

Divisibilité, PGCD et congruences

Ce qui se cache derrière les astuces d'une feuille de terminale

Michel Hua

Octobre 2026

Résumé

En terminale, on calcule $(2n+1) \wedge (n+3)$ en écrivant $2n+1 = 2(n+3) - 5$, et l'on conclut que ce PGCD divise 5. Le geste est familier, mais il soulève une question : quelles transformations du couple (a, b) a-t-on le droit de faire sans changer le PGCD ? On reprend une feuille de révision de terminale (divisibilité, PGCD, congruences) en cherchant, derrière chaque astuce, l'énoncé général qui la rend évidente. La réponse à la question de départ est l'action du groupe $\text{GL}_2(\mathbb{Z})$. Viennent ensuite le coût de l'algorithme d'Euclide (théorème de Lamé), le développement de Pierce, l'exposant du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, l'obstruction modulo 16 dans le problème de Waring pour les puissances quatrièmes et le paramétrage des triplets pythagoriciens. Deux énoncés de la feuille d'origine étaient faux ; on explique pourquoi et on les corrige (remarques 2.3 et 5.3).

Leçons concernées. 142 (PGCD et PPCM, algorithmes de calcul), 120 (Anneaux $\mathbb{Z}/n\mathbb{Z}$), 126 (Exemples d'équations en arithmétique), 121 (Nombres premiers).

Développements possibles. Théorème 2.1 avec sa réciproque ; théorème de Lamé 2.7 ; propositions 5.2 et 5.4 ; théorème 6.1 et corollaire 6.3.

Prérequis. Division euclidienne, algorithme d'Euclide, théorème de Bézout, lemme de Gauss, congruences, petit théorème de Fermat. Un peu de calcul matriciel 2×2 .

Notations. Pour $a, b \in \mathbb{Z}$, on note $a \wedge b \geq 0$ leur PGCD, avec $0 \wedge 0 = 0$. Les résultats de base (Bézout, lemme de Gauss, factorialité de $\mathbb{Z}$) sont supposés connus ; ils sont démontrés par exemple dans [2].

Table des matières

1	La question de départ	2
2	Le PGCD sous l'action de $\text{GL}_2(\mathbb{Z})$	2
2.1	L'énoncé	2
2.2	Les deux usages : corriger la feuille, et calculer	3
2.3	L'algorithme d'Euclide comme produit de matrices	4
2.4	Coût de l'algorithme d'Euclide	4
3	Le développement de Pierce	5
4	Ordres et exposant de $(\mathbb{Z}/n\mathbb{Z})^\times$	6
5	Puissances quatrièmes modulo 16 et problème de Waring	8

6	Triplets pythagoriciens	9
7	Retour à la question de départ	10
8	Exercices	11
9	Corrigés	11

1 La question de départ

Partons d'un calcul que tout élève de terminale a fait. Soit n un entier. On cherche $(2n + 1) \wedge (n + 3)$.

On écrit $2n + 1 = 2(n + 3) - 5$. Un diviseur commun de $2n + 1$ et de $n + 3$ divise donc 5. Le PGCD vaut 1 ou 5. Il vaut 5 exactement quand 5 divise les deux nombres, c'est-à-dire quand $n \equiv 2 \pmod{5}$.

Le raisonnement repose sur un principe simple : *ce qui divise a et b divise toute combinaison $\alpha a + \beta b$* . On l'utilise sans cesse. L'algorithme d'Euclide lui-même remplace (a, b) par $(b, a - qb)$ sans changer le PGCD.

D'où la question qui guide cette feuille.

On remplace (a, b) par $(\alpha a + \beta b, \gamma a + \delta b)$. Quand le PGCD est-il conservé ?

La feuille d'origine répondait : toujours. C'est faux, et la section suivante dit exactement quand c'est vrai. Les sections d'après suivent le même fil : un exercice de la feuille, puis l'énoncé général qui l'explique.

2 Le PGCD sous l'action de $\text{GL}_2(\mathbb{Z})$

2.1 L'énoncé

Écrivons la transformation sous forme matricielle. On pose

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Z}), \quad \begin{pmatrix} a' \\ b' \end{pmatrix} = M \begin{pmatrix} a \\ b \end{pmatrix}.$$

Une inclusion est gratuite : tout diviseur commun de a et b divise a' et b' . Le vrai problème est de *revenir en arrière*, c'est-à-dire de récupérer a et b à partir de a' et b' . Il faudrait inverser M . Or, dans $\mathbb{Z}$, on ne peut inverser M qu'à un facteur $\det M$ près. C'est ce facteur qui mesure la perte possible.

Théorème 2.1. Soit $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Z})$, et pour $(a, b) \in \mathbb{Z}^2$ posons $\begin{pmatrix} a' \\ b' \end{pmatrix} = M \begin{pmatrix} a \\ b \end{pmatrix}$, $d = a \wedge b$, $d' = a' \wedge b'$.

1. On a $d \mid d'$ et $d' \mid (\det M) d$.
2. En particulier, si $M \in \text{GL}_2(\mathbb{Z})$, c'est-à-dire $\det M = \pm 1$, alors $d' = d$.
3. Réciproquement, si $d' = d$ pour tout $(a, b) \in \mathbb{Z}^2$, alors $\det M = \pm 1$.

Idée de la preuve. Pour le point 1, on va dans un sens par les combinaisons, et dans l'autre par la comatrice, qui est l'inverse de M « sans la division par $\det M$ ». Le point 2 en découle aussitôt. Pour la réciproque, il faut fabriquer un contre-exemple. Si un nombre premier p divise $\det M$, la matrice M n'est plus inversible modulo p : elle a un noyau. Un vecteur de ce noyau est envoyé sur un couple divisible par p . Il reste à le choisir premier entre ses coordonnées.

Démonstration. 1. Tout diviseur commun de a et b divise $a' = \alpha a + \beta b$ et $b' = \gamma a + \delta b$, donc $d \mid d'$. Pour l'autre sens, on utilise la comatrice : ${}^t\text{com}(M) M = (\det M) I_2$. Les entiers $(\det M) a$ et $(\det M) b$ sont donc des combinaisons entières de a' et b' . Ainsi d' les divise, donc divise leur PGCD, qui est $|\det M| d$.

