Chapitre 08
Arithmétique

aut

1 Relations de divisibilité et de congruence dans $\mathbb{Z}$.

1.1 Divisibilité

Définition 1

Soient a et b deux entiers relatifs. On dit que a divise b et on écrit $a|b$ s'il existe un entier relatif k tel que $b = ak$. On dit alors que a est un diviseur de b et que b est un multiple de a.
L'ensemble des multiples de a est noté $a\mathbb{Z}$ et est défini par

$$a\mathbb{Z} = \{ka, k \in \mathbb{Z}\}.$$

Exemple 2

3 divise 9. Pour tout entier k, 1 divise k et k divise 0.
Tout nombre est son propre diviseur.
$2\mathbb{Z}$ est l'ensemble des entiers pairs.

Proposition 3

(i) La relation de divisibilité est une relation d'ordre sur $\mathbb{N}^*$. C'est une relation réflexive et transitive sur $\mathbb{Z}$.

Soit $(a, b, c, d) \in \mathbb{Z}^4$.

2. Si $a|b$ et $b \neq 0$, alors $|a| \leqslant |b|$.

3. Si $d|a$ et $d|b$, alors pour tous u et v entiers relatifs, $d|(au + bv)$.

4. Si $a|c$ et $b|d$, alors $ab|cd$.

Démonstration

1. Déjà vu dans le chapitre 5.

2. Si $a|b$, on dispose de $k \in \mathbb{Z}$ tel que $b = ka$. Or, $b \neq 0$ donc $k \neq 0$. Donc $|k| \geqslant 1$, donc $|a|.|k| \geqslant |a|$, donc $|b| \geqslant |a|$.

3. $d|a$ et $d|b$ donc on dispose de k et k' dans $\mathbb{Z}$ tels que $a = kd$ et $b = k'd$.
Soit $(u, v) \in \mathbb{Z}^2$. Alors

$$au + bv = dku + dk'v = d(ku + k'v)$$

donc $d|au + bv$.

4. Pour vous.

■

Remarque 4

1. La divisibilité n'est pas antisymétrique sur $\mathbb{Z}$: $3|-3$ et $-3|3$.
2. On utilise souvent la contraposée du (ii) : si $a|b$ et $|a| \geqslant |b|$, alors $b = 0$.

1.2 Congruences

Définition 5

Soient a, b et n trois entiers relatifs. On dit que a est congru à b modulo n et on utilise l'une des notations suivantes

$$a \equiv b[n],\ a \equiv b(n),\ a = b[n],\ a = b(n),\ a = b \mod n$$

n divise $a - b$, c'est-à-dire s'il existe un entier relatif k tel que $a = kn + b$.

Proposition 6

La relation de congruence est une relation d'équivalence.

Démonstration

Cf. Chapitre 5. ■

Proposition 7 (Autres propriétés de la relation de congruence)

Soient a, b, c, d, n cinq entiers tels que

$$a \equiv b[n] \text{ et } c \equiv d[n].$$

Alors

(i) $a + c \equiv b + d[n]$.
(ii) $ca \equiv cb[n]$.
(iii) $ac \equiv bd[n]$.
(iv) $\forall k \in \mathbb{N}, a^k \equiv b^k[n]$.
(v) $\forall m \in \mathbb{Z}, am \equiv bm[nm]$.

Démonstration

1. $a \equiv b[n]$ donc $n|(b-a)$
   $c \equiv d[n]$ donc $n|(d-c)$.
   Donc $n|(b-a)+(d-c)$, donc $n|(b+d)-(c+a)$, donc $a + c \equiv b + d[n]$.
2. $a \equiv b[n]$, $n|b-a$ donc $n|c(b-a)$, donc $ca \equiv cb[n]$.
3. $a \equiv b[n]$, donc $ac \equiv bc[n]$.
   $c \equiv d[n]$ donc $bc \equiv bd[n]$
   Donc, par transitivité, $ac \equiv bd[n]$.
4. Récurrence sur k.

5. $a \equiv b[n]$ donc $n|b-a$ donc $nm|m(b-a)$ donc $am \equiv bm[mn]$.

■

Proposition 8

$\forall (a,n) \in \mathbb{Z}^2,\ n|a \Leftrightarrow a \equiv 0[n]$.

Remarque 9 (Et exemples)

1. On ne peut pas « simplifier des congruences » : si $ac \equiv bc[n]$, alors rien ne nous dit que $a \equiv b[n]$.
Par exemple, $2 \times 7 \equiv 2 \times 4[6]$, mais $7 \not\equiv 4[6]$.

2. Montrer que $3|10^{2020} + 2^{2021}$.
Idées : trouver des congruences simples : $10 \equiv 1[3]$, donc $10^{2020} \equiv 1[3]$.
De même, $2 \equiv -1[3]$ donc $2^{2021} \equiv (-1)^{2021}[3]$ donc $2^{2021} \equiv -1[3]$.
Donc $10^{2020} + 2^{2021} \equiv 0[3]$ donc 3 divise $10^{2020} + 2^{2021}$.

3. Les congruences nous permettent aussi de comprendre les différents critères de divisibilité.

1.3 Division euclidienne

Proposition 10

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

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$$

On dit que l'on a effectué la division euclidienne de a par b. a est appelé dividende, b diviseur, q le quotient et r le reste.

