ona değecek şekilde toplar yerleştirmek) zordu, bu iş dördüncü boyutta, en azından pratik bakımdan, daha da sorunludur; çünkü, beşinci, altıncı ve hatta boyut ailesinin daha yüksek üyeleri şöyle dursun, çoğumuz daha böyle bir boyutun varlığıyla uğraşmaktayız.

Matematikçiler bu bakımdan bizden çok daha şanslılar; çünkü bu daha yüksek boyutlar (özellikle de daha yüksek boyutlu küreler), sağ duyumuz için zor olsalar da matematiksel olarak ifade edilmeleri görece daha kolaydır. Örneğin, öğrencilik döneminde biraz cebir ve grafik çizme görmüş olanlar bir çemberin denklemlerinin $x^2 + y^2 = 1$ olduğunu belki anımsayabilirler. Bunun anlamı şudur: Eğer bir grafik kâğıdı alır, y değerlerini bir eksen üstünde ("kuzey" doğrultusu diyelim) ve x değerlerini buna dik olan bir başka eksen üstünde ("doğu" diyelim) işaretlerseniz, o zaman denklemi sağlayan x ve y değerleri;

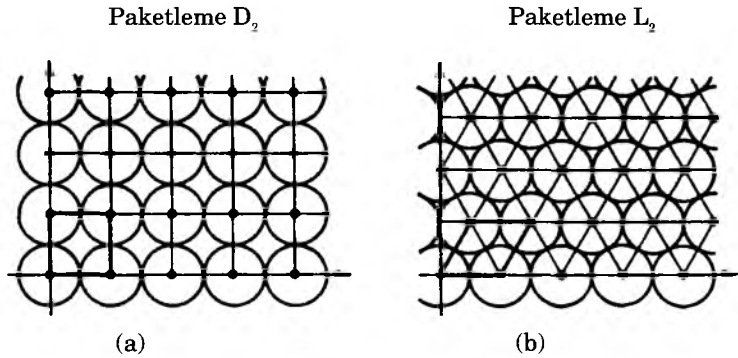
$$x = 1, y = 0; x = \sqrt{(1/2)}, y = \sqrt{(1/2)}; x = 0, y = 1$$

ve bunun gibi sayısız başka çift, merkezi $x = 0, y = 0$ 'da, yarıçapı 1 olan bir çember "çizerler". Eğer bu notasyona yabancı iseniz, kendiniz deneyiniz. Üç boyutta, "yukarı"yı temsil edecek bir başka eksene gerek var. Eğer buna z ekseni dersek, merkezi $x = y = z = 0$ noktasında olan 1 yarıçaplı kürenin denklemi $x^2 + y^2 + z^2 = 1$ 'dir, buna "birim" küre denir. Çoğumuzun üç boyutlu kâğıdı olmadığı için bunu doğrulamak biraz daha zordur, ancak böyle olduğuna güvenin. Ancak burada bir düzen görmeye başladık. Eğer dördüncü bir boyutumuz varsa ve ona w diyorsak, o zaman $w^2 + x^2 + y^2 + z^2 = 1$ denklemiyle tanımlanan nesneye (onu dört boyutlu bir kâğıda çizersek) "dört boyutlu birim küre" demek tutarlı olur. Daha yüksek boyutlara çıkarken sonunda harfler tükenir bu nedenle "eksenleri" $x_1, x_2, x_3, x_4, \dots, x_n, \dots$, olarak adlandırmak daha uygundur, bu yolla eğer yüz boyutlu bir kürenin denklemini yazmak istiyorsak onu kolayca yazabiliriz.

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + \dots + x_{98}^2 + x_{99}^2 + x_{100}^2 = 1$$

Bununla ne yapacağımızı bilmeyebiliriz ancak önemli olan bu değildir. Önemli olan, örneğin, dört ya da yüz boyutta öpme sayısı probleminin artık bir cebir problemine dönüşmüş olmasıdır ve matematikçilerce bulunacak kesin bir yanıtı vardır. Görülüyor ki, paketleme problemleri matematiksel olarak iyice tanımlanmış ifadeler gerektirmektedir ve araştırılacak konulardan birisi de budur. Bu yolla, bizi bölgesel üç boyutlu fiziksel dünyaya kapatmış olan zincirleri kırarak sorgulayıp araştıracağımız çok boyutlu bir Eukleides evrenine açılırız. Artık, n boyutlu uzayda (n istenildiği kadar büyük olabilir) birim küreyi veya topu tanımlayabildiğimize göre, “Hangi boyuttaki Eukleides uzayında birim kürenin hacmi veya yüzeyi en büyüktür?” gibi sorular sorabiliriz. Bunun gerektirdiği matematik, çoğumuzun uzamı dışında olsa da bunun belirli bir yöntemi vardır ve yamt, hacim için $n = 5$, yüzey alanı için $n = 7$ 'dir. Daha büyük boyutlar için hacmin giderek küçülmesi ve n sonsuza yaklaşırken hacmin de sıfıra yaklaşması çok şaşırtıcıdır. Sonsuz boyutlu birim topun hacmi sıfırdır. Bu limit bölgesinde beysbol veya kriket oynamak çok zor olsa gerek!

Çok boyutlu uzayda küreyi yoğun paketleme arayışında ilk önce “kafes paketleme”, yani bir şekilde tekrarlanan bir paketleme düzenini, ele alırsak işimiz biraz kolaylaşır. Öyleyse en kolay paketleme düzeni, her kürenin, merkezi bir “kafes noktasına” gelecek şekilde konulmasıyla sağlanır. İki boyutlu uzayda bu kafes noktaları, m ve n tamsayı olmak üzere, $x = m$, $y = n$ noktalarıdır; bunlar bir dama tahtasındaki karelerin köşe noktalarını oluştururlar. Bu kafese D_2 denilir ve Şekil 13 (a)da gösterilmiştir. Bunun paketleme oranının 0,785398... (tam değeri π bölü 4'tür) olduğunu kolayca hesaplayabiliriz. Ancak iki boyutta, bunun en yoğun paketleme olmadığını biliyoruz. En yoğun paketleme Şekil 13 (b)de görülen, dikkatle düzenlediğimiz portakalların veya top güllerinin tabanını oluşturan düzgün altıgen paketlemesidir. Elementer geometri kullanarak bunun paketleme oranı-



Şekil 13.

mn 0,9069.... civarında olduğu gösterilebilir ve “katlı kafes” olarak bilinir. Örneğimizdeki iki boyutlu katlı kafes L_2 sembolüyle gösterilir. Üç boyutlu katlı kafes olan L_3 , katlarının üst üste konulmasıyla elde edilir; bunu yaparken, üst konulan katın kürelerinin, alttaki katın en derin deliklerinde “yuvalanması”na dikkat edilir. Daha önceki portakal yerleştirme deneyiminden, bunun ön merkezli kübik bir kafes oluşturduğunu biliyoruz. Buna L_3 diyoruz ve daha önce de belirttiğimiz gibi, üç boyutta bilinen en yoğun kafes paketlemesi budur.

Bu katlı kafesler oluşturma yöntemi matematiksel olarak, dört veya daha çok boyuta genişletilebilir. Örneğin L_4 , 4’üncü boyutta L_3 kafeslerinin, en verimli paketleme verecek biçimde yuvalanarak üst üste konulmasıyla elde edilir. Bunu resmetmek nerdeyse olanaksızdır; çünkü beynimiz yalnızca fiziksel deneyimlerimizin üç boyutlu dünyasındaki şeyleri hayal edebilir. Ancak matematiksel olarak bu yöntem kesin belirlidir ve L_4 , L_5 , L_6 , ... vb. gibi bir katlı kafesler dizisi oluşturur. 25’inci boyuta kadar olan katlı kafeslerin özellikleri ayrıntılı olarak incelenmiş bulunmaktadır. 10’a kadar olan n’lerin her biri için bir ve yalnızca bir L_n kafesi olmasına karşın, 14 ve 24 arasındaki n değerleri için durum farklıdır. 11’inci boyutta 2 katlı kafes 12 ve 13’üncü boyutların ikisinde de üçer kafes ve 25’inci boyutta ise tam 23 tane katlı kafes bulunmaktadır.

Bu katlı kafes L_n 'lerden, 8'inci boyuta kadar olanlar için olanaklı en yoğun paketlemenin kafes paketleme olduğu ispatlanmıştır ve bu boyutlarda, daha yoğun bir amorf (kafes olmayan) paketleme bulunamamıştır. Gerçekte katlı kafesler, 32'ye kadar olan her boyut için 10, 11, 12 ve 13 dışında bilinen en yoğun paketlemelerdir (bunların yazıldığı dönemde 48'inci boyuta kadar olan katlı kafes örnekleri hesaplanmış durumdadır. 10, 11, 12, 13 boyut için K paketlemeleri denilen bir başka kafesli paketleme dizilerinin daha yoğun olduğu bilinmektedir; 32'den büyük boyutlar için ise yine bir başka (P paketlemesi) düzen daha iyi sonuç vermektedir. Ancak 8'den büyük olan hiçbir boyutta en iyi olan kafes paketlemenin hangisi olduğu kesin olarak bilinmemektedir, ayrıca katlı olmayan yani amorf bir paketlemenin en yoğun olduğu herhangi boyutun var olup olmadığı saptanamamıştır. 11, 12 ve 13'üncü boyutlarda, şimdiye kadar bulunan bütün kafes paketlemelerden daha yoğun olan amorf paketlemelerin bulunmuş olması ilginçtir.

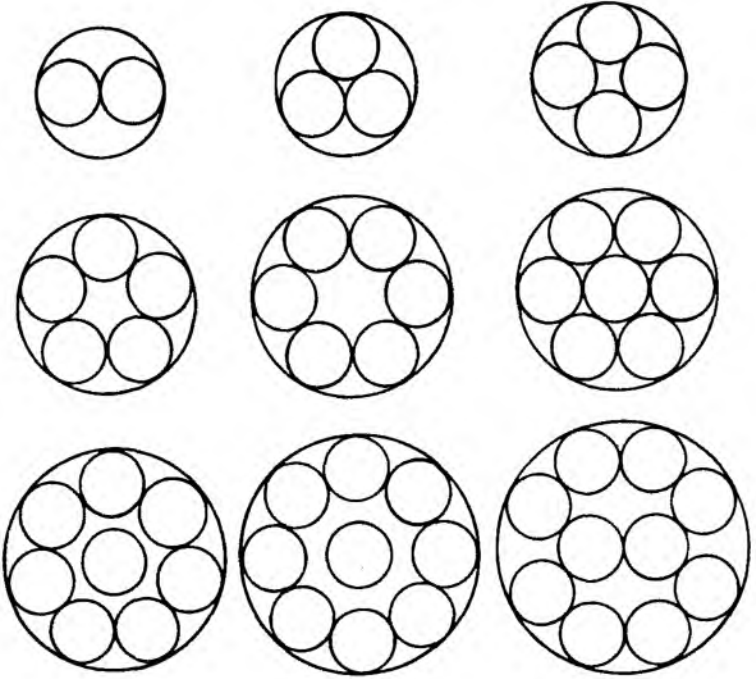
Bell Laboratuvarındaki NJA Sloane'un, bu alanda çalışan bazı araştırmacılarla yaptığı yeni bir çalışma bize büyük boyutların bilinmeyenler okyanusuna kıyasla, bilinen paketleme adalarının boyutu hakkında bir fikir vermektedir. Araştırmacılar 100.000'e kadar olan boyutlarda matematiksel paketlemeler oluşturdular. Bu bilinmeyen sularda, yeni kafes paketlemelerin yoğunluğu, üçüncü boyuttaki paketlemenin daha çok boyuta doğrudan bir genellemesi durumunda elde edilen yoğunluğun en az $10^{40.000}$ katıdır, ancak yine de, genel teoreme göre mümkün olabilecek yoğunluğa kıyasla, 10^{4000} kat daha küçüktür.

24'üncü boyut biraz özel bir konumdadır. Bu boyuttaki katlı kafes paketlemesi olan L_{24} için yoğunluk, teorik olarak bulunan üst limite, 8'den büyük bütün boyutlarda olduğundan çok daha yakındır. (8'inci boyut için en yoğun kafes paketlemesini veren kesin çözüm bilinmektedir). Bu paketleme ilk olarak, Glasgow Üniversitesi'nden John Leech tarafından 1965'te keşfedilmişti. İlk 24 boyut için var olan en yoğun kafes paketleme olduğu nerdeyse kesindir. Bu, ilginç bir sonuçtur, çünkü

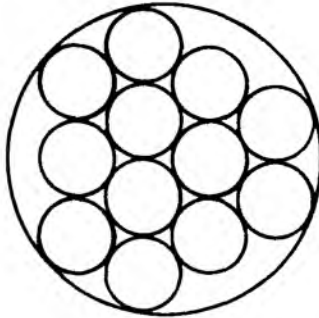
şimdiye kadar öpme problemi sadece farklı dört boyut için çözülebilmiştir; bunlar, önemsiz olan bir ve ikinci boyutlarla (öpme sayıları, sırayla, 2 ve 6'dır) 3'üncü boyut (öpme sayısı, daha önce verilen, 12) ve öpme sayısı 240 olan 8'inci boyuttur.

Ulu yüceliklerden aşağıya inerek, büyük ölçüdeki bilgisizliğimiz yerinde durmaktadır; hâlâ bir kutunun içinde kaç top sallanabileceğini bilmiyoruz, ne üç boyutta ne de daha büyüğünde. Eğer kutunun çevresinin biçimini saptar, küreler yerine de çemberler koyarsak, iki boyutta bile yanıtlanamayan birçok soru bulunuyor. Hepiniz bilardo oyununun, on beş topu bir bilardo masasında üçgen şeklinde kümeleyip bunları bir vuruşla bozarak başladığını sanırım bilirsiniz. Bu, 15 çemberi olanaklı en küçük kenar uzunluğu olan eşit kenarlı üçgen biçimde paketleme problemidir ve bu durumda özel "bilardo masası" paketlemesinin elde edilebilecek en verimli paketleme olduğunu ispatlamak zor değildir. Eğer üçgenden tek bir top çıkarırsanız öbür topların hâlâ birbirlerine kenetlenmiş olduğunu yani hiçbirinin hareket edemediğini görürsünüz. Bu, sanki 14 topu paketleyen en küçük üçgenin, 15 top paketleyen üçgenle aynı boyutta olduğunu kanıtıyor gibi görünüyor ancak bildiğim kadarıyla bunun kesin ispatı yapılmamıştır. Şimdi bir top daha çıkarırsak ne olur? Bunu denerseniz kalan 13 topun artık rahatça hareket edebildiklerini görürsünüz. 13 top alabilen en küçük üçgenin 14 veya 15 top alandan daha küçük olduğu anlaşılıyor. Ancak ne kadar daha küçük? En verimli (yani yoğun) durumda topların düzeni ne şekildedir? Sadece iki boyut ve birkaç değişken içeren bu çok basit durumun bile hâlâ çözülmemiş olması çok şaşırtıcıdır.

Daha genel durum için, birbirinin aynı olan çemberleri, üst üste binmeden, belirli şekillerdeki sınırlar içine paketleme problemi için genel bir çözüm yoktur (sınır bölgesi bir kare veya çember gibi basit olsa bile). Bunlar için sadece bazı özel durumlarda, olanaklı en iyi çözüm verilebilmiştir; az sayıda çember söz konusu olduğunda veya çok özel, çok simetrik bazı durumlarda, örneğin, çemberlerin sayısı 4, 9, 16, 25, 36.... vb. gibi tam kare olduğunda bunları bir kare içine



Şekil 14.