2. Si $\det M = \pm 1$, on a $d \mid d'$ et $d' \mid d$, d'où $d = d'$ puisque les deux sont positifs.

3. Supposons $\det M \neq \pm 1$ et construisons (a, b) avec $a \wedge b = 1 < d'$.

Si $\det M = 0$, les colonnes de M sont liées. Il existe donc $(a, b) \neq (0, 0)$, qu'on peut prendre premiers entre eux en divisant par leur PGCD, avec $M \begin{pmatrix} a \\ b \end{pmatrix} = 0$. Alors $d' = 0 \neq 1$.

Sinon, soit p premier divisant $\det M$. La réduction $\overline{M} \in M_2(\mathbb{F}_p)$ a un déterminant nul, donc n'est pas inversible. Il existe donc $(u, v) \in \mathbb{F}_p^2$ non nul avec $\overline{M} \begin{pmatrix} u \\ v \end{pmatrix} = 0$. Quitte à échanger les rôles des deux coordonnées, $u \neq 0$. On choisit $a \in \{1, \dots, p-1\}$ représentant u . Il reste à choisir b dans la classe v modulo p , premier avec a . Comme $a \wedge p = 1$, les entiers $v + kp$, $0 \leq k < a$, parcourent toutes les classes modulo a . L'un d'eux, noté b , vérifie $b \equiv 1 \pmod{a}$, donc $a \wedge b = 1$. Par construction, $a' \equiv b' \equiv 0 \pmod{p}$, donc $p \mid d'$ et $d' \neq d$. $\square$

Remarque 2.2. Pourquoi le déterminant, et pas autre chose? Parce que la question « peut-on revenir en arrière avec des coefficients entiers? » est exactement la question « M^{-1} est-elle à coefficients entiers? ». Comme $\det M \cdot \det M^{-1} = 1$ dans $\mathbb{Z}$, cela force $\det M = \pm 1$. Le théorème dit que cette condition algébrique est aussi la bonne condition arithmétique.

2.2 Les deux usages : corriger la feuille, et calculer

On peut maintenant répondre à la question de départ, et voir où la feuille se trompait.

Remarque 2.3. La feuille d'origine demandait de montrer que $a \wedge b = (\alpha a + \beta b) \wedge (\gamma a + \delta b)$ pour tous entiers $\alpha, \beta, \gamma, \delta$. C'est faux. Prenons $M = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, de déterminant -2 , et $(a, b) = (1, 1)$. On obtient $(a', b') = (2, 0)$, de PGCD 2, alors que $1 \wedge 1 = 1$. Ce contre-exemple n'est pas un hasard : c'est celui que fabrique la preuve du point 3. Avec $p = 2$, le noyau de $\overline{M}$ est engendré par $(1, 1)$, et l'on prend $a = b = 1$. Le théorème 2.1 dit exactement quand l'énoncé est vrai : quand $\det M = \pm 1$.

Revenons au calcul du début. On l'a fait « à la main », mais il entre dans le cadre du théorème : on a

$$\begin{pmatrix} 2n+1 \\ n+3 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} n \\ 1 \end{pmatrix}, \quad \det = 5.$$

Le point 1 donne aussitôt $(2n+1) \wedge (n+3) \mid 5(n \wedge 1) = 5$. Le 5 de l'astuce, c'est le déterminant. Voici un exemple complet, tiré de la feuille, où l'on utilise cette remarque deux fois.

Exemple 2.4. Soit $n \geq 5$, $a = n^3 - n^2 - 12n$ et $b = 2n^2 - 7n - 4$. On cherche $a \wedge b$.

Première étape : factoriser. On trouve

$$a = n(n-4)(n+3), \quad b = (n-4)(2n+1).$$

Le facteur $n-4 > 0$ est commun. Il reste à comparer $n(n+3)$ et $2n+1$.

Deuxième étape : deux PGCD élémentaires, par le théorème.

- On a $\begin{pmatrix} 2n+1 \\ n+3 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} n \\ 1 \end{pmatrix}$, de déterminant 5. Donc $(2n+1) \wedge (n+3)$ divise $5(n \wedge 1) = 5$.

Il vaut 5 si et seulement si $n \equiv 2 \pmod{5}$, puisque $2n+1 \equiv 0$ et $n+3 \equiv 0 \pmod{5}$ équivalent tous deux à $n \equiv 2 \pmod{5}$.

- On a $\begin{pmatrix} n \\ 2n+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} n \\ 1 \end{pmatrix}$, de déterminant 1. Donc $n \wedge (2n+1) = n \wedge 1 = 1$.

Troisième étape : recoller. Par le lemme de Gauss, si $c \wedge n = 1$, alors $(nm) \wedge c = m \wedge c$: un facteur premier avec c ne change pas le PGCD. Comme $n \wedge (2n+1) = 1$, on peut enlever le facteur n :

$$a \wedge b = (n-4) \cdot (n(n+3) \wedge (2n+1)) = (n-4) \cdot ((n+3) \wedge (2n+1)) = \begin{cases} 5(n-4) & \text{si } n \equiv 2 \pmod{5}, \\ n-4 & \text{sinon.} \end{cases}$$

Vérification. Pour $n = 7$, on a $7 \equiv 2 \pmod{5}$. On calcule $a = 343 - 49 - 84 = 210$ et $b = 98 - 49 - 4 = 45$. Et en effet $210 \wedge 45 = 15 = 5 \cdot (7 - 4)$.

2.3 L'algorithme d'Euclide comme produit de matrices

On a vu que les matrices de déterminant ± 1 conservent le PGCD. Peut-on aller plus loin, et dire que ce sont *les seules* contraintes ? Autrement dit, deux couples de même PGCD se déduisent-ils toujours l'un de l'autre par une matrice de $\text{GL}_2(\mathbb{Z})$? La réponse est oui, et c'est l'algorithme d'Euclide qui le montre.

Remarque 2.5. Le théorème dit que l'orbite de (a, b) sous $\text{GL}_2(\mathbb{Z})$ est contenue dans $\{(a', b') : a' \wedge b' = d\}$. En fait elle lui est égale. Une étape de l'algorithme d'Euclide s'écrit

$$\begin{pmatrix} b \\ a - qb \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \quad \det \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = -1.$$

L'algorithme est donc une suite de multiplications par des matrices de $\text{GL}_2(\mathbb{Z})$, qui ramène (a, b) à $(d, 0)$. Tout couple de PGCD d est ainsi dans l'orbite de $(d, 0)$. En particulier, les vecteurs primitifs de $\mathbb{Z}^2$ (ceux de PGCD 1) forment une seule orbite, celle de $(1, 0)$.

