Arithmétique

« La Mathématique est la reine des sciences et l'Arithmétique est la reine des mathématiques. »

— Carl Friedrich Gauss (1777–1855)

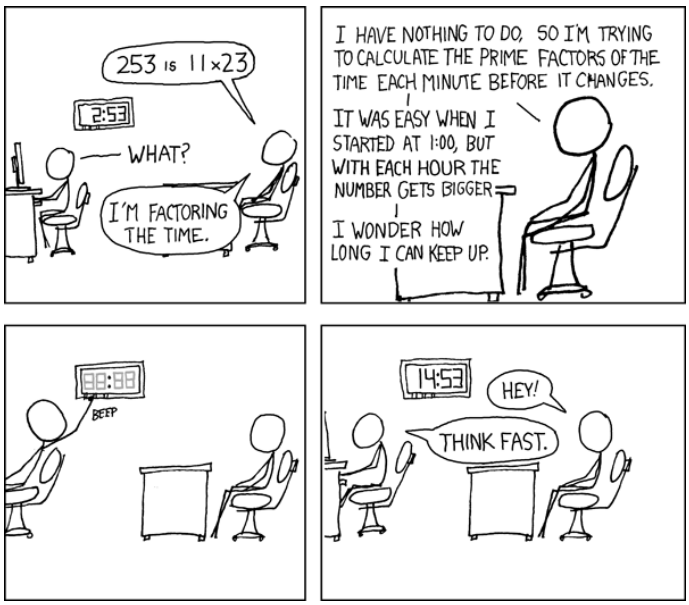

Table des matières

1 Divisibilité, division euclidienne

1.1 Relation de divisibilité

Définition 1.1

Soit $a, b \in \mathbb{Z}$. On dit que a *divise* b lorsqu'il existe $k \in \mathbb{Z}$ tel que $b = ka$.

Remarques

⇨ Soit $a, b \in \mathbb{Z}$ tels que $a|b$. Alors $-a|b$, $a|-b$ et $-a|-b$. Autrement dit, lorsqu'on parle de divisibilité, le signe n'est pas significatif.

⇨ Soit $a \in \mathbb{Z}$. Alors $a|1$ si et seulement si $a = \pm 1$.

⇨ Soit $a, b, c \in \mathbb{Z}$. Si $ac|bc$ et $c \neq 0$, alors $a|b$

Proposition 1.2

La relation de divisibilité
- est réflexive : $\forall a \in \mathbb{Z}, \quad a|a$.
- est transitive : $\forall a, b, c \in \mathbb{Z}, \quad [a|b \quad \text{et} \quad b|c] \quad \Longrightarrow \quad a|c$.
- n'est pas antisymétrique. Cependant

$$\forall a, b \in \mathbb{Z}, \quad [a|b \quad \text{et} \quad b|a] \quad \Longleftrightarrow \quad a = \pm b.$$

Remarques

⇨ La relation de divisibilité n'étant pas antisymétrique sur $\mathbb{Z}$, ce n'est pas une relation d'ordre. Cependant, si $a, b \in \mathbb{N}$, on a

$$[a|b \quad \text{et} \quad b|a] \quad \Longleftrightarrow \quad a = b.$$

En particulier, la relation de divisibilité est une relation d'ordre sur $\mathbb{N}$.

⇨ Quel que soit $n \in \mathbb{Z}$, $1|n$ et $n|0$. En particulier, pour la relation de divisibilité, $\mathbb{N}$ admet 1 pour plus petit élément et 0 pour plus grand élément.

⇨ Soit $a, b \in \mathbb{N}$. Si $a|b$ et $b \neq 0$, alors $a \leqslant b$.

Proposition 1.3

Soit $a, b, c \in \mathbb{Z}$ et $k_1, k_2 \in \mathbb{Z}$. Alors

$$[a|b \quad \text{et} \quad a|c] \quad \Longrightarrow \quad a|\left(k_1 b + k_2 c\right).$$

Exercices 1

⇨ Soit $a, b, c \in \mathbb{Z}$. Les assertions suivantes sont-elles vraies ?
- Si a divise $b + c$, alors a divise b et c.
- Si a et b divisent c, alors ab divise c.

⇨ Déterminer les entiers $n \in \mathbb{N}$ tels que $n|n + 8$.

1.2 Congruence, division euclidienne

Définition 1.4

Soit $a, b \in \mathbb{Z}$ et $m \in \mathbb{N}^*$. On dit que a est *congru* à b modulo m et on note

$$a \equiv b \quad [m]$$

lorsque $m|\left(a - b\right)$, c'est-à-dire lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b + km$.

