TÉORÈME CHINOIS

1 Cours

Le point de départ pour ce qui suit est le Théorème fondamental de l'arithmétique, qui affirme que tout entier se décompose en produit de premiers de manière unique à permutation des facteurs près. Une conséquence directe est le Lemme de Gauss : si $d \mid ab$ et $\text{pgcd}(d, a) = 1$ alors $d \mid b$.

Définition 1. Soit a, b et n trois entiers tels que $n \neq 0$. On dit que a est congruent à b modulo n si n divise $b - a$. Dans ce cas on écrit $a \equiv b \mod n$.

Théorème 1. Soit a, b, c et d des entiers tels que $a \equiv b \mod n$ et $c \equiv d \mod n$. Alors on a :

1. $a + c \equiv b + d \mod n$;
2. $ac \equiv bd \mod n$.

Démonstration. Soit x et y deux entiers tels que $b - a = nx$ et $d - c = ny$.

1. On a $(b + d) - (a + c) = n(x + y)$ et ainsi $b + d \equiv a + c \mod n$.
2. On a $bd - ac = bd - bc + bc - ac = b(d - c) + c(b - a) = (by + cx)n$ et ainsi $bd \equiv ac \mod n$.

□

Exercice 1. Calculez le dernier chiffre de 2017^{2017}.

Solution 1. La clé de la solution est que le dernier chiffre d'un entier est égal au reste de cet entier modulo 10. D'une part on a $2017^{2017} \equiv 7^{2017} \mod 10$. D'autre part on a $7^4 \equiv 49^2 \equiv 9^2 \equiv 81 \equiv 1 \mod 10$. Ainsi on obtient

$$7^{2017} \equiv 7^{4 \cdot 504 + 1} \equiv (7^4)^{504} \cdot 7 \equiv 1 \cdot 7 \equiv 7 \mod 10.$$

Donc le dernier chiffre est 7.

Théorème 2 (d'existence de l'inverse). Soit a et n deux entiers tels que $\text{pgcd}(a, n) = 1$. Alors il existe un entier u appelé inverse de a modulo n tel que $au \equiv 1 \mod n$.

Démonstration. On considère la fonction

$$\begin{array}{rccc} \varphi : & [[0, n-1]] & \to & [[0, n-1]] \\ & x & \mapsto & ax \bmod n, \end{array}$$

où $[[u, v]] = [u, v] \bigcap \mathbb{Z}$ et $ax \mod n$ est le reste de ax à la division par n.

Montrons que φ est injective. Pour cela, soit x_1 et x_2 deux éléments de $[[0, n - 1]]$ tels que ax_1 et ax_2 ont le même reste à la division par n. Alors

$n \mid ax_1 - ax_2 = a(x_1 - x_2)$ et, comme $\text{pgcd}(a, n) = 1$, le Lemme de Gauss implique que n divise $x_2 - x_1$. Or, $|x_2 - x_1| < (n-1) - 1 < n$ donc $x_1 = x_2$. Cela montre que φ est injective et, comme son domaine et codomaine sont des ensembles finis de même cardinal (même ensemble), φ est également surjective. En particulier, il existe x tel que $\varphi(x) = 1$ soit de manière équivalente $ax \equiv 1 \mod n$. □

Remarque 1. L'ensemble des restes modulo un premier p est muni des quatre opérations : addition, soustraction, multiplication et division ($b/a = bu$ où u est l'inverse de a).

Théorème 3 (Bezout). Soit a et b deux entiers relatifs non-nuls. Alors il existe des entiers relatif u et v tels que

$$\text{pgcd}(a, b) = au + bv.$$

Démonstration. On traite d'abord le cas où $\text{pgcd}(a, b) = 1$. On applique le Théorème d'existence de l'inverse pour a et b : il existe u tel que $au \equiv 1 \mod b$ ou de manière équivalente $v = -\frac{1-au}{b}$ est un entier relatif. On a donc $1 = au + vb$ avec u et v entiers relatifs.

