EL-CEBR
ALGEBRA
CEBİR

Babamın Anısına...

ve Aileme...

Erhan GÜLER

3.10.1995
Salı

$A = \{a \mid p(a)\}$

$A = \{a \in \mathbb{Z} \mid a > 0\} = \{1, 2, 3, \ldots\}$

$B = \{a \in \mathbb{R} \mid \sqrt{a} \in \mathbb{Z}\} = \{0, 1, 4, 9, 16\}$

$A \times A$ nın boş olmayan herhangi bir alt kümesi

$A \times B$ nin " " "

$\phi \neq \overset{f}{\sim} \subset A \times B$

$(a,b) \in \sim$ $a \sim b$

$(a,b) \in f$ afb $b = f(a)$ fonksiyon: özel bir bağıntı.

i- $\forall a \in A$, $(a, *) \in f$ $\quad * = f(a)$

ii- $(a, *) \notin f$ $\quad (a, \square)$ fonksiyonda A nın bir elemanı B nin farklı bir elemanına gitmez.

- $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ (bire-bir olma)
- $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\forall b \in B$ için $f(a) = b$ o.s. $\exists a \in A$ (örten olma)

Fonksiyon 1:1 ve örten ise tersi vardır.

$f: A \to B$ $\quad b \in B$, $f^{-1}(b) = \{a \in A \mid f(a) = b\}$ 1:1 ve örten ise bu küme bir tek elemandan oluşur.

$f: \mathbb{R} \longrightarrow \mathbb{R}$
$x \longrightarrow |x|$ $\qquad f^{-1}(3) = \{3, -3\}$, $f^{-1}(-4) = \phi$

Denklik bağıntısı : Yansıma, Simetri, Geçişme

$\phi \neq \sim \subset A \times A$

i- $\forall a \in A$, $a \sim a$ $\quad (a,a) \in \sim$ (yansıma)

ii- $(a,b) \in \sim \Rightarrow (b,a) \in \sim$ $\qquad a \sim b \Rightarrow b \sim a$ (simetri)

iii- $(a,b) \in \sim$ ve $(b,c) \in \sim \Rightarrow (a,c) \in \sim$

$a \sim b$ ve $b \sim c \Rightarrow a \sim c$ (geçişme)

Denklik sınıfı :

$a \in A$, $\bar{a} = \{b \in A \mid a \sim b\}$ a ile bağıntılı olan tüm bağıntıların kümesi.

$a,b \in \mathbb{Z}$, $a \sim b \overset{tm}{\iff} 5 \mid a-b$ ($\overset{tm}{\iff}$: tanım)

$a \equiv b \pmod 5 \iff 5 \mid a-b$

$\bar{8} = \{\dots, -7, -2, 3, 8, 13, \dots\}$ $\quad \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}$

Herbiri $\mathbb{Z}$ nin bir alt kümesidir. Bu kümelerin birleşimi $\mathbb{Z}$ yi verir.

$\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} \cup \bar{4} \cup \bar{5} \cup \bar{6} \cup \bar{7}$

Denklik bağıntısı varsa, kümeyi ayrık kümelere ayırabiliriz.

Kümenin ayrışımı verilip, denklik bağıntısı istenirse;

$A = \bigcup_{i \in I} A_i \quad i \neq j \quad i,j \in I$ için $A_i \cap A_j = \emptyset$

$\forall a,b \in A$, $a \sim b \overset{tm}{\iff} a,b \in A_i$ denklik bağıntısıdır. Gösterelim.

$a \sim b \Rightarrow a,b \in A_i$ $\quad A_i \# A_j$ olsa $b \in A_i \cap A_j$ olur.

$b \sim c \Rightarrow b,c \in A_j$ $\quad$ O halde $A_i = A_j$ dir.

$A = \{a,b,c\}$ A üzerinde denklik bağıntısı yazalım.

① $A = \{a\} \cup \{b\} \cup \{c\}$ ③ $A = \{b\} \cup \{a,c\}$ ⑤ $A = \{a,b,c\}$

② $A = \{a\} \cup \{b,c\}$ ④ $A = \{c\} \cup \{a,b\}$

Her üçü birbiriyle bağıntılı olsun.

$\beta_5 = \{(a,a),(b,b),(c,c),(a,b),(b,a),(a,c),(c,a),(b,c),(c,b)\}$

$\bar{a} = \{a,b,c\}$ $\quad \bar{c} = \bar{b} = \{a,b,c\}$

$\beta_1 = \{(a,a),(b,b),(c,c)\}$

$\beta_2 = \{(a,a),(b,b),(c,c),(a,b),(b,a)\}$

$\beta_3 = \{(a,a),(b,b),(c,c),(b,c),(c,b)\}$

$\beta_4 = \{(a,a),(b,b),(c,c),(a,c),(c,a)\}$

- $\forall x,y \in A$, $x \sim y \overset{tm}{\iff} x = y$

Denklik bağıntısı eşitliğin genelleştirilmiş halidir.

$3,8 \in \mathbb{Z}$ $\quad 3 \neq 8$ $\quad 3 \equiv 8 \pmod 5$

$A, \sim$ $\quad A/_{\sim} = \{\bar{a} \mid a \in A\}$

denklik sınıflarından oluşan kümeyi A/N ile gösteririz.