Remarque

⇨ Si $m \in \mathbb{N}^*$, la relation binaire $\mathcal{R}$ définie sur $\mathbb{Z}$ par

$$\forall a, b \in \mathbb{Z} \quad a\mathcal{R}b \quad \Longleftrightarrow \quad a \equiv b \ [m]$$

est une relation d'équivalence.

Proposition 1.5

Soit $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ et $m \in \mathbb{N}^*$ tels que

$$a_1 \equiv b_1 \quad [m] \quad \text{et} \quad a_2 \equiv b_2 \quad [m].$$

Alors, si $k_1, k_2 \in \mathbb{Z}$ et $k \in \mathbb{N}$

$$k_1 a_1 + k_2 a_2 \equiv k_1 b_1 + k_2 b_2 \quad [m] \qquad a_1 a_2 \equiv b_1 b_2 \quad [m] \qquad \text{et} \qquad a_1^k \equiv b_1^k \quad [m].$$

Remarque

⇨ Soit $m, n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. Alors $a \equiv b \ [m] \Longleftrightarrow an \equiv bn \ [mn]$.

Exercices 2

⇨ Montrer que pour tout $n \in \mathbb{N}$, 11 divise $3^{n+3} - 4^{4n+2}$.

⇨ Trouver les $n \in \mathbb{N}$ tels que $10^n + 5^n + 1$ est un multiple de 3.

⇨ Montrer qu'un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3. De même, montrer qu'un entier est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9. Enfin, montrer qu'un nombre est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.

Proposition 1.6

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que

$$a = qb + r \quad \text{et} \quad 0 \leqslant r < b.$$

q est appelé *quotient* de la division euclidienne de a par b, r son *reste*.

Remarques

⇨ Si $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, le reste de la division euclidienne de a par b est l'unique élément r de $[\![0, b-1]\!]$ tel que $a \equiv r\ [b]$.

⇨ Les langages Python et OCaml possèdent tous les deux une division entière et un opérateur « modulo ». Si $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, la division entière s'obtient avec `a // b` en Python et avec `a / b` en OCaml. L'opérateur « modulo » s'obtient quant à lui avec `a % b` en Python et `a mod b` en OCaml. Si on note q la division entière de a par b et r le résultat de l'opérateur modulo, on aura toujours $a = qb + r$. En Python, ce sont respectivement le quotient et le reste de la division euclidienne de a par b. C'est aussi le cas en OCaml lorsque $a \geqslant 0$. Cependant, lorsque $a < 0$, ce n'est plus le cas. Par exemple, la division entière de -7 par 2 renvoie -3 alors que le quotient de la division euclidienne de -7 par 2 est -4.

⇨ Si $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, on montre qu'il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = qb + r$ et $0 \leqslant r < |b|$. On peut donc ainsi étendre la définition de la division euclidienne au cas où $b \in \mathbb{Z}^*$. Mais en pratique, on effectuera toujours des divisions euclidiennes par des entiers strictement positifs.

Exercice 3

⇨ Déterminer le reste de la division euclidienne de 4852^{203} par 5.

2 Pgcd, ppcm

2.1 Plus grand commun diviseur

Définition 2.1

Soit $a, b \in \mathbb{Z}$. Il existe un unique entier positif p tel que
- $p|a$ et $p|b$
- $\forall q \in \mathbb{Z}, \quad [q|a \quad \text{et} \quad q|b] \Longrightarrow q|p$

On l'appelle pgcd (*plus grand commun diviseur*) de a et de b et on le note $\text{pgcd}\,(a, b)$ ou $a \wedge b$.

Remarques

⇨ Si $a, b \in \mathbb{Z}$, les diviseurs de a et de b sont les diviseurs de $a \wedge b$.

⇨ Soit $a, b \in \mathbb{N}$. Pour la relation d'ordre de divisibilité sur $\mathbb{N}$, l'ensemble des diviseurs de a et de b n'est rien d'autre que l'ensemble des minorants de $\{a, b\}$. La définition précédente montre donc que cet ensemble admet un plus grand élément (au sens de la divisibilité) qui est $a \wedge b$. Autrement dit, au sens de la divisibilité, l'ensemble $\{a, b\}$ admet une borne inférieure qui est $a \wedge b$.