Démonstration

Diviser, c'est soustraire !
Existence. Soit $A = \{a - bk,\ k \in \mathbb{N}\} \cap \mathbb{N}$.
A est une partie de $\mathbb{N}$, non vide ($a \in A$) donc A admet un plus petit élément. Notons cet élément r.
$r \in A$ donc on dispose de $q \in \mathbb{N}$ tel que $r = a - bq$, i.e. $a = bq + r$.
$r \in A$ donc $r \geqslant 0$. Montrons que $r < b$.
Si on avait $r \geqslant b$, alors $r - b \geqslant 0$, et

$$r - b = a - bq - b = a - b(q+1).$$

Donc $r - b \in A$, et $r - b < r$, ce qui contredit la minimalité de r.
Donc $r < b$, l'existence est ainsi démontrée !
Unicité. Soient $((q,r),(q',r')) \in (\mathbb{N}^2)^2$, tels que

$$\begin{cases} a = bq + r,\ 0 \leqslant r < b \\ a = bq' + r',\ 0 \leqslant r' < b \end{cases}$$

En soustrayant les deux équations, $0 = b(q-q') + r - r'$, i.e. $r' - r = b(q-q')$.
Donc $b|r'-r$.
Or,

$$0 \leqslant r' < b \text{ et } -b < r \leqslant 0,$$

donc $-b < r' - r < b$, donc $b|r'-r$ et $|r'-r| \leqslant b$, donc $r = r'$.
Donc $b(q-q') = 0$ donc $(b \neq 0)$ $q = q'$.
D'où l'unicité. ■

Proposition 11

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

$$\begin{cases} a = bq + r \\ 0 \leqslant r < |b| \end{cases}$$

Démonstration

L'unicité se démontre exactement comme précédemment. Pour l'existence :

- si $b > 0$ et $a \leqslant 0$, on fait exactement comme avant, sauf qu'on regarde $A = \{a - bk,\ k \in \mathbb{Z}\} \cap \mathbb{N}$.
- si $b < 0$, on écrit $b = -c$, $c > 0$, et on fait la division euclidienne de $-a$ par c : $-a = qc + r$, $0 \leqslant r < c$.
  - si $r = 0$, $a = qb$ et c'est bon,
  - si $r \neq 0$, $q = -qc - r = qb - r = (q+1)b + (-b-r)$, et

$$0 < -b - r < |b|.$$

■

Remarque 12

1. Attention, la division euclidienne de 20 par 3 est $20 = 3 \times 6 + 2$, alors que la division euclidienne de -20 par 3 est $-20 = 3 \times (-7) + 1$.
2. On utilise une division euclidienne pour montrer que $\mathbb{U}_n = \{e^{\frac{2ik\pi}{n}},\ k \in [\![0, n-1]\!]\}$.
3. Le quotient de la division euclidienne de a par b est $\left\lfloor \frac{a}{b} \right\rfloor$. **Exercice** : le démontrer !

Exercice 13

Quel est le dernier chiffre de 18^{2020} ?

Proposition 14 (Écriture d'un nombre dans une base)

Soit b un entier supérieur ou égal à 2. Pour tout entier n non nul, il existe un unique entier

r et un unique $(r+1)-uplet$ $(a_0, a_1, \dots, a_r) \in [\![0, b-1]\!]^{r+1}$ tel que

$$n = \sum_{k=0}^{r} a_k b^k.$$

On note alors $n = \overline{a_r \dots a_0}^b$.

Démonstration

Existence. On montre cette propriété par récurrence **forte** sur $n \in \mathbb{N}^*$.
Initialisation. $1 = 1 \times b^0$.
Hérédité. Soit $n \in \mathbb{N}^*$, $n \geqslant 1$, tel que $\mathcal{P}_0, \dots, \mathcal{P}_{n-1}$ soient vraies.
Effectuons la division euclidienne de n par b : $n = bq + r$, $0 \leqslant r \leqslant b-1$.

- si $q = 0$, $n = r \times b^0$, et c'est gagné.
- sinon, $q < n$, donc, comme $\mathcal{P}_q$ est vraie, on dispose de $N \in \mathbb{N}$, de $(a_0, \dots, a_N) \in [\![0, b-1]\!]^{N+1}$, $a_N \neq 0$, tels que

$$q = \sum_{k=0}^{N} a_k b^k.$$

Donc $n = b.\sum_{k=0}^{N} a_k b^k + r b^0 = r b^0 + a_0 b^1 + a_1 b^2 + \dots + a_N b^{N+1}$.

D'où l'hérédité et le résultat !
Unicité. Soit $n \in \mathbb{N}^*$. Supposons qu'il existe N et M dans $\mathbb{N}$, $(a_0, \dots, a_N)$, $(c_0, \dots, c_{N'})$ tels que $a_N \neq 0$, $c_{N'} \neq 0$, et

$$n = \sum_{k=0}^{N} a_k b^k = \sum_{k=0}^{N'} c_k b^k.$$

Sans perte de généralité, on peut supposer $N \geqslant N'$, et poser $c_{N'+1} = c_{N'+2} = \dots = c_N$. Montrer l'unicité revient alors à démontrer que $(a_0, \dots, a_N) = (c_0, \dots, c_N)$ (si $a_N \neq 0$, alors $c_N \neq 0$ nécessairement).
Supposons que ce ne soit pas le cas. Alors la partie

$$A = \{k \in [\![0, N]\!],\ a_k \neq c_k\}$$

est une partie de $\mathbb{N}$, non vide, donc admet un plus petit élément. Notons-le k_0. Alors, en particulier,

$$a_0 = c_0,\ a_1 = c_1,\ \dots, a_{k_0-1} = c_{k_0-1}.$$

Donc l'égalité des deux décompositions se réécrit

$$\sum_{k=k_0}^{N} a_k b^k = \sum_{k=k_0}^{N} c_k b^k$$

ou, plus précisément,

$$a_{k_0} b^{k_0} + \sum_{k=k_0+1}^{N} a_k b^k = c_{k_0} b^{k_0} + \sum_{k=k_0+1}^{N} c_k b^k.$$

