ALG 7 | Arithmétique dans $\mathbb{Z}$

L'arithmétique est une très bonne école pour apprendre les mathématiques : elle contient des calculs et offre une belle variété de démonstrations.

L'Arithmétique, Pinturicchio

LES débuts de l'Arithmétique sont liés à la numération. Certaines civilisations développèrent indépendemment des méthodes de calcul (Chine, Babylone, Egypte) mais il faudra attendre l'époque d'Euclide pour voir apparaître une véritable théorie mathématique. Diophante développera ce corpus en y apportant l'étude des équations d'inconnues entières.

En 1621, Bachet donna la première édition gréco-latine de Diophante avec un copieux commentaire. Il vérifia pour les 325 premiers entiers qu'ils sont bien la somme de quatre carrés au plus (théorème des qautre carrés, dit parfois de Bachet). D'autre part dans ses *Problèmes plaisans et délectables* de 1624, il énonça que si a et b sont premiers entre eux, il existe x et y tels que $ax+by=1$ (théorème de Bezout). Il établissait cette importante relation grâce à l'algorithme d'Euclide. Fermat, lisant Diophante dans l'édition de Bachet, alla beaucoup plus loin. Citons parmi ses découvertes :

- ⇛ *le petit théorème de Fermat* : pour tout p premier et a non divisible par p, $p \mid a^p - a$;
- ⇛ *l'équation de Fermat* : $x^2 = \mathrm{A}y^2 + 1$ avec $\mathrm{A} \in \mathbb{N}$ qui n'est pas un carré parfait ;
- ⇛ *les nombres de Fermat* : ils sont de la forme $2^{2^n}+1$, soit $3, 5, 17, 257, 65537, 4294967297$, etc. On croyait à l'époque qu'ils étaient premiers. Mais 4294967297 ne l'est pas ;
- ⇛ *le grand théorème de Fermat*[1] : pour tout entier n, $n>2$, l'équation $x^n+y^n=z^n$ n'a pas de solution non triviale dans $\mathbb{Z}^3$.

Le XVIII$^{\text{e}}$ siècle ne connut que peu de développements en Arithmétique, les mathématiciens s'intéressèrent surtout à l'Algèbre et à l'Analyse naissante (voir l'invention commune du calcul différentiel par Leibniz et Newton). On peut tout de même citer les noms d'Euler et de Lagrange dont les contributions à la reine des sciences furent non négligeables.

Au XIX$^{\text{e}}$ siècle, les noms de Legendre et Gauss dominent. Adrien-Marie Legendre (1752-1833) débute en 1794 et sa grande œuvre demeure *la Théorie des Nombres* publiée en 1830. Carl-Friedrich Gauss (1777-1855) écrit les *Disquisitionnes arithmeticae* en 1801 : cet ouvrage contraste fortement avec celui de Legendre car est empli d'une rigueur toute nouvelle. On y trouve la première étude correcte des congruences et plusieurs preuves de la loi de réciprocité quadratique.

L'Arithmétique a connu un regain d'intérêt au XX$^{\text{e}}$ siècle grâce au développement de l'informatique. La cryptologie, science du codage, utilise de nombreux résultats pointus d'Arithmétique (corps finis, tests de primalité, etc).

Bezout

Legendre

Gauss et Fermat

1. Voir les preuves des cas $n=4$ par Fermat, $n=3$ par Euler, puis les travaux de Sophie Germain Germain et de Kummer au XIX$^{\text{e}}$ siècle. La première démonstration du cas général dans le grand théorème de Fermat a été donnée par Andrew Wiles en 1994.

1. Divisibilité et division euclidienne

1.1. Diviseurs et multiples

On commence par rappeler le vocabulaire de base.

Définition 7.0. Diviseurs et multiples

Soit $(a,b) \in \mathbb{Z}^2$.

- On dit que a divise b (ou que a est un diviseur de b ou encore que b est un multiple de a) s'il existe $c \in \mathbb{Z}$ tel que $b = ac$.
- On note cette propriété $a \mid b$.

Proposition 7.1. Propriétés de la relation de divisibilité

Pour tous entiers relatifs a, b, c et d :

a. La relation de divisibilité est réflexive et transitive sur $\mathbb{Z}$.

b. Si $d \mid a$ et $d \mid b$, alors pour tout (u,v) dans $\mathbb{Z}^2$, $d \mid au+bv$.

c. Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$.

d. Si $a \mid b$, alors pour tout entier naturel n, $a^n \mid b^n$.

La relation de divisibilité est antisymétrique[2] sur $\mathbb{N}$ pas sur $\mathbb{Z}$, car pour tout (a,b) dans $\mathbb{Z}^2$:

$$\begin{aligned}\big(a \mid b \text{ et } b \mid a\big) &\iff |a| = |b| \\ &\iff a = \pm b\end{aligned}$$

1.2. Le théorème de la division euclidienne

Le lecteur se souvient (avec émotion) de ses premiers cours sur la division : on peut payer la somme de 20 euros au moyen de 4 billets de 5 euros. La division euclidienne étend l'idée de division aux cas elle ne tombe pas juste, i.e. lorsqu'il y a un reste. Par exemple, on peut commencer à payer 23 euros avec 4 billets de 5, il reste alors 3 euros à payer : $23 = 4 \times 5 + 3$.

Le théorème de la division euclidienne est une mise en forme de la division enseignée et pratiquée dans « les petites classes, *celle que l'on pose* (cf. ci-contre) :

$$701 = 4 \times 175 + 1$$

701	4
− 400	175
= 301	
− 280	
= 21	
− 20	
= 1	

Plus généralement, $a = bq + r$ avec $0 \leqslant r < b$:

a	b
r	q

L'algorithme sous-jacent est simple dans le cas où $a \geqslant 0$ et $b > 0$: on retranche b à a tant que le résultat est supérieur ou égal à b.

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

Theoreme 7.2. de la division euclidienne

Soit $(a,b)\in\mathbb{Z}^2$ avec $b\neq 0$. Il existe un unique couple $(q,r)\in\mathbb{Z}^2$ tel que $a=qb+r$ et $0\leqslant r<|b|$.

