Arithmétique

Marc SAGE

1^{ier} juillet 2008

Table des matières

Les pgcd et ppcm de deux entiers a et b seront notés

$$\begin{cases} a \wedge b := \mathrm{pgcd}\,(a,b) \\ a \vee b := \mathrm{ppcm}\,(a,b) \end{cases}.$$

Pour un entier $n \geq 2$ et p un nombre premier, on rappelle que la *valuation* p-adique, notée $v_p(n)$, est la puissance de p qui apparaît dans la décomposition de n en facteurs premiers, de sorte que tout entier s'écrit

$$n = \prod_{p \text{ premier}} p^{v_p(n)}.$$

Pour p premier, le corps[1] à p éléments sera noté

$$\mathbb{F}_p := \mathbb{Z}/_{p\mathbb{Z}}.$$

On rappelle également le principe de la *descente infinie*, dû à Fermat : pour montrer qu'une équation n'a pas de solutions, on associe à toute solution s un certain entier $n(s) \in \mathbb{N}$, et on montre qu'à partir d'une solution s l'on peut construire une solution s' telle que $n(s') < n(s)$. On obtient ainsi par récurrence une suite strictement décroissante d'entiers naturels, ce qui est impossible. On peut aussi considérer par l'absurde une solution s minimisant $n(s)$ et contredire la minimalité de $n(s)$, ce qui revient exactement au même.

1 Mise en jambe

1. *Soit $n \geq 2$ un entier. Parmi n entiers, montrer que l'on peut toujours en choisir dont la somme est multiple de n.*
2. *Soit un nombre entier x de six chiffres divisible par 13, mettons $x = abcdef$ en base 10. Montrer que $bcdefa$ est aussi divisible par 13.*
3. *En notant $\tau(n)$ le nombre de diviseurs d'un entier $n \geq 1$, montrer l'identité*

$$\prod_{d|n} d = \sqrt{n}^{\tau(n)}.$$

Solution proposée.

1. Il s'agit là d'une application du principe des tiroirs. Nous pouvons former n tiroirs correspondant chacun à un reste possible modulo n. Identifions alors toutes les sommes que l'on peut former à des chaussettes et rangeons chaque chaussette dans le tiroir correspondant. Comme il y a $2^n - 1 > n$ sommes possibles, un tiroir contient deux chaussettes, donc la différence des deux sommes correspondantes est multiple de n. Mais des coefficients négatifs peuvent apparaître. Pour pallier ce problème, on ne regarde que les sommes associées à des parties *croissantes* de notre ensemble $\{a_1, ..., a_n\}$ d'entiers. On peut en trouver n, par exemple les $a_1 + ... + a_k$ pour $1 \leq k \leq n$. Si deux chaussettes sont dans un même tiroir, c'est fini par ce qui précède. Sinon, chacun des n tiroirs contient au plus une chaussette, mais comme il y a n chaussettes, le tiroir numéro n en contient une, *CQFD*.
2. Notons $y = bcdefa$. Exprimons y en fonction de x modulo 13 (sachant que $x \equiv 0$ par hypothèse) :

$$y = 10x - 10^6 a + a \equiv \left(1 - 10^6\right) a.$$

Il suffit donc de montrer que $10^6 = 1$ modulo 13 :

$$10^6 \equiv (-3)^{3\times 2} = \left(3^3\right)^2 = 27^2 \equiv 1^2 = 1, \text{ } \textit{CQFD}.$$

[1] Le terme mathématique "corps" se dit "**f**ield" en anglais, d'où la lettre $\mathbb{F}$ choisie pour $\mathbb{F}_p$.

3. L'idée est de faire intervenir la bijection $d \mapsto \frac{n}{d}$ de l'ensemble des diviseurs de n, laquelle sépare ce dernier en les diviseurs $< \sqrt{n}$ (il y en a $\frac{\tau(n)}{2}$, moins 1 si n est un carré), ceux $> \sqrt{n}$ (idem) et éventuellement $\sqrt{n}$.

Si n n'est pas un carré, on obtient ainsi

$$\prod_{d|n} d = \prod_{d|n,\ d<\sqrt{n}} d \prod_{d|n,\ d>\sqrt{n}} d = \prod_{d|n,\ d<\sqrt{n}} d \prod_{d|n,\ d<\sqrt{n}} \frac{n}{d} = \prod_{d|n,\ d<\sqrt{n}} d \cdot \frac{n}{d} = n^{\frac{\tau(n)}{2}} = \sqrt{n}^{\tau(n)},$$

et pour n impair on a de même

$$\prod_{d|n} d = \sqrt{n} \prod_{d|n,\ d<\sqrt{n}} d \cdot \frac{n}{d} = \sqrt{n} n^{\frac{\tau(n)-1}{2}} = \sqrt{n}^{\tau(n)}.$$

2 Une identité à connaître sur l'indicatrice d'Euler

Pour n un entier ≥ 1, on note $\varphi(n)$ le nombre d'entiers parmi $\{1, ..., n\}$ qui sont premiers avec n. φ est appelée *indicatrice d'Euler*. On rappelle que φ peut être définie par[2]

$$\left\{ \begin{array}{c} \varphi(1) = 1 \\ \varphi\left(p^{\beta}\right) = p^{\beta} - p^{\beta-1} \text{ si } p \text{ est premier et } \beta \geq 1 \\ \varphi(ab) = \varphi(a)\varphi(b) \text{ si } a \text{ et } b \text{ sont premiers entre eux} \end{array} \right. .$$

Montrer que pour tout entier $n \geq 1$ on a

$$\sum_{d|n} \varphi(d) = n.$$

Solution proposée.

Première méthode (brutale).