** $a \sim b \Leftrightarrow 5 \mid a-b$

$\mathbb{Z}_5 = \mathbb{Z}/N = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ → denklik sınıflarının kümesi.

Ödev // 4 ve 5 elemanlı küme üzerinde denklik sınıflarını yazın.

$\{0,1,2,3,4\}$ bağıntının tam temsilciler kümesidir.

Her denklik sınıfından birer tane eleman almakla oluşturulan kümeye tam temsilciler sistemi diyoruz.

$\{5,11,7,13,24\}$ tam temsilciler kümesidir.

TAM SAYILAR

$\forall a,b \in \mathbb{Z}, (b \neq 0)$ b/a diyeceğiz. Eğer $a = bt$ o.ş. $\exists t \in \mathbb{Z}$.
($b \mid a$: b, böler a'yı) b ve t'ye a'nın çarpan veya bölenleri denir.

1°) $\forall n \in \mathbb{Z}$ için $\mp 1 \mid n$ dir.

$n \mid \mp 1 \Leftrightarrow n = \mp 1$

2°) $m \mid n$ ve $n \mid p \Rightarrow m \mid p$

3°) $m \mid n$ ve $n \mid m \Rightarrow m = \mp n$

4°) $m \mid n$ ise $\mp m \mid \mp n$

$3 \mid 6 \quad 6 = 2.3$, $-3 \mid 6 \quad 6 = (-2)(-3)$, $-3 \mid -6 \quad -6 = 2(-3)$

$3 \mid -6 \quad -6 = (-2).3$

5°) $\left.\begin{matrix} m \mid n \\ m \mid p \end{matrix}\right\} \Rightarrow \forall x,y \in \mathbb{Z}, \; m \mid nx + py$

6°) $m \neq 0 \quad m \mid n \Rightarrow |m| \leq |n|$

4. özellikten dolayı $\mathbb{Z}^+$ da inceleme (bölünebilme) yapacağız.

$\mathbb{Z}^-$ de aynı şekilde incelenebilir.

Asal Sayı: Kendisinden ve 1'den başka bir böleni olmayan pozitif sayılara asal sayı denir.

Önerme // Sıfır ve ∓1 den farklı her tamsayının en az bir asal böleni vardır.

İspat // $a \in \mathbb{Z}$ ve $a \neq 0, \mp 1$ olsun.

$M = \{ d \in \mathbb{Z}^+ \mid d|a \, , d \neq 1 \}$ $\quad M \subset \mathbb{Z}^+$

$|a| | a \, , |a| < M \Rightarrow M \neq \emptyset$ $\quad$ (p : M nin en küçük elemanı.)

$\mathbb{Z}^+$ dan alınan her tamsayının alt kümelerinin en küçük elemanı vardır.

$\mathbb{Z}^-$ den " " " en büyük " " .

En küçük elemanı p ile gösterelim. p asal ise önerme ispatlanır. p asal değilse, p nin öz bölenleri (q ve r gibi) vardır.

p asal değilse : $p = qr$ ve $1 < q, r < p$ $\exists q, r \in \mathbb{Z}^+$ vardır.

$q|p \, , p|a \Rightarrow q|a \Rightarrow q \in M$ # (çelişki)

q'yu en küçük bulduk. Fakat p yi en küçük asal olarak aldığımız için çelişki olur. O halde p en küçük asal olmak zorundadır.

Teorem : (Euclide) Sonsuz sayıda asal vardır.

İspat // $P = \{ p_1, p_2, \ldots, p_n \}$ Kabul edelim ki P sonlu tane asal sayıyı göstersin. Bu kümede bulunmayan bir tane de olsa asal bulursak, kümenin asal olduğu ortaya çıkar.

$a = p_1 p_2 \ldots p_n + 1$ tamsayısını düşünelim. a'nın bir asal böleni vardır. Bunu q ile gösterelim. Kabulden dolayı $q \in P \Rightarrow$

$q | p_1 p_2 \ldots p_n$ (5. özellikten $q|a$)

$q | a - p_1 p_2 \ldots p_n = 1$ # çelişkidir. $(m|nx+py)$

O halde $q \notin P$

$$\left\{ \begin{matrix} q|a \\ q|(p_1 p_2 \ldots p_n) \end{matrix} \right\} \Rightarrow q | ax + (p_1 p_2 \ldots p_n) y \, , \quad \left\{ \begin{matrix} 5|15 \\ 5|20 \end{matrix} \right\} \Rightarrow 5 | 20x + 15y \;\; \exists x, y$$

$x = 1$ ve $y = -1$ için $q | a - p_1 p_2 \ldots p_n$ olur.

O halde sonsuz sayıda asal sayı vardır.

Teorem : $\forall m,n \in \mathbb{Z}, (m \neq 0)$ $n = qm + r$ ve $0 \leq r < |m|$ o.ş. $q, r \in \mathbb{Z}$ vardır.

$7 = 1.5 + 2$, $-7 = (-2)5 + 3$, $5 = 0.7 + 5$, $5 < |-7| = 7$.

