MARADÉKOS OSZTÁS TÉTELE:

$\forall\ a,b \in \mathbb{Z},\ b>0$ számpárhoz $\exists!\ q,r \in \mathbb{Z}$ számpár, melyre

$$a = bq + r \quad \text{és} \quad 0 \le r < b$$

BIZONYÍTÁS: Létezés biz.: válasszuk úgy q-t, hogy

$$qb \le a < (q+1)b \longrightarrow r = a - qb.$$

Egyértelműség biz: tfh. $\exists$ egy $r'q'$ páros is, melyre

$$a = q'b + r' \quad \text{és} \quad 0 \le r' < b$$

Ekkor $\quad qb + r = q'b + r'$

$$(q-q')b = r' - r$$

$\underline{0 \le r < b}$ és $0 \le r' < b$

így $r' - r < b$

ugyanakkor a baloldal miatt

$r' - r$ osztható b-vel

$\longrightarrow r' - r = 0$

$\Rightarrow r = r',\ q = q'$

KÖZÖS OSZTÓ: Egy a szám b és c közös osztója, ha $a|b$ és $a|c$

LEGNAGYOBB KÖZÖS OSZTÓ: ha b és c számok közül legalább az egyik $\neq 0$, akkor lnko-juk a közös osztóik közül a legnagyobb. Jelölés $(b;c)$

RELATÍV PRÍMEK: a és b számok, ha $(a,b) = 1$.

EUKLIDESZI ALGORITMUS:

Adott b és $c>0$ $\mathbb{Z}$ számokra alkalmazzuk a maradékos osztást a következőképpen:

$$\begin{aligned}
b &= c q_1 + r_1 & 0 &\le r_1 < c \\
c &= r_1 q_2 + r_2 & 0 &\le r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 & 0 &\le r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n & 0 &\le r_{n} < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0 & &\underline{r_{n+1} = 0}
\end{aligned}$$

Ekkor a b és c számok lnko-ja r_n.

BIZONYÍTÁS: – $r_1 > r_2 > r_3 \dots,\ r_i \in \mathbb{Z} \rightarrow$ előbb-utóbb $r_{n+1} = 0$

– b és c közös osztói ugyanazok, mint c és r_1-é az 1. egyenlet szerint:

$$b = cq_1 + r_1$$

$\rightarrow x|b$ és $x|c \rightarrow x|r_1$ és

$y|c$ és $y|r_1 \rightarrow y|b$

$$\rightarrow (b,c) = (c,r_1) = (r_1,r_2) = \dots = (r_n, r_{n+1}=0) = r_n$$

$\forall\, b, c \in \mathbb{Z}$, melyek közül legalább az egyik $\neq 0$, $\exists\, s, t \in \mathbb{Z}$, hogy

$$(b, c) = sb + tc$$

BIZONYÍTÁS: Euklidesz-alg:

$$r_1 = b - q_1 c = b + (-q_1) c$$

$$r_2 = c - q_2 r_1 = c - q_2 b + q_2 q_1 c = \underbrace{-q_2}_{\tilde{s}} b + \underbrace{(1 + q_1 q_2)}_{\tilde{t}} c$$

$$\vdots$$

QED $\quad r_n = sb + tc$ valami számpárossal.

MODULO N INVERZ: a mod. N inverze b-nek, ha $ab \equiv 1 \mod N$

MODULO N INVERZ TÉTEL:

1.) Egy $a \in \mathbb{Z}$ szám modulo N inverze akkor és csak akkor létezik, ha

$$(a, N) = 1$$

2.) Ha létezik inverz, az az N-nél kisebb $\mathbb{Z}^+$ számok között egyértelmű

BIZONYÍTÁS: 1.) Ha $\exists\, b \in \mathbb{Z}^+$, melyre $ab \equiv 1 \mod N$

$ab - qN = 1$ valamely q-ra

$$(a, N)\left[\frac{a}{(a,N)} b - \frac{N}{(a,N)} q\right) = 1$$

azaz (a, N) osztója 1-nek és $\in \mathbb{Z}^+$

$\rightarrow (a, N) = 1$

(csak akkor): ha $(a, N) = 1$ a fenti tétel szerint

$$(a, N) = sa + tN = 1$$

$b = s$ választással (b az inverz)

$ba + tN = 1 \rightarrow ba = -tN + 1$

azaz $ba \equiv 1 \mod N$

2.) Legyen $b \neq b'$ $0 < b, b' < N$ $\in \mathbb{Z}^+$ számok, melyekre

$$ab \equiv ab' \equiv 1 \mod N$$

$$a(b - b') \equiv 0 \mod N$$

QED $\rightarrow$ N osztója $b - b'$-nek, de $\forall 2b < N$ ~~$\rightarrow b - b' = 0$~~ ellentmondás.

