Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Temel Kavramlar

Prof. Dr. Şenol EREN

Ders 3

Bölüm 2

Tam Sayılar ve Rasyonel Sayılar

2.1 Tam Sayılar

Bu bölümde Soyut Matematik dersinde inşa ettiğiniz tam sayılar kümesinin temel özellikleri incelenecektir.

$\mathbb{Z}$ de ikili işlem, toplama ve çarpma $\forall x, y \in \mathbb{Z}$ için $(x,y) \longrightarrow x+y$ ve $(x,y) \longrightarrow x.y$ şeklinde tanımlanabilir.

Ayrıca çıkarma işlemi $x, y \in \mathbb{Z}$ için $x-y = x+(-y)$ toplama işlemi yardımıyla tanımlanabilir.

Toplama ve çarpma işlemlerinin şu özellikleri vardır.

$\mathbb{Z}_1$: Birleşme Kuralı;

$(x+y)+z = x+(y+z)$, $(xy)z = x(yz)$

$\mathbb{Z}_2$: Değişme Kuralı;

$x+y = y+x$, $x.y = y.x$

$\mathbb{Z}_3$: Etkisiz Eleman;

$x+0=x \quad , \quad x.1=x$

$\mathbb{Z}_4$: Toplamsal Ters Eleman;

$x+(-x)=0$

Her tam sayının çarpımsal tersi yoktur. Çarpımsal terslerinin olması için rasyonel sayılar inşa edilir.

$\mathbb{Z}_5$: Dağılma Kuralı;

$x(y+z)=xy+xz$

Ayrıca dağılma özelliği genelleştirilerek;

$(x_1+\dots+x_m)(y_1+\dots+y_n)=x_1y_1+x_1y_2+\dots+x_ry_s$ yazılabilir.

$\mathbb{Z}_6$: $\forall x,y \in \mathbb{Z}$, $x.y \neq 0 \Rightarrow x\neq 0$, $y\neq 0$ dır.

Bu özellik tam sayılar kümesinde sıfır bölen yoktur şeklinde ifade edilir. Bunun sonucu olarak $x,y,z \in \mathbb{Z}$, $z\neq 0$ ve $xz=yz \Rightarrow x=y$ kısaltma özelliği sağlanır.

Z_7: $x_1 \leq x_2$ ve $y_1 \leq y_2 \Longrightarrow x_1 + y_1 \leq x_2 + y_2$ dir.

Z_8: $x \leq y$ ve $z > 0$ ise $xz \leq yz$ dir.

Tanım 2.1.1 Bir a tam sayısının mutlak değeri $|a|$ ile gösterilir ve

$$|a| = \begin{cases} a; & a \geq 0 \text{ ise} \\ -a; & a < 0 \text{ ise} \end{cases}$$

ile tanımlanır.

Mutlak değer şu özelliklere sahiptir.

M_1: $\forall a \in \mathbb{Z}$ için $|a| \geq 0$

M_2: $|a| = 0 \Longleftrightarrow a = 0$

M_3: $\forall a, b \in \mathbb{Z}$ için $|a+b| \leq |a| + |b|$

Teorem 2.1.2 $m, n \in \mathbb{Z}^+$ ve $x, y \in \mathbb{Z}$ için

i) $x^m \cdot x^n = x^{m+n}$

ii) $(x^m)^n = x^{mn}$

iii) $(xy)^m = x^m \cdot y^m$ dir.

Tanım 2.1.3 $a, b \in \mathbb{Z}$ için $b = ac$ olacak şekilde $\exists c \in \mathbb{Z}$ varsa a, b yi böler denir ve $a|b$ ile gösterilir.

Eğer a, b yi bölmüyorsa $a \nmid b$ ile gösterilir.

0 ın her katı 0 olduğundan $0|0$ ve $0|a$ ise $a = 0$ dır.

Teorem 2.1.4 $a, b, c \in \mathbb{Z}$ için

i) $\mp 1 | a$ ve $\mp a | a$ dır

ii) $a | \mp 1 \iff a = \mp 1$ dir.

iii) Eğer $a|b$ ve $b|c$ ise $a|c$ dir.

iv) Eğer $a|b$ ve $b|a$ ise $a = \mp b$ dir.

v) Eğer $a|b$ ise $\mp a|\mp b$

vi) Eğer $a|b$ ve $a|c$ ise $\forall x,y\in\mathbb{Z}$ için $a|bx+cy$ dir.