⇨ Soit $a, b \in \mathbb{N}$. Si l'un des deux entiers est non nul, le pgcd de a et de b est le plus grand (au sens de l'ordre) diviseur commun de a et b.

Proposition 2.2

$$\begin{aligned}
&\forall a \in \mathbb{Z}, && a \wedge 0 = |a| \\
&\forall a \in \mathbb{Z}, && a \wedge 1 = 1 \\
&\forall a, b \in \mathbb{Z}, && a \wedge b = 0 \quad \Longleftrightarrow \quad [a = 0 \quad \text{et} \quad b = 0]
\end{aligned}$$

Proposition 2.3

$$\begin{aligned} \forall a, b \in \mathbb{Z}, \quad & a \wedge b = b \wedge a \\ \forall a, b \in \mathbb{Z}, \quad & a \wedge b = (-a) \wedge b = a \wedge (-b) = (-a) \wedge (-b) = |a| \wedge |b| \\ \forall a, b, k \in \mathbb{Z}, \quad & (ka) \wedge (kb) = |k| (a \wedge b) \end{aligned}$$

Définition 2.4

Soit $a_1, \dots, a_n \in \mathbb{Z}$. Il existe un unique entier positif p tel que
- $\forall i \in [\![1, n]\!], \quad p | a_i$
- $\forall q \in \mathbb{Z}, \quad [\forall i \in [\![1, n]\!], \quad q | a_i] \Longrightarrow q | p$

On l'appelle pgcd (plus grand commun diviseur) de la famille $(a_1, \dots, a_n)$ et on le note $\operatorname{pgcd}(a_1, \dots, a_n)$ ou $a_1 \wedge \cdots \wedge a_n$.

Remarque

⇨ Le pgcd d'une famille d'entiers $(a_1, \dots, a_n)$ ne dépend pas de l'ordre de ces derniers.

Proposition 2.5

Soit $a_1, \dots, a_n \in \mathbb{Z}$ et $p \in [\![1, n-1]\!]$. Alors

$$a_1 \wedge \cdots \wedge a_n = (a_1 \wedge \cdots \wedge a_p) \wedge (a_{p+1} \wedge \cdots \wedge a_n).$$

2.2 Algorithme d'Euclide

Proposition 2.6

Soit $a, b, k \in \mathbb{Z}$. Alors

$$a \wedge b = a \wedge (b + ka) = (a + kb) \wedge b.$$

En particulier, si $b \in \mathbb{N}^*$ et r est le reste de la division euclidienne de a par b, on a

$$a \wedge b = b \wedge r.$$

Exercices 4

⇨ Calculer $105 \wedge 147$.

⇨ Soit $n \in \mathbb{N}$. Calculer $(3n+1) \wedge (2n)$, puis $(n^4 - 1) \wedge (n^6 - 1)$.

⇨ Soit (F_n) la suite, appelée suite de Fibonacci, définie par

$$F_0 \coloneqq 0, \quad F_1 \coloneqq 1, \quad \text{et} \quad \forall n \in \mathbb{N}, \quad F_{n+2} \coloneqq F_{n+1} + F_n.$$

Montrer que pour tout $n \in \mathbb{N}$, $F_n \wedge F_{n+1} = 1$.

Remarque

⇨ Si $a, b \in \mathbb{N}$, l'algorithme suivant, appelé algorithme d'Euclide, calcule le pgcd de a et b.

```
def pgcd(a, b):
    """pgcd(a: int, b: int) -> int"""
    while b != 0:
        a, b = b, a % b
    return a
```

2.3 Relation de Bézout

Proposition 2.7

Soit $a, b \in \mathbb{Z}$. Alors il existe $u, v \in \mathbb{Z}$ tels que

$$ua + vb = a \wedge b.$$

Exercices 5

⇨ Trouver une relation de Bézout pour 105 et 147.

⇨ Soit $n, m \in \mathbb{N}^*$. Montrer que

$$\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m}.$$

Définition 2.8

Soit $a, b \in \mathbb{Z}$. On dit que a et b sont *premiers entre eux* lorsque $a \wedge b = 1$.

Remarque

⇨ Soit $a, b \in \mathbb{Z}$. Puisque $a \wedge b$ est un diviseur commun à a et b, il existe $a', b' \in \mathbb{Z}$ tels que $a = a'(a \wedge b)$ et $b = b'(a \wedge b)$. Si $(a, b) \neq (0, 0)$, alors a' et b' sont premiers entre eux.