Tümevarımla ispatlanır. //

TANIM : Pozitif d tamsayısına a ve b tamsayılarının ebob denir, eğer ;

i- $d|a$ ve $d|b$

ii- a ve b nin her ortak k böleni için $k|d$ oluyorsa,

$d = (a,b)$ veya $ebob(a,b)$ ile gösterilir.

$(a,b) = (a,-b) = (-a,b) = (-a,-b)$

Önerme // $\forall 0 \neq a,b \in \mathbb{Z}$ nin ebob vardır ve $(a,b) = d$ ise $ax + by = d$ o.ş. $\exists x,y \in \mathbb{Z}$ vardır.

İspat // $S := \{ ax + by \mid \exists x,y \in \mathbb{Z},\ ax + by > 0 \}$

$x = a$ ve $y = b$ alırsak , $aa + bb = a^2 + b^2 > 0$ olur.

Dolayısıyla $S \neq \emptyset$ olur. S nin en küçük elemanı vardır. Bunu d ile gösterelim. İddia ediyoruz ki, d ; a ile b'nin ebob'dur. (Yani d, hem a yı hem de b yi böler.)

$a = qd + r$ ve $0 \leq r < d$ o.ş. (Bölme algoritmasından dolayı.)

$\exists q,r \in \mathbb{Z}$ vardır. $\exists x,y \in \mathbb{Z}$, $d = ax + by$ dir.

$a = q(ax + by) + r \Rightarrow r = (1 - qx)a + (-qy)b \Rightarrow r \in S$, $r \neq 0$

ve d , S nin en küçük elemanı olduğundan $r = 0$ olmalıdır.

$a = qd$ olur. Ve $d|a$ olur. Aynı işlemler yapılarak $d|b$ olduğu gösterilebilir. 1. şart sağlanmış oldu. 2. şartın sağlandığını gösterelim.

ii- k, a ve b nin herhangi bir ortak böleni olsun.

$a = km$, $b = kn$ o.ş. $\exists m,n \in \mathbb{Z}$ vardır.

$d = ax + by = k(mx + ny) \Rightarrow k|d$ 2. şart sağlanır //

{ -34 ve 16 sayılarının ortak böleni 2 dir.

$-34(-1) + 16(-2) = 2$ }

İki tamsayının ebob'u 1 ise bu tamsayılara aralarında asaldır denir.

Teorem: $(m,n)=1$ ve $m \mid nc \Rightarrow m \mid c$

İspat // $(m,n)=1 \Rightarrow 1=mx+ny$ o.ş. $\exists\, x,y \in \mathbb{Z}$ vardır.

$\Rightarrow c = mcx + ncy$ $\quad \left.\begin{matrix} m \mid mc \\ m \mid nc \end{matrix}\right\} \Rightarrow m \mid (mc)x + (nc)y = c$

p asal sayısı verilsin. $\exists n \in \mathbb{Z}$, $(p,n)=1$ veya $p \mid n$

Sonuç: $p \mid ab \Rightarrow p \mid a$ veya $p \mid b$

$6 \mid 3.4 \Rightarrow 6 \nmid 3$ ve $6 \nmid 4 \Rightarrow 6$ asal değildir.

{Eski sınav sorusu: $\left(\frac{a}{b}\right)^n \in \mathbb{Z} \Rightarrow \frac{a}{b} \in \mathbb{Z}$ dir.}

Önerme // $(a,b)=d$ olsun.

$\left.\begin{matrix} a=a'd \\ b=b'd \end{matrix}\right\} \Rightarrow (a',b')=1$ dir.

- $(34,16)=2 \quad \left(\frac{34}{2}=17,\ \frac{16}{2}=8\right)=1$ dir.

İspat // $(a',b')=k>1$ olsun. $a'=kl$, $b'=kt$ o.ş. $\exists\, l,t \in \mathbb{Z}$.

$\left.\begin{matrix} a=l(kd) \\ b=t(kd) \end{matrix}\right\} \Rightarrow (kd)$, a ve b nin bir ortak böleni olur.

$kd>d$ bir çelişkidir. $k>1$ kabul ettik. O halde a ve b nin ebob'u d verildiğinden $k>1$ olamaz. $(a',b')=1$ olmalıdır. //

$\left\{\begin{matrix} (a,b)=d \\ a'=ad \\ b'=bd \end{matrix}\right\} \Rightarrow \left(\frac{a}{d},\frac{b}{d}\right)=1 \quad (a',b')=1$

$\forall n \in \mathbb{Z}\ (n>1)$, $n=p_1^{\alpha_1}.p_2^{\alpha_2}.\dots.p_t^{\alpha_t}$ (p_i asal, $\alpha_i \in \mathbb{N}$)

Önerme // $(m,n)=1$ olsun. $(a,mn)=1 \Leftrightarrow \exists r,s \in \mathbb{Z}$ vardır ki,

$(r,m)=1=(s,n)$ ve $a=nr+ms$ dir. Veya;

{$(a,mn)=1 \Leftrightarrow (r,m)=1=(s,n)$ ve $a=nr+ms$ o.ş $\exists r,s \in \mathbb{Z}$.}

$n \in \mathbb{Z}^+$, $\varphi(n)=\#\{1 \le A < n,\ (d,n)=1\}$

$\varphi(2)=1$ $\quad \varphi(4)=2$ $\quad \varphi(6)=2$ $\quad \varphi(8)=4$ $\quad \varphi(269)=268$ //

$\varphi(3)=2$ $\quad \varphi(5)=4$ $\quad \varphi(7)=2$

↓ asal.