Mais a_{k_0} et c_{k_0} sont dans $[\![0, b-1]\!]$ donc $a_{k_0} b^{k_0}$ et $c_{k_0} b^{k_0}$ sont dans $[\![0, b^{k_0}-1]\!]$... cela fait penser à une division euclidienne ! Effectuons la division euclidienne des deux membres par b^{k_0+1} :

$$a_{k_0} b^{k_0} + \sum_{k=k_0+1}^{N} a_k b^k = a_{k_0} b^{k_0} + b^{k_0+1} \sum_{k=k_0+1}^{N} a_k b^{k-k_0-1}$$

et

$$c_{k_0} b^{k_0} + \sum_{k=k_0+1}^{N} c_k b^k = c_{k_0} b^{k_0} + b^{k_0+1} \sum_{k=k_0+1}^{N} c_k b^{k-k_0-1}$$

Par unicité du reste de la division euclidienne, $a_{k_0} = c_{k_0}$, absurde, car par définiton $a_{k_0} \neq c_{k_0}$. Donc A est vide, donc $(a_0, \dots, a_N) = (c_0, \dots, c_N)$. D'où l'unicité ! ■

Remarque 15

On a en fait $r = [\log_b(n)] + 1$.

Remarque 16

En fait, la preuve de l'existence de la décomposition en base b donne un **algorithme** de décomposition en base b : l'algorithme des divisions successives. Illustrons-le avec la base 2.

2 PGCD et PPCM

Remarque 17

Quand on dit « soit $(a_0, \dots, a_n)$ n nombres non tous nuls », c'est que l'on veut dire que $(a_0, \dots, a_n) \neq (0, \dots, 0)$.

Proposition 18 (et defi)

Soient a et b deux entiers non tous nuls.

(i) L'ensemble des diviseurs entiers naturels de a et b admet un plus grand élément (pour le relation d'ordre usuel sur $\mathbb{N}$). On le nomme plus grand commun diviseur de a et b et on le note $\text{pcdg}(a, b)$ ou $a \wedge b$.

(ii) L'ensemble des multiples entiers naturels non nuls de a et b admet un plus petit élément (pour la relation d'ordre usuel sur $\mathbb{N}$). On le nomme plus petit commun multiple à a et b et on le note $\text{ppcm}(a, b)$ ou $a \vee b$.

Remarque 19

Par convention, on dira que $0 \wedge 0 = 0$.

Démonstration

1. Soit $A = \{k \in \mathbb{N},\ k|a \text{ et } k|b\}$. Alors $A \subset \mathbb{N}$ et, comme $1 \in A$, $A \neq \emptyset$. De plus, si $a \neq 0$, alors pour tout k dans A, $k \leqslant |a|$. De même pour b.
   Comme a ou b est non nul, A est majoré, donc admet un plus grand élément.
2. $B = \{k \in \mathbb{N},\ a|k \text{ et } b|k\}$. $B \subset \mathbb{N}$, $B \neq \emptyset$ ($ab \in B$), donc B admet un plus petit élément.

■

Exemple 20

$15 \wedge 12 = 3$.

Proposition 21 (Relation de Bézout)

Soient a, b deux entiers non tous nuls. Alors il existe deux entiers u et v tels que

$$au + bv = a \wedge b.$$

Démonstration

- Considérons $CL(a,b) = \{au + bv,\ (u,v) \in \mathbb{Z}^2\}$ et $CL^+(a,b) = CL(a,b) \cap \mathbb{N}^*$.
  $CL^+(a,b) \subset \mathbb{N}$, $CL^+(a,b) \neq \emptyset$ (car $a^2 + b^2 \in CL(a,b)$ et $a^2 + b^2 > 0$) donc $CL^+(a,b)$ admet un plus petit élément δ.
  Démontrons que $\delta = a \wedge b$.
- Déjà, on démontre que δ est un diviseur commun à a et b.
  Effectuons la division euclidienne de a par δ :

  $$a = \delta q + r,\ 0 \leqslant r \leqslant \delta - 1.$$

  Alors $r = a - \delta q$. Mais $\delta \in CL^+(a,b)$ donc on dispose de $(u,v) \in \mathbb{Z}^2$ tels que $\delta = au + bv$.
  Donc

  $$r = a - (au + bv)q = a(1 - uq) + b(-vq) \in CL(a,b).$$

  Si on avait $r > 0$ on aurait $r \in CL^+(a,b)$ et $r < \delta$, absurde par minimalité de δ.
  Donc $r = 0$, donc $\delta | a$.
  De même, $\delta | b$.
- Montrons que δ est le plus grand diviseur commun.
  Soit d un diviseur commun (positif) à a et b. $d|a$ et $d|b$ donc $d|au + bv$, donc $d|\delta$. Comme $\delta > 0$, $d \leqslant \delta$.
  Donc $\delta = a \wedge b$.

Donc $a \wedge b = au + bv$.
■

Corollaire 22

Soit δ un diviseur commun à a et b. Alors δ divise $a \wedge b$.

Démonstration

Donné par la preuve précédente. ■

Remarque 23

En fait, la relation de Bézout nous permet de dire que l'ensemble des diviseurs > 0 communs à a et b a un plus grand élément **pour la relation** $|$**.**

Exercice 24

1. Déterminer, si $n \in \mathbb{N}$, $n \wedge (n+1)$, $n \wedge (n+2)$, $n^2 \wedge (n^2-n)$.
2. Déterminer $12 \wedge 15$.