Exercice 6

⇨ Soit $a, b \in \mathbb{Z}$ deux entiers premiers entre eux. Calculer $(a - b) \wedge (a + b)$.

Proposition 2.9

Soit $a, b \in \mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que

$$ua + vb = 1.$$

Exercice 7

⇨ Soit $n \in \mathbb{N}^*$. On se place dans le groupe $(\mathbb{U}_n, \times)$ et on pose $\omega := \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$. Montrer que si $k \in \mathbb{Z}$, le groupe engendré par ω^k est égal à $\mathbb{U}_n$ si et seulement si k et n sont premiers entre eux.

Proposition 2.10

- Soit $a, b, c \in \mathbb{Z}$ tels que $a \wedge b = 1$ et $a \wedge c = 1$. Alors $a \wedge (bc) = 1$.
- Plus généralement, si $a \in \mathbb{Z}$ est premier avec chaque élément d'une famille d'entiers $b_1, \ldots, b_n \in \mathbb{Z}$, alors a est premier avec leur produit.
- Soit $a, b \in \mathbb{Z}$ deux entiers premiers entre eux et $m, n \in \mathbb{N}$. Alors $a^m \wedge b^n = 1$.

Exercices 8

⇨ Soit $a, b \in \mathbb{Z}$ deux entiers premiers entre eux. Montrer que $a + b$ et ab sont premiers entre eux.

⇨ Résoudre sur $\mathbb{Z}$ l'équation $2n \equiv 7$ [9].

Définition 2.11

Soit $n \in \mathbb{N}^*$. On dit que $a \in \mathbb{Z}$ est inversible modulo n lorsqu'il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1$ $[n]$.

Proposition 2.12

Soit $n \in \mathbb{N}^*$. Alors $a \in \mathbb{Z}$ est inversible modulo n si et seulement si $a \wedge n = 1$.

Proposition 2.13

Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Alors il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que

$$u_1 a_1 + \cdots + u_n a_n = a_1 \wedge \ldots \wedge a_n.$$

Définition 2.14

Soit $a_1, \ldots, a_n \in \mathbb{Z}$.

- On dit que $a_1, \ldots, a_n$ sont *deux à deux premiers entre eux* lorsque

$$\forall i, j \in [\![1, n]\!] \quad i \neq j \Longrightarrow a_i \wedge a_j = 1.$$

- On dit que $a_1, \ldots, a_n$ sont *premiers entre eux dans leur ensemble* lorsque

$$a_1 \wedge \cdots \wedge a_n = 1.$$

Remarque

⇨ Si les entiers $a_1, \ldots, a_n$ sont deux à deux premiers entre eux, alors ils sont premiers entre eux dans leur ensemble. Cependant, la réciproque est fausse. Par exemple, $a_1 = 2$, $a_2 = 3$ et $a_3 = 6$ sont premiers entre eux dans leur ensemble, mais ne sont pas deux à deux premiers entre eux.

Proposition 2.15

Soit $a_1, \dots, a_n \in \mathbb{Z}$. Alors $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble si et seulement si il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que

$$u_1 a_1 + \cdots + u_n a_n = 1.$$

Exercice 9

⇨ Trouver les solutions entières de l'équation

$$a^2 + b^2 = 3c^2.$$

2.4 Lemme de Gauss

Théorème 2.16

Soit $a, b, c \in \mathbb{Z}$. Alors

$$[a|bc \quad \text{et} \quad a \wedge b = 1] \quad \Longrightarrow \quad a|c.$$

Exercices 10

⇨ Soient $a, b, c \in \mathbb{Z}$ tels que $a \wedge c = 1$. Montrer que

$$(ab) \wedge c = b \wedge c.$$

⇨ Résoudre l'équation $105u + 147v = 21$ dans $\mathbb{Z}$.

⇨ Trois comètes passent régulièrement dans le ciel Shadok. La première, la comète Gabu, passe tous les 10 jours depuis le deuxième jour d'existence de leur planète. La seconde, la comète Zomeu passe tous les 21 jours depuis le cinquième jour d'existence de leur planète. Enfin, la comète Gibi passe tous les 6 jours depuis le troisième jour d'existence de leur planète. Est-il possible d'admirer les comètes Gabu et Zomeu le même jour dans le ciel Shadok ? Si oui, lesquels ? Même question pour les comètes Gabu et Gibi.

⇨ Soit $(G, \star)$ un groupe et $x \in G$ un élément d'ordre fini $n \in \mathbb{N}^*$. Étant donné $k \in \mathbb{Z}$, calculer l'ordre de x^k.