17 den önce hiçbir sayı bölmez.

Teorem: $(m,n)=1 \Rightarrow \varphi(mn)=\varphi(m).\varphi(n)$

$\varphi(mn) = \#\{1 \le a < mn \;,\; (a,mn)=1\}$

$\varphi(m) = \#\{1 \le r < m \;,\; (r,m)=1\}$

$\varphi(n) = \#\{1 \le s < n \;,\; (s,n)=1\}$

$\left\{ \begin{array}{l} (n?+m?, mn)=1 \\ \varphi(m)\varphi(n) \lesseqgtr \varphi(mn) \end{array} \right\}$

ispat// $(m,n)=1 = nx+my$ o.s $\exists x,y \in \mathbb{Z}$.

$\Rightarrow$: $a = n(ax)+m(ay)$ $\qquad r=ax,\ s=ay$

$(r,m)=t \Rightarrow t/r$ ve $t/m \Rightarrow t/a$, $t/mn \Rightarrow t/(a,mn)=1 \Rightarrow t=1$

$(s,n)=1$ oldugu benzer sekilde gösterilir.

$\Leftarrow$: $(a,m)=d$ diyelim. $d/a-ms=nr$ $\Rightarrow d/r$, $d/(r,m)=1$ $d=1$

$(m,n)=1$ ve $d/m \Rightarrow (d,n)=1$

$(a,m)=1$ dir. //

Benzer sekilde $(a,n)=1$ olur.

Euler Fonksiyonunun özellikleri :

1- $(m,n)=1 \iff \varphi(mn)=\varphi(m)\varphi(n)$

2- p asal ise $\varphi(p)=p-1=p(1-\frac{1}{p})$ $\left\{ \begin{array}{l} \varphi(p): p \text{ den küçük, } p \text{ ile aralarında} \\ \text{asal sayıların sayısı.} \end{array} \right\}$

3- p asal ve $n>0$, $\varphi(p^n)=p^n-p^{n-1}=p^n(1-\frac{1}{p})$

4- $m=p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_t^{\alpha_t} \Rightarrow \varphi(m)=m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\dots(1-\frac{1}{p_t})$

$\varphi(m)=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\dots\varphi(p_t^{\alpha_t})$

$=p_1^{\alpha_1}(1-\frac{1}{p_1})p_2^{\alpha_2}(1-\frac{1}{p_2})\dots p_t^{\alpha_t}(1-\frac{1}{p_t})$

$=p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_t^{\alpha_t}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\dots(1-\frac{1}{p_t})$

$=m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\dots(1-\frac{1}{p_t})$ dir. //

3. özellik : $\#\{1 \le s < p^n \;,\; (s,p^n) \neq 1\} = p^{n-1}$

$1p, 2p, \dots, p.p, \dots, p^2.p, \dots p^{n-1}.p = p^n$

p nin, p^{n-1} -inci katına kadar olan sayılar p^n ile aralarında asal değildir.

$(s,p^n) \neq 1 \Rightarrow s=kp$ $\quad \{(p^n,p^n)\neq 1\}$

Sorular :

1- $\forall m,n \in \mathbb{Z}$ $(m \neq 0)$ için $n = qm + r$ ve $|r| \leq \frac{|m|}{2}$ o.ş. $\exists q,r \in \mathbb{Z}$.

(Bu yazılış tek türlü değildir.)

Çözüm // Euclide bölme algoritmasından (tamsayılarda kalanlı bölmeden),

$n = qm + r$ ve $0 \leq r < |m|$ o.ş $q,r \in \mathbb{Z}$ vardır.

i- $r \leq \frac{|m|}{2}$ ise ispat tamamdır.

ii- $r > \frac{|m|}{2}$ ise $n = \underbrace{(q+1)}_{q'} m + \underbrace{r-m}_{r'} = q'm + r'$

$r > \frac{|m|}{2} \Rightarrow |r-m| < \frac{|m|}{2}$ dir. //

2- $(a, mn) = 1 \Leftrightarrow (a,m) = 1 = (a,n)$ dir.

Çözüm // $\Rightarrow$: $(a,mn) = 1$ olsun. $(a,m) = d > 1$ olsa, d nin p gibi bir asal böleni vardır.

$p \mid a$
$p \mid m \Rightarrow p \mid mn$ ve $p \mid a \Rightarrow p \mid (a,mn) = 1$ # } $(a,n) = 1$ olduğu da görülür. }

$\Leftarrow$: $(a,mn) = k > 1$ olsa, k nın bir q asal böleni vardır.

$q \mid mn \Rightarrow q \mid m$ veya $q \mid n$ # $\Rightarrow k = 1$ olur. //

3- $\forall a,b \in \mathbb{Z}$ için $ax + by = 1$ o.ş. $\exists x,y \in \mathbb{Z}$ ise $(a,b) = 1$ dir.