Cassons $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ en produit de facteurs premiers (avec $r = 0$ si $n = 1$). On calcule comme une brute en utilisant les propriétés de φ rappelées plus haut :

$$\begin{aligned} \sum_{d|n} \varphi(d) &= \sum_{\substack{d=\prod_{i=1}^{r} p_i^{\beta_i} \\ 0\leq\beta_1\leq\alpha_1 \\ \cdots \\ 0\leq\beta_r\leq\alpha_r}} \varphi(d) = \sum_{\substack{0\leq\beta_1\leq\alpha_1 \\ \cdots \\ 0\leq\beta_r\leq\alpha_r}} \varphi\left(\prod_{i=1}^{r} p_i^{\beta_i}\right) = \sum_{\substack{0\leq\beta_1\leq\alpha_1 \\ \cdots \\ 0\leq\beta_r\leq\alpha_r}} \prod_{i=1}^{r} \varphi\left(p_i^{\beta_i}\right) = \prod_{i=1}^{r} \sum_{0\leq\beta\leq\alpha_i} \varphi\left(p_i^{\beta}\right) \\ &= \prod_{i=1}^{r} \left(\sum_{\beta=1}^{\alpha_i} \left(p_i^{\beta} - p_i^{\beta-1}\right) + 1 \right) = \prod_{i=1}^{r} \left(\left(p_i^{\alpha_i} - 1\right) + 1\right) = \prod_{i=1}^{r} p_i^{\alpha_i} = n. \end{aligned}$$

Deuxième méthode (moins brutale).

Raisonnons par récurrence sur le nombre r de facteurs premiers de n.

Pour $r = 1$, $n = p^{\alpha}$, donc

$$\sum_{d|n} \varphi(d) = \sum_{\beta=0}^{\alpha} \varphi\left(p^{\beta}\right) = \sum_{\beta=1}^{\alpha} \left(p^{\beta} - p^{\beta-1}\right) + 1 = (p^{\alpha} - 1) + 1 = n.$$

[2]En fait, la bonne définition de $\varphi(n)$ est le cardinal $\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}\right|$ des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Sa multiplicativité résulte alors immédiatement du théorème chinois.

Pour la suite, soit $n = p^a m$ où $p \wedge m = 1$. Alors

$$\sum_{d|n} \varphi(d) = \sum_{\substack{d|m \\ d'|p^\alpha}} \varphi(dd') = \sum_{\substack{d|m \\ d'|p^\alpha}} \varphi(d)\varphi(d') = \sum_{d|m} \varphi(d) \sum_{d|p^\alpha} \varphi(d') = mp^\alpha = n$$

en appliquant les cas 1 et $r-1$.

En fait, on a fait le même calcul que lors de la méthode brutale, sauf que la récurrence nous a épargné les signes et conditions multiples peu agréables à se coltiner.

Troisième méthode (dénombrement).

On observe qu'une fraction $\frac{k}{n}$ où $1 \leq k \leq n$ se met sous forme irréductible $\frac{a}{d}$ ssi a est premier avec d (et bien sûr $1 \leq a \leq d$). À d fixé, il y a donc exactement $\varphi(d)$ fractions $\frac{k}{n}$ dont la réduite a pour dénominateur d. Comme il y a n telle fractions en tout, on en déduit le résultat. Ploum.

3 Formule de Legendre et deux applications

Démontrer la formule de Legendre[3]*, qui donne la valuation p-adique d'une factorielle :*

$$v_p(n!) = \sum_{v \geq 1} \left\lfloor \frac{n}{p^v} \right\rfloor.$$

Montrer, en notant $S_p(n)$ la somme des chiffres de n en base p, que cette quantité vaut également

$$v_p(n!) = \frac{n - S_p(n)}{p-1}.$$

Solution proposée.

On regarde à p fixé la contribution en p de chaque entier compris entre 2 et n. Pour un entier $v \geq 1$, notons $\mathcal{M}_v$ les multiples de p^v dans $\{1, ..., n\}$ et $m_v = \#\mathcal{M}_v$ le nombre de tels multiples.

Il y a déjà les multiples de p qui apportent chacun une contribution de 1. Puis les multiples de p^2 apportent chacun un facteur 2 dans le calcul de $v_p(n!)$, mais on a déjà compté en partie leur contribution dans les multiples de p, de sorte que la contribution supplémentaire de $\mathcal{M}_2$ est en fait de 1 pour chacun de ces multiples. Ainsi de suite, chaque multiple de p^{v+1} contribue de $v+1$, mais la partie v a déjà été comptée dans la contribution de $\mathcal{M}_v$, ce qui donne au final une contribution de 1 pour tous les multiples. Ainsi :

$$v_p(n!) = \sum_{v \geq 1} m_v.$$

Si l'on n'est pas convaincu, en notant a_v le nombre d'entiers de $\{1, ..., n\}$ de valuation v, il est clair que $v_p(n!) = \sum_{v \geq 1} v a_v$, ce que l'on peut réécrire sous la forme

$$\begin{aligned} a_1 + 2a_2 + 3a_3 + 4a_4 + ... &= (a_1 + a_2 + a_3 + a_4 + ...) + \\ &\quad (a_2 + a_3 + a_4 + ...) + \\ &\quad (a_3 + a_4 + ...) + \\ &\quad (a_4 + ...) + ... \end{aligned}$$

Maintenant, $\sum_{i \geq v} a_i$ compte les entiers de $\{1, ..., n\}$ dont la valuation est $\geq v$, *i.e.* les multiples de p^v, d'où $\sum_{i \geq v} a_i = m_v$.

Il reste à calculer m_v. Or, ce dernier vérifie

$$m_v p^v \leq n < (m_v + 1) p^v \iff m_v \leq \frac{n}{p^v} < m_v + 1 \iff m_v = \left\lfloor \frac{n}{p^v} \right\rfloor.$$

[3]On a noté $\lfloor x \rfloor$ la *partie entière* d'un réel x, qui rappelons-le est caractérisée par l'encadrement

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

Quant à la seconde formule, plus anecdotique (il faut le dire), écrivons $n = a_N a_{N-1}...a_1 a_0$ en base p, de sorte que $\left\lfloor \frac{n}{p^v} \right\rfloor = a_N a_{N-1}...a_{v+1} a_v$ (raisonner comme en base dix où diviser par 10^v revient à déplacer la virgule de v places vers la gauche). Il en résulte

$$\begin{aligned}
v_p(n!) = \sum_{v \geq 1} \left\lfloor \frac{n}{p^v} \right\rfloor &= \left(a_1 + a_2 p + a_3 p^2 + a_4 p^3 + ...\right) + \\
&\quad \left(a_2 + a_3 p + a_4 p^2 + ...\right) + \\
&\quad (a_3 + a_4 p + ...) + \\
&\quad (a_4 + ...) + ... \\
&= a_1 + a_2(p+1) + a_3\left(p^2 + p + 1\right) + a_4\left(p^3 + p^2 + p + 1\right) + ... \\
&= a_1 \frac{p-1}{p-1} + a_2 \frac{p^2-1}{p-1} + a_3 \frac{p^3-1}{p-1} + a_4 \frac{p^4-1}{p-1} + ... \\
&= \frac{a_1 p + a_2 p^2 + a_3 p^3 + ... - (a_1 + a_2 + a_3 + ...)}{p-1} \\
&= \frac{(n - a_0) - (S_p(n) - a_0)}{p-1}, \textit{ CQFD.}
\end{aligned}$$

Application 1. *Par combien de zéros se termine* 100! *?*

Solution proposée.