- Les entiers naturels q et r sont appelés *quotient* et *reste* dans la division euclidienne de a par b. En particulier, $b\,|\,a \iff$ le reste dans la division euclidienne de a par b est nul.
- Soit $n\in\mathbb{N}^*$. Effectuons la division euclidienne de n^3+n^2+2n+1 par $n+1$. Naturellement, on factorise par $n+1$:

$$n^3+n^2+2n+1=(n+1)n^2+n+1+1=(n+1)\left(n^2+1\right)+1$$

Comme $0\leqslant 1<n+1$, $n+1\in\mathbb{Z}$ et $n^2+1\in\mathbb{Z}$, le quotient et le reste dans la division euclidienne de n^3+n^2+2n+1 par $n+1$ valent respectivement n^2+1 et 1.

Division euclidienne et partie entière

En reprenant les notation du théorème de la division euclidienne 1.2 :

$$\forall (a,b)\in\mathbb{Z}\times\mathbb{N}^*,\ q=\left\lfloor\frac{a}{b}\right\rfloor \quad\text{et}\quad r=a-b\left\lfloor\frac{a}{b}\right\rfloor$$

1.3. Congruences

Définition 7.3. Congruences

Soit $n\in\mathbb{Z}^*$ et $(a,b)\in\mathbb{Z}^2$.

⇛ On dit que a est congru à b modulo n si $n\,|\,a-b$.

⇛ On écrit alors $a\equiv b\,[n]$.

Il est clair que $b\,|\,a$ *si et seulement si* $a\equiv 0\,[b]$. La relation $\equiv\,[n]$ est *une relation d'équivalence* sur $\mathbb{Z}$:

$$\forall (a,b,c)\in\mathbb{Z}^3,\ \begin{cases} a\equiv a\,[n] & \text{(la relation est réflexive)}\\ a\equiv b\,[n]\implies b\equiv a\,[n] & \text{(la relation est symétrique)}\\ a\equiv b\,[n]\text{ et }b\equiv c\,[n]\implies a=c\,[n] & \text{(la relation est transitive)}\end{cases}$$

Règles de calcul sur les congruences (↯ 7.1)

La première règle est la compatibilité des congruences avec les opérations + et × de $(\mathbb{Z},+,\times)$.

a. $\forall\left(a,b,a',b'\right)\in\mathbb{Z}^4,\ \begin{cases} a\equiv b\,[n]\\ a'\equiv b'\,[n]\end{cases}\implies\begin{cases} a+a'\equiv b+b'\,[n]\\ a\times a'\equiv b\times b'\,[n]\end{cases}$

b. On en déduit que $\begin{cases}\forall (a,b)\in\mathbb{Z}^2,\ \forall p\in\mathbb{N},\ a\equiv b\,[n]\implies a^p\equiv b^p\,[n]\\ \forall (a,b)\in\mathbb{Z}^2,\ \forall c\in\mathbb{Z},\ a\equiv b\,[n]\implies a\times c\equiv b\times c\,[n]\end{cases}$

c. En fait, on a plus précisément, $\forall (a,b)\in\mathbb{Z}^2,\ \forall c\in\mathbb{Z},\ a\equiv b\,[n]\implies a\times c\equiv b\times c\,[n\times c]$.

d. Pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, $\begin{cases} a \equiv r\,[b] \\ 0 \leqslant r < |b| \end{cases} \iff$ r est le reste dans la division euclidienne de a par b.

- Illustrons sans plus tarder l'efficacité de ces règles de calcul en démontrant que, pour tout entier naturel n, $2^{4^n}+5$ est divisible par 7. On va procéder par récurrence sur n. Comme $2+5=7$, le résultat est acquis au rang 0. Soit $n \in \mathbb{N}$. Supposons la propriété vraie au rang n. On a $2^{4^n} \equiv -5 \equiv 2\,[7]$ d'où
$$2^{4^{n+1}}+5 \equiv \left(2^{4^n}\right)^4+5 \equiv 2^4+5 \equiv 21 \equiv 0\,[7]$$
d'où la propriété au rang $n+1$.
- Les congruences sont les bottes de sept lieues de l'arithmétique : elles permettent d'obtenir en peu de calculs des informations sur des nombres très grands. Calculons par exemple le reste dans la division euclidienne de 10^6 par 7. On a $10 \equiv 3\,[7]$ d'où $10^2 \equiv 9 \equiv 2\,[7]$ et donc $10^6 \equiv 2^3 \equiv 1\,[7]$. Ainsi, le reste dans la division euclidienne de 10^6 par 7 vaut 1.
- Les congruences sont un outil intéressant pour résoudre (ou à défaut de mieux comprendre) une équation diophantienne, i.e. une équation polynomiale à coefficients dans $\mathbb{Z}$ à une ou plusieurs inconnues entières. Considérons par exemple l'équation $\mathscr{E} : x^2+3y^3=17$. Nous allons la réduire modulo 3 : si $x \in \mathbb{Z}$, alors $x^2 \equiv 17 \equiv 2\,[3]$. Un tableau de congruence permet de conclure que l'équation $x^2 \equiv 2\,[3]$ n'a aucune solution.

  Il est justifié par les calculs suivants :

  $$x \equiv 0\,[3] \implies x^2 \equiv 0\,[3]\,,\ x \equiv 1\,[3] \implies x^2 \equiv 1\,[3]\,,\ x \equiv 2\,[3] \implies x^2 \equiv 4 \equiv 1\,[3]$$

x	0	1	2
x^2	0	1	1

2. Numération de position en base quelconque

L'idée la plus simple pour *représenter un entier naturel* est d'utiliser un même symbole répété plusieurs fois. On peut ainsi énumérer la liste des premiers entiers naturels non nuls : ⋆, ⋆⋆, ⋆⋆⋆, ⋆⋆⋆⋆, etc. Cette méthode élémentaire se révèle très vite coûteuse en étoiles et en temps ! À la manière des Romains, on peut tenter quelques économies en regroupant 5 étoiles en un seul symbole V ou signifier 10 étoiles par la lettre X.

