Stage olympique de Saint-Malo

Cours – Arithmétique

Vendredi 1 août 2003

par

François Lo Jacomo

Table des matières

1 Introduction

Quand vous avez appris l'addition et la multiplication, vous avez commencé par additionner et multiplier des entiers, puis des nombres décimaux, des nombres réels... et vous avez sans doute eu la sensation que cela revenait au même : en tant qu'opérations, l'addition des entiers ou des réels, la multiplication des entiers ou des réels se manipulent quasiment de la même manière. Et pourtant, les entiers et les réels sont deux objets mathématiques très différents. L'arithmétique, l'étude des nombres entiers, est un chapitre à part et réputé difficile des mathématiques, où certains problèmes d'apparence anodine peuvent rester des siècles sans solution.

Il est donc fondamental, quand des nombres apparaissent dans un problème, de bien voir s'il s'agit de nombres entiers ou de nombres réels, en sachant que les méthodes de résolution n'ont rien à voir et la difficulté est tout autre. Sauf lorsque cela sera précisé, les nombres qui interviennent dans ce chapitre sont des entiers relatifs (positifs, négatifs ou nuls), éléments de $\mathbb{Z}$.

Une notion joue un rôle essentiel dans l'étude des nombres entiers, et elle est dénuée de tout intérêt dans l'étude des nombres réels : la divisibilité. Un entier a est *divisible* par un entier b s'il existe un entier q tel que $a = bq$. On dit également que b *divise* a, ou que b est *diviseur* de a, et on note $b|a$.

Signalons tout de suite quelques propriétés immédiates de la divisibilité :
- tout entier $a \in \mathbb{Z}$ divise 0 et est divisible par 1 et a ;
- si $a|b$ et $b|c$, alors $a|c$;
- soit m un entier non nul, alors $a|b$ si et seulement si $ma|mb$;
- si $a|b$ et $a|c$, alors $a|bx+cy$ pour tous entiers x et y ; en particulier $a|b-c$ et $a|b+c$.

Mais on peut citer encore plus fondamental que cela : le fait qu'il n'existe pas d'entier strictement compris entre 0 et 1. Si, par exemple, b divise a et $|b| > |a|$, alors $a = 0$; sinon, en écrivant $a = bq$, le quotient $|q| = \frac{|a|}{|b|}$ serait un entier strictement compris entre 0 et 1.

Cela va nous permettre de résoudre un premier exercice :

Exercice : Trouver tous les couples d'entiers (a, b) supérieurs ou égaux à 2 tels que $ab - 1$ soit divisible par $(a-1)(b-1)$.

Solution :
► Il est clair que $ab-1 > a(b-1) > (a-1)(b-1)$. Si $ab-1$ est divisible par $(a-1)(b-1)$, l'entier q tel que $ab - 1 = q(a-1)(b-1)$ est nécessairement strictement supérieur à 1, donc au moins égal à 2. Or :

$$\frac{ab-1}{(a-1)(b-1)} < \left(\frac{a}{a-1}\right)\left(\frac{b}{b-1}\right)$$

Supposons $a \leqslant b$ (a et b jouent des rôles symétriques).

$$\frac{a}{a-1} = 1 + \frac{1}{a-1} \geqslant \frac{b}{b-1}$$

Si en outre $a \geqslant 4$, on va avoir :

$$\frac{b}{b-1} \leqslant \frac{a}{a-1} \leqslant \frac{4}{3}$$

d'où :

$$\frac{ab-1}{(a-1)(b-1)} < \left(\frac{4}{3}\right)^2 < 2$$

Donc on a nécessairement $a = 2$ ou $a = 3$.

Si $a = 2$, $\left(\frac{a}{a-1}\right)\left(\frac{b}{b-1}\right) \leqslant 2^2 = 4$, donc q ne peut valoir que 2 ou 3. Pour $q = 3$, $ab - 1 = q(a-1)(b-1)$ devient $2b - 1 = 3(b-1)$ donc $b = 2$; pour $q = 2$, on obtient $2b - 1 = 2(b-1)$ qui n'a pas de solutions.

Si $a = 3$, $\left(\frac{a}{a-1}\right)\left(\frac{b}{b-1}\right) \leqslant \left(\frac{3}{2}\right)^2 = 2,25$, donc q ne peut valoir que 2 et $ab - 1 = q(a-1)(b-1)$ devient $3b - 1 = 4(b-1)$ d'où $b = 3$.

Les seules solutions sont donc $a = b = 2$ et $a = b = 3$. ◀

Autre solution :

▶ Si $ab - 1$ est divisible par $(a-1)(b-1)$, le facteur $(a-1)$ divise lui aussi $ab - 1$. Or il divise $b(a-1)$, donc il divise la différence $(ab-1) - b(a-1) = b - 1$. Et pour la même raison $(b-1)$ divise $a(b-1)$, donc également $a - 1$. On en déduit que $a - 1 = b - 1$. En effet, de manière très générale, si q et q' sont deux entiers tels que $qq' = 1$, alors soit $q = q' = 1$, soit $q = q' = -1$; donc si x divise y et y divise x, il va exister deux entiers q et q' tels que $y = xq$ et $x = yq'$ et donc tels que $qq' = 1$, ce qui entraîne $x = y$ ou $x = -y$ (exclu en l'occurrence puisque $a - 1$ et $b - 1$ sont strictement positifs). Dès lors, $a = b$ et le problème se ramène à trouver a tel que

$$\frac{a^2-1}{(a-1)^2} = \frac{a+1}{a-1} = 1 + \frac{2}{a-1}$$

soit entier, ce qui est vérifié pour $a - 1 = 1$ et $a - 1 = 2$, et pour eux seuls. ◀

2 Division euclidienne

Les principales propriétés de la divisibilité des entiers découlent de la division euclidienne :

Théorème 1 (Division euclidienne)

Soit b un entier strictement positif. Tout entier $a \in \mathbb{Z}$ s'écrit, de manière unique, $a = bq + r$ avec $q \in \mathbb{Z}$ et $0 \leqslant r < b$.

Le *reste* r de la division euclidienne joue un rôle plus important que le *quotient* q, et le fait que r soit strictement inférieur à b est essentiel.

Pour prouver l'existence des entiers q et r, on considère la progression arithmétique $\ldots, a+2b, a+b, a, a-b, a-2b, \ldots$ et on appelle $r = a - qb$ le plus petit terme positif ou nul de la progression. Si r était supérieur ou égal à b, $r - b = a - (q+1)b$ serait un terme positif ou nul de la progression, strictement inférieur à r, ce qui contredit l'hypothèse. Quant à l'unicité, si $a = bq + r = bq' + r'$, la différence $r - r' = b(q' - q)$ est divisible par b. Or $|r - r'| < b$. Donc $r - r' = 0$, *ie* $r = r'$ et $q = q'$.

La division euclidienne permet, pour commencer, de déterminer les diviseurs communs à deux entiers a et b grâce à l'algorithme d'Euclide.

Algorithme d'Euclide

Soient $a = a_0$ et $b = a_1$ deux entiers strictement positifs tels que $b < a$. À titre d'exemple, on peut choisir $a = a_0 = 1848$ et $b = a_1 = 804$. La division euclidienne leur associe deux entiers positifs ou nuls q_1 et $a_2 < a_1$ tels que $a_0 = a_1 q_1 + a_2$. Dans notre exemple, $1848 = 804 \times 2 + 240$. Si a_2 est strictement positif (ici, $a_2 = 240$), la division euclidienne de a_1 par a_2 s'écrit $a_1 = a_2 q_2 + a_3$, avec $0 \leqslant a_3 < a_2$. Ici $804 = 240 \times 3 + 84$. Et ainsi de suite :

$$\begin{array}{lc|c} & a_2 = a_3 q_3 + q_4 & 240 = 84 \times 2 + 72 \\ & \vdots & 84 = 72 \times 1 + 12 \\ \text{jusqu'à} & a_{k-1} = a_k q_k + a_{k+1} & 72 = 12 \times 6 + 0 \end{array}$$

avec $a_{k+1} = 0$. Ceci se produit inévitablement au bout d'un nombre fini d'opérations, car les restes a_i décroissent strictement, et il n'existe qu'un nombre fini d'entiers entre 0 et a_1. Soit $d = a_k$ le dernier reste non nul. Dans notre exemple, $d = 12$. On a $a_{k-1} = a_k q_k + a_{k+1} = a_k q_k$ (puisque $a_{k+1} = 0$) donc d divise a_{k-1} : 12 divise 72. Et si d divise a_i et a_{i+1}, d divise aussi $a_{i-1} = a_i q_i + a_{i+1}$. Ici, 12 divise 72, 84, 240, 804 et 1848. L'entier d est donc un diviseur commun à $a = a_0$ et $b = a_1$.