Remarque

⇨ Soit $a, b, c \in \mathbb{Z}$ tels que $(a, b) \neq (0, 0)$. On cherche les solutions entières de l'équation

$$(E) \qquad ua + vb = c$$

— Si $a \wedge b$ ne divise pas c, il n'y a aucune solution.

— Sinon, il existe $c' \in \mathbb{Z}$ tel que $c = c'(a \wedge b)$. En utilisant l'algorithme d'Euclide, on trouve $u'_0, v'_0 \in \mathbb{Z}$ tels que $u'_0 a + v'_0 b = a \wedge b$. On a donc $(c'u'_0)a + (c'v'_0)b = c$ ce qui nous donne une solution particulière à l'équation (E). Soit $a', b' \in \mathbb{Z}$ tels que $a = a'(a \wedge b)$ et $b = b'(a \wedge b)$. Alors a' et b' sont premiers entre eux. On a alors :

$$\begin{aligned} \forall u, v \in \mathbb{Z} \quad ua + vb = c &\iff ua + vb = (c'u'_0)a + (c'v'_0)b \\ &\iff (u - c'u'_0)a = (c'v'_0 - v)b \\ &\iff (u - c'u'_0)a' = (c'v'_0 - v)b' \quad (E') \end{aligned}$$

Si le couple (u, v) est solution de (E'), on en déduit que b' divise $(u - c'u'_0)a'$. Or a' et b' sont premiers entre eux, donc d'après le lemme de Gauss, b' divise $u - c'u'_0$. Il existe donc $k \in \mathbb{Z}$ tel que $u = c'u'_0 + kb'$. En reportant cette égalité dans (E'), on trouve $v = c'v'_0 - ka'$. Réciproquement, on vérifie que de tels u et v sont bien solution de (E'). L'ensemble des solutions de (E) est donc

$$\mathcal{S} = \{(c'u'_0 + kb', c'v'_0 - ka') \mid k \in \mathbb{Z}\}$$

Proposition 2.17

Soit $r \in \mathbb{Q}$.

— Alors, il existe un unique couple $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que

$$r = \frac{a}{b} \quad \text{et} \quad a \wedge b = 1.$$

Cette écriture est appelée *forme irréductible* de r.

— De plus, si $p \in \mathbb{Z}$ et $q \in \mathbb{Z}^*$, $r = p/q$ si et seulement si il existe $k \in \mathbb{Z}^*$ tel que $p = ka$ et $q = kb$.

Remarque

⇨ Si $P(x) = a_n x^n + \cdots + a_1 x + a_0$ est un polynôme à coefficients entiers et $r = p/q$ est une racine rationnelle de P, mise sous forme irréductible, alors $q|a_n$ et $p|a_0$. On a ainsi un moyen de trouver toutes les racines rationnelles d'un polynôme à coefficients entiers.

Exercices 11

⇨ Rechercher les racines rationnelles de $P(x) = 2x^3 + x^2 + x - 1$. En déduire une factorisation de ce polynôme.

⇨ Soit $n \in \mathbb{N}$. Montrer que $\sqrt{n}$ est soit entier, soit irrationnel.

Proposition 2.18

— Soit $a, b, c \in \mathbb{Z}$. On suppose que $a|c$, $b|c$ et $a \wedge b = 1$. Alors $ab|c$.
— Plus généralement si $a \in \mathbb{Z}$ est divisé par chaque élément d'une famille $b_1, \ldots, b_n \in \mathbb{Z}$ d'entiers deux à deux premiers entre eux, alors il est divisé par leur produit.

2.5 Plus petit commun multiple

Définition 2.19

Soit $a, b \in \mathbb{Z}$. Il existe un unique entier positif p tel que
— $a|p \quad$ et $\quad b|p$
— $\forall q \in \mathbb{Z}, \quad [a|q \quad$ et $\quad b|q] \Longrightarrow p|q$
On l'appelle ppcm (*plus petit commun multiple*) de a et de b et on le note $\text{ppcm}(a, b)$ ou $a \vee b$.

Remarques

⇨ Si $a, b \in \mathbb{Z}$, les multiples de a et de b sont les multiples de $a \vee b$.