Proposition 25

1. $a \wedge b = |a| \wedge |b|$.
2. (Commutativité) Soit $(a,b) \in \mathbb{Z}^2$, avec $(a,b) \neq (0,0)$. Alors $a \wedge b = b \wedge a$.
3. (Associativité du pgcd) Soit $(a,b,c) \in \mathbb{Z}^3$, $(a,b,c) \neq (0,0,0)$. Alors $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.
4. (Multiplicativité du pgcd) Soit $(a,b) \in \mathbb{Z}^2$, $(a,b) \neq (0,0)$, $n \in \mathbb{Z}^*$. Alors $(na) \wedge (nb) = |n| a \wedge b$.
5. (Élément absorbant) Pour tout a dans $\mathbb{Z}$, $a \wedge 1 = 1$.
6. (Neutre) Soit $a \neq 0$. Alors $a \wedge 0 = a$.
7. (Proposition de l'algorithme d'Euclide) Soit $(a,b) \in \mathbb{Z}^2$, $b \neq 0$, $k \in \mathbb{Z}$. Alors $a \wedge b = (a + kb) \wedge b$.
   En particulier, si r est le reste de la division euclidienne de a par b, $a \wedge b = b \wedge r$.

Démonstration

Toutes ces preuves sont essentiellement triviales.

1. Évident.
2. Évident.
3. Notons $d = (a \wedge b) \wedge c$ et $\delta = a \wedge (b \wedge c)$. Alors
   - d divise a, b et c donc d divise a et $b \wedge c$ donc d divise δ.
   - De même, δ divise d.

   Donc, comme d et δ sont strictement positifs, ils sont égaux.
4. Soient u, v tels que $a \wedge b = au + bv$.
   Si $d = (na) \wedge (nb)$ et $\delta = |n|(a \wedge b)$, alors
   - $(a \wedge b)$ divise a et b donc $|n|(a \wedge b)$ divise na et nb. Donc δ divise na et nb, donc δ divise d.
   - d divise na et nb donc d divise $|n|ua + |n|vb = \delta$.

   Donc, étant positifs, $d = \delta$.
5. Évident
6. Évident
7. Soit $d = a \wedge b$ et $\delta = (a + kb) \wedge b$: on montre que $d|\delta$ et $\delta|d$ à l'aide de combinaisons linéaires.

■

Proposition 26 (Algorithme d'Euclide)

Soient $(a,b) \in (\mathbb{Z}^*)^2$. On définit la suite $(r_n)_{n\in\mathbb{N}}$ comme suit :

- $r_0 = |a|$,

- $r_1 = |b|$,
- pour tout n dans $\mathbb{N}$, si $r_{n+1} \neq 0$, r_{n+2} est le reste de la division euclidienne de r_n par r_{n+1}. Sinon, $r_{n+2} = 0$.

Alors il existe N dans $\mathbb{N}$ tel que $r_{N+1} = 0$ et $r_N = a \wedge b$.

Démonstration

- Existence de N : pour tout n dans $\mathbb{N}$ tel que $r_{n+1} \neq 0$, r_{n+2} est le reste de la division euclidienne de r_n par r_{n+1} donc $r_{n+2} < r_{n+1}$. Donc la suite $(r_n)_{n\in\mathbb{N}}$ est une suite d'entiers strictement décroissante tant qu'elle n'est pas nulle : $r_0 > r_1 > \cdots \geqslant 0$. On ne peut donc pas avoir une infinité de termes non nuls, donc $(r_n)_{n\in\mathbb{N}}$ est nulle à partir d'un certain rang. Donc l'algorithme se termine.
- Soit alors $N \in \mathbb{N}$ tel que $r_{N+1} = 0$ et $r_N \neq 0$. On montre alors que $r_n \wedge r_{n+1} = a \wedge b$ par récurrence sur $n \in [\![0, N]\!]$.
  Initialisation. $r_0 \wedge r_1 = |a| \wedge |b| = a \wedge b$.
  Hérédité. Si $r_n \wedge r_{n+1} = a \wedge b$, alors comme r_{n+2} est le reste de la division euclidienne de r_n par r_{n+1}, $r_n \wedge r_{n+1} = r_{n+1} \wedge r_{n+2}$.
  D'où l'hérédité et le résultat.
  En particulier, $a \wedge b = r_N \wedge r_{N+1} = r_N \wedge 0 = r_N$.

■

Remarque 27

1. C'est un bon programme informatique à écrire !
2. On peut une relation de Bézout à partir de l'algorithme d'Euclide : exemple de $103 \wedge 72$.
3. Plus précisément, si on définit (s_n) et (t_n) par $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$,

$$t_{n+2} = t_n - q_{n+2} t_{n+1}$$
$$s_{n+2} = s_n - q_{n+2} s_{n+1}$$

où q_{n+2} est le quotient de la division de r_n par r_{n+1}, alors $a \wedge b = a s_N + b t_N$ (exercice)

Définition 28

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

Théorème 29 (Bézout)

Soient $(a, b) \in \mathbb{Z}^2$. a et b sont premiers entre eux si, et seulement si

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

Démonstration

$\boxed{\Rightarrow}$ Si $a \wedge b = 1$, c'est évident par la relation de Bézout.

$\boxed{\Leftarrow}$ Supposons que l'on dispose de $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$. Donc, comme $a \wedge b$ divise a et b, $a \wedge b$ divise $au + bv = 1$ donc $a \wedge b$ divise 1 donc, étant positif, il est égal à 1.