Mais qui plus est, d est le *plus grand diviseur commun* à a et b, noté généralement $\textsc{Pgcd}\,(a, b)$ (abréviation de Plus Grand Commun Diviseur). C'est non seulement le plus grand au sens où tout autre diviseur commun strictement positif de a et b est inférieur à d, mais en outre, tout diviseur commun de a et b divise d. Cela se démontre en redescendant différemment l'algorithme d'Euclide : dans notre exemple :

$$\begin{aligned} 240 &= 1848 - 804 \times 2 = a - 2b \\ 84 &= 804 - 240 \times 3 = b - 3\,(a - 2b) = -3a + 7b \\ 72 &= 240 - 84 \times 2 = (a - 2b) - 2\,(-3a + 7b) = 7a - 16b \\ 12 &= 84 - 72 = (-3a + 7b) - (7a - 16b) = -10a + 23b \end{aligned}$$

De manière générale, si deux restes successifs de l'algorithme d'Euclide s'écrivent $a_{i-1} = u_{i-1}a + v_{i-1}b$ et $a_i = u_i a + v_i b$, le reste suivant $a_{i+1} = a_{i-1} - a_i q_i$ s'écrit bien aussi :

$$a_{i+1} = (u_{i-1} - u_i q_i)\, a + (v_{i-1} - q_i v_i)\, b = u_{i+1}a + v_{i+1}b$$

donc, de proche en proche, tous les restes de l'algorithme d'Euclide s'écrivent sous cette forme, y compris le dernier reste non nul : $d = au + bv$.

Ceci prouve simultanément deux choses : ce dernier reste non nul de l'algorithme d'Euclide est bien le plus grand diviseur commun de a et b, car tout diviseur commun de a et b divise $au + bv = d$. Mais en outre :

Théorème 2 (Bézout)

Si d est le plus grand diviseur commun de deux entiers a et b ($d = \textsc{Pgcd}\,(a, b)$), il existe deux entiers u et v tels que $d = au + bv$.

Cas particulier important : si a et b n'ont pas de diviseur commun autre que 1 et -1, on dit que a et b sont *premiers entre eux* et il existe deux entiers u et v tels que $au + bv = 1$.

Remarquons que u et v sont des entiers *a priori* quelconques ; ils ne sont pas uniques : pour tout q, on a encore $d = a(u - bq) + b(v + aq)$. Mais ils sont premiers entre eux : s'ils avaient un diviseur commun d', dd' diviserait au et bv donc $d = au + bv$, ce qui n'est possible que si $d' = 1$ ou -1. En choisissant, parmi les $(u - bq)$, le reste de la division de u par b, on peut imposer $0 \leqslant u < b$. Si b ne divise pas a (a et b strictement positifs), u est non nul, donc on a également $0 \geqslant v > -a$. En effet, d, diviseur de a, est inférieur ou égal à a donc à au. Et $au - b < 0$, or $d > 0$.

De ce théorème de Bézout découle en particulier le théorème de Gauss :

Théorème 3 (Gauss)

Si $a|bc$ et a est premier avec b, alors $a|c$.

En effet, puisque a et b sont premiers entre eux, il existe u et v tels que $au + bv = 1$. Comme a divise bc, il divise $a(uc) + (bc)v = (au + bv)c = c$.

Le théorème de Gauss dit que si a est premier avec b et avec c, alors il est premier avec le produit bc. En effet, tout diviseur d de a est premier avec b (si d et b avaient un diviseur commun, celui-ci serait diviseur commun de a et b). Si a et bc avaient un diviseur commun d, celui-ci, premier avec b, devrait diviser c, ce qui n'est pas possible car a et c sont premiers entre eux.

Nous avons là une propriété forte de la divisibilité dans $\mathbb{Z}$, il existe d'autres ensembles de nombres où la divisibilité ne vérifie pas le théorème de Gauss. Munis de ce théorème de Gauss, nous sommes maintenant bien armés pour étudier la décomposition d'un entier en facteurs premiers.

Mais avant cela, un mot de la notion de PPCM (plus petit commun multiple), qui complète utilement celle de PGCD.

PPCM et PGCD

Soient a et b deux entiers strictement positifs. Il existe deux entiers strictement positifs d et m tels que :

- d divise a et b, et tout diviseur commun de a et b divise d
- m est divisible par a et par b, et tout multiple commun de a et b est multiple de m.

d est le PGCD de a et b, et m leur PPCM (plus petit commun multiple). Ces deux entiers vérifient en outre $dm = ab$.

Nous avons déjà étudié le PGCD, il reste à prouver les propriétés du PPCM. Si n est divisible par a et par b, $n = aa' = bb'$, donc n est divisible par d, PGCD de a et b :

$$\frac{n}{d} = \frac{a}{d} \cdot a' = \frac{b}{d} \cdot b'$$

Or $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux : s'ils avaient un diviseur commun d', dd' serait diviseur commun de a et b, et d ne serait pas le PGCD. $\frac{a}{d}$ divise $\frac{b}{d} \cdot b'$ en étant premier avec $\frac{b}{d}$, donc (théorème de Gauss) $\frac{a}{d}$ divise b' : il existe q tel que $b' = \frac{a}{d} \cdot q$, ce qui entraîne $n = bb' = \frac{ab}{d} \cdot q$.

Tout multiple commun de a et b est donc multiple de $\frac{ab}{d}$, et $m = \frac{ab}{d} = a \cdot \frac{b}{d} = b \cdot \frac{a}{d}$ est bien multiple de a et de b, ce qui achève la démonstration.

Remarquons au passage que si a et b sont premiers entre eux, leur PPCM est égal à leur produit, et tout multiple commun de a et b est multiple du produit ab. Plus généralement, si $a_1, a_2, \ldots, a_k$ sont k entiers deux à deux premiers entre eux, tout multiple commun de $a_1, a_2, \ldots, a_k$ est divisible par le produit $a_1 a_2 \ldots a_k$. Cela se démontre « de proche en proche », par récurrence sur k, a_k étant premier avec $a_1 a_2 \ldots a_{k-1}$.

3 Nombres premiers

Définition 1 *Un entier naturel $p > 1$ est dit* premier *s'il a exactement deux diviseurs naturels, 1 et p.*

1 n'est pas premier ; tous les nombres premiers sauf 2 sont impairs.

Si n est un entier et p un nombre premier, soit p divise n, soit p est premier avec n. En particulier, p est premier avec tous les entiers naturels strictement inférieurs à p.

Le plus petit diviseur naturel $p > 1$ d'un entier n est obligatoirement premier : s'il admettait un diviseur strictement compris entre 1 et p, celui-ci diviserait n et p ne serait pas le plus petit diviseur de n

Théorème 4 (Décomposition en facteurs premiers)

Tout entier naturel n se décompose d'une et d'une seule manière en un produit de facteurs premiers – abstraction faite de l'ordre des facteurs.

Ce théorème fondamental se démontre en deux temps : existence de la décomposition d'une part, unicité d'autre part. L'existence est assez simple : par l'absurde, supposons qu'il existe des entiers naturels qui n'admettent pas de décomposition, et soit n le plus petit d'entre eux. Soit n n'admet pas de diviseur strictement compris entre 1 et n, et n est premier par définition. Soit il admet un diviseur d, donc $n = dq$. Les entiers d et q sont tous deux compris entre 1 et n donc tous deux admettent une décomposition en facteurs premiers (puisque n est le plus petit n'admettant pas de décomposition). Le produit de ces deux décompositions est une décomposition de n. Contradiction.

L'unicité nécessite le théorème de Gauss. Il est clair que deux nombres premiers distincts sont premiers entre eux. Supposons que n admette deux décompositions distinctes et classons les nombres premiers par ordre croissant :

$$n = p_1 p_2 \ldots p_k = p'_1 p'_2 \ldots p'_{k'}$$

avec $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$ et $p'_1 \leqslant p'_2 \leqslant \ldots \leqslant p'_{k'}$. Soit i le plus petit indice tel que $p_i \neq p'_i$. Le nombre $n' = \frac{n}{p_1 p_2 \cdots p_{i-1}} = \frac{n}{p'_1 p'_2 \cdots p'_{i-1}}$ est divisible par p_i et par p'_i. Or si $p_i < p'_i$, p_i est strictement inférieur à tous les facteurs premiers p'_j de la seconde décomposition de n' (puisque $p'_i \leqslant p'_j$ pour $i \leqslant j$), il est donc premier avec chacun de ces nombres premiers, et d'après le théorème de Gauss, il est premier avec leur produit n', ce qui contredit le fait que p_i est, dans la première décomposition, un facteur premier de n'. Il en va de même si $p'_i < p_i$.

Deux « exercices » classiques pour mettre en application le théorème de Gauss et les nombres premiers :

Exercice : Si p est un nombre premier, pour tout k strictement compris entre 0 et p, le coefficient binomial $\mathrm{C}_p^k = \frac{p!}{k!(p-k)!}$ est divisible par p.

Solution :
► Rappelons que $p! = 1 \times 2 \times \ldots \times p$, avec $0! = 1! = 1$. Les C_p^k forment le triangle de Pascal et la relation $\mathrm{C}_{p+1}^k = \mathrm{C}_p^k + \mathrm{C}_p^{k-1}$ permet de prouver qu'ils sont tous des entiers. L'important est que si p est premier, il apparaît au numérateur et pas au dénominateur, donc on ne peut pas simplifier par p. Autrement dit :

$$p! = \mathrm{C}_p^k \cdot k!\,(p-k)!$$

Or p divise $p!$ et est premier avec tous les entiers $1, \ldots, k$ (car $k < p$), ainsi qu'avec $1, \ldots, p-k$ (car $k > 0$), donc avec leur produit $k!\,(p-k)!$. Donc p divise C_p^k. ◄

Exercice : Il existe une infinité de nombre premiers.