⇨ Soit $a, b \in \mathbb{N}$. Pour la relation d'ordre de divisibilité sur $\mathbb{N}$, l'ensemble des multiples de a et de b n'est rien d'autre que l'ensemble des majorants de $\{a, b\}$. La définition précédente montre donc que cet ensemble admet un plus petit élément (au sens de la divisibilité) qui est $a \vee b$. Autrement dit, au sens de la divisibilité, l'ensemble $\{a, b\}$ admet une borne supérieure qui est $a \vee b$.

Proposition 2.20

$$\begin{aligned} \forall a \in \mathbb{Z}, &\quad a \vee 0 = 0 \\ \forall a \in \mathbb{Z}, &\quad a \vee 1 = |a| \\ \forall a, b \in \mathbb{Z}, &\quad a \vee b = 0 \Longleftrightarrow [a = 0 \quad \text{ou} \quad b = 0] \end{aligned}$$

Remarque

⇨ Si $a, b \in \mathbb{N}^*$, $a \vee b$ est, au sens de l'ordre, le plus petit multiple commun strictement positif de a et b.

Proposition 2.21

$$\begin{aligned} \forall a, b \in \mathbb{Z}, &\quad a \vee b = b \vee a \\ \forall a, b \in \mathbb{Z}, &\quad a \vee b = (-a) \vee b = a \vee (-b) = (-a) \vee (-b) = |a| \vee |b| \\ \forall a, b, k \in \mathbb{Z}, &\quad (ka) \vee (kb) = |k| (a \vee b) \end{aligned}$$

Proposition 2.22

Soit $a, b \in \mathbb{Z}$.
— Si $a \wedge b = 1$, alors
$$a \vee b = |ab| .$$
— De manière générale
$$(a \wedge b)(a \vee b) = |ab| .$$

Remarque

⇨ On peut définir $a \vee b \vee c$ mais attention, en général, $(a \wedge b \wedge c)(a \vee b \vee c) \neq |abc|$.

Exercice 12

⇨ Résoudre dans $\mathbb{Z}$ l'équation $a \vee b = a + b - 1$.

3 Nombres premiers

3.1 Nombres premiers

Définition 3.1

On dit qu'un entier $p \geqslant 2$ est *premier* lorsque ses seuls diviseurs positifs sont 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Remarques

⇨ Par convention, 1 n'est pas un nombre premier.

⇨ Un nombre $p \geqslant 2$ n'est pas premier si et seulement si il existe $a, b \geqslant 2$ tel que $p = ab$.

⇨ Soit p un entier supérieur ou égal à 2. Pour montrer que p est premier, il suffit de montrer que k ne divise pas p pour tout entier k compris (au sens large) entre 2 et $\sqrt{p}$.

Exercices 13

⇨ Pour tout $n \in \mathbb{N}$, on définit le n-ième nombre de Mersenne comme $M_n = 2^n - 1$. Montrer que si M_n est premier, alors n est premier. La réciproque est-elle vraie ?

⇨ Soit p un nombre premier supérieur ou égal à 5. Montrer que $24 | p^2 - 1$.

⇨ Soit $n \in \mathbb{N}^*$. Montrer qu'il existe n nombres consécutifs non premiers

Proposition 3.2

Soit p un nombre premier et $n \in \mathbb{Z}$. Alors $p|n$ ou $p \wedge n = 1$.

Exercice 14

⇨ Soit p un nombre premier.

1. Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.
2. Montrer que

$$\forall a, b \in \mathbb{Z}, \quad (a+b)^p \equiv a^p + b^p \quad [p].$$

Proposition 3.3: Petit théorème de Fermat

Soit p un nombre premier et $m \in \mathbb{Z}$ un entier qui n'est pas un multiple de p. Alors

$$m^{p-1} \equiv 1 \ [p].$$

Proposition 3.4

Soit p un nombre premier.

— Si $a, b \in \mathbb{Z}$, alors

$$p|ab \iff [p|a \quad \text{ou} \quad p|b].$$

— Plus généralement, p divise un produit si et seulement si il divise un de ses facteurs.

Proposition 3.5

Tout entier supérieur ou égal à 2 admet un diviseur premier.

Remarque

⇨ Soit $n \geqslant 2$. On cherche l'ensemble des nombres premiers inférieurs ou égaux à n. Pour cela, on utilise le crible d'Ératosthène :

— On forme une table avec tous les entiers compris entre 2 et n.
— On raye tous les multiples de 2.
— On cherche le plus petit entier qui n'est pas rayé : c'est 3 et il est premier. On raye alors tous les multiples de 3.
— On cherche ensuite le plus petit entier qui n'est pas rayé (c'est 5). Il est premier car on a trouvé tous les nombres premiers strictement inférieurs à celui-ci et on a rayé tous leurs multiples. On raye alors tous les multiples de 5.
— On continue ainsi jusqu'à ce qu'on trouve un nombre premier dont le carré est strictement supérieur à n. Les nombres qui ne sont pas rayés sont les nombres premiers compris entre 2 et n.

