L'arithmétique modulaire

Définition du modulo

Dans cette section, on cherche premièrement à déterminer si un nombre est divisible par un autre. Si c'est facile de savoir si le nombre est divisible par 2, c'est moins facile de savoir s'il est divisible par 7. Par exemple, comment savoir si 7965 est divisible par les nombres premiers 7, 11, 13, 17…

Bien qu'il existe des trucs pour plusieurs cas, nous allons utiliser une méthode plus générale qui fonctionne à tous coups : l'arithmétique modulaire

Voici à quoi ressemble la notation

$$25 \equiv 1 \pmod 3$$

Cela signifie que quand on divise 25 par 3, le reste de la division est 1

De façon générale

$$A \equiv R \pmod m$$

Signifie que quand on divise *A* par *m*, le reste de la division est *R*.

Évidemment, si un nombre *m* est un diviseur de *A*, il n'y aura pas de reste et on aura

$$A \equiv 0 \pmod m$$

Ainsi, si on veut savoir si 7 est un facteur de 7965, on cherche le reste de la division de 7965 par 7, c'est-à-dire *x* dans l'équation

$$7965 \equiv x \pmod 7$$

Si x = 0, cela voudra dire que 7 est un facteur de 7965.

En fait, cette notation est un peu plus générale que cela. Par exemple, on peut écrire

$$15 \equiv 8 \pmod 7$$

Puisque 15 et 8 ont les mêmes restes quand on les divise par 7. On dit alors que 15 et 8 sont congruents en mode *m*.

Voici les propriétés du module

1) $a + b \equiv a \pmod m + b \pmod m$

2) $ab \equiv a \pmod m \cdot b \pmod m$

Si $a \equiv b \pmod m$, alors

3) $a + c \equiv b + c \pmod m$

4) $a - c \equiv b - c \pmod m$

5) $a \cdot c \equiv b \cdot c \pmod m$

6) $a^c \equiv b^c \pmod m$

On retrouve les preuves de ces propriétés en annexe

La divisibilité

Avec les deux premières propriétés, on peut savoir assez facilement si un nombre est divisible par un autre. Commençons par un cas simple. Est-ce que 600 est divisible par 7

$$\begin{aligned}
600 &\equiv 600 \pmod 7 \\
&\equiv (6\cdot 10\cdot 10) \pmod 7 \\
&\equiv 6 \pmod 7 \cdot 10 \pmod 7 \cdot 10 \pmod 7 \quad \text{(propriété 2)} \\
&\equiv -1 \pmod 7 \cdot 3 \pmod 7 \cdot 3 \pmod 7 \\
&\equiv (-1\cdot 3\cdot 3) \pmod 7 \\
&\equiv -9 \pmod 7 \\
&\equiv 5 \pmod 7
\end{aligned}$$

600 n'est donc pas divisible par 7.

Exemple : Est-ce que 7965 est un multiple de 7

$$\begin{aligned}
7965 &\equiv (7\cdot 1000 + 9\cdot 100 + 6\cdot 10 + 5) \pmod 7 \\
&\equiv (7\cdot 10\cdot 10\cdot 10 + 9\cdot 10\cdot 10 + 6\cdot 10 + 5) \pmod 7 \\
&\equiv (0\cdot 3\cdot 3\cdot 3 + 2\cdot 3\cdot 3 + -1\cdot 3 + -2) \pmod 7 \\
&\equiv (0 + 18 - 3 - 2) \pmod 7 \\
&\equiv 13 \pmod 7 \\
&\equiv 6 \pmod 7
\end{aligned}$$

On sait donc que 7 n'est pas un facteur de 7965.

Exemple : Est-ce que 7956 est un multiple de 13

$$\begin{aligned}
7956 &\equiv (7\cdot 10\cdot 10\cdot 10 + 9\cdot 10\cdot 10 + 5\cdot 10 + 6) \pmod{13} \\
&\equiv (7\cdot -3\cdot -3\cdot -3 + -4\cdot -3\cdot -3 + 5\cdot -3 + 6) \pmod{13} \\
&\equiv (7\cdot -27 + 12\cdot -3 + -15 + 6) \pmod{13} \\
&\equiv (7\cdot -1 + -1\cdot -3 + -2 + 6) \pmod{13} \\
&\equiv (-7 + 3 - 2 + 6) \pmod{13} \\
&\equiv 0 \pmod{13}
\end{aligned}$$

On sait donc que 7956 est divisible par 13.