Exemple 2.6. Pour $(210, 45)$: $210 = 4 \cdot 45 + 30$, puis $45 = 1 \cdot 30 + 15$, puis $30 = 2 \cdot 15 + 0$. On passe successivement par

$$(210, 45) \mapsto (45, 30) \mapsto (30, 15) \mapsto (15, 0),$$

avec les quotients $q = 4, 1, 2$. Le produit des trois matrices correspondantes envoie $(210, 45)$ sur $(15, 0)$.

2.4 Coût de l'algorithme d'Euclide

Puisque l'algorithme d'Euclide est l'outil central, on veut savoir combien il coûte. L'intuition est la suivante : l'algorithme est lent quand les quotients sont petits, car alors les restes diminuent peu. Le pire cas est celui où tous les quotients valent 1. On retrouve alors la relation $r_{i-1} = r_i + r_{i+1}$, qui est celle de Fibonacci. Le livre de Demazure [1] replace ce résultat dans l'étude du coût des algorithmes arithmétiques.

On note (F_k) la suite de Fibonacci, $F_1 = F_2 = 1$, $F_{k+2} = F_{k+1} + F_k$, et $\varphi = \frac{1+\sqrt{5}}{2}$.

Théorème 2.7 (Lamé, 1844). *Soit $a > b \geq 1$. Si l'algorithme d'Euclide appliqué à (a, b) effectue k divisions, alors $b \geq F_{k+1}$ et $a \geq F_{k+2}$. Par conséquent $k \leq 1 + \log_\varphi b$.*

Idée de la preuve. On remonte l'algorithme depuis la fin. Le dernier reste non nul vaut au moins 1, l'avant-dernier au moins 2. Ensuite, chaque reste est au moins la somme des deux suivants, comme pour Fibonacci. On compare donc les restes, lus à l'envers, à la suite de Fibonacci.

Démonstration. On pose $r_0 = a$, $r_1 = b$ et $r_{i-1} = q_i r_i + r_{i+1}$ avec $0 \leq r_{i+1} < r_i$, pour $1 \leq i \leq k$, où $r_k \neq 0$ et $r_{k+1} = 0$.

- On a $r_k \geq 1 = F_2$.

- Ensuite $r_{k-1} = q_k r_k > r_k$ impose $q_k \geq 2$, donc $r_{k-1} \geq 2 = F_3$.
- Pour $i < k$, on a $q_i \geq 1$, donc $r_{i-1} \geq r_i + r_{i+1}$.

Une récurrence descendante donne alors $r_{k-j} \geq F_{j+2}$ pour $0 \leq j \leq k$: pour $j \geq 2$, on a $r_{k-j} \geq r_{k-j+1} + r_{k-j+2} \geq F_{j+1} + F_j = F_{j+2}$. Avec $j = k-1$ et $j = k$, on obtient $b \geq F_{k+1}$ et $a \geq F_{k+2}$.

Enfin $F_{k+1} \geq \varphi^{k-1}$, par récurrence : c'est vrai pour $k = 0$ et $k = 1$, et l'hérédité vient de $\varphi^{k-2} + \varphi^{k-3} = \varphi^{k-3}(\varphi+1) = \varphi^{k-1}$, car $\varphi^2 = \varphi+1$. Donc $b \geq \varphi^{k-1}$, c'est-à-dire $k \leq 1 + \log_\varphi b$. $\square$

Remarque 2.8. La borne est atteinte pour deux termes consécutifs de la suite de Fibonacci : tous les quotients valent 1, sauf le dernier, qui vaut 2. Par exemple, pour $(13, 8) = (F_7, F_6)$,

$$13 = 1 \cdot 8 + 5, \quad 8 = 1 \cdot 5 + 3, \quad 5 = 1 \cdot 3 + 2, \quad 3 = 1 \cdot 2 + 1, \quad 2 = 2 \cdot 1 + 0.$$

On fait $k = 5$ divisions, et l'on a bien $b = 8 = F_6 = F_{k+1}$ et $a = 13 = F_7 = F_{k+2}$. La figure 1 montre ce trajet dans le plan : chaque étape est une matrice de $\text{GL}_2(\mathbb{Z})$, et les couples successifs restent collés à la droite de pente $1/\varphi$, puisque $F_k/F_{k+1} \rightarrow 1/\varphi$. Les restes décroissent donc d'un facteur φ à chaque étape, et pas plus vite : c'est exactement le pire cas. Le coût est donc $O(\log b)$ divisions. Comme la taille de b (son nombre de chiffres) est de l'ordre de $\log b$, l'algorithme est linéaire en la taille des entrées.

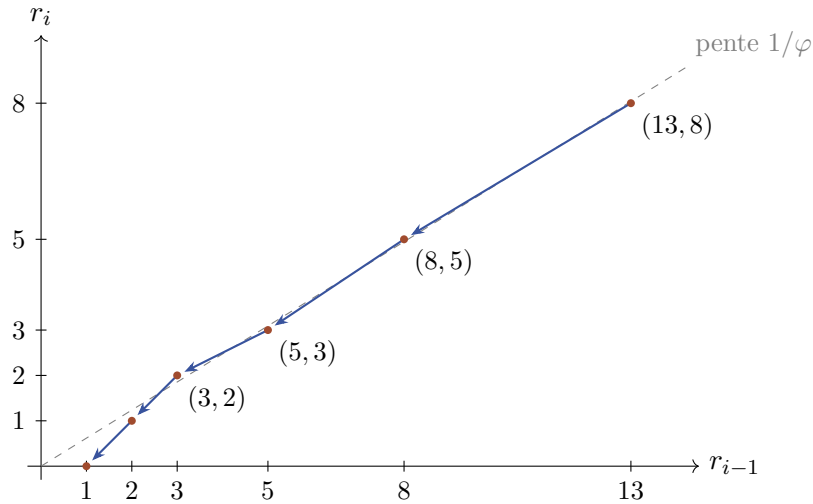


FIG. 1 : L'algorithme d'Euclide sur $(13, 8)$. Chaque flèche est la multiplication par une matrice $\begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$ de déterminant -1 , ici toujours avec $q = 1$ sauf à la dernière étape. Le trajet aboutit à $(1, 0)$: tous ces couples sont dans l'orbite de $(1, 0)$, et ils longent la droite de pente $1/\varphi$.