Au cours des siècles, les mathématiciens ont élaboré divers systèmes de numération, c'est-à-dire de représentation des entiers naturels. Le mieux connu des lecteurs est certainement le système décimal à position inventé en Inde vers 400 : un entier naturel n est représenté par son chiffre des unités a_0, des dizaines a_1, etc., jusqu'à un chiffre a_m (chiffre des milliers si $m=3$, des millions si $m=6$, des milliards si $m=9$, etc.) :

$$3456 = \underbrace{3}_{\text{milliers}} \times 10^3 + \underbrace{4}_{\text{centaines}} \times 10^2 + \underbrace{5}_{\text{dizaines}} \times 10^1 + \underbrace{6}_{\text{unités}} \times 10^0$$

Plus généralement, on note $n = a_m \dots a_1 a_0$ ou plus rigoureusement $n = \overline{a_m \dots a_1 a_0}^{10}$ afin de se souvenir qu'il s'agit des chiffres de n dans le système décimal pour lequel la base vaut $b=10$.

Le lecteur pourra s'entraîner aux écritures décimales grâce au test (↯ **7.2**).

Plus généralement, pour tout entier $b \geqslant 2$, on peut écrire n en base b, c'est-à-dire déterminer des chiffres $a_0, \dots, a_m \in [\![0, b-1]\!]$ tels que

$$n = a_0 + a_1 b + a_2 b^2 + \ldots + a_m b^m, \quad \text{ce que l'on écrira} \quad n = \underline{a_m \cdots a_1 a_0}_b$$

La proposition suivante généralise ce résultat à une base b quelconque et établit l'unicité des *chiffres* $a_0, a_1, \ldots, a_m$ de n en base b.

Proposition 7.3. Numération en base b

Soit $n \in \mathbb{N}^*$ et $b \in \mathbb{N}$ tel que $b \geqslant 2$. Il existe un unique entier naturel m et des entiers uniques a_0, a_1, …, a_m dans $[\![0, b-1]\!]$ tels que

$$n = a_0 + a_1 b + a_2 b^2 + \ldots + a_m b^m \quad \text{et} \quad a_m \neq 0$$

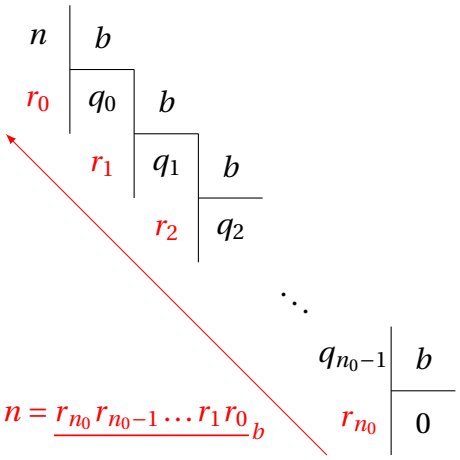
ce que l'on écrit de manière condensée $n = \underline{a_m \ldots a_1 a_0}_b$. On dit qu'il s'agit du développement (ou encore de l'écriture) en base b de n.

✕ Par exemple, codons en base deux l'entier $n = \underline{10043}_{10}$. On a

$$\begin{cases} 10043 = 2\times 5021 + 1\,,\ 5021 = 2\times 2510 + 1\,,\ 2510 = 2\times 1255 + 0\,,\ 1255 = 2\times 627 + 1 \\ 627 = 2\times 313 + 1\,,\ 313 = 2\times 156 + 1\,,\ 156 = 2\times 78 + 0\,,\ 78 = 2\times 39 + 0 \\ 39 = 2\times 19 + 1\,,\ 19 = 2\times 9 + 1\,,\ 9 = 2\times 4 + 1\,,\ 4 = 2\times 2 + 0\,,\ 2 = 2\times 1 + 0\,,\ 1 = 2\times 0 + 1 \end{cases}$$

On en déduit que $n = \underline{1\,0\,0\,1\,1\,1\,0\,0\,1\,1\,1\,0\,1\,1}_2$.

Algorithme de décomposition en base b (↯ 7.3)



On applique la méthode par divisions successives décrite à la proposition 2

On calcule le couple quotient-reste (q_0, r_0) dans la division de n par b, puis le couple quotient-reste (q_1, r_1) dans la division de q_0 par b, puis le couple quotient-reste dans la division de q_1 par b, etc.

En notant q_{n_0} le premier quotient nul obtenu au cours de l'algorithme, on a

$$n = \underline{r_{n_0} r_{n_0-1} \ldots r_1 r_0}_b$$

Lorsque $b > 10$, on utilise des lettres pour décrire les chiffres en base b. En effet, l'écriture $\underline{10}_{11}$ est ambigüe : s'agit-t-il de $1\times 11^1 + 0\times 11^0$ ou de 10×11^0 ? Ainsi, dans le cas de $b = 16$ (base dite *hexadécimale*), la liste des chiffres s'écrit 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

✕ D'après l'algorithme décrit ci-dessus, le chiffre des unités d'un entier naturel n est le reste dans la division euclidienne de n par 10. Déterminons par exemple le chiffre des unités de 8^{103}. On commence par examiner la réduction modulo 10 des premières puissances de 2 :

$$2^4 \equiv 16 \equiv 6\,[10]\,,\ 2^5 \equiv 12 \equiv 2\,[10]$$

On choisit la valeur la plus petite : $2^5 \equiv 2\,[10]$. Comme $309 = 5\times 61 + 4$, on en déduit que

$$8^{103} \equiv (2^5)^{61}2^4 \equiv 2^{65} \equiv (2^5)^{13} \equiv 2^{13} \equiv (2^5)^2 2^3 \equiv 2^5 \equiv 2\,[10]$$

Ainsi, le chiffre des unités de 8^{103} vaut 2. Le lecteur pourra s'entraîner au moyen du test **↯ 7.4.**

Le lecteur est renvoyé au test (**↯ 7.4**) pour un exercice du même type.