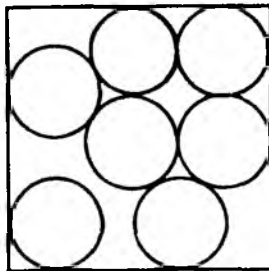


Şekil 15.

paketlemek gibi problemler için olanaklı en iyi çözüm verilebilmiştir. Yanıtların tam olarak bilindiği durumlarda bile sonuçlar sürprizlerle doludur. Örneğin, çemberleri en küçük alanlı dairesel bir sınır içine paketleme probleminde 2 ila 10 çember için olanaklı en iyi çözümler Şekil 14'te gösterilmiştir. Sekiz veya dokuz çember, için en yoğun paketlemelerin, tamamen özgürce hareket edebilen birer çember içerdiğini görüyoruz. Sağ duyu bunu öngörmez ama yine de bu doğrudur! Şekil 15 size, 12 çemberin bir çember içinde en verimli paketlenmesi gibi görünüyor mu? Hayır değildir. Daha iyisini düşünebilir misiniz? Bundan daha iyi olan ve bazı çemberlerin sadece iki komşuya dokunduğu en az bir çözüm var, halbuki Şekil 15'te her çember en az üç komşuya dokunmaktadır; yine bir paradoks var gibi.

Bu oyun üç boyutta da oynanabilir; küreleri en küçük hacimli küresel sınır içine paketlemek. Küre sayısının çok küçük olduğu durumlar dışında, bu problem hakkında bilinenler daha da azdır. Küpleri küpler içine paketlemek ise daha da zordur; tabii eğer yine küplerin sayısı tam küp olan sayılar (8, 27, 64, 125, ... gibi), veya onlara çok yakın sayılar değillerse. Farklı biçimleri farklı sınırlar içine pakitleyerek nerdeyse tükenmez sayıda akıl karıştıran problemler oluşturabiliriz.

Bulunabilen az sayıdaki tam çözümlerin çoğuna sahip olan iki boyuta dönerek, Şekil 16'da, yedi çemberin bir kare içine en verimli biçimde paketlenişine bir göz atalım. Bu da



Şekil 16.

inanılması çok zor olan problemlerden birisidir. Hatta, okuyucunun, arkadaşlarıyla (daha iyisi düşmanlarıyla) bu çemberleri paketleyecek daha iyi bir yol bulamayacakları üzerine gireceği bir çok bahsi kazanacağından eminim. Şu köşede tek başına kalmış çember her halde daha yakınlara sıkıştırılabilir. Ancak inanın, yedi çember için daha iyi bir paketleme bulunamaz ve siz kazanırsınız. Bunun ispatı ilk defa 1965'te verilmiştir.

Son olarak da, paketleme probleminin kareleri, kare şeklinde bir sınır içine paketleme türüne biraz değinelim. Kenar uzunluğu L olan bir karenin içine olabildiğince çok birim kareyi (yani kenar uzunluğu bir olan kare) üst üste gelmeyecek şekilde paketlemek istediğimizi varsayalım. Eğer L bir tamsayı ise (ona N diyelim) yanıt bellidir ve tam paketleme (yani paketleme oranı $f = 1$) kolayca yapılabilir. Eğer L , örneğin, N 'den biraz daha büyükse örneğin, $L = N + (1/10)$ olursa ne olur? Bu durumda ne yapmalıyız? Çözüm için ilk akla gelen, $N = L$ için tam çözüm olan $N \times N$ kareyi doldurup, geriye kalan ince şerit şeklindeki bölgeyi (yaklaşık $N/5$ birim kare) kaçınılmayan israf olarak sineye çekmektir. Gerçekten de eğer N küçük bir sayı ise yapabileceğimiz en iyi şey budur. Ancak genel olarak daha iyi düzenlemeler bulunabilir, ama çoğu problem için en iyi düzenlemenin ne olduğu kesin olarak bilinmemektedir.

Bu sonuca varmamıza izin veren şudur: N 'nin büyük değerleri için $N/5$ 'ten çok daha küçük bir alanın israf edildiği paketlemelerin var olduğu ispatlanmıştır. Olanaklı en küçük kullanılmayan alanı N 'nin bir fonksiyonu olarak ifade etmeyi bilmiyoruz; ancak " N^2 artı kaçınılmayan israf" düzeninin N 'nin 80'den büyük değerleri için "en iyi" çözüm olmadığı ve N 'nin 30 gibi küçük değerleri için de, en iyi olabileceği yukardaki ispatla saptanmıştır. Diğer yandan, bir fazla kareyi "sıkıştırmak" için ne yapmamız gerektiği konusunda hiçbir ipucu yoktur. Daha büyük sayılar için problemin boyutunu kavramak için 10^{10} birim karenin kenar uzunluğu $L = 10^5$ olan bir büyük kare içine güzelce yerleştirildiğini düşünün. Tam olarak yerleştirilebilirler ve pa-

ketleme oranı, $f = 1$ 'dir. Şimdi büyük karenin kenar uzunluğunu bir birim uzunluğun *yüzde biri* kadar artırın, yani $L = 10^5 + 0,01$ olsun. Bu niceliğin önemli olmayacak kadar küçük olduğunu düşünüyorsunuz. Ancak bu kaçınılamaz, nerdeyse görünmez olan ince şerit şeklindeki kullanılmayan alan, 2000 birim karedir ve ayrıca 10^{10} birim karenin yerleri akıllıca değiştirilerek, en az 520 (belki, daha da çok) birim kare daha eklenebilmektedir. Bunun gerçekten, en iyi nasıl yapılacağı ise yine hiç bilinmemektedir.

XIV. Bölüm

Ara Boyutlar

Matematik (özellikle geometriyle ilgili olduğunda), 20. yüzyıla gelene kadar, ifadelerinde Euclides döneminden beri süregelen idealist kavramlar kullanıyordu. Eğriler (arada, keskin bir dönemeç dışında) düzgündü ve klasik bir anlamda “terbiyeli” fonksiyonlarla matematiksel olarak ifade edilebiliyorlardı. Eğrinin her noktasındaki eğimi ve eğrilik derecesi sorulabilirdi ve makul yanıtlar alınabilirdi. İçinde yaşadığımızı düşündüğümüz düzenli dünyanın nerdeyse bütün özelliklerinin bu “düzgün” eğrilerle ifade edilebileceği kabul edilmişti. Bunlara “analitik” deniliyordu ve çok özellerdi. Konunun uzmanı olmayanlar için bunun anlamı aşağıda aktaracağım uçaksavar silahlarla ilgili öyküyle çok daha iyi açıklanabilir.

Sıcaklığa duyarlı roketler öncesinde uçakları yerde konuşturulmuş silahlarla düşürmek bir sürü matematiksel bilgi gerektiriyordu. Problem şuydu: Hedef hareket halinde olduğu için hedef alınacak nokta, mermi oraya vardığında uçağın bulunacağı nokta olmalıydı. Eğer doğrudan uçağa nişan alsaydınız uçağı vuramazdınız çünkü, mermi oraya vardığında uçak gitmiş olurdu. Bu nedenle bir ayarlama yapmak zorunluydu. Eğer uçağın hızı biliniyorsa (veya güvenilir biçimde hesaplanabiliyorsa) o zaman söz edilen sorunu dikkate alacak bir “düzeltme” yapılabilirdi. Sorun nerdeyse halledilmişti; “büyük farkla ıskalamak” yerine “az farkla ıskalanıyordu”, ama yine de ıskalanıyordu. Yanlış olan neydi?

Ortaya yeni bir problem çıktı: Söz konusu olan uçaklar yükselmekte olan uçaklardı bu nedenle de hızları sabit de-

ğildi. Başka deyişle, hızları artıyordu. Ancak, en azından ilke olarak, ivmeleri de (yani hızın değişme hızı) hesaplanabilir ve bir düzeltme daha yapılabilirdi. Ama hayır! İvme de sabit değildi ve yeni bir düzeltmeye gerek vardı. Uçaksavar kullananlar için bütün bunlar çok sinir bozucuydu ve sonunda hesaplamayı bir yana bıraktılar; yine de insan üstü bir varlık bu düzeltme sürecini durmadan yaparsa, en sonunda bir isabet kaydedileceğine olan (hiç olmazsa teorik olarak) inançları sürüyordu. Gerçekler göz önüne alındığında, hesaplama becerilerinin sınırlı olmasına üzülmeleri yersizdi; çünkü düzeltmeler sonsuza dek sürdürülse bile bir yararı olamazdı. Örneğin, eğer merminin ateşlendiği anda pilot öğle yemeğini unuttuğunu fark edip dönmeğe karar verirse hedef yine kaçırılırdı.

Gerçek neden şudur: Uçağın geçmişteki hareketinin bütün ayrıntıları ile bilinmesi bile, onun geleceğin *herhangi* bir anındaki konumunu saptamak için yeterli değildir.

Halbuki matematikteki bütün düzgün (yani analitik) eğrilerde bu özellik vardır; eğrinin bir bölümünün *tam* olarak bilinmesi, kalanını da kesin biçimde belirler. Bu nedenle uçağın konumunun zamana göre fonksiyonunun analitik olmadığı sonucuna varırız. Matematik, analitik fonksiyonlarla doludur (çünkü yazılımaları ve hesaplanmaları “kolay”dır) ama gerçek dünyada onlara hemen hemen hiç rastlanmaz. Doğa böyle bir betimlemeye uyacak ölçüde basit ve düzenli değildir. Bulutlar küresel, dağlar konik, göller de eliptik değildirler, yıldırım düz doğru üstünde gitmez. Gerçekte, doğadaki nesnelere ne kadar yakından bakarsak, onların çoğunun “tam anlamda” düzgünlükten yoksun olduklarını o kadar daha iyi fark ederiz. Şu anlamda ki, onlara ne kadar yaklaşırsak, onların giderek küçülen düzeylerde ama hep aynı ölçüde düzensiz olduklarını görürüz. Bunun belki de en bilinen örneği, ünlü Fransız Matematikçi Benoit Mandelbrot tarafından verilmiş örnektir. Boyutlar arası düzensizlikler konusundaki araştırmalara öncülük etmiş ve 1967’de “İngiltere kıyılarının uzunluğu nedir?” başlıklı klasik bir makale yayınlamıştır.

Bir uzay yolcusunun Dünya'ya, Britanya Adaları doğrultusunda yaklaştığını düşünün, yaklaştıkça kıyı şeridinde daha fazla ayrıntı görebilecektir. Uzaktan görünmeyen daha küçük koylar ve burunlar giderek belirginleşecek, daha da yakınlaşınca bu koyların ve burunların da kendilerine özgü yapıları olduğu görülecektir. Kaya şekillerinin ayrıntıları için metreler gerekirken çakıtaşlarının yerleri santimetrelerle ifade edilecektir. Sonunda, eğer amacınız insan çıldırtmak ise, kum taneciklerini de teker teker ölçebilirsiniz; suyun hareketini durdurabildiğinizi varsayıyoruz.

Eğer İngiltere kıyılarının uzunluğu için yapılan "en iyi" tahmin de tuhaf bir olgu göze çarpar: Bu iş içinde kullanılan cetvel ne kadar küçük ölçekli ise tahmin edilen uzunluk da o ölçüde artar. Bu yetmezmiş gibi, daha da ürkütücü bir başka şey saptanmıştır: Cetvel küçüldükçe bu ölçümlerin yaklaştığı bir limit değer bulmak istenirse bu limitin sınırsızca arttığı (veya başka deyişle sonsuz olduğu) görülmüştür. Bu anlamda, İngiltere kıyı şeridinin, uzunluğu sonsuz hassasiyetle ölçüldüğünde sınırsızdır, ya da isterseniz, ileri süreceğiniz her uzunluktan daha uzundur.

Gerçekte, Dr. Mandelbrot bu konuya el atmadan önce de bu gözlem yapılmıştı. Uzunluk birimi (L diyelim) küçüldükçe kıyı şeridinin uzunluğu sadece sınırsızca artmakla yetinmiyor, kuvvet yasası şeklinde artıyordu; yani, n negatif bir sayı olmak üzere, L^n gibi artıyordu. Örneğin, eğer $n = -1/2$ ise, ölçü birimi her yarılandığında, kıyı uzunluğu $1/2$ 'nin $-1/2$ 'nci kuvveti kadar artacaktır, bu sayı (kesirler ve kuvvetlerle ilgili cebir kurallarını hatırlayanlar bilecektir) 2 'nin kare köküne eşittir. Günümüzde cebirden çok elektronik hesap makinelerine güvenenler, $y = 0,5$, $x = -0,5$ alarak y^x tuşuna basarlarsa karekök 2 'ye eşit olan $1,4142...$ değerini okuyabilirler. Dünyanın birçok kıyı şeridi ve kara sınırları için bu n sayısı dikkatle hesaplanmış bulunmaktadır; n 'nin değeri yaklaşık $-0,2$ olarak bulunmuştur; ancak farklı ülkeler için farklı (ama tekrarlanabilir gibi görünen) değerler elde edilmiştir.

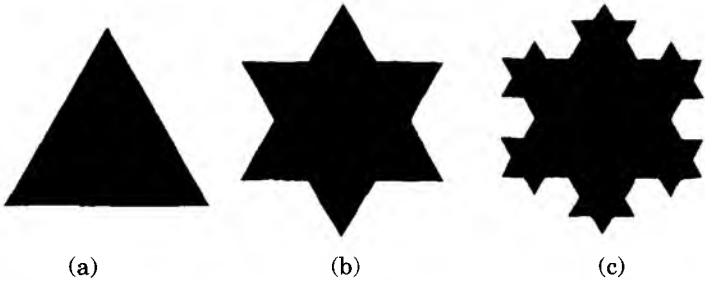
Bu kıyı şeridi veya sınır boyu, analitik anlamda düzgün olursa n 'nin sıfır olmasını bekleyebiliriz. Bu durumda, ölçü bi-

rimi uzunluğu küçüldükçe uzunluklar da uygun bir sonlu sayıya yaklaşır. Bir çemberin çevresi gibi tek boyutlu bir çizgiden de beklenen budur. Mandelbrot'un yaptığı, n kuvveti ve D ile göstereceğimiz boyut kavramı arasında $1 - D = n$ şeklinde bir bağıntı kurmaktır. Bir boyutlu Euclides doğruları için $D = 1$ alırsak, beklendiği gibi $n = 0$ 'dır. Ancak sınırlar ve kıyılar için, n 'nin negatif değerleriyle, D için 1,23 ve 1,18 gibi değerler bulunur. Bu da ilk defa kesirli boyut kavramını gündeme getirir.

Kesirli boyutlar formal olarak daha önce, 1919'da filozof yazar ve (daha sonra da) matematikçi olan Felix Hausdorff tarafından kullanılmıştı ancak, onun ele aldığı nesneler sıradışı birkaç geometricinin karmaşık beyinlerinin oldukça patolojik ürünleriydi. Mandelbrot ise dünyanın bu tür şeylerle dolu olduğunu, şimdiye kadar bilinmeyen "ara boyutlar" ülkesinde hemen hemen bütün gerçek dünya objelerini bulmanın olası olduğunu iddia ediyordu. Günümüzde "fraktal" boyut denilen D sayısı bu objeler hakkında kesin bir şeyler ölçmektedir ve $D = 1$ ve $D = 2$ limit değerleri de bir ve iki boyutlu klasik görünümle tutarlıdır. Dr. Mandelbrot, D değeri tamsayı olmayan bütün şekilleri betimlemek için, Latince'de düzgün olmayan anlamına gelen "fractus"tan türettiği fraktallar sözcüğünü kullanmıştır. Fraktallar, $D = 1$ ve $D = 2$ arasındaki boyutlarla sınırlı olmasa da, biz kolaylık için, önce bu bölgeyi ele alacağız. Bu arada Büyük Britanya'nın Batı kıyısının fraktal boyutunun yaklaşık 1,25 olduğunu da belirtelim.