Tanım 2.1.5 $a,b\in\mathbb{Z}$ için $a|b$ ve $b|a$ ise a ile b ye ilgili tam sayılar denir.

Teorem 2.1.4 (iv) den sıfırdan farklı her tam sayı bir pozitif tam sayı ile ilgilidir. İlgililik bağıntısı bir denklik bağıntısı olduğundan, bölünebilme söz konusu olduğunda pozitif tam sayıları düşünmek yeterlidir.

Tanım 2.1.6 Pozitif bölenleri yanlız 1 ve kendisi olan 1 den büyük tam sayılara asal tam sayı denir.

Teorem 2.1.7 Her $a>1$ tam sayısının en az bir asal böleni vardır.

İspat: $A=\{d \in \mathbb{Z} \mid d>1$ ve $d \mid a\}$ olsun. $a \mid a$ olduğundan $a \in A$, $A \neq \emptyset$ olur. Pozitif tam sayılar iyi sıralı olduğundan Anın bir en küçük elemanı vardır, buna p diyelim. p nin asal olduğunu gösterirsek ispat biter.

p asal olmasaydı $p=q \cdot r$ ve $1<q<p$ olacak şekilde $\exists q, r \in \mathbb{Z}$ bulunurdu.

$q \mid p$ ve $p \mid a \Rightarrow q \mid a$ olup $q \in A$ olur. Bu da p nin seçimi ile çelişir. Şu halde p asaldır.

Teorem 2.1.8 (Euclid) Sonsuz sayıda asal sayı vardır.

İspat: Kabul edelim ki asal sayılar kümesi $P=\{p_1, \ldots, p_n\}$ sonlu olsun. $a=p_1 \cdot p_2 \cdot \ldots \cdot p_n+1$ tam sayısı 1 den büyük, o halde en az bir asal p böleni vardır.

$p \in P$ dir. $p | p_1 \cdots p_n$ ve $p | a - p_1 \cdots p_n = 1$ yani $p = \mp 1$ bulunur. Bu ise p nin asal oluşuyla çelişir.

Teorem 2.1.9 Her $a > 1$ tam sayısı bir takım (sonlu sayıda) asal sayıların çarpımı olarak yazılabilir.

Teorem 2.1.10 pozitif m ve n tam sayıları verildiğinde, tek türlü olarak belirli öyle bir q, r tam sayıları vardır ki $n = qm + r$ ve $0 \leq r < m$ olur.

İspat: 2. tümevarım prensibini uygulayalım. $n = 1$ olsun. Eğer $m = 1$ ise $q = 1, r = 0$ ve $m > 1$ ise $q = 0, r = 1$ alınarak $n = 1$ için iddia doğrudur.

$n < m$ ise $q = 0$, $r = n$ alınabilir. $m \leq n$ ise $0 \leq n - m < n$ olur ve $n - m = q_1 m + r$ ve $0 \leq r < m$ olacak şekilde $\exists q_1, r \in \mathbb{Z}$ var. $n = (1 + q_1) m + r$ olacağından iddia n içinde doğrudur.

Şimdi q ve r nin tekliğini gösterelim.

$n = q_1 m + r_1 = q_2 m + r_2$, $0 \leq r_1, r_2 < m$ ve $r_1 \neq r_2$ olsun.

$r_2 > r_1$ alalım. $q_1 m + r_1 = q_2 m + r_2 \Rightarrow (q_1 - q_2) m = r_2 - r_1$

bulunur. $0 < r_2 - r_1 < m$ olduğundan, $0 < (q_1 - q_2) m < m$ dir.

fakat $1 \leq q_1 - q_2 \Rightarrow m \leq (q_1 - q_2) m$ olduğundan

$r_1 \neq r_2$ olmasının bizi çelişkiye götürdüğü anlaşılır.

$r_1 = r_2$ ve dolayısıyle $q_1 = q_2$ olmalıdır.

