DMat-17

$a, b \in \mathbb{Z}$, $a \neq 0$.
Vi siger at a går op i b, skrives $a \mid b$,
hvis der findes $c \in \mathbb{Z}$ så $b = ac$

$a, b, c \in \mathbb{Z}$
$a \mid b \ \wedge \ a \mid c \ \Rightarrow \ a \mid nb + mc$, hvor $n, m \in \mathbb{Z}$.
$a \mid b \ \wedge \ b \mid c \ \Rightarrow \ a \mid c$.

$a, d \in \mathbb{Z},\ d \geq 1$.
Der findes entydige tal $q, r \in \mathbb{Z}$ så

$$a = dq + r, \quad 0 \leq r < d.$$

Vi skriver: $r = a \mod d$.

Hvis $d \geq 1$: $\quad d \mid a \Leftrightarrow a \mod d = 0$.

$m \in \mathbb{Z}^+,\ a, b \in \mathbb{Z}$.
a er kongruent med b modulo m, skrives $a \equiv b \pmod{m}$,
hvis $m \mid a - b$.

$a \equiv b \pmod{m} \Leftrightarrow (a \mod m) = (b \mod m)$.

I udregninger modulo m kan et tal a erstattes af (f.eks.) $a \mod m$.

(Dette gælder ikke tal i en eksponent.)

$p \in \mathbb{Z}, p \geq 2$ er et primtal hvis 1 og p er de eneste positive hele tal, der går op i p
Hvis p ikke er et primtal så siger vi at at p er et sammensat tal.

Ethvert helt tal n, $n \geq 2$ er et (produkt af) primtal.

Der findes uendeligt mange primtal.

Det største primtal man kender er $2^{43112609} - 1$.

$a, b \in \mathbb{Z}$. ($a \neq 0$ eller $b \neq 0$)
Største fælles divisor af a og $b = \gcd(a, b)$
er det største tal der går op i både a og b

Hvis

$$a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \text{ og } b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n},$$

hvor $e_i \geq 0$ og $f_i \geq 0$ er hele tal for alle i så er

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_n^{\min(e_n, f_n)}.$$

$a, b \in \mathbb{Z}^+$
Det mindste fælles multiplum af a og $b = \mathrm{lcm}(a, b)$
er det mindste tal $m \in \mathbb{Z}^+$ som opfylder $a \mid m$ og $b \mid m$.

Hvis

$$a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \text{ og } b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n},$$

hvor $e_i \geq 0$ og $f_i \geq 0$ er hele tal for alle i så er

$$\mathrm{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_n^{\max(e_n, f_n)}.$$

$\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$

Pseudo-tilfældige tal.

$m, a \in \mathbb{Z},\ 2 \leq a < m.$

En talfølge $x_0, x_1, x_2, \ldots$ defineres rekursivt ved
Basis: $x_0 = \ldots$ et tal som opfylder $0 < x_0 < m$
Rekursion: for $n \geq 0$ er $x_{n+1} = (a \cdot x_n) \mod m$.

(Så er $x_n = (a^n \cdot x_0) \mod m$ for alle $n \geq 0$.)

Ønskes:

$$\{x_0, x_1, \ldots, x_{m-2}\} = \{1, 2, \ldots, m-1\}, \quad x_{m-1} = x_0.$$

Dette kræver at m er et primtal: hvis $m = ab$ så er enten alle eller ingen x_i multiplum af a.

Eksempel.

$m = 2^{31} - 1 = 2147483647$ et primtal.
$a = 7^5 = 16807$

$$
\begin{aligned}
x_0 &= 1000000000 \\
x_1 &= 792978578 \\
x_2 &= 307447164 \\
x_3 &= 418830666 \\
x_4 &= 1983092243 \\
x_5 &= 885126661 \\
x_6 &= 704568658 \\
x_7 &= 460605448 \\
x_8 &= 1864700748
\end{aligned}
$$