FERMAT-TÉTEL:

Ha egy $c \in \mathbb{Z}$ nem osztható N prímmel, akkor

$$c^{N-1} \equiv 1 \mod N$$

BIZONYÍTÁS: $\forall c \in \mathbb{Z}$-re a $c, 2c, 3c, \ldots, (N-1)c$ számok különbözőek mod N

ugyanis ha $ic \equiv jc \mod N$ $i \neq j$ fennállna $0 < i, j < N$

$(i-j)c = qN$ lenne, c nem osztható N-nel, $i-j$-nek kellene oszthatónak lennie, de $0 < i, j < N$ miatt ↯

$\rightarrow$ $c, 2c, 3c, \dots, (N-1)c$ ha mod N vesszük, az
$1, 2, 3, \dots, N-1$ számok permutációját adják

Ha $i = 1, 2, \dots, n$-re $a_i \equiv b_i \mod N \rightarrow a_1 \cdot a_2 \cdot \dots \cdot a_n \equiv b_1 \cdot b_2 \cdot \dots \cdot b_n \mod N$

ebből: $1 \cdot 2 \cdot 3 \cdot \dots \cdot (N-1) \equiv c \cdot 2c \cdot 3c \cdot \dots \cdot (N-1)c$

avagy

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (N-1) \equiv c^{N-1} \cdot (1 \cdot 2 \cdot 3 \cdot \dots \cdot (N-1)) \mod N$$

$$\rightarrow \quad 1 \equiv c^{N-1} \mod N$$

QED

<u>ÁLTALÁNOSÍTOTT FERMAT-TÉTEL:</u> Legyen $N_1 N_2$ különböző prímek és $(a, N_1, N_2) = 1$, ekkor ~~a, N_1~~

$$a^{(N_1-1)(N_2-1)} \equiv 1 \mod N_1 N_2$$

BIZONYÍTÁS: $(a, N_1, N_2) = 1 \rightarrow (a, N_1) = 1$ és $(a, N_2) = 1$

Mivel N_1 és N_2 prím, $a^{N_1-1} \not\equiv 0 \mod N_2$ és $a^{N_2-1} \not\equiv 0 \mod N_1$

így a Fermat-tétel szerint

$$\left.\begin{aligned} \left(a^{N_1-1}\right)^{N_2-1} &\equiv 1 \mod N_2 \\ \left(a^{N_2-1}\right)^{N_1-1} &\equiv 1 \mod N_1 \end{aligned}\right\} \text{QED}$$

$c \equiv 1 \mod N_1$
$c \equiv 1 \mod N_2$
$c - 1 \equiv 0 \mod N_1$
$c - 1 \equiv 0 \mod N_2$
$\rightarrow N_1$ és N_2 is osztója $c - 1$-nek.

QED

ÁLTALÁNOSÍTOTT FERMAT TÉTEL 2.:

Legyen $M = N_1 \cdot N_2 \cdot \dots \cdot N_n$ N_i prímekkel és $(a, M) = 1$

$$a^{\phi(M)} \equiv 1 \mod M$$

ahol $\phi(M) = (N_1 - 1)(N_2 - 1) \cdot \dots \cdot (N_n - 1) = \phi(N_1, N_2, \dots, N_n)$

EULER FÜGGVÉNY: $\phi(N_1, N_2, \dots, N_n) = (N_1 - 1)(N_2 - 1) \cdot \dots \cdot (N_n - 1)$

RSA-algoritmus

1.) Válasszunk 2 db nagy prímszámot: p_1 és p_2

2.) Számítsuk ki az Euler-függvényt $\phi(p_1 p_2) = (p_1-1)(p_1-2)$ szorzatukat

$m = p_1 p_2$

3.) Válasszunk egy $1 \le e < \phi(m)$ egészet, melyre

$(\phi(m), e) = 1$

(véletlenszerű választás)

4.) Számítsuk ki e inverzét mod $\phi(m)$

$d = e^{-1} \bmod \phi(m)$ (ez létezik az mod N inverz tétel miatt)

