Ali Nesin

Nesin Yayıncılık Ltd. Şti.künye...

Ali Nesin

Fen Liseleri İçin Matematik 3

Tamsayılar Yapısı

İçindekiler

Önsöz 1

1 Tamsayı Kümesinin Tanımı **3**

2 İşlemler ve Sıralama **7**
2.1 Toplamsal Ters 7
2.2 Toplama 8
2.3 Çarpma 9
2.4 Üs Alma 10
2.5 Çıkarma 11
2.6 Dağılma Özelliği Üzerine 12
2.7 Sıralama 17
2.8 Mutlak Değer 20

3 Tamsayıların Aksiyomları **27**

4 Tamsayılarda Bölme **35**
4.1 Bölme ve Bölünme 35
4.2 Tamsayılarda Kalanlı Bölme 39

5 Bézout Teoremi **47**

6 Asallar üzerine Biraz Daha **57**

7 Aritmetiğin Temel Teoremi **63**

8 En Küçük Ortak Kat **73**

9 Birkaç Diofantus Denklemi **77**
9.1 Doğrusal Diafontos Denklemleri 77
9.2 $x^2 + y^2 = z^2$ Denklemi 80

10 $n\mathbb{Z} + a$ Kümeleri **89**

Kaynakça ve Okuma Listesi **97**

Dizin **99**

Simgeler Dizini **101**

Önsöz

Ali Nesin / 20 Kasım 2017

Önceki kitapta [2. Kitap] doğal sayılarla ve doğal sayıların toplama ve çarpma işlemleriyle ve sıralama ilişkisiyle tanışmıştık. Bu kitapta tamsayılarla tanışacağız.

İlk iki bölümde tamsayıları oldukça yapay ve biçimsel bir biçimde tanımlayıp bazı temel özelliklerini göreceğiz. Okur, tamsayıları geçmiş yıllardan bildiğinden, sıkıcı olmamak için çok fazla ayrıntıya girmeyeceğiz. Ama üçüncü bölümde tamsayıları yeniden, en baştan ve bambaşka bir bakış açısıyla ele alacağız. Üçüncü bölümde tamsayıları tanımlamayacağız, sadece tamsayıların toplama, çarpma ve sıralamaya dair aksiyomlarını, yani hiç tartışmadan kabul ettiğimiz özelliklerini yazıp, tamsayıların diğer özelliklerini bu aksiyomlardan hareketle kanıtlayacağız. Yani üçüncü bölümde yaklaşımımız "aksiyomatik" olacak. Umarım okur ilk iki bölümü sıkıcı, üçüncü bölümü heyecanlı bulur.

Daha sonraki bölümlerde tamsayıların daha ileri düzeyde özelliklerini göreceğiz. Daha çok asallara ve asallığa odaklanacağız. Aritmetiğin Temel Teoremi olarak bilinen, bir doğal sayının asalların çarpımı olarak tek bir biçimde yazılacağı olgusunu kanıtlayacağız elbette, bu çok önemli. Ama okurun (liselerde ne yazık ki hiç konu edilmeyen) Bézout Teoremi'ni es geçmemesi gerekir. Bézout Teoremi olmadan doğal sayılarda ve tamsayılarda fazla ileri gidilemez. Nitekim Bézout Teoremi'nin yardımı olmadan Aritmetiğin Temel Teoremi bile kanıtlanamaz.

Bölüm 9 ve 10 ilk okuyuşta atlanabilir ya da yaz tatilinde okunabilir. Ama diğer tüm bölümler temeldir, hepsinin dikkatlice okunması gerekir.

Kitabı baştan sonra okuyarak birçok değerli düzeltme ve önerilerde bulunan Ali Törün, Mehmet Kıral, ve Mustafa Yağcı ve onlarca öğretmene sonsuz teşekkürler.

1. Tamsayı Kümesinin Tanımı

Doğal sayılarda toplama ve çarpma gibi iki işlem olduğunu biliyoruz, yani iki doğal sayının toplamının ve çarpımının gene bir doğal sayı olduğunu biliyoruz. Ama doğal sayılarda çıkarma işlemi yapılamaz, bazen yapılabilse de her zaman yapılamaz, örneğin doğal sayılarda 12'den 7'yi çıkarabiliriz ama 7'den 12'yi çıkaramayız, çünkü 5 bir doğal sayıdır ama -5 bir doğal sayı değildir. Yani doğal sayılarda çıkarma işlemi tam bir işlem değildir, olsa olsa "kısmi" bir işlemdir, bazen yapılır bazen yapılmaz.

Doğal sayılarda, toplamayı kullanarak "kısmi" bir çıkarma işlemini şu yöntemle tanımlayabiliriz: a ve b herhangi iki doğal sayı olsun. Eğer

$$a + x = b$$

eşitliğini sağlayan bir x doğal sayısı varsa, bu x doğal sayısı bir tanedir, bu eşitliği sağlayan ikinci bir x doğal sayısı daha yoktur (çünkü $a+x = b = a+y$ ise a'ları sadeleştirip $x = y$ buluruz). Yegâne olan bu x sayısını $b - a$ olarak gösterelim. Örneğin $7 + x = 12$ denklemi $x = 5$ için sağlandığından, yani $7+5 = 12$ olduğundan, verdiğimiz tanım gereği $5 = 12-7$ olur. Ve $5+7 = 12$ olduğundan aynı zamanda $12 - 5 = 7$ olur. Böylece doğal sayılarda kısmi bir çıkarma işlemi tanımlanır. Bu işlem tabii ki ilkokuldan beri bildiğimiz çıkarma işlemidir: 12 fasulyeden 7 fasulye çıkarırsak geriye 5 fasulye kalır... Bu bölümde 7 fasulyeden 12 fasulye çıkarma becerisini kazanacağız!

Doğal sayılarda örneğin $12 + x = 7$ denkleminin bir çözümü yoktur, dolayısıyla doğal sayılarda $7 - 12$ anlamına gelebilecek bir sayı yoktur. Doğal sayıların bu kusurunun üstesinden gelmek için her x doğal sayısı için, "eksi x" adını vereceğimiz ve $-x$ olarak göstereceğimiz yepyeni ve gıcır gıcır bir sayı icat ediyoruz (ya da yaratıyoruz), tek bir istisnayla ama:

$$-0 = 0$$

eşitliğini kabul ediyoruz, -0 gıcır gıcır bir sayı olmayacak yani, -0 sayısı bir önceki kitapta [2. Kitap] haşır neşir olduğumuz 0 sayısına eşit olacak. Ve işte kümesi tamsayılar:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Demek ki, tanım gereği, tamsayılar kümesi doğal sayılardan ve doğal sayıların "eksi"lerinden oluşuyor. Bir başka deyişle $\mathbb{N} \subseteq \mathbb{Z}$ oluyor ama $\mathbb{Z}$ kümesinde $\mathbb{N}$'deki sayılar dışında bir de bunların eksileri ya da "negatif"leri var. Bu dediğimizi daha matematiksel bir dille söyleyelim: Eğer

$$-\mathbb{N} = \{0, -1, -2, -3, -4, \dots\}$$

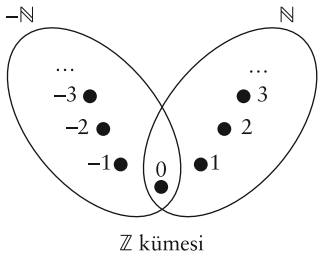
tanımını yaparsak,

$$\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$$

olur. Ayrıca,

$$\mathbb{N} \cap -\mathbb{N} = \{0\}$$

olduğu da belli. Şekil aşağıda.



$\mathbb{Z}$ kümesi

$\mathbb{N} \setminus \{0\}$ kümesindeki sayılara ***pozitif tamsayılar***, $-\mathbb{N} \setminus \{0\}$ kümesindeki sayılara ***negatif tamsayılar*** adı verilir. Örneğin 5 pozitiftir ama -5 negatiftir. 0 sayısı ne pozitif ne de negatiftir.

Tamsayıları biçimsel, yani anlamdan uzak bir biçimde tanımladık. -5 diye bir sayı olsun dedik ve oldu! Matematikçinin amacı budur işte, duyumsadığı dış dünyayı ve evrende olan biteni biçimsel ve tamamen zihinsel bir biçimde kâğıda kaydetmek. Biz de öyle yaptık. Daha fazlasını yapacağız.

Bu bölümün devamında tamsayılarda toplama, çıkarma, çarpma, üs alma gibi işlemlerden ve tamsayıların sıralanmasından bahsedeceğiz.

Notlar

1.1. Tamsayılar kümesinin gösterildiği $\mathbb{Z}$ harfi, Almanca sayılar anlamına gelen "zahlen"in z'sidir. Doğal sayılar kümesinin simgesi olan $\mathbb{N}$ de Batı dillerinde doğal anlamına gelen "natural" kelimesinden ve türevlerinden kaynaklanır.

1.2. Toplama işareti olan + ilk defa 1360'da Nicole Oresme (1323-1382) tarafından kullanılmıştır. + işareti, Latince "ve" anlamına gelen *et* kelimesinden üretilmiştir. (*et* kelimesinden üretilen bir başka işaret gene "ve" anlamına gelen & işaretidir.)

Fransız Nicole Oresme Ortaçağ'ın en ilginç düşünürlerindendi. Ekonomi, matematik (olasılık, koordinat sistemi), fizik (optik ve mekanik), astronomi, felsefe, din ve astroloji gibi çok çeşitli konularda önemli etkisi olmuştur. Fransız kralı Charles V'in yakın dostu ve danışmanıydı. Astronomide çağdaşlarının birçoğu gibi yıldızların, planetlerin, güneşin ve dünyanın hareketi üzerine düşünmüştür. **Gökyüzünün ve Dünya'nın Kitabı** adlı

eserinde, Aristo'nun iddiasının aksine, dünyanın sabit olmayabileceği düşüncesiyle uzun süre boğuşmuş, örneğin dünyanın kendi etrafında dönmesinin Doğu'dan Batı'ya doğru esen korkunç boyutlarda bir rüzgara neden olacağı, dolayısıyla dünyanın dönemeyeceği düşüncesinin saçma olduğunu ve aslında devasa yıldız ordusunun dünyanın etrafında dönmesindense, dünyanın kendi etrafında dönmesinin daha kolay ve ekonomik olacağı, bunun için daha az enerji gerektiğini söylemiştir. Yani kendisinden 200 yıl sonra yaşamış olan Kopernik'in keşfettiğini keşfetmesine ramak kalmıştır. Ne yazık ki dünyanın bal gibi de dönebileceğine dair uzun tartışmalarını, belki de, hatta muhtemelen Kilise'den çekinerek, diğer birçok bilgin gibi kendisinin de, dünyanın değil, yıldızların dünyanın etrafında döndüğünü düşündüğünü yazarak sonlandırmıştır.

1.3. Eksi işareti ilk kez 1489 yılında Alman matematikçi Johannes Widmann tarafından ticaret aritmetiğini konu eden bir kitabında kullanılmıştır. Kitaptan bir sayfa aşağıda. Tahmin edileceği üzere Widmann eksi işaretini borcu ya da zararı göstermek için kullanmıştır. Daha önce, örneğin, $x^3 - 3x + 5 = 0$ yazılmaz, $x^3 + 5 = 3x$ yazılırdı.

Johannes Widman'ın kitabından bir sayfa.
Eksiler biraz fazla uzun...

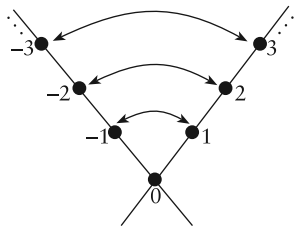
Almanya'da + ve − işaretleri kullanılırken, Fransa ve İtalya'da bu simgeler yerine p ve m harfleri kullanılıyordu, p "plus" için, m "minus" için. İşaret savaşı Almanya'yla diğer Avrupa ülkeleri arasında bir yüzyıldan fazla devam etti. Almanlar p ve m harflerini hiçbir zaman kabullenmediler, ama + ve − yavaş yavaş Avrupa'nın diğer ülkelerine yerleşti. Nedendir bilmiyorum, + ve − simgelerine en uzun süre direnen İspanya olmuş. Matematiksel simgeler için harf kullanmak bir gelenekti, ama bu harfler sayılar için kullanılan simgelerle karışıyordu, örneğin çarpmanın simgesi olan × simgesi elle yazıldığında x ile karışabilir, bu yüzden × yerine · kullanılır, hatta hiçbir şey yazılmaz.

2. İşlemler ve Sıralama

Bölüm 3'te tamsayılar üzerine tanımlanan toplama, çıkarma, çarpma ve sıralamayı çok daha matematiksel olarak (yani aksiyomatik olarak) ele alacağız. Burada sadece okurun geçmiş bilgilerini tazelemeyi amaçlıyoruz. Yeni bir anlatım biçimiyle karşılaştığınızdan, bu bölümü okurken, konuyu matematiksel olarak ele aldığımız kanısına varabilirsiniz, aldanmayın! Asıl matematiği bir sonraki bölümde göreceksiniz.

2.1 Toplamsal Ters

Tamsayıların ***toplamsal tersleri*** şöyle tanımlanır: Bir $n \in \mathbb{N}$ doğal sayısının toplamsal tersi $-n$ tamsayısıdır ve $-n$ tamsayısının toplamsal tersi n doğal sayısıdır.



Toplamsal ters işlemi

Tanıma göre, 0'ın toplamsal tersi -0, yani 0'dır. Örneğin 5'in toplamsal tersi -5 ve -5'in toplamsal tersi de 5'tir.

Doğal sayı olsun ya da olmasın, bir n tamsayısının toplamsal tersi $-n$ olarak yazılır; mesela -5'in toplamsal tersi $-(-5)$ olarak yazılır. Dolayısıyla, tanım gereği, $-(-5) = 5$ olur. Daha genel olarak, her n tamsayısı için

$$-(-n) = n$$

eşitliği doğrudur, bir başka deyişle bir tamsayının toplamsal tersinin toplamsal tersi tamsayının kendisidir; örneğin

$$-(-5) = 5 \text{ ve } -(-(-5)) = -5$$

olur. Demek ki peşpeşe gelen iki eksi işareti gereksizdir, ikisi birden silinebilir. Daha devam edecek olursak,

$$-(-(-(-5))) = -(-5) = 5$$

eşitliğini elde ederiz.

2.2 Toplama

$\mathbb{N}$ kümesinde olduğu gibi $\mathbb{Z}$ kümesinde de toplama ve çarpma işlemleri tanımlanabilir. Okurun zaten önceki yıllardan aldığı eğitimden bildiklerini uzun uzun tekrarlamayacağız, sadece birkaç örnek vermekle yetineceğiz. Önce toplama örnekleri:

$$\begin{aligned}
7+5 &= 12,\\
7+(-5) &= 2,\\
(-7)+5 &= -2,\\
5+(-7) &= -2,\\
(-5)+7 &= 2,\\
(-5)+(-7) &= -12,\\
(-5)+5 &= 0,\\
5+(-5) &= 0.
\end{aligned}$$

0, toplamanın etkisiz ögesidir, yani her $x \in \mathbb{Z}$ için

$$x + 0 = 0 + x = x$$

olur.

$$x + y = y + x \text{ ve } x + (y + z) = (x + y) + z$$

gibi okurun önceki yıllardan bildiği eşitlikler de doğrudur, ama bunların sıkıcı ve pek yaratıcı olmayan kanıtlarını vermeyeceğiz. Birinci eşitlik (yani değişme özelliği) sayesinde tamsayıları hangi sırayla topladığımızın önemi olmadığı ve ikinci eşitlik (yani birleşme özelliği) sayesinde tamsayıları toplarken parantezlere ihtiyacımızın olmadığı çıkar. Örneğin $((y + z) + x) + (t + s)$ yerine çok daha basit olarak $x + y + z + t + s$ yazabiliriz.

Her x tamsayısını toplamsal tersi olan $-x$ ile toplarsak 0 elde ederiz, yani her $x \in \mathbb{Z}$ için

$$x + (-x) = (-x) + x = 0$$

olur.

Toplamada sadeleştirme de mümkündür: $a + x = b + x$ ise $a = b$ olur.

Alıştırmalar

2.1. $\{x + x : x \in \mathbb{Z}\}$ kümesinin 5 ögesini bulun.

2.2. $\{x + x : x \in \mathbb{Z} \setminus \mathbb{N}\}$ kümesinin 3 ögesini bulun.

2.3. $\{x + (-x) : x \in \mathbb{Z}\}$ kümesinin kaç ögesi vardır?

2.4. $\{(x + x) + (-x) : x \in \mathbb{Z}\} = \mathbb{Z}$ eşitliğini kanıtlayın.

2.5. $\{x + 2 : x \in \mathbb{Z}\} = \mathbb{Z}$ eşitliğini kanıtlayın.
2.6. $a \in \mathbb{Z}$ sabit bir tamsayı olsun. $\{x + a : x \in \mathbb{Z}\} = \mathbb{Z}$ eşitliğini kanıtlayın.
2.7. $a \in \mathbb{Z}$ sabit bir tamsayı olsun. $\{(x + x) + a : x \in \mathbb{Z}\} \neq \mathbb{Z}$ eşitsizliğini kanıtlayın.
2.8. $A = \{0, 1\}$ olsun. $\{(x + x) + a : x \in \mathbb{Z},\ a \in A\} = \mathbb{Z}$ eşitliğini kanıtlayın.
2.9. $A = \{3, 8\}$ olsun. $\{(x + x) + a : x \in \mathbb{Z},\ a \in A\} = \mathbb{Z}$ eşitliğini kanıtlayın.
2.10. $A = \{3, 7\}$ olsun. $\{(x + x) + a : x \in \mathbb{Z},\ a \in A\} = \mathbb{Z}$ eşitliği doğru mudur?
2.11. $x + y = 1$ denkleminin tamsayılarda kaç çözümü vardır?

2.3 Çarpma

Çarpma işlemine geçelim. x ve y tamsayılarının çarpımı $x \times y$ ya da $x \cdot y$ ya da çok daha basit olarak xy olarak yazılır. Okurun tamsayıları çarpmayı bildiğini varsayarak sadece birkaç çarpma örneği vermekle yetinelim:

$$\begin{array}{lcr} 7 \times 5 & = & 35, \\ 7 \times (-5) & = & -35, \\ (-7) \times 5 & = & -35, \\ (-7) \times (-5) & = & 35. \end{array}$$

Aynen toplamada olduğu gibi, çarpmada da değişme ve birleşme özelliği geçerlidir: Her x, y, $z \in \mathbb{Z}$ için,

$$xy = yx \text{ ve } x(yz) = (xy)z$$

olur. Böylece, tamsayıları hangi sırayla çarptığımızın önemi olmadığı ve parantezlerin gereksiz olduğu anlaşılır. Örneğin $((yz)x)(ts)$ yerine çok daha basit olarak $xyzts$ yazabiliriz.

1, çarpmanın etkisiz ögesidir, yani her $x \in \mathbb{Z}$ için

$$x \times 1 = 1 \times x = x$$

olur. 0 ise çarpmanın yutan ögesidir, yani her $x \in \mathbb{Z}$ için

$$x \times 0 = 0 \times x = 0$$

olur. Bir sayının toplamsal tersini, sayıyı -1 ile çarparak da bulabileceğimizi biliyorsunuzdur:

$$(-1) \times x = -x.$$

Buradan da, x yerine -1 alarak,

$$(-1) \times (-1) = -(-1) = 1$$

buluruz.

Kaydadeğer birkaç özellik daha:

Eğer $xy = 1$ ise ya $x = y = 1$ ya da $x = y = -1$ olur.

Eğer $xy = 0$ ise x ya da y'den en az biri 0 olmak zorundadır.

Eğer $ax = bx$ ise ve $x \neq 0$ ise $a = b$ olur.

$x, y \in \mathbb{Z}$ sayıları için, ne zaman $xy \in \mathbb{N}$ olur? Eğer x ve y birer doğal sayıysa bu olur elbette; ama ayrıca x ve y sayıları $-\mathbb{N}$ kümesinin ögeleriyse de olur. Bir başka deyişle

$$xy \in \mathbb{N} \Longleftrightarrow (x,\, y \in \mathbb{N} \text{ ya da } x,\, y \in -\mathbb{N})$$

eşdeğerliği geçerlidir.

2.4 Üs Alma

Aynen doğal sayılarda olduğu gibi, tamsayılarda da üs alma işlemi vardır. Eğer $n \in \mathbb{N}$ ve $x \in \mathbb{Z}$ ise, $x^0 = 1$ olarak ve eğer $n > 0$ ise x^n sayısı x'i kendisiyle n defa çarpımı olarak tanımlanır, örneğin,

$$x^2 = xx,\ x^3 = xxx,\ x^4 = xxxx = x^2x^2.$$

Daha somut örnekler:

$$(-2)^3 = -8,\ 3^4 = 81,\ (-3)^4 = 81.$$

x^2 sayısına x'in karesi, x^3 sayısına x'in küpü adı verilir. x^4 ise x'in dördüncü kuvveti olarak ifade edilir. Karesi 4 olan tek bir doğal sayı vardır: 2. Ama karesi 4 olan iki tamsayı vardır: 2 ve -2.

0^0 ifadesinin 1 olarak tanımlandığına dikkatinizi çekerim. Bu ifade bazen tanımsız bırakılır, ama biz burada daha ziyade cebir yapıyoruz ve cebirde 0^0 ifadesinin 1 olarak tanımlanmasında yarar vardır.

Doğal sayıların üsleri için geçerli olan tüm özdeşlikler tamsayıların üsleri için de geçerlidir. Örneğin,

$$(xy)^n = x^n y^n,\ x^n x^m = x^{n+m},\ (x^n)^m = x^{nm}.$$

Bu eşitlikler kanıtlanabilir tabii ama şimdi kanıtlamamayı tercih ediyoruz, bir başka kitaba bırakıyoruz.

x^{n^m} ifadesinin iki anlamı olabilir:

$$(x^n)^m \text{ ya da } x^{(n^m)}.$$

Bu iki sayı genellikle birbirine eşit değildir. Birincisi x^{nm} sayısına eşittir, ama ikincisi genellikle değildir. Örneğin $x = 2$, $n = 2$ ve $m = 3$ ise,

$$(x^n)^m = x^{nm} = 2^6 = 64 \text{ ve } x^{(n^m)} = 2^8 = 256$$

olur. Demek ki "üs alma işlemi" birleşme özelliğini sağlamaz.

-1'in kuvvetleri özellikle önemlidir, bahsetmek lazım: Eğer n çift bir doğal sayıysa $(-1)^n = 1$ olur, aksi halde $(-1)^n = -1$ olur. Bu şöyle gösterilir.

$$(-1)^n = \begin{cases} 1 & \text{eğer } n \text{ çift ise} \\ -1 & \text{eğer } n \text{ tek ise} \end{cases}$$

Genel olarak, her $x \in \mathbb{Z}$ için, $x^2 \in \mathbb{N}$ olur, hatta bir tamsayının tüm çift kuvvetleri bir doğal sayıdır, yani her $x \in \mathbb{Z}$ ve her $n \in \mathbb{N}$ için $x^{2n} \in \mathbb{N}$ olur.

Asallara Ayrışma. 0'dan farklı doğal sayıların asalların çarpımı olarak yazıldığını biliyoruz [2. Kitap, Teorem 6.3]. Tamsayılar, doğal sayıların ± 1 çarpımı olduğundan, tamsayıları da ± 1 kere asalların çarpımı olarak yazabiliriz. Örneğin,

$$-3516 = -2^6 \cdot 5 \cdot 141$$

olur. Doğal sayılar da tabii ki eskisi gibi asallara ayrışır:

$$3516 = 2^6 \cdot 5 \cdot 141.$$

Demek ki her n tamsayısı, sonlu sayıda $p_1, \ldots, p_k$ asalı ve aynı sayıda $n_1, \ldots, n_k$ doğal sayısı için,

$$n = s(n) p_1^{n_1} \cdots p_k^{n_k}$$

olarak yazılır. Buradaki $s(n)$, n'nin işaretidir, yani n pozitif bir doğal sayıysa $s(n) = 1$, negatif bir tamsayıysa $s(n) = -1$ olur. p_i asallarını küçükten büyüğe sıralamak gelenektendir. Ayrıca, 0'a eşit olanlarını atarsak, n_i doğal sayılarının pozitif olduklarını varsayabiliriz.

2.5 Çıkarma

Doğal sayılarda da olan bu toplama ve çarpma işlemleri dışında, tamsayılarda bir de doğal sayılarda olmayan çıkarma işlemi vardır. Çıkarma işlemi, toplamsal ters ve toplama işlemleri yardımıyla şöyle tanımlanır:

$$x - y = x + (-y).$$

Örneğin,

$$\begin{aligned} &7 - 5 = 7 + (-5) = 2, \\ &5 - 7 = 5 + (-7) = -2, \\ &7 - (-5) = 7 + (-(-5)) = 7 + 5 = 12, \\ &(-7) - 5 = (-7) + (-5) = -12, \\ &(-7) - (-5) = (-7) + (-(-5)) = (-7) + 5 = -2. \end{aligned}$$

Toplama çıkarma yaparken bazı kısaltmalar yapılır:

$$\begin{array}{lll} (-7)+5 & \text{yerine} & -7+5, \\ (-7)+(-5) & \text{yerine} & -7-5 \end{array}$$

yazılır. x ve y ile ifade edecek olursak:

$$\begin{array}{lll} (-x)+y & \text{yerine} & -x+y, \\ (-x)+(-y) & \text{yerine} & -x-y \end{array}$$

yazılır. Bu eşitlikler sadece x ve y doğal sayıları için değil, tamsayılar için de geçerlidir.

$$x-(y-z)=x-y+z$$

gibi eşitliklere ya da

$$x+y=z \Rightarrow x=z-y$$

gibi önermelere okurun aşina olduğunu biliyoruz, dolayısıyla üstünde durmuyoruz.

Çıkarma işlemi birleşme özelliğini sağlamaz, yani

$$x-(y-z)=(x-y)-z$$

eşitliği her x, y, z tamsayısı için doğru değildir. Bkz. Alıştırma 2.23.

2.6 Dağılma Özelliği Üzerine

Tamsayılarda toplamayla çarpma arasında çok sıkı bir bağ olduğu düşünülebilir ilk bakışta, çünkü ne de olsa pozitif bir n ile bir sayıyı çarpmak o sayıyı kendisiyle n defa toplamak demek, eğer n negatifse n ile çarpmayı toplamayla ifade etmek de çok zor değil. Ama bu his yanıltıcı. Toplamayla çarpma arasındaki yegâne ilişki aslında dağılma özelliği ve dağılma özelliği de çok güçlü bir ilişki değil.

Örneğin dağılma özelliği sayesinde

$$(x-y)(a-b+c)=xa-xb+xc-ya+yb-yc$$

gibi eşitlikler elde ederiz. Aşağıdaki eşitlikler herkesin bilmesi gereken (ve kanıtı gayet kolay) meşhur eşitliklerdir.

$$\begin{array}{l} (x+y)^2=x^2+2xy+y^2 \\ (x-y)^2=x^2-2xy+y^2 \\ (x+y)(x-y)=x^2-y^2 \end{array}$$

Bunlar dağılma ve değişme ($xy=yx$) özelliği kullanılarak kolaylıkla kanıtlanabilir.

Bir başka örnek verelim:

$$(x-1)(y-1) = xy - x - y + 1.$$

Muhtemelen kolay gelmiştir, sonuç olarak $x-1$ ile $y-1$'i çarpıyoruz. Ama diyelim

$$xy - x - y + 1$$

ifadesi verildi ve bizden bu ifadeyi x'li ve y'li iki ifadenin çarpımı olarak yazmamız istendi, yani

$$xy - x - y + 1 = (x-1)(y-1)$$

eşitliğini bulmamız istendi. Bu çok daha zor bir uğraştır. Eğer kolay geldiyse daha zorunu verelim:

$$6xy - 8x - 9y + 12$$

ifadesini "çarpanlarına" ayırabilir misiniz? Pek kolay değil değil mi? Ayırabiliriz ama:

$$6xy - 8x - 9y + 12 = (2x-3)(3y-4).$$

Peki ya

$$24xyz - 30xy - 36yz - 32xz + 40x + 45y + 48z - 60$$

ifadesi verilseydi? Bunu çarpanlarına ayırabilir misiniz? Pes edilmeyecek gibi değil... Cevabı söyleyelim:

$$24xyz - 30xy - 36yz - 32xz + 40x + 45y + 48z - 60 = (2x-3)(3y-4)(4z-5).$$

Zorlandıysanız hiç sorun etmeyin, herkes zorlanır. Mecbur kalmadıkça ben yanından bile geçmem. Bu tür sorular hiç kolay değildir. Çarpmak oldukça kolaydır, biraz sabırla

$$(2x-3)(3y-4)(4z-5)$$

ifadesi dağılma özelliği kullanılarak çarpılıp parantezlerinden arındırılabilir ama $24xyz - 30xy - 9yz - 8xz + 40x + 45y + 12z - 60$ gibi bir ifadeyi çarpanlarına ayırmak daha zordur. Yani aslında bu o kadar zor değil, biraz uğraşınca bulunur ama bundan çok daha çetrefilli ifadeleri çarpanlarına ayırmak bayağı daha zordur.

Örnekler

2.12. Eğer x ve y'yi asal çarpanlarına ayırmışsak ve x ve y'nin büyük bir ortak böleni varsa, $x+y$ ve $x-y$ sayılarını da kolaylıkla asal çarpanlarına ayırabiliriz. Örneğin

$$x = 2^3 3^5 5^2 7^2 \text{ ve } y = 3^6 5^2 11$$

ise

$$x + y = 2^3 3^5 5^2 7^2 + 3^6 5^2 11 = 3^5 5^2 (2^3 7^2 + 3 \cdot 11) = 3^5 5^2 425 = 3^5 5^2 25 \cdot 17 = 3^5 5^4 17$$

ve

$$x - y = 2^3 3^5 5^2 7^2 - 3^6 5^2 11 = 3^5 5^2 (2^3 7^2 - 3 \cdot 11) = 3^5 5^2 359$$

olur. (359 asaldır.)

2.13. Toplamanın şu özelliği önemlidir:

$$x + y = z \text{ ise } x = z - y \text{ olur.}$$

Bu özelliği kanıtlamak için $x + y = z$ eşitliğinin her iki tarafına $-y$ eklemek yeterlidir:

$$x = x + 0 = x + (y + (-y)) = (x + y) + (-y) = z + (-y) = z - y.$$

Benzer şekilde,

$$x + y = z + t \text{ ise } x - t = z - y \text{ olur.}$$

Bu özellikler sayesinde $4x + 7 = 3x + 3$ denklemini çözebiliriz mesela. Bunun için $3x$'i eşitliğin soluna, 7'yi eşitliğin sağına taşıyalım: $4x - 3x = 3 - 7$, yani $4x - 3x = -4$ elde ederiz. Ama $4x - 3x = (4 - 3)x = 1 \cdot x = x$ olduğundan, bundan, $x = -4$ çıkar. Nitekim x yerine -4 koyarsak hem $4x + 7$ hem de $3x + 3$ ifadelerinin değeri -9 olur.

2.14. $12x - 5 = 4x + 11$ denklemini çözelim. Bunun için x'leri bir kenara, sabit sayıları diğer tarafa atalım: $12x - 4x = 11 + 5$, ve buradan da $8x = 16$ ve $x = 2$ elde ederiz. Nitekim x yerine 2 koyarsak, hem $12x - 5$ ifadesi hem de $4x + 11$ ifadesi 19'a eşit olur.

2.15. $5x - 4 = 7x + 3$ denkleminin çözümlerini bulalım. Bu denklemden $2x = -7$ çıkar ve bu son eşitliğin tamsayılarda bir çözümü yoktur. Demek ki $5x - 4 = 7x + 3$ denkleminin de çözümü yoktur.

2.16. $(2x - (3x - y)) - ((z - (2x - 4y)) - ((z - y) - (x + 3z)))$ ifadesini sadeleştirelim:

$$\begin{aligned}
&(2x - (3x - y)) - ((z - (2x - 4y)) - ((z - y) - (x + 3z))) \\
&\quad = (2x - 3x + y) \quad - ((z - 2x + 4y) \quad - (z - y \quad - x - 3z)) \\
&\quad = (2x - 3x + y) \quad - (z - 2x + 4y \quad\quad - z + y + x + 3z) \\
&\quad = (2x - 3x + y) \quad - (-x + 5y + 3z) \\
&\quad = 2x - 3x + y \quad\quad + x - 5y - 3z \\
&\quad = -4y - 3z.
\end{aligned}$$

2.17. $(3x - 2)(4y - 7) = 1$ denkleminin tamsayılarda çözümlerini bulalım. Bu eşitliğin doğru olması için, parantez içindeki ifadelerin ikisi birden ya 1'e ya da -1'e eşit olmalıdır.
Önce birinci durumu ele alalım: $3x - 2 = 1 = 4y - 7$ ise $x = 1$ ve $y = 2$ olmalı. İkinci durum: $3x - 2 = -1 = 4y - 7$, yani $3x = 1$ ve $4y = 6$; bu durumda çözüm yoktur. Demek ki $(3x - 2)(4y - 7) = 1$ denkleminin tamsayılarda tek bir çözümü vardır: $x = 1$ ve $y = 2$.

2.18. $(3x - 2)(4y - 7) = -1$ denkleminin tamsayılarda çözümlerini bulalım. Bu eşitliğin doğru olması için, parantez içindeki ifadelerin biri 1'e diğeri -1'e eşit olmalıdır.
Önce $3x - 2 = 1$ ve $4y - 7 = -1$ durumunu ele alalım. Bu durumda $x = 1$ ve $4y = 6$ olur. $4y = 6$ denkleminin tamsayılarda bir çözümü olmadığından, bu durumda sistem çözülemez. Şimdi de $3x - 2 = -1$ ve $4y - 7 = 1$ durumunu ele alalım. Bu sefer ikinci denklemin çözümü var ama birincisinin yok. Sonuç olarak $(3x - 2)(4y - 7) = -1$ denkleminin tamsayılarda çözümü yoktur.

