2. Hafta 1. Ders

Monday, September 23, 2019 2:09 PM

Sayılar Kuramına Giriş

Tersinin Olması

- Aralarında asal olması lazım.
  ($3^{-1} \bmod 5$) 3,5 aralarında asal.

Bölme

(bazı) (tam sayı)

$a | b \Rightarrow \exists k \in I, b = k.a$

(a b'yi böler)

Teoremler

① $a|b \wedge a|c \Rightarrow a|(b+c)$

$b = t.a \quad c = s.a$

$b+c = a(t+s) = k.a, \quad k = (t+s)$

② $a|b \Rightarrow \forall c \in I, a|bc$

③ $a|b \wedge b|c \Rightarrow a|c$

Asal Sayılar (prime number)

Asimetrik şifrelemede çok yaygındır.
Şifrelemede çok önemlidir.

$p > 1 \quad \neg(\exists q \,(q \in 2,3 \dots p-1) \wedge q|p)$

Bölme İşlemi

$a \in I$ ise $\exists d \in N^+ \Rightarrow a = d.q + r \wedge 0 \leq r < d$

- negatif de olur.

örnek

$-7 = -3.3 + 1$ olmaz

$-7 = -2.3 - 1$ olur.

OBEB (gcd)

(greater common division)

$gcd(a,b) = 1$ ise aralarında asal olur.

Modül Aritmetiği

$m \in N^+ \quad a,b \in I$

$r = a \pmod m \iff a = q.m + r \wedge 0 < r < m$

- $0 \leq a < m \Rightarrow r = a \wedge q = 0$
- $a = m \Rightarrow r = 0 \wedge q = 1$
- $a = q.m \Rightarrow r = 0 \wedge q = \frac{a}{m}$

Sabit Kuvvetlik

$((a \bmod m) \bmod m) = a \bmod m$

Modül Denkliği

$a \pmod m = b \pmod m = r$

özellikler

$a = b \pmod m \quad c = d \pmod m$ ise;

- $(a+c) \pmod m = (b+d) \pmod m$
- $(a.c) \pmod m = (b.d) \pmod m$

Öklid Algoritması ile OBEB (gcd) hesaplama (Euclid Algorithm)

(ALES için hız)

Yardımcı Teorem

$gcd(a,b) = d \quad gcd(b,r) = d'$

d ile d' aynıdır.

İspat

$d|a \quad d|b \Rightarrow d|a \wedge d|(-q.b) \Rightarrow d|(a - bq) \Rightarrow d|r$

- $gcd(a,b) = cd(a,b) \leq gcd(b,r)$

$d'|b \wedge d'|r \Rightarrow d'|q.b \wedge d'|r \Rightarrow d'|(bq+r) \Rightarrow d'|a$

$gcd(a,b) = ?$

$a = bq_1 + r$

$r_2 = r_1$

FOTO

Base of Algebra

$\alpha = t.252 + s.198 \Rightarrow t, s, \alpha = ? \quad t, s, \alpha \in I$

$18 = 54 - 1.36$
$36 = 198 - 3.54$
$54 = 252 - 1.198$

Euclid Algorithm'den geliyor.

$\Rightarrow 18 = 54 - 1.36$
$= 54 - 1(198 - 3.54)$
$= (-1).198 + 4.54$
$= (-1.198) + 4.(252 - 4.198)$

$18 = 4.252 - 5.198$

(18 → α, 4 → t, −5 → s)

Örnek-1

$3^{-1} \pmod 5 = ?$

$5 = 1.3 + 2$
$3 = 1.2 + 1$
$2 = 1.2 + 0$

$2 = 5 - 1.3$

$1 = 3 - 1.2$
$= 1.3 - 1.(5 - 1.3)$

$1 = (-1).5 + (2).3$

(−1 → $5^{-1} \pmod 3$, 2 → $3^{-1} \pmod 5$)

Örnek-2

$3^{-1} \pmod{12} = ?$

aralarında asal değildir, yani yok.

2. Hafta 2. Ders

Monday, September 23, 2019 3:12 PM

Teoremler (Özellikler)

① $a \cdot c = b c \pmod m \land \gcd(c,m) = 1$

$\boxed{a \equiv b \pmod m}$

② $a \cdot c = b \cdot c \pmod m \land \gcd(c,m) = i$

$\boxed{a \equiv b \pmod k \land (k = m/i)}$

③ $a \cdot x = b \pmod m \land \gcd(a,m) = 1$

$\boxed{x = a^{-1} \cdot b \pmod m}$

④ $a \cdot x = b \pmod m \land \gcd(a,m) = d \land d | b$ ise;

$\boxed{x = \bar{a}' \cdot b' \pmod{m'} \quad a' = \frac{a}{d} \quad b' = \frac{b}{d} \quad m' = \frac{m}{d}}$

Extended Euclid Algorithm

$g = \gcd(n,m) = t \cdot n + u \cdot m$

$\gcd(n,m) = \gcd(r_0, r_1) \dots \gcd(r_m, 0) = r_n$

```
funch gcd(n,m):
  if m=0 then gcd:=n
  else gcd(m, n mod m)
```

```
func gcdext(n,m,g,t,u):
  if m=0 then g=n, t=1, u=0
  else gcdext(m, n mod m, g,t,u)
    s:=u
    u:= t - ⌊n/m⌋·u
    t:=s          (atama)
  end {gcdext}
```

gcdext kodu
doğrusal denklem çözümü
1024 bitte olsun (?)
a'ını bir ver
x'i bul

Örnek

$19 \cdot x = 37 \pmod{141}$

$x = 19^{-1} \cdot 37 \pmod{141}$

$\boxed{x = 52 \cdot 37 = 91 \pmod{141}}$

Euclid Algorithm

$141 = 7 \cdot 19 + 8$
$19 = 2 \cdot 8 + 3$
$8 = 2 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

(1 → aralarında asal)

$8 = 141 - 7 \cdot 19$
$3 = 19 - 2 \cdot 8$
$2 = 8 - 2 \cdot 3$
$1 = 3 - 1 \cdot 2$

$1 = 3 - 1(8 - 2(19 - 2(141 - 7 \cdot 19)))$

$1 = (-7) \cdot 141 + (52) \cdot 19$

(52 → $19^{-1} \pmod{141}$)

Örnek

$14 = 8 \pmod 6$

$7 \cdot 2 = 4 \cdot 2 \pmod 6$

$\boxed{7 = 4 \pmod 3}$

Örnek

$3x = 4 \pmod 7$

$x = 3^{-1} \cdot 4 \pmod 7$

$3^{-1} \cdot 3 \equiv 1 \pmod 7$

$3^{-1} = 5$

$x = 5 \cdot 4 \pmod 7$

$\boxed{x = 4}$

Örnek

$28x = 14 \pmod{21}$

$7 \cdot x \cdot 4 = 7 \cdot 2 \pmod{3 \cdot 7}$ → ④

$4x = 2 \pmod 3$

$2x \cdot 2 = 2 \cdot 1 \pmod 3$ → $\gcd(2,3) = 1$ gider

$2x = 1 \pmod 3$

$x = 2^{-1} \pmod 3$

$\boxed{x = 2}$

Örnek

$55^{-1} \pmod{87} = ?$

f ← gcdext(87,55)

f(55, 87 mod 55 = 32)
f(32,23)
f(23,9)
f(9,5)
f(5,4)
f(4,1) — $g=1$ $t=0$ $u=$
f(1,0) — $g=1$ $t=1$ $u=0$

(sıfır varsa durulur)