Cours d'Arithmétique
Niveau Math Sup

Table des matières

1 Les entiers et la divisibilité

Définition 1.1. Soient $a, b \in \mathbb{Z}$.
On dit que a divise b s'il existe $k \in \mathbb{Z}$ tel que

$$b = ak.$$

Notation :

$$a \mid b.$$

Exemple 1.2. — $3 \mid 12$
— $5 \nmid 14$

Proposition 1.3. Si $a \mid b$ et $a \mid c$, alors :

$$a \mid (b+c), \qquad a \mid (b-c).$$

Plus généralement,

$$a \mid (\lambda b + \mu c)$$

pour tous $\lambda, \mu \in \mathbb{Z}$.

2 Division euclidienne

Théorème 2.1 (Division euclidienne)**.** Pour tout $a \in \mathbb{Z}$ et tout $b \in \mathbb{N}^*$, il existe un unique couple (q, r) tel que

$$a = bq + r$$

avec

$$0 \leq r < b.$$

Exemple 2.2.

$$47 = 5 \times 9 + 2.$$

Le reste de la division de 47 par 5 est donc 2.

3 PGCD et algorithme d'Euclide

Définition 3.1. Le plus grand commun diviseur de deux entiers a et b est noté

$$\gcd(a, b).$$

Théorème 3.2 (Algorithme d'Euclide)**.** Si

$$a = bq + r,$$

alors

$$\gcd(a, b) = \gcd(b, r).$$

Exemple 3.3. Calculons $\gcd(252, 105)$.

$$252 = 105 \times 2 + 42$$

$$105 = 42 \times 2 + 21$$

$$42 = 21 \times 2.$$

Donc

$$\gcd(252, 105) = 21.$$

3.1 Théorème de Bézout

Théorème 3.4 (Bézout)**.** Pour tous entiers $a, b \in \mathbb{Z}$, il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$au + bv = \gcd(a, b).$$

En particulier,

$$\gcd(a, b) = 1 \iff \exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1.$$

4 Nombres premiers

Définition 4.1. Un entier $p \geq 2$ est premier si ses seuls diviseurs positifs sont 1 et p.

Exemple 4.2.

$$2, 3, 5, 7, 11, 13, \ldots$$

Théorème 4.3 (Théorème fondamental de l'arithmétique)**.** Tout entier $n \geq 2$ s'écrit de manière unique, à l'ordre près, comme produit de nombres premiers.

Exemple 4.4.

$$360 = 2^3 \times 3^2 \times 5.$$

4.1 Lemme d'Euclide

Théorème 4.5. Si p est premier et

$$p \mid ab,$$

alors

$$p \mid a \qquad \text{ou} \qquad p \mid b.$$

4.2 Infinité des nombres premiers

Théorème 4.6 (Euclide)**.** Il existe une infinité de nombres premiers.

5 PPCM

Définition 5.1. Le plus petit commun multiple de deux entiers a et b est noté

$$\operatorname{lcm}(a, b).$$

Proposition 5.2.

$$\gcd(a, b) \times \operatorname{lcm}(a, b) = |ab|.$$

6 Congruences

Définition 6.1. Soit $n \geq 2$.

On dit que a est congru à b modulo n si

$$n \mid (a - b).$$

Notation :

$$a \equiv b \pmod{n}.$$

Exemple 6.2.

$$17 \equiv 2 \pmod{5}$$

car

$$17 - 2 = 15.$$

Proposition 6.3. Les congruences sont compatibles avec l'addition et la multiplication.

7 Inverses modulo n

Définition 7.1. Un entier a admet un inverse modulo n s'il existe b tel que

$$ab \equiv 1 \pmod{n}.$$

Théorème 7.2. a est inversible modulo n si et seulement si

$$\gcd(a, n) = 1.$$

Exemple 7.3. Cherchons l'inverse de 3 modulo 7.

$$3 \times 5 = 15 \equiv 1 \pmod{7}.$$

Ainsi,

$$3^{-1} \equiv 5 \pmod{7}.$$

8 Petit théorème de Fermat

Théorème 8.1 (Petit théorème de Fermat)**.** Si p est premier et $a \not\equiv 0 \pmod{p}$, alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

Exemple 8.2.

$$2^6 = 64 \equiv 1 \pmod{7}.$$

9 Théorème d'Euler

Théorème 9.1. Si $\gcd(a, n) = 1$, alors

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

où φ désigne l'indicatrice d'Euler.

10 Systèmes de congruences

Théorème 10.1 (Théorème chinois)**.** Le système

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

admet une unique solution modulo mn lorsque m et n sont premiers entre eux.

Exemple 10.2. Résoudre

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

Une solution est

$$x \equiv 8 \pmod{15}.$$

11 Exercices

Niveau 1

Exercice 11.1. Calculer :

1) $\gcd(168, 252)$
2) $\operatorname{lcm}(84, 126)$

Exercice 11.2. Décomposer 5040 en facteurs premiers.

Exercice 11.3. Résoudre

$$7x \equiv 1 \pmod{26}.$$

Niveau 2

Exercice 11.4. Montrer que

$$n^3 - n$$

est divisible par 6.

Exercice 11.5. Résoudre

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

Niveau 3

Exercice 11.6. Déterminer tous les entiers n tels que

$$\varphi(n) = 8.$$

Exercice 11.7. Montrer que

$$\sqrt{2} \notin \mathbb{Q}.$$

12 Conseils de travail

L'arithmétique demande :

— de la rigueur rédactionnelle ;
— la maîtrise des raisonnements élémentaires ;
— une bonne pratique des congruences ;
— la capacité à manipuler les décompositions en facteurs premiers.

À connaître parfaitement :

— division euclidienne ;
— algorithme d'Euclide ;
— théorème de Bézout ;
— congruences ;
— nombres premiers ;
— petit théorème de Fermat.

13 Références

— Daniel Perrin — *Cours d'algèbre*

— Jean-Marie De Koninck et Armel Mercier — *Arithmétique*

— Ramis, Deschamps, Odoux — *Algèbre MP/MP**

— Ivan Niven — *Introduction à la théorie des nombres*