Le nombre de zéros est la puissance maximale de 10 qui apparaît dans le produit 100!. Puisque les 2 apparaissent plus souvent que les 5, on recherche la puissance maximale de 5 dans 100!, *i.e.* la valuation 5-adique de 100!. On applique Legendre :

$$v_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor + 0 = 20 + 4 = 24.$$

Application 2. *Pour des entiers $a, b \geq 1$, montrer que $\binom{a+b}{a}$ divise $\binom{2a}{a}\binom{2b}{b}$.*

Solution proposée.

Il s'agit de montrer l'intégralité du quotient

$$\frac{\binom{2a}{a}\binom{2b}{b}}{\binom{a+b}{a}} = \frac{(2a)!\,(2b)!}{a!b!\,(a+b)!},$$

donc de montrer que la valuation p-adique du numérateur est plus grande que celle du dénominateur pour tout p premier, *i.e.* (en utilisant Legendre)

$$\begin{aligned}
& v_p((2a)!) + v_p((2b)!) \overset{?}{\geq} v_p(a!) + v_p(b!) + v_p((a+b)!) \\
\iff & \sum_{v \geq 1} \left\lfloor \frac{2a}{p^v} \right\rfloor + \sum_{v \geq 1} \left\lfloor \frac{2a}{p^v} \right\rfloor \overset{?}{\geq} \sum_{v \geq 1} \left\lfloor \frac{a}{p^v} \right\rfloor + \sum_{v \geq 1} \left\lfloor \frac{b}{p^v} \right\rfloor + \sum_{v \geq 1} \left\lfloor \frac{a+b}{p^v} \right\rfloor \\
\iff & \sum_{v \geq 1} \left\lfloor \frac{2a}{p^v} \right\rfloor + \left\lfloor \frac{2a}{p^v} \right\rfloor \overset{?}{\geq} \sum_{v \geq 1} \left\lfloor \frac{a}{p^v} \right\rfloor + \left\lfloor \frac{b}{p^v} \right\rfloor + \left\lfloor \frac{a+b}{p^v} \right\rfloor.
\end{aligned}$$

Il suffit donc de montrer que

$$\left\lfloor \frac{2a}{p^v} \right\rfloor + \left\lfloor \frac{2a}{p^v} \right\rfloor \overset{?}{\geq} \left\lfloor \frac{a}{p^v} \right\rfloor + \left\lfloor \frac{b}{p^v} \right\rfloor + \left\lfloor \frac{a+b}{p^v} \right\rfloor.$$

Simplifions déjà en effectuant une division euclidienne de a et b par p^v : $\left\{ \begin{array}{l} a = a'p^v + \alpha \\ b = b'p^v + \beta \end{array} \right.$. On veut donc

$$\begin{aligned}
2a' + \left\lfloor \frac{2\alpha}{p^v} \right\rfloor + 2b' + \left\lfloor \frac{2\beta}{p^v} \right\rfloor &\overset{?}{\geq} a' + b' + (a' + b') + \left\lfloor \frac{\alpha+\beta}{p^v} \right\rfloor \\
\iff \left\lfloor \frac{2\alpha}{p^v} \right\rfloor + \left\lfloor \frac{2\beta}{p^v} \right\rfloor &\overset{?}{\geq} \left\lfloor \frac{\alpha+\beta}{p^v} \right\rfloor.
\end{aligned}$$

Si l'on montre que, pour tous réels positifs x, y,

$$\lfloor 2x \rfloor + \lfloor 2y \rfloor \geq \lfloor x+y \rfloor ,$$

on aura gagné. Or, si par exemple $x \geq y$, on a $2x \geq x+y$, d'où $\lfloor 2x \rfloor \geq \lfloor x+y \rfloor$ et le résultat vu que $\lfloor 2y \rfloor \geq 0$.

4 Une équation diophantienne

Résoudre pour des entiers $a, b \geq 1$ l'équation $a^b = b^a$.

Solution proposée.

Première méthode (arithmétique).
On peut supposer $a \leq b$ par symétrie, et même $a \geq 2$ vu que

$$a = 1 \implies 1^b = b^1 \implies (a,b) = (1,1)$$

qui est clairement solution. On se ramène à des entiers premiers entre eux en posant $\left\{ \begin{array}{l} a = \delta\alpha \\ b = \delta\beta \end{array} \right.$ avec $\left\{ \begin{array}{l} \alpha \wedge \beta = 1 \\ \delta = a \wedge b \end{array} \right.$ et $\alpha \leq \beta$. On obtient :

$$\begin{aligned} \delta^b \alpha^b = \delta^a \beta^a \quad & \implies \quad \beta^a \mid \delta^{b-a} \alpha^b \implies \beta^a \mid \delta^{b-a} \implies \beta^a \leq \delta^{b-a} \implies a^b = b^a = \delta^a \beta^a \leq \delta^b \\ & \implies \quad a \leq \delta \implies \alpha = \frac{a}{\delta} \leq 1 \implies \alpha = 1 \implies a \mid b. \end{aligned}$$

On peut donc écrire $b = ka$ avec $k \in \mathbb{N}^*$. L'équation se réécrit

$$b^a = a^b = a^{ka} = \left(a^k\right)^a \iff b = a^k \iff ka = a^k \iff k = a^{k-1}.$$

On voit que, pour k grand, la puissance à droite écrase le terme de gauche. Précisément, dès que $k \geq 2$ on a $2^k \geq 2k$, donc

$$k = a^{k-1} \geq 2^{k-1} \geq k \implies a = 2 \text{ et } k = 2.$$

Les solutions sont donc les couples (a,a) pour $a \geq 1$ (correspondant à $k = 1$), $(2,4)$ et $(4,2)$.