Büyük Britanya'nın Batı kıyısının fraktal boyutu, deneysel ölçümler gerektirdiği için, sadece yaklaşık olarak bilinmektedir. Fraktallarla ilgili en kesin kavramlar, fraktallara yol açan basit geometrik yöntemler bulgulamakla elde edilirler. Bunların belki de en basit olanı ve fraktal kavramını göstermek için en çok kullanılanı Koch kar tanecığı denilen şekildir. Bu ilginç şekli elde etmek için bir eşkenar üçgen alırız (Şekil 17 (a)). Bunun her kenarında üç eşit aralık işaretlenir ve ortadaki bölümler çıkarılır. Buralara, kenarları çıkarılan uzunluklar kadar olan daha küçük eşkenar üçgenlerin iki kenarı, konulur; elde edilen, Şekil 17 (b)de görülen "Süleyman'ın Mührü"dür.

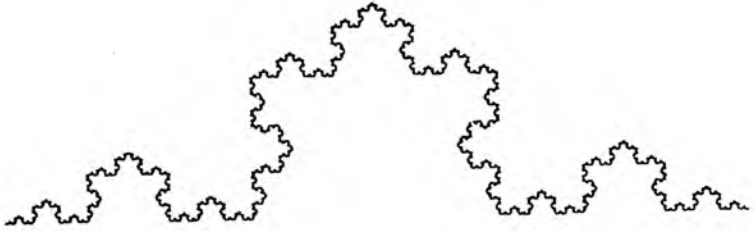
Şekil 17 a, b, c bu işlem sonucunda ilk üçgenin her kenarının yerine bir kırık çizgi gelmiştir ve uzunluğu ilk kenar uzunluğunun $4/3$ katı olmuştur. Bu nedenle, çevrenin yeni uzunluğu eskisinin $4/3$ katı olmuştur ve düz olan kenar uzunluğu da eskisinin $1/3$ katıdır.



Şekil 17.

İlk çevre uzunluğuna P_0 , kenar uzunluğunda L_0 dersek, yeni çevre $P_1 = (4/3) P_0$ ve yeni kenar uzunluğu $L_1 = (1/3) L_0$ olur. Şimdi yeni kenarları kullanarak aynı işlemi tekrarlırsak, daha da kertikli olan ikinci bir şekil elde ederiz (Şekil 17 (c)). Burada da, yeni kenar uzunluğu eskisinin $1/3$ katı ($L_2 = 1/3 L_1$), çevre ise yine $4/3$ katıdır ($P_2 = (4/3) P_1$). Görülüyor ki bu süreç, ilke olarak, *ad infinitum* tekrarlanabilir; ancak oluşan kar tanesini çizmek de aynı ölçüde zorlaşır. Beşinci aşamadan sonra (yani, P_5, L_5) taneciğin üst bölümü Şekil 18’de gösterilmiştir. Sonunda çıkıntılar o kadar artar ve küçülür ki artık çizilemezler ve sonsuz limite gidildiğinde “eğri”nin her noktasında bir çıkıntı yer alır. Eğrinin sürekli veya düzgün hiçbir bölümü yoktur; bir “fraktal” olmuştur.

Bu fraktalın, limit durumuna yaklaşıırken aldığı şekli çizemiyorsak da, onun hakkında çok özel bir şey biliyoruz. Onun yapılanma sürecinin her aşamasında, ne kadar ilerlemiş olsak da (yani milyonuncu, milyarınca veya trilyonuncu adımda) $(n+1)$ ’inci aşamadaki çevre uzunluğu P_{n+1} , her zaman, bir önceki aşamadaki çevre uzunluğu P_n ’nin $4/3$ katı,



Şekil 18.

$(n+1)$ 'inci aşamadaki kenar uzunluğu L_{n+1} de bir önceki adımdaki L_n 'nin $1/3$ katı olacaktır. Bu nedenle, n 'nin her değeri için $P_{n+1} = 4/3 P_n$ ve $L_{n+1} = 1/3 L_n$ denklemlerini yazabiliriz. Mandelbrot'un boyut D tanımına göre, P_n 'yi, aynı zamanda, bir sabit sayı çarpı $(L_n)^{1-D}$ ve P_{n+1} 'i de aynı sabit sayı çarpı $(L_{n+1})^{1-D}$ olarak yazabiliriz. Bu son iki denklemden birini öbürü ile bölerek "Mandelbrot denklemi" olan

$$(P_{n+1} / P_n) = (L_{n+1} / L_n)^{1-D}$$

elde edilir. Ancak her n için,

$$P_{n+1} / P_n = 4/3 \text{ ve } L_{n+1} / L_n = 1/3$$

olduğundan, yukardaki denklem bize,

$$4/3 = (1/3)^{1-D}$$

eşitliğini verir. Bu denklemin çözümü, logaritmik olarak

$$D = \log(4) / \log(3)$$

şeklinde yazılabilir.

Eğer log tuşu olan bir hesap makineniz varsa D 'nin 1,261859...'a eşit olduğunu doğrulayabilirsiniz. Bunu, Büyük Britanya'nın Batı kıyısının 1,25 olan boyutuyla kıyaslarsak, anlaşılan odur ki, Koch'un kar taneciği bu kıyıdan

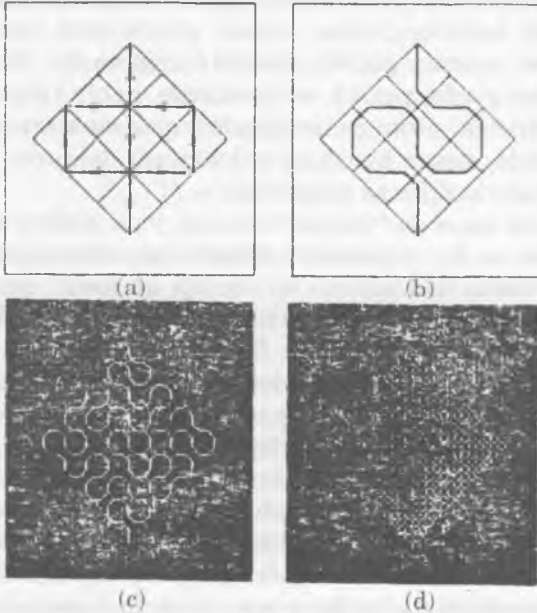
birazcık daha “çıkıntılıdır”. Ancak çıkıntılı sözcüğü bu farkı ifade etmeğe yeterli değildir; çünkü her ikisi de, sözcüğün normal anlamıyla, sonsuz sayıda çıkıntılıdır, fraktal boyut kavramının önemi de tam bu durumda ortaya çıkmaktadır. Sonsuz çıkıntılı bu eğrilerin kesin tanımlanmış bir özelliğini, onları niceliksel olarak kıyaslamamızı sağlayacak biçimde ifade etmektedir.

Şekil 17 ve 18’deki şekillerin sonsuz çıkıntılı limiti olarak elde edilen eğri, ilk olarak 1904’te Alman matematikçi Helge van Koch tarafından, incelenmişti. Bu eğri, özellikleri o dönemin matematiğiyle tanımlanamayan, sonsuz uzunluktaki sürekli eğriler için kesin bir örnekti. Daha sonraki on veya yirmi yıl içinde bu türden birçok başka eğri bulundu ve tartışıldı. Ancak “matematik kurumu” ve akademik toplumun çoğunluğu onları büyük bir kuşkuyla karşıladı ve “canavarlar galerisi”, “patolojik” hatta “psikopat” olarak betimlediler. Onları, gerçek dünya ile hiçbir ilgisi olmayan şeytani çizimler olarak değerlendirdiler. Ancak günümüzde bunun neredeyse tam tersinin geçerli olduğu anlaşılmıştır. Fraktallar doğada her yerde, yaprak ve çiçeklerde, nehir yataklarında, göl kıyılarında, atom çekirdiğindeki parçacıkların dağınık izleklerinde, uçsuz bucaksız gökyüzünü dolduran galaksi kümelerinde karşımıza çıkıyorlar.

Koch kar taneciği “düzenli” denilen, yani çizilme kuralları belirli olan ve hiç değişmeden tekrarlanan fraktallara bir örnektir. Düzenli fraktalların bir özelliği de şudur: Eğrinin bir bölümünü ne kadar büyütürseniz büyütün, eğri *tam* olarak aynı şekilde görünmeyi sürdürür. Bu özelliğe “tam kendi benzeri” diyoruz. Kıyı şeritleri gibi şeylerin bu ölçüde bir hassasiyetle kendi benzerleri olmadıkları açıktır. Sadece istatistiksel bir anlamda bu özelliğe sahiptirler. Böyle eğriler için fraktal boyutları tanımlamamıza olanak sağlayan da onların, ortalama olarak, *kendi benzerleri olmalarıdır*. Bu nedenle, daha az kesin bir biçimde düzenli olan bu fraktallara “rasgele fraktallar” diyoruz. Bunlar büyütüldüklerinde ayrıntılarda rasgele farklılıklar görünse de, bunların dışında ve ötesinde, kendine benzerliği sürdüren ortalama bir özellik (yani fraktal boyut) içerirler.

Düzenli başka fraktallar, ilke olarak, kolayca tanımlanabilir ve çizilebilirler. Ancak uygulamada çizilmeleri çok zordur. Yine de bilgisayar çizim teknikleriyle onların, ilk tekrarlanma aşamalarının birçoğunu kapsayan resimlerini elde edebiliyoruz. $D = 1$ ve $D = 2$ arasında olan daha büyük boyutlu fraktalları oluşturmak için, doğru parçasını uzatma aşamalarında uygulanacak çizimleri daha karmaşık bir biçimde tanımlamak yeterlidir. Örneğin, bir kare ile başlayıp, her kenarının ortasındaki $1/3$ 'lük bölümde bir üçgen yükseltmek yerine bir başka kare yükseltebiliriz. Büyümesinin her aşamasında bu eğri, çevresinin uzunluğunu $5/3$ kat yapar ve kar tanecığı örneğindeki benzer hesaplamalar yaparak $\log(5) / \log(3) = 1,46497\dots$ veya yaklaşık $3/2$ değerinde bir kesirli boyut elde ederiz.

Artık sıra $D = 2$ 'ye yavaş yavaş yaklaşıp yaklaşamayacağımız konusunu incelemeye gelmiştir. Eğer fraktal boyutlar



Şekil 19.

kavramının gerçekten bir anlamı varsa iki boyutlu alanın tümünü dolduran bir eğri var olmalıdır. Bu boşluk dolduran eğrilerin en ünlüsü ilk olarak 1890'da İtalyan matematikçi Guiseppe Peano'nun önerdiği eğridir. Onun nasıl oluşturulduğu Şekil 19'da gösterilmiştir. Süreç bir kare ve onun dört kenarından her birini üç eşit parçaya bölmekle başlıyor. Bunu, karenin, Şekil 19 (a)da gösterildiği gibi, daha küçük dokuz kareye bölünmesi olarak da düşünebiliriz. Peano eğrisi, aşağıdan yukarıya bir düz köşegen çizerek başlıyor, bunu daha sonra, şekilde gösterilen okları izleyerek, küçük karelerin hepsinin köşegenleri boyunca giden sürekli bir doğru ile değiştiriyoruz. Bu eğrinin şeklini "görmeye" yardımcı olmak için, genellikle, Şekil 19 (b)de görüldüğü gibi, dik açılı dönme noktalarında köşeleri kesme uygulamasına gidilir. Formal gelişmede bunu dikkate almazsak, dokuz küçük kareden her birinin düz doğrusal bir köşegeni bulunduğunu ve bunların başlangıçtaki kareye benzediklerini görürüz. Bu nedenle küçük karelerden her birini daha da küçük dokuz kareye ayırarak Peano fraktalını, ikinci aşamada $9^2 = 81$ (köşeleri kesilmiş) doğru parçasından oluşacak şekilde çizmeye devam ederiz (Şekil 19 (c)). Bundan sonra, üçüncü aşamada (Şekil 19 (d)), $9^3 = 729$ doğru parçası olmalıdır ve böylece *ad infinitum* ilerler.

Bu eğrinin çizimini sonsuz sayıda doğru parçası olana kadar sürdürürsek, sonuçta elde edilen eğrinin ilk karenin tüm alanını dolduracağı oldukça aşikâr olsa gerek. Eğri gerçekten bir $D = 2$ fraktalı gibi görünüyor. Bu, Mandelbrot'un fraktal boyut tanımlamasına uymakta mıdır? Eğrinin oluşma sürecinin ilk aşamalarında kenar uzunluğu L her adımda 3 kat azalmaktadır, çevre uzunluğu ise üç kat artmaktadır. $P_{n+1} / P_n = 3$ ve $L_{n+1} / L_n = 1/3$ bağlantılarını Mendelbrot denkleminde yerine koyarsak D için aşağıdaki sayısal ilişkiyi elde ederiz:

$$3 = (1/3)^{1-D}$$

Logaritmalara hakkında fazla bir şey bilmeseniz bile, I. Bölüm'den negatif kuvveti (örneğin, $3^{-x} = (1/3)^x$) hatırlamanız,

fiziksel olarak da tutarlı olan $D = 2$ (yani, $x = -1$) sonucunu doğrulamak için yeterlidir. Demek ki, formal tanımlama, bizim daha basit tamsayı boyutlar kavramlarımızla da tutarlıdır. Başka $D = 2$ fraktallar icad etmek zor değildir. Bu tür ilk “şeytan eğrisi”nin mucidinin anısına $D = 2$ fraktallarına artık topluca Peano eğrileri denilmektedir.

Fraktal boyutlar sadece $D = 1$ ve $D = 2$ arasına özgü değildir. Boyutları 1’den küçük olan fraktalları düşünmek özellikle kolaydır. Bunlar düzenli bir biçimde kolayca hazırlanabilirler. Örneğin bir düz doğru parçası ile başlar ve onu üç eşit parçaya ayırırsak, orta bölümü çıkarmayı düşünebiliriz. Her birinin uzunluğu ilk doğrusunun üçte biri kadar olan, aralarındaki aralığın uzunluğu da yine bu uzunluk kadar olan iki doğru parçası kalmıştır. Yeni “kenar uzunluğu” ilk uzunluğun $1/3$ katıdır, yeni “çevre” uzunluğu ise ilk çevrenin $2/3$ katıdır. Bu daha küçük doğru parçalarının her biri, aynı şekilde bölünerek bu işlem sonsuza kadar sürdürülebilir. Sonuçta, sonsuz sayıda, sonsuz küçük doğru parçalarından oluşan, bir tür gri (eğer ilk doğru siyah ise) bir doğru parçası kalır. Bu tuhaf görünümlü bir nesnedir, ancak “Mandelbrot’un formülünü kullanarak boyutunu kolayca saptayabiliriz. Oluşum sürecinde her n için $L_{n+1} = 1/3 L_n$ ve $P_{n+1} = (2/3) P_n$ olduğunu hatırlayarak,

$$2/3 = (1/3)^{1-D}$$

yazarız. Denklemin çözümü $D = \log(2) / \log(3) = 0,6309...$ ’dur. Farklı ayrıntıları olan bu tür “kesip çıkarma” işlemleriyle, D değeri sıfırla bir arasında değişen, başka fraktallar da bulabiliriz. Son fraktal doğru, ne kadar daha az gri ise, boyut da o ölçüde küçüktür; sonunda D sıfıra yaklaşırken doğru da gözden kaybolur. Bu türden ilginç bir fiziksel model ağaçların yapısında da görülür. Her ağaç dalının daha küçük iki dala ayrılması, bu dallarında tekrar daha küçük iki dala ayrılmasından oluşan sürekli dallara ayrılma süreci sonunda ağaç Mandelbrot’un “fraktal şemsiye” dediği bir genel görünüm kazanır.

