Arithmétique

Prérequis
Division euclidienne. Algorithme d'Euclide. Théorèmes de Gauss, de Bezout et de Fermat. Décomposition en facteurs premiers.

Division euclidienne

Calcul 23.1 — Variations sur le signe.

Effectuer la division euclidienne de a par b, on donnera le résultat sous la forme « (quotient, reste) ».

a) $a = 61$ et $b = 9$ ..... c) $a = 61$ et $b = -9$ .....

b) $a = -61$ et $b = 9$ ..... d) $a = -61$ et $b = -9$ .....

Calcul 23.2 — Diviseur et reste inconnus.

On divise 524 par un entier non nul inconnu, d. Le quotient vaut 26 et le reste r.

a) d vaut ..... b) r vaut .....

Calcul 23.3 — Arithmétique modulaire.

On rappelle que deux entiers a et b sont congrus modulos n, ce qu'on note $a \equiv b \pmod{n}$, si et seulement s'ils ont même reste de division euclidienne par n.

a) Le reste de 5^{2021} par 3 vaut ..... b) Le reste de 3^{2022} par 5 vaut .....

Calcul 23.4 — Encore des modulos.

La notation a^{b^c} désigne le nombre a à la puissance « b puissance c ». À ne pas confondre avec $(a^b)^c = a^{b\times c}$

Le chiffre des unités de $2\,023^{2022^{2021}}$ est .....

PGCD et PPCM

Calcul 23.5 — Réduction de fractions.

On notera $a \wedge b$ le plus grand diviseur commun de a et b et $a \vee b$ leur plus petit multiple commun.

a) $10\,010 \wedge 2\,772$ vaut ..... c) $729 \vee 360$ vaut .....

b) la forme irréductible de $\dfrac{10\,010}{2\,772}$ est d) $\dfrac{1}{360} - \dfrac{2}{729}$. .....

Calcul 23.6 — Systèmes diophantiens.

Déterminer tous les couples d'entiers naturels (a, b) tels que :

a) $\begin{cases} a^2 - b^2 = 9792 \\ a \wedge b = 24 \end{cases}$ ..... b) $\begin{cases} a \times b = 360 \\ a \vee b = 60 \\ 6 < a < b \end{cases}$ .....

Coprimalité, relation de Bezout et théorème de Gauss

Calcul 23.7 — Inverse modulo 13.

L'objectif de cet exercice est de résoudre l'équation de congruence $5x+4 \equiv 7 \pmod{13}$. Pour ce faire, on cherche un inverse pour 5 modulo 13, c'est-à-dire un reste noté $\text{inv}_{13}(5)$ tel que $5 \times \text{inv}_{13}(5) \equiv 1 \pmod{13}$.

a) Donner une solution dans $\mathbb{Z}^2$ de l'équation diophantienne $5u + 13v = 1$. ..... ☐

b) Déterminer l'inverse de 5 modulo 13. ..... ☐

c) Résoudre l'équation $5x + 4 \equiv 7 \pmod{13}$ dans $\mathbb{Z}$. ..... ☐

Calcul 23.8 — Équation diophantienne.

Soit N le nombre de couples d'entiers (x, y) solution de l'équation $(E) : 19x-6y = 1$ et vérifiant $1999 \leqslant x \leqslant 2023$ et (x_0, y_0) celle de ces solutions qui maximise y.

N vaut ..... ☐ (x_0, y_0) vaut ..... ☐

Décomposition en facteurs premiers et théorème de Fermat

Calcul 23.9 — Décomposer pour décomposer.

Donner la décomposition en facteurs premiers des entiers suivants. Il s'agit ici d'appliquer au maximum les critères élémentaires de divisibilité (par 2, 3, 4, 5 et 9).

a) 2 022 ..... ☐ c) 2 021 ..... ☐

b) 2 023 ..... ☐ d) 2 027 ..... ☐

Calcul 23.10 — Diviseur et quotient inconnus.

On divise 477 par un entier non nul inconnu, n. Le quotient est q et le reste vaut 8.

a) n vaut ..... ☐ b) q vaut ..... ☐

Calcul 23.11 — Arithmétique modulaire.