5.) Az m és e értékeket nyilvánosságra hozzuk, p_1 és p_2 titokban marad

$\underline{k}^P = (m, e)$

$\underline{k}^S = (d, p_1, p_2)$

6.) $1 \le x < m$ nyílt üzenetre a titkosító eljárás $1 \le y < m$ rejtett üzenetet ad, melyre

$$\boxed{\begin{aligned} y &= x^e \bmod m \\ x &= y^d \bmod m \end{aligned}} \qquad x, y \in \mathbb{N}$$

TÉTEL: az $y \equiv x^e \bmod m$ és az $x \equiv y^d \bmod m$ egymás inverz műveletei

BIZONYÍTÁS: $d \cdot e = q \cdot \phi(m) + 1$ mivel $d = e^{-1} \bmod \phi(m)$

$$y^d \equiv (x^e)^d \equiv x^{ed} \equiv x^{q\phi(m)+1} \bmod m$$

a) $(x, m) = 1$ esetén a Fermat-tétel ált. 2. miatt

$x^{\phi(m)} \equiv 1 \bmod m$ QED

b) $(x, m) > 1$ esetén

mivel $m = p_1 p_2$ $x < m$ vagy $p_1 | x$ vagy $p_2 | x$

Legyen $p_1 | x \longrightarrow x = w \cdot p_1$ $(w, m) = 1$

$$x^{q\phi(m)+1} \equiv \underbrace{w^{q(\phi(m))+1}}_{\text{Fermat ált 2 miatt}} \cdot p_1^{q\phi(m)+1} \bmod m$$

$\left.\begin{aligned} w^{q\phi(m)} &\equiv 1 \\ w^{q\phi(m)+1} &\equiv w \end{aligned}\right\} \bmod m$

$$p_1^{q\phi(m)+1} \equiv p_1 \left(p_1^{q\phi(m)}\right) \equiv$$

$$\equiv p_1 \underbrace{\left(p_1^{p_2-1}\right)^{q(p_1-1)}}_{\text{Fermat miatt } 1} \equiv$$

$$\equiv p_1 \bmod p_2$$

és nyilván $p_1^{q(\phi(m))+1} \equiv 0 \mod p_1$

$$\begin{cases} p_1^{q\phi(m)+1} - p_1 = 0 \mod p_1 \\ p_1^{q\phi(m)+1} - p_1 = 0 \mod p_2 \end{cases}$$

$$p_1^{q\phi(m)+1} - p_1 = 0 \mod p_1 p_2 = m$$

$$p_1^{q\phi(m)+1} = p_1 \mod m$$

$$x^{q\phi(m)+1} = w \cdot p_1 = x \mod m$$

pl.

Egyirányú függvény:

Egy invertálható f fv-t egyirányúnak nevezünk, ha értelmezési tartományának tetszőleges x elemére $f(x)$ kiszámítása egyszerű, ám gyakorlatilag irreálisan nehéz egy tetszőleges y értékkészletbeli elemhez az $y = f(x)$-beli x kiszámítása.

RSA esetén $y = x^e$ kiszámítása (mod m) egyszerű, míg $x = y^d$ kiszámítása csak d és m ismeretében könnyű,

Csapda típusú egyirányú függvény

Olyan egyirányú fv, melynek dekódolása ugyan irreálisan nehéz, de egy tiz. információ birtokában könnyű.

PRÍMEK előállítása

Véletlen prímválasztáshoz az RSA algoritmusban.

CSEBISEV-tétel (Pafnutyij Lvovics Csebisev)(1821-1894)

- Legyen $\Pi(n)$ az $n \in \mathbb{Z}^+$-nál kisebb prímek száma

$\Pi(n) \approx \frac{n}{\ln n}$

A biztonságos nagyságrend RSA-algoritmusban $p_1 \cdot p_2 \sim 10^{300}$

$p_i \approx 10^{150} \approx 2^{500}$

Válasszunk egy s számot, ami 502 bites pl. Mekkora esélye van annak, hogy prímet választunk.

$$\frac{\Pi(2^{502}) - \Pi(2^{501})}{2^{502} - 2^{501}} \approx \frac{2^{501} \frac{1}{501 \ln 2}}{2^{501}} \approx \frac{1}{350}.$$

Csak páratlanok között keresünk $p \approx \frac{1}{175}$

Hogyan döntsük el, hogy prímek-e:

s-et választottuk.

legyen $2 \leq b < s$ alap $b \in \mathbb{Z}$

Ha s prím, akkor $b^{s-1} = 1 \mod s$ $\rightarrow$ ha $b^{s-1} \neq 1$, akkor nem prím.

Ha $b^{s-1} = 1 \mod s$, akkor s lehet prím.

ezt r db kül. bázisra megism, vr, hogy prímünk van.