En reprenant les notations de la proposition 2, $m+1$ est le nombre de chiffre(s) en base b de n.

Proposition 7.4. Nombre de chiffres en base b (↯ 7.5)

Soit $b \in \mathbb{N} \setminus \{0,1\}$, $n \in \mathbb{N}^*$ et $p \in \mathbb{N}^*$.

a. Le nombre de chiffre(s) en base b de n vaut p si et seulement si $b^{p-1} \leqslant n < b^p$.

b. Le nombre de chiffres en base b de n est égal à $1 + \left\lfloor \dfrac{\ln n}{\ln b} \right\rfloor$.

Le lecteur terminera en beauté ce paragraphe en résolvant les tests (**↯ 7.6**) et (**↯ 7.7**).

3. Plus grand commun diviseur et plus petit commun multiple

Définition 7.5. Diviseurs et multiples

Pour $a \in \mathbb{Z}$, on note $\mathscr{D}_a$ l'ensemble des diviseurs de a et $a\mathbb{Z}$ l'ensemble des multiples de a. Attention, seule la notation $a\mathbb{Z}$ est universelle.

Ainsi, $\mathscr{D}_0 = \mathbb{Z}$, $\mathscr{D}_3 = \{-3,-1,1,3\}$ et $\mathscr{D}_6 = \{-6,-3,-2,-1,1,2,3,6\}$.

Plus généralement, pour a dans $\mathbb{Z}^*$, on a $\mathscr{D}_a \subset [\![-|a|, |a|]\!]$ donc $\mathscr{D}_a$ est fini et puisqu'il contient $|a|$, on a $|a| = \max \mathscr{D}_a$.

Pour tout a dans $\mathbb{Z}$, on a $\mathbb{Z} := \{ak ; k \in \mathbb{Z}\}$.

3.1. Plus grand commun diviseur

Pour deux entiers relatifs quelconques a et b, l'intersection $\mathscr{D}_a \cap \mathscr{D}_b$ est l'ensemble des diviseurs communs à a et b. L'objectif de ce paragraphe est de mieux comprendre la structure de cet ensemble. Par exemple,

$$\mathscr{D}_6 \cap \mathscr{D}_{15} = \{-3,-1,1,3\} = \mathscr{D}_3$$

Nous allons établir plus généralement qu'il existe un unique δ dans $\mathbb{N}$ tel que $\mathscr{D}_a \cap \mathscr{D}_b = \mathscr{D}_\delta$, nombre appelé « plus grand commun diviseur » de a et b.

Lemme 7.5.

Pour $(a,b,n) \in \mathbb{Z}^3$, si $a \equiv b\,[n]$, alors $\mathscr{D}_a \cap \mathscr{D}_n = \mathscr{D}_b \cap \mathscr{D}_n$.

Considérons $(a,b) \in \mathbb{N}^2$ tel que $b \neq 0$. Appliquons l'algorithme suivant :

⇛ On pose $r_0 := a$ et $r_1 := b$.

⇛ Tant que $r_i \neq 0$, on calcule le reste r_{i+1} dans la division euclidienne de r_{i-1} par r_i.

Pour $i \in \mathbb{N}$, si r_i et r_{i+1} sont définis, alors $0 \leqslant r_i < r_{i+1}$. Comme il n'existe pas de suite d'entiers naturels strictement décroissante, on en déduit que l'algorithme s'arrête après un nombre fini d'itération(s). Notons n_0 l'indice du premier reste nul obtenu (hors initialisation). On a $r_{i+1} \equiv r_{i-1}\,[r_i]$ pour tout $i \in [\![1, n_0 - 1]\!]$, on déduit du lemme que $\mathscr{D}_{r_{i-1}} \cap \mathscr{D}_{r_i} = \mathscr{D}_{r_i} \cap \mathscr{D}_{r_{i+1}}$ pour les les mêmes indices. Ainsi

$$\mathscr{D}_a \cap \mathscr{D}_b = \mathscr{D}_{r_0} \cap \mathscr{D}_{r_1} = \mathscr{D}_{r_2} \cap \mathscr{D}_{r_1} = \cdots \mathscr{D}_{r_{n_0-1}} \cap \mathscr{D}_{r_{n_0}} = \mathscr{D}_{r_{n_0-1}} \cap \underbrace{\mathscr{D}_0}_{=\mathbb{Z}} = \mathscr{D}_{r_{n_0-1}}$$

On peut en déduire la définition suivante.

Définition 7.6. Plus grand commun diviseur de deux entiers

Soit $(a, b) \in \mathbb{Z}^2$.

⇛ Il existe un unique $\delta \in \mathbb{N}$ tel que $\mathscr{D}_a \cap \mathscr{D}_b = \mathscr{D}_\delta$.

⇛ Cet entier δ est appelé PGCD de a et b (plus grand commun diviseur) et noté $a \wedge b$.

En particulier, $0 \wedge 0 = 0$ et, si $(a, b) \neq (0, 0)$, alors on a $a \wedge b = \max \mathscr{D}_a \cap \mathscr{D}_b$.

✗ Calculons par exemple la plus grand commun diviseur de 2309 et 2275 :

$2309 = 2275 \times 1 + 34$, $2275 = 34 \times 66 + 31$, $34 = 31 \times 1 + 3$, $31 = 3 \times 10 + 1$, $3 = 1 \times 3 + 0$

On en déduit que $2309 \wedge 2275 = 1$.

Cet algorithme a été mis au point par Euclide, dont il a hérité du nom.

Calcul du plus grand commun diviseur par l'algorithme d'Euclide (↯ 7.8)

Soit a et b deux entiers naturels tels que $b \neq 0$. On pose $r_0 = a$ et $r_1 = b$.

✗ Tant que $r_i \neq 0$, on calcule le reste r_{i+1} dans la division euclidienne de r_{i-1} par r_i.

