Çalışma Notları

Wednesday, November 6, 2019 7:04 PM

Teoremin Olması

- Arabında asal dizileri. $(n \perp m)$
- $\pi(x) = \frac{x}{\ln x}$

Modüler Aritmetik

- $a \equiv r \pmod m \rightarrow a = qm + r$
- $\frac{a}{t} \equiv \frac{b}{t} \pmod{\frac{m}{t}}$

$t = gcd(m, gcd(a,b))$

örnek

$14 \equiv 8 \pmod 6$

$t = gcd(6, \underbrace{gcd(14,8)}_{2}) = 2$

$9 \equiv 4 \pmod 8$

Euclid Algoritması

$gcd(1180, 482) =$

$1180 = 2.482 + 216$

$482 = 2.216 + 50$

$216 = 4.50 + 16$

$50 = 3.16 + 2$

$16 = 8.2 + 0$ → 0'da dur

$gcd(.) = 2$

Doğrusal Denklem Oluşturma

$gcd(n, m) = s.n + t.m$ → $m^{-1} \pmod n$

↓ $n^{-1} \pmod m$

$gcd(252, 198) = ?$ → 18

$252 = 1.198 + 54$

$198 = 3.54 + 36$

$54 = 1.36 + 18$

$36 = 2.18 + 0$

$gcd(.) = 18$

$18 = 54 - 1.36$

$18 = 54 - (198 - 3.54)$

$18 = 4(252 - 198) - 198$

$18 = 4.252 - 5.198$

$1 = 4.14 - 5.11$

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

Extended Euclid Algoritması

$gcdext(89, 55) = \alpha$

$(55, 32)$ → $89 \pmod{55}$

$(32, 23)$

$(23, 9)$

$(9, 5)$

$(5, 4)$

$(4, 1)$

$(1, 0)$

$gcd(.) = 1$

$t_0 = 0$ $s_1 = t_0 - \lfloor n_1/m_1 \rfloor . s_0$

$t_0 = 1$ $s_0 = 0$

$gcd(.)$ $n^{-1} \pmod m$ $m^{-1} \pmod n$

$\alpha = t.n + m.s$

$t_n = s_{n-1}$

$s_n = t_{n-1} - \lfloor n_n / m_n \rfloor . s_{n-1}$

Sözde Asallar

$2^{n-1} \equiv 1 \pmod n \Rightarrow n$ asaldır.

↳ Asallar uyar ama asal olmayanlar da uyabilir.

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

$2^{10} \equiv 1 \pmod{11}$ $2^{30} \equiv 1 \pmod{31}$

$11 \perp 31$

$31.11 = 341$

Modüler Üzeyde Kuvvet

- $x^2 \equiv 1 \pmod{35}$

⇓

$x \equiv \mp 1 \pmod 5$

$x \equiv \mp 1 \pmod 7$

Chinese Remaining Teorem

$x = n_1 \pmod{m_1}$

$x = n_2 \pmod{m_2}$

⋮

$x = n_n \pmod{m_n}$

$M = \prod_{i=1}^{n} m_i$

$x = \sum_{i=0}^{n} n_i . \frac{M}{m_i} \left(\frac{M}{m_i}\right)^{-1} \pmod M$ → m_i'ye göre tersi

Modüler Birim Elemanlar

Toplamada ∃ m → mod uzayı

Kuvvetde ∃ $p-1$ → asal

$a = a + m$

$a^{-1} = a^{p-2}$

Fermat

p: asal $\Rightarrow$ $\boxed{a^{p-1} \equiv 1 \pmod p}$ ∧ $gcd(a,p) = 1$

Euler Fonksiyonu

$\Phi(10) = \{1, 3, 7, 9\}$ → 10'dan küçük 10 ile arabında asal sayılar

$\varphi(10) = 4$

$\varphi(p) = p-1$

$\varphi(p^2) = p.(p-1)$

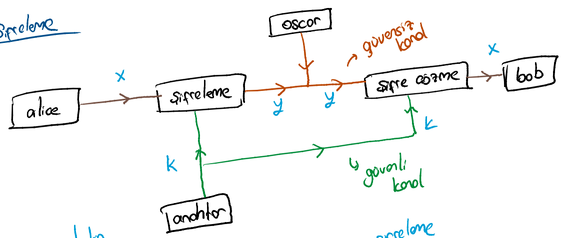
$\varphi(a.b) = \varphi(a).\varphi(b)$

↳ $a \perp b$

Euler-Fermat

$gcd(a, m) = 1 \Rightarrow \boxed{a^{\varphi(m)} \equiv 1 \pmod m}$

Şifreleme



orijinal metin ↖ P: plain text

şifreli metin ↙ C: Cipher Text

K: Key Space ↓ şifreleme anahtarı

E: Encryption ↳ şifreleme

D: Decryption ↳ şifre çözme

Shift Cipher

↳ Kaydırmalı şifreleme → A→B B→C

$y = e_k(x) = (x+k) \pmod m$

$x = e_d(y) = (y-k) \pmod m$

m: Anahtar uzayı