3 Le développement de Pierce

L'exercice 4 de la feuille d'origine décrit un algorithme sans le nommer. Il ressemble à l'algorithme d'Euclide, avec une différence : on divise toujours le *même* nombre y par les restes successifs, au lieu de diviser chaque reste par le suivant. On va voir que cela produit une écriture de x/y comme somme alternée d'inverses d'entiers. Elle porte le nom de T. A. Pierce, qui l'a étudiée en 1929 [4].

Proposition 3.1. *Soit $0 < x < y$ deux entiers. On pose $r_0 = x$, puis, tant que $r_{i-1} \neq 0$, on effectue la division euclidienne $y = q_i r_{i-1} + r_i$ avec $0 \leq r_i < r_{i-1}$. L'algorithme s'arrête après*

un nombre fini n d'étapes, avec $r_n = 0$, et

$$\frac{x}{y} = \frac{1}{q_1} - \frac{1}{q_1 q_2} + \frac{1}{q_1 q_2 q_3} - \cdots + \frac{(-1)^{n+1}}{q_1 q_2 \cdots q_n}, \quad 1 \leq q_1 < q_2 < \cdots < q_n.$$

Idée de la preuve. L'arrêt vient de ce que les restes décroissent strictement. Pour la formule, une seule division suffit à exprimer r_{i-1}/y en fonction de r_i/y ; on itère, comme on développe une fraction continue. La croissance des quotients vient de ce que l'on divise y par des restes de plus en plus petits.

Démonstration. Les restes $r_0 > r_1 > \cdots$ sont des entiers positifs, donc l'algorithme s'arrête.

Comme $y - r_i = q_i r_{i-1}$, on a, pour $i \geq 1$,

$$\frac{r_{i-1}}{y} = \frac{1}{q_i} - \frac{1}{q_i} \cdot \frac{r_i}{y}.$$

On part de $r_0/y = x/y$, on remplace r_1/y par son expression en fonction de r_2/y , et ainsi de suite jusqu'à $r_n = 0$. On obtient la formule annoncée.

Pour la croissance, on a d'abord $q_{i+1} = \lfloor y/r_i \rfloor \geq \lfloor y/r_{i-1} \rfloor = q_i$ puisque $r_i < r_{i-1}$. Supposons maintenant $q_{i+1} = q_i = q$. Alors $y = q r_{i-1} + r_i = q r_i + r_{i+1}$, d'où $q(r_{i-1} - r_i) = r_{i+1} - r_i$. Le membre de gauche est > 0 et celui de droite < 0 , ce qui est absurde. La croissance est donc stricte. $\square$

Exemple 3.2. Développons $17/45$. On divise 45 par les restes successifs :

$$45 = 2 \cdot 17 + 11, \quad 45 = 4 \cdot 11 + 1, \quad 45 = 45 \cdot 1 + 0.$$

Les quotients sont $2 < 4 < 45$, donc

$$\frac{17}{45} = \frac{1}{2} - \frac{1}{2 \cdot 4} + \frac{1}{2 \cdot 4 \cdot 45} = \frac{180 - 45 + 1}{360} = \frac{136}{360}.$$

On vérifie que $136/360 = 17/45$ en simplifiant par 8.

Pour $2/(2k+1)$ avec $k \geq 1$: $2k+1 = k \cdot 2 + 1$, puis $2k+1 = (2k+1) \cdot 1 + 0$. Donc $\frac{2}{2k+1} = \frac{1}{k} - \frac{1}{k(2k+1)}$.

Remarque 3.3. Le même algorithme, appliqué à un réel $t \in]0, 1[$ (avec $q_i = \lfloor 1/t_{i-1} \rfloor$, $t_0 = t$, $t_i = 1 - q_i t_{i-1}$), s'arrête si et seulement si t est rationnel. Par exemple $\frac{1}{e} = \sum_{k \geq 0} \frac{(-1)^k}{k!} = \frac{1}{2} - \frac{1}{2 \cdot 3} + \frac{1}{2 \cdot 3 \cdot 4} - \cdots$ a pour chiffres $q_i = i+1$. La condition de croissance stricte est indispensable : sans elle, le développement n'est pas unique, puisque $\frac{1}{q} - \frac{1}{q(q+1)} = \frac{1}{q+1}$.

4 Ordres et exposant de $(\mathbb{Z}/n\mathbb{Z})^\times$

Plusieurs exercices de la feuille demandent le dernier chiffre d'une énorme puissance, ou la divisibilité d'une différence de puissances. Ils reposent tous sur la même idée : modulo n , les puissances d'un entier premier à n sont *périodiques*. Il suffit donc de connaître une période commune à tous ces entiers. La plus petite s'appelle l'exposant du groupe.

Pour $n \geq 2$, on note $\lambda(n)$ l'exposant du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ (fonction de Carmichael) : c'est le plus petit $m \geq 1$ tel que $u^m \equiv 1 \pmod{n}$ pour tout u premier à n . Par le théorème chinois, $\lambda(n)$ est le PPCM des $\lambda(p^k)$ pour $p^k \parallel n$, avec $\lambda(p^k) = p^{k-1}(p-1)$ pour p impair, $\lambda(2) = 1$, $\lambda(4) = 2$ et $\lambda(2^k) = 2^{k-2}$ pour $k \geq 3$. Il divise l'indicatrice d'Euler $\varphi(n)$, et il est souvent bien plus petit : $\lambda(60) = 4$ alors que $\varphi(60) = 16$.

Exemple 4.1 (Exercices 9 et 12 de la feuille). 1. On cherche le chiffre des unités de $\sum_{i=0}^{400} 7^i$.

On travaille modulo 10. On a $\lambda(10) = \text{ppcm}(1, 4) = 4$, et en effet les puissances de 7 modulo 10 forment le cycle 1, 7, 9, 3, de somme $20 \equiv 0$. Comme la somme a $401 = 4 \cdot 100 + 1$ termes, elle contient 100 cycles complets, de contribution nulle, plus le dernier terme $7^{400} \equiv 1$. On obtient $\sum_{i=0}^{400} 7^i \equiv 1 \pmod{10}$: le chiffre des unités est 1.

On peut aussi passer par la formule $\frac{7^{401}-1}{6}$. Mais attention : diviser par 6 n'est pas permis modulo 10, car 6 n'y est pas inversible. Il faut connaître $7^{401} - 1$ modulo 60 pour connaître le quotient modulo 10. Comme $\lambda(60) = 4$, on a $7^{401} \equiv 7 \pmod{60}$, donc $7^{401} - 1 \equiv 6 \pmod{60}$ et le quotient est $\equiv 1 \pmod{10}$.