Fraktal boyut kavramı ikiden büyük değerlere de uzatılabilir. Örneğin, dümdüz bir alüminyum folyo, iki boyutlu bir yüzeye çok iyi bir yaklaşımdır. Ancak onu buruşturursanız, onun iki artı bir şey boyutunda bir fraktala dönüştürürsünüz. Bu fraktal boyutun kesin değeri folyonun ne kadar kırıkkı olduğuna bağlıdır ve fraktal kar taneciği eğrisi için kullanılan yöntemle tümüyle benzer bir yöntemle bunu saptayabiliriz (en azından ilke olarak). Aradaki tek fark, bu örnekte, cetvelle uzunluk ölçmek yerine, sürekli küçülen “ölçü plakaları”yla alan ölçüyor olmamızdır.

Boyutu “iki ve az bir şey” olan düzenli bir fraktal için, örneğin kare şeklinde bir alanla başlayabiliriz; bunu Peano eğrisinde yaptığımız gibi daha küçük dokuz kareye böleriz. Ancak burada, ortadaki kareyi yukarıya, üçüncü boyuta çekerek bir “küp” oluşturacağız. Bunun sonucunda ortaya çıkan obje, kare kafalı bir insan için yapılmış kare bir şapka görünümünde olacaktır ve birbirlerine eşit olan ve dokuzu yatay, dördü düşey on üç kare içerecektir. Şimdi bu karelerden her biri, ikinci aşamanın başladığı kareler gibi ele alınarak onların her birisinde kare “şapkalar” oluşturulabilir. Bu sürecin sonsuza kadar sürdürülebileceği aşikârdır. Her aşamada yüzey alanı $13/9$ kat arttığından sonuçta oluşan yüzey alanı sonsuzdur ve bu da boyutun ikiden büyük olduğuna bir işarettir. Bu kırıkkı nesnenin fraktal boyutunun $\log(13) / \log(3) = 2,3347\dots$ olduğunun doğrulanmasını size bırakıyorum.

Boyutu ikiden büyük olan rasgele fraktallara çok yaklaşık olan yüzeyler bilgisayar grafikleri ve rasgele sayı üreticileriyle oluşturulabilirler. Bu yolla elde edilen sıra dağlar benzeri şekiller istatistiki olarak kendi benzerleridirler ve çok az bilgisayar süresi kullansalar bile çok gerçekçi görünen resimlere yol açarlar. Bunlar bilgisayar sanatında matematiğin gücünü kanıtlamaya başlamışlardır ve resimlerin yapısında matematiksel modellerin kullanımı yoluyla çok etkileyici, yeni sanatsal kavramların geliştirilebileceğine işaret etmektedirler.

Bilgisayarlarda model kullanma yöntemi formal olarak üçten daha büyük boyutlu fraktallara da kolayca uygulan-

bilmektedir. Bu yapıları görsel olarak tam algılayamasak bile dört boyutlu bu objelerin üç boyutlu izdüşümlerini (veya dilimlerini) elde etme olanağımız vardır ve bunlar objeyi bizim görüş alanımıza getirmekte yardımcı olabiliyorlar. Ancak yine de onları yeterince algılamış olmuyoruz; hiç küp görmemiş bir insanın bir küpün iki boyutlu bir dizi resmine bakarak onun özelliklerini tam olarak algılayamayacağı gibi. Fakat resimlerle gösterme bakımından yapabileceğimiz en iyi şeyin bu olduğu anlaşıyor.

Fraktallar konusundaki çalışmalar bilimin birçok dalında yararlı fikirlere de kaynak sağlamaktadır. Süngerler, bulut yapılanmaları, nehir havzaları ve duman zerreciklerinin ortak yanları yok gibidir, ancak son zamanlarda bunların hepsi bilimsel yayınlarda fraktallarla ilgili olarak yer almışlardır. Gelecekte fraktalların bilimin birçok farklı alanında etkin olacakları kesin görünmektedir; özellikle biyoloji, coğrafya ve ekonomide. Birçok araştırma laboratuvarı temel araştırma bütçelerinin dikkate değer bir bölümünü fraktal sistemlere ayırmaktadır ve tümüyle bu konunun tartışıldığı araştırma toplantıları düzenlenmektedir. Yine de bütün bu girişimler yalnızca bir başlangıçtır; fraktalların boyutsal ayrıcalıkları dışında temel hiçbir özelliği henüz kavranmış değildir. Ünlü bir bilimcinin deyişiyle, fraktallar fiziği, hâlâ doğmayı bekleyen bir konudur. Uygulamada şimdilik, yalnızca bilgisayar grafikleri konusunda önemli etkinlikleri olmuştur. Özellikle de *Yıldız Savaşları* türü filimlerin “efektleri”ni yaratmak için giderek artan biçimde fraktallar kullanılmaktadır.

XV. Bölüm

Kaosa Giden Yol

Matematiğin dünyası bir çok insan için anlaşılmasız olduğu halde, genel olarak onun düzenli bir alan olduğu düşünülür. Büyük bir dikkatle, çok kesin olan sorular sorulur ve kesin yanıtlar aranır ve çoğu kez de bulunur. Matematiksel düşüncenin daha soyut derinliklerinde pusuya yatmış bekleyen, huzursuzluk verici bir mantıksal sorun olduğu doğrudur, ancak cebimizdeki hesap makinesinde taşıdığımız türden olan aritmetik bir anlamda kolaydır. Her sorunun “düzenli” bir yanıtı vardır. I. Bölüm’de karşılaştığımız, tuşuna ilk bastığımızda makinemizi şaşırtan 0^0 sayısı bile biraz düşündürdükten sonra teslim olmuştur.

Cep hesap makineleri dünyasında korkulacak bir şey olmadığını biliyoruz. Aritmetik çok kesin bir bilim dalıdır ve hesap makinemiz (bazılarımız için de bilgisayarlar) de bir dosttur. Bir problemi, (bir veya bir arada bir dizi denklemi) formal olarak çözemediğimiz zaman bize yardım etmeye hazırdır. Birazcık elementer cebir görmüş olanlar için bazı denklemleri çözmek öyle kolaydır ki hesap makinesinin yardımını gerekmez. Örneğin çoğumuz $x^2 - 3x + 2 = 0$ denklemini cebirsel çarpanlara ayırma yoluyla kolayca çözerek $x = 1$ ve $x = 2$ tam çözümlerini bulabiliriz. Ancak daha iyi bir yöntem bilmiyorsak, basit birkaç olanak deneyerek yanıtları elde edebiliriz.

Diğer yandan $x^3 - x^2 - 3x + 3 = 0$ gibi daha zor bir denklem için hesap makinesi yararlı olabilir (biraz daha fazla cebir bilgisi olanlar, x için tam yanıtı bulabilirler). Bu bilgiye sahip olmayanlar ise kolay birkaç tamsayı deneyebilirler (burada da $x = 1$, hemen bir çözüm verir) ancak var olan

öteki iki yanıt o kadar aşıkâr değildir. Hesap makinesi de işte burada işe yarar; denklemleri kesin olarak çözemese de kesin yanıtla çok yakın yaklaşık bir sayısal yanıt saptamamıza olanak sağlar. Örneğin, sol tarafta $x = 1,7$ değerini koyarsak sağ tarafta $-0,0770 \dots$ elde ederiz; bu da beklediğimiz sıfır değerine oldukça yakındır. Bu nedenle $x = 1,7$ değeri de bir başka çözüme yakındır, ama ne kadar yakın? Sırasıyla $x = 1,71, 1,72, 1,73$ ve $1,74$ sayılarını deneyerek (hesap makinemizle) sağ taraf için $-0,0538\dots, -0,0299\dots, -0,0051\dots$ ve $0,0204\dots$ buluruz. En sondaki iki sayı $x = 1,73$ ve $x = 1,74$ arasında “sıfırdan geçtiğinden” (yani negatiften pozitifte geçtiğinden) x için $1,73$ 'ten büyük, $1,74$ 'ten küçük olan bir çözüm olduğunu varsayabiliriz. Ayrıca daha fazla veya en azından makinemizin gücü yettiği kadar ondalık hanesi kullanarak bu çözüme giderek daha yaklaşabiliriz.

Ancak bunu yapabileceğimizi nereden *biliyoruz*? Çünkü basit matematik düzenlidir. Eğer “başlangıç sayısını” (örneğin x) birazcık değiştirirsek, sağ taraftaki yanıt da aynı ölçüde küçük bir miktar değişir. Bu örnek için, aritmetiğin düzenli olduğuna yönelik inancımız tümüyle yerindedir ve tam çözüm olan $\sqrt{3}$ sayısına cep hesap makinemizin izin verdiği en iyi yaklaşım olan $x = 1,73205080\dots$ sayısını buluruz. Üçüncü çözüm de $x = -\sqrt{3}$ 'tür.

Daha acımasız matematikçilerin, acımasızca planladıkları bazı denklemlerin, x 'in özel bir değeri yakınlarında (hatta bazılarının her yerde) daha az düzenli davranabileceklerini düşünsek bile bunların, sözcüğün alışlagelmiş anlamıyla “basit” denklemler olmayacaklarından da kuşku duymayız ve bu güvenimiz yersiz değildir. Bilimcilerin ve matematikçilerin çoğu da aynı güven duygusuna sahipti. Bu güven, Massachusetts Teknoloji Enstitüsü'nden Edward Lorenz 1960'da bir gün, güçlü bilgisayarını Dünya atmosferinin bir modelini ifade eden 13 tane denklem grubunun yaklaşık bir sayısal çözümünü için programlayıncaya kadar sürdü.

Problemin içerdiği aritmetik karmaşıktı, bu nedenle de bir bilgisayarın sayısal yardımı gerekiyordu ama içerilen denklemlerin her biri elementerdi; yani düzenli biçimde dav-

ranacağına inanılan türdendi. Yukarıdaki basit örnekte yaptığımız gibi Lorenz'de tam çözüme oldukça yakın olan bir dizi deneme sayısı ele alarak daha hassas bir yaklaşım bulmaya girişti. Deneme sayılarını çok ufak ölçüde değiştirerek bilgisayarı "tekrar deneme" için harekete geçirdi ve yeni sonuçları beklerken bir fincan kahve içmeye gitti. Geri döndüğünde bilgisayarın yeni çıktısının bir öncekine göre daha iyi olan yaklaşık bir çözüm vermediğini, ondan tümüyle farklı bir çözüm verdiğini gördü. Önce bilgisayar hatasından kuşkulandı, ancak her şeyi kontrol ettikten sonra korkunç bir gerçeğin farkına vardı: Bu bir dizi denklem için başlangıç sayılarında yapılan çok küçük değişiklikler "yanıt"ta çok büyük düzensiz değişimlere yol açıyordu. Bu, bir hava tahmin uzmanının hayallerini de yok ediyordu. "O zaman, eğer gerçek hava durumu da böyle davranıyorsa, uzun vadeli hava tahminlerinde bulunmanın olanaksız olacağını anladım." demişti Lorenz.

Edward Lorenz'in karşılaştığı şey kaotik davranma kavramıydı. Bu bağlamda kaos öngörülemez, önceden tahmin edilmeme anlamına gelmektedir. Meteorolojik denklemler bağlamında bunun anlamı, başlangıç koşullarındaki ufak bir değişimin (örneğin bir derecelik bir sıcaklık farkının) bir ay sonraki bir günün güneşli olması veya çok yağmurlu bir gün olmasına yol açabilmesiydi. Demek oluyor ki, meteorolojik verilerin herhangi bir hassasiyet derecesi ile bilinmesi (ilgili her niceliğin kesin değerinin bilinmesi dışında) uzak geleceğe dönük yaklaşık bir doğru tahmin yapılması için yeterli değildir. Kaotik davranışta, başlangıç koşullarındaki çok küçük bir değişiklik bile sonucun tanınmasını olanaksız kılacak ölçüde büyük değişimlere neden olabilmektedir. Ayrıca başlangıç koşulları için alınan iki dizi değerler arasındaki farklar büyüdükçe düzensiz durum da o ölçüde daha çabuk ortaya çıkmaktadır.

Uygulamada bütün ölçümlerin sonlu derecede deneysel hassasiyeti olması, bizi herhangi bir kaotik sistemin nihai durumunu niteliksel olarak öngörmenin bile olanaksız olduğu sonucuna götürür. Ancak yine de her şey yitirilmiş değil-

dir. Lorenz başlangıç değerlerini son derece küçük miktarlarda değiştirerek bilgisayardan denklemleri için olanaklı binlerce çözümü vermesini istedi ve çözümlerin tümüyle rasgele olmadığını saptadı. Sayıların rasgele olduğu doğrudur, ancak bunlar bazı olanaklı davranış sınırları içinde kalıyorlardı. Yoksa bu rasgele çılgınlığın da bir tür yöntemi mi vardı? Örneğin, bugünden bir yıl sonrasının hava durumu hakkında pek fazla bir tahmin yapamayacağımızı kabul etsek bile “izin verilen” olanaklı sınırlar dışında kalan birçok durumu saptayabiliriz. Çünkü hava durumunun hepimizce bilinen bazı yönleri vardır; kışlar soğuk olur, yazlar sıcak olur, muson ve kasırga mevsimleri vardır ve en düşük ve en yüksek sıcaklıkların da oldukça iyi belirlenmiş sınırları vardır. Kaos içindeki bu düzen görüntüsünün kaynağı nedir?

Bu tür soruları ele almadan önce biçimlerinin basitliği nedeniyle düzenli davranmaları beklenen bu basit matematiksel denklemlerin düzenli bölgeden çıkıp kaos bölgesine nasıl geçtiklerini tam olarak anlamaya gerek vardır. Yapılacak ilk şey hangi tür denklemlerin kaotik çözümlere yol açtığını saptamaktır. İkincisi ise, eğer mümkünse, bu tür denklemlerin öngörülebilir bölgeden kaos bölgesine tam olarak nasıl geçtiğini araştırmaktır. İlk ipuçlarından birisi, biraz beklenmedik bir kaynaktan, 1970’lerin ortalarında yapılan ve mevsimsel olarak üreyen böceklerin yıllık nüfuslarını inceleyen bir araştırmadan elde edildi.