Bu örnekler kolay gelmiş olmalı. Aşağıdaki alıştırmalar da muhtemelen kolay gelecektir. Birazdan çok daha zor sorulara rastlayacağız, bunları ısınma hareketleri olarak addedebilirsiniz. Daha zor bir soru istiyorsanız, $3x - 2 = 7y + 4$ denkleminin tamsayılardaki (ya da doğal sayılardaki) **tüm** çözümlerini bulmaya çalışabilirsiniz; örneğin $x = -12$, $y = -6$ bu çözümlerden biridir, ama başkaları da vardır.

Alıştırmalar

2.19. $x = 2^4 3^5 5^6$ ve $y = 2^5 3^3 5^4$ ise $x + y$ ve $x - y$ sayılarını asallarına ayırın.

2.20. $x = 2^4 3^5 5^6$ ve $y = 2^5 3^3 5^4$ ise $6x + 8y$ ve $4x - 9y$ sayılarını asallarına ayırın.

2.21. $x = 2^4 3^5 5^6$, $y = 2^5 3^3 5^4$ ve $z = 2^3 3^4 5^5$ ise $x + y + z$, $x - y - 2z$ ve $xy - z^2$ sayılarını asallarına ayırın.

2.22. "İki sayının toplamının toplamsal tersi, sayıların toplamsal terslerinin toplamına eşittir" ifadesini matematiksel dilde ifade edin.

2.23. Toplama işleminin birleşme özelliği vardır, yani $x + (y + z) = (x + y) + z$ olur. Çarpma işleminin de birleşme özelliği vardır: $(xy)z = x(yz)$. Çıkarma işleminin birleşme özelliği var mıdır? Yoktur. Nitekim $x - (y - z) = (x - y) - z$ eşitliği ancak $z = 0$ için doğrudur. Bunu kanıtlayın.

2.24. Bir n tamsayısı için $(1 - 3n)(n + 3)$ biçiminde yazılan tüm asal sayıları bulun.

2.25. Bir n tamsayısı için $3n^2 + 4n + 1$ türünden yazılan tek bir asal olduğunu kanıtlayın. Bu asalı bulun.

2.26. $(x - (y - x + (x - y))) - (y - 2x + (-y + x))$ ifadesini sadeleştirin.

2.27. $(x - (-y - 3x - (2x - y))) - (3y - 2x - (-y - x))$ ifadesini sadeleştirin.

2.28. $x - ((-y - 3x - (2x - y)) - (3y - 2x - (-y - x)))$ ifadesini sadeleştirin.

2.29. $2(x - (y - x + (x - y))) - 3(y - 2x + (-y + x))$ ifadesini sadeleştirin.

2.30. $(2x - (3x + y)) - ((z - (2x - 4y)) - ((z - y) - (x - 3z)))$ ifadesini sadeleştirin.

2.31. $2(x - 3(y - x + 4(x - y))) - 5(y - 2x + 2(-y + x))$ ifadesini sadeleştirin.

2.32. $(x - y)(x + z) - (x + y)(x - z) + (y + z)(x - y)$ ifadesini sadeleştirin.

2.33. $3x - 2 = 4x - 6$ denklemini tamsayılarda çözün.

2.34. $3x - 10 = 4x - 6$ denklemini tamsayılarda çözün.

2.35. $-2x - 2 = -x - 6$ denklemini tamsayılarda çözün.

2.36. $-2x - 10 = -x - 6$ denklemini tamsayılarda çözün.

2.37. $3x - 5 = 2x + 9$ denklemini tamsayılarda çözün.

2.38. $3x - 5 = 10x + 9$ denklemini tamsayılarda çözün.

2.39. $3x - 5 = 8x + 9$ denklemini tamsayılarda çözün.

2.40. $(x - 1)(x + 1)(y - 3)(z + 4) = 0$ denklemini tamsayılarda çözün.

2.41. $(x - 1)^2 = -4$ denklemini tamsayılarda çözün.

2.42. $(x - 2)(x + 1) = 0$ denklemini tamsayılarda çözün.

2.43. $(x + 3)(x - 2)(x + 1) = 0$ denklemini tamsayılarda çözün.

2.44. $(x + 3)(3x - 2)(x + 1) = 0$ denklemini tamsayılarda çözün.

2.45. $(x + 3)^2 = 0$ denklemini tamsayılarda çözün.

2.46. $(x + 3)^2(3x - 2)^3(x + 1)^4 = 0$ denklemini tamsayılarda çözün.

2.47. $(x - 2)(y + 1) = 1$ denklemini tamsayılarda çözün.

2.48. $(x - 2)(x + 1) = 1$ denklemini tamsayılarda çözün.

2.49. $(x - 2)^2 = 1$ denklemini tamsayılarda çözün.

2.50. $x^3 = 8$ denklemini tamsayılarda çözün.

2.51. $x^4 = 16$ denklemini tamsayılarda çözün.

2.52. $x^2 = x$ denklemini tamsayılarda çözün.

2.53. $x^2 = -x$ denklemini tamsayılarda çözün.

2.54. $(x - 2)(x + 1) = 4$ denklemini tamsayılarda çözün.

2.55. $(x + 3)(3y - 2)(z + 1) = 1$ denklemini tamsayılarda çözün.

2.56. $(5x - 4)(4y - 7) = 1$ denkleminin tamsayılarda çözümlerini bulun.

2.57. $(3x-5)(4y-7)=1$ denkleminin tamsayılarda çözümlerini bulun.

2.58. $(3x-10)(4y-9)=1$ denkleminin tamsayılarda çözümlerini bulun.

2.59. $(3x-4)(4y-7)=-1$ denkleminin tamsayılarda çözümlerini bulun.

2.60. $(5x-3)(4y-9)=-2$ denkleminin tamsayılarda çözümlerini bulun.

2.61. $(5x-3)(4y-9)=2$ denkleminin tamsayılarda çözümlerini bulun.

2.62. $(3x-1)(4y-3)(5z-4)=6$ denkleminin tamsayılarda çözümlerini bulun. (Pek hoş bir soru değil doğrusu, çünkü dikkate alınması gereken biraz fazla şık var, bunun için özür dilerim; gene de bu tür denklemleri çözebilmek, en azından çözüm yöntemlerini bilmek gerekiyor.)

2.63. $(x-2)(3y-2)=(x-2)(5y-4)$ denkleminin tüm tamsayı çözümlerini bulun.

2.64. $(3x-2y)(2x-3y)=-1$ denkleminin tamsayılarda çözümlerini bulun.

2.65. $(x+3)(y-1)-(x+2)(y+3)=0$ denkleminin tamsayılarda çözümlerini bulun.

2.66. $(x^2+y^2)(z^2+t^2)=(xz+yt)^2+(xt-yz)^2$ eşitliğini kanıtlayın. Bu ifadeden iki karenin toplamı olan tamsayılar kümesinin çarpma altında kapalı olduğunu çıkarın.

2.67. Her x, $y\in\mathbb{Z}$ için $x\star y=xy-x-y+2$ tanımını yapalım.
a. $x\star(y\star z)=(x\star y)\star z$ eşitliğini kanıtlayın.
b. $x\star y=y\star x$ eşitliğini kanıtlayın.
c. $x\star 1=1$ eşitliğini kanıtlayın.
d. $x\star 2=x$ eşitliğini kanıtlayın.

Notlar

2.68. Siz yaşlarımdayken, lisedeyken yani, hesap makinaları daha yeni yeni popüler oluyordu. Galiba popüler tek bir marka vardı, Texas Instruments. Her yerde reklamlarını görüyorduk ama ağzımızın suları akarak bakıyorduk, çünkü çok pahalıydılar, kalitesine göre 1200 dolar ve üstü gibi kalmış aklımda. Tabii program filan da yazılabiliyordu, yani öyle sadece toplama, çarpma yapabilen makinalar değildi. Ama o kadar parayı toparlayabilmemiz mümkün değildi. Duyduk ki Polonya'da eşdeğer makinalar 300 dolara üretiliyormuş. Biz, matematiğe meraklı üç arkadaş 300'er dolar toparlayıp babası hariciyeci olan bir başka arkadaşımıza makinaları ısmarladık. Tatillerde restoranlarda bulaşıkçılık yaptığımdan o kadar param vardı. Arkadaşlarım herhalde ailelerinden istediler. Makinalar geldiğinde sevinçten havaya uçtuk, kartları filan vardı, yazdığımız programları daha sonra kullanmak üzere kartlara kaydetmemiz gerekiyordu; ama gel gör ki makinalarımız Polonya notasyonu kullanıyordu. Yani $x+y$ yerine $+\ x\ y$ ve $x\times y$ yerine $\times\ x\ y$ yazmak gerekiyordu. Böylece parantezlere gerek kalmıyordu, örneğin $x\times(y+z)$ için

$$\times\ x\ +\ y\ z$$

yazmak, $(x\times y)+z$ için

$$+\ \times\ x\ y\ z$$

yazmak, $x+(y\times z)$ için

$$+\ x\ \times\ y\ z$$

yazmak gerekiyordu. x/y için ise

$$\div\ x\ y$$

yazmalıydık.

$$\frac{\frac{x}{y}+z}{t}+5$$

gibi bir ifade

$$+\ \div\ +\ \div\ x\ y\ z\ t\ 5$$

olarak yazılıyordu. Böylece parantezlere gerek kalmıyordu. Kısa zamanda alıştık ama, hatta o kadar alıştık ki, normal gösterime dönmekte zorlandık.
Polonya notasyonunu Polonyalı matematiksel mantıkçı Łukasiewicz 1924'te bulmuştur. Matematikte ve mantıkta artık kullanılmasa da bilgisayar bilimlerinde hâlâ kullanılıyor.

2.7 Sıralama

Doğal sayıların bildiğimiz

$$0 \leq 1 \leq 2 \leq 3 \leq \dots$$

sıralamasını tamsayılara şöyle genişletelim:

1. Doğal sayıların sıralaması eskisi gibi olsun. Örneğin 3 hâlâ daha 5'ten küçük olacak, çünkü doğal sayılarda da öyleydi.
2. Yeni eklediğimiz "eksili sayılar"ın hepsi tüm doğal sayılardan daha küçük olsun; yani her n, $m \in \mathbb{N}$ için,

$$-n \leq m$$

olsun. Örneğin $-1 \leq 5$, $-5 \leq 1$ ya da $-3 \leq 0$. Ve elbette $-0 \leq 0$.
3. Son olarak "eksili sayıların" sıralaması doğal sayıların sıralamasının tam tersi olsun, bir başka deyişle her n, $m \in \mathbb{N}$ için,

$$-n \leq -m \iff m \leq n$$

olsun. Örneğin $-5 \leq -3$ çünkü $3 \leq 5$.

Demek ki tamsayıları şöyle sıralıyoruz:

$$\dots \leq -3 \leq -2 \leq -1 \leq 0 \leq 1 \leq 2 \leq 3 \leq \dots$$

Eğer $\leq$ sıralaması yerine (aynen $\leq$ sıralamasını tanımladığımız gibi) $<$ sıralamasını tanımlarsak,

$$\dots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \dots$$

olur. Tahmin edileceği üzere ve elbette,

$$x < y \iff (x \leq y \text{ ve } x \neq y)$$

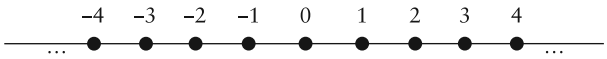
ve

$$x \leq y \iff (x < y \text{ ya da } x = y)$$

eşdeğerlikleri geçerlidir. Yani $\leq$ sıralamasıyla $<$ sıralamasından biri biliniyorsa, diğeri de bilinir; her birini diğerinin yardımıyla tanımlayabiliriz.

$x \geq y$ önermesini $y \leq x$ olarak ve $x > y$ önermesini $y < x$ olarak tanımlıyoruz.

Bu sıralamanın resmi de şöyle:



Küçükten büyüğe doğru soldan sağa sıralanmış doğal sayılar.

Görüldüğü üzere tamsayıların ne en küçük ögesi var ne de en büyük: Eğer x bir tamsayıysa $x-1$ tamsayısı x'ten küçüktür ve $x+1$ tamsayısı x'ten büyüktür.

Doğal sayılarda olduğu gibi tamsayılarda da n ile $n+1$ arasında bir sayı yoktur. Yani n hangi tamsayı olursa olsun, $n \leq x \leq n+1$ ise x ya n'ye ya da $n+1$'e eşit olmak zorundadır.

Tamsayıların kareleri negatif olamaz tabii, yani kareler $\mathbb{N}$ kümesindedirler. Örneğin $(-5)^2 = (-5)(-5) = 25 \in \mathbb{N}$ olur.

Tamsayıların sıralamasının daha sonra sık sık referans vereceğimiz birkaç önemli özelliğini yazalım:

S1. Yansıma. Her $u \in \mathbb{Z}$ için $u \leq u$ olur.
S2. Antisimetri. Her $u, v \in \mathbb{Z}$ için, eğer $u \leq v$ ve $v \leq u$ ise $u = v$ olur.
S3. Geçişkenlik. Her $u, v, w \in \mathbb{Z}$ için, eğer $u \leq v$ ve $v \leq w$ ise $u \leq w$ olur.
S4. Tamsıralama. Her $u, v \in \mathbb{Z}$ için ya $u \leq v$ ya da $v \leq u$ olur.
ST. Toplamayla Uyum. Her $u, v, w \in \mathbb{Z}$ için, eğer $u \leq v$ ise $u + w \leq v + w$ olur.
SÇ. Çarpmayla Uyum. Her $u, v, w \in \mathbb{Z}$ için, eğer $u \leq v$ ve $0 \leq w$ ise $uw \leq vw$ olur.

ST özelliğinin diğer istikameti de doğrudur, nitekim eğer $u + w \leq v + w$ ise, her iki tarafa da $-w$ ekleyerek ST'den dolayı $u \leq v$ elde ederiz. Mesela

$$u \leq v \iff u - v \leq v - v \iff u - v \leq 0$$

olur ($u \leq v$ eşitsizliğinin taraflarına $-v$ eklersek $u-v \leq 0$ eşitsizliğini, $u-v \leq 0$ eşitsizliğinin taraflarına v eklersek $u \leq v$ eşitsizliğini buluruz.) Taraflara bir de $-u$ eklersek, buradan

$$u \leq v \iff -v \leq -u$$

eşdeğerliğini buluruz.

S3, ST ve SÇ özellikleri $\leq$ yerine $<$ için de geçerlidir. Ama S2'de $\leq$ yerine $<$ koyarsak S2 anlamsızlaşır. S1 ve S4 için şu değişiklikler yapılmalı:

S1′. Yansımama. Her $u \in \mathbb{Z}$ için $u < u$ önermesi yanlıştır.
S4′. Tamsıralama. Her $u, v \in \mathbb{Z}$ için ya $u < v$ ya $u = v$ ya da $v < u$ olur.

Eğer $w = 0$ ise SÇ özelliğinin diğer istikameti doğru olmayabilir tabii, ama eğer $w > 0$ ise, diğer istikamet de doğrudur: Eğer $uw \leq vw$ ve $w > 0$ ise $u \leq v$ olmak zorundadır. Bir başka deyişle eşitsizliklerde pozitif sayıları

sadeleştirebiliriz, örneğin $6x \leq 9y$ ise $2x \leq 3y$ olur. Bunu kanıtlayalım. Diyelim $uw \leq vw$ ve $w > 0$. Amacımız $u \leq v$ önermesini kanıtlamak. Olmayana ergi yöntemine başvuracağız. Diyelim $u \leq v$ önermesi yanlış. O zaman $v < u$ önermesi doğru olur, dolayısıyla $v \leq u$ önermesi doğru olur. Ama $0 \leq w$ olduğundan, SÇ'den dolayı $vw \leq uw$ olur. S2'den de $uw = vw$ çıkar. Buradan $(u - v)w = 0$ ve hemen ardından $u - v = 0$ elde edilir (çünkü $w \neq 0$), yani $u = v$ bulunur. Buradan da $u \leq v$ çıkar.

En Küçük ve En Büyük Ögeler. Boş olmayan her doğal sayı kümesinin bir en küçük ögesi vardır, bunu biliyoruz (İyisıralama Özelliği, [2. Kitap, sayfa 81]). Bu özellik tamsayılarda geçerli değildir. Örneğin $\mathbb{Z}$, $\mathbb{Z}$'nin bir altkümesidir (tabii ki!) ama $\mathbb{Z}$'nin en küçük ögesi yoktur. Öte yandan tamsayılarda bazı altkümelerin en küçük ögesi vardır. Açıklayalım:

Eğer bir $X \subseteq \mathbb{Z}$ altkümesinin tüm ögeleri belli bir a tamsayısından büyükse, a'ya X'in bir ***altsınırı*** adı verilir. Örneğin -500, -300'den büyük sayılardan oluşan kümenin bir altsınırıdır. -400 ve -600 de bu kümenin birer altsınırıdır. Eğer a sayısı X altkümesinin bir altsınırıysa, a'dan küçük her sayı da X'in bir altsınırıdır elbette. Altsınırı olan kümelere ***alttan sınırlı küme*** denir. Alttan sınırlı olan ama boşküme olmayan her $X \subset \mathbb{Z}$ altkümesinin en küçük bir ögesi vardır. Bu ögeye kümenin ***minimal*** ögesi denir. Örneğin -100'den büyük ve 7'ye bölünen en küçük tamsayı -98'dir. Bu sayı

$$\min X$$

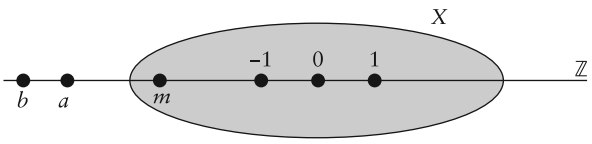
olarak yazılır. Bir başka örnek:

$$\{x \in 5\mathbb{Z} : x \geq -342\}$$

kümesi alttan sınırlıdır, mesela -402 tarafından. Bu kümenin en küçük ögesi -340'tır, yani

$$\min \{x \in 5\mathbb{Z} : x \geq -342\} = -340$$

olur.



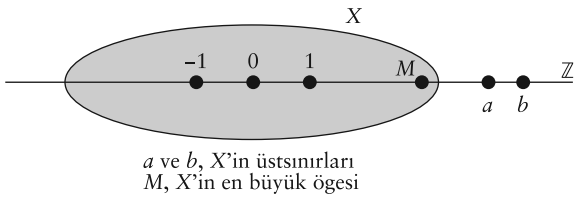
a ve *b*, *X*'in altsınırları
m, *X*'in en küçük ögesi

Benzer şekilde eğer boş olmayan bir altkümenin tüm ögeleri belli bir tamsayıdan küçükse (matematiksel jargonla, altküme ***üstten sınırlıysa***), o zaman o kümenin en büyük bir ögesi vardır. Bu ögeye kümenin maksimal ögesi

denir. Örneğin -100'den küçük ve 7'ye bölünen en büyük tamsayı -105'tir. X'in en büyük ögesi

$$\max X$$

olarak gösterilir.



a ve b, X'in üstsınırları
M, X'in en büyük ögesi

Boş olmayan sonlu kümelerin her zaman en küçük ve en büyük ögeleri vardır tabii. Örneğin

$$\min\{-40,\ -30,\ 0,\ 5,\ 26\} = -40 \text{ ve } \max\{-40,\ -30,\ 0,\ 5,\ 26\} = 26$$

olur.

2.8 Mutlak Değer

x herhangi bir tamsayı olsun. $\max\{x, -x\}$ sayısı, yani x ile $-x$ sayısının en büyüğü $|x|$ olarak gösterilir:

$$|x| = \max\{x, -x\}.$$

$|x|$ sayısına x'in ***mutlak değeri*** adı verilir. Örneğin,

$$\begin{array}{lcl} |5| & = & 5 \\ |-5| & = & 5 \\ |0| & = & 0 \\ |3-5| & = & |-2| = 2 \\ |-3|+|5| & = & 3+5=8 \\ ||-3|-|5|| & = & |3-5| = |-2| = 2 \end{array}$$

olur. Demek ki doğal sayıların mutlak değeri kendilerine eşittir, negatif sayıların mutlak değerleri ise sayının toplamsal tersine eşittir. Yani

$$|x| = \begin{cases} x & \text{eğer } x \geq 0 \text{ ise} \\ -x & \text{eğer } x \leq 0 \text{ ise} \end{cases},$$

bir başka deyişle,

$$x \in \mathbb{N} \Longleftrightarrow |x| = x$$

ve

$$x \leq 0 \Longleftrightarrow |x| = -x$$

olur. Görüldüğü üzere, her x için

$$-|x| \leq x \leq |x|$$

oluyor. Bununla

$$-|y| \leq y \leq |y|$$

eşitsizliklerini taraf tarafa toplarsak,

$$-(|x| + |y|) \leq x + y \leq |x| + |y|$$

buluruz. Bu iki eşitsizliği şöyle ayıralım:

$$x + y \leq |x| + |y| \text{ ve } -(x + y) \leq |x| + |y|.$$

Demek ki

$$\pm(x + y) \leq |x| + |y|.$$

Ama $|x + y| = \pm(x + y)$. Bundan da

$$|x + y| \leq |x| + |y|$$

çıkar. Bu çok meşhur bir eşitsizliktir. Adı bile vardır: Üçgen Eşitsizliği. Bunu bir teorem olarak yazmakta yarar var:

Teorem 2.1 (Üçgen Eşitsizliği)**.** *Her x ve y tamsayısı için $|x + y| \leq |x| + |y|$ olur.* □

Bu teoremden ilginç bir eşitsizlik daha çıkar. x ve y iki tamsayı olsun. Üçgen eşitsizliğinden,

$$|y| = |x + (y - x)| \leq |x| + |y - x|,$$

yani

$$|y| - |x| \leq |y - x| = |x - y|$$

çıkar. x'le y'nin yerlerini değiştirirsek,

$$|x| - |y| \leq |x - y|$$

buluruz. Demek ki

$$\pm(|x| - |y|) \leq |x - y|.$$

Ama $||x| - |y|| = \pm(|x| - |y|)$ olduğundan, bu da

$$||x| - |y|| \leq |x - y|$$

demektir. Bir teorem daha kanıtladık.

Teorem 2.2. *Her x ve y tamsayısı için $||x| - |y|| \leq |x - y|$ olur.* □

Örnekler

2.69. $x^2 = |x|^2$ eşitliği doğrudur ama $x^3 = |x|^3$ eşitliği ancak x bir doğal sayıysa doğrudur. Eğer x negatifse, $|x^3| = -3$ olur.

2.70. Her x ve y için $|xy| = |x| \cdot |y|$ olur. Bunun kolay kanıtını okura bırakıyoruz.

2.71. Eğer $a < 0$ ise $|x| = a$ denkleminin hiç çözümü yoktur. Ama $|x| = 0$ denkleminin tek bir çözümü vardır: $x = 0$. Ve son olarak eğer $x > 0$ ise $|x| = a$ denkleminin iki çözümü vardır: $x = a$ ve $x = -a$. Bu iki çözümü $x = \pm a$ olarak tek bir eşitlikle göstermek çoğu zaman kolaylık sağlar. "$x = \pm a$" şu anlama gelir: x sayısı ya a'ya ya eşittir ya da $-a$'ya. $|x| = |a|$ denkleminin her zaman en az bir çözümü vardır; eğer $x \neq 0$ ise iki çözümü vardır: $x = \pm a$.

2.72. $|x-3| = 5$ denkleminin tüm çözümlerini bulalım. Mutlak değerden kurtulmak istiyorsak, bu denklemi iki denkleme dönüştürmek zorundayız. $|x - 3| = 5$ demek, ya $x - 3 = 5$ ya da $x - 3 = -5$ demektir. Buradan da iki çözüm olduğu anlaşılır: $x = 8$ ve $x = -2$.

2.73. $|2x - 3| = |4x - 9|$ denkleminin çözümlerini bulalım. Bu eşitlik iki durumda mümkün: $2x - 3 = 4x - 9$ ya da $2x - 3 = -(4x - 9)$. Bu denklemler de sırasıyla $x = 3$ ve $x = 2$ çözümlerini verir.

2.74. $|2x-3| = |5x-11|$ denkleminin tamsayılarda çözümlerini bulalım. Bu eşitlik iki durumda mümkün: $2x - 3 = 5x - 11$ ya da $2x - 3 = -(5x - 11)$. Birincisi $3x = 8$ demektir ki bunun tamsayılarda bir çözümü yoktur. İkincisi ise $7x = 14$ demektir, bunun çözümü de $x = 2$'dir.

2.75. $|2x-3| = |7x-10|$ denkleminin tamsayılarda çözümlerini bulalım. Bu eşitlik iki durumda mümkün: $2x-3 = 7x-10$ ya da $2x-3 = -(7x-10)$. Birincisi $5x = 7$ demektir ki bunun tamsayılarda bir çözümü yoktur. İkincisi ise $9x = 13$ demektir ki bunun da tamsayılarda bir çözümü yoktur. Demek ki denklemimizin tamsayılarda çözümü yoktur.

2.76. Eğer a, $b \geq 2$ ise $ab \geq a + b$ eşitsizliğini kanıtlayalım. Aşağıdaki eşitsizliklerin eşdeğer olduğunu kontrol etmeyi okura bırakıyorum:

$$\begin{array}{ll} ab & \geq \quad a+b \\ ab-a-b & \geq \quad 0 \\ ab-a-b+1 & \geq \quad 1 \\ (a-1)(b-1) & \geq \quad 1 \end{array}$$

Eğer a, $b \geq 2$ ise son eşitsizlik elbette doğru.

Alıştırmalar

2.77. $-5 < x < 7$ eşitsizliklerini sağlayan kaç x tamsayısı vardır?

2.78. $-5 < x < 7$ ve $-3 < x < 10$ eşitsizliklerini sağlayan kaç x tamsayısı vardır?

2.79. $|x| < 10$ eşitsizliğini sağlayan kaç tane x tamsayısı vardır?

2.80. $|3x| < 10$ eşitsizliğini sağlayan kaç tane x tamsayısı vardır?

2.81. $|x - 3| < 10$ eşitsizliğini sağlayan kaç tane x tamsayısı vardır?

2.82. $|2x - 3| < 10$ eşitsizliğini sağlayan kaç tane x tamsayısı vardır?

2.83. $|50x - 3| < 10$ eşitsizliğini sağlayan kaç tane x tamsayısı vardır?

2.84. $|50x - 41| < 10$ eşitsizliğini sağlayan kaç tane x tamsayısı vardır?

2.85. $|x - 3| < 816$ eşitsizliğini sağlayan kaç tane x tamsayısı vardır?

2.86. $|50x - 41| < 200$ eşitsizliğini sağlayan kaç tane x tamsayısı vardır?

2.87. $|x - 3| = -2$ denkleminin tamsayılardaki tüm çözümlerini bulun.

2.88. $|(x - 3)(x + 5)| = 0$ denkleminin tamsayılardaki tüm çözümlerini bulun.

2.89. $|(x - 3)(x + 5)| = 1$ denkleminin tamsayılardaki tüm çözümlerini bulun.

2.90. $|3x + 5| = 4$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.91. $|3x - 14| = |1 - 2x|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.92. $|5x - 11| = |3 - 2x|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.93. $|5x - 11| = |3 - 8x|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.94. $|x - 1| = |x + 1|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.95. $|x - 3| = -2$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.96. $|x - 2| = |x + 8|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.97. $|2 - x| = |x + 8|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.98. $|x + 3| = |x + 5|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.99. $|x - 2| = |x + 6|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.100. $|4x + 3| = |x + 12|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.101. $|4x + 3| = |x + 6|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.102. $|4x + 3| = |3x + 4|$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.103. $|(x - 1)(x + 4)| < 8$ eşitsizliğini sağlayan tüm x tamsayılarını bulun.
2.104. $|(x - 1)(x + 4)| > 100$ eşitsizliğini sağlayan kaç tane x tamsayısı vardır?
2.105. $|(x - 3)(y + 5)| = 1$ denkleminin tamsayılardaki tüm çözümlerini bulun.
2.106. Hangi x tamsayıları için $(3x - 1)(2x - 1) < 0$ olur?
2.107. Hangi x tamsayıları için $(x - 1)(x + 4)(x - 7) < 0$ olur?
2.108. Hangi x tamsayıları için $(3x - 1)(4 - x)(x - 7) > 0$ olur?
2.109. Her x tamsayısı için $||x|| = |x|$ eşitliğini kanıtlayın.
2.110. Hangi x tamsayıları için $|(x - 1)(x + 4)| = (x - 1)(x + 4)$ eşitliği sağlanır?
2.111. $a|b$ ve $b > 0$ ise, $a \leq b$ olduğunu kanıtlayın.
2.112. Her $n \in \mathbb{Z}$ için $n + |n| \geq 0$ olduğunu kanıtlayın. Hangi n tamsayıları için eşitlik olur?
2.113. Eğer $a > 0$ ise $s(a) = 1$, eğer $a < 0$ ise $s(a) = -1$, eğer $a = 0$ ise $s(a) = 0$ tanımını yapalım. $s(a)|a| = a$ ve $|a| = as(a)$ eşitliklerini kanıtlayın. Her a ve b için $s(ab) = s(a)s(b)$ eşitliğini kanıtlayın. $s(a)$'ya a'nın ***işareti*** adı verilir.
2.114. Her a, b, c tamsayısı için $\max\{\max\{a, b\}, c\} = \max\{a, \max\{a, b\}\}$ eşitliğini kanıtlayın.
2.115. Her a, b, c tamsayısı için $|a - b| \leq |a - c| + |c - b|$ eşitliğini kanıtlayın. (İpucu: Üçgen eşitsizliği.)
2.116. Eğer $0 < w$ ve $uw < vw$ ise $u < v$ önermesini kanıtlayın.
2.117. a, b, c, d tamsayıları $a < b$ ve $c < d$ eşitsizliklerini sağlıyorsa, $ac < bd$ olmak zorunda mı? Ya kanıtlayın ya da karşıörnek verin.
2.118. Herhangi bir n tamsayısı için $n < x < n + 1$ eşitsizliklerini sağlayan bir x tamsayısı olmadığını kanıtlayın. Aynı şekilde n ile $n-1$ arasında bir tamsayı olmadığını kanıtlayın.
2.119. $r > 0$ bir tamsayı olsun. Her $x \in \mathbb{Z}$ için $|x| < r$ ile $-r < x < r$ önermelerinin eşdeğer olduğunu kanıtlayın.
2.120. Hangi a ve b tamsayıları için $ab \geq a + b$ olur. İpucu: Bkz. Örnek 2.76.
2.121. Hangi x ve y tamsayıları için $|x + y| = |x| + |y|$ olur? (Bkz. Teorem 2.1.)
2.122. Hangi x ve y tamsayıları için $|x + y| = x + y$ olur?
2.123. Hangi x ve y tamsayıları için $|x + y| = x - y$ olur?
2.124. Hangi x ve y tamsayıları için $||x| - |y|| = |x - y|$ olur? (Bkz. Teorem 2.2.)
2.125. Hangi x ve y tamsayıları için $||x| - |y|| = x - y$ olur?
2.126. Hem $|x + 2y| = 1$ hem de $|2x - 3y| = 9$ eşitliğini sağlayan tüm x ve y tamsayılarını bulun.

Notlar

2.127. Aritmetiksel işlemlerin hayattaki karşılığını anlatmaya çalışalım.

Doğal sayılarda toplamanın hayattaki karşılığı kolaydır: 2 elma 3 elma daha 5 elma ettiğinden $2+3=5$ olmalıdır.

5 elmadan 2'sini yersek geriye 3 elma kalır. Bu yüzden $5-2=3$ olur, ya da olmalıdır.

Eğer hava 2 dereceyse ve 5 derece soğursa, hava -3 derece olur. Eğer 2 liram varsa ve 5 lira harcarsam, 3 lira borcum olur. Bu nedenlerle $2-5=-3$ olur.

Eğer 10 lira borcum varsa, yani -10 liram varsa ve borcumun 7 lirasını ödersem 3 lira borcum olur, yani -3 liram olur. Bu yüzden $-10+7=-3$ olur.

Eğer hava -2 dereceyse ve 5 derece daha soğursa, hava -7 derece olur. Bu yüzden $-2-5=-7$ olur.

3 elma ağacımın her birinde 4 elma varsa toplam 12 elmam var demektir. Bu yüzden $3\times 4=12$ olur.

3 kişinin her birine 2'şer lira borcum varsa, toplam 6 lira borcum vardır. Böylece $3\times(-2)=-6$ olmalıdır.

$(-3)\times 2=-6$ eşitliğinin hayattaki karşılığını bulmak biraz daha zor. -3 ile çarpmak ne demektir? Bu işlem hayatta neye tekabül ediyor? Şu örnek sanırım iyi anlatıyor: Eğer her ağaca çıktığımda 2 elma topluyorsam, ağaca 3 defa eksik çıkarsam, 6 elma daha az toplamış olurum. Ağaca üç defa eksik çıkmayı ağaca -3 defa çıkmak olarak ve 6 tane daha az elma olmayı -6 olarak algılarsak, bu örnek $(-3)\times 2$ işleminin sonucunun -6 olması gerektiğini gösterir.

Peki $(-3)\times(-2)$ neden 6 olmalı? Şu örnekle anlatmaya çalışayım: Her sinemaya gidişimde 2 lira harcıyorsam (yani -2 lira kazanıyorsam!), 3 defa sinemaya gitmezsem (yani sinemaya -3 defa daha fazla gidersem!) cebimdeki para 6 lira artar!

Hayatın kâğıda geçirilmiş haline matematik denir!

2.128. Aritmetiksel işlemlerden sözetmişken, sıfır tane sayıyı toplama ya da çarpma gibi bir işleme sokmaktan sözedelim.

5×3, beş tane 3'ü toplamak anlamına gelir:

$$5\times 3=3+3+3+3+3.$$

4×3, dört tane 3'ü toplamak anlamına gelir. 1×3, bir tane 3'ü toplamak anlamına gelir. Dolayısıyla 0×3, sıfır tane 3'ü toplamak anlamına gelir. Size sıfır tane 3 veriyorum, hadi toplayın bu 3'leri de görelim! Tanım gereği, sıfır tane sayıyı toplamak 0'dır. Başka bir nedenden değil, tanımdan! Bu yüzden $0\times 3=0$ olur.