Çözüm // $(a,b) = k \Rightarrow k \mid a$ ve $k \mid b \Rightarrow k \mid ax$ ve $k \mid by \Rightarrow k \mid ax + by = 1$

$\Rightarrow k = 1 = (a,b)$ dir. //

4- $(m,n) = 1$, $a,b,m \in \mathbb{Z}$, $\begin{matrix} m \mid a \\ n \mid a \end{matrix} \Rightarrow mn \mid a$ dır.

Çözüm // $m \mid a \Rightarrow a = mk$, $\exists k \in \mathbb{Z}$ ve $n \mid a \Rightarrow a = nt$, $\exists t \in \mathbb{Z}$

$a = mk = nt \Rightarrow m \mid t \Rightarrow t = mr$ o.ş $r \in \mathbb{Z}$.

$a = nt = (mn)r \Rightarrow mn \mid a$ dır. //

5- $(m,n) = 1 \Rightarrow (m+n, mn) = 1$ dir.

Çözüm // $(m+n, mn) = d > 1$ olsun. d nin en az bir p asal böleni vardır.

$p \mid d$ olduğundan $p \mid m+n$, $p \mid mn \Rightarrow p \mid m$ veya $p \mid n$

$p \mid m$ olsa $p \mid m+n$ olduğundan $p \mid n$ olur $p \mid (m,n) = 1$ olduğundan çelişkidir. //

$A|B$, $A|B+C$ $\Rightarrow A|C$ dir. $B=AK$, $B+C=A.T$ $\Rightarrow C=AT-B$
$= AT-AK$
$C=A(T-K) \Rightarrow A|C$ olur. //

6- Bir tamsayının n-inci dereceden kökü rasyonel sayı ise bu sayı tamsayı olmak zorundadır.

Çözüm // $\sqrt[n]{a} \in \mathbb{Q} \Rightarrow \sqrt[n]{a} \in \mathbb{Z}$ $(a \in \mathbb{Z}^+)$

1.= $\sqrt[n]{a} = \frac{r}{s}$ $(r,s)=1$ o.ü. $a = \left(\frac{r}{s}\right)^n = \frac{r^n}{s^n} \Rightarrow r^n = as^n$ olur.

$(r,s)=1$ dir. $s>1$ olsa s nin bir p asal böleni vardır.

$p|s \Rightarrow p|as^n = r^n \Rightarrow p|r$ olur. $p|(r,s)=1$ olduğundan

1'i bölemez. $s>1$ olamaz. $s=1$ dir.

2.= $\frac{r}{s} \in \mathbb{Q} \Rightarrow \left(\frac{r}{s}\right)^n \in \mathbb{Z}$ o.p. $\exists n \in \mathbb{N}$ varsa $\frac{r}{s} \in \mathbb{Z}$ old. gösterin.

$\left(\frac{r}{s}\right)^n = a \in \mathbb{Z} \Rightarrow \frac{r^n}{s^n} = a \Rightarrow r^n = as^n \Rightarrow (r,s)=1$ dir.

$s>1$ olsa s nin bir p asal böleni vardır.

$p|s \Rightarrow p|as^n = r^n \Rightarrow p|(r,s)=1$ dir. p asal olduğundan $s>1$ olması ile çelişir. O halde $s=1$ dir. //

7- $(a,b)=1 \Rightarrow (a+b, a-b)=1$ veya 2 dir.

Çözüm // $(a+b, a-b)=d$ olsun.

$d|(a+b+a-b)=2a$, $d|(a+b-a+b)=2b$ $\Rightarrow$ $d|(2a,2b)=2(a,b)$

$d|2 \Rightarrow d|1 \vee d|2$ //

8- $(a,b)=1 \Rightarrow (a+b, a^2-ab+b^2)=1$ veya 3 olur.

Çözüm // $a^2-ab+b^2 = (a+b)^2-3ab$

$(a,b)=1 \Rightarrow (a+b, a^2-ab+b^2)=d>1$ olsun.

$d|a+b$, $d|a^2-ab+b^2 = (a+b)^2-3ab$

$d|a+b \Rightarrow d|(a+b)^2$ ve $d|(a+b)^2-3ab \Rightarrow d|3ab$

d'nin bir p asal böleni vardır. Çünkü $d>1$

$p|d$; $p|d|3ab \Rightarrow p|3ab \Rightarrow p|a$ veya $p|b$ veya $p|3$

old. göster.

$p|a+b$ old. $p|a$ olsa $p|b$ olur. $p=3$ old. gösterelim. $t>1$ olsa

$t-1>0$ $d=3^t$, $3^t = d|3ab \Rightarrow 3|3^{t-1}|ab$. $3|a \vee 3|b$ olamaz.