■

Corollaire 30

Soient a et b deux entiers. Alors $a' = \dfrac{a}{a \wedge b}$ et $b' = \dfrac{b}{a \wedge b}$ sont premiers entre eux.

Démonstration

Il suffit de diviser une relation de Bézout entre a et b par $a \wedge b$. ■

Théorème 31 (Gauss)

Soient $(a, b, c) \in \mathbb{Z}^3$ tels que a divise bc et $a \wedge b = 1$. Alors a divise c.

Démonstration

$a \wedge b = 1$ donc on dispose de $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$.
Alors $acu + bcv = c$.
Or, a divise a et a divise bc, donc a divise $acu + bvc = c$. ■

Proposition 32 (Gauss bis)

Soit $(a, b, c) \in \mathbb{Z}^3$, (a, b) non tous nuls. Si $a|c$, $b|c$ et $a \wedge b = 1$, alors $ab|c$.

Démonstration

$a \wedge b = 1$ donc on dispose de $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$. Alors $acu + bcv = c$.
$a|c$ donc $ab|bcv$, $b|c$ donc $ab|acu$. Donc $ab|c$. ■

Exemple 33

1. Soient $n \in \mathbb{N}^*$, $k \in \mathbb{Z}$. CNS sur k pour que k soit inversible modulo n, i.e. qu'il existe $\ell \in \mathbb{Z}$, $k\ell \equiv 1[n]$?
2. Soient $n \in \mathbb{N}^*$. On note $\omega_k = e^{\frac{2ik\pi}{n}}$. CNS sur ω_k pour que ω_k engendre $\mathbb{U}_n$, i.e. que

$$\forall \alpha \in \mathbb{U}_n,\ \exists p \in \mathbb{N},\ \alpha = \omega_k^p.$$

Proposition 34

Soient $(a, b, c) \in \mathbb{Z}^3$, $n \in \mathbb{Z}$. Si $ab \equiv ac[n]$ et **si** a **et** n **sont premiers entre eux**, alors $b \equiv c[n]$.

Remarque 35

On comprend l'idée d'« inversibilité modulo n » mentionnée dans l'exemple précédent.

Proposition 36

Soit $r \in \mathbb{Q}$. Il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $p \wedge q = 1$ et $r = \frac{p}{q}$.
$\frac{p}{q}$ est appelée écriture irréductible du rationnel r.

Démonstration

- **Existence.** Soit $r \in \mathbb{Q}$. ON dispose de $a \in \mathbb{Z}$, de $b \in \mathbb{N}^*$ tels que $r = \frac{a}{b}$. Alors

$$r = \frac{\frac{a}{a \wedge b}}{\frac{b}{a \wedge b}},$$

  et on a déjà vu que $\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premiers entre eux. D'où l'existence.

- **Unicité.** Soient $(a, a') \in \mathbb{Z}^2$, $(b, b') \in (\mathbb{N}^*)^2$ tels que $a \wedge b = 1$, $a' \wedge b' = 1$ et $\frac{a}{b} = \frac{a'}{b'}$. Alors $ab' = a'b$. Donc
  — $b' | a'b$ et $b' \wedge a' = 1$ donc $b' | b$,
  — $b | ab'$ et $b \wedge a = 1$ donc $b | b'$.
  Comme b et b' sont dans $\mathbb{N}^*$, $b = b'$. Donc $a = a'$.
  D'où l'unicité.

■

Exercice 37

1. (Re)démontrer que $\sqrt{2} \notin \mathbb{Q}$.
2. Montrer que l'équation $x^3 - x^2 + x + 1 = 0$ n'a pas de solutions rationnelle.

Proposition 38

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.

1. $a \vee b = \frac{ab}{a \wedge b}$,
2. tout multiple commun à a et b est multiple de $a \vee b$.

Démonstration

Notons $\frac{ab}{a \wedge b}$.

1. On montre que m est un multiple de a et de b.
   - $a \wedge b | a$ donc $\frac{a}{a \wedge b} \in \mathbb{Z}$, donc $\frac{a}{a \wedge b} b = m$ est un multiple de b,

- de même, $a \wedge b | b$ donc $\frac{b}{a \wedge b} a = m$ est un multiple de a.

Donc m est un multiple commun à a et à b.

2. Soit M un multiple commun à a et à b. Alors on dispose de k et de ℓ dans $\mathbb{Z}$ tels que $M = ka$ et $M = \ell b$. Donc $ka = \ell b$ donc, comme $a \wedge b | a$ et $a \wedge b | b$,

$$k \frac{a}{a \wedge b} = \ell \frac{b}{a \wedge b}.$$

Or,

- $\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premiers entre eux,
- comme $\frac{a}{a \wedge b}$ divise $\ell \frac{b}{a \wedge b}$, par le théorème de Gauss, $\frac{a}{a \wedge b}$ divise v, i.e. $v = p \frac{a}{a \wedge b}$.

Donc $M = pb \frac{a}{a \wedge b} = pm$, donc m divise M, donc $(M \neq 0)$ $m \leqslant M$.

3. Donc $m = a \vee b$, et le deuxième point est aussi prouvé.

■

On peut aussi définir le pgcd de n éléments (on ne va pas démontrer les propriétés suivantes)

Définition 39

Soient $n \in \mathbb{N}^*$, $(a_1, \dots, a_n) \in \mathbb{Z}^n$, non tous nuls.

1. L'ensemble des diviseurs positifs communs à $(a_1, \dots, a_n)$ admet un plus grand élément, noté $\mathrm{pgcd}(a_1, \dots, a_n)$.