Mevsimlere göre böcek nüfusunu saptadığı düşünülen denklemler, hava tahmini denklemlerinin tersine, çok basitlerdi; cep hesaplayıcısı kadar basit! Örneğin, özel çevre koşulları nedeniyle nüfusu hep 500.000 olan bir böcek toplumunun var olduğunu düşünelim. İlk yılın nüfusuna x_1 milyon (yani, sabit nüfus için $x_1 = 0,5$ ’tir) ikinci yılın nüfusuna da x_2 milyon dersek, matematiksel modele göre

$$x_2 = 2x_1(1 - x_1)$$

olur; burada sağ tarafın anlamı, 2 çarpı x_1 çarpı $(1 - x_1)$ ’dir. Benzer şekilde üçüncü mevsimdeki nüfus da

$$x_3 = 2x_2 (1 - x_2)$$

olur ve bu şekilde $n + 1$ 'inci mevsimdeki nüfus olan x_{n+1} milyon, bir mevsim öncesindeki nüfus olan x_n milyon cinsinden,

$$x_{n+1} = 2x_n (1 - x_n)$$

bağıntısıyla ifade edilir. Bu denklem akla yakındır, çünkü eğer ilk mevsimde çevrenin bekleyebileceğinden çok böcek varsa (örneğin 800.000, yani $x_1 = 0,8$) ikinci yılda bu x_2 'ye, iki çarpı 0,8 çarpı 0,2'ye, yani $x_2 = 0,32$ 'ye düşecektir (ya da 320.000 böceğe). Bu düşük nüfusla koşullar nüfus artışına elverişli olacak ve üçüncü yıl nüfusu x_3 , 2 çarpı 0,32 çarpı 0,68 yani $x_3 = 0,4352$ (ya da 435.200 böcek) olacaktır ve beklentimizi doğrulamaktadır.

İlk yıl için 0 ile 1 arasında herhangi bir sayı ile başlayarak denklemlerin öngördüğü nüfusları kolayca bulabiliriz. Böylece yukarıda verilen $x_1 = 0,8$ nüfusu ile başlayarak: x_2 , x_3 , x_4 ,... sayısı dizisini yazabiliriz:

$$0,8; 0,32; 0,4352; 0,4916; 0,49986; 0,499999$$

Bu bize, altıncı yılda sabit nüfusa eriştiğimizi göstermektedir. Gerçekte 0 ile 1 arasında olan istediğiniz herhangi bir x değeri ile başlarsanız da yine sabit bir $x = 0,5$ limitine varırsınız. Bundan daha basit bir şey olabilir mi? Bu sabit değere (örneğimizde $x = 0,5$) bazen “sabit nokta” ve bütün yollar sonunda ona ulaşıyor görüldüğünden “kararlı sabit nokta” veya “çekici” de denilir. Yukarıdaki denklemlerin bir başka sabit noktası olduğu dikkatinizden kaçmış olabileceği için, bu önemlidir. Bu ikinci sabit nokta $x = 0$ 'dır. Eğer $x_1 = 0$ ile başlarsanız dizideki x_2 , x_3 , x_4 ... sayılar için bulacağınız değerler hep sıfır çıkar. “Eğer başlangıçta hiçbir böceğiniz yoksa yıllar sonra bir böceğiniz olsa bile çok şanslısınız.” demenin matematiksel ifadesi budur. Öyleyse $x = 0$ değeri de bir sabit noktadır. Ancak 0 kararsız bir sabit noktadır, çünkü x_1 için sıfır olmayan ne kadar küçük bir sayı seçerseniz seçin, x_n sayı di-

zisinin değerleri $x = 0$ 'dan uzaklaşıp çekici sabit nokta olan $x = 0,5$ 'e doğru gideceklerdir; deneyin ve görün.

Demek oluyor ki, denklemler hiç olmazsa saçma değiller, aynı zamanda kaotik olmaktan da çok uzaklar. Hatta onlara “çok düzenli” diyebiliriz; 0,5 hedefine çok düzenli biçimde yaklaşıyorlar. Şimdi de sabit nüfusun 0,6875 milyon (yani 687.500 böcek olduğunu varsayalım. Bu sayının özel hiçbir yanı yoktur; onu sadece $x = 0,5$ 'ten büyük olduğu için (özellikle araştırmak istediğim yön bu olduğu için) seçtim. Mevsimlere göre değişimleri veren denklemini yazmak da kolay:

$$x_{n+1} = 3,2x_n (1 - x_n).$$

Bu denklem bir öncekinden, sadece sağdaki 2 çarpanı yerine 3,2 almasıyla farklı. Eğer cep hesap makinenizi alır ve $x_1 = 0,6875$ 'le başlarsanız ürettiğiniz $x_2, x_3, \dots, x_n, \dots$ dizisinin bütün sayılarının aynı 0,6875 sayısı olduğu görürsünüz. Öyleyse bu gerçekten de bir sabit nokta çözümüdür. Eğer 687500 böcek ile başlarsanız, o zaman sonsuza kadar aynı sayıda böceğiniz olacaktır. Ancak $x = 0,6875$ bir “çekici” midir? Bunu siz kontrol edebilirsiniz. O zaman x_n dizisinde sayıların iki değer arasında gidip geldiklerini, 0,799 ve 0,513 sayılarına yakın değerler arasında salındıklarını göreceksiniz. Benim dokuz haneye kadar gidebilen hesap makinemle dizi, sonunda

$$a, b, a, b, a, b, a, b, \dots$$

şekline dönüşüyor; burada $a = 0,799455490$ ve $b = 0,513044510$ 'dur. Ne oluyor? Görülen odur ki, sabit $x = 0,6875$ kararlı olmayan bir noktadır. Kararlı olan durum ise 799.455 böcekli (inandırıcı olmak uğruna böceğin kesirlerini yok sayacağız) gereğinden daha kalabalık bir mevsim ile 513.044 böcekli gereğinden az nüfuslu mevsim arasında sürekli dalgalanma durumudur. Fiziksel bakımdan bu hayli olanaklıdır. Denklemlerimiz abes bir sonuç vermemiş, sadece beklenenden biraz daha karmaşık bir durum ortaya koymuşlardır.

Ancak daha kötüsüne de hazır olun. Sabit noktamızın değerini artırdıkça bizim basit denklemlerimiz de inanılması zor şeyler yapmaya başlıyorlar. Sabit nokta için $x = 5/7$ değeri ile bizim güçlü denklemlerimiz

$$x_{n+1} = 3,5 x_n(1 - x_n)$$

olur ve kolayca doğrulayabileceğiniz gibi $x = 5/7$ böcek nüfusu sonsuza dek kendi kendisini yeniler. Başka bir x değeri ile (hatta bütün durumlar için var olan önemsiz $x = 0$ değeri dışındaki herhangi bir değerle) başlarsak ne olur? Hesap makinenizi yine çalıştırın. Önemsiz olmayan sabit noktanın (burada $x = 5/7$) bir çekici olmadığını görürsünüz; ancak şimdi kararlı çözüm, iki yerine dört sayı içerir ve dizi aşağıdaki şekli alır:

$$a, b, c, d, a, b, c, d, a, b, c, d, \dots$$

Burada da (benim dokuz haneli hassasiyet derecesiyle) $a = 0,382819683$, $b = 0,826940707$, $c = 0,500884210$ ve $d = 0,874997264$ 'tür. Bu durum için de fiziksel açıklamayı tasavvur edebiliriz. Mevsim "a" olduğunda nüfus gereğinden azdır ve bu, bir sonraki "b" mevsiminde nüfus artışına neden olur ve "c" mevsiminde bir azalmaya gider. Son olarak, "c" nüfusu gereğinden azdır ve "d" mevsimindeki son artışı kamçılar. Hesaplamaları yapmadan da böyle bir salınım durumunun sonuçta giderek, sabit nokta değeri olan $x = 5/7$ 'ye yaklaşacağını bekleyebilirsiniz; ancak bu hiçbir zaman gerçekleşmez; salınan değerlerin kendileri kusursuzca kararlıdır.

Böylece tanımlayıcı denklemdeki sayısal katsayı 2'den 3,2 ve 3,5'e yükseldiğinde, kararlı limit, çarpıcı biçimde, kararlı bir sabit nokta yerine önce "iki devirli" salınıma daha sonra da "dört devirli" salınıma doğru gitmektedir. Aklımıza hemen, giderek artan bu karmaşıklığın ne kadar süreceği sorusu gelmektedir. Bunun yanıtı, bir anlamda, "sonsuza dek"tir. Sayısal katsayı, son verdiğimiz 3,5 değerinin ötesin-

de büyüyerek “kritik” değer denilen 3,57’ye yaklaştıkça, kararlı tekrarlayan devir düzeni de patlayarak 8, 16, 32, 64, gibi 2’nin giderek artan kuvvetlerine yönelir. Kritik değer in ötesinde ise durum tümüyle kaotik bir hal alır. Bununla kastettiğimiz, sonunda sayıların hiç tekrarlanmadığı, ya da bir anlamda, tekrarlama düzeninin sonsuz sayıda noktalar arasında gidip gelme şeklinde olduğudur. Böylece bizim basit tanımlayıcı denklemimiz olan

$$x_{n+1} = Ax_n (1 - x_n)$$

bizi matematiğin en düzenli bölgesinden giderek artan karmaşıklıkta (ama yine de kararlı olan) tekrarlanan düzenlerden, tümüyle kaotik, davranışlara götürmektedir ve bunlara yol açan, sadece A parametresinin 2’den yavaş yavaş yaklaşık 3,6’ya yükselmesidir.

A’nın 3,6’dan büyük değerleri için, giderek artan bir kaos derecesi ile davranış sürmektedir. “Kaos derecesi”ni ne anlamda kullandığımızı anlamak için düzensiz bir durumu (yani tanımlayıcı denklemde A için kritik değerden daha büyük bir değer aldığımız durumu) ayrıntılarıyla incelememiz gerekiyor.

Kaos’un en korkutucu özelliklerinden birisi şudur: Başlangıç nüfusu olarak alınan farklı iki x_1 değeri, birbirlerine istenildiği kadar yakın seçilseler de, sonunda birbirleriyle hiçbir ilgisi olmayan düzenlere doğru uzaklaşırlar. Böcek üretmeyi tanımlayan denklemlerde $A = 3,9$ alarak bu belirli kaotik özelliği inceleyelim. Özellikle de başlangıç değerleri birbirine çok yakın olan, $x_1 = 0,100$ ve $x_1 = 0,101$ (yani 100.000 ve 101.000 böceği temsil eden) iki böcek toplumunun kaderlerini ele alacağız. Aşağıda verilen sayı sütunları, (üç ondalık hanesiyle verilmiş ancak gerçekte benim güvenilir cep hesap makinesiyle dokuz haneli bir hassasiyetle hesaplanmışlardır) iki farklı nüfusla başlayan bu iki böcek toplumunun şansını, masum görünümümlü yukarıdaki denklem uyarınca, ilk 14 nesil boyunca kıyaslamaktadır.

Nesil	A kümesi	B kümesi
1	0,100	0,101
2	0,351	0,354
3	0,888	0,892
4	0,387	0,376
5	0,925	0,915
6	0,271	0,304
7	0,771	0,825
8	0,690	0,562
9	0,835	0,960
10	0,538	0,150
11	0,969	0,497
12	0,116	0,975
13	0,399	0,095
14	0,935	0,336

Görüldüğü gibi 10. mevsime gelindiğinde iki kümenin nüfusları arasındaki yakınlık tümüyle yok olmuştur.

Düzenli durumdan kaosa giden bu gizemli geçişi izlemek için kullandığımız tanımlayıcı denklemin, hiçbir sihirli özelliği yoktur. Bu tür davranışa yol açacak sayısız başka basit bağlantı yazılabilir. Gerçekte kaosa geçişi araştırmayı bu kadar ilgi çekici yapan da bu tekdüzeliktir. Ortak olan özellik şudur: Denklemdaki bir A parametresi yavaş yavaş kritik bir limite yaklaşırken (bu limit değere $A = L$ diyelim) çözümler, kararlı bir sabit nokta yerine salınım periyotlarının sürekli iki katına çıktığı “periyot katlama” süreciyle kaosa giderler. A sayısı limit değeri olan L’den ne kadar öteye geçerse, birbirine çok yakın başlangıç sayıları olan “nüfuslar” arasındaki ilişkinin sona ermesi için gereken nesil sayısı da o ölçüde azalır. Bu da bize aşıkâr biçimde farklı derecedeki veya güçteki kaotik davranışları ayırdedebilme olanağı sağlar.

Kritik limit olan $A = L$ ’ye “düzenli taraftan yaklaşarak, tekrarlanan devir sayısını iki katına çıkarma, genel davranışın en çarpıcı gösterimini oluşturur. Bu ikiye katlanmala-

rın (veya sonu gelmeyen bir yalınlaştırmaya adanmış matematikçilerin deyişiyle “iki kola ayrılmalara”ın her biri, A parametresi özel değerler aldığı zaman gerçekleşirler; 2^n tekrarlanan değerler alan bir periyodun, katlandığında aldığı değere $A = A_n$ diyelim. Bu özel A sayılarının $A = A_n$ dizisi, (n sonsuza yaklaşırken) kaosu başladığı $A = L$ limit değerine yaklaşır. Bu durumda n büyüdükçe $L - A_n$ sayısı da giderek küçülür. Niceliklerle ifade edildiğinde

$$\frac{A_{n+1} - A_n}{A_{n+2} - A_{n+1}} = d_n$$

oram, n büyüdükçe, hızlı biçimde, tuhaf ama kesin belirli bir sayıya yaklaşır. Bu sayı

$$d = 4,6692016... \text{’dir.}$$

Periyodunu ikiye katlayarak kaosa giden her model için d’nin aynı değeri alması gerçekten şaşırtıcıdır. Ayrıca, bundan bir başka sonuç elde edilebilir; d’nin değeri yukarıdaki sayı olmak koşuluyla, n büyüdükçe $L - A_n$ ’de d^n ’ye orantılı olmaya yönelir. Bu nedenle kaosu hiç de kaotik olmayan bir biçimde başlaması hatta çok kesin biçimde tanımlanmış olması ilginçtir. Kaosu başlamasıyla tanımlayıcı denklemin bütün ayrıntıları artık önemini yitirir ve evrensel bir davranış biçimi ortaya çıkar.

Ancak bütün bunların bilimsel anlamdaki gerçek Kaotik hareket ile ne ilgisi olabilir? Oldukça geniş kapsamlı gerçek fiziksel, kimyasal biyolojik sistemlerin kaosa doğru periyodu ikiye katlayan bir yol izledikleri anlaşılmıştır. Gazlarda çalkantı durumunun başlaması (bunun sıradan bir örneği sigaranın ucundan çıkan dumanın yükselişidir) elektronik devrelerdeki kararlı olmayan elektriksel olgular ve hatta kalp kasının kalbin atış hızını ayarlayan cihaza verdiği reaksiyonlar bu tür sistemlerdir. Yukarıda verilen oranla tanımlanmış olan d değerini ölçmek için yapılan deneysel girişimlerin, farklı bilimsel bağlamlarda, evrensel bir sabit sayıya,

matematiksel teorinin bir ürünü olarak “ortaya çıkan” 4,669... sayısına işaret etmeleri daha da çarpıcı bir olgudur.

Günümüzde etkileyici olarak değerlendirilen bütün bu bulgular, kaosa doğru periyodu ikiye katlayan yolla ilgili yeni ve alışılmadık görünen fikirler, ilk zamanlar akademik dünyanın etkin matematikçileri tarafından hemen kabul görmemişlerdir. Konu ilk olarak Los Alamos’daki bir genç fizikçi tarafından bu bölümde verilenler çerçevesinde; bir cep hesap makinesi kullanılarak “böcek nüfusu” denklemleri bağlamında ortaya atılmıştır. Adı Mitchell Feigenbaum olan bu fizikçinin, evrensel d-sabit sayısının (şimdi ona Feigenbaum sabiti denilmektedir) elde edilmesini konu alan makalesi 1976-1979 arasında, profesyonel matematik dergilerinin editörleri tarafından üç yıl boyunca reddedilmişti. Bu aydınlanmış çağda bir cep hesap makinesiyle oynayarak matematiksel önemi olan ne elde edilebilirdi ki? 1979’da bir İtalyan fizikçi (gerçek dünya çalkantılarının matematiksel modeli olan beş karışık denklemi bilgisayar kullanarak çözmeye çalışırken) periyot katlanması olgusuyla karşılaştı ve ancak o zaman Feigenbaum’un çalışması ciddiye alındı.

