3. Hafta 1

Monday, September 30, 2019 2:19 PM

Ç.L. Kalan Teoremi

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$\vdots$
$x \equiv a_n \pmod{m_n}$
$\} \; x = ?$

$m_1 \perp m_2 \perp m_3 \dots \perp m_n$

$x = (a_1 M_1 y_1 + a_2 M_2 y_2 \dots a_n M_n y_n) \pmod m$

$M_i = \frac{m}{m_i} = \frac{m_1 . m_2 \dots m_i \dots m_n}{m_i}$

Örnek

$x \equiv 9 \pmod{13}$
$x \equiv 8 \pmod{11}$
$x \equiv 7 \pmod{7}$
$\} \; x = ?$

Çözüm: $x = 933$

$x = (a_1 M_1 y_1 + \dots x_3 . M_3 . y_3) \pmod m$

$m = 13 . 11 . 7 = 1001$

$M_1 = 11.7 = 77$ — $M_1 . y_1 \equiv 1 \pmod{m_1}$ — $= 77 \pmod{13} = 12$
$M_2 = 13.7 = 91$ — $M_2 . y_2 \equiv 1 \pmod{m_2}$ — $= 91 \pmod{11} = 3$
$M_3 = 13.11 = 143$ — $M_3 . y_3 \equiv 1 \pmod{m_3}$ — $= 143 \pmod 7 = 3$

aralarında asal

$y_1 = (12)^{-1} \pmod{13} = 12$
$y_2 = 3^{-1} \pmod{11} = 4$
$y_3 = 3^{-1} \pmod 7 = 5$

$13 = 1.12 + 1$
$1 = 11 + 0$

$1 = 1.13 + (-1).12$

$12^{-1} \pmod{13}$

Ç.L. Teoremi kullanılır: RSE Cripto Analiz (Şifre Kırma)

$3^{-1} \pmod{11}$

Örnek

$15x \equiv 21 \pmod{48}$
$166x \equiv 46 \pmod{22}$
$x \equiv 5 \pmod{13}$
$\} \; x = ?$

(1) $15x \equiv 21 \pmod{48}$
$5x \equiv 7 \pmod{16}$ — aralarında asal

$x = 5^{-1} . 7 \pmod{16}$
$x = 13 . 7 \pmod{16}$
$x = 91 \pmod{16}$

$x = 11 \pmod{16}$

(2) $166x \equiv 46 \pmod{22}$
$12x \equiv 2 \pmod{22}$
$6x \equiv 1 \pmod{22}$

$x = 6^{-1} . 1 \pmod{22}$
$x = 2 \pmod{22}$

(3) $x \equiv 5 \pmod{13}$

$x = a_1 M_1 y_1 + \dots + a_3 M_3 y_3 \pmod m$

$M_1 = 22 . 13$
$M_2 = 16 . 13$
$M_3 = 16 . 22$

Çözüm: $x = 2059$

! Asimetrik şifreleme algoritmalarında modüller uzay olarak "asal sayı" kullanılır. (Aralarında asal olduğundan dolayı) !

Örnek

$3^{-1} \pmod{11} = ?$

$11 \pmod 3 = 2$ — gcdext (11, 3, g, t, v)
gcdext (3, 2 ...
$3 \pmod 2 = 1$ — gcdext (2, 1, ...
$2 \pmod 1 = 0$ — gcdext (1, 0, ...
→ $t = 1$, $v = 0$

$g = 1$ → aralarında asaldır, tersi vardır.
1 olmazsa tersi yoktur.
algoritma 0 ise

g	t	v
$g = 1$	$t = -1$	$v = 4$
$g = 1$	$t = 1$	$v = -1$
$g = 1$	$t = 0$	$v = 1$
$g = 1$	$t = 1$	$v = 0$

$v := t - \lfloor \frac{n}{m} \rfloor . v$

$1 = (-1) . 11 + 4 . 3$

$3^{-1} \pmod{11}$

Sözde Asallar

Soru: $2^{n-1} \equiv 1 \pmod m \Rightarrow n =$ asal sayı

↳ Asallar bunu sağlar
↳ Ama asal olmayanlar da sağlayabilir

Örnek

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

$341 = 11 . 31$ asal değil!

$2^{10} = 93.11 + 1 \quad 2^{10} \equiv 1 \pmod{11}$

$2^{340} = (2^5)^{68}$

$(2^{10})^{34}$

$2^5 = 32 \pmod{31}$

$31.11 = 341$

Teorem

$a \equiv 1 \pmod p \Rightarrow a^n \equiv 1 \pmod p$

Kanıt:

$a \equiv 1 \pmod p \Rightarrow p \mid (a - 1)$

$a^{n-1} = (a-1)(a^{n+1} \dots + 1)$

$p \mid (a-1) \Rightarrow p \mid a^{n-1}$

$a^n \equiv 1 \pmod p$

Teorem

$p_1 \mid a \quad p_2 \mid a \quad p_1 \perp p_2 \Rightarrow p_1 . p_2 \mid a$

İspat:

$a = k . p_1 \quad p_2 \mid a \Rightarrow p_2 \mid k . p_1 \Rightarrow p_2 \mid k$

$a = p_1 p_2 . \ell \wedge p_2 . \ell = k$

3. Hafta 2

Monday, September 30, 2019 3:16 PM

Fermat Teoremi

p asal $\wedge$ $\gcd(a,p)=1$

$$a^{p-1} \equiv 1 \pmod p$$

örnek

$a \cdot x \equiv b \pmod p$

örnek

$29^{1000} \pmod{37} = 26$ fermat ile gösterin.

① 37 asal ✓

② $29^{36} \equiv 1 \pmod{37}$

③ $29^{36 \cdot 27 + 28} = 29^{1000}$ (1)

④ $29^{28} \pmod{37} = (-8)^{28} \pmod{37}$

$= (-2^3)^{28} \pmod{37}$

$= 2^{84} \pmod{37}$ $\quad 2^{36} \equiv 1 \pmod{37}$

$= 2^{36 \cdot 2 + 12} \pmod{37} = 2^{12} \pmod{37} = 26$

$2^5 \cdot 2^5 \cdot 2^2$

$-5 \quad -5$

25

$100 \pmod{37} = 26$

Euler Fonksiyon $\varphi(m)$

Tanım: $\forall m \in \mathbb{N}$, $\varphi(m)$: m'den küçük ve m ile aralarında asal olan sayıların sayısı.

$\varphi(10) = 4$

$\Phi_{10} = \{1, 3, 7, 9\}$

$\varphi(p) = p-1$

genel formül ↓

$$\varphi(n) = n \cdot \prod_{p_i \mid n} \left(1 - \frac{1}{p_i}\right)$$

örnek

$\varphi(45) = ?$ $\quad 45 = 5 \cdot 3^2$

① $\varphi(45) = 45 \cdot \left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{3}\right)$

$= 45 \cdot \frac{4}{5} \cdot \frac{2}{3} = 24$

$a \perp b$ ise $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

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

Euler Fermat Teoremi

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

m asal ise "fermat teoremi"ne eşit olur. ($\varphi(p) = p-1$)

örnek

$321^{51} \pmod{49} = 8$

$x = a^{-1} \cdot b \pmod m \Rightarrow x = a^{\varphi(m)-1} \cdot b \pmod m$

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

$a^{\varphi(m)} = a \cdot a^{\varphi(m)-1}$