2. On veut montrer que $\frac{(7^{2004})^{2014} - (3^{2004})^{2014}}{2014 - 2004}$ est un entier. Soit $N = 2004 \cdot 2014$, multiple de 4. Comme $\lambda(10) = 4$, on a $7^N \equiv 3^N \equiv 1 \pmod{10}$, donc 10 divise $7^N - 3^N$. Le quotient est bien entier. Comme $\lambda(40) = \text{ppcm}(2, 4) = 4$, on a même $40 \mid 7^N - 3^N$.

Le même outil, l'ordre d'un élément, explique un exercice d'apparence très différente : trouver un multiple de n qui ne s'écrit qu'avec des 1.

Proposition 4.2 (Exercice 5 de la feuille). On note $R_k = \frac{10^k - 1}{9} = \underbrace{1 \dots 1}_k$.

1. Tout entier $n \geq 1$ possède un multiple dont l'écriture décimale ne comporte que des 0 et des 1.
2. Si $n \wedge 10 = 1$, alors $n \mid R_k$ si et seulement si $\text{ord}_n(10) \mid k$. En particulier n divise un nombre formé uniquement de 1.

Idée de la preuve. Pour le point 1, on n'a besoin de rien savoir sur n : parmi $n+1$ nombres, deux ont le même reste modulo n , et leur différence convient. Pour le point 2, on traduit « n divise R_k » en une congruence sur 10^k , et l'on reconnaît la définition de l'ordre.

Démonstration. 1. Parmi $R_1, \dots, R_{n+1}$, deux ont le même reste modulo n (principe des tiroirs), disons R_p et $R_{p'}$ avec $p < p'$. Alors n divise $R_{p'} - R_p = 10^p R_{p'-p}$, qui s'écrit avec $p' - p$ chiffres 1 suivis de p chiffres 0.

2. On a $n \mid R_k \iff 9n \mid 10^k - 1 \iff 10^k \equiv 1 \pmod{9n}$, et 10 est inversible modulo $9n$ car $n \wedge 10 = 1$. Les k qui conviennent sont donc les multiples de l'ordre de 10 modulo $9n$. $\square$

Exemple 4.3. Pour $n = 6$ (non premier à 10), on applique le point 1. Modulo 6, on a $R_1 = 1$, $R_2 = 11 \equiv 5$, $R_3 = 111 \equiv 3$, $R_4 = 1111 \equiv 1$. Les restes de R_1 et R_4 coïncident, donc 6 divise $R_4 - R_1 = 1110 = 6 \cdot 185$.

Pour $n = 7$, on applique le point 2. On a $\text{ord}_7(10) = 6$ et $\text{ord}_9(10) = 1$, donc $\text{ord}_{63}(10) = \text{ppcm}(6, 1) = 6$. Ainsi $R_6 = 111111 = 7 \cdot 15873$, et aucun R_k plus court n'est multiple de 7.

Dernier exercice du même genre, où le principe des tiroirs est remplacé par une remarque encore plus simple : parmi n entiers consécutifs, l'un est multiple de n .

Proposition 4.4 (Exercice 13 de la feuille). Tout entier $n \geq 1$ possède un multiple dont l'écriture décimale contient les dix chiffres.

Démonstration. Soit $A = 1234567890$ et k tel que $10^k \geq n$. Les n entiers consécutifs $A \cdot 10^k + j$, $0 \leq j < n$, commencent tous par les chiffres de A , puisque $j < 10^k$ ne touche que les k derniers chiffres. L'un d'eux est multiple de n . $\square$

Exemple 4.5. Pour $n = 7$, on prend $k = 1$. On a $1234567890 \equiv 3 \pmod{7}$, donc $12345678900 \equiv 30 \equiv 2 \pmod{7}$. Avec $j = 5$, on trouve $12345678905 = 7 \cdot 1763668415$.

5 Puissances quatrièmes modulo 16 et problème de Waring

La feuille demandait de montrer que certains entiers ne sont pas somme de peu de puissances quatrièmes. La méthode est celle des obstructions par congruence : on cherche un module où les puissances quatrièmes prennent très peu de valeurs. Le bon module est 16, où elles ne prennent que *deux* valeurs.

Lemme 5.1. *Pour $x \in \mathbb{Z}$, $x^4 \equiv 0 \pmod{16}$ si x est pair et $x^4 \equiv 1 \pmod{16}$ si x est impair.*

Démonstration. Si $x = 2t$ est pair, $x^4 = 16t^4$. Si $x = 2t + 1$ est impair, $x^2 = 4t(t + 1) + 1$, et $t(t + 1)$ est pair, donc $x^2 = 1 + 8m$. Alors $x^4 = 1 + 16m + 64m^2 \equiv 1 \pmod{16}$. $\square$

La conséquence est frappante. Une somme de s puissances quatrièmes est congrue modulo 16 au *nombre de termes impairs*, qui est compris entre 0 et s . Pour atteindre la classe 15, il faut donc au moins 15 termes.

Proposition 5.2. *Un entier $N \equiv 15 \pmod{16}$ n'est pas somme de moins de 15 puissances quatrièmes. En particulier $79 = 4 \cdot 2^4 + 15 \cdot 1^4$ n'est pas somme de moins de 19 puissances quatrièmes.*

Démonstration. La première assertion découle du lemme 5.1, comme on vient de l'expliquer. Pour 79, on peut faire mieux, car 79 est petit. Les seules puissances quatrièmes utilisables sont 1 et 16, puisque $3^4 = 81 > 79$. Une écriture $79 = 16a + b$ avec a seize et b uns utilise $a + b = 79 - 15a$ termes, avec $a \leq 4$. Ce nombre est minimal pour $a = 4$ et vaut alors 19. $\square$

Remarque 5.3. La feuille d'origine affirmait que 2005 n'est pas somme de six puissances quatrièmes non nulles. Elle donnait pourtant l'égalité $2005 = 1^4 + 1^4 + 1^4 + 3^4 + 5^4 + 6^4 = 1 + 1 + 1 + 81 + 625 + 1296$, qui la contredit. L'énoncé correct porte sur 2015. Comme $2015 = 16 \cdot 125 + 15$, la proposition 5.2 montre que 2015 n'est pas somme de six puissances quatrièmes, ni même de quatorze. Pour $2005 = 16 \cdot 125 + 5$, la congruence n'interdit rien à partir de cinq termes, et l'on voit qu'il en suffit de six.

