

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 $b = 9$

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

c) $a = 61$ 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 modulo 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^{1789} par 3 vaut

b) Le reste de 3^{1790} par 5 vaut

Calcul 23.4 — Encore des modulus.



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 $1\,003^{1002^{1001}}$ 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

b) La forme irréductible de $\frac{10\,010}{2\,772}$ est

c) $729 \vee 360$ vaut

d) $\frac{1}{360} - \frac{2}{729}$ vaut

Calcul 23.6 — Systèmes diophantiens.



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

a) $\begin{cases} a^2 - b^2 = 9\,792 \\ a \wedge b = 24 \end{cases}$..

b) $\begin{cases} a \times b = 360 \\ a \vee b = 60 \\ 6 < a < b \end{cases}$

Coprimauté, 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 — Autour d'une équation diophantienne.



On considère N le nombre de couples d'entiers (x, y) solutions de l'équation $(E) : 19x - 6y = 1$ et vérifiant $3\,001 \leq x \leq 3\,331$ et on considère (x_0, y_0) celle de ces solutions qui maximise y .

a) N vaut

b) (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 | <input type="text"/> | c) 2 021 | <input type="text"/> |
| b) 2 023 | <input type="text"/> | d) 2 027 | <input type="text"/> |

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 | <input type="text"/> | b) q vaut | <input type="text"/> |
|-------------------|----------------------|-------------------|----------------------|

Calcul 23.11 — Arithmétique modulaire.



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

- | | | | |
|--|----------------------|-----------------------------------|----------------------|
| a) $3^{24} = 3^{4 \times 6} \pmod{35}$ | <input type="text"/> | d) $5^{61} \pmod{77}$ | <input type="text"/> |
| b) $3^{72} \pmod{35}$ | <input type="text"/> | e) $77^{122} \pmod{143}$ | <input type="text"/> |
| c) $6^{75} \pmod{35}$ | <input type="text"/> | f) $385^{3456} \pmod{4195}$ | <input type="text"/> |