Dans le cas général on pose $d = \text{pgcd}(a, b)$, $a' = a/d$ et $b' = b/d$, ce qui permet d'avoir $\text{pgcd}(a', b') = 1$. On applique le cas déjà traité à a' et b' : il existe deux entiers relatifs tels que $1 = a'u + b'v$. On multiplie par d et on trouve $d = da'u + db'v$ soit $d = au + bv$. □

Lemme 1. Pour tous les entiers n_1, n_2, r_1 et r_2 tels que $\text{pgcd}(n_1, n_2) = 1$ il existe un entier N tel que

$$\begin{aligned} N &\equiv r_1 \mod n_1, \\ N &\equiv r_2 \mod n_2. \end{aligned}$$

Démonstration. On commence par traiter le cas où $r_1 = 1$ et $r_2 = 0$. On applique le Théorème d'existence de l'inverse pour $a = n_2$ et $n = n_1$: il existe un entier u tel que $un_2 \equiv 1 \mod n_1$. On pose $N_1 = un_2$ et on remarque que $N \equiv 1 \mod n_1$ et $N \equiv 0 \mod n_2$.

Le cas $r_1 = 0$ et $r_2 = 1$ est identique, en échangeant n_1 et n_2. On obtient N_2 tel que $N_2 \equiv 0 \mod n_1$ et $N_2 \equiv 1 \mod n_2$.

Passons maintenant au cas général. On pose $N = N_1 r_1 + N_2 r_2$ et on vérifie :

$$\begin{aligned} N \equiv N_1 r_1 + N_2 r_2 \equiv 1 \cdot r_1 + 0 \cdot r_2 \equiv r_1 \mod n_1, \\ N \equiv N_1 r_1 + N_2 r_2 \equiv 0 \cdot r_1 + 1 \cdot r_2 \equiv r_2 \mod n_2, \end{aligned}$$

□

Théorème 4 (chinois). Soit $n_1, \ldots, n_k$ une liste de $k \geq 2$ entiers mutuellement premiers et $r_1, \ldots, r_k$ des entiers. Alors il existe un entier N tel que, pour tout $i = 1, \ldots, k$,

$$N \equiv r_i \mod n_i.$$

Démonstration. On procède par récurrence sur k. Le cas $k = 2$ est traité dans le lemme ci-dessus.

Supposons le résultat vrai pour $k-1$: il existe un entier N' tel que, pour tout $i = 1, \ldots, k-1$, $N' \equiv r_i \mod n_i$. On applique le lemme ci-dessous à $n_1 n_2 \cdots n_{k-1}$ et n_k avec les restes $r_1 = N'$ et respectivement $r_2 = r_k$: il existe un entier N tel que $N \equiv N' \mod n_1 n_2 \cdots n_{k-1}$ et $N \equiv r_k \mod n_k$. On vérifie que pour, tout $i = 1, \ldots, k-1$, $N \equiv N' \mod n_1 n_2 \cdots n_{k-1}$ et en particulier $N \equiv r_i \mod n_i$. □

Remarque 2. Une manière équivalente d'énoncer le Théorème chinois est la suivante : la donnée du reste d'un entier modulo n_1, n_2, ..., n_k est équivalente à donner le reste modulo $n_1 n_2 \cdots n_k$.

Exercice 2 (méthode de factorisation de Fermat). Soit N un entier de la forme $N = p_1 p_2 \cdots p_k$ avec $p_1, \ldots, p_k$ des premiers distincts et soit a tel que $\text{pgcd}(a, n) = 1$. Alors

1. l'ensemble $\{b \in [[1, N-1]] \mid a^2 \equiv b^2 \mod N\}$ a cardinal 2^k.
2. en calculant $\text{pgcd}(N, b-a)$ pour tout b on trouve tous les facteurs premiers de N.

Solution 2.