2. L'ensemble des multiples strictement positifs communs à $(a_1, \dots, a_n)$ admet un plus petit élément. On le note $\mathrm{ppcm}(a_1, \dots, a_n)$.
Si l'un des a_k est nul, on dit que ce ppcm est nul.

Proposition 40

Soient $n \in \mathbb{N}^*$, $(a_1, \dots, a_n) \in \mathbb{Z}^n$. Alors

$$\mathrm{pgcd}(a_1, \dots, a_n) = a_1 \wedge \Big(a_2 \wedge (\cdots \wedge a_n)\Big) = a_1 \wedge \cdots \wedge a_n.$$

(par associativité)

Proposition 41 (Relation de Bézout)

Soient $n \in \mathbb{N}^*$, $(a_1, \dots, a_n) \in \mathbb{Z}^n$. Alors on dispose de $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tels que

$$a_1 u_1 + \cdots + a_n u_n = \mathrm{pgcd}(a_1, \dots, a_n).$$

Définition 42

Soient $n \in \mathbb{N}^*$, $(a_1, \dots, a_n) \in \mathbb{Z}^n$. On dit que $(a_1, \dots, a_n)$ sont premiers entre eux **dans leur ensemble** si $\mathrm{pgcd}(a_1, ; a_n) = 1$.

Proposition 43 (Théorème de Bézout)

Soient $n \in \mathbb{N}^*$, $(a_1, \dots, a_n) \in \mathbb{Z}^n$. Alors $(a_1, \dots, a_n)$ sont premiers entre eux dans leur ensemble si et seulement s'il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tels que

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

Remarque 44

1. Ne pas confondre « premiers entre eux dans leur ensemble » et « premiers entre eux deux à deux ». Si $a = 6$, $b = 15$ et $c = 10$, alors a, b, c sont premiers entre eux dans leur ensemble mais pas deux à deux !
2. On ne peut pas obtenir le ppcm de n nombres en divisant leur produit par leur pgcd. Par exemple, si $a = 6$, $b = 15$ et $c = 10$, $\text{pgcd}(a, b, c) = 1$ et $\text{ppcm}(a, b, c) = 30$.

3 Nombres premiers

3.1 Définition – Théorème fondamental de l'arithmétique

Définition 45

Un entier p supérieur ou égal à 2 est dit premier si ses seuls diviseurs sont ± 1 et $\pm p$.
On note $\mathbb{P}$ l'ensemble des nombres premiers.

Remarque 46

2 est le seul entier pair premier, 1 n'est pas premier.

Proposition 47

Tout entier $n \geqslant 2$ est divisible par au moins un nombre premier.

Démonstration

On démontre par récurrence forte que $\forall 2 \geqslant 2$,

$$\mathcal{P}_n \ : \ n \text{ est divisible par au moins un nombre premier.}$$

Initialisation. 2 est premier et se divise lui-même.
Hérédité. Soit $n \geqslant 3$ tel que $\mathcal{P}_0, \dots, \mathcal{P}_{n-1}$ soient vrais.
Si n est premier, $n|n$ donc $\mathcal{P}_n$ est vraie.
Si n n'est pas premier, on dispose de $(a, b) \in \mathbb{N}^2$, différents de 1 et n, tels que $n = ab$. En particulier, $a \in [\![2, n-1]\!]$ donc, par hypothèse de récurrence, a admet un facteur premier, donc n aussi.
D'où l'hérédité et le résultat. ■

Proposition 48

L'ensemble $\mathbb{P}$ est infini.

Démonstration

On démontre ce résultat par l'absurde.
Supposons que $\mathbb{P}$ est fini, i.e. que $\mathbb{P} = \{p_1, \dots, p_N\}$.
Considérons $K = p_1 \times \cdots \times p_N + 1$.
Alors K a un diviseur premier. Mais comme $K \equiv 1[p_i]$ pour tout i, ce diviseur premier ne peut être aucun des p_i. ABSURDE ■

Proposition 49

1. $\forall (p,q) \in \mathbb{P}^2,\ p \neq q \Leftrightarrow p \wedge q = 1$.
2. $\forall p \in \mathbb{P}$ et $a \in \mathbb{N}$, ou bien $p \wedge a = 1$, ou bien $p|a$.
3. Si $(p,q) \in \mathbb{P}^2$, si $a \in \mathbb{N}$, $p|a$ et $q|a \Rightarrow pq|a$.
4. Si $p \in \mathbb{P}$, si $(a,b) \in \mathbb{N}^2$, alors $p|ab \Rightarrow p|a \wedge p|b$.

Définition 50

Soit $n \in \mathbb{N}^*$, $p \in \mathbb{P}$. Alors l'ensemble

$$\{k \in \mathbb{N},\ p^k | n\}$$

est une partie non vide, majorée de $\mathbb{N}$. Elle admet donc un plus grand élément. On appelle cet élément **valuation p-adique de** n et on le note $v_p(n)$.