Il s'agit en fait d'un résultat fondamental, mais qui donne lieu à tout un tas de développements pour préciser combien il existe de nombres premiers dans un intervalle donné. Les premiers résultats obtenus dans ce domaine proviennent de la décomposition en facteurs premiers de C_{2n}^n.

Mais contentons-nous de ce premier résultat qui peut être traité en exercice et néanmoins utilisé (le plus souvent implicitement) comme un théorème de cours :

Solution :
► Par l'absurde, supposons qu'il existe un nombre fini de nombres premiers $p_1, p_2, \ldots, p_k$. Le nombre $n = p_1 p_2 \ldots p_k + 1$ est premier avec chacun de nombres premiers $p_1, p_2, \ldots, p_n$: si p_i divisait n, comme p_i divise $n-1 = p_1 p_2 \ldots p_k$, p_i diviserait la différence 1. Or n admet au moins un facteur premier, qui n'appartient pas à $\{p_1, \ldots, p_k\}$ ce qui prouve que cet ensemble ne contient pas tous les nombres premiers. ◄

4 Congruences

Tout comme on distingue nombres pairs et nombres impairs ; multiples de 3, nombres de la forme $3k+1$, nombres de la forme $3k+2$; plus généralement, on peut classer les entiers en n classes modulo n, à savoir :

Définition 2 *a est* congru *à b modulo n si et seulement si $a-b$ est divisible par n, ce qui s'écrit :*

$$a \equiv b \pmod{n} \iff n \mid (a-b)$$

Il s'agit bien là d'une relation d'équivalence :
- $a \equiv a \pmod{n}$;
- si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$;
- si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$.

Les classes d'équivalence, au nombre de n, constituent un ensemble fini noté $\mathbb{Z}/n\mathbb{Z}$. Et dans cet ensemble, on peut définir des opération du fait que :

1. si $a \equiv b \pmod{n}$ et $a' \equiv b' \pmod{n}$, alors $a + a' \equiv b + b' \pmod{n}$. En effet, si n divise $a - b$ et $a' - b'$, n divise $(a + a') - (b + b') = (a - b) + (a' - b')$, ce qui permet d'additionner les classes d'équivalence :

$$\text{classe de } a + \text{classe de } b = \text{classe de } (a + b)$$

et le résultat ne dépend pas du choix de a à l'intérieur d'une même classe ni du choix du b à l'intérieur d'une même classe.

2. De même, si $a \equiv b \pmod{n}$ et $a' \equiv b' \pmod{n}$, alors $aa' \equiv bb' \pmod{n}$, car si n divise $a - b$ et $a' - b'$, n divise $aa' - bb' = a'(a - b) + b(a' - b')$.
En particulier, si $a \equiv b \pmod{n}$, $a^2 \equiv b^2 \pmod{n}$: on rappelle que $a^2 - b^2 = (a - b)(a + b)$. Plus généralement pour tout $k \geqslant 0$, $a^k \equiv b^k \pmod{n}$:

$$a^k - b^k = (a - b)\left(a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1}\right)$$

ce qu'on démontre en développant :

$$\begin{array}{rcl} a\left(a^{k-1} + a^{k-2}b + \ldots + b^{k-1}\right) & = & a^k + a^{k-1}b + \ldots + ab^{k-1} \\ - \quad b\left(a^{k-1} + \ldots + ab^{k-2} + b^{k-1}\right) & = & \quad - a^{k-1}b - \ldots - ab^{k-1} - b^k \end{array}$$

3. Il est clair en outre, que si $ma \equiv mb \pmod{n}$ et si m est premier avec n, alors $a \equiv b \pmod{n}$. Il est possible de simplifier modulo n à la condition que le nombre par lequel on simplifie soit premier avec n. En effet, si n divise $ma - mb = m(a - b)$, en étant premier avec m, n divise $a - b$, donc $a \equiv b \pmod{n}$. Cette possibilité de simplifier est à la base du lemme fondamental sur les systèmes de résidus.

Système complet de résidus

Définition 3 *Un ensemble $X = \{x_1, x_2, \ldots, x_n\}$ de n entiers est dit* système complet de résidus *modulo n si pour tout entier $x \in \mathbb{Z}$, il existe un et un seul x_k tel que $x \equiv x_k \pmod{n}$. Autrement dit si X contient un et un seul élément de chaque classe d'équivalence modulo n.*

Cette définition sert essentiellement à énoncer le lemme suivant :

Lemme 5

Si $X = \{x_1, x_2, \ldots, x_n\}$ est un système complet de résidus modulo n et si a est un entier premier avec n, alors $aX = \{ax_1, ax_2, \ldots, ax_n\}$ est un système complet de résidus modulo n.

En effet, si deux éléments de aX appartenaient à la même classe, c'est-à-dire si $ax_i \equiv ax_j \pmod{n}$, n diviserait $a(x_i - x_j)$. Or n est premier avec a donc (théorème de Gauss) n diviserait $x_i - x_j$: x_i et x_j appartiendraient à la même classe ($x_i \equiv x_j \pmod{n}$), ce qui est contraire à l'hypothèse. Comme il existe exactement n classes modulo n et n éléments de aX appartenant tous à des classes distinctes, aX contient un élément dans chaque classe modulo n.

Le principal théorème résultant de ce lemme et le (petit) théorème de Fermat :

Théorème 6 (Fermat)

Soit p un nombre premier et a un entier premier avec p (ou : non divisible par p). Alors $a^{p-1} \equiv 1 \pmod{p}$.

Il en résulte que $a^p \equiv a \pmod{p}$, *ce dernier résultat étant vrai même si a est divisible par p (donc pour tout $a \in Z$).*

Preuve :
► L'ensemble $X = \{0, 1, 2, \ldots, p-1\}$ est un système complet de résidus modulo p. Donc $aX = \{0, a, 2a, \ldots, a(p-1)\}$ est un système complet de résidus modulo p puisque a est premier avec p. Donc chaque $i \in \{1, \ldots, p-1\}$ est congru modulo p, à un $k_i a$ et un seul pour $k_i \in \{1, \ldots, p-1\}$. Le produit :

$$1 \times 2 \times \ldots \times (p-1)$$

est donc congru modulo p à :

$$a \times 2a \times \ldots \times (p-1)\, a = a^{p-1} (1 \times 2 \times \ldots \times (p-1))$$

Or $1 \times 2 \times \ldots \times (p-1)$ est premier avec p, car p est premier donc premier avec $1, 2, \ldots, p-1$. Il en résulte après simplification que 1 est congru à a^{p-1}. ◄

Remarque : Si n n'est pas premier, alors on ne peut pas simplifier par $1 \times 2 \times \ldots \times (n-1)$ qui n'est pas premier avec n. Par contre, considérons l'ensemble X' des entiers de $\{1, \ldots, n-1\}$ qui sont premiers avec n. Il y en a $\varphi(n)$, φ étant appelée la *fonction indicatrice d'Euler*.

Si x est premier avec n, ax est premier avec n puisque a est premier avec n. Donc les éléments de aX' sont dans les mêmes classes que les éléments de X' à permutation près. Autrement dit, le produit P des $x \in X'$ est congru, modulo n, au produit des ax, pour $x \in X'$, donc à $a^{\varphi(n)} P$. Comme P est premier avec n, $a^{\varphi(n)} \equiv 1 \pmod{n}$. C'est une généralisation du théorème de Fermat, toutefois moins importante que le théorème de Fermat lui-même.

Exercice : Si d est le PGCD de a et de b, montrer que $2^d - 1$ est le PGCD de $2^a - 1$ et $2^b - 1$.

Solution :
► Il est clair que, si d divise a, $2^d - 1$ divise $2^a - 1$, car $a = dq$ et :

$$2^{dq} - 1 = \left(2^d - 1\right)\left(2^{d(q-1)} + 2^{d(q-2)} + \ldots + 2^d + 1\right)$$

De même, $2^d - 1$ divise $2^b - 1$. Si a divise b ou b divise a, cela suffit à conclure. Sinon, on peut trouver deux entiers u et v, $1 \leqslant u < b$ et $1 \leqslant v < a$ tels que $d = ua - vb$, d'après une variante du théorème de Bézout. Alors :

$$2^d - 1 = (2^{ua} - 1) - 2^d \left(2^{vb} - 1\right)$$

et il est clair que tout diviseur commun de $2^a - 1$ et $2^b - 1$ divise $2^{ua} - 1$ et $2^{vb} - 1$, donc $2^d - 1$, ce qui prouve que $2^d - 1$ est le plus grand diviseur commun de $2^a - 1$ et $2^b - 1$. ◄

Exercice : Montrer que si n divise $2^n + 1$, alors n est divisible par 3.

Solution :
► Soit p le plus petit facteur premier de n. p divise 2^n+1, donc également $2^{2n}-1 = (2^n+1)(2^n-1)$. Or p divise $2^{p-1}-1$ d'après le théorème de Fermat. Donc p divise 2^d-1, d étant le PGCD de $(p-1)$ et $2n$, d'après l'exercice précédent.

Mais $p-1$ est premier avec n, puisque $p-1<p$ et p est le plus petit facteur premier de n, tout entier strictement inférieur à p est premier avec n. Donc $\text{PGCD}(p-1,2n) = \text{PGCD}(p-1,2) = 1$ ou 2. En d'autres termes, p doit divise $2^1-1=1$ ou $2^2-1=3$: seul $p=3$ convient.