✗ En notant n_0 le plus petit entier tel que $r_{n_0} = 0$, on a $a \wedge b = r_{n_0-1}$

On retiendra que *le pgcd est le dernier reste non nul dans l'algorithme d'Euclide*.

3.2. Relation de Bezout

On peut déduire de l'algorithme d'Euclide que le plus grand commun diviseur de deux entiers relatifs a et b est une combinaison linéaire à coefficients entiers relatifs de a et b.

Proposition 7.7. Relation de Bezout

Pour tous entiers relatifs a et b, il existe (u, v) dans $\mathbb{Z}^2$ tel que $a \wedge b = ua + vb$.

Une telle égalité est appelée relation de Bezout entre a et b. En fait, pour tout $i \in [\![0, n_0]\!]$, il existe $(u_i, v_i) \in \mathbb{Z}^2$, $r_i = u_i a + v_i b$.

✗ Il n'y a pas unicité du couple (u, v) dans le théorème ci-dessus. Par exemple :

$$1 = 3 \wedge 2 = 3 \times 1 + 2 \times -1 = 3 \times 5 + 2 \times -7 = 3 \times 7 + 2 \times -10 = \cdots$$

✗ Un tel couple (u,v) se calcule en adaptant l'algorithme d'Euclide.

$$\begin{cases} 2309 &= 2275\times 1+34 \\ 2275 &= 34\times 66+31 \\ 34 &= 31\times 1+3 \\ 31 &= 3\times 10+1 \\ 3 &= 1\times 3+0 \end{cases} \xrightarrow[\text{d'Euclide étendu}]{\text{Algorithme}} \begin{cases} 34 &= a-b \\ 31 &= b-66\times(a-b) = -66a+67b \\ 3 &= a-b+66a-67b = 67a-68b \\ 1 &= -66a+67b-10(67a-68b) = -736a+747b \end{cases}$$

Cette variante est connu sous le nom algorithme d'Euclide étendu.

Les règles de calcul suivantes sont faciles à démontrer à partir de la définition.

Proposition 7.8.

Soit $(a,b)\in\mathbb{Z}^2$ tel que (a,b) et $\delta := a\wedge b$.

a. Pour tout $d\in\mathbb{Z}$, d divise a et b *si et seulement si* d divise δ.

b. Pour tout $k\in\mathbb{Z}$, $(ka)\wedge(kb) = |k|\,a\wedge b$.

c. Il existe $(a',b')\in\mathbb{Z}^2$ tels que $a=\delta a'$, $b=\delta b'$ et $a'\wedge b' = 1$.

C'est ce résultat qui justifie l'écriture sous forme irréductible d'un nombre rationnel. On se ramène à un quotient de deux nombres de pgcd égal à un après factorisation et simplification de leur pgcd :

$$\frac{150}{210} = \frac{5}{7}$$

Définition 7.9. Entiers premiers entre eux

Deux entiers a et b sont dits premiers entre eux si $a\wedge b = 1$.

Attention, il ne faut pas confondre les propositions « a ne divise pas b » et $a\wedge b = 1$. Par exemple, 6 ne divise pas 8 mais $6\wedge 8 = 2$. En revanche, il est vrai que si $a\wedge b = 1$ et $|a|\geqslant 2$, alors a ne divise pas b.

Theoreme 7.10. de Bezout

Pour tout $(a,b)\in\mathbb{Z}^2$, $\big(\exists(u,v)\in\mathbb{Z}^2, 1 = ua+vb\big) \iff a\wedge b = 1$.

D'une façon générale, la proposition $a\,|\,bc$ n'implique nullement que a divise l'un des deux facteurs a ou b. Par exemple, 6 divise 8×9 mais ne divise ni 8, ni 9. Le lemme de Gauss permet cependant de conclure que a divise c sous l'hypothèse $a\wedge b = 1$.

Lemme 7.11. de Gauss

Soit $(a,b,c)\in\mathbb{Z}^3$ tels que $a\wedge b = 1$. Si $a\,|\,bc$, alors $a\,|\,c$.

✗ Nous allons illustrer ce résultat en recherchant toutes les relations de Bezout entre 3 et 2. On sait que $3\times 1+2\times -1=1$. Ainsi, pour (u,v) dans $\mathbb{Z}^2$, on a

$$\begin{aligned} 3u+2v=1 &\iff 3u+2v=3\times 1+2\times -1\\ &\iff 3(u-1)=2(-1-v)\end{aligned}$$

Supposons $3(u-1)=2(-1-v)$. Comme $3\wedge 2=1$, on déduit du lemme de Gauss que 3 divise $-1-v$, i.e. on a $-1-v=3k$ pour un certain $k\in\mathbb{Z}$. On a alors $3(u-1)=2\times 3k$, d'où $u-1=2k$. Finalement $(u,v)=(1+2k,-1-3k)$. Comme la réciproque est facile à vérifier, on en déduit que

$$3u+2v=1 \iff \exists k\in\mathbb{Z},\ (u,v)=(1+2k,-1-3k)$$

3.3. Plus petit commun multiple

Nous allons maintenant déterminer la structure de l'ensemble $a\mathbb{Z}\cap b\mathbb{Z}$ des multiples communs à deux entiers a et b.

Définition 7.12. PPCM (plus petit commun multiple) de deux entiers

Soit a et b deux entiers relatifs non nuls.

⇛ Il existe un unique $\mu\in\mathbb{N}$ tel que $a\mathbb{Z}\cap b\mathbb{Z}=\mu\mathbb{Z}$.

⇛ On le note $a\vee b:=\mu$ et on l'appelle plus petit commun multiple de a et b.

Si $a\neq 0$ et $b\neq 0$, alors $a\vee b=\min\left(\mathbb{N}^*\cap a\mathbb{Z}\cap b\mathbb{Z}\right)$, ce qui qui justifie la terminologie.

