

Chapitre 01 – Corrections

Arithmétique des entiers et congruences

20 exercices progressifs – Solutions détaillées

Exercice 1 – Algorithme d'Euclide

Les divisions euclidiennes successives donnent un dernier reste non nul égal à 6. Le quotient simplifié est $\frac{14}{5}$. En particulier les numérateur et dénominateur réduits sont premiers entre eux.

Exercice 2 – Algorithme d'Euclide

Les divisions euclidiennes successives donnent un dernier reste non nul égal à 21. Le quotient simplifié est $\frac{5}{2}$. En particulier les numérateur et dénominateur réduits sont premiers entre eux.

Exercice 3 – Algorithme d'Euclide

Les divisions euclidiennes successives donnent un dernier reste non nul égal à 12. Le quotient simplifié est $\frac{12}{5}$. En particulier les numérateur et dénominateur réduits sont premiers entre eux.

Exercice 4 – Algorithme d'Euclide

Les divisions euclidiennes successives donnent un dernier reste non nul égal à 17. Le quotient simplifié est $\frac{13}{5}$. En particulier les numérateur et dénominateur réduits sont premiers entre eux.

Exercice 5 – Algorithme d'Euclide

Les divisions euclidiennes successives donnent un dernier reste non nul égal à 21. Le quotient simplifié est $\frac{12}{5}$. En particulier les numérateur et dénominateur réduits sont premiers entre eux.

Exercice 6 – Bézout et inverse

On a $5 \times 5 + 12 \times (-2) = 1$. Donc $\bar{5}$ est l'inverse de $\bar{5}$ modulo 12. Les deux entiers sont premiers entre eux.

Exercice 7 – Bézout et inverse

On a $7 \times 13 + 15 \times (-6) = 1$. Donc $\overline{13}$ est l'inverse de $\bar{7}$ modulo 15. Les deux entiers sont premiers entre eux.

Exercice 8 – Bézout et inverse

On a $8 \times 8 + 21 \times (-3) = 1$. Donc $\bar{8}$ est l'inverse de $\bar{8}$ modulo 21. Les deux entiers sont premiers entre eux.

Exercice 9 – Bézout et inverse

On a $11 \times 11 + 24 \times (-5) = 1$. Donc $\overline{11}$ est l'inverse de $\overline{11}$ modulo 24. Les deux entiers sont premiers entre eux.

Exercice 10 – Bézout et inverse

On a $13 \times 7 + 30 \times (-3) = 1$. Donc $\overline{7}$ est l'inverse de $\overline{13}$ modulo 30. Les deux entiers sont premiers entre eux.

Exercice 11 – Équation diophantienne

Non : le PGCD $6 > 1$ divise tout membre gauche mais ne divise pas 1. La divisibilité par le PGCD est une condition nécessaire, et ici elle échoue.

Exercice 12 – Équation diophantienne

Non : le PGCD $5 > 1$ divise tout membre gauche mais ne divise pas 1. La divisibilité par le PGCD est une condition nécessaire, et ici elle échoue.

Exercice 13 – Équation diophantienne

Non : le PGCD $7 > 1$ divise tout membre gauche mais ne divise pas 1. La divisibilité par le PGCD est une condition nécessaire, et ici elle échoue.

Exercice 14 – Équation diophantienne

Non : le PGCD $8 > 1$ divise tout membre gauche mais ne divise pas 1. La divisibilité par le PGCD est une condition nécessaire, et ici elle échoue.

Exercice 15 – Équation diophantienne

Non : le PGCD $6 > 1$ divise tout membre gauche mais ne divise pas 1. La divisibilité par le PGCD est une condition nécessaire, et ici elle échoue.

Exercice 16 – Approfondissement : Euclide

Un entier divise a et b si et seulement s'il divise b et $a - qb$. Les ensembles de diviseurs communs sont identiques ; leurs plus grands éléments positifs coïncident.

Exercice 17 – Approfondissement : Gauss

Bézout donne $ua + vb = 1$. En multipliant par c : $c = uac + vbc$. Les deux termes du membre droit sont divisibles par a , donc c aussi.

Exercice 18 – Approfondissement : solutions complètes

Une solution est $(2, -1)$. Toute autre vérifie $3(x - 2) = -5(y + 1)$; Gauss donne $x - 2 = 5k$, puis $y + 1 = -3k$. Donc $(x, y) = (2 + 5k, -1 - 3k)$, $k \in \mathbb{Z}$.

Exercice 19 – Approfondissement : Fermat

$2^3 = 8 \equiv 1 \pmod{7}$. Comme $100 = 3 \times 33 + 1$, $2^{100} \equiv 2 \pmod{7}$. Ce calcul direct évite toute hypothèse supplémentaire.

Exercice 20 – Approfondissement : infinité des premiers

Si la liste complète était $p_1, \dots, p_k$, l'entier $N = p_1 \cdots p_k + 1 > 1$ aurait un diviseur premier. Aucun p_i ne divise N , car le reste serait 1. Contradiction.