De fait, 3 divise 2^3+1 et il existe une infinité de n multiples de 3 tels que n divise 2^n+1. ◄

Théorème chinois

Peut-on trouver un nombre impair, qui soit congru à 2 modulo 7 et à 17 modulo 33 ? Certes ! Ce résultat est connu de longue date des Chinois (d'où son nom), et peut s'énoncer ainsi de manière très générale :

Théorème 7

Soient $a_1, a_2, \ldots, a_k$ k entiers positifs deux à deux premiers entre eux, et $b_1, b_2, \ldots, b_k$ k entiers quelconques. Posons $A = a_1 a_2 \ldots a_k$. Il existe un et un seul entier B vérifiant : $0 \leqslant B < A$ tel que le système d'équation :

$$\begin{array}{rcll} x & \equiv & b_1 & (\text{mod } a_1) \\ x & \equiv & b_2 & (\text{mod } a_2) \\ & \vdots & & \\ x & \equiv & b_k & (\text{mod } a_k) \end{array}$$

est équivalent à $x \equiv B \pmod{A}$.

- *x congru à b_1 modulo a_1*
- *x congru à b_2 modulo a_2*

  ...
- *x congru à b_k modulo a_k*

soit équivalent à x congru à B modulo A.

À titre d'exemple $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 7$ et $x \equiv 17 \pmod{33}$ équivaut à $x \equiv 149 \pmod{462}$. Mais comment démontre-t-on ce théorème, et comment trouve-t-on B ?

Pour tout i, posons $A = a_i q_i$ (q_i est le produit de tous les a_j autres que a_i). a_i étant premier avec chaque a_j, par hypothèse, il est premier avec leur produit q_i, donc, d'après Bézout, il existe u_i et v_i tels que $u_i a_i + v_i q_i = 1$, ce qui entraîne $v_i q_i \equiv 1 \pmod{a_i}$. Par ailleurs, $v_i q_i \equiv 0 \pmod{a_j}$ pour tout a_j autre que a_i. De sorte que l'entier

$$B' = b_1 v_1 q_1 + b_2 v_2 q_2 + \ldots + b_k v_k q_k$$

est bien solution du système d'équations. Et il en va de même de tout entier $x \equiv B' \pmod A$, dont un et un seul, B, vérifie $0 \leqslant B < A$.

Réciproquement, si x et x' sont deux solutions du système d'équations, pour tout i on a $x \equiv x' \pmod{a_i}$. Il en découle que $x - x'$ est divisible par chacun des a_i, donc par leur PPCM, en l'occurrence leur produit A (puisqu'ils sont deux à deux premiers entre eux).

Dans notre exemple, on a :

$$A = 2 \times 7 \times 33 = 462$$

$$\begin{array}{rclrcrrcl} a_1 & = & 2 & q_1 & = & 231 & 116 \times 2 - 1 \times 231 & = & 1 \\ a_2 & = & 7 & q_2 & = & 66 & 19 \times 7 - 2 \times 66 & = & 1 \\ a_3 & = & 33 & q_3 & = & 14 & 3 \times 33 - 7 \times 14 & = & 1 \end{array}$$

donc :

$$B' = 1 \times (-1 \times 231) + 2 \times (-2 \times 66) + 17 \times (-7 \times 14) = -2161 = (-10 \times 231) + 149$$

ce qui entraîne $B = 149$.

Exercice : Montrer que quel que soit l'entier n strictement positif, on peut trouver n entiers strictement positifs consécutifs dont aucun n'est premier.

Solution :
► « quel que soit n » signifie ici « aussi grand que soit n », et cet exercice prouve que la distance de deux nombres premiers consécutifs peut être aussi grande que l'on veut. Cette distance de deux nombres premiers consécutifs p_k et p_{k+1} pose d'ailleurs bien des problèmes fort difficiles : il est vraisemblable qu'il existe une infinité de nombres premiers p_k tels que $p_{k+1} - p_k = 2$ (nombres premiers jumeaux), et dans l'autre sens, il est vraisemblable que cette différence $p_{k+1} - p_k$ est majorée, par exemple par une fonction du type $p_{k+1} - p_k < c_1\sqrt{p_k}$, ou même $p_{k+1} - p_k < c_2 (\ln p_k)^2$, c_1 et c_2 étant deux constantes que, suivant les démonstrations, on peut calculer ou on ne peut pas calculer... Mais indépendamment des constantes, ces résultats restent à démontrer.

Toujours est-il que $p_{k+1} - p_k$ n'est pas majoré par une constante, c'est l'objet du présent exercice : grâce au théorème chinois, c'est simple à prouver. Comme il existe une infinité de nombres premiers, choisissons en n : $p_1, p_2, \ldots, p_n$ distincts, donc deux à deux premiers entre eux. Le système d'équations :

$$\begin{array}{rcll} x & \equiv & -1 & \pmod{p_1} \\ x & \equiv & -2 & \pmod{p_2} \\ & \vdots & & \\ x & \equiv & -n & \pmod{p_n} \end{array}$$

est équivalent à $x \equiv B \pmod{A}$, avec $A = p_1 p_2 \ldots p_n$ et $0 < B < A$.

Pour tout i, $A + B + i$ est divisible par p_i, et il n'est pas égal à p_i, car il est strictement supérieur à $A = p_1 p_2 \ldots p_n$. Donc $A + B + i$ n'est pas premier. $A + B + 1, A + B + 2, \ldots, A + B + n$ sont bien n entiers strictement positifs consécutifs dont aucun n'est premier. ◄

5 Exercices

Exercice 1.
Trouver tous les triplets d'entiers strictement positifs x, y, z tels que :

$$\frac{1}{x} + \frac{2}{y} - \frac{3}{z} = 1$$

Exercice 2.
Montrer qu'il existe une infinité de nombres premiers de la forme $6n+5$.

Exercice 3.
Quel est le plus grand diviseur commun de tous les $a^{13}-a$, a prenant toutes les valeurs entières strictement positives ?

Exercice 4.
Montrer que le numérateur de la fraction :

$$1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots+\frac{1}{1333}-\frac{1}{1334}+\frac{1}{1335}$$

est divisible par 2003.

Exercice 5.
Trouver tous les couples d'entiers strictement positifs a et b tels que $\text{PPCM}\,(a,a+5)=\text{PPCM}\,(b,b+1)$.

Exercice 6.
Pour quelles valeurs de l'entier $n>0$, le nombre n^4+4^n est-il un nombre premier ?

Exercice 7 (Théorème de Wilson).
Montrer que $(p-1)!$ est congru à -1 modulo p si et seulement si p est premier.

Exercice 8.
a) Montrer (nombres de Fermat) que si 2^n+1 est premier, n est une puissance de 2. La réciproque est fausse : montrer que $2^{32}+1$ est divisible par $641=5^4+2^4=5\times 2^7+1$.

b) Montrer (nombres de Mersenne) que si 2^n-1 est premier, n est un nombre premier. La réciproque est fausse : le nombre $2^{11}-1$ est divisible par 23.

Exercice 9.
Le symbole $[x]$ désignant la partie entière de x, plus grand entier inférieur ou égal à x, calculer :

$$\left[\frac{n+1}{2}\right]+\left[\frac{n+2}{4}\right]+\left[\frac{n+4}{8}\right]+\ldots+\left[\frac{n+2^k}{2^{k+1}}\right]+\ldots$$

Exercice 10.
On construit une suite d'entiers en posant $u_0=2000^{2003}$ et pour tout $n\geqslant 0$, $u_{n+1}=u_n+7$ si u_n est impair, $u_{n+1}=\frac{u_n}{2}$ si u_n est pair.
Quel est le plus petit entier atteint par cette suite u_n ?

Exercice 11.
Trouver tous les couples d'entiers strictement positifs (x,y) tels que $7^x-3\times 2^y=1$.

Exercice 12.
Montrer que pour tout entier $n\geqslant 3$, il existe deux entiers positifs impairs x_n et y_n tels que :

$$7x_n^2+y_n^2=2^n$$

Exercice 13.
Montrer que toute progression arithmétique infinie qui contient un carré et un cube contient une puissance sixième.

6 Solution des exercices

Exercice 1.

Une condition d'existence de solutions, c'est que $\frac{1}{x} + \frac{2}{y} > 1$. Il est clair que si $x \geqslant 3$ et $y \geqslant 3$, cette condition n'est pas vérifiée. Les solutions vérifient donc $x = 1$ ou $x = 2$ ou $y = 1$ ou $y = 2$.

Pour $x = 1$, l'équation se ramène à $\frac{2}{y} = \frac{3}{z}$, qui admet une infinité de solutions : $y = 2k$, $z = 3k$. De même pour $y = 2$, l'équation se ramène à $\frac{1}{x} = \frac{3}{z}$, qui admet une infinité de solutions : $z = 3x$.

Pour $y = 1$, $\frac{3}{z} = \frac{1}{x} + 1$ donc $\frac{3}{z} > 1$, $z < 3$: $z = 1$ ne fournit pas de solution, $z = 2$ fournit la solution $x = 2$.

Pour $x = 2$, on a $\frac{2}{y} = \frac{3}{z} + \frac{1}{2}$. Ce n'est possible que si $\frac{2}{y} > \frac{1}{2}$, donc $y < 4$: hormis $y = 1$ et $y = 2$ déjà étudiés, cela fournit une solution : $y = 3$ et $z = 18$.

