Université Paris Cité

MM1 - Mathématiques 1

Année 2025-26

L1 Math, Math-Info, METIS, DLMP

Feuille d'exercices n° 1

Arithmétique

Notions du cours. Divisibilité dans $\mathbb{Z}$; notation $x|y$. Diviseurs, multiples. Division euclidienne. Congruences : égalité de deux entiers modulo k. Manipulations de congruences. Résolution de systèmes de congruences à deux équations.
Plus grand commun diviseur de deux entiers strictement positifs, de deux entiers relatifs ; notation $x \wedge y$. Plus petit commun multiple de deux entiers strictement positifs, de deux entiers relatifs ; notation $x \vee y$. Relation $xy = (x \wedge y) \cdot (x \vee y)$. Utilisation des définitions "plus grand élément" et "plus petit élément" relatives à l'ordre de divisibilité. Algorithme d'Euclide. Mise en œuvre de l'algorithme sur de petits nombres.
Entiers premiers entre eux. Lemme de Gauss. Relation de Bézout. Algorithme d'Euclide étendu. Mise en œuvre de l'algorithme d'Euclide étendu sur de petits nombres. Application à la résolution d'équations de type $ax + by = c$ dans $\mathbb{Z}$.
Nombres premiers. Décomposition d'un nombre en facteurs premiers. Unicité de cette décomposition à l'ordre près des facteurs. Expression de $x \wedge y$ et de $x \vee y$ connaissant les décompositions en facteurs premiers de x et de y.

1 Exercices d'entraînement

1.1 Divisibilité et congruences

Exercice 1.

1. En système décimal, comment voit-on simplement qu'un entier est divisible par 4 ?
2. Montrer qu'un entier strictement positif est divisible par 9 si et seulement si la somme de ses chiffres décimaux l'est.

Exercice 2. Montrer que $7 \mid 10a + b$ si et seulement si $7 \mid a - 2b$. Le nombre 2471 est-il divisible par 7 ?

Exercice 3. Montrer que pour tout entier n :

1. 3 divise $n^3 + 5n$.
2. 5 divise $11^n - 6$.
3. $n + 1$ divise $n^{13} + 1$.

Exercice 4. Soit $n \geq 1$ un entier. Déterminer le reste dans la division euclidienne par n de la somme des n premiers entiers strictement positifs.

Exercice 5.

1. Déterminer, suivant les valeurs de $n \in \mathbb{N}$, le reste de la division euclidienne de 2^n par 5.
2. Quel est le reste de la division par 5 de 1357^{2013} ?

Exercice 6.

1. Quel est le dernier chiffre de 7777^{7777} ?
2. Quel est le reste de la division euclidienne de 900^{200} par 7 ?

Exercice 7. Trouver le reste de la division euclidienne de 10^{1000} par 13.

Exercice 8. Résoudre les équations suivantes, d'inconnue $x \in \mathbb{Z}$.

1. $5x \equiv 1 \bmod 7$
2. $7x \equiv 0 \bmod 10$
3. $12x + 5 \equiv 9 \bmod 31$
4. $2^{10}x + 2^8 \equiv 2^4 \bmod 15$
5. $x^2 \equiv 1 \bmod 7$
6. $x^2 \equiv 4 \bmod 13$
7. $x^2 \equiv 3 \bmod 5$

1.2 PGCD et PPCM, nombres premiers entre eux

Exercice 9. Montrer que pour tout entier n :

1. $n(n+1)(n+2)(n+3)$ est divisible par 24.
2. $n(n+1)(n+2)(n+3)(n+4)$ est divisible par 120.

Exercice 10.

1. Calculer $\mathsf{pgcd}(13, 7)$, $\mathsf{pgcd}(13, 20)$, $\mathsf{pgcd}(13, 33)$.
2. Soit $n \in \mathbb{N}$. Calculer $\mathsf{pgcd}(13, 7 + 13n)$.