On sait donc qu'il faut parfois 15 termes, et même 19 pour 79. Mais on pourrait espérer que, pour les *grands* entiers, 15 termes suffisent toujours. La proposition suivante montre que non. L'idée est de combiner la congruence modulo 16 avec une descente : si tous les termes sont pairs, on peut tout diviser par 16.

Proposition 5.4. *Pour tout $k \geq 0$, l'entier $31 \cdot 16^k$ n'est pas somme de 15 puissances quatrièmes (positives ou nulles). Il y a donc une infinité d'entiers qui ne sont pas somme de 15 puissances quatrièmes.*

Démonstration. Par récurrence sur k .

Pour $k = 0$: dans une écriture $31 = \sum_{i=1}^{15} x_i^4$, le nombre de x_i impairs est $\equiv 31 \equiv 15 \pmod{16}$ et ≤ 15 , donc tous les x_i sont impairs. Comme $3^4 = 81 > 31$, ils valent tous ± 1 , et la somme vaut $15 \neq 31$.

Pour $k \geq 1$: si $31 \cdot 16^k = \sum_{i=1}^{15} x_i^4$, le nombre de x_i impairs est $\equiv 0 \pmod{16}$ et ≤ 15 , donc nul. Tous les x_i sont pairs. En divisant par $16 = 2^4$, on obtient $31 \cdot 16^{k-1} = \sum (x_i/2)^4$, ce qui contredit l'hypothèse de récurrence. $\square$

Remarque 5.5. Notons $g(4)$ le plus petit s tel que tout entier soit somme de s puissances quatrièmes, et $G(4)$ le plus petit s tel que tout entier assez grand le soit. Les propositions précédentes donnent $g(4) \geq 19$ (à cause de 79) et $G(4) \geq 16$ (à cause des $31 \cdot 16^k$). Ces bornes sont exactes : $G(4) = 16$ (Davenport, 1939) et $g(4) = 19$ (Balasubramanian, Deshouillers et Dress, 1986). Les minoration sont élémentaires, comme on vient de le voir ; toute la difficulté est dans les majorations. Le chapitre 21 de Hardy et Wright [3] raconte cette histoire et démontre une partie des majorations.

6 Triplets pythagoriciens

L'exercice 3 de la feuille demandait de montrer que 60 divise xyz dès que $x^2 + y^2 = z^2$. On peut le faire à coups de congruences. Mais on comprend mieux en décrivant d'abord *toutes* les solutions : les divisibilités se lisent ensuite sur la formule.

On se ramène aux triplets *primitifs*, où $x \wedge y = 1$: un triplet quelconque en est un multiple. L'idée centrale est une factorisation : $x^2 = z^2 - y^2$, ou plutôt, avec y pair, $(y/2)^2$ s'écrit comme produit de deux entiers premiers entre eux. Dans $\mathbb{Z}$, un tel produit ne peut être un carré que si chaque facteur en est un. Ce paramétrage est classique ; on le trouve, avec d'autres équations du même genre, au chapitre 13 de Hardy et Wright [3].

Théorème 6.1. *Les solutions de $x^2 + y^2 = z^2$ en entiers $x, y, z \geq 1$ avec $x \wedge y = 1$ et y pair sont exactement*

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2,$$

avec $u > v \geq 1$, $u \wedge v = 1$ et $u \not\equiv v \pmod{2}$.

Démonstration. Ces triplets conviennent. L'identité $(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$ se vérifie en développant. Si un premier p divisait x et y , il diviserait z , donc $z + x = 2u^2$ et $z - x = 2v^2$. Comme x est impair (car $u \not\equiv v \pmod{2}$), p est impair, donc p diviserait u^2 et v^2 , ce qui est exclu par $u \wedge v = 1$.

Ce sont les seuls. Si $x \wedge y = 1$, alors x et y ne sont pas tous deux pairs. Ils ne sont pas non plus tous deux impairs, sinon $z^2 \equiv 1 + 1 = 2 \pmod{4}$, alors qu'un carré est $\equiv 0$ ou $1 \pmod{4}$. Avec y pair, x et z sont impairs, et

$$\frac{z+x}{2} \cdot \frac{z-x}{2} = \left(\frac{y}{2}\right)^2.$$

Un diviseur commun des deux facteurs divise leur somme z et leur différence x . Or $x \wedge z = 1$, car un nombre premier qui divise x et z divise $z^2 - x^2 = y^2$, donc y , ce qui contredit $x \wedge y = 1$. Les deux facteurs sont donc premiers entre eux, positifs, et leur produit est un carré. Par factoriabilité de $\mathbb{Z}$, ce sont des carrés u^2 et v^2 , ce qui donne $z = u^2 + v^2$, $x = u^2 - v^2$ et $y = 2uv$. Les conditions sur u et v viennent de $x \wedge y = 1$ et de la parité de x . $\square$

Exemple 6.2. Avec $(u, v) = (2, 1)$, on trouve $(3, 4, 5)$. Avec $(u, v) = (3, 2)$, on trouve $(5, 12, 13)$. Avec $(u, v) = (4, 1)$, on trouve $(15, 8, 17)$. En revanche $(u, v) = (3, 1)$ est exclu, car $u \equiv v \pmod{2}$: il donnerait $(8, 6, 10)$, qui n'est pas primitif.

On peut maintenant lire les divisibilités de l'exercice 3 directement sur le paramétrage.

Corollaire 6.3 (Exercice 3 de la feuille). *Si $x^2 + y^2 = z^2$ avec $x, y, z \geq 1$, alors $3 \mid xy$, l'un de x, y est multiple de 4, et $5 \mid xyz$. En particulier $60 \mid xyz$, et 60 est optimal puisque $(3, 4, 5)$ donne 60.*

Démonstration. On écrit $(x, y, z) = e(x_0, y_0, z_0)$ avec (x_0, y_0, z_0) primitif et, quitte à échanger x et y , $y_0 = 2uv$ comme dans le théorème. Il suffit de traiter le triplet primitif, car multiplier par e conserve les divisibilités.

- L'un de u, v est pair, donc $4 \mid 2uv = y_0$.
- On a $x_0 y_0 = 2uv(u^2 - v^2)$. Si $3 \nmid uv$, alors $u^2 \equiv v^2 \equiv 1 \pmod{3}$, donc $3 \mid u^2 - v^2$.
- On a $x_0 y_0 z_0 = 2uv(u^4 - v^4)$. Si $5 \nmid uv$, le petit théorème de Fermat donne $u^4 \equiv v^4 \equiv 1 \pmod{5}$, donc $5 \mid u^4 - v^4$.