Ondan sonra da doğadaki periyot katlayan süreçleri arayan ve bulan fiziksel deneyler yapıldı. Bu türden ilk başarılı deney Fransa’da yapıldı. Deney sıvı helyum dolu bir kazanı kaosa kaynayınca kadar ısıtmaktan ibaretti. Deneyciler sıvı helyumun “kaynamaya” yaklaşmasını dikkatle izlerken ısının yayılma akıntılarının girdap gibi dönmeye başladığını ve daha sonra da art arda ikiye katlanma süreçleri oldukları açıkça görülen davranışlara girdiğini saptadılar. Bu öncü çalışmayı kısa sürede, onu doğrulayan başka çalışmalar izledi. Düzensizliğe giden yolda gerçekten düzen vardı. En son ve en ilginç uygulamalardan birisi, kalbin, yaşamı sürdüren ritmik atışlardan ölümcül spazmlara (kalp krizine) geçişinin modelini saptama çabasıdır. Gözlenmiş olan kalp atışı bozukluklarının büyük bölümünü ifade edebilen denklemler elde edilmiştir. Burada da, bozukluk başlamadan önce denklemler kalp atışı kaosa giden yolda periyodun iki katına çıktığının açık işaretlerini saptadılar.

Periyodun iki katına çıkmasının kaosa giden tek yol olmadığına bilinmesine karşın, bu yol klasik örnek olmayı sürdürmektedir. Feigenbaum'un öncü çalışmasının bir sonucu olarak kaostun başlaması konusunun özenle araştırılması günümüzde etkin bir bilim koludur. Çeşitli alanlarda çalışan bilimciler kaybedilen zamanı telafi etmek için büyük bir hızla çalışıyorlar. Çünkü kuantum fiziğinin mikro dünyasından astro fiziğin makro dünyasına kadar her yerde kaos var. Bilimsel bir devrimin eşiğindeyiz ve bunun kıvılcımının alçak gönüllü bir cep hesap makinesinden çıkmış olduğunu unutmayalım. Bu yeni alanın hangi hızla gelişeceği ve ondan beklenileni ne ölçüde verebileceğini henüz bilmiyoruz. Ancak araştırma konusunun, kaostun başlamasındaki düzen derecesi olduğunu unutmamak gerekir.

Kaotik durumun kendisi hâlâ sözcüğün ifade ettiği durumdur. Deneysel olarak sonsuz derecede bir hassasiyet olanaksız olduğundan "iyi kontrol edilmiş" bir deneyin sonuçlarının her zaman aynen tekrarlanması gerekmez. Hava tahmincisi bakımından, önümüzdeki bir saat içinde havanın nasıl olacağını tahmin etmek için gökyüzüne bir bakmak hâlâ yeterli olabilir veya global hava verilerini izleyerek, oldukça güvenli biçimde, yarının hava tahmini de yapılabilir; ancak uzun vadeli tahmin her zaman nankör bir iştir.

XVI. Bölüm

Süper Matematik ve Canavar

Çevremiz simetri örnekleriyle doludur. Hatta biz kendimiz ortamımızdan geçen düşey bir doğruya (daha doğrusu, düşey bir düzleme) göre yaklaşık olarak simetrik sayılırız. Gerçekte etrafımızdaki bir çok nesnede yaklaşık olarak bu tür, iki yanlı denilen simetri olduğu için bir aynaya baktığımızda, ayna dünyasında sağın sola, solun da sağa değiştiğini hemen fark edemeyiz. Aynaların neden sadece sağla solu değiştirdiği (neden aşağı ile yukarıyı değiştirmediyi) sorusu, üzerinde derinlemesine düşünmek isterseniz, bu size birkaç uykusuz geceye mal olabilir. Ancak bu bölümde ele aldığımız soru bu değildir ve ben de (size biraz haksızlık olsa da) ona artık değinmeyeceğim. Bazı nesnelerin kendilerine özgü başka tür simetrisi vardır. Örneğin gamalı haç bir tür döngüsel simetriye, bir yıldız ise hem döngüsel hem de iki yanlı simetriye sahiptir. Duvar kâğıdının sistemleri ise daha farklıdır; bütün desen farklı doğrultularda yer değiştirirse de görünümü aynıdır.

Şimdi, “simetri”den ne kastettiğimizi biraz daha kesin biçimde ifade etmeğe çalışalım ve aynı simetriye sahip olan nesnelerin ortak yanlarının ne olduğunu saptayalım. Simetri bir eylem, bir “operasyon” (bu bir yansıma, döndürme veya yer değiştirme olabilir) cinsinden tanımlanır; bu operasyon sonucunda nesne “hâlâ aynı görünür”. Örnek olarak bir kare alalım: Saat yönünde veya ona ters yönde, 90 derece veya 180 derece döndürülürse “hâlâ aynı görünür”. Bu dönmele kare simetri operasyonları denir, ama var olan sadece bunlar değildir. Kareyi iki köşegeninin herhangi birinde veya merkezinden geçen ve kenarlarına paralel olan

doğruların herhangi birisinde yansıtabiliriz. Bu yedi operasyona bir de “olduğun gibi kal” eklenirse sonuçta sekiz simetri operasyonu elde edilir.

Bu durumda karenin sekiz simetri operasyonu altında değişmez (“aynı” için matematiksel ifade) olduğunu söyleriz. Ancak, “Kareyi 270° veya 360° döndürürsem veya ters çevirirsem ne olur? Bunlar da simetri operasyonları değil mi?” diye sorarsanız yanıt “hayır”dır. Bunu açıklamak için, karenin içinde özel olmayan herhangi bir nokta işaretleriz (örneğin bir kenarı boyunca, bir köşenin biraz altında). Bu noktayı başka konuma getiren ancak kareyi “değişmez” bırakan bütün operasyonlar, farklı simetri operasyonlarıdır. Hem kareyi hem de noktayı aynı şekilde hareket ettiren ancak farklı gibi görünen herhangi iki operasyon simetri bakımından aynı sayılırlar.

Bunu açıkladıktan sonra, “Bütün karelerde ortak olan özellik simetri operasyonlarının aynı olmasıdır.” diyebiliriz, ancak bundan fazlası söz konusudur. Çünkü art arda yapılan iki operasyon her zaman bir başka simetri operasyonu ile özdeştir. Bu anlamda, operasyonlar “kapalı” bir küme oluştururlar; eğer bunları alfabenin ilk sekiz harfiyle adlandırarak bir dama tahtası alıp, sıraları ve sütunları A, B, C, D, E, F, G, H ile işaretleyip sonra da karelere, bu operasyonları uyguladığımızda ne bulduğumuzu yazalım. Böylece E sırası ve F sütunundaki kareye, önce E sonra F uyguladığımızda bulacağımız sonucu yazarız. Bu küme kapalı olduğundan bütün dama tahtası A ile H arasındaki harflerin özel bir düzenlemesiyle kaplanacaktır. Buna, bir karenin simetri operasyonlarının “çarpım tablosu” diyoruz. Dama tahtasındaki düzenleme bize kare hakkında başka şeyler de söyler; bunun ne yararı olabilir?

Bu soruyu yanıtlamak için bütün simetrilerin en basiti olan, kendimizin (yaklaşık) simetrisini düşünelim. Bu simetri grubunun (bu tür operasyon kümelerine “grup” denilir) sadece iki operasyonu vardır; birisi “olduğun gibi kal”, bunu I ile göstereceğiz ve “ortamızdan geçen düzlem üzerinde yansıma” için de R harfini kullanacağız. Rasgele bir nokta ola-

rak kol saatimizi kullanırsak yansıma onu sol bileğimizden sağ bileğimize ve eğer solaksak da sağdan sola geçirir. Başka herhangi bir hareket, örneğin takla atmak, yeni bir operasyon sayılmaz; o da “I operasyonu”dur. Çünkü kol saatini daha önce olduğu yerde bırakır (takla sırasında saatin düşmediğini varsayıyoruz). Bizim kendi simetri grubumuzda iki operasyon veya iki eleman bulunuyor, I ve R.

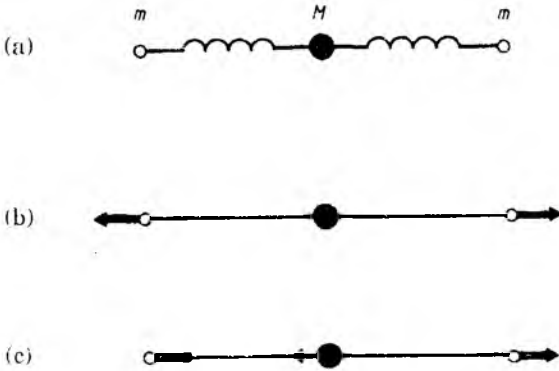
Şimdi onun çarpım tablosunu yazabiliriz. “Olduğun gibi kal” ve ardından gelen “yansıma”nın sonucu yansıma demek olduğundan semboller kullanarak $IR = R$ yazabiliriz. Benzer şekilde $RI = R$ olmalıdır; çünkü yansıma, ardından “olduğun gibi kal” demenin sembolle ifadesidir. Son olarak yansımanın ardından tekrar yansıma gelirse kol saatini ilk olduğu konuma götürdüğü için $RR = I$ ’dir. Bu dört eşitlik 2×2 ’li bir dama tahtasında aşağıdaki gibi bir çarpım tablosu şeklinde yazılabilir:

	I	R
I	I	R
R	R	I

Burada I ve R’yi sayılarla değiştirirsek ve IR’yi de aritmetikteki “I çarpı R” işlemi olarak yorumlarsak çarpım tablosunun tutarlı olduğunu fark ederiz. Ayrıca bunu iki ayrı yolla sağlayabiliriz; önce, $I = 1$, $R = 1$ koyarak, sonra da $I = 1$, $R = -1$ koyarak. Bu seçimlerden ikisi de tablodaki dört denkleme sağlarlar: $II = I$, $IR = R$, $RI = R$, $RR = I$. İki gösterim bulduğumuzu söyleriz; $I = 1$, $R = 1$ ’e simetrik temsil; $I = 1$, $R = -1$ ’e de antisimetrik temsil denir.

Bu bizi nereye götürüyor. Buna göre, örneğin, I, R türü simetriye sahip olan kuvvetlerin etkisiyle gerçekleşen herhangi bir hareket, sadece birbirinden temelde farklı iki türden olabilir; simetrik veya antisimetrik. Bunu iyice anlamak için basit bir örnek seçmek yeterlidir. Şekil 20 (a)da düz bir tel üzerine geçirilmiş üç boncuk görülmektedir; dıştaki boncukların kütleleri aynıdır (m diyelim), ortadaki boncukun kütle-

si farklı olabilir (M olsun) ve dıştaki iki boncuk birbirinin aynı olan iki yayla ortadaki kütleye tutturulmuşlar. Resimden açıkça görüldüğü gibi, bu sistem için ortadaki boncuğun merkezinden, tele dik olarak geçen düzlem bir yansıma simetrisi düzlemidir. Öyleyse bu düzen yukarıda açıklanan simetri sınırlamalarına bağlıdır.



Şekil 20.

Şimdi boncuklara yavaşça dokunarak onları salınım hareketine başlattığımızı düşünelim. Yukarıda verilen “grup teorisi” sadece iki tür “basit” hareketin, yani basit salınımlarla kendini durmadan tekrarlayan (sürtünmenin yol açtığı yavaşlamayı yok sayıyoruz) hareketin olanaklı olduğunu söylemektedir. “Normal modlar” denilen bu hareket biçimleri Şekil 20 (b) ve 20 (c)de gösterilen, sırasıyla, simetrik ve anti-simetrik modlardır. Ancak uygun olan modların bunlar olduğunu nereden biliyoruz ve bunlar hangi anlamda “simetrik” ve “anti-simetrik” oluyorlar?

Önce Şekil 20 (b)ye bakalım. Oradaki oklar, kütlelerin belirli bir andaki hareketlerini göstermektedir. Uçlardaki m kütleleri dışa doğru aynı şekilde hareket etmekte, ortadaki M kütlesi ise hareketsizdir. Salınımın daha sonraki bir döneminde uçlardaki kütleler, aynı şekilde içeriye doğru ha-

reket edeceklerdir ve M kütlesi yine hareketsiz olacaktır. Bu, simetrik mod hareketidir; çünkü I ve R dönüşümleri altında simetrik gösterim olan $I = 1$, $R = 1$ ile aynı temel özellikleri taşır. Örneğin, Şekil 20 (b) yansıma düzleminde yansıtıldığında kendine dönüşür, yani R operasyonu 1 'e eşittir. “Olduğun gibi kal” operasyonu olan I ise her zaman 1 'e eşittir. Bu simetrik mod'da, uçlardaki m kütlelerinin her zaman tam olarak “ters” biçimde hareket etmeleri gerektiğine ve M kütlelerinin tam olarak hareketsiz olması gerektiğine dikkat edin. M 'nin herhangi bir hareketi simetrik mod için gerekli olan $R = 1$ simetri koşuluna ters düşer.

Şimdi Şekil 20 (c)'ye bakalım; bu antisimetrik mod'dur. Bu mod'da dıştaki kütleler aynı yönde eşit biçimde hareket ediyorlar, ortadaki kütle de artık hareket edebilmektedir. Gerçekte, eğer bütün mod'un “ağırlık merkezini” sabit tutmak istiyorsak, o zaman ortadaki kütle, m kütlelerinin hareket yönüne ters olan yönde hareket etmelidir. Bu mod'u yansıma düzleminde yansıtınca ne olur? Şekilde kolayca görüleceği gibi kendi negatifine yansıyacaktır (yani hareketi gösteren bütün oklar ters yöne dönecektir) Demek oluyor ki, bu mod için R operasyonu -1 'e denktir. Yine $I = 1$ ile bu mod'un izin verilen birine uygun düşmektedir; bu sefer $I = 1$, $R = -1$ gösterimlerden antisimetrik gösterime.

Şekil 20 (a)'da verilen düzeni kurar ve uçtaki boncuklardan birini çekip bırakırsanız başlayan hareket Şekil 20 (b) ve 20 (c)'de gösterilen hareketlerden çok farklı (ve çok daha karmaşık) olacaktır. Ancak yine de bu hareket (veya başka türlü başlatarak oluşturacağınız herhangi bir hareket) her zaman bu “normal mod'lar”ın farklı oranlardaki karışımı olarak açıklanabilir. Bu anlamda, normal mod'lar olan simetrik ve antisimetrik mod'lar olanaklı bütün hareketlerin oluşturulabildiği temel mod'lardır ve onların temel yapıları, sadece düzenin simetrisi yoluyla bilinmektedir. Bilmek isteyebileceğimiz her şeyi (örneğin, problemin fiziksel ayrıntılarına bağımlı olan, bu normal modların her birinin frekansını) bize sadece simetrinin söyleyemeyeceği doğrudur ancak her normal mod hareketinin temel düzeni “grup teorisi” ile

yani, simetri operasyonlarının nasıl birleştiklerinin bilinmesiyle tamamen belirlenmiş olur.