Par exemple, si on cherche les nombres premiers inférieurs à 99, on trouve :

		2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Proposition 3.6

L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Remarque

⇨ Cette démonstration est due à Euclide (325–265 avant J.C.).

3.2 Valuation p-adique, décomposition en facteurs premiers

Définition 3.7

Lorsque $n \in \mathbb{Z}^*$ et p est nombre premier, on appelle *valuation p-adique de n* et on note $\mathrm{Val}_p(n)$ le plus grand $\alpha \in \mathbb{N}$ tel que $p^\alpha | n$.

Remarques

⇨ Soit p et q deux nombres premiers. Alors

$$\mathrm{Val}_p(q) = \begin{cases} 1 & \text{si } p = q, \\ 0 & \text{sinon.} \end{cases}$$

⇨ Si $n \in \mathbb{Z}^*$, il n'existe qu'un nombre fini de nombres premiers p tels que $\mathrm{Val}_p(n) > 0$.

Proposition 3.8

Soit $n_1, n_2 \in \mathbb{Z}^*$ et $p \in \mathcal{P}$. Alors

$$\mathrm{Val}_p(n_1 n_2) = \mathrm{Val}_p(n_1) + \mathrm{Val}_p(n_2).$$

Remarques

⇨ Plus généralement, si p est un nombre premier, $n_1, \dots, n_r \in \mathbb{Z}^*$ et $\alpha_1, \dots, \alpha_r \in \mathbb{N}$, alors

$$\mathrm{Val}_p\left(\prod_{k=1}^{r} n_k^{\alpha_k}\right) = \sum_{k=1}^{r} \alpha_k \mathrm{Val}_p(n_k).$$

⇨ Si $n \in \mathbb{Z}^*$, certains auteurs définissent la valuation p-adique de n pour tout entier $p \geqslant 2$. Par exemple la valuation 10-adique de n est le plus grand entier $\alpha \in \mathbb{N}$ tel que 10^α divise n, c'est-à-dire le nombre de 0 à la fin de l'écriture décimale de n. Remarquons cependant que si p n'est pas premier, la propriété de la proposition précédente n'est plus vérifiée.

Exercice 15

⇨ Montrer que $\sqrt[5]{4/3}$ est irrationnel.

Théorème 3.9: Factorisation première

Soit $n \in \mathbb{Z}^*$. Alors, il existe $u \in \{-1, 1\}$, $p_1, \dots, p_r$ des nombres premiers deux à deux distincts et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$ tels que

$$n = u \prod_{k=1}^{r} p_k^{\alpha_k}.$$

De plus, à permutation près des p_k, cette décomposition est unique.

Remarque

⇨ Soit $n \in \mathbb{Z}^*$. On note $u \in \{1, -1\}$ le signe de n. Alors la factorisation première de n s'écrit

$$n = u \prod_{p \in \mathcal{P}} p^{\mathrm{Val}_p(n)},$$

ce produit ne comportant qu'un nombre fini de termes différents de 1.

Proposition 3.10

Soit $n_1, n_2 \in \mathbb{Z}^*$. Alors

— $n_1 | n_2$ si et seulement si

$$\forall p \in \mathcal{P}, \quad \mathrm{Val}_p(n_1) \leqslant \mathrm{Val}_p(n_2).$$

— $n_1 = \pm n_2$ si et seulement si

$$\forall p \in \mathcal{P}, \quad \mathrm{Val}_p(n_1) = \mathrm{Val}_p(n_2).$$

Exercice 16

⇨ Si $n \in \mathbb{N}$ et p est un nombre premier, montrer que

$$\mathrm{Val}_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

En déduire le nombre de zéros à la fin de l'écriture décimale de 2023!.