Comme 3, 4 et 5 sont premiers entre eux deux à deux, $60 \mid xyz$. $\square$

Exemple 6.4. Pour $(5, 12, 13)$: 3 divise $xy = 60$, 4 divise 12, 5 divise 5, et $xyz = 780 = 60 \cdot 13$.

Remarque 6.5. On peut aussi raisonner directement sur les carrés modulo 3, 8 et 5, comme le suggérait la feuille. Le paramétrage a deux autres interprétations, qui expliquent pourquoi il existe. La première est la factorisation $z^2 = (x + iy)(x - iy)$ dans l'anneau factoriel $\mathbb{Z}[i]$: c'est le même argument « produit de deux facteurs premiers entre eux qui est un carré ». La seconde est géométrique : c'est le paramétrage rationnel du cercle unité par la droite de pente $t = v/u$ passant par $(-1, 0)$ (figure 2). En effet, un triplet $x^2 + y^2 = z^2$ donne le point rationnel $(x/z, y/z)$ du cercle $X^2 + Y^2 = 1$. La droite $Y = t(X + 1)$ recoupe le cercle en un second point, qu'on trouve en résolvant une équation du second degré dont on connaît déjà la racine $X = -1$:

$$X = \frac{1 - t^2}{1 + t^2}, \quad Y = \frac{2t}{1 + t^2}.$$

Avec $t = v/u$, on obtient $X = \frac{u^2 - v^2}{u^2 + v^2}$ et $Y = \frac{2uv}{u^2 + v^2}$: c'est le paramétrage du théorème 6.1. Les points rationnels du cercle correspondent ainsi aux pentes rationnelles.

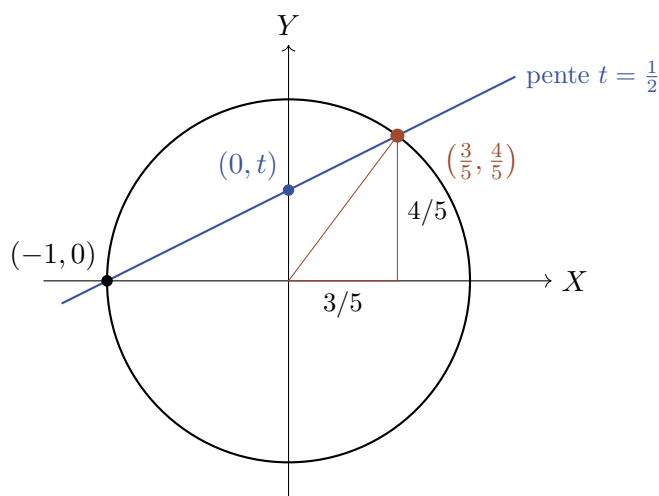


FIG. 2 : La droite de pente t passant par $(-1, 0)$ recoupe le cercle unité au point $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$. Pour $t = \frac{1}{2}$, c'est-à-dire $(u, v) = (2, 1)$, on obtient $(\frac{3}{5}, \frac{4}{5})$ et le triplet $(3, 4, 5)$.

7 Retour à la question de départ

On se demandait quelles transformations $(a, b) \mapsto (\alpha a + \beta b, \gamma a + \delta b)$ conservent le PGCD. La réponse est nette : exactement celles de déterminant ± 1 , c'est-à-dire l'action de $\text{GL}_2(\mathbb{Z})$ (théorème 2.1). Pour les autres, le PGCD peut être multiplié, mais seulement par un diviseur du déterminant. C'est ce qui explique le 5 du calcul initial : $(2n + 1) \wedge (n + 3)$ divise 5 parce que $\det \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} = 5$. Et l'algorithme d'Euclide, qui n'utilise que des matrices de déterminant -1 , montre que deux couples de même PGCD sont toujours reliés par $\text{GL}_2(\mathbb{Z})$.

La même démarche a guidé toute la feuille : derrière chaque astuce, un énoncé général.

Exercice de la feuille	Ce qui l'explique
$(2n + 1) \wedge (n + 3)$, PGCD de polynômes en n	action de $M_2(\mathbb{Z})$, le PGCD varie d'un diviseur de $\det M$
Coût de l'algorithme d'Euclide	le pire cas est Fibonacci (Lamé)
Exercice 4	développement de Pierce, un Euclide où l'on divise toujours y
Derniers chiffres, nombres $1 \dots 1$	périodicité des puissances, exposant $\lambda(n)$ et ordre
Sommes de puissances quatrièmes	elles ne valent que 0 ou 1 modulo 16
$60 \mid xyz$	paramétrage des triplets primitifs

Les deux erreurs de la feuille ont la même origine : un énoncé vrai dans un cas particulier, généralisé trop vite. La première oubliait la condition $\det M = \pm 1$. La seconde confondait 2005, que la congruence n'arrête pas, avec 2015, qui est $\equiv 15 \pmod{16}$.

8 Exercices

Exercice 1. Déterminer les $n \in \mathbb{N}$ tels que $n + 1 \mid 3n^2 + 15n + 19$.

Exercice 2. Soit $n \geq 1$, $M = 9n - 1$ et $N = 9n + 1$. Calculer $M \wedge N$ selon la parité de n , et montrer que $4 \mid 81n^2 - 1$ si et seulement si n est impair.

Exercice 3. Un rectangle $a \times b$ ($a, b \geq 1$ entiers) est découpé en ab carrés unités. Combien de carrés la diagonale traverse-t-elle (en passant par leur intérieur) ?

Exercice 4. Trouver tous les entiers $0 < a < b < c$ avec $abc < 2003$ tels que la somme de deux quelconques d'entre eux soit divisible par le troisième.

Exercice 5. On a $1089 \times 9 = 9801$. Trouver un entier à quatre chiffres N tel que $4N$ s'écrive avec les chiffres de N dans l'ordre inverse.

Exercice 6. Soit $s \geq 1$. Montrer que les sommes de s puissances quatrièmes ne recouvrent pas toutes les classes modulo 16 si $s \leq 14$, et les recouvrent toutes si $s \geq 15$.

9 Corrigés

Exercice 1. L'idée est de faire une division euclidienne de polynômes, pour se ramener à un diviseur de $n + 1$ qui ne dépend plus de n . On a $3n^2 + 15n + 19 = (n + 1)(3n + 12) + 7$. Donc $n + 1 \mid 3n^2 + 15n + 19 \iff n + 1 \mid 7 \iff n + 1 \in \{1, 7\} \iff n \in \{0, 6\}$.