Déterminer, dans chaque cas, le reste de chaque puissance modulo l'entier proposé.

a) $3^{24} = 3^{4\times 6} \pmod{35}$ ..... ☐ d) $5^{61} \pmod{77}$ ..... ☐

b) $3^{72} \pmod{35}$ ..... ☐ e) $77^{122} \pmod{143}$ ..... ☐

c) $6^{75} \pmod{35}$ ..... ☐ f) $385^{3456} \pmod{4\,195}$ ..... ☐

Réponses mélangées

$(7,2)$ $\quad \frac{65}{18} \quad 4 \quad 7 \quad 7 \times 17^2 \quad 20 \quad (2023, 6406) \quad (-7,2)$

$4 \quad 1 \quad 2 \quad 5 \quad 66 \quad (-5,2) \quad 11 \pmod{13} \quad$ il est premier

$5 \quad 6 \quad 2 \quad (12,30) \quad 8 \pmod{13} \quad (6,7) \quad 1 \quad 29\,160 \quad 67$

$154 \quad 43 \times 47 \quad \frac{1}{29\,160} \quad (-6,7) \quad 2 \times 3 \times 337 \quad (9,8) \quad 1$

▶ Réponses et corrigés page 153

Fiche n° 23. Arithmétique

Réponses

23.1 a) ..... $\boxed{(6,7)}$

23.1 b) ..... $\boxed{(-7,2)}$

23.1 c) ..... $\boxed{(-6,7)}$

23.1 d) ..... $\boxed{(7,2)}$

23.2 a) ..... $\boxed{20}$

23.2 b) ..... $\boxed{4}$

23.3 a) ..... $\boxed{2}$

23.3 b) ..... $\boxed{4}$

23.4 ..... $\boxed{1}$

23.5 a) ..... $\boxed{154}$

23.5 b) ..... $\boxed{\frac{65}{18}}$

23.5 c) ..... $\boxed{29\ 160}$

23.5 d) ..... $\boxed{\frac{1}{29\ 160}}$

23.6 a) ..... $\boxed{(9,8)}$

23.6 b) ..... $\boxed{(12,30)}$

23.7 a) ..... $\boxed{(-5,2)}$

23.7 b) .. $\boxed{8 \pmod{13}}$

23.7 c) .. $\boxed{11 \pmod{13}}$

23.8 ..... $\boxed{5}$

23.8 .... $\boxed{(2023,6406)}$

23.9 a) ... $\boxed{2 \times 3 \times 337}$

23.9 b) ..... $\boxed{7 \times 17^2}$

23.9 c) ..... $\boxed{43 \times 47}$

23.9 d). $\boxed{\text{il est premier}}$

23.10 a) ..... $\boxed{67}$

23.10 b) ..... $\boxed{7}$

23.11 a) ..... $\boxed{1}$

23.11 b) ..... $\boxed{1}$

23.11 c) ..... $\boxed{6}$

23.11 d) ..... $\boxed{5}$

23.11 e) ..... $\boxed{66}$

23.11 f) ..... $\boxed{2}$

Corrigés

23.1 a) $61 = 6 \times 9 + 7$.

23.1 b) Puisque $61 = 6 \times 9 + 7$ alors $-61 = (-6) \times 9 - 7 = (-7) \times 9 + 2$.

23.1 c) $61 = 6 \times 9 + 7$ implique $61 = (-6) \times (-9) + 7$.

23.1 d) Comme $61 = 6 \times 9 + 7$ alors $-61 = 6 \times (-9) - 7 = 7 \times (-9) + 2$.

23.2 a) $524 = 26d + r$ avec $0 \leqslant r < d$. On en déduit que $26d \leqslant 524 < 27d$ et $\dfrac{524}{27} < d \leqslant \dfrac{524}{26}$. D'où $d = 20$.

23.2 b) $r = 524 - 26 \times 20 = 4$.

23.3 a) $5 \equiv 2 \pmod 3$ et $5^2 \equiv 2^2 \equiv 4 \pmod 3$. Tout dépend de la parité de 2 021. Finalement $5^{2021} \equiv 5 \equiv 2 \pmod 3$.