1. Dans le cas où $k = 1$ on a $p_1 \mid (a-b)(a+b)$ donc $b = \pm a$: on a 2 solutions. Dans le cas où k est quelconque, soit ε_1, ..., ε_k des éléments de $\{1, -1\}$. D'après le Théorème chinois il existe un unique b tel que, pour tout $i = 1, 2, \ldots, k$, $b \equiv \varepsilon_i a \mod p_i$. Ainsi, le cardinal de l'ensemble est égal au nombre de choix de k-uplets $(\varepsilon_1, \ldots, \varepsilon_k)$: 2^k.
2. Pour tout i, le choix où $\varepsilon_i = 1$ et, pour $j \neq i$, $\varepsilon_j = -1$ donne b tel que $a - b \equiv 0 \mod p_i$ et $a - b \not\equiv 0 \mod \prod_{j \neq i} p_j$. Ainsi $\text{pgcd}(b, N) = p_i$.

Remarque 3. L'algorithme de factorisation crible algébrique, étudié notamment pour mesurer la sécurité de RSA, utilise la méthode de Fermat. Dans l'algorithme, on calcule rapidement des paires (a, b) telles que $a^2 \equiv b^2 \mod N$ de façon que b peut prendre toutes les valeurs de l'ensemble précédent avec une probabilité égale.

Théorème 5 (petit théorème de Fermat). Soit p un nombre premier et a un entier relatif non divisible par p. Alors on a

$$a^{p-1} \equiv 1 \mod p.$$

Démonstration. Rappelons que l'application $x \mapsto ax$, étudiée dans la preuve du Théorème d'existence de l'inverse, est une permutation de l'ensemble $\{1, 2, \ldots, p-$

1}. Puisque dans un produit l'ordre des facteurs ne compte pas on a

$$\prod_{x=1}^{p-1} x \equiv \prod_{x=1}^{p-1} (ax) \mod p.$$

Or, $\prod_{x=1}^{p-1}(ax) = a^{p-1}\prod_{x=1}^{p-1} x$ donc $\prod_{x=1}^{p-1} x \equiv a^{p-1}\prod_{x=1}^{p-1} x \mod p$. Comme $b = \prod_{x=1}^{p-1} x$ n'est pas divisible par p, d'après le Théorème d'existence de l'inverse il existe un entier u tel que $bu \equiv 1 \mod p$. Alors on a

$$\begin{array}{rcll} ub & \equiv & uba^{p-1} & \mod p, \\ 1 & \equiv & a^{p-1} & \mod p. \end{array}$$

□

Remarque 4. Le Théorème de Bezout, le Théorème de l'existence de l'inverse et le Théorème chinois quand $k = 2$ sont trois résultats qui se démontre rapidement l'un à partir de l'autre, et le Petit théorème de Fermat en découle facilement de n'importe lequel des trois. Le Lemme de Gauss et le Théorème fondamental de l'arithmétique se démontre l'un à partir de l'autre mais leur propre preuve à partir des axiomes de l'ensemble $\mathbb{N}$ est relativement artificielle. Nous résumons ces implications dans la Figure 1, le chemin souligné étant celui suivi dans le cours présent.

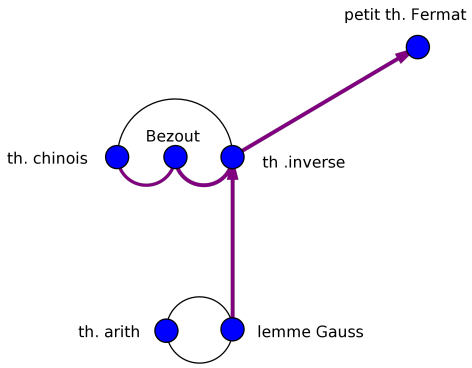

FIGURE 1 – Résultats apparentés au Théorème chinois.