Modüler Aritmetik

$m \neq 0$ olsun. $\forall a,b \in \mathbb{Z}$ için ;

$$a \equiv b \pmod m \iff m \mid a-b$$

$(m \in \mathbb{Z})$ " $\equiv$ " $\mathbb{Z}$ de bir denklik bağıntısıdır.

i- $\forall a \in \mathbb{Z},\ m \mid (a-a) = 0 \Rightarrow a \equiv a \pmod m$ (yansıma)

ii- $a \equiv b \pmod m \Rightarrow m \mid a-b \Rightarrow m \mid -(a-b) = (b-a)$

$\Rightarrow b \equiv a \pmod m$ (simetri)

iii- $a \equiv b \pmod m$ ve $b \equiv c \pmod m \Rightarrow m \mid a-b$ ve $m \mid b-c$

$\Rightarrow m \mid (a-b)+(b-c) = a-c$

$\Rightarrow a \equiv c \pmod m$ (geçişme)

$a \equiv b \pmod m \ \vee\ a \equiv b\ (m)$

$a \in \mathbb{Z},\ \overline{a} = \{b \in \mathbb{Z} \mid m \mid a-b\}$

$\{ m=5,\ \overline{13} = \{\dots 8, 13, 18, 23, \dots\}$

Önerme // $a \equiv b\ (m) \iff a$ ve b'nin m ile bölümünden kalanlar eşittir.

İspat // $\Rightarrow$: $m \mid a-b \Rightarrow a-b = mk$, $\exists k \in \mathbb{Z}$

$$\left.\begin{array}{l} a = q_1 m + r_1 \\ b = q_2 m + r_2 \end{array}\right\} \Rightarrow 0 \le r_1, r_2 < m \text{ o.ş. } \exists q_1, q_2, r_1, r_2 \in \mathbb{Z}.$$

$a = mk + b = q_1 m + r_1 \Rightarrow b = (q_1 - k)m + r_1 = q_2 m + r_2$

$q_1 - k = q_2$, $r_1 = r_2$ (kalanlar eşittir.)

$\Leftarrow$: $\left.\begin{array}{l} a = q_1 m + r \\ b = q_2 m + r \end{array}\right\} \Rightarrow (a-b) = (q_1 - q_2)m \Rightarrow m \mid a-b \Rightarrow a \equiv b\ (m)$ dir. //

$\mathbb{Z}/\equiv \ = \mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ (m-tane denklik sınıfı vardır.)

$(\mathbb{Z}, +, \cdot)$ $\mathbb{Z}$ de çarpma işlemine göre tersi yoktur.

$\overline{a} \oplus \overline{b} = \overline{a+b}$, $\overline{a} \odot \overline{b} = \overline{ab}$

Önerme // $a = a_1\ (m)$, $b = b_1\ (m)$ ise

i- $a+b \equiv (a_1 + b_1)\ (m)$

ii- $a.b \equiv (a_1 . b_1)\ (m)$

(O halde tanım kümesinde iki fonksiyonun farklı iki elemanı yoktur. = iyi tanımlıdır.)

İspat // i- $a-a_1 = mk$, $b-b_1 = mt$ $\Rightarrow (a+b)-(a_1+b_1) = m(k+t)$

$\Rightarrow m \mid (a+b)-(a_1+b_1)$

$\Rightarrow (a+b) \equiv (a_1+b_1) \ (m)$

ii- $a = a_1+mk$, $b = b_1+mt$ $\Rightarrow ab = a_1b_1 + m(a_1t+b_1k+mkt)$

$\Rightarrow m \mid ab - a_1b_1$

$\Rightarrow ab \equiv a_1b_1 \ (m)$ //

$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\bar{2} \odot ? = \bar{1}$ 2 nin tersi yok. 3 ve 4'ün de yok.

$\bar{1} \odot \bar{1} = \bar{1}$, $\bar{5} \odot \bar{5} = \bar{1}$ $\bar{1}$ ve $\bar{5}$ in tersi var.

$\mathbb{Z}_m$ deki denklik sınıfları = kalan sınıfı

$\mathbb{Z}_6$ da, $\bar{2} \odot \bar{3} = \bar{0}$ $\bar{3} \odot \bar{8} = \bar{0}$

TANIM: $\bar{a} \neq 0$ olsun. Eğer, $\bar{a}.\bar{b} = \bar{0}$ o.ş $\exists 0 \neq \bar{b} \in \mathbb{Z}_m$ varsa, $\bar{a}$ ya ($\bar{b}$'ye de) sıfır bölen denir.

TANIM: $(a,m) = 1 \Rightarrow \bar{a} \in \mathbb{Z}_m$'ye asal kalan sınıf denir.

$\bar{a_1} = \bar{a}$ asal, $m \mid a-a_1$ $(a_1, m) = 1$?

Önerme // $a \equiv b \ (m) \Rightarrow (a,m) = (b,m)$ dir.

İspat // $m \mid a-b \Rightarrow a = b+mk$, $(a,m) = t$ dersek,

i- $t \mid a$ ve $t \mid m$ $t \mid a-mk = b$

ii- d, b ile m nin ortak böleni ise $d \mid t$ $\{(b,m) = d\}$

$(a,m) = t \Rightarrow aX+my = t$ o.ş. $\exists X, y \in \mathbb{Z}$.

$d \mid b+mk = a$ ve $d \mid aX+my = t \Rightarrow d \mid t$ dir. //

$\mathbb{Z}_m^* :=$ asal kalan sınıfları kümesi

$:= \{\bar{a} \in \mathbb{Z}_m \mid (a,m) = 1\}$

$o(\mathbb{Z}_m^*) = \varphi(m)$

$\varphi(1453) = 1452$.

↓

asal.

Önerme // İki asal kalan sınıfın çarpımı da asaldır.