23.3 b) $3^2 \equiv 4 \equiv -1 \pmod 5$ d'où $3^4 \equiv (-1)^2 \equiv 1 \pmod 3$. Le reste de 3^n modulo 5 dépend du reste de n modulo 4. Puisque $2\ 022 = 505 \times 4 + 2 \equiv 2 \pmod 4$ alors $3^{2\ 022} \equiv 3^2 \equiv 4 \pmod 5$.

23.4 $2\ 023 \equiv 3 \pmod{10}$ et $3^2 \equiv 9 \equiv -1 \pmod{10}$, par conséquent $3^4 \equiv (-1)^2 \equiv 1 \pmod{10}$. Les restes modulo 10 des puissances de 3 sont périodiques de période 4. Puisque $2\ 022 = 505 \times 4 + 2 \equiv 2 \pmod 4$ alors $\forall n \geqslant 2, 2\ 022^n \equiv 0 \pmod 4$. Finalement $2\ 023^{2022^{2021}} \equiv 3^0 \equiv 1 \pmod{10}$.

23.5 a) L'algorithme d'Euclide s'écrit ici : $10\ 010 = 3 \times 2\ 772 + 1\ 694$, $2\ 772 = 1 \times 1\ 694 + 1\ 078$, $1\ 694 = 1 \times 1\ 078 + 616$, $1\ 078 = 1 \times 616 + 462$, $616 = 1 \times 462 + 154$ et $462 = 3 \times 154 + 0$. Le dernier reste non nul est $10\ 010 \wedge 2\ 772 = 154$.

23.5 b) En utilisant le résultat du a), on établit que $10\ 001 = 154 \times 65$ et $2\ 772 = 154 \times 18$ d'où $\dfrac{10\ 001}{2\ 772} = \dfrac{65}{18}$.

23.5 c) L'algorithme d'Euclide pour 729 et 360 donne : $729 = 2 \times 360 + 9$ et $360 = 40 \times 9 + 0$. D'où $729 \wedge 360 = 9$ et, comme $a \times b = (a \wedge b) \times (a \vee b)$, $729 \vee 360 = \dfrac{360 \times 729}{9} = 40 \times 729 = 29\ 160$.

Ces calculs (et surtout les calculs fractionnaires) auraient été plus digestes en utilisant la décomposition en facteurs premiers des deux entiers : $360 = 36 \times 10 = 2^3 \times 3^2 \times 5$ et $729 = 3^6$. Ainsi $729 \vee 360 = 2^3 \times 3^6 \times 5$... Il faut néanmoins effectuer ce produit d'une façon ou d'une autre.

.....

23.5 d) D'après les calculs faits au c), puisque $\dfrac{360}{729 \wedge 360} = \dfrac{360}{9} = 40$ et $\dfrac{729}{729 \wedge 360} = \dfrac{729}{9} = 81$, on réduit au même dénominateur : $\dfrac{1}{360} - \dfrac{2}{729} = \dfrac{81}{360 \times 81} - \dfrac{2 \times 40}{729 \times 40} = \dfrac{81 - 80}{29\ 160} = \dfrac{1}{29\ 160}$.

.....

23.6 a) Puisque $a \wedge b = 24$, il existe $(x, y) \in \mathbb{N}^2$ premiers entre eux tels que $a = 24x$ et $b = 24y$. Le système s'écrit alors $\begin{cases} (24x)^2 - (24y)^2 = 24^2 \times 17 \\ x \wedge y = 1 \end{cases}$ soit $\begin{cases} (x+y)(x-y) = 17 \\ x \wedge y = 1 \end{cases}$. Ainsi les deux entiers $x + y$ et $x - y$ sont-ils des diviseurs de 17. Puisque x et y sont des naturels, on a $x - y \leqslant x + y$ et donc nécessairement $x + y = 17$ et $x - y = 1$. On obtient une unique solution : $(x, y) = (9, 8)$. On vérifie que $(a, b) = (216, 192)$ est bien (l'unique !) solution du système de départ.

.....