Seconde méthode (analytique).
En passant au logarithme, l'équation se réécrit

$$\frac{\ln a}{a} = \frac{\ln b}{b}.$$

Il est donc judicieux d'étudier la fonction $f : \left\{ \begin{array}{ccc} [1,\infty[& \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{\ln x}{x} \end{array} \right.$. On cherche les droites horizontales coupant le graphe de f en au moins deux points d'abscisses entières (les couples $a = b$ étant trivialement solutions du problème).

Une dérivation donne $f'(x) = \frac{\frac{1}{x} x - \ln x}{x^2}$ qui est du signe de $1 - \ln x$, *i.e.* de $e - x$. On en déduit que f est strictement croissante sur $[1,e]$ et strictement décroissante sur $[e,\infty[$.

Ainsi, si une droite horizontale coupe le graphe de f en $\begin{pmatrix} u \\ f(u) \end{pmatrix}$ et $\begin{pmatrix} v \\ f(v) \end{pmatrix}$ avec $u < v$ entiers, alors u est nécessairement plus petit que e, ce qui impose $u = 1$ ou 2 :

- $u = 1 \implies 0 = \dfrac{\ln u}{u} = \dfrac{\ln v}{v} \implies v = 1\,;$
- $u = 2 \implies \dfrac{\ln 2}{2} = \dfrac{\ln v}{v} \implies 2^v = v^2 \implies v = 2 \text{ ou } 4.$

Finalement, les solutions sont les (a,a) pour $a \geq 1$, $(2,4)$ et $(4,2)$.

5 Équation de Pythagore

On demande de résoudre l'équation en les entiers $x, y, z \geq 1$:

$$x^2 + y^2 = z^2.$$

Solution proposée.

Commençons par quelques simplifications préliminaires.

Quitte à diviser par le pgcd $x \wedge y$, dont le carré doit diviser la somme $x^2 + y^2$ qui vaut z^2 par hypothèse, on peut supposer que x et y sont premiers entre eux.

Ceci implique la primalité relative de x et z (ainsi que de y et z) : en effet, si d divise x et z, d divise z^2 et x^2, donc la différence $z^2 - x^2 = y^2$, d'où $d \mid x^2 \wedge y^2 \wedge z^2 = 1$. On montrerait de même que $y \wedge z = 1$.

On réécrit alors l'équation sous la forme

$$x^2 = (z - y)(z + y).$$

Si les deux termes de droite était premiers entre eux, on pourrait dire qu'ils sont tous deux des carrés et en déduire la forme de y et z puis de x. Mais cela est faux en général (prendre z et y pairs).

On se souvient alors qu'un carré vaut toujours 1 ou 0 modulo 4, ce qui impose à x ou y d'être pair (sinon $z^2 = 2$ modulo 4), disons $x = 2t$. On a donc

$$t^2 = \frac{z-y}{2}\frac{z+y}{2}.$$

Maintenant, les termes de droites $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont premiers entre eux : si d est un diviseur commun, d doit diviser la somme z et la différence y, donc vaudra 1, y et z étant premiers entre eux. On peut donc écrire

$$\begin{cases} \frac{z+y}{2} = u^2 \\ \frac{z-y}{2} = v^2 \end{cases} \quad \text{où } u > v > 0 \text{ sont deux entiers premiers entre eux,}$$

d'où $\begin{cases} z = u^2 + v^2 \\ y = u^2 - v^2 \end{cases}$ et $x = 2t = 2uv$. En remultipliant par le pgcd n de x et y, on trouve les solutions générales :

$$\text{si } \frac{x}{x \wedge y} \text{ est pair, } \begin{cases} x = n2uv \\ y = n\left(u^2 - v^2\right) \\ z = n\left(u^2 + v^2\right) \end{cases} \text{ où } \begin{cases} n > 0 \\ u > v > 0 \\ u \wedge v = 1 \end{cases}.$$

Réciproquement, on vérifie que

$$(2uv)^2 + \left(u^2 - v^2\right)^2 = 4u^2v^2 + \left(u^4 - 2u^2v^2 + v^4\right) = u^4 + 2u^2v^2 + v^4 = \left(u^2 + v^2\right)^2.$$

Remarque. En autorisant des égalités larges dans les conditions sur n, u, v, on rajoute les solutions "évidentes" $(0, n, n)$ et $(n, 0, n)$ pour n décrivant $\mathbb{N}$: faire $v = 0$ ou $u = v$. On obtient ainsi toutes les solutions à l'équation de Pythagore dans $\mathbb{N}^3$.

Pour obtenir les solutions dans $\mathbb{Z}^3$, il suffit de remarquer qu'en prenant les valeurs absolues on tombe dans $\mathbb{N}^3$ et par là même dans ce qui précède : on rajoutera donc des signes $\pm$ devant chaque coordonnée pour couvrir toutes les solutions.

On obtient du coup les solutions de $x^2 + y^2 = z^2$ dans $\mathbb{Q}$ (multiplier par un dénominateur commun), et on retrouve en particulier le paramétrage rationnel du cercle unité :

$$\begin{cases} x = \frac{2t}{1+t^2} \\ y = \frac{1-t^2}{1+t^2} \end{cases} \quad \text{où } t \text{ décrit } \mathbb{Q}.$$

6 Illustrer la descente infinie

Résoudre l'équation suivante en les entiers $a, b, c \geq 1$:

$$a^4 + b^4 = c^2.$$

Solution proposée.

Nous allons faire une descente infinie en utilisant les résulats connus sur les solutions à l'équation de Pythagore.

Soit (a, b, c) une solution minimisant c. Les entiers a, b, c sont donc deux à deux premiers entre eux (diviser par leur pgcd abaisse c) et l'exercice précédent permet d'écrire (en supposant a pair)

$$\begin{cases} a^2 = 2uv \\ b^2 = u^2 - v^2 \\ c = u^2 + v^2 \end{cases} \quad \text{avec } u \wedge v = 1.$$

La deuxième ligne est encore une équation de Pythagore :

$$u^2 = v^2 + b^2 \text{ avec } u \wedge v = 1.$$

b étant impair (il est premier avec a), v doit être pair et l'on a alors

$$\begin{cases} v = 2UV \\ b = U^2 - V^2 \\ u = U^2 + V^2 \end{cases} \quad \text{avec } U \wedge V = 1.$$

On en déduit les trois inconnues à l'aide des paramètres U et V :

$$\begin{cases} a^2 = 4\left(U^2 + V^2\right) UV \\ b = U^2 - V^2 \\ c = \left(U^2 + V^2\right)^2 + 4U^2V^2 \end{cases}.$$

La première ligne exprimant la factorisation d'un carré, on a de bonnes chances d'en tirer de l'information.