Peki sıfır tane sayıyı çarpmak ne demektir? 3^5, beş tane 3'ü çarpmak anlamına gelir:

$$3^5=3\times 3\times 3\times 3\times 3.$$

3^4, dört tane 3'ü çarpmak anlamına gelir. 3^1, bir tane 3'ü çarpmak anlamına gelir. Dolayısıyla 3^0, sıfır tane 3'ü çarpmak anlamına gelir. Size sıfır tane 3 veriyorum, hadi çarpın bu 3'leri! Çarpamazsınız tabii, çarpacak 3 yok çünkü. Tanım gereği, sıfır tane sayıyı çarpmanın sonucu 1'dir. Başka bir nedenden değil, tanımdan! Bu yüzden $3^0=1$ olur.

5! de beş tane sayıyı çarpmak demektir:

$$5!=1\times 2\times 3\times 4\times 5.$$

3! için 1'den 3'e kadar üç tane sayı çarpılır. 0! için 0 tane, yani hiç tane sayı çarpmalı. Bir önceki paragrafta hiç tane sayının çarpımını 1 olarak tanımlamıştık. Demek ki $0!=1$ olmalı.

Hiç tane ögeyi (toplama ya da çarpma gibi ikili bir) işleme sokmak, varsa o işlemin etkisiz ögesi olarak tanımlanır. Örneğin hiç tane kümenin bileşimi, bileşim işleminin

etkisiz ögesi olan $\emptyset$ olarak tanımlanır. Hiç tane kümenin kesişimi ise, varsa evrensel küme olarak tanımlanır; evrensel küme yoksa, hiç tane kümenin kesişimi tanımsız bırakılır.

Ama dikkat, etkisiz ögenin sağdan ve soldan etkisiz öge olması lazım, ikisinden biri yetmez. Örneğin bölme işleminin sağdan etkisiz elemanı vardır: 1, çünkü her x için $x/1 = x$ olur. Ama bölmenin soldan etkisiz ögesi yoktur, çünkü $a/x = x$ denklemini her x için sağlayan bir a yoktur. Bu yüzden bir sayıyı hiç tane eşit parçaya bölme (yani 0'a bölme) tanımsız bırakılmıştır.

2.129. 5 ögeli bir kümenin 8 ögeli altkümesi olamaz. Yani 5 ögeli bir kümenin 8 ögeli altküme sayısı 0'dır.

-5 ögeli bir küme olmadığından, -5 ögeli bir kümenin altkümesi de olamaz, yani -5 ögeli bir kümenin k ögeli altküme sayısı 0'dır.

Ve elbette n ögeli bir kümenin -5 ögeli altküme sayısı da 0'dır.

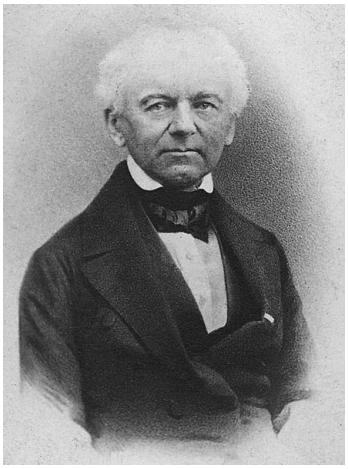
Bu yüzden $n, k \in \mathbb{N}$ için tanımladığımız $\binom{n}{k}$ sayısının tanımı tamsayılara şöyle genelleştirilir:

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{eğer } 0 \leq k \leq n \; ise \\ 0 & \text{aksi halde} \end{cases}$$

Şimdi artık her $n, k \in \mathbb{Z}$ için, n ögeli bir kümenin k ögeli altküme sayısının $\binom{n}{k}$ olduğunu söyleyebiliriz.

2.130. $\binom{n}{k}$ sayıları çok eski zamandan beri biliniyordu. Bu sayıların ayrıntılı bir çalışması 10'uncu yüzyılda yaşamış Hintli matematikçi Halayudha tarafından yapılmıştır. Halayudha şiir üzerine bir kitap ve bir de sözlük yazmıştı.

2.131. Çok kullanışlı $\binom{n}{k}$ gösterimi Alman matematikçi ve fizikçi Andreas von Ettingshausen (1796-1878) tarafından bize hediye edilmiştir. Ettingshausen 1819'da fizik profesörü, iki yıl sonra da Viyana Üniversitesi'nde matematik profesörü olmuştur, kolay elde edilecek bir başarı değil, hele o genç yaşta. Elektrik üreten elektromanyetik makinaları (her ne demekse!) yapan ilk kişidir. Viyena Üniversitesi'ndeki popüler matematik ve fizik dersleri üniversitede yeni bir çığır açmıştır. Bu derslerini derlediği $\binom{n}{k}$ gösterimini bize kazandıran kombinasyon hesapları kitabı ve bir de ayrıca bir fizik ders kitabı vardır.



Andreas von Ettingshausen

3. Tamsayıların Aksiyomları

Önceki iki bölümde tamsayıları tanımladık ve tamsayılar üzerinde tanımlanan toplama ve çarpma işlemlerinden ve sıralama ilişkisinden bahsettik. Sonra da bunların bazı özelliklerini irdeledik. Yaklaşımımız matematiksel olmasına matematikseldi ama doğrusu pek estetik olduğu söylenemezdi. (Ben yazarken sıkıldım, okur kimbilir okurken neler çekmiştir!) Burada aynı konuya çok daha matematiksel ve modern bir bakış açısıyla değineceğiz. Tamsayıların tanımını vermeyeceğiz, tamsayıların tanımıyla hiç mi hiç ilgilenmeyeceğiz, ilgi alanımız tamamen tamsayıların özellikleri olacak[1]. Matematiksel jargonla,

$$(\mathbb{Z},\ +,\ \times,\ <,\ 0,\ 1)$$

"yapısının" en temel özelliklerini sıralayıp diğer tüm özellikleri bu temel özelliklerden hareketle kanıtlayacağız. O "en temel özelliklere" aksiyom adını vereceğiz. Bir başka deyişle, biraz aşağıda sıralayacağımız önermeleri tamsayılar yapısının aksiyomları olarak ele alıp, tamsayıların diğer tüm özelliklerini bu aksiyomlardan hareketle kanıtlayacağız.

Bu bölümü okurken okur sadece önceki iki bölümü değil, tamsayılar hakkında daha önce bildiği her şeyi unutmaya çalışsın, hafızasına ve önbilgilerine başvurmasın. 0'ın 1'den küçük olduğunu bile bilmediğini varsaysın. Tamsayıların özelliklerini (mesela 0'ın 1'den küçük olduğunu) sadece aşağıda sıraladığımız aksiyomları varsayarak kanıtlayacağız.

Biraz yukarıda $(\mathbb{Z},\ +,\ \times,\ <,\ 0,\ 1)$ "yapısından" sözettik. Herhangi bir kuşkuya yer vermemek için buradaki ifadelerin ne olduklarını açıklayalım:

$\mathbb{Z}$ bir kümedir.
$+$, $\mathbb{Z}$ üzerine (ikili) bir işlemdir.
$\times$, $\mathbb{Z}$ üzerine (ikili) bir işlemdir.
$<$, $\mathbb{Z}$ üzerine (ikili) bir ilişkidir.
0, $\mathbb{Z}$'nin bir ögesidir.
1, $\mathbb{Z}$'nin bir ögesidir.

[1] Matematiksel nesnelerin (matematiksel anlamda) ne olduğunun hiç önemli olmadığı, sadece özelliklerinin, yani aslında birbirleriyle ilişkilerinin önemli olduğu çok derin bir olgudur. Şöyle bir örnek vereyim: 2, 4 ve çarpmanın tanımı (yani ne oldukları) matematiksel anlamda hiç önemli değildir, herhangi bir tanım olabilir, yeter ki (mesela) $2 \times 2 = 4$ olsun!

"İkili işlem" ile, işlem yapabilmek için **iki** öge gerekir demek istiyoruz, yani **iki** sayı toplanır, **iki** sayı çarpılır. "İkili ilişki" de "küçüklük-büyüklük ilişkisi için iki öge gerekir", yani ancak **iki** sayı karşılaştırılır demek istiyoruz[2].

$a \times b$ yerine sık sık $a \cdot b$ ya da daha da kısaca ab yazılır; biliyorsunuz...

Şimdi $(\mathbb{Z}, +, \times, <, 0, 1)$ yapısının aksiyomlarını sıralayalım.

T1. Her a, b, c için, $(a + b) + c = a + (b + c)$.
T2. Her a için, $a + 0 = 0 + a = a$.
T3. Her a için, $a + b = b + a = 0$ eşitliklerini sağlayan bir b vardır.
T4. Her a, b için, $a + b = b + a$ olur.
Ç1. Her a, b ve c için, $(ab)c = a(bc)$ olur.
Ç2. Her a için, $a1 = 1a = a$ olur.
Ç4. Her a ve b için, $ab = ba$ olur.
SB. $0 \neq 1$.
Da. Her a, b ve c için, $a(b + c) = ab + ac$ olur.
S1. Her a için, $a < a$ önermesi yanlıştır.
S3. Her a, b ve c için, $a < b$ ve $b < c$ ise $a < c$ olur.
S4. Her a ve b için, ya $a < b$ ya $a = b$ ya da $b < a$ olur.
TS. Her a, b ve c için, $a < b$ ise $a + c < b + c$ olur.
ÇS. Her a, b ve c için, $a < b$ ve $0 < c$ ise $ac < bc$ olur.
Ne. $\{0\} \cup \{x \in \mathbb{Z} : 0 < x\} = \mathbb{N}$ olur ve her iki kümede de toplama, çarpma işlemleri ve sıralama ilişkisi aynıdır[3].

İlk olarak, T1 ile Ç1, T3 ile Ç3, T4 ile Ç4 arasındaki yakın ilişkiyi gözlemleyelim: T aksiyomlarındaki + ve 0 simgeleri Ç aksiyomlarında × ve 1'e dönüşmüş. Fikir aynı, fikrin uygulandığı işlem ve öge farklı. T1 ve Ç1 (bu sırayla) toplama ve çarpmanın birleşme özelliğinin olduğunu, T3 ve Ç3 (yine bu sırayla) toplama ve çarpmanın etkisiz ögesinin varlığını, T4 ve Ç4 (hâlâ bu sırayla) toplama ve çarpmanın değişme özelliğinin olduğunu söylüyor.

Bu arada, T3'ün muadili olan Ç3'ün olmadığına dikkatinizi çekerim, ne de olsa (mesela) $2b = 1$ denklemi tamsayılarda çözülemez (bu denklemin çözülmesi için kesirli sayılara geçmek gerekir, ki o da bir sonraki kitabın konusu olacak).

$\leq$ ikili ilişkisini

$$a \leq b \iff (a < b \vee a = b)$$

[2] "İkili işlem" ve "ikili ilişki" ifadelerini örnekle anlatmaya çalışalım: x^2 birli bir işlemdir, çünkü tek bir sayının karesi alınır, bu işlemi yapabilmek için tek bir sayıya ihtiyaç vardır; ama mesela $xy+z$ üçlü bir işlemdir, çünkü bu işlemi yapabilmek için üç sayıya ihtiyaç vardır. Bunun gibi, "$x > 0$" birli bir ilişkidir, "x, y ile z arasında" ise üçlü bir ilişkidir.

[3] Bu aksiyom yerine, "$\{x \in \mathbb{Z} : 0 < x\}$ kümesi iyisıralıdır" aksiyomunu da kabul edebilirdik. Böylesi belki daha şık olurdu ve genelde böyle yapılır ama o zaman da bir önceki kitapta doğal sayılar için kanıtladığımız her teoremi tekrar kanıtlamak zorunda kalırdık, yani gereksiz bir zaman kaybı olurdu. İki aksiyom birbirine denktir.

olarak tanımlayalım[4]. Demek ki tanıma göre, her $a \in \mathbb{Z}$ için $a \leq a$ olur. Ayrıca (Ne) aksiyomuna göre,

$$\mathbb{N} = \{x \in \mathbb{Z} : x \geq 0\}$$

olur.

Şimdi tamsayılarla ilgili bildiğimiz her şeyi unutup, sadece ve sadece yukarıda sıraladığımız önermelere başvurarak (eski bildiklerimizi ve sezgimizi hiç kullanmadan) bazı temel olguları kanıtlayalım.

A. T1 ve T4'ün Anlamı. T1, tamsayıları toplarken paranteze gerek olmadığını söylüyor. Bu aksiyom sayesinde, örneğin, $(a+b)+c$ ve $a+(b+c)$ yerine $a+b+c$ yazabiliriz. Aynı biçimde, $(a+b)+(c+d)$ ve $(a+(b+c))+d$ yerine $a+b+c+d$ yazabiliriz. T4 de toplama yaparken sıralamanın önemli olmadığını söylüyor. Örneğin, $b+d+c+a$ yerine $a+b+c+d$ yazabiliriz. T1'e ***birleşme özelliği***, T4'e de ***değişme özelliği*** adı verilir.

B. Etkisiz Ögenin Biricikliği. T2, 0'ın toplamanın etkisiz ögesi olduğunu söylüyor. Etkisiz ögenin biricik olduğunu kanıtlayalım: $0'$ ögesi de aynen 0 gibi T2 özelliğini sağlasın, hatta bu özelliğin sadece yarısını sağlasın, hatta diyelim her $a \in \mathbb{Z}$ için,

$$a + 0' = a \text{ ve } 0 + a = a$$

olsun. Yani $0'$ sağdan etkisiz öge, 0 ise soldan etkisiz öge olsun. Bu varsayımlar altına $0 = 0'$ eşitliğini kanıtlayacağız. İlk eşitlik her a tamsayısı için geçerli olduğundan, özel olarak $a = 0$ için de geçerlidir. Birinci eşitliği $a = 0$ özel durumuna uygulayalım:

$$0 + 0' = 0$$

elde ederiz. İkinci eşitliğe $a = 0'$ özel durumuna uygulayalım:

$$0 + 0' = 0'$$

elde ederiz. Son iki eşitlikten,

$$0 = 0 + 0' = 0'$$

çıkar.

C. Toplamsal Ters. Verilmiş bir $a \in \mathbb{Z}$ için T3 özelliğini, hatta T3'ün sadece yarısını sağlayan tek bir $b \in \mathbb{Z}$ olduğunu kanıtlayalım:

$$a + b = b + a = 0 \text{ ve } a + c = 0$$

[4] $\vee$ simgesinin matematikte ve mantıkta "ya da" anlamına gelir. Yani eğer p ve q iki matematiksel önermeyse, $p \vee q$, "ya p ya da q doğru" demektir. Ama dikkat, p ve q önermelerinin her ikisi birden doğruysa da $p \vee q$ önermesi doğru olur.

olsun; bu varsayımlar altında, $b = c$ eşitliğinin geçerli olduğunu kanıtlayacağız. Hatta daha fazlasını kanıtlayabiliriz:

$$b + a = 0 \text{ ve } a + c = 0$$

ise $b = c$ olur. Yani eğer b, a'nın soldan toplamsal tersiyse, c de b'nin sağdan toplamsal tersiyse, $b = c$ olur. İşte tek satırlık kanıtı:

$$b \overset{\text{T2}}{=} b + 0 \overset{\text{V}}{=} b + (a + c) \overset{\text{T1}}{=} (b + a) + c \overset{\text{V}}{=} 0 + c \overset{\text{T2}}{=} c.$$

(Eşitliklerin üstüne kullandığımız aksiyomları yazdık. V ise "varsayım" demektir, yani üstünde V yazan eşitlik, varsayımlardan kaynaklanmaktadır.) Demek ki $b = c$. Yani verilmiş bir a için T3'ü sağlayan b biricik. Benzer şekilde $c+a = 0$ ise de $c = b$ eşitliği kanıtlanabilir.

Tabii a değiştikçe T3 eşitliğini sağlayan b de değişir, ama verilmiş bir a için T3 özelliğini sağlayan b biriciktir, bir ikincisi daha yoktur. O zaman b'ye özel bir ad verebiliriz: b'ye a'nın ***toplamsal tersi*** denir ve b yerine $-a$ yazılır ve bu öge "eksi a" diye okunur. Elbette,

$$(-a) + a = a + (-a) = 0 \tag{1}$$

eşitliği sağlanır ve $-a$ (biraz önce kanıtladığımız üzere) bu eşitlikleri sağlayan yegâne ögedir, hatta daha da fazlasını kanıtladık:

$$b = -a \Leftrightarrow a + b = 0 \tag{2}$$

ve

$$b = -a \Leftrightarrow b + a = 0. \tag{3}$$

Demek ki $y = -x$ eşitliğini kanıtlamak için $x + y = 0$ ya da $y + x = 0$ eşitliklerinden birini kanıtlamak yeterli.

$0 + 0 = 0$ olduğundan, (2)'den ya da (3)'ten dolayı $-0 = 0$ eşitliği çıkar. Hatırlarsanız, birinci bölümde, sayfa 3'te, $-0 = 0$ eşitliğini tamsayıların tanımının içine gömmüştük, burada ise bu eşitliği kanıtladık.

D. Çıkarma. $a + (-b)$ yerine $a - b$ yazılır ve bu işleme ***çıkarma*** denir:

$$a - b = a + (-b).$$

Ayrıca $-a - b$ ifadesi $(-a) - b$ anlamına gelir:

$$-a - b = (-a) - b = (-a) + (-b).$$

Son olarak, $-a + b$ ifadesi de $(-a) + b$ anlamına gelir:

$$-a + b = (-a) + b.$$

Tahmin edilen

$$-(a+b) = -a - b \text{ ve } -(a-b) = b - a$$

gibi eşitlikleri kanıtlamak zor değildir. Birincisini kanıtlayalım misal olarak:

$$\begin{aligned}(a+b)+(-a-b) &= a+b+((-a)+(-b)) \\ &= a+b+(-a)+(-b) \\ &= (a+(-a))+(b+(-b)) \\ &= 0+0=0,\end{aligned}$$

ve bundan ve (C)'den (ya da (2)'den) istenen eşitlik çıkar. Demek ki $-a-b$ sayısı $a+b$ sayısının toplamsal tersidir.

E. Sadeleştirme. $\mathbb{Z}$'de toplamaya göre sadeleştirme yapılabilir, yani eğer $a+c=b+c$ ise $a=b$ olur. Nitekim,

$$\begin{aligned}a &\overset{\text{T2}}{=} a+0 \overset{(1)}{=} a+(c+(-c)) \overset{\text{T1}}{=} (a+c)+(-c) \\ &\overset{\text{V}}{=} (b+c)+(-c) \overset{\text{T1}}{=} b+(c+(-c)) \overset{(1)}{=} b+0 \overset{\text{T1}}{=} b.\end{aligned}$$

Tabii, T4 sayesinde, sadece sağdan değil, soldan da sadeleştirme yapılabilir.

Eğer $a+b=a$ ise $a+b=a=a+0$ olur ve buradan sadeleştirerek $b=0$ buluruz.

F. Tersin Tersi. Yukarıdaki (1) eşitliğinde a yerine $-a$ alırsak,

$$(-(-a))+(-a)=0$$

buluruz. Demek ki

$$(-(-a))+(-a)=0=a+(-a)$$

ve sağdaki $-a$'ları sadeleştirerek

$$a=-(-a)$$

elde ederiz. Özetle, a'nın tersinin tersi a'dır. Bunu şöyle de görebiliriz; T3'te a ve b'nin simetrik rolleri olduğundan b, a'nın tersiyse a da b'nin tersi olur, yani a'nın tersinin tersi a'dır, yani $-(-a)=a$ olur.

G. $a+b=c$ eşitliğinden kolaylıkla $a=c-b$ ve $b=c-a$ eşitlikleri çıkar.

Bundan böyle toplamayla ilgili tüm bu bilgileri ve kimbilir belki de kanıtlamayı unuttuğumuz ama okurun bildiğinden emin olduğumuz başka eşitlikleri de özgürce kullanacağız. Şimdi çarpmanın özelliklerine geçelim.

H. Ç1 ve Ç4'ün anlamı. Ç1, çarpma işlemi için paranteze gerek olmadığını söylüyor. Ç4 de ögeleri çarparken sıralamanın önemli olmadığını söylüyor. Örneğin, $((db)c)a$ yerine $abcd$ yazabiliriz.

Ç1'e (çarpma için) ***birleşme özelliği***, Ç4'e (çarpma için) ***değişme özelliği*** denir.

I. 1'in Biricikliği. Aynen toplamadaki 0 ögesi gibi, Ç2 özelliğini sağlayan 1 ögesinin biricik olduğunu kanıtlayalım: $1'$ ögesi de Ç2 özelliğini sağlasın, yani her $a \in \mathbb{R}$ için, $a1' = a$ olsun. Bunun özel bir durumu olarak, $a = 1$ için $1 \times 1' = 1$ elde ederiz. Demek ki,

$$1' \overset{\text{Ç2}}{=} 1 \times 1' \overset{\text{V}}{=} 1$$

olur.

J. 0'la Çarpma. *Her a için $a0 = 0$ olur*, çünkü,

$$a0 + 0 \overset{\text{T2}}{=} a0 \overset{\text{T2}}{=} a(0+0) \overset{\text{Da}}{=} a0 + a0$$

ve sadeleştirerek (burada (E)'yi kullanıyoruz) $a0 = 0$ buluruz. Benzer bir kanıtla ya da çarpmanın değişme özelliğinden dolayı $0a = 0$ olur.

K. *Her a için, $-a = (-1)a$ olur*, çünkü,

$$0 \overset{\text{J}}{=} 0a \overset{\text{T2}}{=} (1 + (-1))a \overset{\text{Da}}{=} 1a + (-1)a \overset{\text{Ç2}}{=} a + (-1)a$$

ve (C)'ye göre (toplamsal tersin biricikliği),

$$-a = (-1)a \tag{4}$$

olur. Özel bir durum olarak $a = -1$ alırsak,

$$(-1)(-1) = -(-1) = 1$$

buluruz. Ayrıca, (4) sayesinde

$$-(xy) = x(-y) = (-x)y \tag{5}$$

eşitliklerini kolayca kanıtlayabiliriz, mesela

$$-(xy) = (-1)(xy) = ((-1)x)y = (-x)y.$$

(5) eşitlikleri sayesinde $-(xy)$, $(-x)y$ ve $x(-y)$ yerine, daha kısa olarak $-xy$ yazma hakkını kazanırız.

Şimdi sıralamayla ilgili olgulara geçelim. Okurun tanımlarını bildiğinden emin olduğumuz $\leq$, $>$ ve $\geq$ ikili ilişkilerini özgürce kullanacağız.

L. *Eğer $x < y$ ise $-y < -x$ olur.* Nitekim $x < y$ eşitsizliğinin her iki tarafına $(-x) + (-y)$ (yani $-x - y$) sayısını ekleyelim. TS'ye göre sıralama değişmez ve

$$x + ((-x) + (-y)) < y + ((-x) + (-y))$$

eşitsizliğini elde ederiz. Bu da aynen $-y < -x$ demektir.

Bunun özel bir durumu olarak, $y = 0$ alarak,

$$0 < x \iff -x < 0$$

buluruz.

M. *Her a için, $(-a)^2 = a^2 \geq 0$ olur.* (Burada x^2 elbette xx anlamına geliyor.) Birinci eşitlik (K) ve (F)'den çıkar:

$$(-a)^2 = (-a)(-a) \overset{K}{=} (-1)a(-a) = a((-1)(-a)) \overset{K}{=} a(-(-a)) \overset{F}{=} aa = a^2.$$

$a^2 \geq 0$ eşitsizliğini kanıtlayalım. Eğer $0 < a$ ise her iki tarafı da a ile çarpalım, $0 = 0a < aa = a^2$ buluruz. Eğer $a = 0$ ise $a^2 = 0 \geq 0$ olur. Eğer $a < 0$ ise, (L)'den dolayı $0 < -a$ olur ve ilk kanıtladığımızdan, $0 < (-a)^2 = a^2$ çıkar.

N. $0 < 1$ *olur.* Bunu, (M) maddesinde $a = 1$ alarak hemen bulabiliriz. Bir başka kanıt daha sunalım. "Olmayana ergi" yöntemini kullanacağız. Diyelim 0, 1'den küçük değil. O zaman S4 ve SB'ye göre $1 < 0$ olur. Bundan ve (M)'den $0 < -1$ çıkar. Bu son $0 < -1$ eşitsizliğinin her iki tarafını da 0'dan büyük olan -1 ile çarpalım, SÇ'den dolayı $0(-1) < (-1)(-1)$, yani $0 < 1$ çıkar, varsayımımızla çeliştik. Demek ki (SB'den dolayı) $0 < 1$.

O. *Eğer $xy = 0$ ise, ya $x = 0$ ya da $y = 0$ olur.* Bunu kanıtlayalım. Diyelim $x \neq 0$ ve $y \neq 0$. Gerekirse xy eşitliğini -1 ile çarparak ve (5) ve (L)'yi kullanarak $0 < x$ varsayımını yapabiliriz. Benzer şekilde $0 < y$ varsayımını da yapabiliriz. Şimdi $0 < x$ eşitsizliğinin taraflarını 0'dan büyük olduğunu bildiğimiz y ile çarpalım. $0 < xy$ elde ederiz. S1'den dolayı $xy = 0$ olamaz. Demek ki ya $x = 0$ ya da $y = 0$.

Ö. *Eğer $xy > 0$ ise, x ve y her ikisi birden ya pozitif ya da negatif olmak zorundadır.* Nitekim eğer $0 < x$ ve $y < 0$ ise, $0 < -y$ olur. Dolayısıyla $0 < x$ eşitsizliğinin taraflarını pozitif olan $-y$ ile çarparsak $0 < -xy$ buluruz ve bundan da $xy < 0$ çıkar, çelişki. Benzer şekilde $0 < y$ ve $x < 0$ olamaz.

Yukarıdaki olguları kanıtlarken (Ne)'yi (15'inci, yani son aksiyomu) kullanmadığımıza dikkatinizi çekerim. Demek ki bu olgular ilk 14 aksiyomu sağlayan tüm yapılar için geçerli; örneğin, daha sonra tanımlayacağımız

$$(\mathbb{Q}, +, \times, <, 0, 1) \text{ ve } (\mathbb{R}, +, \times, <, 0, 1)$$

(sırasıyla kesirli sayı ve gerçel sayı) yapıları için de geçerlidir, ikinci bir defa kanıtlamaya gerek yok. Ama mesela

$$xy = 1 \text{ ise ya } x = y = 1 \text{ ya da } x = y = -1$$

önermesi $\mathbb{Z}$'de doğru ama $\mathbb{Q}$ ve $\mathbb{R}$'de yanlıştır. Dolayısıyla bu önermeyi kanıtlamak için illa ki (Ne) aksiyomunu kullanmalıyız. Kanıtlayalım:

P. *Eğer* $xy = 1$ *ise, ya* $x = y = 1$ *ya da* $x = y = -1$ *olur.* Bunu kanıtlayalım. $xy = 1 > 0$ olduğundan, (Ö)'den dolayı x ve y (ikisi birden) ya pozitif ya da negatif. Birinci durumda, (Ne)'den dolayı $x, y \in \mathbb{N}$ olur. Ama $xy = 1$ denkleminin doğal sayılarda tek bir çözümü olduğunu biliyoruz: $x = y = 1$. İkinci durumu ele alalım: $x, y < 0$. Bu durumda $0 < -x$, $-y$ ve $(-x)(-y) = 1$ olur. Bir satır önce kanıtladığımızdan $-x = -y = 1$ çıkar, yani $x = y = -1$.

Ola ki bazı basit ve temel olguları kanıtlamayı unutmuşuzdur ya da yer darlığından dolayı kanıtlamamışızdır. Okur o basit olguları kendi başına kanıtlayabilmelidir.

4. Tamsayılarda Bölme

4.1 Bölme ve Bölünme

n, $m \in \mathbb{Z}$ tamsayıları için nm olarak yazılan sayılara n'nin (tamsayı) ***katı*** adı verilir. Örneğin 48, 8'in bir (tamsayı) katıdır, ama aynı zamanda -6'nın da bir katıdır. nm sayısı tabii ki hem n'nin hem de m'nin katıdır, aynı zamanda hem $-n$'nin hem de $-m$'nin katıdır. Bu tanımı şöyle de yapabilirdik: n, $a \in \mathbb{Z}$ olsun; eğer bir $m \in \mathbb{Z}$ için $a = nm$ oluyorsa, a'ya n'nin katı denir. Bir başka tanım da şöyle olabilirdi: Eğer $a = nx$ denkleminin tamsayılarda bir çözümü varsa, a'nın n'nin bir (tamsayı) katı olduğu söylenir.

n'nin (tamsayı) katlarının kümesi $n\mathbb{Z}$ olarak gösterilir:

$$n\mathbb{Z} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}.$$

Görüldüğü üzere "doğal sayı katı olmak"la "tamsayı katı olmak" arasında çok küçük de olsa bir fark var. Örneğin -48, -6'nın bir doğal sayı katıdır (8 katıdır) ve tabii ki aynı zamanda bir tamsayı katıdır (ne de olsa 8 bir tamsayıdır). Ama 48, -6'nın sadece bir tamsayı katıdır (-8 katıdır), bir doğal sayı katı değildir. Bu iki kavram arasındaki fark hemen hemen hiçbir zaman önemli olmayacak, dolayısıyla mecbur kalmadıkça bu iki kavram arasında bir ayrım yapmayacağız. Zaten tamsayılarda, bölünebilirlik açısından, x ile $-x$ arasında bir fark yoktur, biri bir başka sayıyı bölerse diğeri de böler, biri bir başka sayıya bölünürse diğeri de bölünür; bu yüzden sadece bölünmeyle ilgili bir cümle kurulduğunda x ile $-x$ arasında bir ayrım yapmak gereksizdir. Hatta bazı kitaplarda (aslında çoğunda) -5 mesela bir asal kabul edilir, ama 5 ile -5'in "denk" olduğu söylenir.

Eğer a, n'nin bir katıysa, n'nin a'yı (tamsayılarda) ***böldüğü*** ya da a'nın n'ye (tamsayılarda) ***bölündüğünü*** söylenir. Bunu

$$n|a$$

olarak gösteririz. Örneğin 80, 10'un bir katıdır, yani 80, 10'a bölünür, yani 10, 80'i böler. Bir başka örnek: -6 sayısı 18 sayısını $\mathbb{Z}$'de böler, nitekim $(-6)x = 18$

denkleminin $\mathbb{Z}$'de bir çözümü vardır: $x = -3$. Ayrıca n'nin a'nın bir ***böleni*** ya da bazen ***çarpanı*** olduğu söylenir. Örneğin 12'nin bölenleri şu sayılardır:

$$-12,\ -6,\ -4,\ -3,\ -2,\ -1,\ 1,\ 2,\ 3,\ 4,\ 6,\ 12.$$

Bu listeyi şöyle yazmak bize yer ve zaman kazandırır:

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12.$$

Eğer n, a'yı bölüyorsa, $-n$ de a'yı böler; ayrıca n, $-a$'yı da böler. Örneğin 12 ile -12'nin bölenleri aynıdır.

Doğal sayılarda $a|b$ ve $b|a$ ise $a = b$ olmak zorundadır. Tamsayılarda bu doğru olmasa da buna yakın bir ifade doğru: a ve b tamsayıları için $a|b$ ve $b|a$ ise $a = \pm b$ olur, yani a ya b'ye ya da $-b$'ye eşittir.

1 ve -1 tüm tamsayıları böler ve bu iki sayı bu özelliği olan yegâne tamsayılardır. 1 ve -1'den başka ortak böleni olmayan iki tamsayıya ***aralarında asal*** sayılar denir. Örneğin -145 ve 38 aralarında asal sayılardır.

0 her sayıya bölünür çünkü her $n \in \mathbb{Z}$ için $nx = 0$ denkleminin bir çözümü vardır, örneğin $x = 0$. Dikkat ederseniz 0, 0'ı da böler, yani 0, 0'a bölünür. Öte yandan 0 sadece 0'ı böler, başka da bir sayıyı bölmez, çünkü $0x = a$ denkleminin sadece $a = 0$ ise bir çözümü vardır, hatta her x tamsayısı $0x = 0$ denkleminin bir çözümüdür.

Bölünebilirlik ilişkisini kümelerle ifade edebiliriz:

$$m|n \iff n \in m\mathbb{Z} \iff n\mathbb{Z} \subseteq m\mathbb{Z}$$

olur, yani yukarıdaki üç önerme eşdeğerdir, bir başka deyişle biri doğruysa diğerleri de doğrudur. Böylece sayılar kuramıyla kümeler kuramı arasında bir geçiş yapılır ve bu çoğu zaman hayatımızı kolaylaştırır.

Eğer $n \neq 0$ ise ve n, a'yı bölüyorsa, yani $nx = a$ denkleminin tamsayılarda bir çözümü varsa, o zaman bu çözüm bir tanedir, nitekim

$$nx_1 = a \text{ ve } nx_2 = a$$

ise

$$n(x_1 - x_2) = nx_1 - nx_2 = a - a = 0$$

olur; $n(x_1 - x_2) = 0$ eşitliğinden de ($n \neq 0$ olduğundan, sayfa 33'teki O maddesinden dolayı) $x_1 - x_2 = 0$, yani $x_1 = x_2$ elde ederiz. Bu durumda, yani $n \neq 0$ ise ve x tamsayısı $nx = a$ eşitliğini sağlıyorsa, x sayısına "a bölü n" denir ve

$$x = a/n \text{ ya da } x = \frac{a}{n}$$

olarak yazılır. Demek ki her x, a, n tamsayısı için, eğer $n \neq 0$ ise

$$x = a/n \iff nx = a$$

olur.