Teorem 2.1.11. $m \neq 0$ ve $m, n \in \mathbb{Z}$ olsun. Tek türlü olarak belirli öyle $q, r \in \mathbb{Z}$ bulunurki $n = qm + r$ ve $0 \leq r < |m|$ olur.

Tanım: 2.1.12 $n = qm + r$, $0 \leq r < |m|$ ise q ye bölüm r ye de kalan denir. Verilen m ve n tam sayıları için q ve r yi bulmaya da n yi m ile kalanlı bölme denir.

Örnek 2.1.13 i) $n=13$, $m=5$ alınırsa $13=2.5+3$ ve $0\leq 3<5$ tir.

ii) $n=13$, $m=-5$ alınırsa $13=(-2)(-5)+3$ ve $0\leq 3<|-5|$ tir.

Tanım 2.1.14 m ve n sıfırdan farklı tam sayılar olsun.

i) $d\in\mathbb{Z}^+$

ii) $d|m$ ve $d|n$

iii) $k\in\mathbb{Z}$ için $k|m$ ve $k|n$ ise $k|d$

şartlarını sağlayan d tam sayısına m ile n tam sayılarının en büyük ortak böleni denir ve (m,n) veya $ebob(m,n)$ ile gösterilir.

Teorem 2.1.15 Sıfırdan farklı iki tam sayının en büyük ortak böleni vardır ve $d=(m,n)$ ise $d=mx+ny$ olacak şekilde $\exists x,y\in\mathbb{Z}$ bulunabilir.

İspat: $A=\{mx+ny \mid mx+ny>0,\ x,y\in\mathbb{Z}\}$ olsun.

$x=m$, $y=n$ için $m^2+n^2>0$ olup $A\neq\emptyset$ olur. Pozitif tam sayılar iyi sıralı olduğundan A'nın d gibi bir en küçük elemanı vardır. Şimdi $d=(m,n)$ olduğunu gösterelim. m'yi d'ye kalanlı bölelim $m=qd+r$ ve $0\leq r<d$ o. şekilde $\exists q,r\in\mathbb{Z}$ bulunabilir. $d=mx+ny$ olduğundan $m=q(mx+ny)+r \Rightarrow r=m(1-qx)+n(-qy)$ dir. $r\neq 0$ ise $r\in A$ olurki çelişki dolayısıyla $r=0$ olup $d\mid m$ bulunur. Benzer şekilde $d\mid n$ olduğuda gösterilebilir.

$e\in\mathbb{Z}$, $e\mid m$ ve $e\mid n \Rightarrow d=mx+ny$ olup $e\mid d$ dir. Sonuç olarak $d\in A$ olduğundan $\exists x,y\in\mathbb{Z}$ için $d=mx+ny$ bulunur.

Tanım 2.1.16 iki tamsayının en büyük ortak bölenleri 1 ise bu iki sayıya aralarında asaldırlar denir.

Not 2.1.17 m ve n pozitif tam sayılar olsun. ard arda aşağıdaki kalanlı bölmeleri yapalım.

$n = q_1 m + r_1$ ve $0 \leq r_1 < m$ (1)

$m = q_2 r_1 + r_2$ ve $0 \leq r_2 < r_1$ (2)

. . . .

$r_{k-1} = q_{k+1} r_k + r_{k+1}$ ve $0 \leq r_{k+1} < r_k$ (k+1)

$r_k = q_{k+2} r_{k+1} + 0$ . . . (k+2) şeklinde kalan sıfır oluncaya kadar devam edelim. $m > r_1 > r_2 \ldots$ olduğuna dikkat edersek sonlu bir adımdan sonra 0 kalanını bulacağımız aşikardır.

Teorem 2.1.18 (Euclid Algoritması) yukarıda yapılan kalanlı bölmeler arasında sıfırdan farklı en son kalan m ile n nin en büyük ortak bölenidir, yani $r_{k+1}=(m,n)$ dir.

İspat: $r_{k+1}|r_k$ ve $r_{k+1}|q_{k+1}r_k+r_{k+1}=r_{k-1}$ ve bu şekilde devam edilirse $r_{k+1}|m$ ve $r_{k+1}|n$ elde edilir. Şimdi $e\in\mathbb{Z}$

$e|m$ ve $e|n \Rightarrow e|n-q_1m=r_1$

$e|m$ ve $e|r_1 \Rightarrow e|m-q_2r_1=r_2$ böyle devam edilerek $e|r_{k+1}$ bulunur, dolayısıyla $r_{k+1}=(m,n)$ dir.