Il est facile de voir que U est premier avec $U^2 + V^2$: si p était un diviseur premier commun aux deux, p diviserait $\left(U^2 + V^2\right) - UU = V^2$, donc p diviserait V, et comme $U \wedge V = 1$, p vaudrait 1, ce qui n'est pas possible pour un premier. On montrerait de même que $V \wedge \left(U^2 + V^2\right) = 1$. Les trois nombres U, V et $U^2 + V^2$ sont par conséquent premiers entre eux et leur produit est un carré $\left(\frac{a}{2}\right)^2$, donc sont tous les trois des carrés :

$$\begin{cases} U = \alpha^2 \\ V = \beta^2 \\ U^2 + V^2 = \gamma^2 \end{cases}.$$

On en tire une nouvelle solution (α, β, γ) à notre équation de départ. En remarquant que

$$\gamma \leq \gamma^2 = U^2 + V^2 = u < u^2 + v^2 = c,$$

on peut appliquer le principe de descente infinie sur la troisième coordonnée et conclure à la contradiction.

Remarque. On déduit de cet exercice le théorème de Fermat pour $n = 4$: l'équation

$$a^4 + b^4 = c^4$$

n'a pas de solution dans $\mathbb{N}^{*3}$.

7 Une autre équation diophantienne

Résoudre en les entiers $a, b \geq 1$ l'équation

$$3^a - 2^b = 1.$$

Solution proposée.

Laissons déjà de côté la solution évidente $(a, b) = (1, 1)$. On suppose donc $a, b \geq 2$.

L'idée est de factoriser $2^b = 3^a - 1$ ou $3^a = 2^b + 1$; en effet, le terme de gauche est à chaque fois la puissance d'un nombre premier, ce qui forcera les termes factorisés à droite à être aussi des puissances de ce même nombre premier.

Avant cela, réduisons modulo des petits nombres premiers pour avoir de l'information sur a et b. Modulo 3, b doit être impair, donc, modulo 4, a doit aussi être pair (car $b \geq 2$), mettons $a = 2c$. On a donc

$$2^b = 3^{2c} - 1 = (3^c - 1)(3^c + 1)$$

Les deux termes de droite sont des puissances de 2 distantes de 2, donc valent 2 et 4, d'où $3^c - 1 = 2$, $c = 1$ et $a = 2$, puis $2^b = 3^2 - 1 = 8$ et $b = 3$.

Remarque. Ce résultat est un cas particulier de feu la *conjecture de Catalan* (prouvée par Preda Mihăilescu en avril 2002) qui affirme que les seules puissances entières consécutives (non triviales) sont 8 et 9.

Les deux exercices qui suivent mettent en valeur l'utilisation des trinômes de second degré pour la résolution d'équation diophantiennes.

8 Intégralité de $\frac{a^3+b^3-a^2b^2}{(a+b)^2}$

Trouver tous les entiers $a, b \geq 1$ tels que

$$\frac{a^3 + b^3 - a^2b^2}{(a+b)^2}$$

soit un entier relatif, puis naturel.

Solution proposée.

On commencer par simplifier la fraction en faisant apparaître le dénominateur $a + b$ au numérateur :

$$\frac{a^3 + b^3 - a^2b^2}{(a+b)^2} = \frac{(a+b)^3 - 3ab^2 - 3a^2b - a^2b^2}{(a+b)^2} = a + b - \frac{ab}{(a+b)^2}(3(a+b) + ab).$$

En notant $\begin{cases} s := a + b \\ p := ab \end{cases}$, pour $\begin{cases} \text{"}\mathbf{s}\text{omme"} \\ \text{"}\mathbf{p}\text{roduit"} \end{cases}$, il faut que $\frac{p}{s}\left(3 + \frac{p}{s}\right)$ soit entier, ce qui force $\frac{p}{s}$ à être entier : en effet, si $\frac{p}{s} = \frac{u}{v}$ avec $u \wedge v = 1$, on dispose de l'entier

$$\frac{p}{s}\left(3 + \frac{p}{s}\right) = \frac{u}{v}\left(3 + \frac{u}{v}\right) = \frac{3uv + u^2}{v^2},$$

donc

$$v \mid v^2 \mid 3uv + u^2 \implies v \mid u^2 \implies v = 1.$$

Notons k l'entier $\frac{p}{s}$. On sait que a et b sont les racines du trinôme $X^2 - sX + p$. Le discriminant de ce dernier doit donc être un carré δ^2, ce qui s'écrit

$$\delta^2 = s^2 - 4p = s^2 - 4ks.$$

De même, s est racine de $X^2 - 4kX - \delta^2$, donc son discriminant réduit doit être un carré c^2 :

$$c^2 = (2k)^2 + \delta^2.$$

On reconnait là une équation de Pythagore, avec $2k$ pair. On en déduit $\left\{\begin{array}{l} \delta = n\left(u^2 - v^2\right) \\ 2k = n\,(2uv) \\ c = n\left(u^2 + v^2\right) \end{array}\right.$ où n et $u \geq v$ sont des entiers positifs, d'où

$$s = 2k + c = n\left(2uv + \left(u^2 + v^2\right)\right) = n\,(u+v)^2$$

(la solution négative est à rejeter car $s = a + b > 0$). Il en résulte, en supposant $a \leq b$ par symétrie

$$\left\{\begin{array}{l} a = \frac{s-\delta}{2} = \frac{n(u+v)^2 - n\left(u^2-v^2\right)}{2} = \frac{n2uv+2nv^2}{2} = nv\,(u+v) \\ b = \frac{s+\delta}{2} = \frac{n(u+v)^2 + n\left(u^2-v^2\right)}{2} = \frac{n2u^2+2nuv}{2} = nu\,(u+v) \end{array}\right. .$$