Considérons par exemple $a:=12$ et $b:=15$. Un multiple commun m à a et b s'écrit $m=12k=15\ell$ avec $(k,\ell)\in\mathbb{Z}^2$. Ainsi $4k=5\ell$. Comme $4\wedge 5=1$, on déduit du lemme de Gauss que $\ell=4\ell'$ avec ℓ' dans $\mathbb{Z}$, d'où $k=5\ell'$ et finalement $m=60\ell'$. Réciproquement, il est clair que tout multiple de 60 est un multiple de 12 et 15 (car $60=15\times 2=12\times 5$). Ainsi $12\mathbb{Z}\cap 15\mathbb{Z}=60\mathbb{Z}$ et $12\vee 15=60$. Plus généralement :

Proposition 7.13.

Soit $(a,b)\in\mathbb{Z}^2$, $\delta=a\wedge b$ et $(a',b')\in\mathbb{Z}^2$ tels que $a=\delta a'$ et $b=\delta b'$.
On a $a\vee b=\delta|a'b'|$ et donc $|ab|=(a\wedge b)(a\vee b)$. En particulier, si $a\wedge b=1$, alors $a\vee b=|ab|$.

Le calcul du ppcm ne nécessite donc aucun nouvel algorithme : il suffit de connaître le pgcd des deux nombres puis d'effectuer une division euclidienne de plus pou trouve le ppcm des deux nombres.

Proposition 7.14.

Soit $(a,b,k)\in\mathbb{Z}^3$. a) Si $a\wedge b=1$, alors $\left(a\,|\,k \text{ et } b\,|\,k\right)\iff ab\,|\,k$; b) On a $(ka)\vee(kb)=|k|a\vee b$.

4. Nombres premiers

L'ensemble des nombres premiers a beaucoup fasciné et occupé les mathématiciens depuis le début du XIX^{e} siècle. Il fallut attendre Hadamard et La Vallée Poussin en 1896 pour que soit démontré le

théorème des nombres premiers qui précise la répartition des entiers premiers parmi tous les entiers naturels :

$$\pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\ln x} \quad \text{et} \quad p_n \underset{n\to+\infty}{\sim} n\ln n$$

où $\pi(x)$ désigne le nombre d'entiers premiers inférieur à x et $(p_n)_{n\geqslant 1}$ la suite strictement croissante des nombres premiers. Nous nous contenterons dans cette section de démontrer l'infinitude de l'ensemble des nombres premiers puis d'établir le théorème fondamental de l'arithmétique avant d'en proposer quelques applications.

4.1. L'ensemble $\mathbb{P}$ des nombres premiers et le lemme d'Euclide

Un nombre premier est un entier naturel *incassable par division*.

Définition 7.15. Nombres premiers, nombres composés (↯ 7.9)

Soit $p \in \mathbb{N}$.

- L'entier p est dit premier si $p \geqslant 2$ et si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p.
- Un entier naturel différent de 1 et qui n'est pas premier est dit composé.
- On note $\mathbb{P}$ l'ensemble des nombres premiers.

Par exemple, les nombres 2, 3, 5, 7, 11 sont premiers alors que les entiers 4, 6, 8 et 9 sont composés (car $4 = 2\times 2$, etc.). Le lecteur poursuivra avec le test (↯ 7.10).

Les nombres premiers permettent de générer par produit tous les entiers naturels non nuls. Dans la proposition suivante, on considère que 1 est un produit vide de nombres premiers et que tout nombre premier est un produit à un seul terme.

Proposition 7.16. Existence de la factorisation première et un corollaire

a) **Factorisation première** : Tout entier naturel non nul se décompose en un produit de nombres premiers.

b) **Infinitude de $\mathbb{P}$** : L'ensemble des nombres premiers est infini.

Par exemple, la factorisation première de 924 est $2\times 2\times 3\times 7\times 11$. Nous démontrerons un peu plus loin son unicité, à l'ordre près des facteurs (cf. le théorème fondamental de l'arithmétique).

Un nombre entier n composé admet un facteur premier (i.e. un diviseur) inférieur à $\sqrt{n}$. En effet, en notant p le plus petit facteur premier figurant dans la factorisation première de n, on a $n = pn'$ avec $n' \geqslant p$ car n est composé et par minimalité de p. Ainsi, $n \geqslant p^2$ d'où $p \leqslant \sqrt{n}$.

Pour dresser la liste des nombres premiers inférieurs à 100, il serait maladroit de tester, pour chacun d'entre eux, l'existence d'un diviseur strict non trivial (i.e. au moins égal à deux). L'algorithme du crible d'Eratosthène offre une approche plus efficace :

1	**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	100

On commence par supprimer 1 puis tous les multiples de 2 sauf lui-même car ils sont tous composés.

Le plus petit entier strictement supérieur à deux non supprimé est 3. Il est premier car s'il était composé, il aurait été préalablement supprimé en tant que multiple d'un de ses diviseurs premiers stricts. On continue en supprimant les multiples de 3 excepté lui-même car ils sont tous composés.

On poursuit avec 5 puis 7. Arrivés à 11, nous pouvons arrêter l'algorithme car tout nombre composé inférieur à 100 admet un diviseur non trivial inférieur à $\sqrt{100} = 10$: les entiers non supprimés sont donc tous premiers.

Proposition 7.17.

Soit $p \in \mathbb{P}$ et $(a,b) \in \mathbb{Z}^2$.

a) p ne divise pas a *si et seulement si* $p \wedge a = 1$; b) **Lemme d'Euclide** : si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

On étend par récurrence sur $n \in \mathbb{N}^*$ cette propriété : si $p \mid a_1 \cdots a_n$, alors $\exists i \in [\![1,n]\!],\ p \mid a_i$.

En particulier, si $p \mid a^n$ avec $n \in \mathbb{N}^*$, alors $p \mid a$.

L'équivalence du a) est fausse en général, par exemple 12 ne divise pas 15 mais $12 \wedge 15 = 3$.

4.2. Les valuations p-adiques et le théorème fondamental de l'arithmétique

Les valuations p-adiques permettent de décrire plus simplement la factorisation première d'un entier naturel.