Quelques critères de divisibilité célèbres

Évidemment, il est facile de déterminer aussi si le nombre est divisible par 2 et 5. Mais il existe aussi quelques trucs pour d'autres nombres.

Divisibilité par 3

On peut prouver facilement un critère de divisibilité par 3 qui dit que si la somme des chiffres d'un nombre est divisible par 3 alors le nombre est divisible par 3. Prenons par exemple un nombre de 5 chiffres : *abcde*. On a alors

$$\begin{aligned} abcde &\equiv \left(a\cdot 10\cdot 10\cdot 10\cdot 10 + b\cdot 10\cdot 10\cdot 10 + c\cdot 10\cdot 10 + d\cdot 10 + e\right) (\mathrm{mod}\, 3) \\ &\equiv \left(a\cdot 1\cdot 1\cdot 1\cdot 1 + b\cdot 1\cdot 1\cdot 1 + c\cdot 1\cdot 1 + d\cdot 1 + e\right) (\mathrm{mod}\, 3) \\ &\equiv \left(a + b + c + d + e\right) (\mathrm{mod}\, 3) \end{aligned}$$

Exemple : Est-ce que 7965 est divisible par 3

Puisque 7+9+6+5 = 27 est divisible par 3, cela signifie que 7965 est divisible par 3.

Divisibilité par 9

On peut prouver facilement un critère de divisibilité par 9 qui dit que si la somme des chiffres d'un nombre est divisible par 9 alors le nombre est divisible par 9. Prenons par exemple un nombre de 5 chiffres : *abcde*. On a alors

$$\begin{aligned} abcde &\equiv \left(a\cdot 10\cdot 10\cdot 10\cdot 10 + b\cdot 10\cdot 10\cdot 10 + c\cdot 10\cdot 10 + d\cdot 10 + e\right) (\mathrm{mod}\, 9) \\ &\equiv \left(a\cdot 1\cdot 1\cdot 1\cdot 1 + b\cdot 1\cdot 1\cdot 1 + c\cdot 1\cdot 1 + d\cdot 1 + e\right) (\mathrm{mod}\, 9) \\ &\equiv \left(a + b + c + d + e\right) (\mathrm{mod}\, 9) \end{aligned}$$

Exemple : Est-ce que 7965 est divisible par 9

Puisque 7+9+6+5 = 27 est divisible par 9, cela signifie que 7965 est divisible par 9.

Divisibilité par 11

On peut aussi prouver facilement un critère de divisibilité par 11 qui dit que si la somme avec signe alterné des chiffres d'un nombre est divisible par 11 alors le nombre est divisible par 11. Prenons par exemple un nombre de 5 chiffres : *abcde*. On a alors

$$\begin{aligned} abcde &\equiv \left(a\cdot 10\cdot 10\cdot 10\cdot 10 + b\cdot 10\cdot 10\cdot 10 + c\cdot 10\cdot 10 + d\cdot 10 + e\right)(\mathrm{mod}11) \\ &\equiv \left(a\cdot -1\cdot -1\cdot -1\cdot -1 + b\cdot -1\cdot -1\cdot -1 + c\cdot -1\cdot -1 + d\cdot -1 + e\right)(\mathrm{mod}11) \\ &\equiv \left(a-b+c-d+e\right)(\mathrm{mod}11) \end{aligned}$$

Exemple : Est-ce que 7965 est divisible par 11

Puisque -7+9-6+5 = -1 n'est divisible par 11, cela signifie que 7965 n'est pas divisible par 11.

EXERCICES

1. Déterminez, sans calculatrice, si

a) 8748 est divisible par 7

b) 108 439 est divisible par 9

c) 957 est divisible par 11

d) 976 497 est divisible par 3

e) 2 050 545 est divisible par 13

f) 89 760 est divisible par 17

g) 96 257 est divisible par 7

h) 78 656 est divisible par 19

i) 183 489 est divisible par 11

j) 32 344 est divisible par 13

2. Trouver la valeur de *A* pour que le nombre de cinq chiffres *12A3B* soit divisible par 4 et 9 et que $A \neq B$

3. Quand un nombre n est divisé par 5, le reste est 1. Quel est le reste si 3n est divisée par 5?

Le dernier chiffre d'une expression

La plupart du temps, il est assez facile de connaitre le dernier chiffre, mais parfois ce peut être difficile, comme dans le cas de base avec un exposant très grand. Par exemple, si on veut savoir le dernier chiffre de $43^{5\,679}$ ou de $62^{1\,986}$, il est impossible de le savoir directement avec la calculatrice. On peut cependant trouver ce dernier chiffre à l'aide de l'arithmétique modulaire. Pour connaitre le dernier chiffre, on doit trouver le reste quand on divise par 10. On doit donc trouver le modulo 10 du nombre.