$2\mathbb{Z}$ kümesindeki tamsayılara (yani 2'nin katlarına) çift tamsayı (ya da kısaca sayı) denir. $2\mathbb{Z}$ kümesinde olmayan tamsayılar $2\mathbb{Z}+1$ kümesindedir; $2\mathbb{Z}+1$ kümesindeki tamsayılara da tek tamsayı denir. Birazdan bir tamsayının aynı zamanda hem tek hem de çift olmadığını kanıtlayacağız.

Genel olarak, $m\mathbb{Z}+k$ kümesinin ögeleri, $m\mathbb{Z}$ kümesinin ögelerine k sayısı eklenerek elde edilir:

$$m\mathbb{Z}+k=\{mx+k : x\in\mathbb{Z}\}.$$

Örneğin,

$$9\mathbb{Z}+4=\{\ldots,-23,\ -14,\ -5,\ 4,13,\ 22,\ 31,\ 40,\ \ldots\}.$$

Bu arada,

$$9\mathbb{Z}+4=9\mathbb{Z}+13=9\mathbb{Z}+22=9\mathbb{Z}+(-14)$$

gibi eşitliklere dikkatinizi çekerim. $9\mathbb{N}+4\neq 9\mathbb{N}+13$, ama $\mathbb{N}$ yerine $\mathbb{Z}$ aldığımızda eşitlik sağlanıyor.

$a/0$ diye bir sayı tanımlamıyoruz. Ama eğer $n\neq 0$ ise, yukarıda da söylediğimiz gibi, $0/n$ diye bir sayı vardır ve bu sayı 0'a eşittir.

0'ın 0'ı böldüğüne ama $0/0$ diye bir sayının tanımlanmadığına bir defa daha dikkatinizi çekerim. 0, 0'ı böler çünkü $0x=0$ denkleminin çözümü vardır (her tamsayı bu denklemin bir çözümüdür) ama bu çözüm biricik olmadığından $0/0$ diye bir sayı tanımlamıyoruz. "0/0" ifadesini tanımsız bırakıyoruz.

"10/2" ifadesi de henüz tanımı yapılmadığında tanımsızdı. Elbette! Biz bu ifadeyi 5 olarak tanımladık. Ama "0/0" ifadesini tanımsız bırakmayı tercih ettik. İsteseydik tanımlardık (örneğin garip bir nedenden 5'e eşit olarak tanımlayabilirdik) ama hayatımız zorlaşır, kafamız karışırdı.

Örnekler

4.1. $3(7\mathbb{Z}+4)=21\mathbb{Z}+12$ eşitliğini kanıtlamak kolaydır. Nitekim sol taraftaki $3(7\mathbb{Z}+4)$ kümesinden alınan bir sayı, bir n tamsayısı için $3(7n+4)$ olarak yazılır, bu da $21n+12$'ye eşit olduğundan $21\mathbb{Z}+12$ kümesindedir. Diğer taraftan, $21\mathbb{Z}+12$ kümesinden alınan bir sayı, bir n tamayısı için $21n+12$'ye eşittir, ama $21n+12=3(7n+4)$ olduğundan, bu sayı $3(7\mathbb{Z}+4)$ kümesindedir.

4.2. $3(7\mathbb{Z}+4)+2=(21\mathbb{Z}+12)+2=21\mathbb{Z}+14=7(3\mathbb{Z}+2)$ olur.

4.3. $\mathbb{Z}=2\mathbb{Z}\cup(2\mathbb{Z}+1)$ olduğundan,

$$5\mathbb{Z}+3=5(2\mathbb{Z}\cup(2\mathbb{Z}+1))+3=(10\mathbb{Z}\cup(10\mathbb{Z}+5))+3=(10\mathbb{Z}+3)\cup(10\mathbb{Z}+8)$$

olur. Yukarıdaki eşitliklerin her birinin geçerli olduğunu kontrol edin lütfen.

4.4. $\mathbb{Z}=3\mathbb{Z}\cup(3\mathbb{Z}+1)\cup(3\mathbb{Z}+2)$ olduğundan[1],

$$5\mathbb{Z}+4=(15\mathbb{Z}+4)\cup(15\mathbb{Z}+9)\cup(15\mathbb{Z}+14)$$

olur.

[1]Neden? İleride bu tür eşitliklere etraflıca değineceğiz.

4.5. Tabii ki $5\mathbb{Z}-1 = 5\mathbb{Z}+4 = 5\mathbb{Z}+9 = 5\mathbb{Z}-6$ eşitlikleri doğrudur. Bunu metinde de görmüştük. Genel olarak, her $m \in \mathbb{Z}$ için, $n\mathbb{Z}+r = n\mathbb{Z}+r+nm$ olur. Yani $n\mathbb{Z}+r$ kümesinin ögelerine n'nin katlarını eklersek yine aynı kümeyi buluruz.

4.6. $(3\mathbb{Z}+2)(7\mathbb{Z}+3)$ kümesindeki sayıları betimlemek pek o kadar kolay değil. Bu sayılar, n, m tamsayıları için $(3n+2)(7m+3)$, yani $21nm+9n+14m+6$ biçiminde yazılan sayılardır. Bunların ne tür sayılar olduğunu bulmak kolay değildir. Sorunun ciddiyetini anlamak amacıyla, 6 sayısının bu türden bir sayı olmadığını, yani 0'ın $21n+9n+14m$ olarak yazılamayacağını kanıtlamaya çalışabilirsiniz.

Alıştırmalar

4.7. İki tek tamsayının toplamının ve farkının çift sayı olduğunu kanıtlayın.

4.8. Her tek tamsayının iki tamkarenin farkı olarak yazılabileceğini gösterin.

4.9. Eğer a bir çift sayıysa, elbette $a^2 \in 4\mathbb{Z}$ olur. Eğer a bir tek sayıysa, $a^2 \in 4\mathbb{Z}+1$ olduğunu kanıtlayın.

4.10. a ve b birer tek sayıysa, $a^2+b^2 \in 4\mathbb{Z}+2$ olduğunu kanıtlayın. Bundan a^2+b^2'nin bir tek sayı olamayacağını kanıtlayın. Bir önce alıştırmayı kullanarak, bundan a^2+b^2'nin bir tamkare olamayacağını kanıtlayın.

4.11. $p \neq 2$, 3 bir asal sayı olsun. $p \in (6\mathbb{Z}+1)\cup(6\mathbb{Z}+5)$ olduğunu gösterin. Buradan $p^2 \in 6\mathbb{Z}+1$ olduğunu çıkarın.

4.12. n bir tek sayıysa, $n^2 \in 8\mathbb{Z}+1$ olduğunu gösterin.

4.13. n bir tek sayıysa, $n^2 \in (16\mathbb{Z}+1)\cup(16\mathbb{Z}+9)$ olduğunu gösterin. İpucu: İsterseniz bir önceki alıştırmayı ve kanıtlayacağınız $8\mathbb{Z}+1 = (16\mathbb{Z}+1)\cup(16\mathbb{Z}+9)$ eşitliğini kullanabilirsiniz.

4.14. n herhangi bir tamsayıysa, $n^2 \notin (10\mathbb{Z}+2)\cup(10\mathbb{Z}+3)\cup(10\mathbb{Z}+7)\cup(10\mathbb{Z}+8)$ olduğunu gösterin. Yani bir tamkarenin 10 tabanındaki yazılımının 1'ler basamağı 2, 4, 7 ya da 8 olamaz.

4.15. Eğer hem n hem de n^2 sayıları $10\mathbb{Z}+k$ kümesindeyse k'nın 5'e bölündüğünü gösterin.

4.16. a ve b iki tamsayı olsun. $a+b$ ve $a-b$ sayılarının ya her ikisinin birden tek ya da her ikisinin birden çift olduğunu kanıtlayın.

4.17. İki tamkarenin farkının ya tek olduğunu ya da 4'e bölündüğünü kanıtlayın. (İpucu: $a^2-b^2 = (a-b)(a+b)$ eşitliğini ve bir önceki alıştırmayı kullanın.)

4.18. x bir tek sayı olsun. Eğer a ve b tamsayıları için $x = ab$ ise, a ve b tek sayıdır. Dolayısıyla

$$\frac{a+b}{2} \text{ ve } \frac{a-b}{2}$$

tamsayılarından bahsedebiliriz.

$$x = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

olduğunu gösterin. (Bu soru, bu ve önceki kitaplarımızda gösterilmeyen basit cebirsel beceriler gerektiriyor. Okurun bu becerilere aşina olduğunu biliyoruz.) Örneğin, $21 = 7\times 3$ olduğundan,

$$x = \left(\frac{7+3}{2}\right)^2 - \left(\frac{7-3}{2}\right)^2 = 5^2 - 2^2$$

olur.

4.19. Bir önceki alıştırmadan ve $2701 = 55^2 - 18^2$ eşitliğinden hareketle (doğruluğunu kontrol edin eğer bize güvenmiyorsanız), 2701 sayısını asallarına ayırın. (Bu yöntem Fermat'ya aittir. Ama tabii büyük bir sayıyı iki karenin farkı olarak yazabilmek de kolay bir uğraş değildir.)

4.20. Öyle bir x tamsayısı bulun ki, her n doğal sayısı için $x \in n\mathbb{Z} + (n-1)$ olsun.
4.21. $(2\mathbb{Z}+1) \cap (3\mathbb{Z}+2) \cap (5\mathbb{Z}+3)$ kümesinin bir ögesini bulun.
4.22. $(2\mathbb{Z}+1) \cap (3\mathbb{Z}+2) \cap (5\mathbb{Z}+3) = 30\mathbb{Z}+23$ eşitliğini kanıtlayın.
4.23. $(3\mathbb{Z}+1) \cap (5\mathbb{Z}+2) \cap (7\mathbb{Z}+3)$ kümesinin bir ögesini bulun.

Notlar

4.24. Alıştırma 4.19'da adı geçen ve aşağıda resmini gördüğünüz Fermat (1607-1665), 17'nci yüzyılın en önemli iki matematikçisinden biri olduğu söylenebilir. (Diğeri Descartes. Ama Pascal de yabana atılmamalı.) En çok sayılar kuramındaki işleriyle bilinir. Bunun dışında (geometriyi cebire indirgeyen) analitik geometri, olasılık, optik gibi konularda da önemli çalışmaları vardır. Analitik geometriyi Descartes'tan bağımsız olarak bulmuştur. Pascal ile yazışmalarından olasılık kuramı doğmuştur. Daha da önemlisi, türev kavramını Newton'dan 50 yıl önce bulmuştur. Hukuk eğitimi görmüştü ve hayatının sonuna kadar Toulouse'da yüksek hakim olarak çalıştı. Formel bir matematik eğitimi görmedi.

Avrupa'nın bilimsel merkezlerinden uzakta olmasından olacak, Fermat bol bol mektup yazdı. Zamanının ünlü matematikçi ve fizikçileriyle yazışmaları çok ünlüdür. O zamanlarda kanıtlar pek açıklanmazdı, kanıtlar bir çeşit meslek sırrı idi. Bu yüzden bulduğu birçok sonucu nasıl kanıtladığı bilinmemektedir.

4.2 Tamsayılarda Kalanlı Bölme

Doğal sayılarda kalanlı bölmeyi [2. Kitap, Teorem 6.4]'te gördük: Küçük bir kalana razı olursak her doğal sayıyı 0'dan farklı her doğal sayıya bölebiliriz, örneğin 28'i 3'e bölersek 9 çıkar ve kalan da 1'dir:

$$28 = 3 \cdot 9 + 1.$$

Benzer bir bölmeyi tamsayılarda da yapabiliriz. Örneğin 28'i -3'e bölmeye çalışalım. Aşağıdaki eşitliklerden her biri doğrudur:

$$\begin{aligned}
28 &= (-3)\cdot(-11)+(-5)\\
28 &= (-3)\cdot(-10)+(-2)\\
28 &= (-3)\cdot(-9)+1\\
28 &= (-3)\cdot(-8)+4\\
28 &= (-3)\cdot(-7)+7\\
28 &= (-3)\cdot(-6)+10\\
28 &= (-3)\cdot 0+28\\
28 &= (-3)\cdot 1+31\\
28 &= (-3)\cdot 2+34
\end{aligned}$$

Bunun gibi,

$$28 = (-3)q + r$$

türünden daha bir sürü (sonsuz sayıda) eşitlik doğrudur. "Kalanlı bölme" olarak bu sonsuz sayıdaki eşitlikten birini seçmeliyiz. "Kalan" dediğimiz sayı, yukarıdaki eşitliklerin en sağındaki sayılardan biri olacak. "Kalanlı bölme" hangisi olsun? Kalanı 1 olanı (üstten üçüncü eşitliği) seçeceğiz, yani 28'i -3'e kalanlı böldüğümüzde sonuç -9, kalan ise 1 çıkacak:

$$28 = (-3)\cdot(-9)+1.$$

Tanımın böyle olmasını istiyoruz. Kalanın (örnekte 1), bölenin (örnekte -3) mutlak değerinden (örnekte $|-3|$, yani 3) küçük olmasını istiyoruz.

Genel olarak n sayısını m sayısına kalanlı bölmek istediğimizde, kalanın m'nin mutlak değerinden küçük bir doğal sayı olmasını istiyoruz.

Teorem 4.1. *n ve m iki tamsayı olsun. $m \neq 0$ olsun. O zaman*

$$0 \leq r < |m| \text{ ve } n = mq + r$$

koşullarını sağlayan q ve r tamsayıları vardır. Ayrıca bu koşulları sağlayan q ve r tamsayıları biriciktir.

Kanıta girişmeden önce dört örnek verelim:

n	m	q	r	$n = mq + r$ kalanlı bölmesi
29	6	4	5	$29 = 6\cdot 4+5$
29	-6	-4	5	$29 = (-6)\cdot(-4)+5$
-29	6	-5	1	$-29 = 6\cdot(-5)+1$
-29	-6	5	1	$-29 = (-6)\cdot 5+1$

Bu örneklerin her birinde $n = \pm 29$ sayısını $m = \pm 6$ sayısına kalanlı böldük ve $n = mq + r$ eşitliğini sağlayan bir $q \in \mathbb{Z}$ ve bir $r \in \{0, 1, \ldots, |m| - 1\} = \{0, 1, 2, 3, 4, 5\}$ sayısı bulduk.

Genel olarak, teoremin ilk cümlesi, her $m \neq 0$ tamsayısı için

$$\mathbb{Z} = m\mathbb{Z} \cup (m\mathbb{Z} + 1) \cup (m\mathbb{Z} + 2) \cup \ldots \cup (m\mathbb{Z} + (|m| - 1))$$

eşitliğini söylüyor. İkinci cümle ise, yukarıdaki eşitliğin sağındaki $n\mathbb{Z}+i$ altkümelerinin ikişer ikişer ayrık olduğunu söylüyor. Altkümeler ayrık olduğunda, $\cup$ bileşim işareti yerine $\sqcup$ bileşim işareti kullanılır, yani her $m \neq 0$ tamsayısı için,

$$\mathbb{Z} = m\mathbb{Z} \sqcup (m\mathbb{Z} + 1) \sqcup (m\mathbb{Z} + 2) \sqcup \ldots \sqcup (m\mathbb{Z} + (|m| - 1))$$

olur. Örneğin,

$$\mathbb{Z} = 2\mathbb{Z} \sqcup (2\mathbb{Z} + 1)$$

(her tamsayı ya tektir ya çifttir ve ikisi birden olamaz) ya da

$$\mathbb{Z} = 3\mathbb{Z} \sqcup (3\mathbb{Z} + 1) \sqcup (3\mathbb{Z} + 2)$$

ya da

$$\mathbb{Z} = (-4)\mathbb{Z} \sqcup ((-4)\mathbb{Z} + 1) \sqcup ((-4)\mathbb{Z} + 2) \sqcup ((-4)\mathbb{Z} + 3).$$

Tabii $-4\mathbb{Z} = 4\mathbb{Z}$ olduğundan, yukarıdaki eşitlik

$$\mathbb{Z} = 4\mathbb{Z} \sqcup (4\mathbb{Z} + 1) \sqcup (4\mathbb{Z} + 2) \sqcup (4\mathbb{Z} + 3)$$

olarak da yazılabilir ama bir -4'e bölünebilirliğe odaklanmak istediğimizden $(-4)\mathbb{Z}$ yazdık.

Matematiksel jargonla, her $m \in \mathbb{Z}$ sayısı, $\mathbb{Z}$ kümesini, ögelerinin m'ye bölündüğünde kalanlarına göre, $|m|$ farklı "sınıf"a ayırır. Yukarıdaki örneklerde sırasıyla 2, 3 ve 4 sınıf var.

Kanıt: Önce

$$s(m) = \frac{|m|}{m} \tag{1}$$

tanımını yapalım (bkz. Alıştırma 2.113). Eğer $m > 0$ ise $s(m) = 1$, eğer $m < 0$ ise $s(m) = -1$ olur; yani m'nin pozitif ya da negatifliğine göre $s(m) = \pm 1$ olur. Bu tanım kanıtımızı bir parça kısaltacak. Bu arada $|m| = s(m)m$ eşitliğine dikkatinizi çekerim, aşağıda gerekecek.

Şimdi şu kümeye bakalım:

$$A = \{n - mq : q \in \mathbb{Z}\}.$$

Bu küme sonsuzdur çünkü m'yi 0'dan farklı aldık, dolayısıyla farklı q tamsayıları kullanarak kümenin birbirinden farklı $n - mq$ sayılarını elde ederiz.

Bu kümenin 0'dan büyükeşit sayılar içerdiğini görmek de pek zor değil, mesela $q = -s(m)|n|$ alırsak,

$$n - mq = n - m(-s(m)|n|) = n + ms(m)|n| = n + |m||n| \geq n + |n| \geq 0$$

olur. Demek ki $A \cap \mathbb{N}$ kesişimi boşküme değil. Bu kesişimde bulunan en küçük doğal sayıyı alalım. (Burada doğal sayılarda geçerli olan iyisıralama özelliğini kullanıyoruz, bkz. [2. Kitap, sayfa 81].) Bu sayıya r diyelim. $r \in A$ olduğundan, bir $q \in \mathbb{Z}$ için

$$n - mq = r,$$

yani

$$n = mq + r \tag{2}$$

olur. $0 \leq r$ eşitsizliğini zaten biliyoruz, çünkü r'yi bir doğal sayı seçtik. Şimdi $r < |m|$ eşitsizliğini kanıtlayalım. Eğer bu eşitsizlik doğru olmasaydı, o zaman $r \geq |m|$ eşitsizliği doğru olurdu, ki bundan $r - |m| \geq 0$ çıkar. Ama (1) ve (2)'nin bir sonucu olan

$$n = m(q + s(m)) + (r - |m|)$$

eşitsizliğinden, $r - |m|$ sayısının A kümesinde olduğu anlaşılıyor. Ama tabii $m \neq 0$ olduğundan $r - |m| < r$ olur, bu da r'nin A'daki en küçük doğal sayı olmasıyla çelişir. Demek ki $r \leq |m|$ eşitsizliği doğru olmak zorunda.

Şimdi sıra bulunan koşulları sağlayan q ve r tamsayılarının biricik olduğunu kanıtlamaya geldi. Diyelim $0 \leq r$, $r_1 < |m|$ ve q ve q_1 tamsayıları için

$$mq + r = mq_1 + r_1 \tag{3}$$

eşitliği doğru. Bir çelişki elde etmek amacıyla $r_1 > r$ varsayımını yapalım. Bu varsayımdan ve eşitlikten

$$m(q - q_1) = mq - mq_1 = r_1 - r > 0$$

çıkar. Demek ki $m(q - q_1)$ sayısı pozitif. Eğer $m \leq 0$ ise $m \leq m(q - q_1)$ eşitsizliği elbette geçerli; ama $m > 0$ ise $q - q_1 > 0$ olmak zorunda olduğundan aynı eşitsizlik gene geçerli. Demek ki her durumda

$$m \leq m(q - q_1) = r_1 - r < m - r \leq m$$

olur, yani $m < m$ olur, bir çelişki. Demek ki $r_1 > r$ varsayımı doğru olamaz. Aynı şekilde $r > r_1$ varsayımı da doğru olamaz. Demek ki $r = r_1$. Bu ve (3) eşitliği $mq = mq_1$ eşitliğini verir ve $m \neq 0$ olduğundan, bundan da $q = q_1$ çıkar. □

Buraya kadar temel tanımları gördük. Kitabın bundan sonrasında tamsayılarda daha derine ineceğiz. İlk olarak meşhur (ve son derece önemli ve kullanışlı) Bézout teoremlerini kanıtlayacağız. Ardından asallığın, obeb ve okek'in çok daha derinine ineceğiz. Kanıtlayacağımız en temel sonuç Aritmetiğin Temel Teoremi (Teorem 7.2), o sonuç bilinmeden olmaz. Ama dileyen okur, bu kitaba daha sonra geri gelmek üzere, sonraki iki kitaba geçerek önce kesirli ve gerçel sayıların tanımını ve başat özelliklerini görebilir, çok bir sakıncası olmaz, sadece biraz olur.

Örnekler

4.25. Bugün günlerden salıysa, 365 gün sonra günlerden ne olur? Her 7 günde bir günler tekrarlandığından ve

$$365 = 7 \times 52 + 1$$

olduğundan, 365 gün sonra günlerden çarşamba olur.

4.26. Saat 15,30'dan sonra 1000 saat geçerse, saat kaçı gösterir? Her 24 saatte saat eski yerine geri geldiğinden ve

$$100 = 24 \times 41 + 16$$

olduğundan, aradan 16 saat geçtiğini varsayabiliriz. 15,30'a 16 saat eklersek, 31,30 eder. Ama tabii saat 31,30 olamaz, bundan 24'ü çıkarmamız lazım; doğru cevap 7,30'dur.

4.27. Şu anda saat 5'i 10 geçiyor. 1000 dakika sonra saat kaç olur? Her 60 dakikada 1 saat attığından ve

$$1000 = 60 \times 16 + 40$$

olduğundan, 1000 dakikada 16 saat 40 dakika geçti demektir. Dolayısıyla cevap 21,50'dir.

4.28. Saat 4'ü 10 geçtikten sonra yelkovan 9120 derece döndüğünde, saat kaçı gösterir? Her 360 derece dönüşte 1 saat attığından ve

$$9120 = 360 \times 25 + 120$$

olduğundan, aradan 25 saat geçmiş (demek ki 1 gün atmış ve akrep 1 saat ileriyi gösteriyor) ve yelkovan fazladan 120 derece dönmüştür. Her dakika $360/60 = 6$ dereceye tekabül ettiğinden, 120 derece de $120/6 = 20$ dakikaya tekabül eder. Demek ki saat 1 saat 20 dakika sonrayı gösterir, yani saat 5,30 olur.

4.29. $2^6 13^7 + 3^8 11^5$ sayısı 17'ye bölününce kalanını hesaplayalım. $2^4 = 16 \in 17\mathbb{Z} - 1$ ve $2^2 = 4 \in 17\mathbb{Z} + 4$ olduğundan,

$$2^6 = 2^4 2^2 \in (17\mathbb{Z} - 1)(17\mathbb{Z} + 4) \subseteq 17\mathbb{Z} - 4$$

olur. (Aslında yukarıda $\subseteq$ küme içindeliği yerine eşitlik de yazabilirdik, ama bu önemli olmayacak.) Şimdi 13^7 sayısını ele alalım. $13 \in 17\mathbb{Z} - 4$ olduğundan

$$13^2 \in (17\mathbb{Z} - 4)(17\mathbb{Z} - 4) \subseteq 17\mathbb{Z} + 16 = 17\mathbb{Z} - 1$$

olur; buradan da

$$13^7 = (13^2)^3 13 \in (17\mathbb{Z} - 1)13 \subseteq 17\mathbb{Z} - 13 = 17\mathbb{Z} + 4$$

çıkar. Demek ki

$$2^6 13^7 \in (17\mathbb{Z} - 4)(17\mathbb{Z} + 4) \subseteq 17\mathbb{Z} - 16 = 17\mathbb{Z} + 1$$

olur. Şimdi toplanan ikinci terim olan $3^8 \cdot 11^5$ sayısını ele alalım.

$$3^2 = 9 \in 17\mathbb{Z} + 9 = 17\mathbb{Z} - 8$$

olduğundan,

$$3^4 = \left(3^2\right)^2 \in 17\mathbb{Z} + 64 = 17\mathbb{Z} + 13 = 17\mathbb{Z} - 4$$

ve

$$3^8 = \left(3^4\right)^2 \in 17\mathbb{Z} + 16 = 17\mathbb{Z} - 1$$

olur. Öte yandan, $11 \in 17\mathbb{Z} + 11 = 17\mathbb{Z} - 6$ olduğundan,

$$11^2 \in 17\mathbb{Z} + 36 = 17\mathbb{Z} + 2$$

ve

$$11^3 = 11^2 11 \in 17\mathbb{Z} + 22 = 17\mathbb{Z} + 5$$

ve

$$11^5 = 11^2 11^3 \in (17\mathbb{Z} + 2)(17\mathbb{Z} + 5) \subseteq 17\mathbb{Z} + 10$$

olur. Bütün bunlardan

$$3^8 11^5 \in (17\mathbb{Z} - 1)(17\mathbb{Z} + 10) \in 17\mathbb{Z} - 10 = 17\mathbb{Z} + 7$$

çıkar. Daha önce bulduğumuzla birlikte istediğimiz yanıtı buluruz:

$$2^6 13^7 + 3^8 11^5 \in (17\mathbb{Z} + 1) + (17\mathbb{Z} + 7) = 17\mathbb{Z} + 8.$$

Demek ki $2^6 13^7 + 3^8 11^5$ sayısı 17'ye bölündüğünde kalan 8 imiş.

4.30. 0'dan farklı bir doğal (ya da tam) sayının tamsayı böleni sayısı, doğal sayı böleni sayısının iki katıdır çünkü her d doğal sayı böleni için bir de $-d$ tamsayı böleni vardır. Örneğin 15'in doğal sayı bölenleri 1, 3, 5 ve 15'tir, yani 4 tanedir. Ama doğal sayı bölenleri bunun iki misli kadardır, çünkü bu sayılara bir de -1, -3, -5 ve -15 eklenir.

4.31. Eğer a ve b sayıları bir $m > 1$ sayısına bölündüğünde kalan 1 ise, ab de m sayısına bölündüğünde kalan 1 olur. Nitekim eğer $a = mx + 1$ ve $b = my + 1$ ise

$$ab = (mx + 1)(my + 1) = m(mxy + x + y) + 1$$

olur. Demek ki m'ye bölündüğünde kalanın 1 olduğu sayıların çarpımı da m'ye bölündüğünde kalanı 1 olur.

4.32. Bir önceki örnekten, eğer a sayısı bir $m > 1$ sayısına bölündüğünde kalan 1 ise, a'nın tüm kuvvetlerinin de m'ye bölündüğünde kalanın 1 olduğu anlaşılır.

Alıştırmalar

4.33. $2^6 13^7$ sayısı 18'e bölününce kalan kaç olur?

4.34. $3^8 11^5$ sayısı 18'e bölününce kalan kaç olur?

4.35. $2^6 13^7 + 3^8 11^5$ sayısı 18'e bölününce kalan kaç olur?

4.36. $2^6 13^7 + 3^8 11^5$ sayısı 19'a bölününce kalan kaç olur?

4.37. Bir n sayısı $m > 1$ sayısına bölündüğünde kalan $m - 1$ ise, n^2 sayısının m'ye bölündüğünde kalanın 1 olduğunu kanıtlayın.

4.38. Bir n sayısı $m > 1$ sayısına bölündüğünde kalanı $m - 1$ ise, n^k sayısının m'ye bölündüğünde kalanın 1 ya da -1 olduğunu kanıtlayın. Kalan ne zaman 1, ne zaman -1 olur?

4.39. Bir n sayısı 10'a bölündüğünde kalan 6 ise, her $k > 0$ için, n^k sayısı da 10'a bölündüğünde kalan 6 olur. Kanıtlayın.

4.40. Bir n sayısı 10'a bölündüğünde kalan 5 ise, her $k > 0$ için, n^k sayısı da 10'a bölündüğünde kalan 5 olur. Kanıtlayın.

Bir sonraki bölüme hazırlık olması açısından aşağıdaki örneklere bir göz atmanızı dilerim.

Örnekler

4.41. *4 ve 7'yi toplayarak elde edemeyeceğimiz en büyük sayı kaçtır?*
$18 = 7 + 7 + 4$ olduğundan 18'i elde edebiliriz. $19 = 4 + 4 + 4 + 7$ olduğundan 19'u da elde ederiz. $20 = 4+4+4+4+4$ ve $21 = 7+7+7$ olduğundan 20 ve 21'i de elde ederiz. Demek ki 18, 19, 20 ve 21 elde edilebiliyor. Bu sayılara 4'ü ekleyerek tümsayıları elde edebiliriz. Demek eğer $d \geq 18$ ise

$$d = 4a + 7b$$

eşitliğini sağlayan a ve b doğal sayıları var. Ama 17'yi elde edemeyeceğimizi görmek zor değil: Teker teker $b = 0$, 1, 2 denenince a bir doğal sayı çıkmıyor.
Ama sadece toplamaya değil, çıkarmaya da hakkımız olsaydı, o zaman her doğal sayıyı (hatta her tamsayıyı) elde edebilirdik; nitekim eğer $d \in \mathbb{Z}$ rastgele bir tamsayıysa, $a = 2d$, $b = -d$ alarak

$$4a + 7b = d$$

eşitliğini elde ederiz.

4.42. 9 ve 16 litrelik iki kovayla ve iki de çok büyük boş kovayla 7 litreyi ölçebiliriz, bunun için 16 litrelik kovadan 9 litre çıkarmak yeterli. 23 litre de ölçülür: Büyük kovalardan birine iki defa 16'şar litre koyalım, elde edilen 32 litreden 9 litre çıkaralım. Ama mesela 20 litreyi ölçebilir miyiz? Asıl marifet 1 litreyi elde etmede; eğer 1 litre edebilirsek, 1 litre için yaptığımız işlemleri tekrarlayarak (ve yukarıda kullanmadığımız ikinci büyük kovayı kullanarak) istediğimiz miktarı elde edebiliriz.

$$4 \times 16 - 7 \times 9 = 1$$

olduğundan 1 litreyi elde edebiliriz: 4 defa 16 litre koy, 7 defa 9 litre boşalt, geriye 1 litre kalır. Ama 20 litreyi tek bir büyük boş kovayla elde edebilir misiniz?

Alıştırmalar

4.43. a ve b birer tamsayı olsun. $a + b$ ve $a - b$ sayıları 3'e bölünüyorsa a ve b sayılarının da 3'e bölündüğünü gösterin.

4.44. a, b ve c birer tamsayı olsun. $a + b - c$, $a - b + c$ ve $-a + b + c$ sayıları 3'e bölünüyorsa a, b ve c sayılarının da 3'e bölündüğünü gösterin.

4.45. $17\mathbb{Z} + 7$ kümesinin, 17'ye bölündüğünde kalanın 7 olduğu tamsayılar kümesi olduğunu kanıtlayın.

4.46. $(17\mathbb{Z} + 1) \cdot 8 \subseteq 17\mathbb{Z} + 8$ önermesini gösterin.

4.47. $(17\mathbb{Z} + 1) \cdot 24 \subseteq 17\mathbb{Z} + 7$ önermesini gösterin.

4.48. $(17\mathbb{Z} + 3) \cdot 8 \subseteq 17\mathbb{Z} + 7$ önermesini gösterin.

4.49. $(17\mathbb{Z} + 3) \cdot 8 \subseteq 8\mathbb{Z}$ önermesini gösterin.

4.50. $(17\mathbb{Z} + 7) \cdot (17\mathbb{Z} + 8) = 17\mathbb{Z} + 5$ önermesini gösterin.

4.51. $3x + 5y = 7$ eşitliğini sağlayan tüm x ve y tamsayı çiftlerini bulun.

4.52. $5x + 7y = 9$ eşitliğini sağlayan tüm x ve y tamsayı çiftlerini bulun.

4.53. a, b ve c üç tamsayı olsun. $ax + by = c$ eşitliğini sağlayan x_0 ve y_0 tamsayılarının olduğunu varsayalım. Bu denklemin tüm çözümlerinin, $ax + by = 0$ eşitliğini sağlayan x ve y için, $x + x_0$ ve $y + y_0$ biçiminde yazıldığını gösterin.

4.54. p, 5'ten büyük bir asal sayı olsun. $p^2 - 1$'in 24'e bölündüğünü kanıtlayın.

4.55. p, 5'ten büyük bir asal sayı olsun. Ya $p^2 - 1$'in ya da $p^2 - 19$'un 30'a bölündüğünü kanıtlayın.

4.56. 63'e böldüğümüzde 5 kalanını veren, ama 67'ye böldüğümüzde 1 kalanını veren bir sayı bulabilir misiniz? (Siz zahmet etmeyin, biz verelim cevabı: 4289, istenen özellikleri sağlayan en küçük doğal sayıdır. Gelecek bölümlerde bu tür sorulara odaklanacağız. Ama kendi kendinize benzer sorular üretip çözmeye çalışırsanız, sorunun zorluğunu daha iyi kavrayıp gelecek bölümlerde yapacaklarımıza daha fazla değer verirsiniz.)