Définition 7.18. Valuations p-adiques

Pour tout $n \in \mathbb{N}^*$ et $p \in \mathbb{P}$, on note $\nu_p(n)$ le plus grand entier naturel k tel que $p^k \mid n$.

Les valuations p-adiques vérifient la propriété d'additivité suivante.

Proposition 7.19. (Additivité des valuations p-adiques)

Pour tout $(a,b) \in (\mathbb{N}^*)^2$ et $p \in \mathbb{P}$, on a $\forall p \in \mathbb{P},\ \nu_p(ab) = \nu_p(a) + \nu_p(b)$.

Nous avons déjà établi l'existence d'une factorisation première (i.e. une décomposition en produit de nombres premiers) dans le paragraphe précédent. Le théorème fondamental de l'arithmétique reprend ce résultat en ajoutant l'unicité de la factorisation à l'ordre près des facteurs premiers.

Theoreme 7.20. fondamental de l'arithmétique

Soit a un entier naturel tel que $n \geqslant 2$.

a. Il existe une unique famille $(\alpha_p)_{p\in\mathbb{P}}$ presque nulle (i.e. telle que le sous-ensemble des p de $\mathbb{P}$ tels que $\alpha_p \neq 0$ est fini) vérifiant

$$a = \prod_{p\in\mathbb{P}} p^{\alpha_p}$$

b. On a $\forall p \in \mathbb{P}, \quad \nu_p(a) = \alpha_p$.

On remarque que produit figurant dans ce théorème est fini bien que l'ensemble $\mathbb{P}$ ne le soit pas. En fait, à partir d'un certain nombre premier p_0, on a $\nu_p(n) = 0$ et le produit a donc bien un sens (un produit infini de 1 valant par convention 1).

Proposition 7.21. Propriétés des valuations p-adiques (suite et fin)

Pour tous a et b dans $\mathbb{N}^*$:

a. $a \mid b \iff \forall p \in \mathbb{P}, \nu_p(a) \leqslant \nu_p(b)$;

b. $a \wedge b = \prod_{p\in\mathbb{P}} p^{\min\left(\nu_p(a),\nu_p(b)\right)}$ et $a \vee b = \prod_{p\in\mathbb{P}} p^{\max\left(\nu_p(a),\nu_p(b)\right)}$.

Ainsi, puisque $12 = 2^2 \times 3$ et $15 = 3 \times 5$, on a $12 \wedge 15 = 2^0 3^1 5^0 = 3$ et $12 \vee 15 = 2^2 3^1 5^1 = 60$. Considérons à présent $n := 10^4 - 1$. On a

$$n = 9999 = 9 \times 1111 = \underbrace{3^2 \times 11 \times 101}_{\text{factorisation première}}$$

On déduit du b) de la proposition précédente que les diviseurs dans $\mathbb{N}$ de n sont les entiers de la forme $d = 3^a 11^b 101^c$ avec $a \in \{0,1,2\}$, b et c dans $\{0,1\}$. On en dénombre donc $3 \times 2 \times 2$ par le lemme de Bergers et l'unicité de la factorisation première. Plus généralement :

Diviseurs d'un nombre entier

Soit $n \in \mathbb{N}^*$.

⇛ Les diviseurs de n dans $\mathbb{N}$ sont exactement les entiers $m \in \mathbb{N}^*$ tels que $\forall p \in \mathbb{P}, \ \nu_p(m) \leqslant \nu_p(n)$.

⇛ En particulier, on en dénombre $\prod_{p\in\mathbb{P}} \left(1 + \nu_p(n)\right)$.

5. Tests

7.1.

En utilisant des congruences, montrer que, pour tout $n \in \mathbb{N}$, on a :

a. $17 \mid 7^{8n+1} + 10(-1)^n$; **b.** $11 \mid 9^{5n+2} - 4$; **c.** $6 \mid 10^{3n+2} - 4^{n+1}$.

7.2.

Critères de divisibilité en base dix. Pour $n = \underline{a_m \dots a_1 a_0}_{10}$, on a

a. $2 \mid n$ *si et seulement si* $a_0 \in \{0,2,4,6,8\}$;

b. $3 \mid n$ *si et seulement si* $3 \mid a_0 + \dots + a_m$;

c. $4 \mid n$ *si et seulement si* $4 \mid \underline{a_1 a_0}_{10}$;

d. $5 \mid n$ *si et seulement si* $a_0 = 0$ ou $a_0 = 5$;

e. $9 \mid n$ *si et seulement si* $9 \mid a_0 + \dots + a_m$;

f. $11 \mid n$ *si et seulement si* $11 \mid a_0 - a_1 + \dots + (-1)^m a_m$.

7.3.

Écrire $n = \underline{543234}_{10}$ en base 3 et $m = \underline{110011}_2$ en base 6.

7.4.

Déterminer le chiffre des unités de 7^9.

7.5.

Soit $m \in \mathbb{N}^*$. Quel est le plus petit entier naturel non nul ayant m chiffre(s) en base 2 ? Même question avec *le plus grand*.

7.6.

Combien l'entier 10^4 a-t-il de chiffres en base 2 ?

7.7.

En inversant les chiffres en base 2 d'un entier n (0 à la place de 1 et inversement), on obtient un autre entier n'. Exprimer n' en fonction de l'entier n et de son nombre m de chiffres en base 2.

7.8.

Calculer $424 \wedge 68$ par l'algorithme d'Euclide.

7.9.

Déterminer les entiers $n \in \mathbb{N}^*$ tels que $n^2 - 1$ est premier.

7.10.

Montrer que, pour tout $n \in \mathbb{N}$ tel que $n \geqslant 2$, $n^4 + 4$ est composé. On pourra utiliser l'identité remarquable $a^2 + b^2 = (a+b)^2 - 2ab$.

