Chapitre 4

Congruences

4.1 Introduction historique

La mathématique est la reine des sciences et l'arithmétique est la reine des mathématiques.

Carl Friedrich Gauss - 1777-1855, propos rapporté par W. Sartorius von Waltershausen, *Gauss zum Gedächtniss* (1856)

Précédemment évoqué, **Carl Friedrich Gauss**, autrement surnommé le *prince des mathématiciens* par ses contemporains, s'est fait connaître en publiant un ouvrage intitulé **Disquisitiones arithmeticae** en 1801, alors qu'il n'avait que 24 ans. Dans ce livre, il développe la théorie de l'arithmétique modulaire, ou des **congruences**, dont l'étude a eu un impact considérable sur l'arithmétique jusqu'à aujourd'hui.

4.1.1 Casse-tête chinois

Curieusement ce domaine d'étude, qui s'attache aux restes de divisions euclidiennes et leurs propriétés, a été abordé par de nombreux mathématiciens dans l'histoire, jusqu'aux Chinois, dans le *Sunzi Suanjing* (rédigé entre le III^{e} et le V^{e} siècle), qui se posaient des questions de ce type :

> *Soient des objets dont on ignore le nombre. En les comptant 3 par 3 il en reste 2, en les comptant 5 par 5, il en reste 3 et en les comptant 7 par 7, il en reste 2. Combien y a-t-il d'objets ?*

Ce type de problème et leur étude aura notamment donné naissance au fameux **théorème des restes chinois**, mais il faudra attendre Gauss et ses définitions précises pour qu'on parle enfin de congruences.

4.1.2 Ce qui module c'est le reste

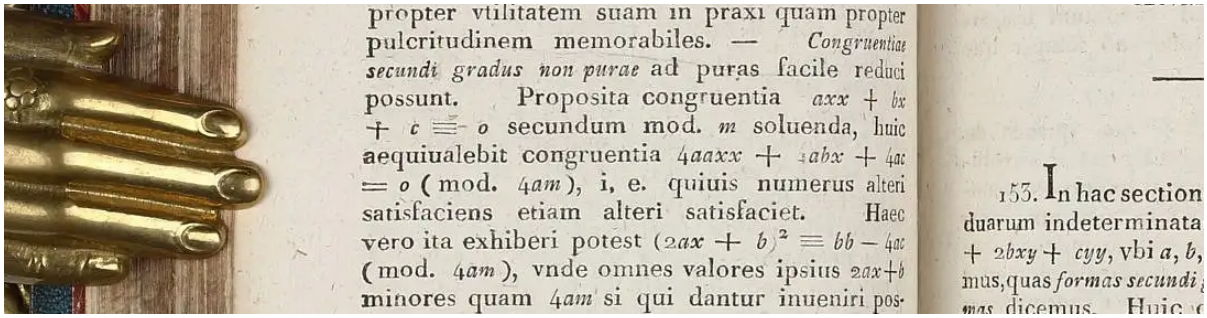
Au lieu de s'intéresser à des problèmes de divisibilité en trimbalant l'entièreté des quotients en plus de leur reste, Gauss eut une idée simple : pourquoi ne pas juste s'intéresser au reste, et effectuer des calculs uniquement à partir de ceux ci ?

En effet, si en divisant par 5, les nombres 146 et 2763 auront respectivement 1 et 3 pour reste, on peut intuitivement se douter que le reste de la division par 5 de leur somme sera 4, sans avoir à calculer $146+2763$... Afin d'éviter ces calculs qui peuvent devenir extrêmement lourds, Gauss introduira lui-même la notation encore utilisée pour donner le reste de la division de 2763 par 5, ou autrement dit pour indiquer que 2763 **congrue** à 3 modulo 5 :

$$2763 \equiv 3\,[5]$$

Muni de cette idée, on s'intéressera dans ce chapitre aux propriétés de la congruence, jusqu'au petit théorème de Fermat, énoncé par Pierre de Fermat en 1640 sans démonstration, et dont la première preuve publiée est due à Euler en 1736.

~


propter vtilitatem suam in praxi quam propter pulcritudinem memorabiles. — *Congruentiae secundi gradus non purae* ad puras facile reduci possunt. Proposita congruentia $axx + bx + c \equiv o$ secundum mod. m soluenda, huic aequiualebit congruentia $4aaxx + 4abx + 4ac \equiv o$ (mod. $4am$), i, e. quiuis numerus alteri satisfaciens etiam alteri satisfaciet. Haec vero ita exhiberi potest $(2ax + b)^2 \equiv bb - 4ac$ (mod. $4am$), vnde omnes valores ipsius $2ax+b$ minores quam $4am$ si qui dantur inueniri pos-

153. In hac section
duarum indeterminata
$+ 2bxy + cyy$, vbi $a, b,$
mus, quas *formas secundi*
mas dicemus. Huic

4.2 Vocabulaire et propriétés

Définition :

Soient $n \geqslant 2$ un entier naturel et a,$b \in \mathbb{Z}$.