Exercice 11. Déterminer les entiers m, n satisfaisant $m + n = 72$ et $m \wedge n = 9$.

Exercice 12. Déterminer $a \wedge b$ et une relation de Bézout $au + bv = a \wedge b$ pour les couples d'entiers (a, b) suivants (utiliser l'algorithme d'Euclide dès que nécessaire).

1. $(a, b) = (5, 7)$
2. $(a, b) = (8, 12)$
3. $(a, b) = (7, 25)$
4. $(a, b) = (169, 60)$
5. $(a, b) = (8911, 213)$
6. $(a, b) = (1444764, 8766)$

Exercice 13. On pose $a = 46848$, $b = 2379$, $c = 8633$ et $d = 4183$. Calculer $a \wedge b$ et $c \wedge d$ de deux façons différentes : avec l'algorithme d'Euclide, et en décomposant les nombres en facteurs premiers. Quelle méthode vous semble plus efficace? (Approfondir cette question en résolvant l'exercice 31).

Exercice 14. Résoudre les équations suivantes, d'inconnues $a, b \in \mathbb{Z}$.

1. $\mathsf{pgcd}(a, b) = 8$
2. $\mathsf{pgcd}(a, b) = 6$
3. $\mathsf{ppcm}(a, b) = 96$

Exercice 15. Les équations suivantes, d'inconnues $x, y \in \mathbb{Z}$, ont-elles une solution ? Si oui, résoudre l'équation.

1. $4x + 7y = 3$
2. $6x + 9y = 3$
3. $45x + 85y = 35$
4. $45x + 85y = 32$
5. $9x + 15y = 11$
6. $9x + 15y = 18$

Exercice 16.

1. Soit $(x, y) \in \mathbb{N}^2$ tel que $\mathsf{pgcd}(x, y) = 1$ et $\mathsf{ppcm}(x, y) = 611$. Déterminer les couples (x, y).
2. Soit $(x, y) \in \mathbb{N}^2$ tel que $\mathsf{pgcd}(x, y) = 13$ et $\mathsf{ppcm}(x, y) = 611$. Déterminer les couples (x, y).
3. Soit $(x, y) \in \mathbb{N}^2$ tel que $\mathsf{pgcd}(x, y) = 13$ et $\mathsf{ppcm}(x, y) = 338$. Déterminer les couples (x, y).
4. Existe-t-il des couples $(x, y) \in \mathbb{N}^2$ tel que $\mathsf{pgcd}(x, y) = 563$ et $\mathsf{ppcm}(x, y) = 10567$?

Exercice 17. Soit $n \geq 2$ un entier.

1. Si n n'est pas premier, montrer que n possède un facteur premier inférieur ou égal à $\sqrt{n}$.
2. En déduire qu'un entier $n \in [10, 100]$ est premier si et seulement si il est premier à 210.

Exercice 18.

1. Soit $n \geq 1$ un entier. Montrer que a et b sont premiers entre eux si et seulement si a^n et b^n le sont.
2. Montrer que a et b sont premiers entre eux si et seulement si $a + b$ et ab le sont.

Pour chacune des deux questions ci-dessus, on cherchera une méthode utilisant la relation de Bézout et une méthode utilisant la primalité.

1.3 Nombres premiers

Exercice 19. Décomposer 15! en produit de nombres premiers.

Exercice 20.

1. Donner l'ensemble des diviseurs de 10, de 30, de 2^5, de 36.
2. Combien y a-t-il de diviseurs de 5! ?
3. Quel est le nombre de diviseurs de 7, de 105, de 2020, de 10000 ?
4. Donner la liste des diviseurs de 36, de 100.

Exercice 21. Donner tous les diviseurs premiers de 2025.

Exercice 22. Soient p un nombre premier et k un entier tel que $1 \leq k \leq p - 1$. Montrer que p divise $\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!}$.

Exercice 23. Soit $n = 167$.