En définitive, les triplets solutions sont $(1, 2k, 3k)$, $(x, 2, 3x)$, $(2, 1, 2)$ et $(2, 3, 18)$.

Exercice 2.

L'idée essentielle est qu'un nombre de la forme $6n+5$ admet nécessairement un facteur premier de la forme $6n+5$. En effet, hormis 2 et 3, tous les nombres premiers sont congrus à 1 ou 5 modulo 6. Or le produit de nombres congrus à 1 modulo 6 est congru à 1 modulo 6 : un nombre congru à 5 modulo 6 est impair et non divisible par 3, et ses facteurs premiers ne peuvent pas être tous congrus à 1 modulo 6.

Par l'absurde, supposons qu'il n'existe qu'un nombre fini de nombres premiers congrus à 5 modulo 6 : $p_1, p_2, \dots p_k$. Faisons le produit $N = p_1 p_2 \dots p_k$ de ces nombres. N est congru à 1 ou 5 modulo 6, suivant que k est pair ou impair. Si N congru à 1 modulo 6, posons $N' = N + 4$, et si N congru à 5 modulo 6, posons $N' = N + 6$. Dans les deux cas, N' est congru à 5 modulo 6. Donc N' possède un facteur premier p congru à 5 modulo 6. Si p était dans l'ensemble $\{p_1, \dots, p_k\}$, N serait divisible par p et N', congru à 4 ou 6 modulo p. C'est impossible, car p ne divise pas 4 ni 6. Donc p n'est pas dans cet ensemble, et l'hypothèse qu'il existe un nombre fini de nombres premiers congrus à 5 modulo 6 conduit à une contradiction.

Exercice 3.

Le plus grand diviseur commun de tous les $a^{13} - a$ divise entre autres $2^{13} - 2 = 8190 = 2 \times 3^2 \times 5 \times 7 \times 13$. Reste à voir si tous ces facteurs premiers divisent tous les $a^{13} - a$.

$a^{13} - a = a\left(a^{12} - 1\right)$. Soit p un nombre premier. Comme p divise $a^{p-1} - 1$ pour tout a non multiple de p (théorème de Fermat), si $p - 1$ divise 12, p divise $a^{12} - 1$ pour tout a non multiple de p, donc p divise $a^{13} - a$ pour tout a, même multiple de p. Cela vaut précisément pour $p = 2$, 3, 5, 7 et 13. Reste à voir si 3^2 divise tous les $a^{13} - a$, et il est clair que ce n'est pas le cas : il suffit de choisir $a = 3$, 9 divise 3^{13} donc ne divise pas $3^{13} - 3$. Le plus grand commun diviseur de tous les $a^{13} - a$ est donc $2730 = 2 \times 3 \times 5 \times 7 \times 13$.

Exercice 4.

Avant tout, il faut savoir que 2003 est un nombre premier. Il faut transformer cette somme avant de la réduire au même dénominateur, et l'idée essentielle est de se débarrasser

des termes négatifs. On écrit :

$$\begin{aligned} S &= 1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots+\frac{1}{1333}-\frac{1}{1334}+\frac{1}{1335} \\ &= \left(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots+\frac{1}{1333}+\frac{1}{1334}+\frac{1}{1335}\right)-2\left(\frac{1}{2}+\frac{1}{4}+\ldots+\frac{1}{1334}\right) \\ &= \frac{1}{668}+\frac{1}{669}+\ldots+\frac{1}{1334}+\frac{1}{1335} \end{aligned}$$

On remarque ensuite que :

$$\frac{1}{668}+\frac{1}{1335}=\frac{2003}{668\times 1335}$$

et plus généralement :

$$\frac{1}{668+k}+\frac{1}{1335-k}=\frac{2003}{(668+k)\times(1335-k)}$$

pour tout k compris entre 0 et 333, de sorte que :

$$S=\frac{2003}{668\times 1335}+\frac{2003}{669\times 1334}+\ldots+\frac{2003}{1001\times 1002}$$

Ce qui peut s'écrire, en posant $S=\frac{p}{q}$:

$$\frac{p}{q}=2003\left(\frac{1}{668\times 1335}+\frac{1}{669\times 1334}+\ldots+\frac{1}{1001\times 1002}\right)=2003\frac{p'}{q'}$$

Il en résulte que $2003p'q=pq'$. Or 2003 est un nombre premier, il est donc premier avec tous les entiers qui lui sont inférieurs, en particulier avec tous les facteurs du dénominateur commun $q'=668\times 1335\times 669\times 1334\times\ldots\times 1001\times 1002$. D'après le théorème de Gauss, comme 2003 est premier avec q' et qu'il divise pq', il divise p, numérateur de S, ce qui achève la démonstration.

Exercice 5.

Les nombres b et $b+1$ étant premiers entre eux, $\textsc{Ppcm}\,(b,b+1)=b\,(b+1)$. Il n'en va pas de même de a et $a+5$: $\textsc{Pgcd}(a,a+5)$ divise 5, et peut donc être égal soit à 1 soit à 5, ce qui conduit à deux cas distincts.

Premier cas : a n'est pas divisible par 5, donc $\textsc{Ppcm}(a,a+5)=a(a+5)$. L'équation se ramène à $a(a+5)=b(b+1)$, soit $a^2-b^2=b-5a$. Si $b\leqslant a$, le premier membre de l'égalité serait positif et le second négatif. Donc $b>a$, $0>a^2-b^2=b-5a>-4a$. Or $a^2-b^2=(a-b)(a+b)$, avec $(a+b)>2a$. Il en résulte que $(a-b)$ ne peut être égal qu'à -1 : si $(a-b)\leqslant -2$, $(a-b)(a+b)<-4a$. Il suffit donc de remplacer a par $b-1$ pour conclure. L'équation devient $(b-1)(b+4)=b(b+1)$ soit $2b-4=0$. De fait, $a=1$ et $b=2$ fournit une solution, la seule pour laquelle a est non divisible par 5.

Deuxième cas : a est divisible par 5, donc $\textsc{Ppcm}(a,a+5)=\frac{a(a+5)}{5}$. Posons $a=5a'$, pour être sûr que la condition « a divisible par 5 » sera vérifiée par les solutions que l'on va trouver. L'équation devient $5a'(a'+1)=b(b+1)$. Soit en multipliant par 4 : $5\left((2a'+1)^2-1\right)=(2b+1)^2-1$. Si l'on pose $y=2a'+1$ et $x=2b+1$, il reste à trouver x et y impairs tels que $5y^2-x^2=4$.

$x=y=1$ convient évidemment, conduisant à $a'=b=0$, solution triviale et exclue car a et b sont supposés strictement positifs. Mais il existe une infinité d'autres solutions, car il s'agit là d'une équation d'un type classique appelée « équation de Pell-Fermat ».

L'idée est d'écrire $x^2-5y^2=\left(x+y\sqrt{5}\right)\left(x-y\sqrt{5}\right)$. Parmi les nombres réels de la forme $\left(a+b\sqrt{5}\right)$, certains sont des « unités », c'est-à-dire vérifient $\left(a+b\sqrt{5}\right)\left(a-b\sqrt{5}\right)=1$ ou -1. Notamment $\left(2+\sqrt{5}\right)\left(2-\sqrt{5}\right)=-1$. Si l'on multiplie $\left(2+\sqrt{5}\right)\left(x+y\sqrt{5}\right)=x'+y'\sqrt{5}$, on a également $\left(2-\sqrt{5}\right)\left(x-y\sqrt{5}\right)=x'-y'\sqrt{5}$, donc $x'^2-5y'^2=(-1)\left(x^2-5y^2\right)$. Ainsi, à partir d'un couple (x,y) vérifiant $x^2-5y^2=-4$, on peut en trouver un autre vérifiant $x'^2-5y'^2=4$, avec $x'=2x+5y$, $y'=x+2y$, puis un autre vérifiant $x''^2-5y''^2=-4$, avec $x''=2x'+5y'=9x+20y$, $y''=x'+2y'=4x+9y$, et une infinité d'autres par le même algorithme. On remarque que si x et y sont impairs, x'' et y'" sont eux aussi impairs.

Mais une autre remarque importante est que, par un tel algorithme, on peut, à partir d'une solution quelconque, en trouver une autre plus petite, sous certaines conditions. Si (x,y) vérifient $x^2-5y^2=-4$, $(9x-20y,4x-9y)$ vérifient la même relation, et on a $0<9x-20y<x$ sauf si $x\geqslant\frac{5}{2}y$ ou $x\leqslant\frac{20}{9}y$. Si $x\geqslant\frac{5}{2}y$, $x^2-5y^2>0$ ne peut pas être égal à -4. Par contre, si $x<\frac{20}{9}y$, $x^2-5y^2<-\frac{5}{81}y^2$ peut être égal à -4 pour peu que $y^2<4\times\frac{81}{5}$, donc que $y\leqslant 8$. On cherche à la main (ou à la machine) toutes les solutions pour lesquelles $y\leqslant 8$, en n'oubliant pas que x et y sont supposés impairs : on trouve $(1,1)$ et $(11,5)$. Toutes les autres s'y ramènent par réitération de l'algorithme ci-dessus. Comme cet algorithme peut être utilisé dans les deux sens, toutes les solutions de l'équation cherchée se déduisent de ces deux solutions-ci, mais il y en a une infinité. On peut écrire $x_k+y_k\sqrt{5}=\left(1+\sqrt{5}\right)\left(9+4\sqrt{5}\right)^k$ et ${x'}_k+{y'}_k\sqrt{5}=\left(11+5\sqrt{5}\right)\left(9+4\sqrt{5}\right)^k$, (x_k,y_k) et $({x'}_k,{y'}_k)$ sont toutes les solutions de $x^2-5y^2=-4$. Tous ces entiers sont impairs et on en déduit toutes les solutions $a_k=\frac{5}{2}(y_k-1)$, $b_k=(\frac{1}{2}(x_k-1)$, ${a'}_k=\frac{5}{2}({y'}_k-1)$, ${b'}_k=\frac{1}{2}({x'}_k-1)$, de $\textsc{Ppcm}(a,a+5)=\textsc{Ppcm}(b,b+1)$ pour lesquelles a est divisible par 5. La première d'entre elles est $a=10$, $b=5$.