23.6 b) Puisque $\forall (a, b) \in \mathbb{Z}^2, ab = (a \wedge b) \times (a \vee b)$, le système l'énoncé équivaut à $\begin{cases} a \times b = 360 \\ a \wedge b = 6 \\ 6 < a < b \end{cases}$. Posons $a = 6x$ et $b = 6y$ de sorte que $x \wedge y = 1$. On obtient le système équivalent $\begin{cases} xy = 10 \\ x \wedge y = 1 \\ 1 < x < y \end{cases}$.

Puisque $10 = 2 \times 5$ et $1 < x < y$, la seule solution du système est $(x, y) = (2, 5)$ et, par conséquent $(a, b) = (12, 30)$.

.....

23.7 a) L'algorithme d'Euclide pour 13 et 5 donne : $13 = 2 \times 5 + 3$; $5 = 1 \times 3 + 2$; $3 = 1 \times 2 + 1$. On "remonte" ces égalités : $1 = 3 - 1 \times 2 = 3 - (5 - 1 \times 3) = 2 \times 3 - 1 \times 5 = 2 \times (13 - 2 \times 5) - 1 \times 5 = 2 \times 13 - 5 \times 5$. Et $(-5, 2)$ est solution.

.....

23.7 b) D'après le a) : $5 \times (-5) + 2 \times 13 = 1$ d'où $5 \times (-5) \equiv 1 \pmod{13}$. Ainsi $\text{inv}_{13}(5) \equiv 8 \equiv -5 \pmod{13}$.

.....

23.7 c) $5x + 4 \equiv 7 \pmod{13} \iff 5x \equiv 3 \pmod{13}$. On en déduit que $8 \times 5x \equiv 8 \times 3 \equiv 24 \equiv 11 \pmod{13}$ et, puisque 8 est l'inverse de 5 modulo 13, que $x \equiv 11 \pmod{13}$. Réciproquement, on vérifie que tous les entiers congrus à 11 modulo 13 sont solution de l'équation. Son ensemble de solutions est donc $\{x \in \mathbb{Z} \mid x \equiv 11 \pmod{13}\}$.

.....

23.8 L'algorithme d'Euclide pour 19 et 6 se résume à $19 = 3 \times 6 + 1$ et $6 = 6 \times 1 + 0$. Ceci donne directement une solution particulière de (E) : $(1, 3)$. Si (x, y) est solution de (E) alors $19x - 6y = 19 \times 1 - 6 \times 3$ et $19(x - 1) = 6(y - 3)$. $19 \wedge 6 = 1$ et 19 divise $6(y - 3)$, d'après le théorème de Gauss, 19 divise $y - 3$. Ainsi $\exists k \in \mathbb{Z}, y = 19k + 3$. On en déduit que $19(x - 1) = 6 \times 19k$ et finalement que $x = 6k + 1$. On a prouvé que si (x, y) est solution de (E) alors $\exists k \in \mathbb{Z}, (x, y) = (6k + 1, 19k + 3)$. Réciproquement, un couple de cette forme vérifie $19(6k + 1) - 6(19k + 3) = 19 - 18 = 1$ et est bien solution de (E). D'où l'ensemble des solutions de l'équation : $\mathcal{S} = \{(6k + 1, 19k + 3) \mid k \in \mathbb{Z}\}$.

$$\begin{cases} (x, y) \in \mathcal{S} \\ 1999 \leqslant x \leqslant 2023 \end{cases} \iff \begin{cases} (x, y) = (6k + 1, 19k + 3) \\ 1999 \leqslant 6k + 1 \leqslant 2023 \end{cases} \iff \begin{cases} (x, y) = (6k + 1, 19k + 3) \\ 333 \leqslant k \leqslant 337 \end{cases}.$$

Il y a $N = 337 - 333 + 1 = 5$ entiers entre 333 et 337 inclus.

.....

23.8 $k \mapsto 19k + 3$ est une fonction croissante de k, le plus grand y est donc atteint lorsque $k = 337$. D'où $(x_0, y_0) = (2023, 6406)$.

.....