6. Solutions

7.1.

a. On a $7^2 = -2\,[17]$ donc $7^4 = (-2)^2 = 4\,[17]$ ainsi $7^8 = 4^2 = -1\,[17]$. Ainsi

$$\begin{aligned} 7^{8n+1} + 10(-1)^n &= 7(7^8)^n + 10(-1)^n\,[17] \\ &= 7(-1)^n + 10(-1)^n\,[17] \\ &= 0\,[17] \end{aligned}$$

b. On a

$$\begin{aligned} 9^{5n+2} - 4 &= (-2)^{5n+2} - 4\,[11] \\ &= 4\left((-32)^n - 1\right)\,[11] = 4\left(1^n - 1\right) = 0\,[11] \end{aligned}$$

c. On a

$$\begin{aligned} 10^{3n+2} - 4^{n+1} &= 4^{3n+2} - 4^{n+1}\,[6] \\ &= \left(4^{2n+1} - 1\right)4^{n+1}\,[6] \end{aligned}$$

Comme 4^{n+1} est divisible par 2 et $4^{2n+1} - 1 = 0\,[3]$, on a $\left(4^{2n+1} - 1\right)4^{n+1} = 0\,[6]$.

7.2.

Commençons par écrire que $n = a_0 + 10a_1 + \ldots + a_m 10^m$.

a. Puisque $2 \mid 10^k$ pour tout $k \geqslant 1$, $n \equiv a_0\,[2]$ et donc $n \equiv 0\,[2]$ *si et seulement si* $a_0 \equiv 0\,[2]$, d'où le résultat puisque $a_0 \in \{0, 1, \ldots, 9\}$.

b. Comme $10 \equiv 1\,[3]$, on a $10^k \equiv 1\,[3]$ pour tout k dans $\mathbb{N}$. Ainsi, $n \equiv a_0 + a_1 + \ldots + a_m\,[3]$ et donc $n \equiv 0\,[3]$ *si et seulement si* $a_0 + a_1 + \ldots + a_m \equiv 0\,[3]$.

c. Comme $4 \mid 100$, $4 \mid 10^k$ pour tout entier $k \geqslant 2$. Ainsi $n \equiv a_0 + 10a_1\,[4]$ et donc $n \equiv 0\,[4]$ *si et seulement si* $\underline{a_1 a_0}_{10} \equiv 0\,[4]$.

d. Comme $5 \mid 10$, $5 \mid 10^k$ pour tout entier $k \geqslant 1$, ainsi $n \equiv a_0\,[5]$ et donc $n \equiv 0\,[5]$ *si et seulement si* $a_0 \equiv 0\,[5]$ c'est-à-dire $a_0 = 0$ ou 5 puisque $a_0 \in \{0, 1, \ldots, 9\}$.

e. Comme $10 \equiv 1\,[9]$, on a $10^k \equiv 1\,[9]$ pour tout k dans $\mathbb{N}$. Ainsi, $n \equiv a_0 + a_1 + \ldots + a_m\,[9]$ et donc $n \equiv 0\,[9]$ *si et seulement si* $a_0 + a_1 + \ldots + a_m \equiv 0\,[9]$.

f. Comme $10 \equiv -1\,[11]$, on a $10^k \equiv (-1)^k\,[11]$ pour tout k dans $\mathbb{N}$. Ainsi, $n \equiv a_0 - a_1 + \ldots + (-1)^m a_m\,[11]$ et donc $n \equiv 0\,[11]$ *si et seulement si* $a_0 - a_1 + \ldots + (-1)^m a_m \equiv 0\,[11]$.

7.3.

⇛ On applique l'algorithme du cours :

543234	3	181078	3
0	181078	1	60359
60359	3	20119	3
2	20119	1	6706
6706	3	2235	3
1	2235	0	745
745	3	248	3
1	248	2	82
82	3	27	3
1	27	0	9
9	3	3	3
0	3	0	1
1	3		
1	0		

On trouve donc $\underline{1000121011210}_3$.

⇛ On a $m = 2^5 + 2^4 + 2 + 2^0 = 51_{10}$. On applique l'algorithme du cours,

51	6	8	6
3	8	2	1
1	6		
1	0		

On trouve donc $\underline{123}_6$.

7.4.

On a $7^2 = -1\,[10]$ donc $7^8 = (-1)^4 = 1\,[10]$ et $7^9 = 7\,[10]$. Le chiffre des unités de 7^9 est 7.

7.5.

Le plus petit :

$$\underbrace{10\cdots0_2}_{m \text{ chiffres}} = 2^{m-1}$$

Le plus grand :

$$\underbrace{11\cdots1_2}_{m \text{ chiffres}} = 2^{m-1} + \cdots + 2 + 1 = 2^m - 1$$

7.6.

Le nombre de chiffres en base 2 de $n = 10^4$ vaut

$$m = 1 + \left\lfloor \frac{\ln(n)}{\ln(2)} \right\rfloor = 1 + \left\lfloor \frac{4\ln(10)}{\ln(2)} \right\rfloor = 14$$

7.7.

On a

$$n + n' = 2^{m-1} + 2^{n-2} + \cdots + 2^1 + 2^0 = 2^m - 1$$

ainsi $n' = 2^m - n - 1$.

7.8.

On a $424 = 68 \times 6 + 16$ donc $424 \wedge 68 = 68 \wedge 16$. Comme $68 = 16 \times 4 + 4$, on a $68 \wedge 16 = 16 \wedge 4 = 4$.

7.9.

Après une petite étude au brouillon, on opte pour une disjonction des cas :

- Si $n = 1$, alors $n^2 - 1$ n'est pas premier.
- Si $n = 2$, alors $n^2 - 1$ est clairement premier.
- Pour tout $n \in \mathbb{N}$, $n^2 - 1 = (n-1)(n+1)$. Pour $n \geqslant 3$, $n^2 - 1$ est donc composé.

7.10.

Pour tout $n \in \mathbb{N}$,

$$\begin{aligned} n^4 + 4 &= (n^2+2)^2 - (2n)^2 \\ &= (n^2 - 2n + 2)(n^2 + 2n + 2) \end{aligned}$$

Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. Comme

$$n^2 + 2n + 2 > 1 \quad \text{et} \quad n^2 - 2n + 2 = n(n-2) + 2 > 1$$

l'entier $n^4 + 4$ est composé.