DMat-18

Lad $a, b \in \mathbb{Z}$ (enten $a \neq 0$ eller $b \neq 0$).
Så findes der $s, t \in \mathbb{Z}$ som opfylder:

$$\mathrm{gcd}(a, b) = s \cdot a + t \cdot b.$$

(s og t er *ikke* entydige, f.eks.:

$$(s + b) \cdot a + (t - a) \cdot b = s \cdot a + t \cdot b.)$$

Euklids udvidede algoritme

Lad $a, b \in \mathbb{Z}^+$.

$a = q_1 b + r_1$

$$r_1 = a - q_1 \cdot b$$

$b = q_2 r_1 + r_2$

$$r_2 = b - q_2 r_1 = -q_2 \cdot a + (1 + q_1 q_2) \cdot b$$

$r_1 = q_3 r_2 + r_3$

$$r_3 = r_1 - q_3 r_2 = (1 + q_2 q_3) \cdot a + (-q_1 - q_3 - q_1 q_2 q_3) \cdot b$$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$

$$r_n = s \cdot a + t \cdot b$$

$r_{n-1} = q_{n+1} r_n$

Så er $\gcd(a, b) = r_n = sa + tb$

Lad $m \in \mathbb{Z}^+$, og $a, \overline{a} \in \mathbf{Z}$.

$\overline{a}$ siges at være invers til a modulo m hvis

$$a\overline{a} \equiv 1 \pmod{m}.$$

(Så er a også invers til $\overline{a}$ modulo m.)

a har en invers modulo m hvis og kun hvis $\gcd(m, a) = 1$.

Hvis $\gcd(m, a) = 1 = sm + ta$ (fra Euklids udvidede algoritme) så
er t en invers til a modulo m og
$\overline{a}$ er invers til a hvis og kun hvis $\overline{a} \equiv t \pmod{m}$.

Kinesisk restsætning
Lad $m_1, m_2, \ldots m_n \in \mathbb{Z}^+$ så gcd$(m_i, m_j) = 1$ når $i \neq j$.
Lad $a_1, a_2, \ldots a_n \in \mathbb{Z}$.
Så findes der $x \in \mathbb{Z}$ som opfylder

$$x \equiv a_1 \pmod{m_1},$$

$$x \equiv a_2 \pmod{m_2},$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}.$$

Løsningen x kan beregnes som

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n,$$

hvor $M_i = \frac{m}{m_i}$, $m = m_1 m_2 \cdots m_n$ og y_i er invers til M_i modulo m_i, for $i = 1, 2, \ldots, n$.

Løsningen x er entydig modulo m. D.v.s. et tal x er løsning hvis og kun hvis

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n \pmod{m}$$

Kinesisk restsætning, $n = 2$
Lad $m_1, m_2 \in \mathbf{Z}^+$ så gcd$(m_1, m_2) = 1$.
Lad $a_1, a_2 \in \mathbb{Z}$.
Så findes der $x \in \mathbb{Z}$ som opfylder

$$x \equiv a_1 \pmod{m_1},$$

$$x \equiv a_2 \pmod{m_2}.$$

Løsningen x kan beregnes som

$$x = a_1 m_2 y_1 + a_2 m_1 y_2,$$

hvor $1 = y_2 m_1 + y_1 m_2$ (som fås fra Euklids udvidede algoritme).

Løsningen x er entydig modulo $m = m_1 m_2$. D.v.s. et tal x er løsning hvis og kun hvis

$$x \equiv a_1 m_2 y_1 + a_2 m_1 y_2 \pmod{m}$$

Fermats sætning

Hvis p er et primtal og $a \in \mathbb{Z}$, $p \nmid a$ så er

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

Hvis $a^{n-1} \not\equiv 1 \pmod{n}$ og $n \nmid a$ så er n ikke et primtal.

$a^{n-1} \mod n$ beregnes ved "modular exponentiation", d.v.s. ved gentagen anvendelse af:

$$a^{2k} \mod n = (a^k \mod n)^2 \mod n$$

$$a^{2k+1} \mod n = ((a^k \mod n)^2 \cdot a) \mod n$$

RSA kryptering

A vil sende besked M til B, $M \in \mathbb{N}$.

B vælger primtal p og q og $e > 0$ så $\gcd((p-1)(q-1), e) = 1$.
B finder $d > 0$ så $de \equiv 1 \pmod{(p-1)(q-1)}$. D.v.s. d er invers til e modulo $(p-1)(q-1)$.
B sender $n = pq$ og e til A.

Vi antager $0 \leq M < n$ ellers deles beskeden i mindre dele.

A udregner $C = M^e \mod n$ ved "modular exponentiation" og sender C til B.

B udregner $C^d \mod n$ da dette tal er lig med M.

B bruger også modular exponentiation, men kan eventuelt udregne

$$C^d \mod p \quad \text{og} \quad C^d \mod q,$$

og bruge den kinesiske restsætning.