On vérifie réciproquement que

$$\frac{ab}{a+b} = \frac{nv\,(u+v)\,nu\,(u+v)}{nv\,(u+v) + nu\,(u+v)} = \frac{n^2uv\,(u+v)^2}{n\,(u+v)\,(u+v)} = nuv \in \mathbb{N}.$$

Passons à la deuxième question : on veut à présent que $s - \frac{p}{s}\left(3 + \frac{p}{s}\right)$ soit un entier *positif*. Remarquer que $nuv = \frac{p}{s} > 0$, donc $n, u, v \geq 1$. Ceci implique

$$\begin{aligned} 0 \leq \frac{s - \frac{p}{s}\left(3 + \frac{p}{s}\right)}{nuv} &= \frac{n\,(u+v)^2 - nuv\,(3 + nuv)}{nuv} \\ \Longrightarrow\ 0 \leq \frac{u}{v} + 2 + \frac{v}{u} - 3 - nuv &\leq u + v - 1 - uv = \underbrace{(u-1)}_{\geq 0}\underbrace{(1-v)}_{\leq 0} \leq 0. \end{aligned}$$

On en déduit $u = v = 1$, et de plus le cas d'égalité dans l'inégalité utilisée $-nuv \leq -uv$ impose $n = 1$. Les valeurs de a et b tombent alors d'elles-mêmes :

$$\left\{\begin{array}{l} a = nv\,(u+v) = 2 \\ b = nu\,(u+v) = 2 \end{array}\right. .$$

Réciproquement, pour ces valeurs, on trouve

$$\frac{a^3 + b^3 - a^2b^2}{(a+b)^2} = \frac{8 + 8 - 4 \times 4}{4^2} = 0 \in \mathbb{N}.$$

9 Le carré parfait $\frac{a^2+b^2}{1+ab}$

Soient a et b des entiers ≥ 1. Montrer par une descente infinie que, si $\frac{a^2+b^2}{1+ab}$ est entier, alors c'est un carré parfait.

Solution proposée.

On raisonne comme le suggère l'énoncé : considérons par l'absurde un couple $(a, b) \in \mathbb{N}^{*2}$ tel que $\frac{a^2+b^2}{1+ab}$ soit un entier k non carré, et cherchons à construire une solution plus "petite". C'est la présence de carrés, donc d'équation du second, qui permettra de descendre les marches vers l'enfer.

Il est déjà clair que $k \neq 0$, et si de plus $a = b$, alors $k = \frac{2a^2}{1+a^2} = 2 - \frac{2}{a^2+1}$ n'est entier que pour $a = \pm 1$, auquel cas $k = 1$ qui est un carré parfait, ce qui est exclu. Par symétrie, on peut imposer $a > b$.

L'équation $k = \frac{a^2+b^2}{1+ab}$ se réécrit sous la forme d'un trinôme en a :

$$a^2 - (kb)\,a + \left(b^2 - k\right) = 0.$$

Elle admet une autre solution en a, mettons a', qui est entière car $a' = kb - a$, et qui est positive : en effet, on a clairement $k = \frac{a'^2+b^2}{1+a'b}$ par définition de a', donc $k\,(1 + ba') = a'^2 + b^2 > 0$, d'où $1 + ba' > 0$, $ba' \geq 0$ et $a' \geq 0$.

Si a' était nul, on trouverait $k = \frac{a^2+0^2}{1+0} = a^2$, cas que l'on a exclu. On peut donc supposer que (a', b) est une nouvelle solution dans $\mathbb{N}^{*2}$.

Il reste à trouver la quantité qui décroît lorsque l'on passe de (a, b) à (a', b). C'est là que l'on va utiliser l'hypothèse $a > b$. Cette dernière permet en effet d'écrire

$$a' = \frac{b^2 - k}{a} < \frac{b^2 - k}{b} < b,$$

d'où $\max\{a', b\} = b < a = \max\{a, b\}$. La quantité recherchée est donc $\max\{a, b\}$.

10 Calcul des sommes de Newton dans $\mathbb{F}_p$

Calculer $S_k := \sum_{x\in\mathbb{F}_p} x^k$ pour $k \in \mathbb{Z}$, selon que $p - 1$ divise k ou non.

Solution proposée.

Première méthode (groupes).

Laissons déjà de côté le cas $k = 0$ qui donne

$$S_0 = \sum_{x\in\mathbb{F}_p} x^0 = \sum_{x\in\mathbb{F}_p} 1 = |\mathbb{F}_p| = p = 0.$$

On peut alors indexer la somme sur le groupe $\mathbb{F}_p^*$ vu que $0^k = 0$. Un argument classique consiste alors à dire que, puisqu'un groupe est invariant par translation d'un élément quelconque a, on a

$$S_k = \sum_{x\in\mathbb{F}_p^*} x^k = \sum_{x\in\mathbb{F}_p^*} (ax)^k = \sum_{x\in\mathbb{F}_p^*} a^k x^k = a^k S_k.$$

Ainsi, ou bien il y a un $a \in \mathbb{F}_p^*$ tel que $a^k \neq 1$ et alors $S_k = 0$, ou bien $a^k = 1$ pour tout $a \in \mathbb{F}_p^*$ et alors $S_k = 1 + ... + 1 = p - 1 = -1$. On a donc

$$S_k = \left\{ \begin{array}{c} 0 \text{ si } \exists a \in \mathbb{F}_p^*,\ a^k \neq 1 \\ -1 \text{ si } \forall a \in \mathbb{F}_p^*,\ a^k = 1 \end{array} \right. .$$

Précisons ces deux conditions selon que $p - 1$ divise k ou pas.

Supposons $p - 1 \mid k$. Alors pour tout a dans $\mathbb{F}_p^*$, le PTF[4] nous donne

$$a^k = \left(a^{p-1}\right)^{\frac{k}{p-1}} = 1^{\frac{k}{p-1}} = 1.$$

Suppposons réciproquement que $\forall a \in \mathbb{F}_p^*,\ a^k = 1$. L'ordre de tout $a \in \mathbb{F}_p^*$ doit donc diviser k, et comme il divise également $p - 1$ par le PTF, les ordres des $a \in \mathbb{F}_p^*$ doivent diviser le pgcd $d := k \wedge (p - 1)$. Ainsi, le polynôme $X^d - 1$ s'annule sur $\mathbb{F}_p^*$, donc a au moins $p - 1$ racines, d'où $p - 1 \leq d$; d étant par ailleurs un diviseur de $p - 1$, on a l'égalité $k \wedge (p - 1) = p - 1$, d'où $k \mid p - 1$.