5. Bézout Teoremi

İki doğal sayının en büyük ortak bölen kavramını önceki kitapta ele almıştık. Aynı kavramı bu bölümde başka bir bakış açısıyla irdeleyeceğiz.

a ve b iki tamsayı olsun, ama her ikisi birden 0 olmasın. Doğal sayılarda olduğu gibi, a ve b'nin en büyük ortak bölenini obeb(a, b) olarak göstereceğiz. Örneğin -15 ile 9'un en büyük ortak böleni 3'tür. -15 ile -9'un da en büyük ortak böleni 3'tür. Elbette

$$\text{obeb}(a, b) = \text{obeb}(|a|, |b|)$$

olur, yani tamsayılarda obeb ile doğal sayılarda obeb arasında pek bir fark yoktur. Mesela şu doğrudur: Eğer $d = \text{obeb}(a, b)$ ise, obeb$(a/d, b/d) = 1$ olur, yani a/d ile b/d birbirlerine asaldır.

a ve b tamsayılarını sabitleyip şu kümeye bakalım:

$$A = \{au + bv : \ u, \ v \in \mathbb{Z}, \ au + bv > 0\}.$$

A elbette $\mathbb{N}$ kümesinin bir altkümesidir. Ayrıca boşküme değildir, çünkü eğer $u = a$ ve $v = b$ alırsak, $a^2 + b^2$ sayısının A'da olduğunu anlarız (ya a ya da b sayısı 0'dan farklı olduğundan, $a^2 + b^2 \neq 0$ olur). Demek ki A, $\mathbb{N}$'nin boş olmayan bir altkümesi. İyisıralama özelliğinden dolayı [2. Kitap, sayfa 81] A'nın en küçük bir ögesi vardır. A'nın bu en küçük ögesine d diyelim. Şimdi d'nin a ve b sayılarının en büyük ortak böleni olduğunu iddia ediyoruz ve hemen kanıtlamaya koyuluyoruz. $d \in A$ olduğundan, u, $v \in \mathbb{Z}$ tamsayıları için,

$$d = au + bv$$

olur. a'yı d'ye kalanlı bölelim: Bir $0 \leq r < d$ ve bir $q \in \mathbb{Z}$ için

$$a = dq + r$$

olur. Bu iki eşitlikten,

$$a = (au + bv)q + r$$

elde ederiz. Buradan,

$$0 \leq r = a(1 - uq) + (-bq)v$$

çıkar. Demek ki d'den daha küçük olan r sayısının A kümesinde olmasına ramak kalmış; 0'dan farklı olsa A'da olacak! d'den küçük pozitif bir doğal sayı A'da olamayacağından, $r = 0$ olmalı. Demek ki $a = dq + r = dq + 0 = dq$ ve d, a'yı bölüyor. Benzer biçimde d'nin b'yi de böldüğü çıkar. Böylece d sayısının a ve b'nin ortak bir böleni olduğunu kanıtlamış olduk.

Şimdi d'nin a ve b'nin en büyük ortak böleni olduğunu kanıtlamalıyız. Ama bu çok kolay: Eğer e sayısı a ve b'yi bölüyorsa, $d = au + bv$ eşitliğinden dolayı e sayısı d'yi de böler. $d > 0$ olduğundan bundan $e \leq d$ çıkar (Alıştırma 2.111).

Bu kanıtladığımızı "teorem" adı altında kaydedelim:

Teorem 5.1. *a ve b iki tamsayı olsun ama her ikisi birden 0 olmasın. a ve b'nin en büyük ortak böleni, u, $v \in \mathbb{Z}$ için,*

$$d = au + bv > 0$$

eşitsizliğini sağlayan en küçük d doğal sayısıdır. □

Bu teoremin bariz ama çok kullanışlı bir sonucu:

Teorem 5.2 (Bézout Teoremi I)**.** *a ve b iki tamsayı olsun ama her ikisi birden 0 olmasın. $d = \text{obeb}(a, b)$ olsun. O zaman*

$$d = au + bv$$

eşitliğini sağlayan u ve v tamsayıları vardır. □

Bu teoremin ters istikameti doğru değildir, yani $d = au + bv$ eşitliğini sağlayan u ve v tamsayılarının varlığı d'nin illa a ve b'nin en büyük ortak böleni olduğu anlamına gelmez; örneğin

$$23 = 7 \times 5 + 4 \times (-3)$$

olur ama 7 ile 4'ün en büyük ortak böleni 23 değildir! Öte yandan, şimdi kanıtlayacağımız üzere, eğer $d = 1$ ise, yukarıdaki teoremin ters istikameti de doğrudur.

Teorem 5.3 (Bézout Teoremi II)**.** *a ve b birbirine asal iki tamsayıysa, o zaman*

$$au + bv = 1$$

eşitliğini sağlayan u ve v tamsayıları vardır. Bunun ters istikameti de doğrudur: Eğer $au + bv = 1$ eşitliğini sağlayan u ve v tamsayıları varsa, a ve b aralarında asaldır.

Kanıt: Birinci önerme bir önceki teoremin özel bir durumu. İkinci önermeyi kanıtlayalım: Eğer bir d doğal sayısı a ve b sayılarını bölüyorsa, o zaman d sayısı $au + bv$ sayısını da böler, yani 1'i de böler. Demek ki $d = 1$ olmak zorundadır. □

Örneğin $45 \times 3 + 67 \times (-2) = 1$ olduğundan, 45 ile 67 aralarında asaldır.

Tabii $au + bv = 1$ ise, a ile b aralarında asal olduğu gibi, a ile v de ve hatta u ile v de aralarında asaldır.

Katsayıları Bulmak. Verilmiş a ve b tamsayıları için,

$$au + bv = \text{obeb}(a, b)$$

eşitliğini sağlayan u ve v sayılarının varlığını Teorem 5.2'de kanıtlamıştık. Bu sayılara katsayı diyelim. Bu bölümü u ve v katsayılarını bulmanın bir yöntemini göstererek bitirelim.

$\text{obeb}(a, b) = d$ olsun. [2. Kitap, Örnek 4.7 ve Örnek 6.68]'de d'yi bulmanın bir yöntemini açıklamıştık. Burada aynı yöntemi bir defa daha göreceğiz. Amacımız

$$d = au + bv$$

eşitliğini sağlayan u ve v katsayılarını bulmak. (d'yi henüz bilmeyebiliriz, yani $au+bv = d$ denkleminin üç bilinmeyeni olabilir: u, v ve d.) Bu arada, bu eşitliği sağlayan sonsuz sayıda u ve v tamsayıları olduğunu söyleyelim, nitekim eğer $au + bv = d$ oluyorsa, her $k \in \mathbb{Z}$ için $a(u + kb) + b(v - ka) = d$ olur.

u ve v katsayılarını bulmadan önce a ve b'yi makyajdan geçirelim:

Birinci Makyaj: Her şeyden önce a ve b'yi doğal sayı alabileceğimizi görelim: Eğer $|a|u + |b|v = d$ eşitliğini sağlayan u ve v'yi bulabiliyorsak, $au_1 + bv_1 = d$ eşitliğini sağlayan u_1 ve v_1 tamsayıları da bulunabilir; nitekim a ve b'nin pozitif ya da negatifliğine göre $u_1 = \pm u$ ve $v_1 = \pm v$ tanımlarını yaparsak $au_1+bv_1 = d$ olur. Bu sayede bundan böyle a ve b'nin doğal sayı olduklarını varsayabiliriz. Öyle de yapalım.

İkinci Makyaj: Ayrıca eğer $b = 0$ ise $d = a$ olur ve $u = 1$ almak yeterlidir (v için istediğiniz sayıyı seçebilirsiniz). Demek ki bundan böyle $b > 0$ varsayımını yapabiliriz. Aynı nedenden $a > 0$ varsayımını da yapabiliriz. Öyle yapalım, bundan böyle a ve b pozitif olsun.

Üçüncü Makyaj: Gerekirse a ve b'nin rollerini değiştirerek, yani a yerine b ve b yerine a alarak, $b \leq a$ varsayımını da yapabiliriz. Öyle yapalım, artık $0 < b \leq a$ olsun.

Demek ki artık $0 < b \leq a$ varsayımları altında çalışıyoruz.

Şimdi $d = au + bv$ eşitliğini sağlayan u ve v tamsayı çiftlerinden birini bulmaya girişelim. Tabii a ve b ne kadar büyükse, u ve v katsayılarını bulmak o kadar zor olur. Ama mesela b sayısı çok küçükse (mesela 0 ise, hatta 1 ise de), o zaman u ve v sayılarını bulmak kolaydır. Birazdan sunacağımız yöntemin anafikri bu: a ve b sayılarının katsayılarını bulmak için, b'den daha küçük bir r için b ve r sayılarının katsayılarını bulmanın yeterli olacağını göreceğiz. Bir başka deyişle, problemi,

$$b < a$$

sayılarından, bir r sayısı için

$$r < b$$

sayılarına indirgeyeceğiz. Böylece katsayılarını bulmak istediğimiz sayıları sürekli küçülteceğiz, ta ki katsayıları bulmanın kolay olduğu duruma kadar, mesela ikisinden biri 0 olana kadar.

Yöntemi açıklayalım: a'yı b'ye kalanlı bölelim: Bir q sayısı ve $0 \leq r < b$ eşitsizliklerini sağlayan bir r sayısı için

$$a = bq + r \tag{1}$$

olur. Bu eşitlikten hemen anlaşılacağı üzere a ve b sayılarının ortak bölenleriyle b ve r sayılarının ortak bölenleri elbette aynıdır [2. Kitap, Teorem 6.6]. Dolayısıyla

$$d = \text{obeb}(a, b) = \text{obeb}(b, r)$$

olur. $0 \leq r < b$ olduğundan, b ve r sayıları için $bu_1 + rv_1 = d$ eşitliğini sağlayan u_1 ve v_1 katsayılarını ve (eğer henüz bilmiyorsak) d'yi de bulmak daha kolaydır. (Mesela $r = 0$ ise yaşadık!) Diyelim

$$d = bu_1 + rv_1 \tag{2}$$

eşitliğini sağlayan u_1 ve v_1 katsayılarını bir biçimde bulduk. (1)'den çıkan

$$r = a - bq$$

eşitliğini (2)'ye yerleştirelim:

$$d = bu_1 + rv_1 = bu_1 + (a - bq)v_1$$

elde ederiz. Bu eşitliği düzenlersek,

$$d = av_1 + b(u_1 - qv_1)$$

buluruz. Demek ki

$$u = v_1 \text{ ve } v = u_1 - qv_1$$

tanımları istediğimiz $d = au + bv$ eşitliğini sağlar.

Eğer (2)'yi sağlayan u_1 ve v_1 katsayılarını bulmak kolay değilse, aynı yöntem devam ettirilir: b, r'ye bölünür ve süreç devam ettirilir. Sayılar sürekli küçüldüğünden, bir zaman sonra ikisinden biri 0 olacaktır; o zaman da hem d bulunur hem de katsayılar.

Yukarıdaki yöntemi pratikte uygulamak çok kolay olmayabilir, çünkü yukarıda anlattığımız süreç birkaç adım uzayınca a'lar, b'ler r'ler birbirine karışabilir. Aşağıdaki örneklerde bu karmaşayı önlemenin pratik bir yolunu göreceğiz.

Anlattığımız yöntem kolaylıkla bir bilgisayar programına dönüştürülebilir, yani gösterdiğimiz yöntem aslında bir "algoritma"dır. Tabii "algoritma"yı program diline dönüştürmek için bir programlama dili bilmek gerekir. Biz burada sadece ana düşünceyi anlattık. Çeşitli ihtiyaçlara cevap veren onlarca programlama dili vardır; okur bu dillerden birini başka kaynaklardan öğrenmelidir.

Örnekler

5.1. $a = 25$, $b = 7$ olsun. Bu iki sayı aralarında asal, yani $d = 1$. Amacımız

$$25u + 7v = 1$$

eşitliğini sağlayan u ve v tamsayılarını bulmak. Aynı soruyu bir sonraki örnekte metinde anlatılan yöntemle çözeceğiz, ama burada çok daha ilkel bir yöntem kullanacağız. 25'in katından 1 fazlasını ya da 1 eksiğini bulana kadar 7'yi 1, 2, 3 gibi doğal sayılarla çarpalım. $7 \times 7 = 49$ eder ve bu sayı 25×2'nin 1 eksiğidir:

$$7 \times 7 = 25 \times 2 - 1$$

ya da

$$1 = 25 \times 2 + 7 \times (-7).$$

Demek ki $u = 2$ ve $v = -7$ almak yeterli. Başka çözümler de vardır. Örneğin $u = 9$, $v = -32$ sayıları aynı eşitliği sağlar. Genel olarak, her $k \in \mathbb{Z}$ için $u = 2 + 7k$ ve $v = -7 - 25k$ sayıları aynı eşitliği sağlar. Başınız sıkıştığında bu ilkel yönteme başvurabilirsiniz ama büyük sayılarla uzun süre alabilir.

5.2. Gene $a = 25$, $b = 7$ olsun. Bu iki sayı aralarında asal, yani $d = 1$. Amacımız

$$25u + 7v = 1$$

eşitliğini sağlayan u ve v tamsayılarını bulmak. Bu sefer metinde açıkladığımız yöntemi kullanacağız. 25'i 7'ye kalanlı bölelim:

$$\underline{25} = \underline{7} \times 3 + \underline{4}$$

(ileride kolaylık olsun diye ilgilendiğimiz sayıların altını çizdik) ve 7 ve 4 için istediğimiz u ve v sayılarını bulalım. Bu iki sayı için aranan u ve v sayılarını bulmak kolay:

$$1 = \underline{7} \times (-1) + \underline{4} \times 2.$$

Şimdi eşitliğin sağındaki 4 yerine, bir önceki eşitlikte beliren $\underline{4} = \underline{25} - \underline{7} \times 3$ eşitliğini yerleştirelim:

$$1 = \underline{7} \times (-1) + \underline{4} \times 2 = \underline{7} \times (-1) + (\underline{25} - \underline{7} \times 3) \times 2 = \underline{25} \times 2 + \underline{7} \times (-7)$$

elde ederiz. Demek ki $u = 2$ ve $v = -7$ istediğimiz $25u + 7v = 1$ eşitliğini sağlıyor.

5.3. Bu sefer $a = 43$, $b = 127$ olsun. $a < b$ olduğpundan, yukarıda açıkladığımız üçüncü makyaja uyacak olursak, a ile b'nin yerlerini değiştirip, $a = 127$ ve $b = 43$ ile çalışmamız lazım. Ama öyle yapmayalım, bakalım başımıza ne iş gelecek.
Hem en büyük ortak böleni, hem de u ve v katsayılarını bulacağız. İlk bölmeyi yapalım (yani a'yı b'ye bölelim) ve önemli sayıların altını çizelim:

$$\underline{43} = \underline{127} \times 0 + \underline{43}.$$

Yeni sayılarımız 127 ve 43. Başlangıçtaki sayılarımız 43 ve 127 idi, şimdi 127 ve 43 oldu! Üçüncü makyajdaki değişiklik kendiliğinden gerçekleşti! Tabii üçüncü makyajı yerine getirip ta en baştan $a = 127$ ve $b = 43$ almak daha akıllıca olurdu. Genel olarak a'yı b'den büyükeşit almak süreci hızlandırır. Biz de öyle yaptığımızı varsayalım, $a = 127$ ve $b = 43$ alalım.
Şimdi 127'yi 43'e bölelim:

(Birinci Adım) $$\underline{127} = \underline{43} \times 2 + \underline{41}.$$

Şimdi 43'ü 41'e bölelim:

(İkinci Adım) $$\underline{43} = \underline{41} \times 1 + \underline{2}.$$

Ardından 41'i 2'ye bölelim:

(Üçüncü Adım) $$\underline{41} = \underline{2} \times 20 + \underline{1}.$$

En büyük ortak böleni bulmak için bu kadarı yeter bize çünkü

$$\underline{1} = \underline{41} - \underline{2} \times 20$$

eşitliğinden

$$d = \text{obeb}(43, 127) = \text{obeb}(43, 41) = \text{obeb}(41, 2) = 1$$

eşitliğini biliyoruz. Şimdi

$$43u + 127v = 1$$

eşitliğini sağlayan u ve v tamsayılarını bulalım. Yukarıdaki üç adımda elde edilen eşitlikleri kullanarak kalanları (en sağdaki sayıları) tecrit edelim:

$$\begin{array}{rcl} \underline{41} & = & \underline{127} - \underline{43} \times 2 \\ \underline{2} & = & \underline{43} - \underline{41} \times 1 \\ \underline{1} & = & \underline{41} - \underline{2} \times 20 \end{array}$$

Şimdi en son eşitlikten başlayarak yukarı doğru çıkalım:

$$\begin{array}{rcl} \underline{1} & = & \underline{41} - \underline{2} \times 20 \\ & = & \underline{41} - (\underline{43} - \underline{41} \times 1) \times 20 \\ & = & \underline{41} \times 21 - \underline{43} \times 20 \\ & = & (\underline{127} - \underline{43} \times 2) \times 21 - \underline{43} \times 20 \\ & = & \underline{127} \times 21 - \underline{43} \times 62 \\ & = & \underline{127} \times 21 + \underline{43} \times (-62) \end{array}$$

İstediğimizi bulduk: $u = 21$, $v = -62$.

5.4. a ve b iki tamsayı tamsayı olsun. Diyelim $d = \text{obeb}(a, b)$. Elbette a ve b'nin her böleni $a + b$ ve $a - b$ sayılarını da böler. $B(x, y)$, x ve y'nin ortak bölenlerinden oluşan kümeyi simgelesin. Demek ki

$$B(a, b) \subseteq B(a + b, a - b)$$

olur. Öte yandan $a + b$ ve $a - b$'nin bölenleri,

$$(a + b) + (a - b) = 2a \text{ ve } (a + b) - (a - b) = 2b$$

sayılarının da bölenleridir. Demek ki

$$B(a, b) \subseteq B(a + b, a - b) \subseteq B(2a, 2b)$$

olur. $\text{obeb}(x, y) = \max B(x, y)$ olduğundan, bir önceki satırda merkezlenen kapsamalardan,

$$d \leq \text{obeb}(a + b, a - b) \leq 2d$$

ve hemen ardından,

$$1 \leq \text{obeb}(a/d + b/d, a/d - b/d) \leq 2$$

çıkar. Demek ki $\text{obeb}(a/d + b/d, a/d - b/d)$ ya 1'e ya da 2'ye eşit. Aslında buradan kolaylıkla şu sonuç çıkar:

$$\text{obeb}(a/d+b/d, a/d-b/d) = \begin{cases} 1 & \text{eğer } a/d \text{ ve } b/d\text{'nin biri tek diğeri çiftse} \\ 2 & \text{eğer } a/d \text{ ve } b/d\text{'nin ikisi de tek ya da ikisi de çiftse} \end{cases}$$

Demek ki

$$\text{obeb}(a+b, a-b) = \begin{cases} d & \text{eğer } a/d \text{ ve } b/d\text{'nin biri tek diğeri çiftse} \\ 2d & \text{eğer } a/d \text{ ve } b/d\text{'nin ikisi de tek ya da ikisi de çiftse} \end{cases}$$

Şimdi $d = 1$ varsayımını yapalım, yani a ile b aralarında asal olsun; bu varsayım altında

$$\text{obeb}(a+b, a-b) = \begin{cases} 1 & \text{eğer } a \text{ ve } b\text{'nin biri tek diğeri çiftse} \\ 2 & \text{eğer } a \text{ ve } b\text{'nin ikisi de tek ya da ikisi de çiftse} \end{cases}$$

doğru olur.

Alıştırmalar

5.5. $a = 9$ ve $b = 13$ olsun. $au + bv = 1$ eşitliğini sağlayan u ve v tamsayılarını bulun.

5.6. $a = 149$ ve $b = 13$ olsun. $au + bv = 1$ eşitliğini sağlayan u ve v tamsayılarını bulun.

5.7. $a = 149$ ve $b = 113$ olsun. $au + bv = 1$ eşitliğini sağlayan u ve v katsayılarını bulun.

5.8. $a = 119$ ve $b = 161$ olsun. $d = \text{obeb}(a, b)$'yi bulun ve $au + bv = d$ eşitliğini sağlayan u ve v katsayılarını bulun.

5.9. $a = 323$ ve $b = 391$ olsun. $d = \text{obeb}(a, b)$'yi ve $au + bv = d$ eşitliğini sağlayan u ve v katsayılarını bulun.

5.10. $a = 11323$ ve $b = 2391$ olsun. $d = \text{obeb}(a, b)$'yi ve $au + bv = d$ eşitliğini sağlayan u ve v katsayılarını bulun.

5.11. Kendin sor, kendin yanıtla!

Notlar

5.12. Etienne Bézout[1] 1730-1783 yılları arasında yaşamış Fransız bir matematikçidir. Aile yakınları genellikle esnaflardan ve okuma yazma bilmeyenlerden oluşuyordu. Sadece babası okuyabilmiş ve hukukçu olmuştu, ancak davalara girecek kadar üst düzey bir hukukçu değildi. Geleneklere göre Etienne Bézout'nun da hukukçu olması beklenirdi, ancak Euler'in bir kitabını okumasıyla fikir değiştirmiştir. "Bir gün bir kitap okudum ve bütün hayatım değişti" misali...

Daha çok cebirde ve cebirsel geometride önemli buluşları vardır. Örneğin iki eğrinin kesiştikleri nokta sayısını kestirebilmiştir. (Eğer eğrilerin ortak bileşeni yoksa, kesişim noktası sayısı en fazla eğrilerinin derecelerinin çarpımı kadar olabilir. Yani örneğin $y = x^3 - x + 1$ ile $y^2 = xy^4 + 1$ eğrileri en fazla $3 \times 5 = 15$ noktada kesişebilir. Bunu okumadığınızı varsayabilirsiniz!)

Önemli matematiksel sonuçlarına rağmen, çağında daha çok ders kitaplarıyla tanınmıştı. Ders kitapları İngilizceye de çevrilmiş ve İngiltere'de ve Kuzey Amerika'da (Harvard Üniversitesi'nde mesela) uzun yıllar kullanılmıştır.

1783'te yüksek ateş sonucu genç sayılabilecek bir yaşta ölmüştür. Bugün, birçok kişinin ölümüne neden olan yüksek ateşin İzlanda'daki Laki volkanının patlamasıyla oluşan sülfürik asit buharından kaynaklandığı anlaşılmıştır.

[1] Bezu diye okunur.

Bu arada Bézout'nun, bu kitapta bahsettiğimiz (ve daha nice kitapta bahsedilen) teoreme çok benzeyen ama kanıtı biraz daha zor olan "polinomlarla" ilgili bir teorem kanıtladığını da söyleyelim. Bugün Bézout'ya atfedilen teorem, aslında 150 yıl kadar önce, Méziriac (1581-1638) tarafından kanıtlanmıştır.
Ölümünden sonra doğduğu şehir olan Némours'a, yine Némours'da doğmuş olan heykeltıraş Justin-Chrysostome Sanson tarafından yapılan heykeli dikilmiştir.

Bézout'nun heykelinin resmi. Heykeltıraş: Justin-Chrysostome Sanson. Kaynak: Catalogue Illustré du Salon 1886, direktör F.-G. Dumas, Librarie d'Art L. Baschet, Paris.

5.13. Algoritma kelimesi, yaklaşık 780-850 yılları arasında yaşamış olan Fars kökenli matematikçi, gökbilimci ve coğrafyacı el Harezmi'den (ya da Hârizmî'den) gelmektedir. El Harizmi tarihin en önemli matematikçilerinden biridir. Şu anda Özbekistan sınırları içinde kalan Harezm bölgesinin Hive şehrinde doğmuştur, ama eserlerini, Abbasiler'in yönetimi altında bir bilim, kültür ve sanat merkezi konumuna yükselen Bağdat'ta vermiştir. Bazıları el Harezmi'nin Bağdat'ta doğduğunu, muhtemelen atalarının Harezm bölgesinden

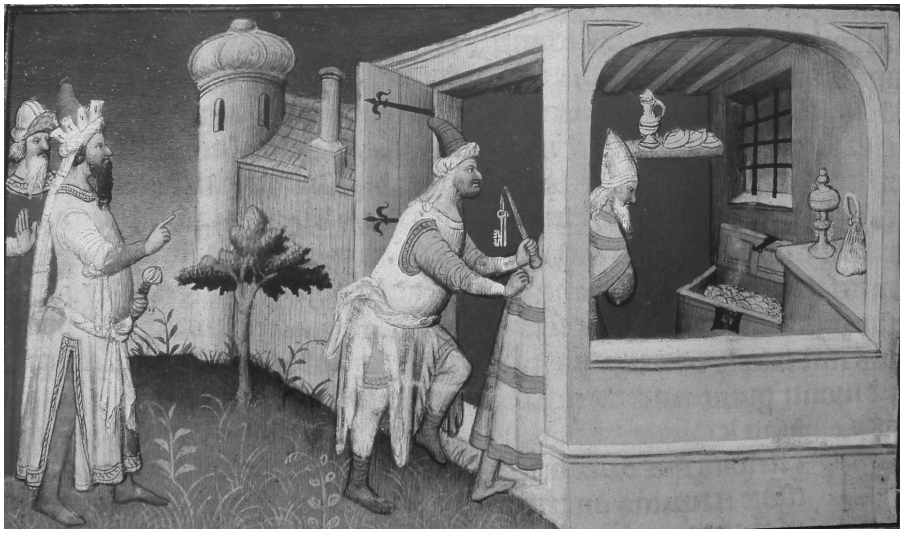
geldiğini düşünüyor.

5.14. Cebir kitabına yazdığı önsözden sofu bir Müslüman olduğu anlaşılan el Harizmi'nin, ya kendisinin gençliğinde ya da atalarının bir tarihte zerdüşt olduğu tahmini de var. Zerdüştlük, 3500 yıl önce Zerdüşt tarafından kurulmuş (muhtemelen ilk) tek tanrılı bir dindi. Bilgeliği ve bilgiyi kutsardı. Eski Yunan filozoflarından Heraklit'ten çağımızın dinlerine kadar düşünce ve inanç dünyasını çok etkilemiş bir dindir.

5.15. Harezmi Abbasiler döneminde yaşamıştır. Abbasiler'in 750'de başlayan Irak bölgesindeki egemenliği, 850'lerde en üst düzeyini bulmuş, 1250'lerde Moğolların bir kolu olan İlhanlılar'ın istilasıyla sona ermiştir.

Cengiz Han'ın oğlu Hülagu Han'ın önderliğinde 1243'te Selçuk Türklerini yenen Moğollar, 1256 yılında İran'ı ele geçirmiş, Tebriz merkezli İlhanlılar devletini kurmuş ve 1257-8 yıllarında Abbasilerin başkenti Bağdat'ı yerle bir etmiştir. Deyim yerindedir! Nitekim Bağdat'ta insanlığın en değerli en az 500 yıllık bilimsel ve kültürel hazinesi bir haftada yok olmuştur; cami, saray, kütüphane, hastane gibi ne kadar mimari eser varsa hiçbirinden taş üstüne taş kalmamıştır. Özellikle Bağdat kütüphanesi çağının en değerli, en tanınmış kütüphanelerindendi. Kütüphanede bulunan ve yüzyılların emeği olan tıptan astronomiye kadar sayısız bilimsel, kültürel ve tarihî eser bir anda kül olmuştur. Ölümden kurtulanların anlattığına göre Dicle nehri mürekkepten siyaha bürünmüş. Bağdat'ın Moğol istilası insanlık tarihinin en büyük trajedilerinden biridir, barbarlığın en üst seviyesidir.

Anadolu'yu da ele geçiren İlhanlıların egemenliği neyse ki ancak 1 yüzyıl sürebilmiştir.



Hülagu Han, Bağdat'ın alınışından sonra, şehri kendisine teslim etmeyi reddeden (ve daha sonra, savaş iyiye gitmeyince, anlaşma önerisi reddedilen) Abbaslı Halife Mustasım'ı açlığa mahkûm ederken.

6. Asallar üzerine Biraz Daha

Bézout teoreminin şu sonucu eminim hoşunuza gidecektir:

Teorem 6.1. *İki tamsayının çarpımını bölen bir asal sayı, çarpılan iki tamsayıdan birini mutlaka böler. Ayrıca bu özelliği sağlayan* 1*'den büyük her doğal sayı asaldır.*

Mesela eğer 5, ab sayısını bölüyorsa, bu iki sayıdan biri mutlaka 5'e bölünür, çünkü 5 asal. Ama asal olmayan sayılar için bu doğru olmayabilir, örneğin 6 sayısı 10×9 sayısını böler ama 6 ne 10'u ne de 9'u böler.

Kanıt: Diyelim p bir asal ve ab çarpımını bölüyor. p'nin ya a'yı ya da b'yi böldüğünü göstereceğiz. Gerekirse a yerine $-a$ ve b yerine $-b$ alarak a ve b'nin doğal sayı olduklarını varsayabiliriz. Diyelim p, a'yı bölmüyor. Bu durumda p'nin b'yi böldüğünü göstermeliyiz. p bir asal olduğundan ve a'yı bölmediğinden p ile a'nın ortak böleni 1'dir, yani bu iki sayı aralarında asaldır. Bézout teoremine göre

$$pu + av = 1$$

eşitliğini sağlayan u ve v tamsayıları vardır. Bu eşitliğin her iki tarafını da b ile çarpalım:

$$pub + (ab)v = b.$$

Eşitliğin sol tarafı p'ye bölünür çünkü varsayımımıza göre $p|ab$. Demek ki eşitliğin sağ tarafı, yani b de p'ye bölünür.

Teoremin ikinci kısmını kanıtlayalım şimdi. Teoremin ilk kısmında yazan özelliği sağlayan bir $p > 1$ doğal sayısı alalım. Yani her a ve b tamsayısı için, eğer $p|ab$ ise, ya $p|a$ ya da $p|b$ olsun. Amacımız p'nin bir asal sayı olduğunu göstermek. Diyelim bir a doğal sayısı p'yi bölüyor. Amacımız a'nın ya 1'e ya da p'ye eşit olduğunu göstermek. $a|p$ olduğundan, bir $b \in \mathbb{N}$ sayısı için

$$p = ab$$

olur. Ama $p|p$ olduğundan, bu eşitlikten $p|ab$ çıkar. Dolayısıyla, varsayıma göre ya $p|a$ ya da $p|b$ olmalı. Birinci durumda ($a|p$ olduğundan) $a = p$ olur, tam istediğimiz gibi. İkinci durumda bir c için $b = pc$ olur ve bundan da

$$p = ab = acp$$

çıkar, ki bu da $ac = 1$ ve dolayısıyla $a = 1$ demektir, bu da tam istediğimiz gibi. Kanıtımız tamamlanmıştır. □

Bu teorem, p ikiden fazla sayının çarpımını böldüğünde de geçerlidir tabii ki, örneğin eğer p asalı abc sayısını bölüyorsa, o zaman a, b ve c sayılarından (en azından) birini bölmek zorundadır. Bunu bir sonuç olarak kaydedelim:

Sonuç 6.2. *p bir asal ve $a_1, \ldots, a_n$ herhangi n tane doğal sayı olsun. Eğer $p|a_1 \cdots a_n$ ise p asalı $a_1, \ldots, a_n$ sayılarından en az birini böler.* □

Teorem 6.1'i şöyle de genelleştirebiliriz:

Sonuç 6.3. *0'dan farklı a, b, c doğal sayılarını alalım. Eğer a sayısı bc çarpımını bölüyorsa ve a ve b aralarında asalsa, a sayısı c'yi böler.*

Kanıt: Diyelim bir x sayısı için

$$ax = bc.$$

Ayrıca a ve b aralarında asal olduğundan,

$$au + bv = 1$$

eşitliğini sağlayan u ve v tamsayıları vardır. Bu eşitliğin her iki tarafını da c ile çarpalım:

$$auc + bcv = c$$

elde ederiz. Eğer bc yerine ax yazarsak,

$$auc + axv = c$$

elde ederiz. Ama a sol tarafı bölüyor; demek ki sağ tarafı da bölüyor. □

Aynı sonucu şöyle de kanıtlayabiliriz:

Kanıt: Diyelim kanıtlamak istediğimiz önerme yanlış. Önermenin yanlış olduğu sayılar arasında a'nın en küçük olduğu bir a, b, c üçlüsü seçelim. Demek ki a sayısı bc'yi bölüyor ve a ile b aralarında asal ama a, c'yi bölmüyor; ayrıca a bu özellikleri sağlayan en küçük pozitif doğal sayı.

a, c'yi bölmediğinden, a sayısı 1'e eşit olamaz. Demek ki $a > 1$. Teorem 6.1'e göre a bir asal da olamaz.

a'yı bölen pozitif bir p asal sayısı vardır [2. Kitap, Teorem 6.2]. Bu p asalı elbette bc'yi de böler (çünkü a, bc'yi bölüyor). Demek ki Teorem 6.1'e göre p ya b'yi ya da c'yi böler. Ama a ile b aralarında asal olduğundan, p, b'yi bölemez. Dolayısıyla p, c'yi bölmek zorunda. Şimdi a_1 ve b_1 doğal sayıları için

$$a = pa_1 \text{ ve } c = pc_1$$

yazalım. a asal olmadığından, $a_1 \neq 1$ (aksi halde $a = pa_1 = p$ olurdu, yani a bir asal olurdu). Şimdi $a = pa_1$ sayısı $bc = bpc_1$ sayısını böldüğünden, a_1 sayısı bc_1 sayısını böler. Ayrıca a_1 ve b sayıları aralarında asaldır (çünkü a ve b sayıları aralarında asal). $a_1 < a$ olduğundan, a üzerine varsayımımızdan dolayı (a önermeye en küçük karşıörnekti) a_1'in c_1'i böldüğünü söyleyebiliriz. Demek ki $a = pa_1$ sayısı $c = pc_1$ sayısını böler. □

Sonuç 6.4. *Aralarında asal iki doğal sayı bir doğal sayıyı bölüyorsa, çarpımları da böler.*

Kanıt: Diyelim aralarında asal olan n ve m sayıları x'i bölüyor. O zaman bir y için $x = ny$ olur. Buradan da m'nin ny'yi böldüğü çıkar. Sonuç 6.3'e göre m, y'yi böler, yani bir z için $y = mz$ olur. Bundan da $x = ny = n(mz) = (nm)z$ olur. Demek ki nm sayısı x'i böler. □

Yaptıklarımızı uygulayarak Fermat'nın Küçük Teoremi'nin [2. Kitap, Teorem 7.6] bir versiyonunu bulalım:

Sonuç 6.5 (Fermat'nın Küçük Teoremi)**.** *p bir asal ve n, p'ye bölünmeyen bir tamsayı olsun. O zaman p asalı $n^{p-1} - 1$ sayısını böler.*

Kanıt: Daha önce kanıtladığımız Fermat'nın Küçük Teoremi'ne [2. Kitap, Teorem 7.6] göre p asalı $n^p - n$ sayısını böler. Ama

$$n^p - n = n(n^{p-1} - 1)$$

olduğundan Teorem 6.1'e göre p asalı ya n'yi ya da $n^{p-1} - 1$ sayısını böler. p ile n aralarında asal olduğundan ancak ikinci şık geçerli olabilir, yani p asalı $n^{p-1} - 1$ sayısını böler. □

Sonuç 6.6. *p bir asal ve $1 \leq k < p$ bir doğal sayı olsun. O zaman p, $\binom{p}{k}$ sayısını böler.*

Kanıt: İki farklı kanıt sunacağız.