Démonstration

On remarque que comme $p \geqslant 2$, $p^k \underset{k \to +\infty}{\longrightarrow} +\infty$, donc on dispose de K dans $\mathbb{N}$ tel que $p^K > n$.
D'où le caractère borné de la partie. ■

Proposition 51

Soit $n \in \mathbb{N}^*$, $p \in \mathbb{P}$, $k \in \mathbb{N}$. Alors

$$p^k | n \Leftrightarrow k \leqslant v_p(n).$$

Démonstration

Notons $A = \{k \in \mathbb{N},\ p^k | n\}$.
Si $p^k | n$, alors $k \in A$, donc, comme $v_p(n)$ est le plus grand élément de A, $k \leqslant v_p(n)$.
Si $k \leqslant v_p(n)$, comme $p^{v_p(n)} | n$, et que $p^k | p^{v_p(n)}$, par transitivité, p^k divise n. ■

Proposition 52

Soit $n \in \mathbb{N}^*$, $p \in \mathbb{P}$, $m \in \mathbb{N}$. Alors les ASSE :

1. $m = v_p(n)$
2. $p^m | n$ et $p^{m+1} \nmid n$
3. Il existe q dans $\mathbb{N}^*$ tel que $n = p^m q$ et $p \wedge q = 1$.

Démonstration

Procédons par implications circulaires.

1. Supposons que $m = v_p(n)$. Alors par définition, si
$$A = \{k \in \mathbb{N},\ p^k | n\},$$
$p^m | n$ mais, comme m est le plus grand élément de A, $p^{m+1} \nmid n$.
2. Si $p^m | n$ et $p^{m+1} \nmid n$, alors on sait que $n = p^m q$ avec $q \in \mathbb{N}$. Mais, si p divisait q, alors p^{m+1} diviserait n, absurde. Donc $p \nmid q$.
3. Si $n = p^m q$ avec $p \nmid q$, alors, déjà, $p^m | n$ donc $m \in A$. Mais s'il existait k tel que $k > m$ et p^k divise n, alors $n = p^k d = p^m q$, donc $p^{k-m} d = q$, donc, comme $k - m > 0$, $p | q$, absurde ! Donc $m = v_p(n)$.

■

Proposition 53

Soit $p \in \mathbb{P}$, $(n, m) \in (\mathbb{N}^*)^2$. Alors
$$v_p(nm) = v_p(n) + v_p(m).$$
Par récurrence immédiate, pour tout k dans $\mathbb{N}$, $v_p(n^k) = k v_p(n)$.

Démonstration

Notons $a = v_p(n)$, $b = v_p(m)$. Alors on dispose de q et r dans $\mathbb{N}^*$ tels que $n = p^a q$, $m = p^b r$, avec q et r non divisibles par p. Donc $nm = p^{a+b} qr$ et, comme p est premier, p ne divise pas qr. D'où le résultat. ■

On arrive ensuite au théorème fondamental de l'arithmétique.

Théorème 54

Soit n un entier naturel non nul, $n \geqslant 2$. Alors
$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)},$$
le produit étant en fait sur un nombre fini de termes (les p tels que $v_p(n) \neq 0$).
Plus précisément, il existe un entier m, m nombres premiers $p_1, \ldots, p_m$, m entiers naturels non nuls $\alpha_1, \ldots, \alpha_m$ tels que
$$n = \prod_{k=1}^{m} p_k^{\alpha_k}.$$
De plus, cette décomposition est unique.

Pour démontrer l'unicité, on aura besoin d'un Lemme.

Lemme 55

Soient $r \in \mathbb{N}^*$, $(p_1, \dots, p_r)$ r nombres premiers distincts, $(\alpha_1, \dots, \alpha_r)$ r entiers naturels, et

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}.$$

Alors pour tout i dans $[\![1, r]\!]$,

$$v_{p_i}(n) = \alpha_i.$$

Démonstration

Soit $i \in [\![1, r]\!]$. Alors

$$n = p_i^{\alpha_i} \times \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} p_j^{\alpha_j}.$$

Or, pour tout j dans $[\![1, r]\!]$ différent de i, p_i ne divise pas p_j donc, comme p_i est premier, p_i ne divise pas $p_j^{\alpha_j}$, donc, toujours comme p_i est premier, p_i ne divise pas $\prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} p_j^{\alpha_j}$. Par caractérisation de la valuation, on en déduit que $v_{p_i}(n) = \alpha_i$. ■

Démonstration

- **Existence.** On démontre le résultat par récurrence forte.
  Initialisation. $2 = 2$, c'est gagné.
  Hérédité. Soit n dans $\mathbb{N}$ tel que la proposition soit vraie jusqu'au rang $n-1$. Alors n admet un facteur premier p_0. On sait alors que $n = q.p_0^{v_{p_0}(n)}$, où $q \in [\![1, n-1]\!]$. Par hypothèse de récurrence, on sait que $q = \prod_{p \in \mathbb{P}} p^{v_p(q)}$. Mais alors,

  $$n = p_0^{v_{p_0}(n)} \times \prod_{p \in \mathbb{P}} p^{v_p(q)}.$$

  Mais, si $p \in \mathbb{P}$, $v_p(n) = v_p(p_0^{v_{p_0}(n)}) + v_p(q)$, donc,
  — si $p = p_0$, $v_p(q) = 0$,
  — si $p \neq p_0$, $v_p(n) = v_p(q)$.
  Donc $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$.
  D'où l'hérédité et le résultat.
- **Unicité.** C'est immédiat par le lemme précéden !

■

Corollaire 56

Soient m et n des entiers naturels non nuls. Alors

$$m = n \Leftrightarrow \forall p \in \mathbb{P},\ v_p(n) = v_p(m).$$

Exemple 57

- On peut utiliser la notion de valuation pour démontrer le plus simplement possible que $\sqrt{2}$ est irrationnel. Supposons en effet que $\sqrt{2} \in \mathbb{Q}$. Alors on dispose de p et q entiers naturels non nuls tels que $\sqrt{2} = \frac{p}{q}$. Alors $2q^2 = p^2$. Or, $v_2(2q^2) = 1 + 2v_2(q)$, donc ce nombre est impair, alors que $v_2(p^2) = 2v_2(p)$, qui est pair. Absurde !
- Il est intéressant de remarquer que $v_p(n) \leqslant \log_p(n)$.