On peut d'abord simplifier le problème en se concentrant uniquement sur le dernier chiffre puisque, selon la propriété 6, on a

$$43^{5679} \equiv 3^{5679} \pmod{10}$$
$$62^{1986} \equiv 2^{1986} \pmod{10}$$

Il y a 3 cas évidents : si la base est 0, 5 ou 6. C'est évident puisque toutes les puissances de 0 se terminent par 0, toutes les puissances de 5 se terminent par 5 et toutes les puissances de 6 se terminent par 6.

Ensuite, on a deux possibilités. Premièrement, on peut chercher un facteur qui se termine par 1 ou 9. C'est utile pour les cas ou la base se termine par 1, 3 (puisque $3^2=9$), 7 (puisque $7^2 = 49$) et 9.

Ainsi on a

$$\begin{aligned} 43^{5679} &\equiv 3^{5679} \pmod{10} \\ &\equiv \left(\left(3^2\right)^{2839} 3\right) \pmod{10} \\ &\equiv \left((-1)^{2839} 3\right) \pmod{10} \\ &\equiv (-1 \cdot 3) \pmod{10} \\ &\equiv 7 \pmod{10} \end{aligned}$$

Et on sait donc que ce chiffre se termine par 7

On peut aussi chercher un cycle dans le dernier chiffre des facteurs. Par exemple, il y a un cycle pour le dernier chiffre des puissances de 2 puisque 2^1 =2, 2^2=4, 2^3 =8, 2^4 =16 et 2^5 =32, on voit que le dernier chiffre revient le même quand l'exposant augmente de 4. On peut donc enlever tous les multiples de 4 à l'exposant. Cette technique fonctionne bien quand le dernier chiffre est 2 (cycle de 4), 3 (cycle de 4), 4 (cycle de 2), 7 (cycle de 4), 8 (cycle de 4) et 9 (cycle de 2)

Ainsi, on a, pour $2^{1\,986}$

$$2^{1986} \equiv 2^2 \pmod{10}$$

(Puisque 1984 est un multiple de 4 et qu'on peut enlever les multiples de 4 à l'exposant tant qu'on veut.) Donc

$$\begin{aligned} 2^{1986} &\equiv 2^2 \pmod{10} \\ &\equiv 4 \pmod{10} \end{aligned}$$

Ce chiffre se termine donc par 4

On peut aussi utiliser cette technique pour $43^{5\,678}$. On a alors

$$\begin{aligned} 43^{5679} &\equiv 3^{5679} \pmod{10} \\ &\equiv \left(3^3\right) \pmod{10} \\ &\equiv (7) \pmod{10} \end{aligned}$$

À la deuxième ligne, nous avons diminué la puissance de 5676, qui est un multiple de 4, puisque le cycle des exposants en base 3 est de 4.

Exemple : Quel est le dernier chiffre de $3\,244^{567}$?

On a

$$\begin{aligned} 324^{4567} &\equiv 4^{4567} \pmod{10} \\ &\equiv 4 \pmod{10} \end{aligned}$$

À la deuxième ligne, nous avons diminué la puissance de 4566, qui est un multiple de 2, puisque le cycle des exposants en base 4 est de 2.

Exemple : Quel est le dernier chiffre de $7^{42} + 42^7$

$$\begin{aligned} 7^{42} + 42^7 &\equiv \left(7^{42} + 2^7\right) \pmod{10} \\ &\equiv \left(7^2 + 2^3\right) \pmod{10} \\ &\equiv (49 + 8) \pmod{10} \\ &\equiv (57) \pmod{10} \\ &\equiv 7 \pmod{10} \end{aligned}$$

Le dernier chiffre est donc 7

Parfois, on peut trouver les deux derniers chiffres d'un nombre. Évidemment, c'est 0 si la base se termine par 0 et que l'exposant est 2 ou plus! Par contre, il n'y a rien de facile pour les bases se terminant par les autres nombres. Parfois, on peut être chanceux comme c'est le cas avec l'exemple suivant.