Üçgen, kare, dikdörtgen ve sayısız başka şekillerin simetri durumları için de benzer tartışmalar yapılabilir. Her biri için bütün simetri operasyonlarını saptayıp, çarpım tablosunu ve sayısal aritmetik gösterimi bulabiliriz. Simetri operasyonlarının sayısı (buna grubun “mertebesi” denilir) arttıkça gösterimler de daha karmaşıklaşır ve karmaşık sayılar gibi daha gelişmiş matematiksel kavramlar gerektirseler de bunlar yine de varlardır ve çoğu kez bize bazı şaşırtıcı şeyler anlatırlar. Bazen tamamen farklı görünen iki problemin simetri bakımından aynı oldukları yani, simetri operasyonlarının farklı olmasına karşın tümüyle özdeş çarpım tablolarına yol açtıkları ortaya çıkar. Bazen de iki veya daha fazla gösterim (veya normal mod’lar) birbirleriyle özellikle bağlantılıdır (simetri operasyonları ile birbirlerine dönüşürler) ve bu nedenle de onlarla ilgili fiziksel durumlar ne olursa olsun aynı frekansa sahiptirler.

Aynı kavramları, üç boyutlu şekillere de uygulayabiliriz, örneğin küp için 48 simetri operasyonu (bunların 24’ü dönme, 24’ü de yansıma içerir) bulabiliriz. Bu kavramlar yanal hareketleri de içerecek şekilde genişletilebilirler. Örneğin duvar kâğıdının sadece 17 farklı simetrisi vardır. Üç boyutta ki benzer problem çok daha zordur; kristallerdeki atom düzenlemeleri için tam 230 simetri olanağının söz konusu olması buna örnektir. Bunlara “uzay grupları” denilir ve sofratuzu (sodyum klorür) ve metalik demirin atom yapısının sınıflandırılmasında büyük önem taşırlar.

Bilimciler atomik yapıları deneysel olarak saptamak için, maddeden alınan bir örnek üzerine x-ışınları veya nötronları odaklayarak kristal kafesi düzeninden geçen ışınların nasıl farklı yönlerde ayrıldıklarını (bilimciler buna “saçınım” der) gözlerler. Kırılan ışınların çıktıkları farklı doğrultuları (ışınların hiç kırılmadıkları simetri doğrultuları da aynı önemi taşır) belirleyen kristalin uzay grubudur. Bu nedenle saçılan ışınların görece güçlerinin ve doğrultularının dikkatle ölçülmesi, sonuçta atomik yapının tümünün saptanmasına ola-

nak sağlar. “Uzay grubu” simetrisinin getirdiği bilinen bazı sınırlamalar, atomların konumlarını belirleme işini çok basitleştirmektedir.

Şimdiye kadar ele aldığımız simetrilerin hepsi bir çeşit sürekli olmayan, “sıçrama” türünden operasyonlarla ilgili olmuştur; 60°’lik bir dönme veya belirli sabit bir uzaklığa yanal hareket gibi. “Sürekli” denilen simetri grupları da vardır; bunlarla (iki boyutta) bir daire ve (üç boyutta) bir küre arasında bağlantı kurulabilir. Bu şekiller, sonsuz küçük ölçüde dönme operasyonundan sonra bile değişmezler. Bunlar, sırasıyla bir eksene göre simetrik olan veya küresel simetrik olan sistemlerle ilgili konularda bilimciler için önemlidirler.

Örneğin, hidrojen atomunu ele alalım. Ağır bir çekirdekten (bir nokta büyüklüğünde bir kütle de diyebiliriz) ve çevresinde dönen tek bir elektrondan oluşur. Elektron, hareket denklemleri uyarınca hareket eder; bu denklemler küresel bir uzayın simetri koşullarını da içerirler. Bu örnekle ilgili matematiksel ayrıntılar böyle bir kitabın kapsamı dışında kalır ancak olanaklı yörüngeler, daha önce irdelediğimiz üç boncuk probleminin simetrik ve antisimetrik mod’ları kadar kesinlikle tanımlanmışlardır. Elektronun gerçekte, ufacık bir parçacık olarak değil de, daha çok çekirdeği çevreleyen bir “bulut” olarak düşünülmesi gerekmektedir ki konunun uzmanı olmayan çoğunluk için bu kolay değildir. Simetri kısıtlamaları da bu bulut için izin verilen şekillerle kendilerini ortaya koyarlar. En basit şekil, tam küresel simetrisi olan şekildir ve bilimciler buna s durumu derler (buradaki s ’nin simetri veya küre ile bir ilgisi yoktur). Daha başka şekiller arasında karmaşık yönlerde çan şeklinde yuvarlak çıkıntıları olan bulutları da sayabiliriz, ama bunların hepsi kürenin sürekli simetri grubu ile kesin olarak tanımlanmışlardır.

Ancak “grup teorisi”nin büyük gücü söz ettiğimiz şeylerin çok ötelere uzanır. Şimdiye kadar grup operasyonlarını üçgen, kare, küp, küre, kristal yapılar gibi gerçek nesnelerin düzenlenmeleri bağlamında kullandık. Bilimcinin dünyası böyledir. Gerçek matematikçiler ise düşüncelerinin, fiziksel dünyanın ötesine uzanmasına izin verirler. “Oralar-

da” geometrik simetriler dışında kalan birçok farklı simetri, keşfedilmeyi beklemektedir. Örneğin, VII. Bölüm’de tartıştığımız saat aritmetiğini ele alalım. Normal bir 12-saatlik saate $8 + 2 = 10$, $8 + 6 = 2$, $6 + 9 = 3$, $6 + 6 = 0$ vb. olduğunu gördük. “Toplama” işlemi altında sayılar “kapalı” bir küme oluştururlar (yani sağ tarafta bulunan sayı da kümenin elemanıdır). Sıfır ise “olduğun yerde kal” durumunu sağlama işlevini yapar. 12 saat yerine üç saat için de bütün toplama işlemlerini kolayca yazabiliriz:

$$\begin{array}{lll} 0 + 0 = 0 & 0 + 1 = 1 & 0 + 2 = 2 \\ 1 + 1 = 2 & 1 + 2 = 0 & 2 + 2 = 1 \end{array}$$

Şimdi 0, 1, 2 rakamlarına daha önce simetri elemanlarının üstlendiği rolü verirsek ve aralarındaki işlemi de toplama olarak belirlersek aşağıdaki “çarpım” tablosunu hemen yazabiliriz.

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Bu tabloyu rakamlar yerine harfler kullanarak tekrar yazabiliriz; bunu yaparken 0’ın etkisiz eleman olan I’nın yerine geçtiğine ($0 = I$) dikkat ederek, 1 ve 2’yi keyfi olarak, $1 = A$ ve $2 = B$ şeklinde tanımlayarak

	I	A	B
I	I	A	B
A	A	B	I
B	B	I	A

elde ederiz. Bunun, Isle of Man’ın ambleminin simetri operasyonlarını inceleyerek bulacağımız çarpım tablosuyla aynı olduğunu artık kolayca doğrulayabilirsiniz. Bu adanın

amblemi birbirlerinden 120° lik açılarla ayrılmış ve ayaklarının birleştiği orta noktada birbirlerine tekme atan üç bacak şeklindedir (başka deyişle yansıma simetrisi olmayan 3'lü döngüsel simetrisi olan bir şekil).

Burada çok ilginç bir şey dikkat çekiyor; farklı iki bağlamda *aynı* grup çarpım tablosu ortaya çıkıyor. Acaba bütün 3. mertebe operasyon gruplarının tabloları hep aynı mıdır ve öyleyse bu "grup"ların temsil ettikleri örneklerin modelleri olma dışında ve onlardan bağımsız olan farklı ve mutlak bir anlamları mı var? Yanıt, evettir ve aynı şey daha önce ele aldığımız 2'nci mertebe gruplar için de doğrudur. Bütün 4'üncü mertebeden gruplar için de bu geçerli midir? Eğer 4-saat aritmetiği ve dik dörtgenin "çarpım" tabloları ile bunu kontrol ederseniz yanıtın hayır olduğunu görürsünüz. Ancak mertebesi 4 olan sadece iki farklı grup vardır ve onları üreten de yukarıda söz edilen örneklerdir.

Daha yüksek mertebelerin çarpım tablolarını incelediğimizde, bu "nesneler"in, genel bir anlamda simetriyle ilgili oldukları halde herhangi belirli bir içerikten bağımsız olan ve onların dışında bir varlıkları olduğunu anlıyoruz. Bir matematikçi bu tablolara baktığında sadece oradaki düzeni görür. Onun için önemli olan yalnızca işlemler grubunun yapısıdır. İşlemlerin türü veya elemanlar değil bunların ne şekilde bağlantılı oldukları önemlidir. Öyleyse tümüyle soyut öğelerle bir "grup" tanımlamak ve çarpım tablolarının düzenine yansıyan bir tür "süper matematik" yaratmak mümkündür. "grup teorisi" denilen süper matematik sadece dört kuralla tanımlanır.

(1) Bir "grup", A, B, C...vb elemanlardan oluşan bir kümedir, bu elemanlar birbirleriyle birleştirilebilirler. Herhangi bir elemanın birleşimi olan AB de grubun bir elemanıdır.

(2) Elemanlardan biri, I, "olduğun gibi kal" veya etkisiz elemandır; gruptaki bütün A elemanları için $IA = AI = A$ 'dır.

(3) Gruptaki her A elemanı için $AA^{-1} = A^{-1}A = I$ olacak şekilde bir A^{-1} elemanı vardır.

(4) Gruptaki tüm A, B, C elemanları için; $A(BC) = (AB)C$, buradaki parantez "önce o iki elemanı birleştir" anlamına gelir.

Daha önce gördüğümüz örneklerin, tümüyle soyut olan bu kuralları sağladığını artık kolayca kontrol edebilirsiniz. Süper matematikçi, A, B, C, vb. elemanlarını gerçek fiziksel işlemlerle ilintilemeden, bu kuralları kullanarak belirli bir mertebede kaç grup (yani çarpım tablosu) olacağını bulabilir. Bunun listesinin başlangıcı aşağıdaki gibidir.

Mertebe	Grup sayısı
1	1
2	1
3	1
4	2
5	1
6	2
7	1
8	5
9	2
10	2
11	1
12	5

Her grup kendine özgü “kişiliği” olan tek bir matematiksel nesnedir ve grup teorisi konusunda çalışanlar onlarla yakın dostluk kurar ve onlara özel isimler verirler. Onların gerçek önemi çok daha derinlere gider. Çünkü nasıl ki aritmetikte her tamsayı tek bir şekilde asal çarpanlara ayrılabilir (örneğin, $60 = 2 \times 2 \times 3 \times 5$), her grup da bir anlamda, “çarpanlara” ayrılabilir. Bazı grupların içinde daha küçük gruplar vardır; öyle ki grup, bu küçük grupların “çarpımı” olarak ifade edilebilir. Öyleyse grup teorisinin “asal sayıları”, sadece kendilerine ve özdeşlik elemanı 1’ya ayrılabilen gruplardır. Bunlar grup teorisinin yapı taşlarıdır ve “sonlu mertebeden basit gruplar” olarak adlandırılırlar. Onları tümüyle sınıflandırma çabası, yüzyılı aşkın bir süre sonunda ancak 1980’lerin ortasında tamamlanmıştır.

Bu iş için gereken çabanın boyutu, nihai ispatın 500'den fazla teknik dergide yayınlanmış 10.000 sayfadan fazla basılmış yayın içermesinden anlaşılabilir. Bu çalışmaların çoğunluğu 1940'ların sonları ile 1980'lerin başlarında yapılmış ve 100'den fazla matematikçinin çabasıyla gerçekleşmiştir. Bütün bu çalışmalar tekrar gözden geçirilip , özetlendikten sonra bile sonucun 1000 sayfadan fazla bir metin içermesi beklenmektedir.

Sonsuz sayıda, sonlu mertebeden basit grup olmasına şaşırmamak gerekir; çünkü asal sayıların sayısı da sonsuzdur. Ancak grup teorisinin problemleri daha karmaşıktır; çünkü birden fazla sonsuz grup aileleri olmasının yanında, bu sonsuz grup ailelerinin hiçbirisine uymayan ("ayrık" denilen) bazı gruplar da bulunmaktadır. Sonsuz ailelerin en basit örneği, bir asal sayı kadar elemanı olan saat-sayı gruplarıdır; başka deyişle $n = 2, 3, 5, 7, 11, 13$ vb. olmak koşuluyla n -saat grupları. Bunların dışındaki sonsuz basit grup ailesini ayrıntılarıyla sınıflandırmak daha zordur; ancak sonunda bu tür 17 aile daha oluşturulmuştur ve artık bu 18 aile ile listenin tamamlanmış olduğu bilinmektedir.

Ayrık basit grupların ilk beşi, daha 1860'larda bulunmuştu. Bunların en küçüğünün mertebesi 7920, diğerlerinin ise sırayla 95.040, 443.520, 10.200.960 ve 244.823.040'dır. Bunların önemsiz olmadığı ortadaydı; çünkü bir yüzyıl boyunca bilinen yegane basit ayrık gruplar olarak kaldılar. Daha sonra, 1966'da o zaman Avustralya'daki Monash Üniversitesi'nde görev yapan Zvonimir Janako altıncıyı keşfetti ve bu, ayrıkların modern çağı diyebileceğimiz dönemi başlattı. Ondan sonra da 1970'lerin sonlarına kadar bu acaip yeni ayrık yaratıklar nerdeyse her yıl birer birer ortaya çıkmaya başladılar. Büyüklükleri gerçekten çok etkileyiciydi, bir çoğunun 1010'dan fazla elemanı vardı. 1982'de zirveye erişildi; Princeton'daki Institute of Advanced Study'den Robert Griess Jr. o zamana kadar bulunanlardan çok çok daha büyük bir ayrık grup inşa etmeyi başardı. Büyüklüğü nedeniyle ona "canavar" deniliyordu.

Eleman sayısı 808.017.424.794.512.875.886.459.904.961.710.757.005.754.368.000.000.000'dan az değildi; bu sayı yaklaşık 8×10^{53} dür, bu nedenle de çarpım tablosunda 6×10^{107} konum bulunmaktadır. Var olan en büyük ayrık grup olduğu bilinmektedir ve çok etkileyici bir şeyin simetri özelliklerini temsil ettiği kuşku götürmez. Bu bir şey nedir? Bu bir şey, XIII. Bölüm'de tartıştığımız 24 boyutlu katlı kafes paketlenmesi olan L_{24} 'ün simetrik özellikleriyle çok yakından ilişkilidir.

Sonuçta keşfedilen ayrık grup sayısı 26'dır, bunların en büyüğü de canavardır. İkinci en büyük yani "canavar yavrusu"nun 4×10^{33} kadar elemanı var. Bu da çok büyük, bir sayıdır; ancak yine de merteye bakımından canavarın kendisinden 10^{20} kat daha küçüktür. En küçük ayrık, daha önce değindiğimiz 7920 elemanlı gruptur. *Bütün* basit sonlu grupların tam olarak sınıflandırılması hakkındaki son teorem sadece 26 ayrık örneğinin var olduğunu iddia etmektedir; sonsuz grup ailelerinin bir parçası olarak sınıflandırılmaktan kaçınan sadece 26 başı boş grup. Bunlar ve daha önce söz ettiğimiz 18 sonsuz aile, grup teorisinin, ya da başka deyişle en genel ve soyut anlamda simetrinin nihai yapı taşlarının oluştururlar.