$\bar{a}, \bar{b} \in \mathbb{Z}_m^* \Rightarrow \overline{ab} \in \mathbb{Z}_m^*$ dir.

İspat // $(a,m)=1=(b,m)$

$(a,m)=1 \Rightarrow ax+my=1$ o.ş. $\exists x,y \in \mathbb{Z}$.

$\Rightarrow b = bax + bmy$ (*) olur. $(ab,m)=k$ diyelim.

(*) eşitliğinden dolayı $k \mid abx+mby = b$

$k \mid b$, $k \mid m \Rightarrow k \mid (b,m)=1 \Rightarrow k=1$ dir.

Önerme // $0 \neq \bar{a} \in \mathbb{Z}_m$ olsun.

$\bar{a}$ sıfır bölendir $\Leftrightarrow$ $\bar{a}$ asal kalan sınıf değildir.

İspat // $\Rightarrow$: $\exists \bar{0} \neq \bar{b} \in \mathbb{Z}$ ki, $\bar{a}.\bar{b} = \bar{0} \Rightarrow m \mid ab$.

$\bar{a}$ asal kalan sınıf olsaydı $(a,m)=1$ olurdu.

$m \mid ab \Rightarrow m \mid b \Rightarrow \bar{b} = \bar{0}$ #

O halde; $\bar{a}$, asal kalan sınıf değildir.

$\Leftarrow$: $\bar{a}$ asal kalan sınıf olmasın. $(a,m)=d>1$

$a = a'd$, $m = m'd$ $\Rightarrow (a',m')=1$ $\exists a', m' \in \mathbb{Z}$.

$\Rightarrow am' = (a'd)m' = a'm$

$\Rightarrow \overline{am'} = \bar{0} \Rightarrow \bar{a}.\bar{m'} = \bar{0}$

$\bar{m'} \neq \bar{0} \Rightarrow \bar{a}$ sıfır bölendir. //

$\overline{m'} = \bar{0} \Rightarrow m' = mk$

$m = mkd \Rightarrow 1 = kd$ olur $d>1$

ANIM: $\bar{0} \neq \bar{a} \in \mathbb{Z}_m$, $\bar{a}.\bar{c} = \bar{1}$ o.ş. $\exists \bar{0} \neq \bar{c} \in \mathbb{Z}_m$ varsa

$\bar{c}$'ye $\bar{a}$ nın tersi denir.

Önerme // $\bar{a} \in \mathbb{Z}_m$ olsun. $\bar{a}$ tersi var $\Leftrightarrow$ $\bar{a}$ asal kalan sınıfıdır.

İspat // $\Rightarrow$: $\bar{a} \in \mathbb{Z}_m$ nin tersi olsun. Yani $\bar{a}.\bar{c} = \bar{1}$ o.ş. $\exists \bar{c} \in \mathbb{Z}_m$ olsun.

$\bar{a}$ nın sıfır bölen olmadığını gösterirsek, $\bar{a}$ asal kalan sınıf olur.

$\exists \bar{0} \neq \bar{b} \in \mathbb{Z}_m$, $\bar{a}.\bar{b} = \bar{0}$ olsun. $\bar{c}(\bar{a}.\bar{b}) = (\bar{c}\bar{a})\bar{b} = \bar{b} = \bar{0}$ #

O halde $\bar{a}$ sıfır bölen değildir.

$\Leftarrow$: $\bar{a}$ bir asal kalan sınıfı olsun. $(a,m)=1$ ve $xa+ym=1$:O.B.T

$\exists x,y \in \mathbb{Z}$ vardır. $xa \equiv 1 \pmod m$ V $\bar{x}.\bar{a} = 1$ olur.

O halde $\bar{a}$ nın tersi vardır.

$\star$ $\mathbb{Z}_6 = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$ tersi vardır. ⇕

$(\bar{6},\bar{1}) = \bar{1}$ $(\bar{6},\bar{5}) = \bar{1}$ $\bar{5}$ ve $\bar{1}$ asal kalan sınıfıdır.

$\mathbb{Z}_{54}$'de kaç tane sıfır bölen eleman var?

$\varphi(54)$ tane asal sınıf vardır. O hariç 53 eleman vardır.

$53 - \varphi(54)$ tane $(53-18=35)$ sıfır bölen vardır.

Sıfırın kendisi, sıfır bölen değildir.

Sonuç: p asal ise $\mathbb{Z}_p$ de sıfırdan farklı her kalan sınıfının tersi vardır. ($\mathbb{Z}_p = \{\bar{0},\bar{1},\dots,\overline{p-1}\}$ $\bar{p}$ ile bu sayılar aralarında asal.)

Teorem: (EULER):

$m \in \mathbb{Z}$, $(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$ veya $\bar{a}^{\varphi(m)} = \bar{1}$ dir.

İspat// $(a,m)=1 \Rightarrow a \in \mathbb{Z}_m^*$

$f : \mathbb{Z}_m^* \to \mathbb{Z}_m^*$, $\bar{x} \to \overline{ax}$ $(\bar{a}.\bar{x} \in \mathbb{Z}_m^*)$ dir. Önceki önermeden.

