Préparation à l'agrégation externe de Mathématiques 2026-2027
Université Paris Cité-Grands Moulins

Arithmétique

Muriel Livernet

1. Cours

Notions du cours. Ordre de divisibilité dans $\mathbb{N}$, dans $\mathbb{Z}$; notation $x|y$. Diviseurs, multiples. Plus grand commun diviseur de deux entiers strictement positifs, de deux entiers relatifs ; notation $x \wedge y = \mathsf{pgcd}(x, y)$. Plus petit commun multiple de deux entiers strictement positifs, de deux entiers relatifs ; notation $x \vee y = \mathsf{ppcm}(x, y)$. Relation $xy = (x \wedge y) \cdot (x \vee y)$.

Division euclidienne.

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.

Entiers premiers entre eux. Lemme de Gauss. Relation de Bézout.

Lien entre congruences modulo n et l'anneau $\mathbb{Z}/n\mathbb{Z}$. Résolution de systèmes de congruences à deux équations (Lemme chinois).

Algorithme d'Euclide étendu

Soient $a > b > 1$ deux entiers. On cherche à calculer $\mathsf{pgcd}(a, b)$ ainsi que les coefficients de Bezout, à savoir un couple $(u, v) \in \mathbb{Z}^2$ tels que

$$au + bv = \mathsf{pgcd}(a, b).$$

L'algorithme d'Euclide permet de trouver rapidement $\mathsf{pgcd}(a, b)$. L'algorithme d'Euclide étendu permet d'extraire les coefficients de Bezout. On présente cela sous la forme d'un tableau :

Etape	r	u	v
0	$r_0 = a$	$u_0 = 1$	$v_0 = 0$
1	$r_1 = b$	$u_1 = 0$	$v_1 = 1$
i	r_i	u_i	v_i

Pour tout $i \geq 1$, r_{i+1} est le reste de la division euclidienne de r_{i-1} par r_i. Cela nous fournit les formules du tableau :

$$r_{i+1} = r_{i-1} - r_i q_i, \quad u_{i+1} = u_{i-1} - u_i q_i, \quad v_{i+1} = v_{i-1} - v_i q_i.$$

On montre par récurrence que pour tout i on a $r_i = au_i + bv_i$. Ainsi la colonne r du tableau correspond à l'algorithme d'Euclide classique, le dernier reste non nul est $\mathsf{pgcd}(a, b)$.

Exemple : $a = 120$ et $b = 23$

Etape	Division euclidienne	r	u	v
0		$r_0 = 120$	$u_0 = 1$	$v_0 = 0$
1		$r_1 = 23$	$u_1 = 0$	$v_1 = 1$
2	$120 = 23 * \underline{5} + 5$	$r_2 = 5$	$u_2 = 1$	$v_2 = -5$
3	$23 = 5 * \underline{4} + 3$	$r_3 = 3$	$u_3 = u_1 - \underline{4}u_2 = -4$	$v_3 = v_1 - \underline{4}v_2 = 21$
4	$5 = 3 * \underline{1} + 2$	$r_4 = 2$	$u_4 = u_2 - \underline{1}u_3 = 5$	$v_4 = v_2 - \underline{1}v_3 = -26$
5	$3 = 2 * \underline{1} + 1$	$r_5 = 1$	$u_5 = u_3 - 1u_4 = -9$	$v_5 = v_3 - 1v_4 = 47$
6	$2 = 1 * \underline{2} + 0$	$r_6 = 0$		

2. Exercices

Exercice 2.1. Montrer que pour tout entier n on a :

(1) 3 divise $n^3 + 5n$.

(2) 5 divise $11^n - 6$.

(3) $n + 1$ divise $n^{13} + 1$.

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

Exercice 2.2. Montrer que $7 \mid 10a + b$ si et seulement si $7 \mid a - 2b$.

Exercice 2.3. Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ un entier décomposé en produits de facteurs premiers. Combien a-t-il de diviseurs ? Combien 5! a-t-il de diviseurs ?

Exercice 2.4. Soient p un nombre premier et k un entier tel que $1 \leq k \leq p-1$. Montrer que p divise $\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!}$. Cela permet de montrer que si A est un anneau commutatif unitaire de caractéristique p alors l'application $A \to A$ qui à x associe x^p est un morphisme d'anneaux (appelé morphisme de Frobenius).

Exercice 2.5. 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 2.6. Montrer que 1013 est un nombre premier.

Exercice 2.7. Déterminer $a \wedge b$ et une relation de Bézout $au + bv = a \wedge b$ pour les couples d'entiers (a, b) suivants

(1) $(a, b) = (8, 12)$ (2) $(a, b) = (7, 25)$ (3) $(a, b) = (169, 60)$

Exercice 2.8. Les équations suivantes, d'inconnues $x, y \in \mathbb{Z}$, ont-elles une solution ? Si oui, résoudre l'équation.

(1) $4x + 7y = 3$ (3) $45x + 85y = 35$ (5) $9x + 15y = 11$

(2) $6x + 9y = 3$ (4) $45x + 85y = 32$ (6) $9x + 15y = 18$

Exercice 2.9. Déterminer les couples $(x, y) \in \mathbb{N}^2$ vérifiant

(1) $\mathsf{pgcd}(x, y) = 1$ et $\mathsf{ppcm}(x, y) = 611$.

(2) $\mathsf{pgcd}(x, y) = 13$ et $\mathsf{ppcm}(x, y) = 611$.

Exercice 2.10. Soient a, b des entiers non nuls et $n > 1$. Soit r le reste de la division euclidienne de a par b. Montrer que le reste de la division euclidienne de $n^a - 1$ par $n^b - 1$ est $n^r - 1$. En déduire que $\mathsf{pgcd}(n^a - 1, n^b - 1) = n^{\mathsf{pgcd}(a,b)} - 1$.

Exercice 2.11. (1) Quel est le dernier chiffre de 7777^{7777} ?

(2) On rappelle que si p est un nombre premier et p ne divise pas x alors $x^{p-1} \equiv 1 \mod p$. En déduire le reste de la division euclidienne de 900^{200} par 7 et le reste de la division euclidienne de 10^{1000} par 13.

Exercice 2.12. Résoudre les équations suivantes, d'inconnue $x \in \mathbb{Z}$.

(1) $7x \equiv 0 \bmod 10$

(2) $12x + 5 \equiv 9 \bmod 31$

(3) $x^2 \equiv 4 \bmod 13$

(4) $x^2 \equiv 3 \bmod 5$

Exercice 2.13. Résoudre les systèmes de congruences suivants.

$$\begin{cases} x \equiv 2 \bmod 7 \\ x \equiv 3 \bmod 11 \end{cases} \quad \text{et} \quad \begin{cases} x \equiv 4 \bmod 21 \\ x \equiv 10 \bmod 33 \end{cases}$$

Exercice 2.14. 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 2.15. (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 2.16. Soit $a \geq 2$ un entier.

(1) Montrer que pour tout $n > 0$, $a - 1$ 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 ?