2 EXERCICES

1

1. Source des exos :

2.1 Principe du groupement des termes

Exercice 3 (Roumanie 2009). Soit m et n deux entiers non-nuls, $m > 1$. Montrez que $N = m^4 + 4n^4$ n'est pas premier.

Solution 3. On cherche à écrire le nombre sous la forme $a^2 - b^2 = (a-b)(a+b)$. Un carré proche de N est $(m^2 + 2n^2)^2 = m^4 + 4n^2 + 4m^2n^2$. Ainsi $N = (m^4 + 2n^2)^2 - (2mn)^2$.

Exercice 4 (adaptation d'après OIM 1979). Si a et b sont des entiers tels que $\frac{a}{b} = \frac{1}{673} + \frac{1}{674} \cdots + \frac{1}{1344}$ alors 2017 divise a.

Solution 4. On pose $N = 672$ et on remarque que $2017 = 3N + 1$ est premier. Alors

$$\frac{a}{b} = \sum_{k=N+1}^{2N} \frac{1}{k} = \sum_{i=1}^{N/2} \frac{1}{N+i} + \frac{1}{2N+1-i} = (3N+1) \sum_{i=1}^{N/2} r,$$

où $r = \frac{1}{(N+i)(2N+1-i)}$. En mettant au dénominateur commun, $r = \frac{\alpha}{\beta}$ où $\beta = (2N)!/N!$ et $\alpha = \sum_{i=1}^{N/2} \prod_{j \neq i} (N+j)(2N+1-j)$. Comme $3N+1$ est premier, $3N+1$ ne divise pas β donc l'exposant de $3N+1$ dans r est positif ou nul. On conclue que $2017 = 3N + 1$ divise a.

Exercice 5 (liste courte de OBM 2001). Soit a, b et n trois entiers supérieurs à 1 tels que $2^n - 1 = ab$. Alors $N = ab - (a-b) - 1$ est de la forme $k4^m$ avec k impair. Indication : regardez l'exposant de 2 dans aN.

Solution 5. Puisque a divise $2^n - 1$ qui est impair, a est impair donc l'exposant de 2 dans aN et dan N sont les mêmes.

On a $N = (a+1)(b-1)$ et alors $aN = (a+1)(ab-a)$ donc

$$aN = (a+1)(2^n - (a+1)).$$

On écrit $a + 1 = \alpha 2^m$ avec α impair, ce qui est toujours possible. Comme $2^m \leq \alpha 2^m = a + 1 < ab + 1 = 2^n$ on a $n > m$. On a utilisé $b > 1$ sans quoi $N = 0$ et l'exercice est immédiat. Alors on a

$$aN = (\alpha 2^m)(2^n - k2^m) = \alpha 2^m \cdot 2^m (2^{n-m} - \alpha) = k4^m,$$

où $k = \alpha(2^{n-m} - \alpha)$ est impair.

2.2 Principe de la considération des restes modulo un entier bien choisi

Exercice 6 (ex. de prépataions Roumanie 2012). Déterminer les premiers p tels que $p+4$, $p+6$, $p+10$, $p+12$, $p+16$ et $p+22$ soient tous premiers.

— Éléments de principe en théorie des nombres, Manuela Prajea 2012.
— Le théorème chinois, Evan Chen 2015.

Solution 6. Nous allons essayer de montrer que ces nombres ne peuvent pas être tous premiers sauf pour éventuellement un nombre fini de p. Pour cela on cherche n tel que au moins un de ces nombres est divisible par n. On essaie tour à tour $n = 2, 3, 5, 7$. Pour $n = 7$ on a :

$$\begin{aligned} p &\equiv p && \mod 7, \\ p+4 &\equiv p+4 && \mod 7, \\ p+6 &\equiv p+6 && \mod 7, \\ p+10 &\equiv p+3 && \mod 7, \\ p+12 &\equiv p+5 && \mod 7, \\ p+16 &\equiv p+2 && \mod 7, \\ p+22 &\equiv p+1 && \mod 7. \end{aligned}$$