On dit que les entiers a et b sont **congrus modulo** n si et seulement si a et b ont le même reste dans la division euclidienne par n. On note alors :

$$a \equiv b \mod n \qquad \text{ou} \qquad a \equiv b\ (n) \qquad \text{ou} \qquad a \equiv b\ [n]$$

ex : • *On peut voir par exemple que :*

$$337 \equiv 1\ [3] \qquad \textit{car :} \qquad 337 = 3 \times 112 + 1 \ \textit{et}\ 1 = 3 \times 0 + 1$$

Ou bien :

$$337 \equiv 10\ [3] \qquad \textit{ou} \qquad 1 \equiv 1\ [3]$$

En effet 337, 10 *et* 1 *sont tous congrus à* 1 *modulo* 3*, ils sont donc congrus entre eux.*

• *Un nombre x est pair si et seulement si $x \equiv 0\ [2]$. Il est impair si et seulement si $x \equiv 1\ [2]$.*

Proposition 1 :

Soient $n \geqslant 2$ et k deux entiers naturels, a, b, c et d quatre entiers tels que :

$$a \equiv c\ [n] \qquad \text{et} \qquad b \equiv d\ [n]$$

On a alors :

- $a + b \equiv c + d\ [n]$
- $a \times b \equiv c \times d\ [n]$
- $a^k \equiv c^k\ [n]$

◦ Démonstration : On procède point par point :

• Par définition, il existe q_a, q_b, q_c et q_d quatre entiers relatifs et r, r' deux entiers naturels strictement plus petits que n tels que :

$$a = q_a n + r, \qquad c = q_c n + r \qquad \text{et} \qquad b = q_b n + r', \qquad d = q_d n + r'$$

Or :

$$\begin{aligned} a + b &= q_a n + r + q_b n + r' \\ &= (q_a + q_b)n + (r + r') \\ \text{et : } c + d &= q_c n + r + q_d n + r' \\ &= (q_c + q_d)n + (r + r') \end{aligned}$$

On en déduit donc que $a+b$ et $c+d$ auront le même reste dans la division euclidienne par n, donc :

$$a + b \equiv c + d\ [n]$$

• Avec les mêmes hypothèses :

$$\begin{aligned} a \times b &= (q_a n + r) \times (q_b n + r') \\ &= q_a q_b n^2 + q_a n r' + r q_b n + r r' \\ &= n(q_a q_b n + q_a r' + q_b r) + r r' \\ \text{et : } c \times d &= (q_c n + r) \times (q_d n + r') \\ &= q_c q_d n^2 + q_c n r' + r q_d n + r r' \\ &= n(q_c q_d n + q_c r' + q_d r) + r r' \end{aligned}$$

On en déduit donc que $a \times b$ et $c \times d$ auront le même reste dans la division euclidienne par n, donc :

$$a \times b \equiv c \times d\ [n]$$

• On procède par récurrence sur k et on utilise le point précédent.

□

Proposition 2 :
Soient $n \geqslant 2$, a et b deux entiers. On a alors :

$$a \equiv b\ [n] \quad \Leftrightarrow \quad a - b \equiv 0\ [n] \quad \Leftrightarrow \quad \exists k \in \mathbb{Z},\ a = b + kn$$

∘ Démonstration : La première équivalence découle de la proposition précédente, car sachant que $-b \equiv -b\ [n]$:

$$\begin{aligned} a \equiv b\ [n] &\Leftrightarrow a + (-b) \equiv b + (-b)\ [n] \\ &\Leftrightarrow a - b \equiv 0\ [n] \end{aligned}$$

Ce résultat nous dit donc que $a - b$ et 0 ont le même reste dans la division euclidienne par n, or 0 a nécessairement 0 comme reste, donc $a - b$ est divisible par n, autrement dit il existe un $k \in \mathbb{Z}$ tel que $a - b = kn$, d'où le résultat.