Seconde méthode (séries génératrices).

On part de la factorisation $X^{p-1} - 1 = \prod_{\lambda\in\mathbb{F}_p^*} (X - \lambda)$, exprimant que tout élément λ de $\mathbb{F}_p^*$ vérifie $\lambda^{p-1} = 1$ (PTF). On va en prendre la dérivée logarithmique, puis utiliser le développement en série formelle $\frac{1}{1-X} = 1 + X + X^2 + ...$ On va d'abord faire apparaître du $1 - (*)$ pour ne pas s'embêter avec les signes.

En regardant le produit des racines de $X^{p-1} - 1$, on récupère $-1 = \prod_{\lambda\in\mathbb{F}_p^*} (-\lambda)$, d'où $\prod_{\lambda\in\mathbb{F}_p^*} \lambda = (-1)^p$, puis

$$1 - X^{p-1} = -\prod_{\lambda\in\mathbb{F}_p^*} (X - \lambda) = -\prod_{\lambda\in\mathbb{F}_p^*} \lambda \prod_{\lambda\in\mathbb{F}_p^*} \left(\frac{X}{\lambda} - 1\right) = (-1)^{p-1} \prod_{\lambda\in\mathbb{F}_p^*} (\lambda X - 1) = \prod_{\lambda\in\mathbb{F}_p^*} (1 - \lambda X)$$

[4] petit théorème de Fermat

(pour l'avant-dernière égalité, on a dit que l'application $\lambda \mapsto \frac{1}{\lambda}$ était une bijection du groupe $\mathbb{F}_p^*$). On prend maintenant la dérivée logarithmique :

$$\frac{-(p-1)X^{p-2}}{1-X^{p-1}} = \sum_{\lambda\in\mathbb{F}_p^*} \frac{-\lambda}{1-\lambda X} \implies -X^{p-2}\sum_{i\geq 0}\left(X^{p-1}\right)^i = \sum_{\lambda\in\mathbb{F}_p^*}\lambda\sum_{i\geq 0}(\lambda X)^i$$

$$\implies -X^{p-1}\sum_{i\geq 0} X^{i(p-1)} = \sum_{i\geq 0}\left(\sum_{\lambda\in\mathbb{F}_p^*}\lambda^{i+1}\right)X^{i+1} \implies \sum_{i\geq 1} -X^{i(p-1)} = \sum_{i\geq 1} S_i X^i.$$

En identifiant les coefficients en X, on retrouve le même résultat que précédemment.

Remarque. Le resultat pourrait s'exprimer à l'aide de la fonction caractéristique de $\mathbb{N}$:

$$\forall k\geq 1,\ S_k = -\chi_{\mathbb{N}}\left(\frac{k}{p-1}\right).$$

11 Loi de réciprocité quadratique par le calcul des sommes de Gauss

On se place dans le corps $\mathbb{F}_p$. On rappelle que le groupe multiplicatif $\mathbb{F}_p^*$ est cyclique.
On s'intéresse à la question suivante : un entier a donné est-il un carré modulo un multiple de p ?
On définit pour cela le *symbole de Legendre*

$$\left(\frac{a}{p}\right) := \begin{cases} 0 \text{ si } a \text{ est nul modulo } p \\ 1 \text{ si } a \text{ est un carré modulo } p \\ -1 \text{ si } a \text{ n'est pas un carré modulo } p \end{cases}.$$

Soit $x\in\mathbb{F}_p^*$. Montrer que $\begin{cases} x \textit{ est un carré dans } \mathbb{F}_p^* \textit{ ssi } x^{\frac{p-1}{2}} = 1 \\ x \textit{ n'est pas un carré dans } \mathbb{F}_p^* \textit{ ssi } x^{\frac{p-1}{2}} = -1 \end{cases}$.
En déduire les relations $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *et* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Ainsi, pour calculer $\left(\frac{a}{p}\right)$, il suffit de le connaitre pour a premier. On laissera de côté le cas $a=2$ de côté pour l'exercice[5].

Soient p et q deux nombres premiers impairs distincts. On cherche un rapport entre $\left(\frac{q}{p}\right)$ et $\left(\frac{p}{q}\right)$. Pour cela, de la même manière que l'on introduit dans $\mathbb{R}$ un nombre i imaginaire qui engendre les toutes les racines du polynôme X^4-1 (on agrandit $\mathbb{R}$ et tombe sur $\mathbb{C}$), on va rajouter à $\mathbb{F}_q$ un élément ξ qui engendre les racines de X^p-1 (cela revient à construire un corps K de décomposition du polynôme X^p-1 sur $\mathbb{F}_q$), et on considère la somme dite *de Gauss* :

$$G = \sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)\xi^a$$

(qui est un élément du gros corps K).

Montrer que $G^2 = \left(\frac{-1}{p}\right)p$*, puis que* $G^q = \left(\frac{q}{p}\right)G$*, et en déduire la loi de réciprocité quadratique :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Application : 11 *est-il un carré modulo* 509 *?*

Solution proposée.
On a toujours $x^{\frac{p-1}{2}} = \pm 1$ car le carré vaut 1 (PTF).

[5] On peut calculer $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ pour p premier.

Si $x=c^2$ est un carré, alors $x^{\frac{p-1}{2}}=c^{2\frac{p-1}{2}}=c^{p-1}=1$ par le PTF.

Si $x^{\frac{p-1}{2}}=1$, écrivons $x=g^k$ où g est un générateur de $\mathbb{F}_p^*$. On a alors $g^{k\frac{p-1}{2}}=1$, donc l'ordre $p-1$ du générateur g doit diviser $k\frac{p-1}{2}$, disons $k\frac{p-1}{2}=l\,(p-1)$. Ceci implique $\frac{k}{2}=l$, d'où k pair et $x=g^k=\left(g^{\frac{k}{2}}\right)^2$ carré.