Tous les restes modulo 7 sont atteints donc un des nombres est divisible par 7. Il ne peut pas être 7 sauf s'il est égal à 7. Les nombres $p+10$, $p+12$, $p+16$ et $p+22$ sont supérieurs à 7. Il reste trois cas :

- $p + 6 = 7$. Alors $p = 1$ n'est pas premier.
- $p + 4 = 7$. Alors $p + 6 = 7 + 2 = 9$ n'est pas premier.
- $p = 7$. Alors $\{p, p+4, p+6, p+10, p+16, p+22\} = \{7, 11, 13, 17, 19, 23, 29\}$, qui sont tous premiers.

Exercice 7 (BalticWay 2010). Déterminez les entiers n qui ont la propriété que la représentation décimale de n^2 contient uniquement des chiffres impairs.

Solution 7. On note a et b les 2 derniers chiffres de n. Alors $n = 100n' + 10a + b$ pour un entier n'. Les deux derniers chiffres de n^2 sont donnés par le reste modulo 100 de n^2. On a

$$n^2 \equiv (100n' + 10a + b)^2 \equiv (10a + b)^2 \equiv 20ab + b^2 \mod 100.$$

L'avant-dernier chiffre de n^2 a donc la même parité que le chiffre des unités de b^2. Comme le dernier chiffre de n est impair, donc $b \in \{1, 3, 7, 9\}$. Si on note $f(b)$ l'avant dernier chiffre de b alors on a $f(1) = 0$, $f(3) = 0$, $f(5) = 2$, $f(7) = 4$ et $f(9) = 8$. Il est donc impossible que l'avant dernier chiffre de n^2 soit impair quand n est impair.

Le seul cas qui reste pour que la représentation décimale de n^2 contienne uniquement des chiffres impairs est qu'il n'ait pas de chiffre des dizaines : $n^2 < 10$. On a les solutions $n = 1$ et $n = 3$.

Exercice 8 (Iran 1999). Soit p un nombre premier tel que $p \geq 5$. Alors 43 divise $7^p - 6^p - 1$.

Solution 8. Le fait que p soit premier ne sert qu'à montrer que le reste de p modulo 6 est soit 1 soit 5. En effet, les nombres premiers supérieurs à 3 sont impairs donc le reste modulo 6 est impair : 1, 3 ou 5. S'il valait 3 alors p serait divisible par 3.

Montrons par récurrence que pour tout n, $7^{6n+1} - 6^{6n+1} - 1$ et $7^{6n+5} - 6^{6n+5} - 1$ sont divisibles par 43. Pour $n = 0$ on a $7^1 - 6^1 - 1 = 0$ et

$$7^5 - 6^5 - 1 \equiv 49^2 \cdot 7 - 36^2 \cdot 6 - 1 \equiv 42 \cdot 6 - 42 \cdot 7 - 1 \equiv 0 \mod 43.$$

Pour passer de n à $n+1$ on calcule

$$\begin{aligned} 7^6 \equiv (7^2)^3 \equiv 49^3 \equiv 6^3 \equiv 36 \cdot 6 \equiv (-7) \cdot 6 \equiv -42 \equiv 1 \quad & \mod 43, \\ 6^6 \equiv (6^2)^3 \equiv 36^3 \equiv (-7)^3 \equiv 49 \cdot (-7) \equiv -42 \equiv 1 \quad & \mod 43. \end{aligned}$$

2.3 Applications du théorème chinois et de celui de Bezout

Exercice 9. Une centaine de canards forment différentes formations. D'abord ils se mettent en rangées de 3 et il y a 1 qui reste seul, ensuite ils forment des rangées de 5 mais il y a 2 laissés de côté, finalement ils se mettent en groupes de 7 et il leur manque 1 pour compléter la formation. Combien sont-ils ?

