Théorème fondamental de l'arithmétique

Tout entier $n > 0$ est un produit de nombres premiers

$$n = p_1^{a_1} \times \cdots \times p_n^{a_n}, \quad p_i \text{ premier}, \quad a_i > 0$$

Et ce produit est unique (à un ordre près).

Exemples :

$72 = 2^3 3^2$, $25 = 5^2$, $100 = 5^2 2^2$, $39375 = 7^1 3^2 5^4$

Application: Preuve que $\log_5 7$ est irrationnel

Supposons que

$$\log_5 7 = \frac{p}{q}, \quad \text{où} \quad \frac{p}{q} \text{ est irréductible}$$

$$5^{(p/q)} = 7 \equiv 5^p = 7^q$$

Contradiction!, car 5^p doit être un nombre différent de 7^q.

Cryptographie à clé publique (RSA)

- Alice publie deux nombres entiers n et e.
- Bob brise son message M en nombres $m_i < n$.
- Bob publie les valeurs $c_i = m_i^e \bmod n$.
- Alice sait que $n = pq$, p et q premiers, et connaît un d tel que $de \equiv 1 \bmod (p-1)(q-1)$.
- Alice décode le message en calculant $c_i^d \bmod n$.

Pourquoi $c_i^d \equiv m_i \bmod n$?

On a

$$\begin{aligned} c_i^d \equiv (m_i^e)^d \equiv m_i^{de} \equiv m_i^{k(p-1)(q-1)+1} \\ \equiv m_i(m_i^{(p-1)(q-1)})^k \bmod n \end{aligned}$$

$$\equiv m_i(m_i^{(p-1)(q-1)})^k \bmod p \equiv m_i(m_i^{(p-1)(q-1)})^k \bmod q$$

Par le petit théorème de Fermat

(on a $\text{pgcd}(m_i, p) = \text{pgcd}(m_i, q) = 1$)

$$m_i^{(p-1)} \equiv 1 \bmod p \quad \text{et} \quad m_i^{(q-1)} \equiv 1 \bmod q$$

Par substitution, on obtient

$$c_i^d \equiv m_i(1)^{k(q-1)} \equiv m_i \bmod p$$

De même,

$$c_i^d \equiv m_i(1)^{k(p-1)} \equiv m_i \bmod q$$

En combinant ces deux équivalences et le fait que $\text{pgcd}(p, q) = 1$, on obtient

$$\boxed{c_i^d \equiv m_i(1)^k \pmod{pq} \equiv m_i \bmod n}$$

Le groupe multiplicatif modulo 7

La table de multiplication

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	$\boxed{1}$	2	3	4	5	6
2	0	2	4	6	$\boxed{1}$	3	5
3	0	3	6	2	5	$\boxed{1}$	4
4	0	4	$\boxed{1}$	5	2	6	3
5	0	5	3	$\boxed{1}$	6	4	2
6	0	6	5	4	3	2	$\boxed{1}$

La table d'addition

	0	1	2	3	4	5	6
0	$\boxed{0}$	1	2	3	4	5	6
1	1	2	3	4	5	6	$\boxed{0}$
2	2	3	4	5	6	$\boxed{0}$	1
3	3	4	5	6	$\boxed{0}$	1	2
4	4	5	6	$\boxed{0}$	1	2	3
5	5	6	$\boxed{0}$	1	2	3	4
6	6	$\boxed{0}$	1	2	3	4	5

Débordement arithmétique sur ordinateur

Supposons des registres de 32 bits. Les calculs sur les entiers positifs se font modulo 2^{32}.

Si $xy - zw < 2^{32}$, tout débordement intermédiaire ne produit pas d'erreur de calcul.

Exemple:

$$235165 \times 176325 - 96474 \times 429807 = 268107$$
$$235165 \times 176325 = 41,465,468,625$$
$$96474 \times 429807 = 41,465,200,518$$

mais $41,465,468,625 > 2^{32}$ ainsi le calcul effectué est plutôt

$$41,465,468,625 \bmod 2^{32} - 41,465,200,518 \bmod 2^{32}$$
$$2,810,762,961 - 2,810,494,854 = 268107$$

Ce qui est le bon résultat.

Si on sait que le résultat est entre 0 et m alors tous les calculs peuvent être faits modulo m.

Propriétés

$$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$
$$(a+b) \bmod m = ((a \bmod m)+(a \bmod m)) \bmod m$$
$$(a^b) \bmod m = ((a \bmod m)^b) \bmod m$$

Matrice

Une matrice $n \times m$ est formée de $n \times m$ éléments disposés en n **lignes** et m **colonnes**.

$$A_{n\times m} = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} = [a_{ij}]_{nm}$$

Pour $n = m$, on a une matrice carrée.

La matrice identitée $n \times m$

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Opérations

Addition

$$A_{nm} + B_{nm} = [a_{ij} + b_{ij}]_{nm}$$

L'addition est associative et commutative :

$A + (B + C) = (A + B) + C$, $A + B = B + A$.

Multiplication

$$A_{np} \times B_{pm} = [c_{ij}]_{nm} = [\sum_{k=1}^{p} a_{ik} b_{kj}]_{nm}$$

La multiplication est associative mais **pas** commutative.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$

mais

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ea + fc & eb + fd \\ ga + hc & gb + hd \end{pmatrix}$$