□

ex : • *De* $34 \equiv 6\ [7]$ *et* $131 \equiv 5\ [7]$*, on déduit alors que :*

$$\begin{aligned} 34 + 131 \equiv 6 + 5\ [7]\ &\equiv 11\ [7] \equiv 4\ [7] \\ \textit{ou}\ \ 34 \times 131 \equiv 6 \times 5\ [7]\ &\equiv 30\ [7]\ \equiv 2\ [7] \end{aligned}$$

• *Quel est le dernier chiffre de* 3^{153} *?*
On sait que $3 \equiv 3\ [10]$*, donc :*

$$\begin{aligned} 3^2 &\equiv 9\ [10] \\ \Rightarrow 3^3 &\equiv 3 \times 9\ [10]\ \equiv 27\ [10]\ \equiv 7\ [10] \\ \Rightarrow 3^4 &\equiv 3 \times 7\ [10]\ \equiv 21\ [10]\ \equiv 1\ [10] \end{aligned}$$

On en déduit donc que :

$$3^{152} = (3^4)^{38} \equiv 1^{38}\ [10]\ \equiv 1\ [10]$$

Enfin :

$$3^{153} = 3 \times 3^{152} \equiv 3 \times 1\ [10]\ \equiv 3\ [10]$$

Le dernier chiffre de 3^{153} *sera donc un* 3*.*

4.3 Petit théorème de Fermat

Petit théorème de Fermat :
Soit p un nombre premier. Pour tout entier a, on a :

$$a^p \equiv a\ [p]$$

Si de plus a n'est pas divisible par p, on a :

$$a^{p-1} \equiv 1\ [p]$$

∘ Démonstration : On montre d'abord, par récurrence sur $a \in \mathbb{N}$, la propriété P_a : « $a^p \equiv a\ [p]$ ».

— **Initialisation :** $0^p = 0$, donc P_0 est vraie.

— **Hérédité :** Soit $n \in \mathbb{N}$. Supposons que $n^p \equiv n\ [p]$. D'après la formule du binôme :

$$\begin{aligned} (n+1)^p &= \sum_{k=0}^{p} \binom{p}{k} n^k 1^{p-k} \\ &= \sum_{k=0}^{p} \binom{p}{k} n^k \end{aligned}$$

On remarque alors que pour tout $0 < k < p$:

$$\begin{aligned}\binom{p}{k} &= \frac{p!}{k!(p-k)!} \\ &= \frac{p}{k} \times \frac{(p-1)!}{(k-1)!(p-k)!} \\ &= \frac{p}{k} \times \frac{(p-1)!}{(k-1)!(p-1-(k-1))!} \\ &= \frac{p}{k} \times \binom{p-1}{k-1}\end{aligned}$$

d'où l'égalité : $p \times \binom{p-1}{k-1} = k \times \binom{p}{k}$

Or cette égalité signifie que p divise $k \times \binom{p}{k}$, mais p ne peut pas diviser k puisque $0 < k < p$, donc d'après le Lemme d'Euclide, p divise $\binom{p}{k}$.
Ainsi dans notre calcul, pour tout $k \in [\![1; p-1]\!]$, le coefficient binomial a un facteur p et est congru à 0 modulo p. On en déduit que :

$$\begin{aligned}(n+1)^p \equiv \binom{p}{0} n^0 + \binom{p}{p} n^p \ [p] \\ \equiv 1 + n^p \ [p] \qquad \text{or par hypothèse } n^p \equiv n \ [p] \\ \equiv 1 + n \ [p]\end{aligned}$$

L'hérédité est donc vérifiée.

— **Conclusion :** Pour tout entier naturel a, $a^p \equiv a \ [p]$.
Si a est un entier négatif, on note r le reste de sa division euclidienne par p : on a $a \equiv r \ [p]$ avec $r \in \mathbb{N}$, donc d'après la Proposition 1 et ce qui précède, $a^p \equiv r^p \equiv r \equiv a \ [p]$.

Pour l'autre résultat, on déduit de ce qui précède que pour tout a non divisible par p :

$$a^p - a \equiv 0 \ [p] \qquad \Rightarrow \qquad a(a^{p-1} - 1) \equiv 0 \ [p]$$

Ce qui signifie que p divise $a(a^{p-1} - 1)$, mais p ne divisant pas a, d'après le Lemme d'Euclide p divise $(a^{p-1} - 1)$, autrement dit :

$$a^{p-1} - 1 \equiv 0 \ [p] \qquad \Rightarrow \qquad a^{p-1} \equiv 1 \ [p]$$

□

ex : • *Ce résultat offre des conclusions surprenantes, par exemple sachant que* 134 *n'est pas divisible par* 13*, on peut en déduire que :*

$$134^{12} \equiv 1 \ [13]$$

Autrement dit, $134^{12} - 1$ *est un multiple de* 13*.*