On en déduit que le symbole de Legendre se calcule explicitement par $\left(\frac{m}{p}\right)=m^{\frac{p-1}{2}}$, d'où sa multiplicativité et le calcul de $\left(\frac{-1}{p}\right)$.

Calculons à présent les puissances de la somme de Gauss G introduite. On vérifie tout d'abord que G est bien définie : en effet, si $a\in\mathbb{F}_p$, la puissance ξ^a ne dépend pas du représentant a modulo p choisi vu que $\xi^p=1$. Avanti ! On multidistribue le carré, puis on somme à puissance de ξ constante :

$$G^2=\left(\sum_{a\in\mathbb{F}_p^*}\left(\frac{a}{p}\right)\xi^a\right)^2=\sum_{a\neq0}\left(\frac{a}{p}\right)\xi^a\sum_{b\neq0}\left(\frac{b}{p}\right)\xi^b=\sum_{a,b\neq0}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\xi^{a+b}=\sum_{c\in\mathbb{F}_p}\left(\sum_{\substack{a+b=c\\a,b\neq0}}\left(\frac{ab}{p}\right)\right)\xi^c.$$

On élimine à présent une variable parmi a et b, mettons b, puis on homogénéise le ab dans le $\left(\frac{ab}{p}\right)$:

$$=\sum_c\left(\sum_{a\neq0,c}\left(\frac{a\,(c-a)}{p}\right)\right)\xi^c=\sum_c\left(\sum_{a\neq0,c}\underbrace{\left(\frac{a^2}{p}\right)}_{=1}\left(\frac{\frac{a(c-a)}{a^2}}{p}\right)\right)\xi^c=\sum_c\left(\sum_{a\neq0,c}\left(\frac{\frac{c}{a}-1}{p}\right)\right)\xi^c.$$

Le changement de variables $d=\frac{c}{a}-1$ nous tend les bras, et pour $c\neq0$ les conditions de sommation $a\neq0,c$ deviennent plus simplement $d\neq0,1$ (il n'y a plus de c, ce qui permet de sortir le ξ^c) :

$$=\sum_{a\neq0}\left(\frac{-1}{p}\right)+\sum_{c\neq0}\left(\sum_{a\neq0,c}\left(\frac{-1}{p}\right)\left(\frac{1-\frac{c}{a}}{p}\right)\right)\xi^c=(p-1)\left(\frac{-1}{p}\right)+\left(\frac{-1}{p}\right)\sum_{c\neq0}\left(\sum_{d\neq0,1}\left(\frac{d}{p}\right)\right)\xi^c.$$

Pour calculer $\sum_{d\neq0,1}\left(\frac{d}{p}\right)$, il convient de remarquer que $\mathbb{F}_p^*$ contient exactement autant de carrés que de non-carrés : considérer le morphisme $\left\{\begin{array}{ccc}\mathbb{F}_p^*&\longrightarrow&\mathbb{F}_p^*\\x&\longmapsto&x^2\end{array}\right.$ d'image les carrés et de noyau $\{\pm1\}$ (qui est bien de cardinal 2 car p, supposé impair, est distinct de 2 et par conséquent $1\neq-1$). Ainsi, $\sum_{d\neq0,1}\left(\frac{d}{p}\right)$ compte tous les carrés avec un 1 (sauf $d=1$) et tous les non-carrés avec un -1. Il en résulte que $\sum_{d\neq0,1}\left(\frac{d}{p}\right)=-1$. Finalement :

$$G^2=\left(\frac{-1}{p}\right)\left(p-1+\sum_{c\neq0}-\xi^c\right).$$

Pour obtenir la somme $\sum_c\xi^c$, il suffit de dire qu'elle vaut le terme en X^{p-1} dans le polynôme $X^p-1=\prod_{i=1}^p\left(X-\xi^i\right)$, i.e. 0. On en tire $\sum_{c\neq0}\xi^c=-1$, d'où

$$G^2=\left(\frac{-1}{p}\right)(p-1+1)=p\left(\frac{-1}{p}\right).$$

Le calcul de G^q sera moins douloureux. En effet, la relation $q\times1=0$ reste valable dans le gros corps K, donc l'élévation à la puissance q reste un morphisme aditif. Comme de plus q est impair, les symboles de Legendre sont inchangés par élévation à la puissance q. Ceci étant dit, on peut écrire

$$\begin{aligned}G^q&=\left(\sum_{a\neq0}\left(\frac{a}{p}\right)\xi^a\right)^q=\sum_{a\neq0}\left(\frac{a}{p}\right)^q\xi^{qa}=\sum_{a\neq0}\left(\frac{a}{p}\right)\xi^{qa}=\sum_{b\neq0}\left(\frac{\frac{b}{q}}{p}\right)\xi^b=\sum_{b\neq0}\underbrace{\left(\frac{\frac{1}{q^2}}{p}\right)}_{=1}\left(\frac{bq}{p}\right)\xi^b\\&=\sum_{b\neq0}\left(\frac{b}{p}\right)\left(\frac{q}{p}\right)\xi^b=\left(\frac{q}{p}\right)\sum_{b\neq0}\left(\frac{b}{p}\right)\xi^b=\left(\frac{q}{p}\right)G.\end{aligned}$$

Puisque $G^2 = p\left(\frac{-1}{p}\right)$ est non nul (car $p \neq q$), on peut simplifier par G et obtenir

$$G^{q-1} = \left(\frac{q}{p}\right).$$

En élevant la première relation trouvée $G^2 = p\left(\frac{-1}{p}\right) = p\,(-1)^{\frac{p-1}{2}}$ à la puissance $\frac{q-1}{2}$, on trouve

$$G^{q-1} = p^{\frac{q-1}{2}}\,(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Le résultat s'obtient en comparant les deux valeurs de G^{q-1}.

Pour l'application, on calcule le symbole de Legendre

$$\begin{aligned}\left(\frac{11}{509}\right) &= (-1)^{5\times 254}\left(\frac{509}{11}\right) = \left(\frac{46\times 11+3}{11}\right) = \left(\frac{3}{11}\right) = (-1)^{5\times 1}\left(\frac{11}{3}\right)\\ &= -\left(\frac{3\times 4-1}{3}\right) = -\left(\frac{-1}{3}\right) = -\,(-1)^{\frac{3-1}{2}} = 1,\end{aligned}$$

donc 11 est bien un carré modulo 509.