1. Pour $p \in \{2, 3, 5, 7, 11\}$, calculer le reste de la division euclidienne de n par p.
2. En déduire que n est un nombre premier.

Exercice 24.

1. Soit $n \in \mathbb{N}$ vérifiant $n \equiv 3\ [4]$. Montrer que n possède un facteur premier p vérifiant $p \equiv 3\ [4]$.
2. Soit $k > 0$ et $p_1, \ldots, p_k$ des nombres premiers congrus à 3 modulo 4. Soit $n = 4p_1p_2 \cdots p_k - 1$. Montrer que n possède un diviseur premier p vérifiant $p \equiv 3\ [4]$ et $p \notin \{p_1, p_2, \ldots, p_k\}$.
3. En déduire qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

2 Exercices d'approfondissement

Exercice 25. Soient $a, b \in \mathbb{N}$. Montrer que $7 \mid a^2 + b^2$ si et seulement si $7 \mid a$ et $7 \mid b$ (indication : vous pouvez étudier les valeurs possibles de a^2 et b^2 modulo 7).

Exercice 26.

1. Montrer que tout nombre impair au carré est congru à 1 modulo 8.
2. Etudier les congruences possibles modulo 8 pour les carrés de nombres pairs.
3. Etudier la congruence modulo 8 de $a^2 + b^2 + c^2$, où a, b, et c sont impairs. Est-ce le carré d'un nombre entier?
4. En déduire la congruence modulo 8 de $2(ab + bc + ac)$. Est-ce le carré d'un nombre entier?
5. $ab + bc + ac$ est-il le carré d'un nombre entier?

Exercice 27. Résoudre les systèmes de congruences suivants.

1. $\begin{cases} x \equiv 2 \bmod 7 \\ x \equiv 3 \bmod 11 \end{cases}$
2. $\begin{cases} x \equiv 4 \bmod 21 \\ x \equiv 10 \bmod 33 \end{cases}$
3. $\begin{cases} x \equiv 3 \bmod 17 \\ x \equiv 4 \bmod 11 \\ x \equiv 5 \bmod 6 \end{cases}$

Exercice 28. Soit n un entier impair et non divisible par 3. Montrer que $n^2 \equiv 1 \bmod 24$.

Exercice 29.

1. Calculer $\mathsf{pgcd}(2^{21} - 1, 2^{35} - 1)$.
2. Montrer que pour tous $n, a, b > 1$, $\mathsf{pgcd}(n^a - 1, n^b - 1) = n^{\mathsf{pgcd}(a,b)} - 1$.

Exercice 30. Soit $a \geq 2$ un entier.

1. Montrer que pour tout $n > 1$, $a - 1$ divise $a^n - 1$.
2. Montrer que si $\frac{a^n - 1}{a - 1}$ est un nombre premier, alors n est un nombre premier.
3. La réciproque est-elle vraie ?

Exercice 31 (complexité de l'algorithme d'Euclide). On rappelle que l'algorithme d'Euclide peut être présenté par la fonction `euclide`$(\cdot, \cdot)$ définie ainsi:

$$\texttt{euclide}(a, b) = \begin{cases} a, & \text{si } b = 0, \\ \texttt{euclide}(b, r), & \text{si } b \neq 0, \text{ et où } a = bq + r \text{ avec } 0 \leq r < b. \end{cases}$$

On appelle *nombre d'étapes* dans l'exécution de l'algorithme le nombre d'appels *récursifs* de la fonction `euclide`. Par exemple, `euclide`$(a, 0)$ s'effectue en 0 étape.
On définit la suite de Fibanocci $(F_n)_{n \geq 0}$ par la relation de récurrence suivante:

$$F_0 = 0, \quad F_1 = 1, \qquad \forall n \geq 0, \quad F_{n+2} = F_n + F_{n+1}\,.$$

1. Montrer par récurrence sur $k \geq 0$ que : si a et b sont deux entiers positifs avec $a > 0$ et $a \geq b$ et si `euclide`(a, b) s'effectue en k étapes, alors $a \geq F_{k+1}$ et $b \geq F_k$.