Birinci Kanıt:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p\,(p-1)!}{k!(p-k)!}$$

olduğundan, p'nin bu sayıyı bölmemesi için, payda bulunan p'nin paydada bulunan bir sayıyla sadeleşmesi lazım, yani (p asal olduğundan) paydada da bir p bulunması lazım. Ama hem k hem de $p-k$ sayısı p'den küçük olduğundan, paydada p bulunmaz.

İkinci Kanıt: [2. Kitap, Örnek 3.104]'te kanıtladığımız, ama cebirsel kanıtı çok basit olan

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

eşitliğini kullanacağız. Belli ki p asalı eşitliğin sağ tarafındaki sayıyı bölüyor. Dolayısıyla p, eşitliğin sol tarafındaki sayıyı da bölüyor. Öte yandan p ile k aralarında asallar. Demek ki p asalı $\binom{p}{k}$ sayısını böler. □

Örnekler

6.1. $145^{136} - 1$ sayısı 137'ye bölünür, çünkü 137 asal bir sayıdır.

6.2. 2^{27} sayısı 17'ye bölündüğünde kaç kalır? Sonuç 6.5'e göre, 2^{16}, 17'ye bölündüğünde 1 kalır, yani $2^{16} \in 17\mathbb{Z} + 1$ olur. $2^{27} = 2^{16}2^{11}$ olduğundan, şimdi 2^{11}'in kalanını hesaplayalım.

$$2^4 = 16 \in 17\mathbb{Z} - 1$$

olduğundan,

$$2^8 = (2^4)^2 \in 17\mathbb{Z} + 1$$

olur. Demek ki

$$2^{27} = 2^{16}2^8 2^3 = 2^{16}2^8 8 \in (17\mathbb{Z} + 1) \cdot (17\mathbb{Z} + 1) \cdot 8 \subseteq 17\mathbb{Z} + 8.$$

Buradan kalanın 8 olduğu çıkar. Yani 17 asalı $2^{27} - 8$ sayısını böler.

6.3. Ama Fermat'nın Küçük Teoremi asal olmayan sayılar için yanlıştır. Örneğin $2^5 - 1 = 31$ olur ve bu sayı 6'ya bölünmez. Ama bazen de p asal olmamasına karşın, p, $2^{p-1} - 1$ sayısını bölebilir. Örnek için aşağıdaki nota bakınız.

Alıştırmalar

6.4. 2^{28} sayısı 17'ye bölündüğünde kaç kalır?

6.5. 2^{29} sayısı 17'ye bölündüğünde kaç kalır?

6.6. 2^{36} sayısı 37'ye bölündüğünde kaç kalır?

6.7. 2^{39} sayısı 37'ye bölündüğünde kaç kalır?

6.8. 3^{39} sayısı 37'ye bölündüğünde kaç kalır?

6.9. 6^{39} sayısı 37'ye bölündüğünde kaç kalır?

6.10. 37^{37} sayısı 37'ye bölündüğünde kaç kalır?

6.11. $37^{37} - 36^{37}$ sayısı 37'ye bölündüğünde kaç kalır?

6.12. $37^{37} - 5^{37}$ sayısı 37'ye bölündüğünde kaç kalır?

6.13. $37^{37}5^{39}$ sayısı 37'ye bölündüğünde kaç kalır?

6.14. $32^{36}5^{39}$ sayısı 37'ye bölündüğünde kaç kalır?

6.15. $n > 0$ bir doğal sayı olsun. n'den küçükeşit ve n'ye asal olan doğal sayı sayısı $\varphi(n)$ olarak gösterilir. φ'ye ***Euler φ fonksiyonu*** adı verilir[1]. Örneğin $\varphi(6) = 2$ olur çünkü 6'dan küçük sadece 1 ve 5 doğal sayıları 6'ya asaldır.
Eğer p asalsa, $\varphi(p) = p - 1$ olduğunu kanıtlayın. Aynı varsayım altında $\varphi(p^2) = p^2 - p$ olduğunu kanıtlayın. Daha genel olarak, eğer p asalsa, her pozitif n doğal sayısı için, $\varphi(p^n) = p^n - p^{n-1}$ olduğunu kanıtlayın. İpucu: p^n küçük kaç doğal sayı p'ye bölünür?

Notlar

6.16. Sonuç 6.5'te kanıtladığımız Fermat'nın Küçük Teoremi'ne göre, eğer $p > 2$ bir asalsa, p, $2^{p-1} - 1$ sayısını (ya da $2^p - 2$ sayısını) böler. Bunun tersi doğru mudur? Yani eğer $p > 2$ bir tamsayıysa ve p, $2^{p-1} - 1$'yi bölüyorsa, p asal mıdır?

[1] φ, Yunan alfabesinin küçük f harfidir ve "fi" olarak okunur. Büyük harf fi, Φ olarak yazılır.

Eski Çinliler de bu soruyu sormuşlar ve yaptıkları hesaplarda p hep asal çıkmıştır. Gerçekten de $2 < p < 300$ için bu doğrudur. Öte yandan

$$p = 341 = 11 \times 31$$

için doğru değildir: 341 asal olmamasına karşın $2^{341} - 2$'yi böler. Demek ki Çinliler yanılmışlar [E]. Bir iki hesap yaparak matematiksel bir gerçek bulunmaz. Kanıt gerekir. Eğer p, $2^p - 2$'yi bölüyorsa ama asal değilse, p'ye ***yalancı asal*** adı verilir. Örneğin 341 bir yalancı asaldır[2].

$$561,\ 645,\ 1105,\ 1387,\ 1729,\ 1905$$

sayıları da yalancı asallardır. Kaç tane yalancı asal vardır? Sonsuz tane vardır, çünkü eğer p bir yalancı asalsa, $2^p - 1$ de bir yalancı asaldır. Okur bunu alıştırma olarak kanıtlayabilir. Demek ki $2^{341} - 1$ de bir yalancı asaldır.

[H]er p için, $2^p - 1$ tek bir sayıdır. Dolayısıyla yukarıdaki yöntemle bulunan yalancı asalların hepsi tektir. Bundan da şu "doğal" soru çıkar: Çift yalancı asal var mıdır? Evet! 1950'de D. H. Lehmer 161.038'in bir yalancı asal olduğunu kanıtladı. 161.038 sayısını bulmak kolay değil ama bu sayının yalancı asallığını kanıtlamak oldukça kolay. Kanıtlayalım. 161.038'in $2^{161.038} - 2$ sayısını böldüğünü kanıtlamak istiyoruz. Önce 161.038'i asallarına ayıralım:

$$161.038 = 2 \times 73 \times 1103.$$

Demek ki 73 ve 1103'ün $a = 2^{161.037} - 1$ sayısını böldüğünü kanıtlamalıyız. 161.037'yi asallarına ayıralım:

$$161.037 = 3^2 \times 29 \times 617 = 9 \times b.$$

Burada $b = 29 \times 617$ olarak aldık elbet. Eğer $c = 2^9$ ise, bundan da şu çıkar:

$$a = 2^{161.037} - 1 = \left(2^9\right)^b - 1 = c^b - 1.$$

Demek ki $c-1$, yani 2^9-1, yani 511, yani 7×73 sayısı, a'yı bölüyormuş. Dolayısıyla 73 de a'yı bölüyordur. Şimdi sıra 1103'ün a'yı böldüğünü kanıtlamakta. Aynı akıl yürütmeyi yapacağız.

$$d = 3^2 \times 617 \text{ ve } e = 2^{29}$$

olsun. Hesaplayalım:

$$a = 2^{161.037} - 1 = \left(2^{29}\right)^d - 1 = e^d - 1.$$

Demek ki

$$e - 1 = 1103 \times 486.737,$$

a'yı bölüyormuş. Kanıtımız bitmiştir.

1951'de N. W. H. Beeger sonsuz sayıda çift yalancı asal olduğunu kanıtladı.

6.17. Eğer $p > 1$, her n için $n^p - n$'yi bölüyorsa ve asal değilse, p'ye ***çok yalancı asal*** adı verilir. Çok yalancı asal sayı var mıdır? Evet. En küçük çok yalancı asal sayı 561'dir.

$$561 = 3 \times 11 \times 17$$

olduğundan 561 asal değildir. Öte yandan 561, her n için

$$n^{561} - n$$

ifadesini böler. Bunu da kanıtlamak oldukça kolaydır, sonuç olarak sayının 3'e, 11'e ve 17'ye bölündüğünü kanıtlamak yeterli. Kanıt için okur [H]'ye bakabilir.

[2] 341'in yalancı asal olduğu 1819'da Sarrus tarafından bulunmuştur.

6.18. Fermat'nın Küçük Teoremi'ne göre (Sonuç 6.5), eğer p asalsa,

$$1^{p-1},\ 2^{p-1},\ \ldots,\ (p-1)^{p-1}$$

sayıları p'ye bölündüğünde 1 kalır. Dolayısıyla bu $p-1$ sayının toplamı olan

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1}$$

sayısı p'ye bölündüğünde kalan $p-1$'dir. Bunun tersi de doğru mudur? Yani n herhangi bir sayıysa ve

$$1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1}$$

sayısı n'ye bölündüğünde kalan $n-1$ ise, n asal mıdır? 1950'de Giuga adında bir matematikçi 1985'te yanıtın $n < 10^{1700}$ için "evet" olduğunu gösterdi. Genel sorunun yanıtı bugün de (2014) bilinmiyor:

Giuga Sorusu: *n herhangi bir sayıysa ve*

$$1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1}$$

sayısı n'ye bölündüğünde kalan $n-1$ ise, n asal mıdır?

6.19. $n > 0$ bir doğal sayı olsun. n'den küçükeşit ve n'ye asal olan doğal sayı sayısı $\varphi(n)$ olarak gösterildiğini Alıştırma 6.15'te söylemiştik. Aynı alıştırmaya göre, eğer p asalsa, $\varphi(p) = p-1$ olur (bunun kanıtı çok basit). Dolayısıyla Fermat'nın Küçük Teoremi'ni, "eğer p asalsa, her n için, p, $n^{\phi(p)} - 1$ sayısını böler" olarak da okuyabiliriz. Bu önerme sadece asallar için değil, her $p > 0$ doğal sayısı için doğrudur. Yani her p sayısı, asal olsun ya da olmasın, her n için $n^{\phi(p)} - 1$ sayısını böler. Bunu Euler kanıtlamıştır. Örnek, $\phi(12) = 4$ olduğundan, 12 sayısı $5^4 - 1$ sayısını böler. 12 sayısı $n^4 - 1$ olarak yazılan tüm sayıları böler. Euler'in bu teoremini bu kitapta kanıtlamayacağız.

7. Aritmetiğin Temel Teoremi

Bir önceki ciltte [2. Kitap, Teorem 6.3]'te, pozitif her doğal sayının asalların çarpımı olarak yazıldığını kanıtlamıştık. Aynı kanıtı, kitabın bütünlüğü açısından, buraya da alalım. Önce bir yardımcı teorem kanıtlayalım:

Teorem 7.1. 1 *dışında her doğal sayı bir asala bölünür.*

Kanıt: $n \neq 1$ herhangi bir doğal sayı olsun. n'nin bir asal sayıya bölündüğünü göstereceğiz. 0 sayısı tabii ki her asala bölünür, örneğin 2'ye bölünür. Bundan böyle $n \neq 0$ olsun. Demek ki $n \geq 2$. Bir tanım yapalım:

$$A = \{p \in \mathbb{N} \setminus \{0, 1\} : \ p, n\text{'yi böler}\}$$

olsun. Yani A, n'yi bölen 0 ve 1'den farklı doğal sayılardan oluşan küme. $n \in A$ olduğundan (çünkü, n, n'yi böler ve $n \neq 0, 1$), A boşküme değildir. İyisıralama Özelliği'nden [2. Kitap, sayfa 81] dolayı A'nın en küçük ögesi vardır. A'nın bu en küçük ögesine p adını verelim. p en az 2 tabii ki. p'nin bir asal olduğunu kanıtlarsak istediğimizi kanıtlamış olacağız. Eğer p bir asal olmasaydı, 1'den büyük ama p'den küçük a ve b sayıları için $p = ab$ olacaktı. Ama $a|p$ ve $p|n$ olduğundan $a \in A$ olur. Böylece A'da p'den küçük bir öge bulmuş olduk, oysa p, A'nın en küçük ögesiydi, bir çelişki. Demek ki p bir asalmış. □

Teorem 7.2 (Aritmetiğin Temel Teoremi)**.** 0*'dan büyük her doğal sayı sonlu sayıda asalın çarpımıdır.*

Kanıt: Hiç tane sayının çarpımını 1 olarak tanımlandığından [2. Kitap, sayfa 21], 1 sonlu sayıda asal sayının çarpımıdır, nitekim 1 sayısı hiç tane asal sayının çarpımıdır. Bundan böyle 1'den büyük sayılara odaklanalım. 1'den büyük her doğal sayının sonlu sayıda asalın çarpımı olarak yazılacağını göstereceğiz. (Tabii bazı asallar çarpımda birkaç defa kullanılabilir.)

Diyelim teorem doğru değil. O zaman 1'den büyük en az bir doğal sayı sonlu sayıda asalın çarpımı olarak yazılmaz. Bu varsayımdan bir çelişki elde edeceğiz ve böylece teorem kanıtlanmış olacak.

$$A = \{n \in \mathbb{N} \setminus \{0\} : \ n \text{ sonlu sayıda asalın çarpımı değil}\}$$

olsun. Varsayımımıza göre $A \neq \emptyset$. Bir önceki paragrafa göre de $1 \notin A$, yani A'nın ögeleri 2'den büyükeşit olmak zorunda. İyisıralama Özelliği'nden [2. Kitap, sayfa 81] dolayı A'nın en küçük bir ögesi vardır, diyelim n. Teorem 7.1'e göre n bir asala bölünür, diyelim p asalına bölünüyor. Bu durumda bir m doğal sayısı için

$$n = pm \tag{1}$$

olur.

Elbette $m \neq 0$ çünkü aksi halde $n = 0$ olurdu. Eğer $m = 1$ ise $n = pm = p \cdot 1 = p$ olur ve p asal olduğundan n sayısı asalların (tek bir asalın, p'nin) çarpımı olur. Demek ki $m \geq 2$ olmak zorunda.

(1) eşitliğinden dolayı $m < n$ olur. n, A'nın en küçük ögesi olduğundan, $m \notin A$ olmak zorunda, yani m asalların çarpımıdır. Demek ki pm, yani n de asalların çarpımıymış. (m'yi veren asalların çarpımını bir de p ile çarparsak n'yi elde ederiz.) Çelişki. Demek ki $A = \emptyset$. □

Önceki kitapta bunları yapmıştık, burada bir defa daha tekrar ettik. Şimdi, daha fazlasını kanıtlayacağız, pozitif her doğal sayının asalların çarpımı olarak **tek** bir biçimde yazıldığını kanıtlayacağız. Örneğin,

$$3500 = 2 \times 2 \times 5 \times 5 \times 5 \times 7$$

olur. (Eşitliğin sağ tarafındaki sayıların her biri asaldır.) Tabii 3500'ü,

$$3500 = 7 \times 5 \times 5 \times 2 \times 5 \times 2$$

olarak da yazabiliriz, ama bu iki yazılım arasında çok büyük bir fark yoktur, sadece çarpımı alınan asalların yerleri değişmiş. Eğer asalları küçükten büyüğe doğru sıralayacak olursak, birazdan kanıtlayacağımız üzere, bir sayıyı asalların çarpımı olarak tek bir biçimde yazabiliriz.

Bir önceki bölümde kanıtladığımız Teorem 6.1'i canalıcı bir biçimde kullanacağımız okurun gözünden kaçmamalıdır. (Zaten teoremin kanıtı bu yüzden bu kadar gecikti.)

Teorem 7.3 (Aritmetiğin Temel Teoremi)**.** *Her pozitif doğal sayı sonlu sayıda pozitif asalın çarpımı olarak yazılır. Ayrıca eğer* $p_1 \leq \ldots \leq p_n$ *ve* $q_1 \leq \ldots \leq q_m$ *asalları için*

$$p_1 \cdots p_n = q_1 \cdots q_m$$

ise $n = m$ *olur ve her* $i = 1, \ldots, n$ *için* $p_i = q_i$ *olur.*

Kanıt: Birinci önermeyi Teorem 7.2'de kanıtlamıştık. İkinci önermeyi kanıtlayalım. Diyelim $p_1 \leq \ldots \leq p_n$ ve $q_1 \leq \ldots \leq q_m$ asalları için

$$p_1 \cdots p_n = q_1 \cdots q_m$$

eşitliği geçerli. Eğer $n = 0$ ise, yani eşitliğin sol tarafında çarpılacak p asalı yoksa, o zaman (sıfır tane sayının çarpımı tanım gereği 1 olduğundan, bkz. [2. Kitap, sayfa 21]), eşitliğin sol tarafı 1'e eşit olur ve

$$1 = q_1 \cdots q_m$$

eşitliğini elde ederiz. Ama q asalları 1'den büyüktür ve çarpımları 1 olamaz; dolayısıyla eşitliğin sağ tarafında da q asalı yok, yani $m = 0$. Bu durumda (yani $n = 0$ durumunda) istediğimizi kanıtladık.

Bundan böyle $n > 0$ varsayımını yapabiliriz. Benzer biçimde $m > 0$ varsayımını da yapabiliriz.

Eşitlikte beliren asalların en büyüğü ya p_n ya da q_m olmalıdır. Diyelim $p_n \geq q_m$. (Aksi halde p'lerle q'lerin rollerini değiştirin.) p_n asalı,

$$p_1 \cdots p_n = q_1 \cdots q_m$$

eşitliğinin sol tarafını böler; demek ki sağ tarafını da böler. Sonuç 6.2'ye göre p_n asalı q asallarından birini böler, diyelim q_j asalını bölüyor. Demek ki $p_n \leq q_j \leq q_m$. Ama varsayımımıza göre $p_n \geq q_m$. Buradan $p_n = q_m$ eşitliği çıkar. Böylece eşitliğin iki tarafında beliren son asalların birbirlerine eşit olduklarını kanıtladık. Bu asalları sadeleştirelim:

$$p_1 \cdots p_{n-1} = q_1 \cdots q_{m-1}$$

elde ederiz. Ne yaptık? $p_1 \cdots p_n = q_1 \cdots q_m$ eşitliğinin sonundaki asalları sadeleştirip, benzer eşitliğin daha az sayıda asalla gerçekleştiğini kanıtladık. Bir sonraki aşamada, aynı yöntemle p_{n-1} ve q_{m-1} asallarını yok edelim. Bunu böylece iki taraftan birindeki asallar tükeninceye kadar, yani eşitliğin bir tarafında 1 elde edinceye kadar devam edelim. Eşitliğin bir tarafı 1'e eşitse, diğer tarafta da asal kalmayacağını yukarıda görmüştük. Demek ki eşitliğin iki tarafındaki asallar aynı anda tükenmeli, yani $n = m$ olmalı. Asalların birbirine eşit olduğu da kanıttan anlaşılıyor olmalı. □

Bir sayıyı asallarına ayrıştırırken aynı asal birkaç kez belirebilir. Örneğin

$$a = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 13 \cdot 13 \cdot 13 \cdot 13$$

ayrışımında 2 tam üç kez belirmiş, 5 iki kez belirmiş, 13 de dört kez belirmiş. Bu sayıyı

$$a = 2^3 5^2 13^4$$

olarak yazmak bize yer ve zaman kazandırır. Eğer dilersek arada eksik olan asalları da tamamlayabiliriz:

$$a = 2^3 3^0 5^2 7^0 11^0 13^4$$

olur. Şöyle de yazabiliriz tabii:

$$a = 2^3 3^0 5^2 7^0 11^0 13^4 17^0 19^0.$$

Bu yazılımları kullanarak aritmetiğin temel teoremini şöyle ifade edebiliriz:

Teorem 7.4 (Aritmetiğin Temel Teoremi)**.** *Her pozitif doğal sayı, birbirinden farklı $p_1, \ldots, p_k$ asal sayıları ve pozitif $n_1, \ldots, n_k$ doğal sayıları için*

$$p_1^{n_1} \cdots p_k^{n_k}$$

biçiminde yazılır. Ayrıca eğer p_i asallarını küçükten büyüğe doğru soldan sağa yazarsak bu yazılım biriciktir. □

Örneğin

$$15.750 = 2^1 3^2 5^3 7^1$$

olarak asallarına ayrışır. Bu ayrışımda eğer dilersek asalların yerlerini değiştirebiliriz, örneğin

$$15.750 = 3^2 2^1 7^1 5^3$$

eşitliği de doğrudur. Ama yapabileceğimiz tek değişiklik asalların yerlerini değiştirmektir, eşitliği bozmadan çarpıma yeni bir asal ekleyemeyiz, ya da çarpımda beliren asallardan birini çıkaramayız ya da kuvvetlerle oynayamayız. Az kaldı unutuyordum! Tabii bazı asalların 0'ıncı kuvvetini de ekleyebiliriz:

$$15.750 = 2^1 3^2 5^3 7^1 11^0 13^0$$

Bu son yazılım özellikle iki farklı sayı ele aldığımızda pratiktir. Örnek olarak asallarına ayrılmış iki sayı alalım:

$$a = 2^{23} 5^{12} 11^4 13^7$$
$$b = 2^{17} 3^8 5^{12} 11^9$$

olsun. Eğer kuvvetlerde 0'ın belirmesine izin verirsek

$$a = 2^{23} 3^0 5^{12} 7^0 11^4 13^7$$
$$b = 2^{17} 3^8 5^{12} 7^0 11^9 13^0$$

olarak daha düzgün ve düzenli bir biçimde yazabiliriz. Örneğin a'nın asallara ayrışımında 2^{23} beliriyor, b'nin asallara ayrışımında da 2^{17} beliriyor; o zaman ab'nin asallarına ayrışımında $2^{23+17} = 2^{40}$ belirir. Sonuç olarak

$$ab = 2^{23+17} 3^{0+8} 5^{12+12} 7^{0+0} 11^{4+9} 13^{7+0} = 2^{40} 3^8 5^{24} 7^0 11^{13} 13^7$$

olur. Yani asallarına ayrıştırılmış iki sayının çarpımının asallarına ayrışımını bulmak çok kolaydır, asalların kuvvetlerini toplamak yeterlidir: Asal olsun ya

da olmasın, $p_1, \ldots, p_k$ sayıları ve (illa 0'dan farklı olmak zorunda olmayan) $n_1, \ldots, n_k$ ve $m_1, \ldots, m_k$ doğal sayıları için

$$a = p_1^{n_1} \cdots p_k^{n_k} \text{ ve } b = p_1^{m_1} \cdots p_k^{m_k}$$

ise,

$$ab = p_1^{n_1+m_1} \cdots p_k^{n_k+m_k} \tag{10}$$

olur.

Asallarına ayrıştırılmış sayıların en büyük ortak bölenini de bulmak kolaydır. Yukarıdaki

$$a = 2^{23}3^0 5^{12}7^0 11^4 13^7 \text{ ve } b = 2^{17}3^8 5^{12}7^0 11^9 13^0$$

örneğine devam edelim. obeb(a, b)'nin asallara ayrışımında 2'nin kaçıncı kuvveti belirir? a'da 2^{23} beliriyor, b'de de 2^{17} beliriyor, o zaman obeb(a, b)'de bunların en küçüğü olan 2^{17} belirir. Öte yandan a'nın asallara ayrışımında 3 belirmiyor, o zaman obeb(a, b)'nin asallara ayrışımında da 3 belirmez. obeb(a, b)'nin asallara ayrışımında beliren asallar hem a hem de b'de beliren asallardır ve bu asalların kaçıncı kuvvetlerinin belirdiği a ve b'nin asallara ayrışımlarına bakar bakmaz anlaşılır, hep en küçük kuvvet alınır. Sonuç olarak, obeb(a, b) sayısı,

$$2^{\min\{23,17\}}3^{\min\{0,8\}}5^{\min\{12,12\}}7^{\min\{0,0\}}11^{\min\{4,9\}}13^{\min\{7,0\}}$$

sayısına, yani

$$2^{17}3^0 5^{12}7^0 11^4 13^0$$

sayısına eşit olur. Genel olarak, birbirinden farklı $p_1, \ldots, p_k$ asal sayıları ve (illa 0'dan farklı olmak zorunda olmayan) $n_1, \ldots, n_k$ ve $m_1, \ldots, m_k$ doğal sayıları için,

$$a = p_1^{n_1} \cdots p_k^{n_k} \text{ ve } b = p_1^{m_1} \cdots p_k^{m_k}$$

ise,

$$\text{obeb}(a, b) = p_1^{\min(n_1,m_1)} \cdots p_k^{\min(n_k,m_k)} \tag{11}$$

olur.

Asallarına ayrıştırılmış bir sayının bölenlerini de bulmak kolaydır. Diyelim a sayısı asallarına şöyle ayrılmış olsun

$$a = 2^3 \cdot 5^7 \cdot 11^1.$$

a'nın bölenleri, $i = 0, 1, 2, 3$ ve $j = 0, 1, 2, 3, 4, 5, 6, 7$ ve $k = 0, 1$ sayıları için illa ki

$$2^i \cdot 5^j \cdot 11^k$$

biçiminde olmalıdır. Görüldüğü gibi i için 4, j için 8, k için 2 seçenek var, bu da toplamda $(4+8+2$ değil!$)$ $4\times 8\times 2 = 64$ seçenek verir, yani $2^3\cdot 5^7\cdot 11^1$ sayısının $4\times 8\times 2 = 64$ tane farklı böleni vardır. Bunların en küçüğü $2^0\cdot 5^0\cdot 11^0 = 1$'dir, en büyüğü de sayının kendisi olan $2^3\cdot 5^7\cdot 11^1$ sayısıdır. Örnek olarak (daha küçük, dolayısıyla makul bir sayı olan) $2^3\cdot 5^2\cdot 11^1$ sayısının (ki 2200'e eşit) tüm bölenlerini teker teker yazalım:

$$\begin{array}{llll}
2^0 5^0 11^0 = 1, & 2^1 5^0 11^0 = 2, & 2^2 5^0 11^0 = 4, & 2^3 5^0 11^0 = 8,\\
2^0 5^1 11^0 = 5, & 2^1 5^1 11^0 = 10, & 2^2 5^1 11^0 = 20, & 2^3 5^1 11^0 = 40,\\
2^0 5^2 11^0 = 25, & 2^1 5^2 11^0 = 50, & 2^2 5^2 11^0 = 100, & 2^3 5^2 11^0 = 200,\\
2^0 5^0 11^1 = 11, & 2^1 5^0 11^1 = 22, & 2^2 5^0 11^1 = 44, & 2^3 5^0 11^1 = 88,\\
2^0 5^1 11^1 = 55, & 2^1 5^1 11^1 = 110, & 2^2 5^1 11^1 = 220, & 2^3 5^1 11^1 = 440,\\
2^0 5^2 11^1 = 275, & 2^1 5^2 11^1 = 550, & 2^2 5^2 11^1 = 1100, & 2^3 5^2 11^1 = 2200.
\end{array}$$

Görüldüğü gibi tam $(3+1)(2+1)(1+1) = 24$ tane var. Bu bulduğumuz sonucu not edelim:

Sonuç 7.5. *$p_1^{n_1}\cdots p_k^{n_k}$ biçiminde asallarına ayrışmış bir doğal sayının tam*

$$(n_1+1)\cdots(n_k+1)$$

tane doğal sayı böleni vardır ve bu bölenler $0\le m_j\le n_j$ için

$$p_1^{m_1}\cdots p_k^{m_k}$$

biçiminde yazılırlar. □

Bunun doğrudan bir sonucu:

Sonuç 7.6. *Eğer p bir asal ve n bir doğal sayıysa p^n sayısının tam $n+1$ tane doğal sayı böleni vardır, bunlar da p'nin şu kuvvetleridir: $p^0 = 1$, $p^1 = p$, p^2, $\ldots$, p^{n-1}, p^n.*

Kanıt: Bir önceki sonuçta $k = 1$ alalım. □

Sonuç 7.7. *Eğer p bir asal ve $n > 0$ ve m birer doğal sayıysa, p^n ve m doğal sayılarının aralarında asal olması için yeter ve gerek koşul p'nin m'yi bölmemesidir.*

Kanıt: Bir önceki sonuca göre p^n'nin bölenleri p'nin kuvvetleridir ve 1 dışında bunların hepsi p'ye bölünürler. Buradan da istediğimiz sonuç çıkar. □

Ne yazık ki a ve b asallarının ayrışımı bize $a+b$'nin asallarına ayrışımı hakkında pek bir fikir vermez. Yukarıdaki

$$a = 2^{23}3^0 5^{12}7^0 11^4 13^7 \text{ ve } b = 2^{17}3^8 5^{12}7^0 11^9 13^0$$

örneğine geri dönelim: İlk aşamada $a+b$ sayısının asallarına ayrışımında **en azından**

$$2^{17},\ 5^{12},\ 11^4$$

asal kuvvetlerinin belireceğini söyleyebiliriz:

$$\begin{aligned} a+b &= 2^{23}5^{12}11^4 13^7 + 2^{17}3^8 5^{12}11^9 \\ &= 2^{17}5^{12}11^4(2^6 13^7 + 3^8 11^5), \end{aligned}$$

$a+b$ sayısının asallara ayrışmasını bitirebilmek için ikinci satırda parantez içinde yer alan

$$2^6 13^7 + 3^8 11^5$$

sayısını asallarına ayrıştırmak gerekir ki bu da oldukça zahmetli ve zaman alıcı olabilir. Ama mesela bu sayı bir tek sayı olduğundan (neden?) 2'ye bölünmez; dolayısıyla $a+b$'nin asal çarpımında tam olarak 2^{17} bulunur, 2'nin daha büyük bir kuvveti belirmez. Aynı şekilde $a+b$'nin asallarına ayrışımında 11'in tam 4'üncü kuvveti yani tam tamına 11^4 belirir, 11'in daha büyük bir kuvveti belirmez. Ayrıca $a+b$, 13'e tam bölünmez. Öte yandan $a+b$ çarpımında mesela 17'nin ya da 19'un tam kaçıncı kuvvetinin belirdiğini görmek için (Fermat'nın Küçük Teoremi'ni kullanarak mesela) biraz daha ileri düzeyde hesap yapmak gerekebilir. Hesaplardan korkmayan okur işe koyulabilir. (Bkz. bir sonraki örnek.)

Şöyle bir genel kural çok yanlış değildir: Sadece toplamayla ilgili sorular kolaydır, sadece çarpmayla ilgili sorular da kolaydır, ama hem toplamayla hem de çarpmayla ilgili sorular çok çok zor olabilir, örneğin Fermat'nın Son Teoremi ya da ikiz asallar sanısı ya da Goldbach Sanısı hem toplamayla hem de çarpmayla ilgili önermelerdir.

Örnekler

7.1. Sonuç 7.5'ten şu çıkar: Pozitif bir doğal sayıyı bölen doğal sayı sayısının tek olması için yerekli ve yeter koşul doğal sayının bir tam kare olmasıdır, nitekim Sonuç 7.5'teki

$$(n_1+1)\cdots(n_k+1)$$

sayısının tek olması için her n_i+1 çarpanının tek olması, bunun için de her n_i'nin çift olması gerekir. Bu durumda, $n_i = 2m_i$ yazarsak,

$$p_1^{n_1}\cdots p_k^{n_k} = p_1^{2m_1}\cdots p_k^{2m_k} = (p_1^{m_1}\cdots p_k^{m_k})^2$$

eşitliğini elde ederiz. Bunu bambaşka bir yöntemle [2. Kitap, Örnek 4.12]'de açıklamıştık.

7.2. Aritmetiğin Temel Teoremi'nin bir sonucu şudur: b ve c aralarında asal iki doğal sayı ise ve bc bir tamkareyse, o zaman b ve c de birer tamkaredir. Bunu kanıtlayalım. Diyelim bir a doğal sayısı için $bc = a^2$ oluyor. a'yı asallarına ayıralım, diyelim,

$$a = p_1^{n_1}\cdots p_k^{n_k}.$$

O zaman

$$bc = a^2 = p_1^{2n_1}\cdots p_k^{2n_k}$$

olur. Sağ tarafta beliren $p_i^{2n_i}$ asal kuvvetleri bc'yi bölmeli. Ama p_i asalı hem b'yi hem c'yi bölemez, sadece ikisinden birini bölebilir. Demek ki $p_i^{2n_i}$ ya b'yi ya da c'yi böler, ama ikisini birden bölemez. Ayrıca b ve c'yi bölen her asal da sağ tarafta belirmeli, üstelik aynı kuvvetlerle belirmeli. Buradan b ve c'nin asallara ayrışımında her asalın kuvvetinin çift olduğu anlaşılır, yani b ve c birer karedir.

Bu sonucu kareler yerine başka kuvvetlere genelleştirmek işten bile değildir.