Les ensembles de réels du type $a+b\sqrt{5}$ sont des anneaux d'entiers algébriques, qui possèdent un grand intérêt en arithmétique. Mais il faut prendre garde que la divisibilité ne possède pas nécessairement les mêmes propriétés dans ces ensembles que dans $\mathbb{Z}$, notamment le théorème de Gauss et l'unicité de décomposition en facteurs premiers est rarement vérifiée. Par exemple, $-4=2\times(-2)=\left(1+\sqrt{5}\right)\left(1-\sqrt{5}\right)$. L'étude de la divisibilité dans de tels ensembles a fait beaucoup progresser les mathématiques depuis le XIXème siècle.

Exercice 6.

Il est clair que n doit être impair, sinon n^4+4^n est multiple de 4. Par ailleurs, $n=1$ convient, et il est vraisemblable que c'est la seule solution : si un tel exercice admettait des solutions non triviales, il serait quasiment impossible à résoudre à la main. Mais encore faut-il le prouver.

On utilise pour cela une égalité connue sous le nom d'égalité de Sophie Germain : $x^4+4y^4=\left(x^2-2xy+2y^2\right)\left(x^2+2xy+2y^2\right)$, qui se démontre très élémentairement : $\left(x^2+2y^2\right)^2=x^4+4x^2y^2+4y^4$, donc $x^4+4y^4=\left(x^2+2y^2\right)^2-(2xy)^2$. L'entier $n^4+4^n=n^4+4\left(2^{\frac{n-1}{2}}\right)^2$ sera donc non premier, sauf si l'un des facteurs est égal à 1 ou -1. Or $\left(x^2-2xy+2y^2\right)=(x-y)^2+y^2\geqslant 0$ ne peut être égal à 1 que si l'un des carrés est nul et l'autre égal à 1, de même pour $\left(x^2+2xy+2y^2\right)=(x+y)^2+y^2$. Mais $y=2^{\frac{n-1}{2}}$ n'est jamais nul, et vaut 1 seulement pour $n=1$. Pour tout autre n, n^4+4^n est donc non premier.

Exercice 7.

Un peu moins important que le théorème de Fermat, ce théorème de Wilson s'utilise surtout dans un sens : montrer que si p est premier, $(p-1)!$ congru à -1 modulo p.

Si p est premier, p est premier avec tous les entiers non nuls qui lui sont inférieurs : d'après Bézout, si $0 < a < p$, il existe u tel que $ua + vp = 1$, u est manifestement non nul et quitte à remplacer u par $u + kp$, v par $v - ka$, on peut imposer $0 < u < p$. En d'autres termes, à tout entier a vérifiant $0 < a < p$ on peut associer un autre entier u vérifiant lui aussi $0 < u < p$ et tel que ua congru à 1 modulo p. Cet entier est unique, car ua congru à 1 congru à $u'a$ modulo p entraînerait $(u - u')a$ divisible par p. p ne divisant pas a, p doit diviser $(u-u')$, or $1-(p-1) \leqslant u-u' \leqslant (p-1)-1$: dans cet intervalle, seul 0 est multiple de p. Il en résulte également que si à a on associe u, à u on associe a. Hormis 1 et $p-1$, tous les autres entiers compris entre 1 et $p-1$ peuvent se grouper en paires $\{a, u\}$ telles que au congru à 1 modulo p. Mais peut-on avoir $u = a$? ce qui revient à dire : peut-on avoir a^2 congru à 1 modulo p ? Cela signifierait que $a^2 - 1 = (a-1)(a+1)$ est divisible par p, donc que p divise soit $a-1$ (donc $a = 1$), soit $a+1$ (donc $a = p-1$).

Il convient d'étudier séparément $p = 2$ et $p = 3$. $1! = 1$ congru à -1 modulo 2 et $2! = 2$ congru à -1 modulo 3. Pour tout autre p, les entiers strictement compris entre 0 et p se classent en trois familles : 1, $p-1$, et les autres, ces derniers se groupant en paires $\{a, u\}$ telles que au congru à 1 modulo p. Le produit de tous les entiers autres que 1 et $p-1$ est donc congru à 1 modulo p, et si je multiplie ce produit par 1 et par $p-1$, j'ai $(p-1)!$ congru à -1 modulo p. Par exemple :

$$10! = 1 \times 10 \times (2 \times 6) \times (3 \times 4) \times (5 \times 9) \times (7 \times 8)$$

(2×6), (3×4), (5×9) et (7×8) étant tous quatre congrus à 1 modulo 11, le produit est bien congru à 10 (donc à -1) modulo 11.

Si maintenant p n'est pas premier, p admet au moins un diviseur d strictement compris entre 1 et p. Posons $p = dq$. Si q n'est pas égal à d, q et d apparaissent tous deux dans $(p-1)! = 1 \times 2 \times \ldots \times (p-1)$, donc $(p-1)!$ est divisible par p. Si $q = d$, soit $d \geqslant 3$ et dans le produit $(p-1)! = 1 \times 2 \times \ldots \times (p-1)$ on trouve d et $2d$, ce qui prouve que le produit est divisible par $2d^2$, donc par $p = d^2$. Soit $d = 2$ et $3!$ congru à 2 modulo 4, ce qui achève la démonstration.

Exercice 8.

a) Supposons que n possède un diviseur impair $p > 1$, et posons $n = pq$. Comme $x^p + y^p$ est divisible par $x + y$ lorsque p est impair, $2^n + 1 = (2^q)^p + 1^p$ est divisible par $2^q + 1$, donc n'est pas premier. Pour que $2^n + 1$ soit premier, il est nécessaire que n n'admette que des diviseurs pairs, donc que n soit une puissance de 2. Mais c'est loin d'être suffisant ! Par exemple, comme l'a démontré Euler, $2^{32} + 1$ est divisible par 641. En effet, $641 = 5^4 + 2^4$ divise $2^{28}\left(5^4 + 2^4\right)$ et $641 = 5 \times 2^7 + 1$ divise $\left(5 \times 2^7\right)^4 - 1$, donc 641 divise la différence, à savoir $2^{32} + 1$. Il se peut même que les seuls nombres de Fermat premiers soient pour $n = 1$, 2, 4, 8 et 16. On en a étudié une trentaine d'autres, et aucun d'eux n'était premier (ces nombres de Fermat deviennent vite extrêmement grands).

b) Si n possède un diviseur p autre que 1 et n, posons $n = pq$. $x^p - y^p$ est divisible par $x - y$, que p soit pair ou impair. Donc $2^n - 1 = (2^q)^p - 1^p$ est non premier, car divisible par $2^q - 1$, qui n'est pas égal à 1 puisque $q > 1$. Pour que $2^n - 1$ soit premier, il est nécessaire que n soit premier. Une fois encore, c'est loin d'être suffisant $2^{11} - 1 = 23 \times 89$. Sur plusieurs centaines de milliers de nombres de Mersenne étudiés, moins de quarante sont premiers, mais il demeure probable qu'il existe une infinité de nombres de Mersenne premiers.

Exercice 9.

Il est clair que cette somme ne possède qu'un nombre fini de termes non nuls, $\left[\frac{n+2^k}{2^{k+1}}\right]$ est nul dès que $2^{k+1} > n + 2^k$, donc $2^k > n$. Cet énoncé d'Olympiade internationale se résout

facilement si l'on connaît le lemme : pour tout réel x, $[2x] = [x] + \left[x + \frac{1}{2}\right]$ qui se vérifie immédiatement : si $n \leqslant x < n + \frac{1}{2}$, $[x] = n = \left[x + \frac{1}{2}\right]$ et $[2x] = 2n$, et si $n + \frac{1}{2} \leqslant x < n + 1$, $[x] = n$, $\left[x + \frac{1}{2}\right] = n + 1$, et $[2x] = 2n + 1$. Il en résulte que :

$$\left[\frac{n + 2^k}{2^{k+1}}\right] = \left[\frac{n}{2^{k+1}} + \frac{1}{2}\right] = \left[\frac{n}{2^k}\right] - \left[\frac{n}{2^{k+1}}\right]$$

La somme s'écrit donc :

$$\left([n] - \left[\frac{n}{2}\right]\right) + \left(\left[\frac{n}{2}\right] - \left[\frac{n}{4}\right]\right) + \left(\left[\frac{n}{4}\right] - \left[\frac{n}{8}\right]\right) + \dots$$

et par « simplification téléscopique », elle vaut $[n]$, soit n si n est un entier.