Exercice 2. $M \wedge N$ divise $N - M = 2$, donc vaut 1 ou 2. Si n est pair, M et N sont impairs et $M \wedge N = 1$. Si n est impair, ils sont pairs et $M \wedge N = 2$. Comme $81n^2 - 1 = MN$: si n est impair, M et N sont pairs et $4 \mid MN$; si n est pair, MN est impair.

Exercice 3. Commençons par compter sur un exemple, le rectangle 6×4 de la figure 3. Suivons la diagonale depuis le coin $(0, 0)$: elle part dans un premier carré. Ensuite, chaque fois qu'elle traverse un trait du quadrillage, elle entre dans un nouveau carré.

- Elle traverse les traits verticaux intérieurs $x = 1, 2, 3, 4, 5$: cela fait 5 entrées.
- Elle traverse les traits horizontaux intérieurs $y = 1, 2, 3$: cela fait 3 entrées.

- Si toutes ces traversées avaient lieu en des points différents, on compterait $1 + 5 + 3 = 9$ carrés.
- Mais au point $(3, 2)$, elle traverse un trait vertical et un trait horizontal *en même temps*, exactement par un coin. Elle n'entre alors que dans un seul nouveau carré, celui en diagonale, et on a compté cette entrée deux fois.

Il reste $9 - 1 = 8$ carrés, ce sont les huit carrés grisés de la figure.

Le cas général suit le même compte. Dans un rectangle $a \times b$, la diagonale part dans un carré, traverse $a - 1$ traits verticaux et $b - 1$ traits horizontaux, et on retire une entrée pour chaque coin où elle passe, c'est-à-dire pour chaque point entier intérieur de la diagonale. Reste à compter ces points. La diagonale est la droite $y = \frac{b}{a}x$. Pour $0 < x < a$ entier, y est entier si et seulement si a divise bx . Écrivons $d = a \wedge b$, $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$: la condition devient $a' \mid b'x$, c'est-à-dire $a' \mid x$ par le lemme de Gauss. Les points entiers intérieurs sont donc ceux d'abscisse $a', 2a', \dots, (d-1)a'$: il y en a $d - 1$. Le nombre de carrés traversés est

$$1 + (a - 1) + (b - 1) - (d - 1) = a + b - a \wedge b.$$

Pour 6×4 , on retrouve $6 + 4 - 2 = 8$, avec un seul point entier intérieur, $(3, 2)$, puisque $6 \wedge 4 = 2$.

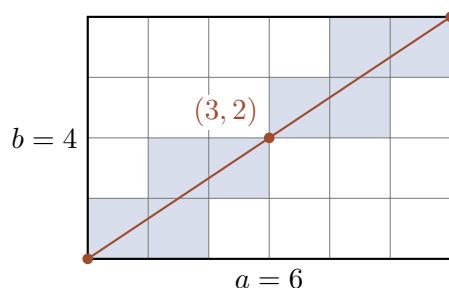


FIG. 3 : Dans un rectangle 6×4 , la diagonale traverse les $8 = 6 + 4 - 2$ carrés grisés. Elle passe par les points entiers $(0, 0)$, $(3, 2)$ et $(6, 4)$: il y en a $6 \wedge 4 + 1 = 3$.

Exercice 4. On exploite les inégalités : un diviseur ne peut diviser qu'un petit nombre de multiples dans un intervalle. On a $c \mid a + b$ et $0 < a + b < 2c$, donc $a + b = c$. Ensuite $b \mid a + c = 2a + b$, donc $b \mid 2a$ avec $0 < 2a < 2b$, d'où $b = 2a$ et $c = 3a$. Réciproquement, $(a, 2a, 3a)$ convient : $3a \mid 3a$, $2a \mid 4a$ et $a \mid 5a$. La condition $6a^3 < 2003$ donne $a \leq 6$. Les solutions sont donc $(a, 2a, 3a)$ pour $1 \leq a \leq 6$.

Exercice 5. Écrivons $N = \overline{abcd}$. On détermine les chiffres un par un, en commençant par les extrêmes. Comme $4N < 10^4$, on a $a \leq 2$; et a , chiffre des unités de $4N$, est pair, donc $a = 2$. Ensuite $4d \equiv 2 \pmod{10}$ et $d \geq 8$ (car $4N \geq 8000$), donc $d = 8$. L'égalité $4(2008 + 100b + 10c) = 8002 + 100c + 10b$ se simplifie en $13b + 1 = 2c$, donc $b = 1$ et $c = 7$. Ainsi $N = 2178$ et $4 \times 2178 = 8712$. On montre plus généralement que 2178, 21978, 219978, ... conviennent pour le facteur 4, et 1089, 10989, ... pour le facteur 9. En base 10, seuls les facteurs 4 et 9 sont possibles (Sutcliffe, 1966).

Exercice 6. Par le lemme 5.1, une somme de s puissances quatrièmes est congrue modulo 16 au nombre $j \in \{0, \dots, s\}$ de termes impairs. Toutes les valeurs de j sont atteintes, avec j termes égaux à 1 et $s - j$ nuls. Les classes atteintes sont donc celles de $0, 1, \dots, \min(s, 15)$: toutes si $s \geq 15$, et seulement $s + 1 < 16$ d'entre elles si $s \leq 14$.

Références

- [1] M. Demazure, *Cours d'algèbre. Primalité, divisibilité, codes*, Cassini. Un cours d'arithmétique tourné vers les algorithmes : algorithme d'Euclide et son coût, tests de primalité, codes correcteurs.
- [2] X. Gourdon, *Les maths en tête. Algèbre et probabilités*, Ellipses. Le manuel de référence des classes préparatoires et de l'agrégation pour les bases : PGCD, Bézout, lemme de Gauss, anneaux $\mathbb{Z}/n\mathbb{Z}$.
- [3] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press (1^{re} édition 1938, 6^e édition revue par D. R. Heath-Brown et J. H. Silverman, 2008). Le grand classique de la théorie des nombres, en anglais ; on y trouve les triplets pythagoriciens (chapitre 13) et le problème de Waring (chapitre 21).
- [4] T. A. Pierce, *On an algorithm and its use in approximating roots of algebraic equations*, Amer. Math. Monthly 36 (1929). L'article d'origine du développement de la section 2.

Source. Feuille de révision de terminale S (2003), d'après les manuels *Hyperbole* et *Bréal*. La partie « Continuité » de cette feuille est reprise dans la leçon 228.