Teorem 7.8. *b ve c aralarında asal iki doğal sayı olsun. $k \in \mathbb{N}$ olsun. Eğer bc bir doğal sayının k'ıncı kuvvetiyse, b ve c de bir doğal sayının k'ıncı kuvvetidir.*
Daha genel olarak, aralarında ikişer ikişer asal sonlu sayıda sayının çarpımı bir k'ıncı kuvvetse, çarpılan sayıların herbiri bir k'ıncı kuvvettir. □

7.3. Eğer bir a sayısını asallarına ayırmışsak, a'nın a^m kuvvetlerini de kolaylıkla asallarına ayırabiliriz tabii: Eğer

$$a = p_1^{n_1} \cdots p_k^{n_k}$$

ise,

$$a^m = p_1^{mn_1} \cdots p_k^{mn_k}$$

olur. Daha genel olarak, $a_1, \ldots, a_s$ sayıları asallarına ayrılmışsa,

$$a_1^{m_1} \cdots a_s^{m_s}$$

sayısı da kolaylıkla asallarına ayrılır.

Alıştırmalar

7.4. 11^9 sayısı 5'e bölündüğünde kalanın 1 olduğunu kanıtlayın.

7.5. 13^7 ile 3^7'nin 5'e bölündüğünde kalanlarının aynı olduğunu kanıtlayın.

7.6. Yukarıdaki alıştırmayı genelleyerek, her n doğal sayısı için 13^n ile 3^n'nin 5'e bölündüğünde kalanlarının aynı olduğunu kanıtlayın.

7.7. $2^6 13^7 + 3^8 11^5$ sayısı 5'in en fazla kaçıncı kuvvetine bölünür?

7.8. $2^5 13^8 + 3^{10} 11^6$ sayısı 17'ye bölündüğünde kalan kaç olur?

7.9. $2^6 13^7 + 3^8 11^5$ sayısı 19'a bölündüğünde kalan kaç olur?

7.10. 10! sayısını asallarına ayırın.

7.11. 1'den farklı bir tek doğal sayıya bölündüğünde her doğal sayının 2'nin bir kuvveti olduğunu gösterin.

7.12. 3, 4 ve 5'e bölündüğünde kalanın 1 olduğu bir sayı bulabilir misiniz?

7.13. 3, 4 ve 5'e bölündüğünde kalanın sırasıyla 2, 3 ve 4 olduğu bir sayı bulabilir misiniz?

7.14. 19, 20 ve 21'e bölündüğünde kalanın 1 olduğu bir sayı bulabilir misiniz?

Notlar

7.15. Asalların sonsuzluğu ve her doğal sayının asalların çarpımı olarak yazılacağı MÖ 300 dolayında yaşamış olan Öklid tarafından kanıtlanmıştır. Öklid, Büyük İskender'in kurduğu İskenderiye'de yaşamıştır. Çağına kadar bilinen matematiği toparladığı Elemanlar adlı 13 ciltlik kitabı tarihin hiç kuşkusuz en etkili matematik kitabıdır, özellikle geometriye muazzam etkisi olmuştur. 19'uncu yüzyıla kadar beli bir seviye üstünde eğitim gören herkesin illa okuması gereken kitap olarak addedilmiştir.

Yüzyıllar boyunca, Öklid'in kitabında sunduğu geometriden farklı geometrilerin olup olmadığı sorusu matematikçileri meşgul etmiştir. Uzun uğraşlar sonucu 19'uncu yüzyılda Öklid-dışı (yani bir noktadan bir doğruya paralel çekilemeyen ya da tam tersine birden fazla paralelin olduğu) başka geometrilerin de olduğu, Alman matematikçi Gauss, Macar matematikçi Bolyai, Rus matematikçi Lobachevski ve Alman matematikçi Riemann tarafından keşfedilmiştir.

7.16. Farklı coğrafyalarda ve farklı kişiler tarafından birbirine çok yakın tarihlerde aynı ya da benzer sonuçların bulunması pek sık rastlanan bir durumdur. Bundan da bazı sonuçların, buluşların, icatların bulunması için çağın uygun olması gerektiği sonucu çıkar.

8. En Küçük Ortak Kat

n ve m iki doğal sayı olsun. Hem n'ye hem de m'ye bölünen sayılar vardır elbette, örneğin nm sayısı bunlardan biridir. İyisıralama Özelliği'ne göre, hem n'ye hem de m'ye bölünen en küçük doğal sayı vardır; n ve m'nin ***en küçük ortak katı*** adı verilen bu sayı

$$\text{okek}(n, m)$$

olarak gösterilir. Örneğin 12 ve 8'in en küçük ortak katı 24'tür, yani

$$\text{okek}(12, 8) = 24$$

olur. Bu arada her m doğal sayısı için,

$$\text{okek}(0, m) = 0$$

eşitliğine dikkat edelim.

En küçük ortak kat olduğundan, $\text{okek}(n, m)$ en fazla nm olabilir elbette.

Bir başka örnek verelim:

$$a = 2^{23}5^{12}11^{4}13^{7} \text{ ve } b = 2^{17}3^{8}5^{12}11^{9}$$

olsun, yani sayılar asallarına ayrışmış biçimde verilmiş olsun. Eğer kuvvetlerde 0'ın belirmesine izin verirsek

$$a = 2^{23}3^{0}5^{12}7^{0}11^{4}13^{7} \text{ ve } b = 2^{17}3^{8}5^{12}7^{0}11^{9}13^{0}$$

olarak da yazabiliriz, ki bu yazılım daha pratik olacak. Bu örnekte a'nın asallara ayrışımında 2^{23} beliriyor, b'nin asallara ayrışımında da 2^{17} beliriyor; o zaman $\text{ekok}(a, b)$'nin asallarına ayrışımında 2^{23} belirir. Diğer asallarda da aynı şey olur. Sonuç olarak $\text{obeb}(a, b)$ sayısı,

$$2^{\max\{23,17\}}3^{\max\{0,8\}}5^{\max\{12,12\}}7^{\max\{0,0\}}11^{\max\{4,9\}}13^{\max\{7,0\}}$$

sayısına, yani

$$2^{23}3^{8}5^{12}7^{0}11^{9}13^{7}$$

sayısına eşit olur. Genel olarak, birbirinden farklı $p_1, \ldots, p_k$ asal sayıları ve (illa 0'dan farklı olmak zorunda olmayan) $n_1, \ldots, n_k$ ve $m_1, \ldots, m_k$ doğal sayıları için

$$a = p_1^{n_1} \cdots p_k^{n_k} \text{ ve } b = p_1^{m_1} \cdots p_k^{m_k}$$

ise,

$$\text{okek}(a, b) = p_1^{\max(n_1, m_1)} \cdots p_k^{\max(n_k, m_k)} \tag{1}$$

olur.

Geçen bölümde, sayfa 67'de bulduğumuz (10) ve (11) formülleriyle, kanıtı kolay olan

$$\max\{a, b\} + \min\{a, b\} = a + b$$

formülünü yukarıdaki (1) formülüyle bir araya getirirsek hemen

$$\text{okek}(a, b)\,\text{obeb}(a, b) = ab$$

eşitliğini bulmuş oluruz. Burada a ve b doğal sayılar tabii, ama her ikisi birden 0 olmamalı çünkü aksi halde obeb tanımlı olmaz. Bu eşitliği not edelim:

Sonuç 8.1. *a ve b her ikisi birden 0 olmayan iki doğal sayıysa,*

$$\text{okek}(a, b)\,\text{obeb}(a, b) = ab$$

olur. □

Teorem 8.2. *a ve b iki doğal sayı olsun. $e = \text{ekok}(a, b)$ olsun. O zaman a ve b'nin ortak katları tam tamına e'nin ortak katlarıdır.*

Kanıt: e sayısı a ve b'nin ortak katı olduğundan, e'nin katları a ve b'nin ortak katlarıdır. Bu kolaydı, diğer istikameti gösterelim. Eğer $a = 0$ ya da $b = 0$ ise, her şey bariz olmalı. Bundan böyle a ya da b'nin 0 olmadığını varsayalım. Böylece artık obeb(a, b)'den bahsedebiliriz. $d = \text{obeb}(a, b)$ olsun. Sonuç 8.1'e göre,

$$ed = ab$$

olur. $b = b_1 d$ yazalım. Yukarıdaki formülden $ed = ab = ab_1 d$, yani

$$e = ab_1$$

çıkar.

x sayısı a ve b'nin bir ortak katı olsun. x'i e'ye bölelim: Bir $q \in \mathbb{N}$ ve $0 \leq r < e$ için

$$x = eq + r$$

olur. x ve e sayıları a ve b'nin katları olduğundan, bu eşitlikten r'nin de a ve b'nin katları olduğu çıkar. Ama e sayısı a ve b en küçük pozitif ortak katı olarak tanımlandığından, bundan $r = 0$ elde ederiz. Demek ki

$$x = eq + r = eq$$

ve x, e'ye bölünüyor. □

Örnekler

8.1. 44.758.272.401 ile 13.164.197.765'in en büyük ortak bölenini ve küçük ortak katını bulalım. Birkaç gün uğraşarak bu sayıları asallarına ayırabiliriz:

$$\begin{aligned} 44.758.272.401 &= 17 \times 17.683 \times 148.891 \\ 13.164.197.76 &= 5 \times 17.6835 \times 148.891 \end{aligned}$$

Böylece

$$\begin{aligned} \text{obeb}(44.758.272.401,\, 13.164.197.76) &= 17.683 \times 148.891 \\ \text{okek}(44.758.272.401,\, 13.164.197.76) &= 5 \times 7 \times 17.683 \times 148.891 \end{aligned}$$

bulunur. Ama çok daha kolayı var. Önce, [2. Kitap, Bölüm 6.5]'te gördüğümüz gibi, en büyük ortak böleni bulalım. Aşağıda, sürekli olarak $\text{obeb}(a, b) = \text{obeb}(a - b, b)$ eşitliğini kullanıyoruz.

$$\begin{aligned} \text{obeb}(44.758.272.401,\, 13.164.197.76) &= \text{obeb}(31.594.074.636,\, 13.164.197.76) \\ &= \text{obeb}(18.429.876.871,\, 13.164.197.76) \\ &= \text{obeb}(5.265.679.106,\, 13.164.197.76) \\ &= \text{obeb}(5.265.679.106,\, 7.898.518.659) \\ &= \text{obeb}(5.265.679.106,\, 2.632.839.553) \\ &= \text{obeb}(2.632.839.553,\, 2.632.839.553) \\ &= \text{obeb}(2.632.839.553,\, 0) \\ &= 2.632.839.553. \end{aligned}$$

Demek ki

$$\text{obeb}(44.758.272.401,\, 13.164.197.76) = 2.632.839.553.$$

Buradan en küçük ortak katı bulmak kolay:

$$\text{okek}(44.758.272.401,\, 13.164.197.76) = \frac{44.758.272.401 \times 13.164.197.76}{2.632.839.553}.$$

(Bir yerlere bir ünlem koymam lazım!) Bu örnek [St, sayfa 110]'dan. Ama isteseydik kendi örneğimizi bulabilirdik, şöyle yapardık: İnternetten mesela, asal sayılar listesine bakarak 17.683 ve 148.891 gibi iki büyük asal seçerdik. Bu sayıları çarpıp bir d sayısı elde ederdik ve arkasından $a = 17d$ ve $b = 5d$ sayılarını hesaplayıp okura sunardık. Sayıları çarpmak kolaydır, asallarına ayırmak zordur, hatta çok zordur.

8.2. Eğer a, b ve c üç pozitif doğal sayıysa,

$$\text{okek}(a,\, \text{okek}(b, c)) = \text{okek}(\text{okek}(a, b),\, c)$$

olur. (Yani okek işlemi birleşme özelliğini sağlar.) Bunun kanıtı oldukça kolaydır ve okura alıştırma olarak bırakılmıştır. Yani okek işlemi birleşme özelliğini sağlar. Dolayısıyla bu ifadeler yerine

$$\text{okek}(a,\, b,\, c)$$

yazabiliriz. Gelecekte öyle de yapacağız. okek(a, b, c) sayısı, a'ya, b'ye ve c'ye bölünen en küçük doğal sayıdır. Genel olarak, eğer X, 0'dan farklı bir öge içeren sonlu bir doğal sayı (ya da tamsayı) kümesiyse, okek X, X'in ortak çarpanların en küçüğünü simgeler. Benzer tanımı obeb için de yapabiliriz ama bu sefer doğal sayı kümesinin sonlu olmasına gerek yoktur.

8.3. Her a için $\text{okek}(a, 1) = a$ olduğundan, 1, okek işleminin etkisiz ögesidir.

Alıştırmalar

8.4. $2^{23}t5^{12}11^4 13^7$, $2^{17}3^8 5^{12}11^9$ ve $2^{11} \cdot 5^{14}13^{12}17^9$ sayılarının ekok'unu bulun.

8.5. obeb işleminin etkisiz ögesi var mıdır?

8.6. Eğer a, b ve c üç pozitif doğal sayıysa,

$$\text{obeb}(a, \text{obeb}(b, c)) = \text{obeb}(\text{obeb}(a, b), c)$$

eşitliğini kanıtlayın.

8.7. $\text{obeb}(a, b)$'nin $\text{okek}(a, b)$'yi böldüğünü kanıtlayın.

8.8. Pozitif a ve b sayıları için $a \star b$ sayısını

$$\frac{\text{okek}(a, b)}{\text{obeb}(a, b)}$$

olarak tanımlayalım. Bu işlem birleşme özelliğini sağlar mı? Etkisiz ögesi var mıdır?

9. Birkaç Diofantus Denklemi

$5x^2 - x^3y = 5y^5 + 7$ gibi, tamsayılarda (hatta doğal sayılarda) çözümü aranan denklemlere ***Diofantus denklemi*** denir. Örneğin $x = 2$ ve $y = 1$ bu denklemin bir çözümüdür; nitekim bu denklemde x yerine 2 ve y yerine 1 koyarsanız eşitlik elde edersiniz. Belki başka çözümleri de vardır, bilmiyorum.

Bazı Diofantus denklemlerinin çözümü yoktur. Örneğin $2x+4y = 5$ denkleminin çözümü olamaz çünkü sol taraf çift, sağ taraf tek. $x^2+1 = 0$ denkleminin de çözümü olamaz. Bunlar kolay. Ama $x^2 + y^2 = z^4$ denkleminin çözümünün olmadığını göstermek pek kolay değil. Tadımlık birkaç Diofantus örneği vereceğimiz bu bu bölümde bu son denklemin tamsayılarda çözümü olmadığını göstereceğiz.

$x^3 + y^3 = z^3$ denkleminin tüm (tamsayı) çözümlerinde x, y ve z'den birinin 0 olması gerekmektedir, ama bunun kanıtı bayağı zordur. Daha genel olarak, eğer $n > 2$ ise, $x^n + y^n = z^n$ denkleminin tüm çözümlerinde de üç sayıdan biri 0 olmak zorundadır. Ama bunun kanıtı daha daha zordur. Fermat'nın Büyük Teoremi olarak bilinen bu teorem, Fermat'dan 350 yıl sonra ancak kanıtlanabilmiştir. Eğer binlerce sayfalık kanıtı bir gün anlarsam size de anlatırım! Bu konuda [2. Kitap, sayfa 32]'ye bakabilirsiniz.

Diofantus denklemlerini çözmek hiç kolay değildir, hatta çözümün olup olmadığını anlamak imkânsız bile olabilir. 1900 yılında ünlü matematikçi Hilbert, Diofantus denklemlerinin çözümünün olup olmadığına karar veren bir algoritmanın (yani bir bilgisayar programının) olup olmadığını sormuştur. Uzun uğraşlar sonunda, Martin Davis, Hilary Putnam ve Julia Robinson adlı matematikçilerin çalışmalarını Yuri Matiyasevich tamamlamış ve 1970'te böyle bir algoritmanın olmadığı kanıtlanmıştır.

Bu bölümde en basit Diofantos denklemleriyle uğraşacağız, ki onların bile hiç kolay olmadığını göreceksiniz.

9.1 Doğrusal Diafontos Denklemleri

Bu altbölümde

$$ax + by = c \tag{1}$$

türünden Diafontos denklemlerini inceleyeceğiz ve bu denklemim tüm çözümlerini bulacağız.

$a = b = 0$ durumunda, eğer $c = 0$ ise her x ve her y sayısı (1) denkleminin bir çözümüdür. Aksi halde, yani $c \neq 0$ ise (1) denkleminin hiç çözümü yoktur. Bundan böyle a ve b'nin her ikisinin birden 0 olmadığını varsayalım.

Eğer 1'den büyük bir p sayısı, a, b ve c sayılarından ikisini bölüyorsa ama üçüncüsünü bölmüyorsa, o zaman (1) denkleminin çözümü olamaz; öte yandan eğer p sayısı a, b ve c'yi bölüyorsa, diyelim

$$a = pa',\ b = pb',\ c = pb'$$

ise, p'yi sadeleştirerek, $ax + by = c$ denklemi yerine $a'x + b'y = c'$ denklemini ele alabiliriz, çünkü bu iki denklemin çözümleri aynıdır, birini çözmek yeter. Demek ki, gerekirse a, b ve c sayılarını sadeleştirerek bu sayıların ikişer ikişer aralarında asal olduklarını varsayabiliriz. Öyle varsayalım. Bu varsayımdan dolayı $a \neq 0$, $b \neq 0$ olmalı.

Bézout Teoremi'ne göre

$$au + bv = 1$$

eşitliğini sağlayan u ve v tamsayıları vardır. Bu eşitliği c ile çarparsak,

$$a(uc) + b(vc) = c \tag{2}$$

eşitliğini buluruz. Demek ki

$$x = uc,\ y = vc$$

sayıları (1) denkleminin çözümüdür. Ama başkaları da var: Kolayca görüleceği üzere, herhangi bir k tamsayısı için,

$$a(uc + kb) + b(vc - ka) = c$$

olur. Demek ki, her $k \in \mathbb{Z}$ için

$$x = uc + kb,\ y = vc - ka$$

sayıları (1) denkleminin bir çözümüdür. Sonsuz sayıda çözüm bulduk. Şimdi tüm çözümlerin bu şekilde olduklarını gösterelim. x ve y sayıları (1) denkleminin çözümü olsun. Demek ki

$$ax + by = c = a(uc) + b(vc)$$

olur. Bunu şöyle yazalım:

$$a(x - uc) = b(vc - y).$$

Ama a ve b aralarında asal. Demek ki

$$b|x - uc \text{ ve } a|vc - y.$$

Demek ki k, $\ell \in \mathbb{Z}$ için

$$x - uc = kb \text{ ve } vc - y = \ell a,$$

yani

$$x = uc + kb \text{ ve } y = vc - \ell a, \tag{3}$$

olur. Bu değerleri (1) denklemine yerleştirelim:

$$a(uc + kb) + b(vc - \ell a) = c$$

elde ederiz. Ama (2) formülünden dolayı $auc + bvc = c$ olduğundan, sadeleştirerek,

$$ab(k - \ell) = 0$$

buluruz. $ab \neq 0$ olduğundan, buradan $k = \ell$ çıkar. Bunu (3)'e yerleştirirsek istediğimiz

$$x = uc + kb \text{ ve } y = vc - ka$$

eşitliklerini buluruz. Kanıtladığımızı yazalım:

Teorem 9.1. *a, b, $c \in \mathbb{Z}$ aralarında ikişer ikişer asal üç tamsayı olsun. u ve v tamsayıları $au + bv = 1$ eşitliğini sağlasın. O zaman $ax + by = c$ denkleminin tüm çözümleri bir $k \in \mathbb{Z}$ için*

$$x = uc + kb,\ y = vc - ka$$

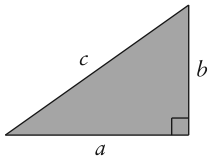
biçiminde yazılır. □

Alıştırmalar

9.1. $2x + 3y = 5$ denkleminin tüm tamsayı çözümlerini bulun.
9.2. $2x + 3y = 9$ denkleminin tüm tamsayı çözümlerini bulun.
9.3. $2x + 3y = 6$ denkleminin tüm tamsayı çözümlerini bulun.
9.4. $2x + 3y = 24$ denkleminin tüm tamsayı çözümlerini bulun.
9.5. $2x + 3y + 5z = 7$ denkleminin tüm tamsayı çözümlerini bulun.

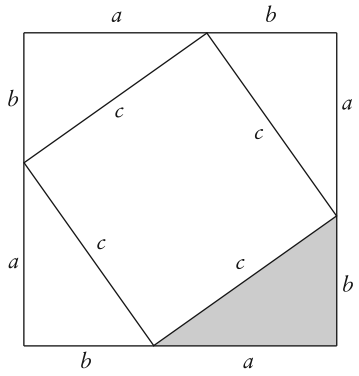
9.2 $x^2 + y^2 = z^2$ Denklemi

Bu denklemle herhalde geometri derslerinde daha önce karşılaşmışsınızdır: Ünlü Pisagor Teoremi'ne göre, bir diküçgenin dik kenarlarının uzunluklarının karelerinin toplamı, üçüncü kenarın (hipotenüsün) karesine eşittir. Şekil aşağıda.



Pisagor Teoremi: $a^2 + b^2 = c^2$.

Söz oraya gelmişken, konumuz olmamasına rağmen Pisagor Teoremi'ni kanıtlayalım. Yukarıdaki gibi bir dik üçgen alalım. Aşağıdaki şekli çizelim.



Büyük karenin her kenarı $a + b$ uzunluğunda, dolayısıyla alanı $(a + b)^2$; bunu aklımızda tutalım. Şimdi aynı alanı başka türlü hesaplayacağız. Bu alan, içindeki beş bölgenin alanının toplamı. Bu bölgelerin dördü bizim dik üçgenimiz ve herbirinin alanı $ab/2$. Böylece dört üçgenin toplam alanı $4 \times ab/2 = 2ab$ olur. Ortada bir de her kenarı c olan bir kare var; bunun da alanı c^2. Demek ki beş bölgenin toplam alanı $2ab + c^2$. Böylece

$$(a + b)^2 = 2ab + c^2$$

eşitliğini kanıtlamış olduk. Sol tarafı açarsak,

$$a^2 + 2ab + b^2 = 2ab + c^2$$

buluruz. Sadeleştirince istediğimiz

$$a^2 + b^2 = c^2$$

eşitliği çıkar. □

$x^2 + y^2 = z^2$ denkleminin her çözümü bize aslında kenarları x, y ve z olan bir diküçgen verir. Eğer çözümler doğal sayıysa, elbette üçgenin kenarlarının uzunluğu doğal sayı olur. Bunlardan en ünlüsü (3, 4, 5) üçgenidir, yani dik kenarları 3 ve 4 olan, hipotenüsü 5 olan dik üçgen. Nitekim

$$3^2 + 4^2 = 5^2$$

olur. Başka tamsayı kenarlı diküçgenler de vardır. Örneğin,

$$5^2 + 12^2 = 13^2.$$

Aşağıdaki teoremde tüm tamsayı kenarlı dik üçgenler gösteriliyor[1].

Teorem 9.2. *$x^2 + y^2 = z^2$ eşitliğinin pozitif tüm doğal sayı çözümleri, gerekirse x ve y'nin rollerini değiştirmeyi kabullenirsek, $d > 0$ ve $u > v > 0$ tamsayıları için*

$$x = d(u^2 - v^2),\ y = 2duv,\ z = d(u^2 + v^2)$$

biçimindedir. Ayrıca her u, v, d seçimi bize bir çözüm verir. Bulunan çözümlerin tekrarlanmamasını istiyorsak, u ve v'yi aralarında asal ve birini tek, diğerini çift alabiliriz; yani bu kısıtlamayla da tüm çözümleri elde ederiz.

Kanıt: Her şeyden önce, verilmiş d, u, v sayıları için teoremdeki

$$x = d(u^2 - v^2),\ y = 2duv,\ z = d(u^2 + v^2)$$

sayıları $x^2 + y^2 = z^2$ eşitliğini sağlar; bunu kontrol etmesi çok kolay, bunun için

$$[d(u^2 - v^2)]^2 + [2duv]^2 = [d(u^2 + v^2)]^2$$

eşitliğini kanıtlamak yeterli. Kolay hesapları okura bırakıyoruz.

Eğer $x^2 + y^2 = z^2$ eşitliğini sağlayan üç x, y, z sayısı bulmuşsak, her d için dx, dy, dz sayıları da bu eşitliği sağlar, yani $(dx)^2 + (dy)^2 = (dz)^2$ olur. Diğer yandan eğer bir d sayısı $x^2 + y^2 = z^2$ eşitliğini sağlayan x, y, z sayılarından ikisini bölüyorsa üçüncüsünü de mecburen böler ve x/d, y/d ve z/d sayıları da aynı eşitliği sağlar, yani $(x/d)^2 + (y/d)^2 = (z/d)^2$ olur. Sonuç olarak, eğer dilersek, $x^2 + y^2 = z^2$ eşitliğini sağlayan x, y, z sayılarının aralarında ikişer ikişer asal olduklarını varsayabiliriz. Sonuç: Eğer ikişer ikişer aralarında asal çözümleri bulursak, bu çözümleri bir d sayısıyla çarparak diğer tüm çözümleri buluruz. Teoremdeki d sayısının da zaten bu görevi görmesi arzulanmış. Bunu biraz daha açalım.

Eğer teoremdeki u ve v sayılarının ortak bir e böleni varsa, o zaman

$$d' = de^2,\ u' = u/e,\ v' = v/e$$

[1] Bu altbölümün bundan sonrası için [S, Bölüm I.2]'den yararlanılmıştır.

sayıları da aynı x, y ve z'yi verir. Bir başka deyişle, eğer istersek, teoremde varlığı ifade edilen u ve v sayılarının aralarında asal olduklarını varsayabiliriz.

Ayrıca eğer u ve v sayılarının her ikisi de tekse, o zaman u^2-v^2 ve u^2+v^2, dolayısıyla x ve z sayıları, dolayısıyla y sayısı da 2'ye bölünür. Demek ki eğer aralarında ikişer ikişer asal x, y, z çözümlerini bulmak istiyorsak,

1. $d = 1$ olmalı,
2. u ve v aralarında asal olmalı,
3. u ve v'den biri tek biri çift olmalı.

Şimdi kanıta geçelim. x, y ve z pozitif doğal sayıları $x^2 + y^2 = z^2$ eşitliğini sağlasın. Yukarıdaki tartışmadan da anlaşılacağı gibi, bu sayıların ikişer ikişer aralarında asal olduklarını varsayabiliriz. Öyle yapalım.

Alıştırma 4.10'a göre, hem x hem y tek sayı olamaz, ikisinden biri çift olmalı. Diyelim y çift. Demek ki x ve z tek olmalı.

Şimdi

$$y^2 = z^2 - x^2 = (z + x)(z - x) \tag{4}$$

eşitliğine göz atalım. Örnek 5.4'e göre,

$$\text{obeb}(z + x, z - x) = 2.$$

Demek ki $z+x$ ve $z-x$ sayıları 2'ye bölünüyorlar. Şimdi şu tanımları yapalım:

$$y = 2y',\ z + x = 2x',\ z - x = 2z'.$$

Elbette x', y', $z' \in \mathbb{Z}$. Ayrıca x' ve y' sayıları aralarında asallar. (4) eşitliğinden,

$$y'^2 = x'z'$$

çıkar. Teorem 7.8'e göre x' ve z' sayıları da birer tamkaredir. Demek ki u ve v doğal sayıları için,

$$x' = u^2 \text{ ve } z' = v^2$$

olur. Buradan

$$\begin{aligned} z + x &= 2x' = 2u^2, \\ z - x &= 2z' = 2v^2, \\ y^2 &= (2y')^2 = 4y'^2 = 4x'z' = 4u^2v^2 \end{aligned}$$

çıkar. Sonuncu eşitlik $y = 2uv$ verir. İlk iki eşitlikten de istenen

$$z = u^2 + v^2 \text{ ve } x = u^2 - v^2$$

eşitlikler bulunur.

Şimdi

$$x = u^2 - v^2,\ y = 2uv,\ z = u^2 + v^2$$

ve

$$x = u_1^2 - v_1^2,\ y = 2u_1v_1,\ z = u_1^2 + v_1^2$$

eşitliklerini varsayalım. İkinci ve üçüncü eşitliklerden,

$$(u + v)^2 = y + z = (u_1 + v_1)^2,$$

yani

$$u + v = u_1 + v_1 \tag{5}$$

çıkar. Birinci eşitliklerden de

$$u^2 - v^2 = x = u_1^2 - v_1^2,$$

yani

$$(u + v)(u - v) = (u_1 + v_1)(u_1 - v_1)$$

çıkar. Bu eşitlik ve (5) bize

$$u - v = u_1 - v_1 \tag{6}$$

verir. (5) ve (6)'yı taraf tarafa toplarsak $u = u_1$, taraf tarafa çıkarırsak $v = v_1$ buluruz. Demek ki aralarında ikişer ikişer asal olan her çözüm, tek bir u ve v çifti tarafından veriliyor. □

Teorem 9.3. *$x^4 + y^4 = z^2$ denkleminin pozitif doğal sayılarda çözümü yoktur.*

Kanıt: Diyelim öyle bir çözüm var, bu çözümlere x, y ve z diyelim. Bu çözümler arasından z'nin en küçük olduğu çözümü alalım.

Eğer bir d sayısı bu sayılardan ikisini bölüyorsa üçüncüsünü de böler ve o zaman da x/d, y/d ve z/d^2 bir başka çözüm olur. Dolayısıyla x, y ve z sayılarının aralarında ikişer ikişer asal olduklarını varsayabiliriz.

Bir önceki teoreme göre aralarında asal u ve v doğal sayıları için

$$x^2 = u^2 - v^2,\ y^2 = 2uv,\ z = u^2 + v^2$$

olur.

$2|y^2$ olduğundan, $2|y$ ve $4|y^2$ olur. Ama $y^2 = 2uv$ olduğundan, bundan u ya da v'nin çift sayı olduğu çıkar. te yandan her ikisinin birden çift olamayacağını biliyoruz, aksi halde x, y ve z aralarında asal olamazlardı.

Diyelim u çift, v tek. O zaman u^2, 4'e tam bölünür, ama v^2, 4'e bölündüğünde 1 kalır. $x^2 = u^2 - v^2$ olduğundan, bundan, x^2'nin 4'e bölündüğünde kalanın 3 olduğu anlaşılır. Ama tamkare sayılar 4'e bölündüğünde kalan ya 0 ya da 1 olmalı, çelişki.

Demek ki u tek, v çift. $v = 2w$ olsun. O zaman

$$y^2 = 2uv = 4uw$$

elde ederiz. u ve w aralarında asal olduğundan, bundan u ve w'nin tamkare oldukları çıkar (Teorem 7.8). Diyelim

$$u = a^2 \text{ ve } w = b^2.$$

Bir önceki teoremi $x^2+v^2 = u^2$ eşitliğine uygulayalım. x, v ve u ikişer ikişer aralarında asallar. Ayrıca v çift. Bir önceki teoreme göre, aralarında asal c ve d sayıları için,

$$x = c^2 - d^2,\ v = 2cd,\ u = c^2 + d^2$$

olur.

$$2cd = v = 2w = 2b^2$$

eşitliklerinden $cd = b^2$ çıkar. Demek ki c ve d birer tamkare. Diyelim $c = x_1^2$ ve $d = y_1^2$. Şimdi

$$x_1^4 + y_1^4 = c^2 + d^2 = u = a^2$$

elde ederiz, yani aynı denklemin ikinci bir çözümü. Ama

$$z = u^2 + v^2 = a^4 + 4b^4 > a^4 \geq a,$$

yani $z > a$. Bu da z'nin en küçük seçim olmasıyla çelişir. □

Alıştırmalar

9.6. $x^4 + y^4 = z^4$ denkleminin pozitif tamsayılarda çözümünün olmadığını gösterin.

9.7. $x^2+y^2 = z^4$ denkleminin pozitif çözümleri vardır. Örneğin $24^2+7^2 = 5^4$. Bu denklemin tüm çözümlerini bulun.

Notlar

9.8. Diofantus, MÖ 201 ile 215 yılları arasında bir tarihte doğmuş İskenderiyeli (Eski Yunan, ama Roma boyunduruluğu altında yaşamış) bir matematikçidir. Yüzyıllar boyunca okunan Aritmetik adlı bir dizi kitabın yazarıdır.

Diofantus

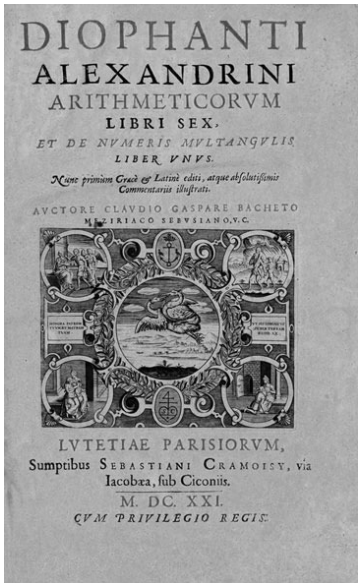
6'ncı yüzyılda yaşamış olan dilbilimci ve matematikçi Metrodus'un Diofantus'la ilgili bir "epigram"ı[2] Diofantus'un yaşını tahmin etmemizi sağlamıştır. Epigram çok sadeleşmiş haliyle şöyle:

Burada Diofantus yatıyor.
Mezar taşı yaşını söylüyor:
Allah ona hayatının 6*'da biri kadar çocukluk verdi.*
Bıyıklarının terlemesi için 12*'de biri daha gerekti.*
Evlenmesi için hayatının 7*'de biri daha geçmeliydi.*
Beş yıl sonra bir oğlu oldu.
Maalesef oğul babasının yarısı kadar yaşadı.
Oğlunun kaybından sonra sayılarda ve bilimlerde teselli arayarak 4 *yıl daha yaşadı.*

Bu öyküye göre Diofantus'un yaşı

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4$$

denkleminin çözümü. Demek ki Diofantus 84 yaşında ölmüştür.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
M. IRIACO SEBVSIANO, V. C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Diofantus'un Aritmetik adlı yapıtının 6'ncı cildinin kapağı. Basım tarihi 1621.

9.9. $x^3 + y^3 = z^3 + t^3$ Diofantus denkleminin tabii ki $x = z$ ve $y = t$ gibi bariz çözümleri vardır. Ama bariz olmayan çözümleri de vardır. Örneğin,

$$12^3 + 1^3 = 9^3 + 10^3 = 1729.$$

Bu 1729 sayısı matematikçiler arasında "taksi sayısı" ya da "Hardy-Ramanujan" sayısı olarak bilinir ve ilginç bir hikâyesi vardır. Başından anlatayım.
Ramanujan (1887-1920), pek matematik eğitimi almamış bir Hint matematik dâhisidir.