Proposition 58

Soient a et b deux entier naturels non nuls. Alors a divise b si, et seulement si

$$\forall p \in \mathbb{P},\ v_p(a) \leqslant v_p(b).$$

Démonstration

$\boxed{\Rightarrow}$ Si $a|b$, alors on dispose de $c \in \mathbb{N}^*$ tel que $b = ac$. Soit $p \in \mathbb{P}$. ALors

$$v_p(b) = v_p(ac) = v_p(a) + v_p(c) \geqslant v_p(a).$$

$\boxed{\Leftarrow}$ Si $\forall p \in \mathbb{P},\ v_p(a) \leqslant v_p(b)$, posons, pour tout p dans $\mathbb{P}$, $\alpha_p = v_p(b) - v_p(a)$. La suite $(\alpha_p)_{p\in\mathbb{P}}$ n'a qu'un nombre fini de termes non nuls.
Posons alors $c = \prod_{p\in\mathbb{P}} p^{\alpha_p}$.
Alors, pour tout p dans $\mathbb{P}$,

$$v_p(ac) = v_p(a) + v_p(b) - v_p(a) = v_p(b),$$

donc $ac = b$. Donc a divise b.

■

Exemple 59

1. (TD10) Soient a et b dans $\mathbb{N}^2$ tels que a^2 divise b^2. Démontrer que a divise b.

2. Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Combien n a-t-il de diviseurs ?

Proposition 60

Soient a et b deux entiers naturels non nuls. Alors

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

Démonstration

- Pour $a \wedge b$, on démontre que pour tout p dans $\mathbb{P}$, $v_p(a \wedge b) = \min(v_p(a), v_p(b))$.
  - Comme $a \wedge b | a$ et $a \wedge b | b$, alors, pour tout p dans $\mathbb{P}$, $v_p(a \wedge b) \leqslant v_p(a)$ et $v_p(a \wedge b) \leqslant v_p(b)$, donc
  $$v_p(a \wedge b) \leqslant \min(v_p(a), v_p(b)).$$
  - Soit $c = \prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b))}$. Alors pour tout p dans $\mathbb{P}$, $v_p(c) = \min(v_p(a), v_p(b))$ donc $v_p(c) \leqslant v_p(a)$ et $v_p(c) \leqslant v_p(b)$.
  Donc $c | a$ et $c | b$ donc, par propriété du pgcd, $c | a \wedge b$, donc $v_p(c) \leqslant v_p(a \wedge b)$, i.e. $\min(v_p(a), v_p(b)) \leqslant v_p(a \wedge b)$.

  D'où le résultat par double inégalité !
- Pour $a \vee b$, on peut ruser ! On remarque simplement que, comme $(a \wedge b) \times (a \vee b) = ab$, alors, si $p \in \mathbb{P}$,
  $$v_p(a \wedge b) + v_p(a \vee b) = v_p(a) + v_p(b),$$
  donc
  $$v_p(a \vee b) = v_p(a) + v_p(b) - \min(v_p(a), v_p(b)) = \max(v_p(a), v_p(b)),$$
  d'où le résultat !

■

Exemple 61

Démontrer que deux nombres sont premiers entre eux si et seulement si leurs carrés sont premiers entre eux.

3.2 Le petit théorème de Fermat

Théorème 62

Soient p un nombre premier, a un entier. Alors
$$a^p \equiv a[p].$$
Si de plus p ne divise pas a,
$$a^{p-1} \equiv 1[p]$$

Pour démontrer ce résultat, on aura besoin de deux lemmes.

Lemme 63

Pour tout entier k de $[\![1, p-1]\!]$, p divise $\binom{p}{k}$.

Démonstration

Soit $k \in [\![1, p-1]\!]$. Alors $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$. Donc $p\binom{p-1}{k-1} = k\binom{p}{k}$. Donc p divise $k\binom{p}{k}$. Comme p est premier avec k (car $k \in [\![1, p-1]\!]$), par le théorème de Gauss, p divise $\binom{p}{k}$. ■

Lemme 64

Soient u et v deux entiers relatifs, alors

$$(u+v)^p \equiv u^p + v^p [p]$$

Démonstration

Par la formule du binôme de Newton,

$$(u+v)^p = \sum_{k=0}^{p} \binom{p}{k} u^k v^{n-k} = u^p + v^p + \sum_{k=1}^{p-1} \binom{p}{k} u^k v^{n-k} \equiv u^p + v^p [p]$$

car pour tout k dans $[\![1, p-1]\!]$, p divise $\binom{p}{k}$. ■

Démonstration (Preuve du petit théorème de Fermat)

Faisons une récurrence sur a, en notant pour tout a dans $\mathbb{N}$, $\mathcal{P}_a : a^p \equiv a[p]$.
Initialisation. $0^p \equiv 0[p]$.
Hérédité. Soit $a \in \mathbb{N}$ tel que $a^p \equiv a[p]$. Alors par le second lemme,

$$(a+1)^p \equiv a^p + 1^p [p],$$

donc, par hypothèse de récurrence,

$$(a+1)^p \equiv a + 1[p]$$

d'où l'hérédité et le résultat.
De plus, si $p \nmid a$, alors $p \wedge a = 1$ donc $a^{p-1} \equiv 1[p]$. ■

Exercice 65

Déterminer le reste de la division euclidienne de 2^{343} par 11.