Solution 9. On note N le nombre de canards et on a $N \approx 100$ donc $0 < N < 200$. Ensuite on a :

$$\begin{aligned} N &\equiv 1 \mod 3, \\ N &\equiv 2 \mod 5, \\ N &\equiv 6 \mod 7. \end{aligned}$$

D'après le Théorème chinois il existe un unique reste modulo $3 \cdot 5 \cdot 7 = 105$ avec ces congruences. Par tâtonnement on trouve que $N \equiv 7 \mod 15$. Il faut énumérer des entiers dans la séquence 7, $7+15$, $7+2\cdot 15$, ... congruent à 6 modulo 7. On trouve que $N = 97 \mod 105$ convient. La condition $0 < N < 200$ montre que $N = 97$.

Remarque 5. En informatique on utilise un principe général selon lequel on montre que le résultat N est compris entre deux valeurs a et b. Ensuite on trouve plusieurs premiers $p_1, p_2, \ldots, p_k$ tels que $p_1 p_2 \cdot p_k > |b-a|$. Les calculs sont fait modulo chacun des premiers, de façon plus rapide qu'en travaillant avec des nombres entiers. À la fin le résultat est l'unique entier entre a et b qui correspond aux résultats trouvés en travaillant modulo p_1, ..., p_k .

Exercice 10. Factorisez 8051 avec la méthode de Fermat.

Solution 10. On essaie d'écrire $N = 8051$ comme $a^2 - b^2$. On a $90^2 = 8100$ donc on prend $a = 90$ et $b = 7$. Alors $N = a^2 - b^2 = (a-b)(a+b) = 83 \cdot 97$.

Exercice 11. On dispose de deux récipients de 5 et respectivement 7 litres. Ils peuvenent être remplis et vidés autant de fois que nécessaire à un robinet. Expliquer comment mesurer 11 litres.

Solution 11. D'après le Théorème de Bezout il existe des entiers relatifs u et v tels que $1 = 5u + 7v$. Pour rendre le Théorème de Bezout effectif on utilise l'algorithme d'Euclide : on remplit le récipient plus grand, on verse sont contenu autant que possible dans le récipient plus petit et on s'est ramené dans la situation 5 et 2

Exercice 12 (Math Prize Olympiad 2010). Montrez que pour tout entier non-nul n, il existe des entiers a et b tels que $4a^2 + 9b^2 - 1$ est divisible par n.

Solution 12. On écrit $n = k2^m$ avec k impair. Le théorème d'existence de l'inverse appliqué à 2 et k donne l'existence d'un entier u tel que $2u \equiv 1 \mod k$. Alors $(2u)^2 + (3 \cdot 0)^2 - 1$ est une solution modulo k. De nouveau le Théorème de l'existence de l'inverse appliqué à 3 et 2^m nous donne l'existence d'un entier v tel que $3v \equiv 1 \mod 2^m$, ce qui donne la solution $(2 \cdot 0)^2 - (3 \cdot v)^2 - 1$ modulo 2^m. Finalement le Théorème chinois permet de combiner la solution modulo k et 2^m pour trouver une solution modulo n.

Exercice 13 (USA 2008/1). Pour tout entier n, il existe n entiers $k_1, \ldots, k_n$ tels que $k_1 \cdots k_n - 1$ est le produit de deux entiers consécutifs.

Solution 13. Il suffit de montrer qu'il existe des entiers de la forme n^2+n+1 avec un nombre de facteurs premiers arbitrairement grand. On considère l'ensemble

$$E = \{p \text{ premier} \mid \exists t \in \mathbb{N} \text{ tel que } t^2 + t + 1 \equiv 0 \mod p\}.$$

Si E était fini on prendrait $N = \prod_{p \in E} p$ et on déduirait que $N^2 + N + 1$ a un facteur dans E, impossible.

On applique le Théorème chinois au k premiers éléments de E avec, pour $i = 1, \ldots, k$, r_i choisit tel que $r_i^2 + r_i + 1 \equiv 0$.