2. En déduire que pour tout entier $k \geq 1$ et pour tous entiers $a, b \geq 0$ avec $a \geq b$, si $b < F_k$ alors $\texttt{euclide}(a, b)$ s'effectue en au plus k étapes.

3. Montrer par récurrence sur $k \geq 0$ que $\texttt{euclide}\, F_{k+1} F_k$ s'effectue en exactement k étapes.

4. On note $\rho = \dfrac{1+\sqrt{5}}{2}$ (appelé *nombre d'or*). En admettant les deux résultats suivants:

   (a) $\lim\limits_{n\to\infty} \dfrac{F_{n+1}}{F_n} = \rho$,

   (b) $F_n \sim \dfrac{\rho^n}{\sqrt{5}}$,

   montrer que le nombre d'étapes pour effectuer $\texttt{euclide}(a, b)$ est $O(\log b)$, c'est-à-dire qu'il existe une constante $C > 0$ telle que, si $N(a, b)$ désigne le nombre d'étapes dans l'évaluation de la fonction $\texttt{euclide}(a, b)$, on a :

$$N(a, b) \leq C \log b\,.$$

Exercice 32. Montrer que $a \wedge b = a \wedge (a - b)$. En déduire une fonction algorithmique `preeuclide` qui calcule le pgcd de deux entiers. Comparer l'exécution des deux algorithmes pour le calcul de $\texttt{preeuclide}(120, 48)$ et $\texttt{euclide}(120, 48)$.

3 Exercices d'évaluation

Exercice 33 (CC MIASHS 2019). Calculer $d = \texttt{pgcd}(188, 55)$ et trouver un couple $(u, v) \in \mathbb{Z}^2$ tel que $d = 188u + 55v$.

Exercice 34 (CC MIASHS 2019). Trouver les solutions dans $\mathbb{Z}$ de l'équation $4x - 20 \equiv 22 \bmod 26$.

Exercice 35 (CC Math et Math-Info 2019).

1. Montrer que 10 divise $4^{11} + 11^{16} + 15$.

2. Quelles sont les solutions $x \in \mathbb{Z}$ de l'équation $7x + 2 \equiv 8 \bmod 9$?

3. Résoudre l'équation $154x + 91y = 7$, d'inconnues $x, y \in \mathbb{Z}$. On détaillera la méthode utilisée.

Exercice 36 (CC Math et Math-Info 2019). On considère l'équation $3x^2 + 2y^2 = z^2$, d'inconnues $x, y, z \in \mathbb{Z}$. On suppose l'existence d'une solution $x, y, z \in \mathbb{Z}$.

1. Montrer que y et z sont divisibles par 3.

2. Montrer que x est aussi divisible par 3.

3. On suppose que l'équation admet une solution d'entiers x, y, z non tous nuls. Soit d le plus grand entier qui divise à la fois x, y et z. Montrer que $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ est solution de l'équation.

4. Montrer que l'équation admet une unique solution $(0, 0, 0)$.

Exercice 37 (CC Math et Math-Info 2019). Soient a, b, c des entiers tels que chacun divise le produit des deux autres. On suppose que a et b sont premiers entre eux. Déterminer c.

Exercice 38 (CC Math et Math-Info 2019).

1. Décomposer en facteurs premiers les nombres 385 et 33. En déduire les valeurs de $\mathsf{pgcd}(385, 33)$ et $\mathsf{ppcm}(385, 33)$.

2. Résoudre l'équation $385x + 33y = 22$, d'inconnues $x, y \in \mathbb{Z}$.

3. Montrer que 15 divise la somme $\displaystyle\sum_{0 \leq k < 2020} 2^k$.

   (*Indication : remarquer que* $1 + 2 + 2^2 + 2^3 = 15$ *et que* 2020 *est divisible par* 4.)