Exercice 10.

Quel peut être le plus petit entier atteint par cette suite u_n ? Si $u_n > 7$, soit u_n est pair et $u_{n+1} = \frac{u_n}{2}$ est inférieur à u_n. Soit u_n est impair, $u_{n+1} = u_n + 7$ est pair, donc $u_{n+2} = \frac{u_n + 7}{2} < u_n$. Il en résulte que la plus petite valeur ne peut pas être strictement supérieure à 7. Mais elle peut être égale à 7, car si $u_n = 7$, les termes suivants sont $14, 7, 14, 7, \dots$ et la suite ne descend plus. Si $u_n = 2$, 4 ou 6, alors $u_{n+1} = \frac{u_n}{2}$ est strictement inférieur à u_n. Si $u_n = 5$, les termes suivants sont $12, 6, 3, 10, 5, 12, \dots$ et la suite descend jusqu'à 3. De même si $u_n = 3$. Enfin, si $u_n = 1$, u_n ne peut pas descendre plus bas, les termes suivants de la suite étant $8, 4, 2, 1, 8, 4, \dots$. Le plus petit entier atteint par cette suite peut être soit 1, soit 3, soit 7, tout dépend quel est le nombre de départ.

Pour atteindre 7, il faut que tous les termes de la suite soient multiples de 7, car u_{n+1} est divisible par 7 si et seulement si u_n est divisible par 7. Or il est clair que 2000^{2003} n'est pas multiple de 7 car 2000 n'est pas multiple de 7. Plus précisément, 2000 congru à 5 modulo 7, car $1995 = 7 \times 285$. 5^2 congru à 4 modulo 7, 5^3 congru à 5×4 congru à 6 modulo 7, 5^4 congru à 5×6 congru à 2 modulo 7, 5^5 congru à 5×2 congru à 3 modulo 7 et (comme permettait de le prévoir le théorème de Fermat) 5^6 congru à 5×3 congru à 1 modulo 7. Pour tout k, 5^{6k} sera donc congru à 1 modulo 7, en particulier 5^{1998} (puisque $1998 = 6 \times 333$). D'où 5^{2003} congru à 5^5 congru à 3 modulo 7, puisque $2003 = 1998 + 5$. Il en résulte que 2000^{2003} congru à 3 modulo 7.

Or l'algorithme transforme un nombre congru à 3 modulo 7 :
- s'il est impair, en un autre nombre congru à 3 modulo 7 (puisqu'on ajoute 7)
- s'il est pair, en un nombre congru à 5 modulo 7 (puisque 2×5 congru à 3 modulo 7)

Un nombre congru à 5 modulo 7 est transformé, s'il est impair, en un autre nombre congru à 5 modulo 7, et s'il est pair, en un nombre congru à 6 modulo 7. Un nombre congru à 6 modulo 7 est transformé, s'il est impair, en un autre nombre congru à 6 modulo 7, et s'il est pair, en un nombre congru à 3 modulo 7.

La boucle est bouclée : à partir d'un nombre congru à 3 modulo 7, en réitérant autant de fois que l'on veut l'algorithme, on ne peut obtenir que des nombres congrus à 5, 6 ou 3 modulo 7. On ne peut donc jamais atteindre le nombre 1 : le plus petit entier atteint par cette suite est 3.

Exercice 11.

Cette équation est plus manipulable si on l'écrit $7^x - 1 = 3 \times 2^y$, car $7^x - 1$ peut se factoriser alors que $7^x - 3 \times 2^y$, on ne peut pas en faire grand chose.

$$7^x - 1 = (7 - 1)\left(7^{x-1} + 7^{x-2} + \dots + 7 + 1\right)$$

On peut donc simplifier par 6, ce qui donne $7^{x-1} + 7^{x-2} + \ldots + 7 + 1 = 2^{y-1}$. Chacun des x termes de la somme de gauche étant impair, une première condition, si $y > 1$, est que x soit pair. Le cas $y = 1$ doit être étudié séparément, et il fournit une solution : $x = y = 1$.

Si $y > 1$ et x pair, on peut regrouper les termes deux par deux et mettre en facteur $(7 + 1)$:

$$(7 + 1)\left(7^{x-2} + 7^{x-4} + \ldots + 7^2 + 1\right) = 2^{y-1}$$

Si $y = 2$ ou $y = 3$, 2^{y-1} n'est pas divisible par $7+1$, donc il ne peut pas y avoir de solution. Si $y = 4$, on trouve une nouvelle solution : $x = 2$, $y = 4$. Pour $y > 4$, en simplifiant par 8, on est ramené à :

$$7^{x-2} + 7^{x-4} + \ldots + 7^2 + 1 = 2^{y-4}$$

Une fois encore, chacun des $\frac{x}{2}$ termes de la somme de gauche étant impair, $\frac{x}{2}$ doit être pair. On peut à nouveau regrouper les termes deux par deux, et écrire :

$$\left(7^2 + 1\right)\left(7^{x-4} + 7^{x-8} + \ldots + 7^4 + 1\right) = 2^{y-4}$$

Seulement là, le membre de gauche est divisible par $7^2 + 1 = 50$, alors que le membre de droite est une puissance de 2, il ne peut pas y avoir égalité. Les seules solutions de l'équation sont donc : $(1, 1)$ et $(2, 4)$.

Exercice 12.

Si l'on n'avait pas la condition « x_n et y_n impairs », cet exercice serait très simple : il suffirait de trouver (x_3, y_3) et (x_4, y_4), et de les multiplier par une puissance de 2 convenable. Pour $n = 3$, $7 \times 1^2 + 1^2 = 2^3$, et pour $n = 4$, $7 \times 1^2 + 3^2 = 4^2$. Donc pour $n = 2k + 3$, $7 \times \left(2^k\right)^2 + \left(2^k\right)^2 = 2^{2k+3}$ et pour $n = 2k + 4$, $7 \times \left(2^k\right)^2 + \left(3 \times 2^k\right)^2 = 2^{2k+4}$.

Mais il faut trouver des nombres impairs. Et montrer qu'ils existent, cela revient habituellement à expliciter un algorithme pour les construire. Le plus simple étant de construire x_{n+1} et y_{n+1} à partir de x_n et y_n, de sorte que :

$$7x_{n+1}^2 + y_{n+1}^2 = 2\left(7x_n^2 + y_n^2\right) \tag{1}$$

Si, à partir de deux entiers x_n et y_n impairs vérifiant $x_n^2 + y_n^2 = 2^n$, on en trouve deux autres, x_{n+1} et y_{n+1} eux aussi impairs vérifiant (1), donc vérifiant $x_{n+1}^2 + y_{n+1}^2 = 2^{n+1}$, le problème est résolu par récurrence, dans la mesure où l'hypothèse de récurrence est vérifiée pour $n = 3$ (et même $n = 4$).

La relation (1) s'obtient avec x_{n+1} et y_{n+1} de la forme :

$$\begin{aligned} x_{n+1} &= ax_n + by_n \\ y_{n+1} &= a'x_n + b'y_n \end{aligned}$$

pour peu que les quatre constantes a, b, a', b' vérifient :

$$\begin{aligned} 7a^2 + a'^2 &= 14 \\ 14ab + 2a'b' &= 0 \\ 7b^2 + b'^2 &= 2 \end{aligned}$$

Nous n'avons pas à résoudre ce système d'équations dans sa généralité, il suffit d'une solution particulière quelle que soit la manière de la trouver. La première équation suggère

un a' multiple de 7, et les deux autres si $a' = 7b$, $b' = -a$, sous réserve que $a^2 + 7b^2 = 2$, donc par exemple que $a = b = \frac{1}{2}$, ou $a = \frac{1}{2}$, $b = -\frac{1}{2}$. En d'autres termes :

$$7\left(\frac{x_n + y_n}{2}\right)^2 + \left(\frac{7x_n - y_n}{2}\right)^2 = 2\left(7x_n^2 + y_n^2\right)$$

tout comme :

$$7\left(\frac{x_n - y_n}{2}\right)^2 + \left(\frac{7x_n + y_n}{2}\right)^2 = 2\left(7x_n^2 + y_n^2\right)$$

Il reste à voir si, dans l'hypothèse où x_n et y_n sont des entiers impairs, $\frac{x_n+y_n}{2}$ et $\frac{7x_n-y_n}{2}$ (respectivement $\frac{x_n-y_n}{2}$ et $\frac{7x_n+y_n}{2}$) sont eux aussi des entiers impairs. $\frac{x_n+y_n}{2}$ et $\frac{x_n-y_n}{2}$ sont manifestement entiers, mais pas de même parité, car leur somme, x_n, est par hypothèse impaire. L'un d'eux est donc impair. Or $\frac{x_n-y_n}{2}$ et $\frac{7x_n+y_n}{2}$ ont pour somme $4x_n$, qui est pair, donc ils sont de même parité. Tout comme $\frac{x_n+y_n}{2}$ et $\frac{7x_n-y_n}{2}$ qui, eux aussi, ont pour somme $4x_n$ et sont donc de même parité. Si $\frac{x_n-y_n}{2}$ est impair, on pose $x_{n+1} = \frac{x_n-y_n}{2}$, $y_{n+1} = \frac{7x_n+y_n}{2}$, sinon on pose $x_{n+1} = \frac{x_n+y_n}{2}$, $y_{n+1} = \frac{7x_n-y_n}{2}$: dans les deux cas, x_{n+1} et y_{n+1} sont des entiers impairs, ce qui achève la démonstration. Notons que si l'un des entiers ainsi obtenus était négatif, il suffirait d'en prendre la valeur absolue.