Proposition 3.11

Soit $n_1, n_2 \in \mathbb{Z}^*$. Alors, le pgcd et le ppcm de n_1 et n_2 sont donnés par les relations

$$\begin{aligned} \forall p \in \mathcal{P}, \quad \mathrm{Val}_p(n_1 \wedge n_2) &= \min(\mathrm{Val}_p(n_1), \mathrm{Val}_p(n_2)) \\ \mathrm{Val}_p(n_1 \vee n_2) &= \max(\mathrm{Val}_p(n_1), \mathrm{Val}_p(n_2)). \end{aligned}$$

Exercice 17

⇨ Soit $a, b \in \mathbb{N}^*$ tels que $a \wedge b = 1$ et ab est un carré parfait (ab est le carré d'un entier). Montrer que a et b sont des carrés parfaits.

3.3 Les grands problèmes d'arithmétique

— **Postulat de Bertrand**
Le postulat de Bertrand affirme que si $n \in \mathbb{N}^*$, alors il existe un nombre premier p tel que $n < p \leqslant 2n$. Cette conjecture fut énoncée par Joseph Bertrand en 1845 et démontrée par Tchebychev en 1848. Bien que ce résultat soit aujourd'hui un théorème, le nom de postulat lui est resté associé.

— **Théorème de la progression arithmétique**
Ce théorème affirme que si a et b sont premiers entre eux, alors il existe une infinité de nombres premiers p tels que $p \equiv a\ [b]$. On le doit à Dirichlet (1805–1859).

— **Théorème des nombres premiers**
Pour tout $n \in \mathbb{N}^*$, on définit π_n comme le cardinal de l'ensemble des nombres premiers inférieurs ou égaux à n. Le théorème des nombres premiers affirme que

$$\pi_n \underset{n \to +\infty}{\sim} \frac{n}{\ln n}$$

Autrement dit, si l'on choisit au hasard un entier entre 1 et n, la probabilité pour qu'il soit premier est de l'ordre de $1/(\ln n)$. Remarquons que cette quantité tend vers 0 lorsque n tend vers $+\infty$, c'est-à-dire que les nombres premiers deviennent « de plus en plus rares » lorsqu'on avance parmi les entiers naturels. Ce théorème fut conjecturé de manière indépendante par Gauss et Legendre vers 1800. Il fut démontré par Hadamard et de la Vallée Poussin en 1896.

— **Grand (ou dernier) théorème de Fermat**
Il s'énonce ainsi :

« Pour tout entier $n \geqslant 3$, il n'existe pas de triplet $(a, b, c) \in \mathbb{N}^{*3}$ tel que $a^n + b^n = c^n$. »

Contrairement au petit théorème, il s'agit d'un résultat extrêmement difficile, dont Fermat n'a pas publié de démonstration. Fermat n'a même jamais affirmé publiquement l'avoir démontré. Il a cependant écrit dans une marge du livre II des Oeuvres de Diophante : « J'ai découvert une démonstration merveilleuse, mais je n'ai pas la place de la mettre dans la marge ». Le livre et cette annotation ont été publiés après sa mort, par son fils. De nombreux mathématiciens ont tenté de le prouver et sont arrivés à des résultats partiels, notamment

— Fermat (1601–1665) le démontre pour $n = 4$.
— Euler (1707–1783) le démontre pour $n = 3$.
— Sophie Germain (1776–1831) apporte un résultat majeur ouvrant la porte à la démonstration du cas $n = 5$, démontré quelques années plus tard par Legendre (1752–1833).
— Kummer (1810–1893) le prouve pour tout $n \in [\![3, 99]\!]$.

En 1993, Andrew Wiles prouve un résultat sur les courbes elliptiques, résultat qui admet le grand théorème de Fermat pour corolaire. La démonstration initiale possède une erreur mais elle sera vite réparée. La conjecture de Fermat devient alors le théorème de Fermat-Wiles.

— **Nombres premiers jumeaux**

On dit qu'un couple $(p, q) \in \mathbb{N}$ est un couple de nombres premiers jumeaux lorsque $q = p + 2$. Par exemple $(3, 5)$, $(5, 7)$, $(11, 13)$ sont des couples de nombres premiers jumeaux. On conjecture qu'il existe une infinité de nombres premiers jumeaux. Bien que l'on pense que cette conjecture est vraie, elle n'a jamais été démontrée. En janvier 2016, le plus grand couple de nombres premiers jumeaux connu est $2\,996\,863\,034\,895 \times 2^{1\,290\,000} \pm 1$.

— **Conjecture de Goldbach**

En 1742, Goldbach (1690–1764) et Euler (1707–1783) énoncent

> « Tout entier pair supérieur ou égal à 4 peut s'écrire comme la somme de deux nombres premiers. »

On pense que cette conjecture est vraie, mais aucune démonstration n'en a jamais été faite.