Öyleyse grup teorisi, bir anlamda, olgunluğa erişmiştir. Ancak bütün bunlar nasıl başladı? Simetri gruplarının icadı, genellikle, 21 yaşındayken anlamsız bir "şeref düellosu"nda tabancayla vurularak ölen, bir matematik harikası genç Fransız dâhi Evariste Galois'ya atfedilir. 1811'de doğmuş olan Galois, Gauss'dan 34 yaş küçüktü, ama saygın Gauss ondan sonra nerdeyse çeyrek yüzyıl daha yaşadı. Günümüzde parçacık fiziğinden Rubik küpüne uzanan simetrilerin anlaşılmasını sağlayan bu matematik dalını yaratmaya başladığında Evariste Galois, on yedi yaşına henüz basmıştı. En ünlü çalışması kendinden önce gelen matematikçilerin neden sadece çok az birkaç tür cebirsel denklem için genel çözüm bulabildiklerini anlama çabasına yönelikti.

Cebirsel denklemler aşağıdakiler gibi denklemlerdir:

$$x + 2 = 5$$

$$x^2 - 4x + 11 = 0$$

$$x^3 + 2x^2 - 6x - 2 = 0$$

$$2x^4 + x^3 + 5x - 7 = 0$$

$$3x^5 - x^4 - 5x^3 + 2x^2 - 7 = 0$$

“Bilinmeyen” x ’in tamsayı katsayılı (bunlardan bazıları sıfır olabilir), tamsayı kuvvetlerinden oluşan denklemler. İçerilen en büyük x kuvvetine denklemin “derecesi” denir, öyleyse yukardaki denklemlerin dereceleri birden beşe kadar sıralanır. Herhangi bir dereceden (örneğin dört) olan en genel denklem

$$Ax^4 + Bx^3 + Cx^2 + Dx + E = 0$$

şeklinde yazılabilir, burada A, B, C, D ve E herhangi bir tamsayı olabilir. Yanıtlanması gereken soru şudur: Bu denklem $x = (A, B, C, D, E)$ ’yi içeren ve bunları temel aritmetik işlemleri olan $+, -, \div, \times$, kuvvetler ve köklerle birleştiren bir ifade) şeklinde çözülebilir mi? Galois’nın döneminde, bir ile dört arasındaki derecelerdeki en genel denklemler için yanıtın “evet” olduğu biliniyordu. Ancak beş ve daha büyük dereceler için yanıt bilinmiyordu.

Birinci ve ikinci dereceler için genel yanıtlar Babillilerden beri bilinmekteydi ve bütün lise cebir kitaplarında yer alıyordu. “Kübik” (üçüncü derece) ve “kuartik” (dördüncü derece) için genel çözüm 16. yüzyılda elde edilmişti. 1820 yılında, Galois bu problemi ele aldığı sırada, genel beşinci derece denklemi “çözmek” için birçok büyük matematikçi, nesiller boyu, 300 yıla yakın bir süre başarı elde edemedен uğraşmıştı.

Galois 17 yaşındayken beşinci dereceden denklemlerin çözümlerini hesaplama konusunda ilk makalesini yazdı. Daha sonraki iki yılda “grup” kavramını ortaya koydu. Bu onun, denklemlerdeki simetri özellikleri nedeniyle, farklı türden

cebirsel denklemlerin çözümleri arasında var olması gereken ilişkileri sistemli bir biçimde bulmasını sağladı. Onun elde ettiği gruplar (onun anısına bunlara Galois grupları denilmektedir) derecesi dörtten büyük olan hiçbir denklemin aranılan biçimde bir genel çözümü olmadığını açıkça gösteriyordu. Genel beşinci derece denklemi çözmek için verilen 300 yıllık çabanın sonuçsuz kalması için iyi bir neden vardı, çünkü çözüm yoktu. Bazı özel beşinci derece denklemler için (A, B, C, D, E sayılarının bazı belirli değerleri için) çözüm elbette vardı; ancak bu çözümler cebirsel yolla değil sayısal yolla bulunabilirlerdi.

Simetri grupları kavramını kullanarak Galois, sadece beşinci derece denklemleri “halletmek”le yetinmemişti; yöntem o denli güçlüydü ki herhangi bir dereceden genel cebirsel denklem için benzer probleme de uygulanabilirdi. “Simetri”nin gücü ilk defa çarpıcı biçimde gösterilmişti. Galois grubu simetriler doğrudan geometri ile ilgili olmasalar da yansımalar ve dönmeler gibi, kesin olarak belirlidirler. Ancak Galois, çağının o kadar önündeydi ki çalışmasının öneminin tümüyle fark edilmesi uzun bir süre almıştır. Eğer Galois’ın ömrü o kadar kısa olmasaydı bu süre belkide çok daha kısa olacaktı. Cebir, bir anlamda Galois tarafından özgür kılınmıştır. Odak noktası, belirli problemlerden genellemelere ve soyutlamalara kaymıştır. “Modern cebir” veya “soyut cebir”in yolunu açmıştır; bu cebir hem işlemlerin hemde onların uygulandıkları niceliklerin soyut olduğu bir süper matematiktir. Geride sadece şekiller kalmıştır (Cheshire kedisinin* gülümsemesi gibi); grup teorisini oluşturan ve kaçınılmaz olarak “canavar” a yol açan şekiller.

* *Alice Harikalar Diyarı* adlı kitaptaki gülümseyen ve gittiğinde geride gülümsemesi kalan kedi. (ç. n.)

Ek Okumalar

- BARNETTE, D. W., 1984; *Map Coloring, Polyhedra and the Four Color Problem* (Washington, DC: Mathematical Association of America)
- BARNSELY, M. F., 1988; *Fractals Everywhere* (San Diego, CA: Academic)
- BROOK, R. J., 1986; *The Fascination of Statistics* (New York: Marcel Dekker)
- CONWAY, J. H. and SLOANE, N. J. A., 1988; *Sphere Packings, Lattices and Groups* (Berlin: Springer)
- CROWE, D. K. and CROWE, D. W., 1988; *Symmetries of Culture* (Seattle, WA: Washington University Press)
- EYNDEN, C. V. 1986; *Elementary Number Theory* (New York: Random House)
- GLEICK, J., 1987; *Chaos, Making a New Science* (New York: Viking)
- GRUNBAUM, B. and SHEPHARD, G. C., 1986; *Tilings and Patterns* (San Francisco: W H Freeman)
- HOGGATT, V. E., 1969; *Fibonacci and Lucas Numbers* (Boston, Mass: Houghton-Mifflin)
- LOWRY, R., 1989; *The Architecture of Change* (Oxford: Oxford University Press)
- MANDELBROT, B. B., 1982; *Fractal Geometry of Nature* (San Francisco: W H Freeman)
- ROSEN, K. H., 1988; *Elementary Number Theory and its Applications*, ikinci baskı (Reading, Mass.: Addison Wesley)
- ROSENFELD, B. A., 1988; *A History of Non-Euclidean Geometry* (Berlin: Springer)
- RUCKER, R. 1977; *Geometry, Relativity and the Fourth Dimension* (New York: Dover)
- 1984; *The Fourth Dimension: Toward a Geometry of Higher Reality* (Boston, Mass: Houghton-Mifflin)
- VAN TILBORG, H. C. A., 1988 *Introduction to Cryptology* (Norwell, Mass.: Kluwer)
- WELSH, D., 1988; *Codes and Cryptography* (Oxford: Oxford University Press)

Dizin

- Abel, R., 106
 Abese indirgeme, 133
 Aksiyomlar, 72, 73, 76
 Algoritma, 19, 116, 124, 165-168, 174
 Altın oran, 12, 16-22, 25, 26
 Altın sarmal, 19, 27
 Anahtarlar (kodlama), 106-109
 Analitik, II, 185, 186, 187
 Appel, K., 137-140
 Aristoteles, 140, 173, 174
 Asal Çarpanlar, 2, 3, 115-118
 Asal sayılar, 2, 3, 95-99, 109, 115-117, 119, 122, 218, 219
 Asimetrik kodlar, 113
 Ayçiçekleri, 13, 16
 Ayrık gruplar, 219

 Basit kusursuz kare, 63-65
 Bellows, George, 19
 Bernoulli, D., 43
 Bidon doldurma, 163, 164, 166
 Bileşik karelenmiş dikdörtgen, 63-65
 Bileşik kusursuz kare, 61-63
 Bileşik sayı, 3, 97
 Bilgisayar güvenliği, 115, 116
 Bilinmeyen transfer, 127, 128
 Blum, M., 126
 Bolyai, J., 79
 Boyut, 2, 9, 17, 18, 20, 55, 57, 58, 60, 63, 74-83, 93, 116, 152, 163, 169-176

 C-net, 59-61
 Canavar, 209, 220, 222
 Carmichael Sayı, 96
 Cebirin temel teoremi, 92

 Cins (genus), 140, 141
 Collatz, L., 29
 Cook, S., 161, 162
 Cunningham sayıları, 122

 Çam kozalakları, 1
 Çarpan, 2, 3, 26, 37, 39, 93, 98, 109, 112, 113, 115-128, 150, 197, 202, 218
 Çarpanlara ayırma, 113, 116-127, 197
 Çarpım, 2, 3, 4, 55, 93, 94, 96, 97, 109, 112, 116, 117, 123, 125, 210, 211, 215-218, 220
 Çekici, 201, 202, 203

 Dantzig, G., 168
 De Morgan, 130, 131, 132
 Değişmez, 210
 Denklik, 92, 93, 94, 95
 Derecesi (bir denklemin), 221, 222
 Dinamik simetri, 19
 Disraeli, 41, 42, 48, 51
 Dodgson, C. L., 22
 Dolu tanesi sayıları, 29, 30, 31, 32, 38
 Dört-renk problemi, 137
 Duijvestijn, 65
 Durağan nokta,
 Düz doğru, 17, 19, 70, 71, 73-75, 78, 150, 186, 193, 194
 Düzdiyar, 74-82
 Düzenli fraktallar, 191
 Düzgün geometrik cisim, 174

 Einstein, 80, 81, 83
 En kusursuz kare, 57, 59-67
 ENİGMA kodu, 106
 Entropi (kodların), 105, 113

- Eşit-açı sarmal, 20
 Eukleides aksiyomları, 69-72
 Eukleides geometrisi, 76, 79
 Eukleides, 69, 70-83, 174, 176, 185, 188
 Eukleides dışı geometri, 79
- Faktoriyel, 93, 97, 98, 101
 Feigenbaum, M., 207, 208
 Felkel, 119
 Fermat'ın küçük teoremi, 93, 97
 Fermat, 93
 Fırdönen kareler, 20
 Fibonacci sarmalı, 14
 Fibonacci sayıları, 10-14, 20, 22, 24-26
 Fraktal boyut, 188, 191-195
 Fraktallar, 188, 191-196
- Galileo, 139
 Galois, E., 220- 222
 Galton, F., 46
 Gauss, 79, 91-93, 97-99, 118, 170, 220
 Genus, bkz. Cins
 Gezgin satıcı problemi, 162, 164
 Gizli mesajlar, 54, 55, 102, 108
 Golomb cetvelleri, 147, 148
 Golomb, S., 152
 Görecelik, 69, 80, 83
 Gösterimler, 213, 214
 Graham, R., 155
 Gregory, D., 172
 Griess, R. Jr., 219
 Gruplar, 53, 108, 111, 127, 137, 138, 153, 214, 215, 217-222
 Guthrie, F., 130
- Haken, W., 137, 139, 140
 Hausdorff, F., 188
 Heawood, P., 140, 141
- İrrasyonel, 12, 22, 25, 26, 76, 170
 İkinci sınıf uğursuzluğu, 46
 İndirgenabilirlik (haritalar), 131-140
 İstatistik, 41, 42, 46-54, 92, 102, 106, 107, 191, 195
- Janko, Z., 219
- Kafes paketleme, 176-178, 220
 Kaos, II, 197, 199, 200, 204-208
 Kare paketleme, 183, 184
 Karekök, 5, 6, 55, 117, 170, 187
 Kareli dikdörtgenler, 59-61, 65
 Kareyi kareleme, 57-59, 62
 Karmakar, N., 168
 Karmaşıklık faktörü, 51
 Kempe, A., 132-135, 140
 Koch kartanesi, 188, 190, 191
 Kodlar, 103, 113
 Kriptografi, 101, 109, 113, 118, 119
 Kulik, 120
 Kusursuz cetvel, 144, 145
 Kusursuz kare, 57-67
 Kutsal kesit, 1, 62-65, 67
 Kuvvet (üs), 3, 4, 80, 111, 130
 Küpü Küplendirme, 67
 Küre paketleme, 171, 174
- Lagrange, 73, 99
 Leech, J., 178
 Lehmer, D. H., 121-123
 Leibnitz, Gottfried von, 98
 Lenstra, H., 118, 124
 Lewis Carroll paradoksu, 22, 24
 Lloyd, S., 57, 58
 Lobachevski, N., 79
 Lorenz, E., 198, 199, 200
 Lucas sayıları, 15, 16, 25
 Lusin, 58
- Mandelbrot, B., 186-188, 190, 193, 194
 Mertebe (grubun), 59-67, 215, 217-220
 Modüler Aritmetik,
 Momentum (sporda), 48-50
- Newton, I., 80, 81, 172
 Normal modlar, 212-214
 NP Problemleri, 155, 161, 163, 164

Ortalamaya dönüş, 46, 47

Ön merkezli kübik paketleme, 170-175

Öpen sayılar, 171

Örnekleme hataları, 51

Paketleme oranı, 169, 170, 176, 182

Peano eğrileri, 193-195

Peano, G., 193

Pi, 55, 76

Piyango, (şans oyunları), 44, 45

Planlama problemleri, 160, 161-163

Plato, 174

Playfair, J., 71

Poisson dağılımı, 54

Poliominolar, 151-153

Pythagoras, 77

Rabin, M., 126

Radyo astronomisi, 144, 149

Randomness,

Rasgele anahtarlı kodlar,

Rasgele fraktallar, 191, 195

Rasgele paketleme, 169, 171, 174

Rasgele yoğun paketleme, 169, 170

Rasyonel kesirler, 25

RED and PURPLE kodlar, 106

Riemann, G. B., 80

Saat Sayıları, 85, 90, 92, 93, 97, 99, 111

Sahte-asal sayılar, 96, 97

Sarmallar, 13, 14, 16

SIGABA kodu, 106

Simetri operasyonu, 210, 214

Simetri, 1, 209, 210, 211-217,
220-222

Simetrik kodlar, 113

Simplex algoritması, 168

Sistematik hatalar, 54

Sloane, 178

Sürekli kesir, 20, 21, 22, 25

Şifre, 1, 101-116, 118, 125-128

Tamsayılar, 2, 3, 24, 26, 30, 57, 93, 94

Toplam, 44, 54, 88, 105, 162, 164,
165, 167

Tribonacci sayıları, 26

TYP EX kodu, 106

Ulusal güvenlik, 1, 115, 116, 118

Uzay grupları, 214

Vigenere şifresi, 103, 104, 105

Willcocks, T.H., 62, 63, 64

Wilson, J.C., 64, 98, 99

Wilson teoremi, 98, 99

Yazı tura atma, 43, 48, 127, 128

Yedigen (düzgün), 92

Z Dase, 119

Bir Sayı Tut...

kozalaklardan ayçiçeklerine,
bahçe düzenlemelerinden şifreli mesajlara
doğada ve günlük yaşantımızda
önemli bir yeri olan
sayıların ilginç dünyasını tanıtıyor.
Kolay anlaşılır bir dille
kaleme alınan kitapta
ünlü matematikçileri bile
şaşırtan problemlerin yanı sıra
fraktallar ve kaos gibi
üzerinde tartışılan
konulara da yer veriliyor.



ISBN 975-403-139-8



Fiyatı: 4.000.000 TL (KDV DAHİL)