Remarque : Mais cet exercice donne l'occasion de présenter un domaine important des mathématiques. On étudie souvent les sommes de deux carrés, en remarquant que le produit de deux sommes de deux carrés est une somme de deux carrés :

$$\left(a^2 + b^2\right)\left(a'^2 + b'^2\right) = \left(aa' - bb'\right)^2 + \left(ab' + ba'\right)^2$$

On justifie ceci en introduisant les entiers Gauss $a + ib$, nombres complexes, où a et b sont entiers et $i^2 = -1$. Il en résulte que $(a + ib)(a - ib) = a^2 + b^2$, que l'on note $|a + ib|^2$, et l'on a :

$$\left|(a + ib)(a' + ib')\right| = |a + ib|\left|a' + ib'\right|$$

ce qui conduit à la relation ci-dessus. Le fait que dans cet ensemble des entiers de Gauss on puisse définir une division euclidienne comme dans $\mathbb{Z}$ permet d'y définir une décomposition en facteurs premiers comme dans $\mathbb{Z}$ et, par exemple, de démontrer que tout nombre premier congru à 1 modulo 4 est somme de deux carrés.

Or cet anneau des entiers de Gauss n'est pas le seul qui mérite d'être étudié, du point de vue de la divisibilité. Nous avons affaire ici à l'anneau des « entiers algébriques » de la forme $\frac{a+ib\sqrt{7}}{2}$, a et b étant de même parité, qui lui aussi possède une division euclidienne et donc une unicité de décomposition en facteurs premiers (ce qui est assez rare dans ce type d'anneaux). Pourquoi le dénominateur 2 ? Cela n'empêche pas ces nombres d'être des entiers algébriques, dans la mesure où un entier algébrique est un nombre (réel ou complexe) racine d'une équation à coefficients entiers, dont le premier coefficient vaut 1. Or $\frac{a+ib\sqrt{7}}{2}$ est racine de $x^2 - ax + \frac{a^2+7b^2}{4}$, et si a et b sont de même parité, a^2 congru à b^2 modulo 4 et le dernier coefficient : $\frac{a^2+7b^2}{4}$ est bien entier. La somme et le produit de deux entiers algébriques étant un entier algébrique, cela justifie que l'on travaille avec cet ensemble, car sans ce dénominateur 2 il manquerait des entiers dans l'ensemble considéré et l'on n'aurait plus les propriétés de division euclidienne et unicité de la décomposition en facteurs premiers.

Si l'on pose :

$$u_n + iv_n\sqrt{7} = 2\left(\frac{1 + i\sqrt{7}}{2}\right)^n$$

il est clair que

$$u_n^2 + 7v_n^2 = \left(u_n + iv_n\sqrt{7}\right)\left(u_n - iv_n\sqrt{7}\right) = 4\left(\frac{1+i\sqrt{7}}{2}\right)^n\left(\frac{1-i\sqrt{7}}{2}\right)^n = 2^{n+2}$$

Comme $\left(\frac{1+i\sqrt{7}}{2}\right)^n$ est entier algébrique, donc de la forme $\frac{a+ib\sqrt{7}}{2}$, en multipliant par 2 ou trouve des u_n et v_n entiers. Et l'unicité de décomposition en facteurs premiers prouve qu'ils sont impairs, mais c'est beaucoup plus que ce que demande le présent exercice. Toujours est-il qu'on a là une expression générale des x_n et y_n cherchés :

$$x_n = |v_{n-2}| \quad \text{et} \quad y_n = |u_{n-2}|$$

avec $u_n + iv_n\sqrt{7} = 2\left(\frac{1+i\sqrt{7}}{2}\right)^n$.

Exercice 13.

Ce problème a été proposé aux Olympiades Internationales 1997, mais il est plus difficile que les problèmes d'arithmétique habituellement posés aux Olympiades.

La première question, c'est le sens à donner à « progression arithmétique infinie ». Si elle est infinie dans les deux sens, c'est l'ensemble des entiers congrus à b modulo a, a étant la raison de la progression arithmétique. Si elle n'est infinie que dans un sens, c'est l'ensemble des $ak + b$ avec k entier positif. Mais cela ne change pas grand chose, car si x^6 congru à b modulo a, tous les $(x + qa)^6$ sont eux aussi congrus à b modulo a, et parmi eux, en prenant q positif suffisamment grand, on en trouve nécessairement de la forme $ak + b$ avec k positif. On supposera donc désormais que la progression arithmétique infinie est l'ensemble des entiers congrus à b modulo a.

Supposons donc qu'il existe des entiers x et y tels que x^2 congru à b modulo a et y^3 congru à b modulo a. Alors x^6 congru à b^3 modulo a et y^6 congru à b^2 modulo a. Si y est premier avec a (ce qui équivaut à : si b premier avec a, car tout nombre premier divisant b et a divise y, et tout diviseur commun de y et a divise b), d'après Bézout il existe u tel que uy congru à 1 modulo a, donc $u^6y^6x^6$ congru à b^3 modulo a, soit : $(ux)^6$ congru à b modulo a, et le problème est résolu... dans ce premier cas.

Mais la difficulté, c'est lorsque b et a ne sont pas premiers entre eux. Et une idée astucieuse est de construire une récurrence sur a. L'hypothèse de récurrence s'énonce ainsi : si une progression arithmétique infinie de raison $a \leqslant n$ contient un carré et un cube, elle contient une puissance sixième. Pour $n = 1$, c'est évident, car la seule progression arithmétique infinie de raison 1, c'est $\mathbb{Z}$ tout entier, qui contient toutes les puissances sixièmes. C'est presque aussi évident pour $n = 2$. Supposons que ce soit vrai pour n, et montrons que si une progression arithmétique infinie de raison $a = n + 1$ contient un carré et un cube, elle contient une puissance sixième. En se limitant au cas où b et a ne sont pas premiers entre eux : appelons d leur PGCD et p un facteur premier de d, p^i étant la plus grande puissance de p divisant d. Deux cas à envisager : soit p ne divise pas $\frac{a}{d}$, soit p ne divise pas $\frac{b}{d}$, car si p divise $\frac{a}{d}$ et $\frac{b}{d}$, d n'est pas le PGCD de a et b.

Si p ne divise pas $\frac{a}{d}$, les congruences x^2 congru à b modulo a et y^3 congru à b modulo a entraînent, a fortiori x^2 congru à b modulo $\frac{a}{p^i}$ et y^3 congru à b modulo $\frac{a}{p^i}$. Mais $\frac{a}{p^i} \leqslant n$, donc, d'après l'hypothèse de récurrence, il existe z tel que z^6 congru à b modulo $\frac{a}{p^i}$. Et d'après le théorème chinois, il existe t tel que :

$$\begin{aligned} t &\equiv z \pmod{\tfrac{a}{p^i}} \\ t &\equiv 0 \pmod{p^i} \end{aligned}$$

puisque p^i est premier avec $\frac{a}{p^i}$. Il en résulte :

$$\begin{array}{rcccl} t^6 & \equiv & z^6 & \equiv & b \quad (\mathrm{mod}\ \frac{a}{p^i}) \\ t^6 & \equiv & 0 & \equiv & b \quad (\mathrm{mod}\ p^i) \end{array}$$

puisque b est divisible par d, donc par p^i. $\left(t^6 - b\right)$ est divisible par $\frac{a}{p^i}$ et par p^i, donc par a puisque $\frac{a}{p^i}$ est premier avec p : il existe bien une puissance sixième congrue à b modulo a.

Si p divise $\frac{a}{d}$ mais ne divise pas $\frac{b}{d}$, p^{i+1} divise a mais pas b, donc tous les termes $ak+b$ de la progression arithmétique sont divisibles par d donc par p^i, mais aucun n'est divisible par p^{i+1}. En particulier, la plus grande puissance de p divisant x^2 est p^i (ce qui prouve que i est pair), et la plus grande puissance de p divisant y^3 est également p^i (ce qui prouve que i est divisible par 3). L'entier i est donc multiple de 6 : $i = 6j$. Et l'on a x divisible par p^{3j} : $x^2 - b$ étant divisible par a, $\left(\frac{x}{p^{3j}}\right)^2 - \left(\frac{b}{p^{6j}}\right)$ est divisible par $\frac{a}{p^{6j}}$. De même, y est divisible par p^{2j}, et $\left(\frac{y}{p^{2j}}\right)^3$ congru à $\frac{b}{p^{6j}}$ modulo $\frac{a}{p^{6j}}$. Comme $\frac{a}{p^{6j}} \leqslant n$, l'hypothèse de récurrence s'applique : il existe z tel que z^6 congru à $\frac{b}{p^{6j}}$ modulo $\frac{a}{p^{6j}}$. Si la différence $z^6 - \frac{b}{p^{6j}}$ est divisible par $\frac{a}{p^{6j}}$, le nombre $\left(zp^j\right)^6 - b$ est divisible par a, on a donc trouvé une puissance sixième, $\left(zp^j\right)^6$, congrue à b modulo a, ce qui achève la démonstration.