Örnek 2.1.19 963 ile 657 sayılarının en büyük ortak bölenini bu yolla bulalım.

$963 = 1.657 + 306$

$657 = 2.306 + 45$

$306 = 6.45 + 36$

$45 = 1.36 + 9$

$36 = 4.9 + 0$

$9 = 45 - 36$

$9 = 45 - (306 - 6.45) = -306 + 7.45$

$9 = -306 + 7.(657 - 2.306)$

$9 = 7.657 - 15.306$

$9 = 7.657 - 15(963 - 657)$

$9 = -15.963 + 22.657$ bulunur

Buradan $x_0 = -15$ $y_0 = 22$ bulunur ayrıca

$9 = (963, 657)$ dir.

Teorem 2.1.20 m ve n sıfırdan farklı ve c herhangi bir tam sayı olsun. $(m,n)=1$ ve $m|nc \Rightarrow m|c$ dir.

İspat: $(m,n)=1$ ise $\exists x,y\in\mathbb{Z}$ için $1=mx+ny$ dir.

$c=c(mx)+c(ny)=(mc)x+(nc)y$ bulunur.

$m|mc$ ve $m|nc$ ise $m\,|\,(mc)x+(nc)y=c$ bulunur.

Sonuç 2.1.21 p asal ve $p|mn$ ise $p|m$ veya $p|n$ dir.

İspat: p asal olduğundan $p|m$ veya $(p,m)=1$ dir.

$(p,m)=1$ ise $1=px+my$, $\exists x,y\in\mathbb{Z}$ var.

$n=npx+mny \Rightarrow p|n$ bulunur.

Teorem 2.1.22 (Aritmetiğin Temel Teoremi) Her $a>1$ tam sayısının asal çarpanlara ayrılışı, sıra düşünmeksizin tek türlüdür.

Tanım 2.1.23 m ve n sıfırdan farklı iki tam sayı olsun.

i) $k \in \mathbb{Z}^+$

ii) $m|k$ ve $n|k$

iii) $m|t$ ve $n|t$ için $k|t$ şartlarını sağlayan $k \in \mathbb{Z}$ sayısına m ile n tam sayılarının enküçük ortak katı denir $[m,n]$ veya okek$[m,n]$ ile gösterilir.

$n = P_1^{m_1} \cdots P_r^{m_r}$ ve $m = P_1^{n_1} \cdots P_r^{n_r}$ ise

$(n,m) = P_1^{\min(m_1,n_1)} \cdots P_r^{\min(m_r,n_r)}$

$[n,m] = P_1^{\max(m_1,n_1)} \cdots P_r^{\max(m_r,n_r)}$ dir.

Teorem 2.1.24 m ve n pozitif tam sayılar olsun $(m,n).[m,n]=m.n$ dir.

Tanım 2.1.25 pozitif n tam sayısı için $1\leq a<n$ ve $(a,n)=1$ olan a tam sayılarının sayısı $\varphi(n)$ ile gösterilir ve Euler fonksiyonu denir.

Euler Fonksiyonunun şu özellikleri vardır.

E_1: p asal ise $\varphi(p)=p-1=p\left(1-\frac{1}{p}\right)$

E_2: p asal ve $t\in\mathbb{N}$ ise $\varphi(p^t)=p^t-p^{t-1}=p^t\left(1-\frac{1}{p}\right)$

E_3: $(m,n)=1$ ise $\varphi(mn)=\varphi(m).\varphi(n)$ dir.

E_4: $m=p_1^{\alpha_1}\ldots p_r^{\alpha_r}$ ise

$\varphi(m)=p_1^{\alpha_1}\ldots p_r^{\alpha_r}\left(1-\frac{1}{p_1}\right)\ldots\ldots\left(1-\frac{1}{p_r}\right)$ dir.

Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Teşekkürler

Cebir I

Prof. Dr. Şenol EREN

Ders 3