Arithmétique modulaire

1 Définition

On travaille souvent avec la division par un nombre fixé. Deux exemples :
- Multiples de 7 jours ne changent pas le jour de la semaine. Seulement le reste dans la division par 7 est important. Par exemple, si c'est lundi dans $100 = 98 + 2$ jours il va être mercredi.
- Multiples de 24 heures ne changent pas l'heure. Par exemple, si c'est 15 heures, dans $100 = 96 + 4$ heures il va être 19 heures.
- Multiples de 10^n ne changent pas les derniers n chiffres. Pour cela seulement le reste dans la division par 10^n est important. Par exemple, $531 + 971 = \ldots 02$.

En général, le nombre fixe pour lequel on divise est appelé *modulus*, il s'agit d'un nombre naturel $m \geqslant 2$. Les restes modulo m se répètent de façon cyclique de 0 jusqu'à $m - 1$.

Nombre	...	-4	-3	-2	-1	0	1	2	3	4	...
Rest dans la division par 3	...	2	0	1	2	0	1	2	0	1	...

Si un nombre entier a laisse un quotient q et un reste r par la division de m, alors pour tout $t \in \mathbb{Z}$ le nombre $a + tm$ a le même reste r :

$$a = qm + r \qquad \Rightarrow \qquad a + tm = \underbrace{(q + t)}_{quotient} m + \underbrace{r}_{rest}$$

On écrit **<u>dans cette note</u>** a_m pour le reste de a modulo m.

2 Arithmétique

C'est remarquable que les restes modulo m sont compatibles avec la somme et le produit : le reste pour la somme de deux nombres est le même que celui de la somme de deux restes, et du même pour la multiplication :

$$(a + b)_m = \Big((a_m) + (b_m)\Big)_m$$

$$(a \cdot b)_m = \Big((a_m) \cdot (b_m)\Big)_m$$

Par exemple (modulo 10 il s'agit de voir le dernier chiffre) :

$$(3319 + 3326)_{10} = (3319_{10} + 3326_{10})_{10} = (9 + 6)_{10} = 5$$

$$(3319 \cdot 3326)_{10} = (9 \cdot 6)_{10} = 4$$

Travailler avec le dernier chiffre (modulo 10) est une méthode pour vérifier (partiellement) un calcul. Aussi regarder la parité des nombres peut être utilisé comme méthode, et il s'agit de travailler le modulo 2, par exemple on voit bien que la somme de deux nombres impairs est pairs :

$$(1+1)_2 = 2_2 = 0$$

• Gràce à l'arithmétique modulaire on peut vite calculer le dernier chiffre d'une puissance, car le dernier chiffre se répète de façon cyclique avec l'exposant, par exemple :

$$2^n \in \{2, 4, 8, 16, 32, 64, 128, 256, \ldots\}$$

donc le dernier chiffre de 2^{102} est 4.

3 Comparaison des restes

Si on connait le reste modulo 24 d'un nombre, on connait aussi le reste modulo 12, par exemple $(23 + 24t)_{12} = 11$ pour tout $t \in \mathbb{Z}$. Par contre, si on connait le reste modulo 12 on a plusieurs possibilités pour le reste modulo 24 : par exemple $(11 + 12t)_{24}$ peut être 11 ou 23.

Certains reste sont dépendants, certains indépendants. Par exemple, les reste modulo 3 et modulo 4 sont indépendants, car toutes combinaisons sont possibles :

Rest modulo 12	0	1	2	3	4	5	6	7	8	9	10	11
Rest modulo 3	0	1	2	0	1	2	0	1	2	0	1	2
Rest modulo 4	0	1	2	3	0	1	2	3	0	1	2	3

Par contre le reste modulo 6 et 8 ne sont pas toujours compatibles : on n'as pas un nombre qui donne reste 4 dans la division par 6 et 3 dans la division par 8 (car $4_2 \neq 3_2$, où $2 = PGCD(6, 8)$).

Théorème Chinois de Restes : Si $m_1, \ldots, m_s$ sont des nombres $\geqslant 2$ qui sont premiers entre eux *deux à deux* et $r_1, \ldots, r_s$ sont des nombres avec $0 \leqslant r_i < m_i$ il existe un nombre a qui a comme reste r_i dans la division par m_i pour tout i. Toutes solutions sont alors les nombres de la forme $a + t \cdot m_1 \cdots m_s$ avec t entier.

Exemple : Les reste modulo 6 et 7 sont toujours compatibles. Si on cherche un nombre de la forme $4 + 6x$ et $3 + 7y$, on peut résoudre l'équation diophantienne $4 + 6x = 3 + 7y$ pour le trouver (mais souvent diviner est plus vite !) Les nombres qui donnent un reste 4 dans la division par 6 et un reste 3 dans la division par 7 sont $\{10 + t42 \; t \in \mathbb{Z}\}$.