$f(\bar{x}_1) = f(\bar{x}_2) \Rightarrow \bar{a}\bar{x}_1 = \bar{a}\bar{x}_2 \Rightarrow \bar{a} \in \mathbb{Z}_m^* \Rightarrow \exists \bar{c} \in \mathbb{Z}_m, \exists \bar{a}\bar{c} = \bar{1}$

$\Rightarrow \bar{x}_1 = \bar{x}_2$ dir. $\Rightarrow$ f, 1:1 dir. $\mathbb{Z}_m^* = \{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{\varphi(m)}\}$

olduğundan, sonlu elemanlı bu kümenin 1:1 olması örten olmasını da gerektirir.

O halde f, $\mathbb{Z}_m^*$ ın elemanlarını aralarında değiştireceğinden

$\bar{a}.\mathbb{Z}_m^* = \mathbb{Z}_m^* \Rightarrow (\bar{a}.\bar{a}_1)(\bar{a}.\bar{a}_2)\dots(\bar{a}.\bar{a}_{\varphi(m)}) = \bar{a}_1.\bar{a}_2\dots\bar{a}_{\varphi(m)}$

$= \bar{a}^{\varphi(m)}\, \bar{a}_1.\bar{a}_2\dots\bar{a}_{\varphi(m)}$

$\overline{a_1.a_2\dots a_{\varphi(m)}} = \bar{a}^{\varphi(m)}\, \overline{a_1 a_2 \dots a_{\varphi(m)}}$ (terslerle çarpsak)

$1 = \bar{a}^{\varphi(m)}$ olur.

Sonuç: (FERMAT): Özel olarak $m=p \in \mathbb{Z}$ asal ise $(\forall a \in \mathbb{Z},)$

$p \nmid a \Rightarrow a^{\varphi(p)} \equiv 1 \pmod p$ $(= a^{p-1} \equiv 1 \pmod p)$

TANIM: $aX \equiv b(\text{mod}\, m)$ şeklindeki bir denklem bir bilinmeyenli lineer kongrüans denir.

Önerme // $(a,m)=1 \Rightarrow aX \equiv b(\text{mod}\, m)$ çözümü vardır. (ve bir tek mod m kalan sınıfıdır.)

1. İspat // $(a,m)=1 \Rightarrow ax_0+by_0$ o.ş. $\exists x_0, y_0 \in \mathbb{Z}$

$\Rightarrow b = abx_0 + bmy_0$

$\Rightarrow a(x_0 b) \equiv b(\text{mod}\, m)$ //

$3X \equiv 5(\text{mod}\, 7)$

$(3,7)=1 = 3\cdot 5 + 7(-2)$

$5 = 3(5\cdot 5) + 7(-2)5$

$3(5\cdot 5) \equiv 5(\text{mod}\, 7)$

2. İspat // $(a,m)=1 \Rightarrow \bar{a} \in \mathbb{Z}_m^* : \exists \bar{c} \in \mathbb{Z}_m^*$ için $\bar{a}.\bar{c} = \bar{1}$ dir.

$\bar{a}.\bar{c}.x = x \equiv cb\,(\text{mod}\, m)$ //

$\left.\begin{matrix} ax_1 \equiv b(m) \\ ax_2 \equiv b(m) \end{matrix}\right\} \Rightarrow a(x_1 - x_2) = ax_1 - ax_2 \equiv 0(m) \Rightarrow \bar{a}(\bar{x_1} - \bar{x_2}) = \bar{0}$

$\Rightarrow \bar{x_1} - \bar{x_2} = \bar{0} \Rightarrow \bar{x_1} = \bar{x_2} \Rightarrow x_1 \equiv x_2(m)$ //

Önerme // $aX \equiv b(\text{mod}\, m)$ nin, (a,m)-tane mod m çözümü var $\Leftrightarrow (a,m) \mid b$

İspat // $\Rightarrow$: $ax_0 \equiv b(m) \Rightarrow ax_0 - b = mk$ o.ş. $\exists k \in \mathbb{Z}$,

$(a,m) \mid ax_0 - mk = b \Rightarrow (a,m) \mid b$

$\Leftarrow$: $(a,m)=d \Rightarrow d \mid b$ olsun. $b = dk$, $\exists k \in \mathbb{Z}$.

$\left.\begin{matrix} a = a'd \\ m = m'd \end{matrix}\right\} \Rightarrow (a',m')=1$, $\exists a', m' \in \mathbb{Z}$.

$(a',m')=1 \Rightarrow a'X \equiv k(\text{mod}\, m')$ kongrüansının bir x_0 çözümü vardır.

yani $a'x_0 \equiv k(m') \Rightarrow a'x_0 - k = m't$, $t \in \mathbb{Z}$.

$\Rightarrow da'x_0 - dk = dm't$

$\Rightarrow ax_0 - b = mt$

$\Rightarrow ax_0 \equiv b(\text{mod}\, m)$

$x_0 + tm'$, $\forall t \in \mathbb{Z}$

$t = qd + r$, $0 \le r < d$ o.ş. $\exists q, r \in \mathbb{Z}$.

$x_0 + (qd+r)m' = x_0 + rm' + m'dq = x_0 + rm' + mq \equiv x_0 + rm'(\text{mod}\, m)$