[2]Epigram, ilginç, eğlenceli, akılda kolay kalan, şaşırtan ya da komik mısralar anlamına geliyor, bir nevi tekerleme yani.

Ramanujan

Hardy ise, yaşını başını almış, ünlü bir İngiliz profesörüdür ve prestijli Cambridge Üniversitesi'nde çalışmaktadır.

Ramanujan, Hardy'yle mektuplaşmaya başlar, ona bulduğu formülleri yollar. Hardy şaşkınlık içindedir. Formüllerin bir kısmını bilir, ama birçok formül de akıllara durgunluk verecek derinlikte ve zorluktadır. Hardy, Ramanujan'ın Cambridge'e gelmesini sağlar[3]. Ramanujan, bulduğu 3900 kadar formülle matematiğe yepyeni bir soluk getirir, yeni araştırma alanları açar. Ne var ki bu formüllerin birçoğu kanıtlanmamıştır, öylesine sunulmuştur. Zaten Ramanujan da tam olarak kanıt kavramını özümsememişti. Formül ortaya atıyor ancak formülün neden doğru olduğunu kimseye anlatamıyordu; kendisine anlatabildiği bile şüpheli.

G. H. Hardy

Beş yıl öncesine kadar Ramanujan'ın formüllerini matematikçiler hâlâ kanıtlamaya çalışıyorlardı. Şimdi formüllerinin hemen hepsinin doğru olduğu biliniyor.

[3]Böyle bir davetin Türkiye'de mümkün olmadığını üzüntüyle söylemek zorundayım. Formel matematik eğitimi almamış biri için herhangi bir resmî kurumdan para bulabilmek mümkün değildir.

1919'da Ramanujan hastalanır, eskiden yakalandığı dizanteri hastalığının açtığı yaralar İngiltere'de yeniden azar. Hindistan'a geri döner, ancak çok genç bir yaşta, 32'sinde hayata gözlerini yumar.

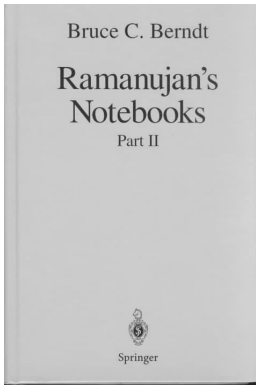
Hardy'ye son yazdığı mektuplar son anlarında bile matematiksel faaliyette olduğunu gösteriyor.

Beyninin nasıl çalıştığını kimse anlayamamıştır.

Yıllar sonra, 1976'da, Ramanujan'ın son yıllarda bulduklarını içeren "kayıp defter"inin bulunması matematikçiler arasında çok heyecan yaratmıştır.

Ramanujan İngiltere'de hastanedeyken, Hardy onu ziyarete gider. Herhalde Ramanujan'ı eğlendirmek için, "Buraya geldiğim taksinin numarası 1729'du. Herhalde hiçbir özelliği olmayan sıkıcı sayılardan biridir" der. Ramanujan, "öyle deme Hardy, der, çok ilginç bir sayıdır 1729, iki (pozitif) küpün toplamı olarak iki farklı biçimde yazılan en küçük sayıdır" der.

İşte bu da 1729'un hikâyesi.



Ramanujan'un not defterlerinin basılmış hali, ikinci cilt

9.10. n'inci taksi sayısı ya da n'inci Hardy-Ramanujan sayısı, n farklı biçimde iki pozitif küpün toplamı olarak yazılan en küçük sayıdır. Hardy ve Wright, böyle bir sayının her n için var olduğunu kanıtlamıştır. Bu sayı $\mathrm{Ta}(n)$ olarak gösterilir. Yukarıda $\mathrm{Ta}(2)$'nin 1729 olduğunu söyledik. $\mathrm{Ta}(1) = 2$ elbette, çünkü $2 = 1^3 + 1^3$.

Bu sayıların nasıl büyüdüğünü göstermek amacıyla birkaç $\mathrm{Ta}(n)$ sayısı verelim:

$$\begin{aligned}
\mathrm{Ta}(3) &= 87.539.319 = 167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3 \\
\mathrm{Ta}(4) &= 6.963.472.309.248 = 2421^3 + 19083^3 = 5436^3 + 18948^3 \\
&= 10200^3 + 18072^3 = 13322^3 + 16630^3 \\
\mathrm{Ta}(5) &= 48.988.659.276.962.496 = 38787^3 + 365757^3 = 107839^3 + 362753^3 \\
&= 205292^3 + 342952^3 = 221424^3 + 336588^3 = 231518^3 + 331954^3
\end{aligned}$$

9.11. Bir başka meşhur Diofantus denklemi, $x^2 - 2y^2 = \pm 1$ ya da $x^2 - 3y^2 = \pm 1$ gibi,

$$x^2 - dy^2 = \pm 1$$

şeklinde yazılan denklemlerdir. (Burada d bir tamkare değildir. Sağ taraftaki sayı da ya 1'dir ya da -1. Marifet her iki denklemin de çözümlerini bulmaktır.) Bu denklemlere Pell denklemleri adı verilir. Mesela $x = 3$, $y = 2$ sayıları $x^2 - 2y^2 = 1$ denkleminin çözümüdür.

$d = 2$ için bazı çözümler Eski Yunan'da ta Pisagor zamanında biliniyordu. Arşimet $d = 3$ için bazı çözümler bulmuştur.

Doğruluğu kolay sayılacak bir hesapla kanıtlanabilen

$$(s^2 - dt^2)(u^2 - dv^2) = (su + dtv)^2 - d(sv + tu)^2$$

eşitliğinden, Eğer

$$x = s,\ y = t \text{ sayıları } x^2 - dy^2 = a \text{ denkleminin çözümüyse}$$

ve

$$x = u,\ y = v \text{ sayıları } x^2 - dy^2 = b \text{ denkleminin çözümüyse}$$

o zaman,

$$x = su + dtv,\ y = sv + tu \text{ sayıları } x^2 - dy^2 = ab \text{ denkleminin çözümü olur}$$

Eğer a, $b = \pm 1$ ise $ab = \pm 1$ olduğundan, bu bize Diofantus denklemlerinin çözümlerini hakkında bir şey söyler: İki Diofantus denkleminin çözümünden kolaylıkla üçüncü bir çözüm daha elde edebiliriz. Bu eşitlik 7'nci yüzyılda yaşamış olan Hintli matematikçi ve gökbilimci Brahmagupta tarafından bulunmuştur. Brahmagupta Pell denklemleri konusunda hatırı sayılır gelişmeler yapmış olan ilk matematikçidir.
Aşağıda, (tamkare olmayan) verilmiş birkaç d için, $x^2 - dy^2 = 1$ denkleminin (bir anlamda) en küçük çözümlerini görüyorsunuz.

d	x	y
2	3	2
3	2	1
5	9	1
6	5	2
7	8	3
8	3	1
10	19	6
11	10	3
12	7	2
13	649	180
14	15	4
15	4	1
17	33	8
18	17	4
19	170	39

Ama mesela $d = 61$ için "en küçük" çözümler bayağı büyük:

$$x = 1.766.319.049 \text{ ve } y = 226.153.980.$$

Öte yandan $d = 60$ için daha makul çözümler bulabiliyoruz:

$$x = 31 \text{ ve } y = 4.$$

9.12. Diofantin denklemleri üzerine birçok araştırma yapılmış, onlarca değerli kitap yazılmıştır. Bu konuda yazılmış kitaplardan biri (üst seviyeden olan) [M]'dir.

10. $n\mathbb{Z} + a$ Kümeleri

Bu başlık altında, obeb ve okek kavramlarını daha modern bir yaklaşımla ele alacağız. Kullanacağımız aygıt, n, $a \in \mathbb{Z}$ tamsayıları için $n\mathbb{Z} + a$ gibi kümeler olacak.

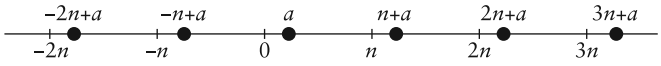
Tanım ve İlk Özellikler. Herhangi bir kuşkuya yer vermemek için, $n\mathbb{Z} + a$ kümelerinin tanımını açık açık yazalım. Burada n ve a birer tamsayıdır ve tanım şöyledir:

$$n\mathbb{Z} + a = \{nk + a : k \in \mathbb{Z}\},$$

yani

$$n\mathbb{Z} + a = \{\ldots, -2n + a,\ -n + a,\ a,\ n + a,\ 2n + a,\ \ldots\}.$$

Demek ki $n\mathbb{Z} + a$ kümesinin ögeleri a'ya n'nin katları eklenerek (ya da n'nin katlarını a'dan çıkararak) elde ediliyor. Burada n ve a herhangi iki tamsayı olabilir.



Koyu noktalar $n\mathbb{Z}+a$ kümesinin ögeleridir.

$n\mathbb{Z} + a$ kümesi

Örneğin $2\mathbb{Z} + 1$ tek tamsayılar kümesidir (yukarıdaki tanımda n yerine 2, a yerine 1 koyun):

$$\begin{aligned} 2\mathbb{Z} + 1 &= \{2x + 1 : x \in \mathbb{Z}\} \\ &= \{\ldots, -6 + 1,\ -4 + 1,\ -2 + 1,\ 1,\ 2 + 1,\ 4 + 1,\ \ldots\} \\ &= \{\ldots, -5,\ -3,\ -1,\ 1,\ 3,\ 5,\ \ldots\}. \end{aligned}$$

Bir başka örnek:

$$\begin{aligned} 5\mathbb{Z} + 2 &= \{5x + 2 : x \in \mathbb{Z}\} \\ &= \{\ldots, -15 + 2,\ -10 + 2,\ -5 + 2,\ 2,\ 5 + 2,\ 10 + 2,\ \ldots\} \\ &= \{\ldots, -13,\ -8,\ -3,\ 2,\ 7,\ 12,\ \ldots\}. \end{aligned}$$

Eğer tanımda $n = \pm 1$ alırsak

$$n\mathbb{Z} + a = \pm\mathbb{Z} + a = \mathbb{Z} + a = \mathbb{Z}$$

olur. Eğer tanımda $n=0$ alırsak

$$n\mathbb{Z}+a=0\mathbb{Z}+a=\{0\}+a=\{a\}$$

olur. Eğer tanımda $a=0$ alırsak

$$n\mathbb{Z}+a=n\mathbb{Z}+0=n\mathbb{Z}$$

olur ve bu $n\mathbb{Z}$ kümeleri toplama, çıkarma ve çarpma işlemleri altında kapalıdır, bir başka deyişle $n\mathbb{Z}$'den alınan iki sayının toplamı, farkı ve çarpımı da bu kümededir. Daha önce de gördüğümüz üzere

$$m|n \iff n\mathbb{Z}\subseteq m\mathbb{Z}$$

olur.

$a\in n\mathbb{Z}+a$ ve $0,\ \pm n\in n\mathbb{Z}$ önermeleri elbette doğrudur.

Eğer $n=\pm m$ ise elbette $n\mathbb{Z}=m\mathbb{Z}$ olur. Bunun ters istikameti de doğrudur. Nitekim eğer $n\mathbb{Z}=m\mathbb{Z}$ ise $n\in n\mathbb{Z}=m\mathbb{Z}$ olur, yani $n\in m\mathbb{Z}$ olur, yani n sayısı m'nin bir katıdır. Benzer nedenden m sayısı da n'nin bir katıdır. Tamsayılarda hesap yaptığımızdan, bu son iki olgudan $n=\pm m$ çıkar.

Ama farklı n ve a sayıları için $n\mathbb{Z}+a$ sayı kümeleri birbirilerine eşit olabilir. Örneğin

$$5\mathbb{Z}+2=5\mathbb{Z}+7=5\mathbb{Z}+12=5\mathbb{Z}-3=-5\mathbb{Z}+2=-5\mathbb{Z}+37=5\mathbb{Z}+37$$

olur. Genel olarak, $n\mathbb{Z}+a$ kümesini betimlemede kullanılan n yerine $-n$ ve a yerine $n\mathbb{Z}+a$ kümesinden herhangi bir sayı koyabiliriz, küme değişmez; bir başka deyişle,

$$n\mathbb{Z}+a=m\mathbb{Z}+b \iff m=\pm n \text{ ve } n|b-a \tag{1}$$

eşdeğerliği geçerlidir. Bu eşdeğerliği kanıtlayalım.

Önce $m=\pm n$ ve $n|b-a$ varsayımlarını yapalım. Demek ki bir $w\in\mathbb{Z}$ tamsayısı için $nw=b-a$ olur. Buradan da

$$m\mathbb{Z}+b=n\mathbb{Z}+b=n\mathbb{Z}+nw+a=n(\mathbb{Z}+w)+a=n\mathbb{Z}+a$$

çıkar. İstediğimizin yarısını kanıtladık.

Şimdi de $n\mathbb{Z}+a=m\mathbb{Z}+b$ eşitliğini varsayalım. $b\in m\mathbb{Z}+b=n\mathbb{Z}+a$ olduğundan $b-a\in n\mathbb{Z}$ olur. Demek ki $n|b-a$. Diyelim $w\in\mathbb{Z}$ tamsayısı için $b-a=nw$. O zaman,

$$n\mathbb{Z}+a=m\mathbb{Z}+b=m\mathbb{Z}+nw+a,$$

yani $n\mathbb{Z}=m\mathbb{Z}+nw$ olur; buradan da $m\mathbb{Z}=n\mathbb{Z}-nw=n(\mathbb{Z}-w)=n\mathbb{Z}$ ve $m=\pm n$ çıkar.

Dolayısıyla eğer $X = n\mathbb{Z} + a$ biçiminde bir kümeyse, n'yi her zaman bir doğal sayı ve a'yı $0, 1, \ldots, n-1$ sayıları arasından seçebiliriz. Bunun için n yerine $|n|$ sayısı ve a yerine, a'yı n'ye böldüğümüzde elde edilen kalanı alabiliriz. Örneğin

$$-7\mathbb{Z} + 23 = 7\mathbb{Z} + 2$$

olur; bir başka örnek:

$$-29\mathbb{Z} + 143 = 29\mathbb{Z} + 27$$

olur.

Toplamlar. Bu paragrafta $n\mathbb{Z}+m\mathbb{Z}$ türünden bir toplamın ne tür bir kümeye eşit olduğunu bulacağız. Örneğin

$$8\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$$

olur. Bir başka örnek:

$$24\mathbb{Z} + 42\mathbb{Z} = 6\mathbb{Z}.$$

Bir örnek daha:

$$24\mathbb{Z} + 36\mathbb{Z} = 12\mathbb{Z}.$$

Konu anlaşılmıştır herhalde! Genel teoremi yazıp kanıtlayalım:

Teorem 10.1 (Bézout Teoremi IV)**.** *a ve b ikisi de aynı anda 0 olmayan iki tamsayı olsun. Eğer $d = \text{obeb}(a, b)$ ise*

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

olur.

Kanıt: Eğer d sayısı hem a'yı hem de b'yi bölüyorsa, $a\mathbb{Z} \subseteq d\mathbb{Z}$ ve $b\mathbb{Z} \subseteq d\mathbb{Z}$ olur. Dolayısıyla

$$a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z} + d\mathbb{Z} = d\mathbb{Z}$$

olur. Bunun özel bir durumu olarak $d = \text{obeb}(a, b)$ alırsak istediğimiz eşitliğin yarısını kanıtlamış oluruz.

Şimdi $d = \text{obeb}(a, b)$ için $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$ önermesini, yani $d \in a\mathbb{Z} + b\mathbb{Z}$ önermesini kanıtlamalıyız, bir başka deyişle $d = au + bv$ eşitliğinin doğru olduğu u, $v \in \mathbb{Z}$ sayılarının varlığını kanıtlamalıyız. Ama bunu Teorem 5.2'de kanıtlamıştık. □

Kesişimler. Önce $n\mathbb{Z} \cap m\mathbb{Z}$ türünden kesişimlerin ne olduklarını bulalım. $n\mathbb{Z} \cap m\mathbb{Z}$ kümesinin ögeleri hem n'ye hem de m'ye bölünen sayılardan oluşur. Okurdan doğruluğunu kendi başına kontrol etmesini isteyeceğimiz örneklerle başlayalım:

$$\begin{aligned} 6\mathbb{Z} \cap 8\mathbb{Z} &= 24\mathbb{Z}, \\ 7\mathbb{Z} \cap 8\mathbb{Z} &= 56\mathbb{Z}, \\ 4\mathbb{Z} \cap 8\mathbb{Z} &= 8\mathbb{Z}, \\ 15\mathbb{Z} \cap 35\mathbb{Z} &= 105\mathbb{Z}. \end{aligned}$$

Şimdi Teorem 10.1'in bir benzerini toplama yerine kesişim için kanıtlayalım.

Teorem 10.2. *a ve b, her ikisi de 0 olmayan iki doğal sayı (ya da tamsayı) olsun. Eğer $e = \text{ekok}(a,b)$ ise*

$$a\mathbb{Z} \cap b\mathbb{Z} = e\mathbb{Z}$$

olur.

Kanıt: $e \in a\mathbb{Z} \cap b\mathbb{Z}$ olduğundan, $e\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$ olur. Diğer istikameti gösterelim. Hem $a\mathbb{Z}$ hem de $b\mathbb{Z}$ kümesinde olan bir sayı, hem a'nın hem de b'nin bir katıdır, dolayısıyla Teorem 8.2'ye göre $e\mathbb{Z}$ kümesindedir[1]. □

Şimdi $n\mathbb{Z}+a$ türünden kümelere geçelim. Bu türden iki kümenin kesişimi ne olur? $(n\mathbb{Z}+a) \cap (m\mathbb{Z}+b)$ kesişimi ne zaman boşküme olur ve boşküme olmadığında hangi kümeye eşit olur?

Birkaç basit örnekle başlayalım:

$$(2\mathbb{Z}+1) \cap (6\mathbb{Z}+4) = \emptyset$$

olur çünkü $2\mathbb{Z}+1$ kümesi tek sayılardan oluşur, oysa $6\mathbb{Z}+4$ kümesinin ögeleri çifttir. Şu örnek de kolay:

$$(2\mathbb{Z}+1) \cap (6\mathbb{Z}+1) = 6\mathbb{Z}+1.$$

ya da

$$3\mathbb{Z} \cap (9\mathbb{Z}+6) = 9\mathbb{Z}+6.$$

Daha zor örnekler var. Örneğin,

$$(18\mathbb{Z}+7) \cap (21\mathbb{Z}+4).$$

Bu kesişimi bulmak yukarıdaki örneklerdeki kesişimleri bulmaktan daha zor. Birazdan doğruluğunu göreceğimiz yanıtı verelim:

$$(18\mathbb{Z}+7) \cap (21\mathbb{Z}+4) = 126\mathbb{Z}+25.$$

Önce $(n\mathbb{Z}+a)\cap(m\mathbb{Z}+b) \neq \emptyset$ varsayımını yapalım. Kesişimden bir s alalım. Demek ki x, $y \in \mathbb{Z}$ için

$$s = nx + a = my + b$$

olur. Demek ki

$$b - a = nx - my \in n\mathbb{Z} + m\mathbb{Z}.$$

[1] Her ne kadar Teorem 8.2 doğal sayı katları için kanıtlanmış gibi görünüyorsa da, tamsayı katları için de aynı teorem aynı kanıtla geçerlidir.

Demek ki, Teorem 10.1'e göre eğer $d = \text{ebob}(n, m)$ tanımını yaparsak,

$$b - a \in n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$$

olur. Böylece eğer $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) \neq \emptyset$ ise $d|b - a$ olduğunu bulduk.

Şimdi $d = \text{ebob}(n, m)$ olsun ve $d|b - a$ varsayımını yapalım; acaba bu koşulla $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) \neq \emptyset$ oluyor mu? Diyelim

$$b - a = dw.$$

Burada w bir tamsayı elbette. Bézout teoremine göre

$$nu + mv = d$$

eşitliğini sağlayan u ve v tamsayıları vardır. Bu son eşitliği w ile çarparsak, $nuw + mvw = dw = b - a$ yani,

$$nuw + a = -mvw + b$$

buluruz. Bu sayıya s dersek, soldaki ifadeden $s \in n\mathbb{Z} + a$ olduğu, sağdaki ifadeden de $s \in m\mathbb{Z} + b$ olduğu çıkar. Demek ki $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) \neq \emptyset$.

Böylece, yukarıdaki iki paragrafta, $d = \text{ebob}(n, m)$ tanımıyla,

$$(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) \neq \emptyset \Longleftrightarrow a \equiv b \bmod d$$

önermesini kanıtlamış olduk.

Şimdi gene $d = \text{ebob}(n, m)$ tanımıyla, $a \equiv b \bmod d$ önermesini varsayıp, boşküme olmadığını artık bildiğimiz $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b)$ kümesinin neye eşit olduğunu bulalım. Kesişimden bir s alalım. $s \in n\mathbb{Z} + a$ olduğundan, $s - a \in n\mathbb{Z}$ olur, yani $n|s - a$. Dolayısıyla sayfa 90'daki (1) eşdeğerliğinden dolayı

$$n\mathbb{Z} + a = n\mathbb{Z} + s$$

olur. Aynı nedenden

$$m\mathbb{Z} + b = m\mathbb{Z} + s$$

olur. Demek ki,

$$(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) = (n\mathbb{Z} + s) \cap (m\mathbb{Z} + s) = (n\mathbb{Z} \cap m\mathbb{Z}) + s,$$

ve eğer $e = \text{ekok}(n, m)$ tanımını yaparsak, Teorem 10.2'ye göre

$$(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) = e\mathbb{Z} + s$$

buluruz. Bulduğumuz sonuçları yazalım:

Teorem 10.3. *n, m, a, $b \in \mathbb{Z}$ olsun. $d = \text{ebob}(n, m)$ ve $e = \text{ekok}(n, m)$ tanımlarını yapalım. $d|a - b$ koşulu, $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b)$ kesişiminin boşküme olmaması için yeter ve gerek koşuldur. Ve bu durumda, kesişimden alınan herhangi bir s için*

$$(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b) = e\mathbb{Z} + s$$

olur. □

Şimdi artık $(18\mathbb{Z} + 7) \cap (21\mathbb{Z} + 4) = 126\mathbb{Z} + 25$ eşitliğinin neden doğru olduğunu biliyoruz: $126 = \text{ekok}(18, 21)$ ve $25 \in (18\mathbb{Z}+7)\cap(21\mathbb{Z}+4)$ olduğundan doğru.

Yukarıdaki teoremin pratik bir değeri olması için kesişimdeki s sayısının nasıl bulunacağı bilinmeli. Bulalım.

n, m, a, $b \in \mathbb{Z}$ olsun. $d = \text{obeb}(n, m)$ tanımını yapalım. $d|a-b$ varsayımını yapalım, ki $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b)$ kesişimi boşküme olmasın. Bir

$$s \in (n\mathbb{Z} + a) \cap (m\mathbb{Z} + b)$$

bulmaya çalışalım. Demek ki x, $y \in \mathbb{Z}$ için,

$$s = nx + a = my + b$$

olmalı. s'yi bulmak demek, $nx + a = my + b$ eşitliğini sağlayan x ve y sayıları bulmak demektir. Bu arada, $nx + a = my + b$ eşitliğini sağlayan bir x ve y sayı çifti varsa, aynı eşitliği sağlayan sonsuz sayıda sayı çifti olduğunu görelim, nitekim eğer $nx + a = my + b$ eşitliği doğruysa, her $k \in \mathbb{Z}$ için

$$n(x + km) + a = m(y + kn) + b$$

eşitliği de doğru olur. Yani $nx+a = my+b$ eşitliğini sağlayan x ve y sayılarından çok vardır, bir sadece bir numune bulmak istiyoruz. Şimdi $nx+a = my+b$ eşitliğini sağlayan x ve y sayılarından birer tane bulalım. Henüz doğruluğunu bilmediğimiz

$$nx + a = my + b$$

eşitliğinden

$$a - b = my - nx$$

çıkar. $d|a - b$ varsayımından dolayı, bir w için

$$dw = a - b$$

olur. Bunu bir önceki eşitliğe taşıyalım:

$$dw = my - nx \tag{2}$$

buluruz. Hâlâ daha x ve y'yi bulamadık ama en azından sağlamaları gereken (2) eşitliğini bulduk.

Şimdi (2) eşitliğini sağlayan x ve y sayılarını bulacağız. $d = \text{obeb}(n, m)$ tanımını kullanalım. Tanımdan dolayı

$$d = nu + mv$$

eşitliğini sağlayan u, v tamsayıları vardır. (Hem de çok vardır.) Bu eşitliği w ile çarpalım:

$$dw = nuw + mvw.$$

Şimdi

$$y = vw \text{ ve } x = -uw$$

tanımlarını yapalım. (Böylece (2) eşitliği doğru oldu.) Şimdi

$$\begin{aligned} nx + a &= -nuw + a = -(d - mv)w + a \\ &= -(d - mv)w + (dw + b) = mvw + b \\ &= my + b \end{aligned}$$

olur. İstediğimizi bulduk: $nx + a = my + b$ ve bu sayı $(n\mathbb{Z} + a) \cap (m\mathbb{Z} + b)$ kesişiminde. Bulduğumuzu yazalım:

Teorem 10.4. *n, m, a, $b \in \mathbb{Z}$ olsun. $d = \text{obeb}(n, m)$ tanımını yapalım. $d|a-b$ varsayımını yapalım. w tamsayısı $dw = a - b$ eşitliğini sağlasın. Ayrıca u, v tamsayıları $d = nu + mv$ eşitliğini sağlasın*[2]*. O zaman*

$$-nuw + a = mvw + b \in (n\mathbb{Z} + a) \cap (m\mathbb{Z} + b)$$

olur. □

Alıştırmalar

10.1. $(21\mathbb{Z} + 6) \cap (35\mathbb{Z} + 20) = e\mathbb{Z} + s$ eşitliğini sağlayan e ve s tamsayılarını bulun.

10.2. $(66\mathbb{Z} + 8) \cap (220\mathbb{Z} + 30) = e\mathbb{Z} + s$ eşitliğini sağlayan e ve s tamsayılarını bulun.

10.3. $(66\mathbb{Z} + 7) \cap (220\mathbb{Z} + 30)$ kümesini bulun.

10.4. $(55\mathbb{Z} + 7) \cap (77\mathbb{Z} + 29)$ kümesini bulun.

10.5. $(14\mathbb{Z} + 1) \cap (35\mathbb{Z} + 29)$ kümesini bulun.

10.6. $(15\mathbb{Z} + 1) \cap (36\mathbb{Z} + 29)$ kümesini bulun.

10.7. $(15\mathbb{Z} + 1) \cap (36\mathbb{Z} + 28)$ kümesini bulun.

10.8. $(15\mathbb{Z} + 2) \cap (36\mathbb{Z} + 29)$ kümesini bulun.

10.9. n ve a iki doğal sayı olsun. Hangi koşullarda $n\mathbb{Z} + a = n\mathbb{Z}$ olur?

10.10. n ve a iki doğal sayı olsun. Hangi koşullarda $n\mathbb{Z} + a$ kümesi toplama işlemi altında kapalı olur?

10.11. n, m ve a üç doğal sayı olsun. Hangi koşullarda $n\mathbb{Z} + a = m\mathbb{Z}$ olur?

[2] Bu eşitliği sağlayan u ve v sayılarının nasıl bulunacağını sayfa 49'da anlatmıştık.

10.12. n, m, a ve b dört doğal sayı olsun. $n\mathbb{Z} + a = m\mathbb{Z} + b$ eşitliğiyle $n\mathbb{Z} + (a - b) = m\mathbb{Z}$ eşitliğinin eşdeğerli olduğunu kanıtlayın.

10.13. n, m, a ve b dört doğal sayı olsun. $n\mathbb{Z} + a = m\mathbb{Z} + b$ ise $n = m$ olduğunu kanıtlayın.

10.14. n, m, a ve b dört doğal sayı olsun. $n\mathbb{Z} + a = m\mathbb{Z} + b$ eşitliği ile

$$n = m \text{ ve } a - b \in n\mathbb{Z}$$

önermesinin eşdeğer olduğunu kanıtlayın.

10.15. $n\mathbb{Z} + 1$ kümelerinin çarpma işlemi altında kapalı olduğunu kanıtlayın, yani bu kümeden iki sayının çarpımı yine bu kümededir.

10.16. $(n\mathbb{Z} + n - 1) \cup (n\mathbb{Z} + 1)$ türünden kümelerin çarpma işlemi altında kapalı olduğunu kanıtlayın.

10.17. $6\mathbb{Z} + 3$ kümesinin çarpma işlemi altında kapalı olduğunu kanıtlayın.

10.18. $15\mathbb{Z} + 6$ kümesinin çarpma işlemi altında kapalı olduğunu kanıtlayın.

10.19. $21\mathbb{Z} + 15$ kümesinin çarpma işlemi altında kapalı olduğunu kanıtlayın.

10.20. Çarpma altında kapalı olan $n\mathbb{Z} + c$ biçiminde başka kümeler bulun.

10.21. $c > 0$ bir doğal sayı olsun. a, c'yi bölen bir sayı olsun. b, $c - 1$'i bölen bir sayı olsun. $n = ab$ olsun. $n\mathbb{Z} + c$ kümesinin çarpma altında kapalı olduğunu kanıtlayın.

Kaynakça

[1. Kitap] Ali Nesin, **Liselilere Matematik 1, Kümeler Kuramı 1**, Nesin Yayıncılık, Eylül 2017.

[2. Kitap] Ali Nesin, **Liselilere Matematik 2, Doğal Sayılar Yapısı**, Nesin Yayıncılık, Eylül 2017.

[E] Edward John Eyre, **Journals of Expeditions of Discovery into Central Australia and Overland from Adelaïd to King George's Sound (1840-1841)**, 2 cilt, Londra 1845, sayfa 324.

[H] Ross Honsberger, **Mathematical Gems**, Dolciani Mathematical Expositions, No 1, Mathematical Association of America, 1973.

[M] Mordell, L. J., **Diophantine Equations**, Academic Press, 1969.

[S] Pierre Samuel, **Théorie Algébrique des Nombres**, Hermann, 1971.

[St] Ian Stewart, **Professor Stewart's Casebook of Mathematical Misteries**, Profile Books 2014.

[W] 2017 yılında Türkiye'de erişimi yasak olan wikipedia. Ama https://tr.wikipedia.org yerine https://tr.0wikipedia.org yazarsanız giriliyor. Normal google aramanızı yapın ve çıkan sayfanın adresinde bulunan wikipedia kelimesinin w'sinden önce bir 0 koyun.

Dizin

0'la çarpma, 32
1, 32

aksiyom, 27
algoritma, 51
altsınır, 19
alttan sınırlı, 19
antisimetri, 18
Arşimet, 87
aralarında asal, 36
Aristo, 5
Aritmetiğin Temel Teoremi, 64, 66
asallara ayrışma, 11
asallara ayrıştırma, 64

Beeger, N.W.H., 61
Bézout Teoremi, 47, 48, 91
Bézout, Etienne, 53, 54
birleşme özelliği, 8–10, 15, 28, 29, 31, 75
Bolyai, János, 70
bölen, 36
bölen sayısı, 68, 69
bölmek, 35
bölünmek, 35
Brahmagupta, 88
Büyük İskender, 70

Charles V, 4
çarpma, 9
çıkarma, 3, 30
çift tamsayı, 37
çokyalancı asal, 61

değişme özelliği, 8, 9, 28, 29, 31
Descartes, René, 39
Diofantus, 84

ekok X, 76
eksi, 3, 4, 30
Elemanlar, 70
etkisiz öge, 8, 9, 29
Euler φ fonksiyonu, 60
Euler, Leonhard, 53

Fermat'nın Küçük Teoremi, 59
Fermat, Pierre de, 38–39

Gauss, Carl Friedrich, 70
geçişkenlik, 18
Giuga Sorusu, 62

Halayudha, 25
Hardy, G. H., 86
Hardy-Ramanujan sayısı, 85, 87

işaret, 23

küp, 10
kalanlı bölme, 39, 40
kare, 10
kat, 35
Kopernik, 5
kuvvet, 10

Lehmer, D.H., 61
Lobachevski, Nicolai Ivanovich, 70
Łukasiewicz, Jan, 17

maksimal öge, 20
max, 20
Méziriac, Claude Gaspard Bachet de, 54
min, 19
minimal öge, 19
mutlak değer, 20

$\mathbb{N}$, 4
negatif, 4
negatif tamsayılar, 4

obeb, 47
Oresme, Nicole, 4
Öklid, 70

Pamuk, Orhan, 53
Pascal, Blaise, 39
Pell denklemleri, 87
Pisagor, 87
Polonya notasyonu, 16
pozitif tamsayılar, 4

Ramanujan, Srinivasa, 85

Riemann, Bernhard, 70

sadeleştirme, 31
Sanson, Justin-Chrysostome, 54
Sarrus, Pierre, 61
sıralama (tamsayılarda), 17

taksi sayısı, 85, 87
tamsıralama, 18
tanımsız, 37
tek tamsayı, 37
tersin tersi, 31
toplama, 8
toplamsal ters, 7, 29, 30

üstten sınırlı, 19

von Ettingshausen, Andreas, 25

Widmann, Johannes, 5
Wright, E. M., 87

yansıma özelliği, 18
yutan öge, 9

$\mathbb{Z}$, 3, 4

Simgeler Dizini

$-x$, 3
$\mathbb{Z}$, 3
$+$, 4, 8, 17, 27
$-$, 7
max, 20
$\pm$, 22, 36
0, 27
1, 27
$<$, 27
$\times$, 27
$\leq$, 29
0, 29
$\vee$, 29
$-a + b$, 30
$-a - b$, 30
$a - b$, 30
$-xy$, 32
$|$, 35
obeb, 47