Exemple : Quel sont les deux derniers chiffres de 2007^{2007}

$2007^{2007} \equiv 7^{2007} \pmod{100}$ Propriété 6 (attention, il faut garder les deux derniers chiffres de la base en mod 100)

On peut ensuite faire

$$\begin{aligned} 2007^{2007} &\equiv 7^{2007} \pmod{100} \\ &\equiv \left(\left(7^4\right)^{501} 7^3 \right) \pmod{100} \\ &\equiv \left(\left(2401\right)^{501} 7^3 \right) \pmod{100} \\ &\equiv \left(\left(1\right)^{501} 7^3 \right) \pmod{100} \\ &\equiv \left(343\right) \pmod{100} \\ &\equiv 43 \pmod{100} \end{aligned}$$

La chance, c'est d'avoir une puissance de 7 pas trop grande qui donne un nombre se terminant par 01!

EXERCICES

1. Quel est le dernier chiffre de

a) $2^{98\,768}$

b) $3^{98\,768}$

c) $4^{98\,768}$

d) $5^{98\,768}$

e) $6^{98\,768}$

f) $7^{98\,768}$

g) $8^{98\,768}$

h) $9^{98\,768}$

ANNEXE

Preuve des propriétés des modules

1) $a+b \equiv a\left(\bmod m\right)+b\left(\bmod m\right)$

Soit les nombres *a = Am + r* et *B = Bm + t.* On a alors

$$\begin{aligned}\left(a+b\right) &= \left(\left(Am+r\right)+\left(Bm+t\right)\right)\\ &= \left(\left(A+B\right)m+\left(r+t\right)\right)\end{aligned}$$

Le reste est *r + t*, ce qui est bien la somme des deux restes de chaque nombre

2) $ab \equiv a\left(\bmod m\right)\cdot b\left(\bmod m\right)$

Soit les nombres *a = Am + r* et *B = Bm + t.* On a alors

$$\begin{aligned}a\cdot b &= \left(\left(Am+r\right)\cdot\left(Bm+t\right)\right)\\ &= \left(ABm^2+Amt+Bmr+rt\right)\\ &= \left(ABm+At+Br\right)m+rt\end{aligned}$$

Le reste est donc rt, ce qui est bien le produit des deux restes de chaque nombre

3) $a+c \equiv b+c\left(\bmod m\right)$

Si a et b on les mêmes restes, alors ces nombres s'écrivent *a = Am + r* et *B = Bm + r.* Si on additionne à chacun un nombre *c = Cm + t*, on a alors

$$a+c=(Am+r)+(Cm+t)=(A+C)m+(r+t)$$ (le reste est *r + t*)

$$b+c=(Bm+r)+(Cm+t)=(B+C)m+(r+t)$$ (le reste est *r + t*)

Les restes sont donc les mêmes.

4) $a-c\equiv b-c\pmod m$

Si a et b on les mêmes restes, alors ces nombres s'écrivent *a = Am + r* et *B = Bm + r*. Si on soustrait à chacun un nombre *c = Cm + t*, on a alors

$$a-c=(Am+r)-(Cm+t)=(A-C)m+(r-t)$$ (le reste est *r - t*)

$$b-c=(Bm+r)-(Cm+t)=(B-C)m+(r-t)$$ (le reste est *r - t*)

Les restes sont donc les mêmes.

5) $a\cdot c\equiv b\cdot c\pmod m$

Si a et b on les mêmes restes, alors ces nombres s'écrivent *a = Am + r* et *B = Bm + r*. Si on multiplie chacun de ces nombres par le nombre *c = Cm + t*, on a alors

$$a\cdot c=(Am+r)(Cm+t)=ACm^2+Amt+Cmr+rt=(ACm+At+Cr)m+rt$$

(le reste est *rt*)

$$b\cdot c=(Bm+r)(Cm+t)=BCm^2+Bmt+Cmr+rt=(BCm+Bt+Cr)m+rt$$

(le reste est *rt*)

Les restes sont donc les mêmes.

6) $a^c \equiv b^c \pmod{m}$

Si a et b on les mêmes restes, alors ces nombres s'écrivent $a = Am + r$ et $B = Bm + r$. Si on fait la puissance c de ces nombres, on a alors

$$a^c = (Am + r)^c$$

Quand on fait cette puissance, il y aura au moins un m dans tous les termes à l'exception du dernier terme qui sera r^c. Par exemple, si c vaut 5 on aura

$$(Am + r)^c = (Am)^5 + 5(Am)^4 r + 10(Am)^3 r^2 + 10(Am)^2 r^3 + 5(Am) r^4 + r^5$$

Tous les termes avec un *m* sont divisibles par *m* et, donc, seul le dernier terme contribue au reste. Le reste est donc r^c. Par le même raisonnement, le reste de

$$b^c = (Bm + r)^c$$

est aussi r^c.

Les restes sont donc les mêmes.