23.9 a) 2 022 est pair et divisible par 3 et $2\ 022 = 2 \times 3 \times 337$. Puisque $\sqrt{337} < 19$ il faut tester la divisibilité de cet entier par tous les premiers inférieurs ou égaux à 17. 337 n'est pas divisible par 5 et on obtient successivement $337 \equiv 1 \pmod{7}$, $337 \equiv 7 \pmod{11}$, $337 \equiv 12 \pmod{13}$ et $337 \equiv 14 \pmod{17}$. 337 est donc premier.

.....

23.9 b) En appliquant les critères, on établit que 2 023 n'est pas divisible par 2, 3 ou 5. La division euclidienne de 2023 par 7 s'écrit $2\,023 = 7 \times 289$. Si on ne reconnaissait pas le carré de 17, il fallait tester la divisibilité par 11 (évidemment négatif), 13 et 17 pour obtenir la décomposition $2\,023 = 7 \times 17^2$.

.....

23.9 c) On a $\sqrt{2\,021} < 45$: il suffit donc de tester la divisibilité par tous les premiers jusqu'à 43. 2 021 n'est pas divisible par 2, 3 ou 5. On obtient (en posant les divisions ?) un résultat négatif pour le test de divisibilité par tous les premiers compris entre 7 et 41. Par contre 43 divise 2 021 et le quotient vaut 47. Enfin, on a $2\,021 = 43 \times 47$, les deux facteurs étant premiers.

.....

23.9 d) On a $\sqrt{2\,027} \approx 45$. Il faut donc tester la divisibilité par tous les premiers jusqu'à 43. C'est le bon moment pour programmer une fonction en Python qui teste la divisibilité de son argument par tous les entiers impairs compris entre 3 et sa racine carrée. Le test est ici systématiquement négatif, 2 027 est donc premier.

.....

23.10 a) On écrit $477 = q \times n + 8$ avec $0 \leqslant 8 < n$. D'où $q \times n = 469$. n est donc un diviseur de 469 strictement supérieur à 8. Puisque la décomposition en facteurs premiers de 469 est $469 = 7 \times 67$, on a nécessairement $n = 67$.

.....

23.10 b) Puisque $469 = 7 \times 67$, on a nécessairement $q = 7$.

.....

23.11 a) D'après le théorème de Fermat, puisque 3 est premier à la fois avec 5 et 7, $3^4 \equiv 1 \pmod 5$ et $3^6 \equiv 1 \pmod 7$. On en déduit, d'une part, que $3^{24} = (3^4)^6 \equiv 1^6 \equiv 1 \pmod 5$ et, de l'autre, que $3^{24} = (3^6)^4 \equiv 1^4 \equiv 1 \pmod 7$. C'est un corollaire connu du théorème de Gauss (à démontrer en exercice !) que puisque $3^{24} - 1$ est divisible par 5 et 7, deux entiers premiers entre eux, alors $3^{24} - 1$ est divisible par $5 \times 7 = 35$. D'où $3^{24} \equiv 1 \pmod{35}$

.....

23.11 b) On déduit immédiatement du a) que $3^{72} \equiv (3^{24})^3 \equiv 1^3 \equiv 1 \pmod{35}$.

.....

23.11 c) Puisque $2 \wedge 5 = 2 \wedge 7 = 1$, on établit comme aux a) et b) que $2^{72} \equiv 1 \pmod{35}$. D'où $6^{72} = (2 \times 3)^{72} = 2^{72} \times 3^{72} \equiv 1 \times 1 \pmod{35}$. Enfin, $6^{75} = 6^{72} \times 6^3 \equiv 1 \times 6^3 \equiv 6 \pmod{35}$.

.....

23.11 d) En procédant comme aux a) et b) avec $5^{6\times10+1}$ modulo 7×11, on obtient que $5^{61} \equiv 5 \pmod{77}$.

.....

23.11 e) Idem avec $(7 \times 11)^{10\times12+2} \pmod{11 \times 13}$: $77^{61} \equiv 77^2 \equiv 66 \pmod{77}$.

.....

23.11 f) Idem pour $(5 \times 7 \times 11)^{12\times16\times18} \pmod{13 \times 17 \times 19}$. On obtient pour reste 1.

.....