Chapitre 2. Arithmétique.

Table des matières

1. Division euclidienne

Définition

Soit $a, b \in \mathbb{Z}$. On dit que a *divise* b ou b *est divisible par* a ou encore a *est un diviseur de* b s'il existe $m \in \mathbb{Z}$ tel que $b = am$. On dit aussi que b est *un multiple de* a. On note $a \mid b$ ou $b \vdots a$.

Exemple

$2 \mid 4$, $\quad 100 \vdots 10$, $\quad -15 \vdots 3$, $\quad n \mid 0 \quad \forall n \in \mathbb{Z}$.

Proposition

1) Si $a \mid b$, $a \neq 0$, $b \neq 0$ *alors* $-\mid b \mid \leqslant a \leqslant \mid b \mid$
si en plus $b \geqslant 0$, *alors* $-b \leqslant a \leqslant b$.
2) Si $a \mid b$ *et* $b \mid c$ *alors* $a \mid c$.
3) Si $a \mid b$ *et* $a \mid c$ *alors* $a \mid (b + c)$.
4) Si $a \mid b$ *et* $a \mid c$ *alors* $a \mid (kb + rc)$ *quelques soient* $k, r \in \mathbb{Z}$.

Démonstration.
1) $\boldsymbol{b = ma}$ alors $|\ \boldsymbol{b}\ | = |\ \boldsymbol{m}\ |\,|\ \boldsymbol{a}\ |$. Puisque $\boldsymbol{m \neq 0}$, on a $|\ \boldsymbol{m}\ | \geqslant \boldsymbol{1}$ et $|\ \boldsymbol{b}\ | \geqslant |\ \boldsymbol{a}\ |$, donc $-|\ \boldsymbol{b}\ | \leqslant \boldsymbol{a} \leqslant |\ \boldsymbol{b}\ |$.Si $\boldsymbol{b \geqslant 0}$ on obtient $-\boldsymbol{b} \leqslant \boldsymbol{a} \leqslant \boldsymbol{b}$.
2) Si $\boldsymbol{b = ma}$, $\boldsymbol{c = nb}$ alors $\boldsymbol{c = nma}$.
3) Si $\boldsymbol{b = ma}$, $\boldsymbol{c = na}$ alors $\boldsymbol{b + c = (m + n)a}$.
4) Si $\boldsymbol{b = ma}$, $\boldsymbol{c = na}$ alors $\boldsymbol{kb + rc = kma + nra = (km + nr)a}$. □

Théorème

(Division euclidienne).
Soit $\boldsymbol{a, b} \in \mathbb{Z}$, *et* $\boldsymbol{b > 0}$. *Alors il existe* $\boldsymbol{m,n} \in \mathbb{Z}$ *uniques, tels que*

$$\boldsymbol{a = bm + n}, \qquad \text{et} \qquad \boldsymbol{0 \leqslant n \leqslant b - 1.}$$

$\boldsymbol{a}$ *est divisible par* $\boldsymbol{b}$ *si et seulement si* $\boldsymbol{n = 0}$.

$\boldsymbol{m}$ *est appelé le quotient et* $\boldsymbol{n}$ *est appelé le reste de la division euclidienne de* $\boldsymbol{a}$ *par* $\boldsymbol{b}$.

Démonstration.
Démontrons d'abord que les nombres n, m existent. On va supposer qu $a \geqslant 0$, et on va procéder par récurrence sur a.

Initialisation. Si $a = 0$ alors $a = 0 \cdot b + 0$.

Hérédité. Supposons que l'on a démontré le théorème pour a et démontrons le pour $a + 1$. On a

$$a = bm + n \quad \text{où} \quad 0 \leqslant n \leqslant b - 1.$$

Supposons d'abord que $n < b - 1$. Alors $a + 1 = bm + (n + 1)$ où $n + 1 < b$, et on a obtenu la division euclidienne de $a + 1$ par b.

Dans le cas $n = b - 1$ nous avons $a + 1 = bm + n + 1 = b(m + 1)$ et la division euclidienne est faite (le reste est égal à 0).

Exercice

Faites le cas $a < 0$.

Démontrons maintenant que les nombres n, m sont uniques. Supposons qu'il en existe deux couples (n, m) et (n', m') vérifiant la conclusion du théorème. On a alors

$$a = bm + n = bm' + n', \text{ et } b(m - m') = n' - n.$$

Supposons que $m \neq m'$ alors $n \neq n'$ et et $(n' - n) \vdots b$. Cela implique $| n' - n | \geqslant b$, ce qui est impossible car $0 \leqslant n, n' \leqslant b - 1$. Donc en fait $m = m'$ et $n' - n = b(m - m') = 0$. □

Exemples

1) $10 = 2 \times 4 + 2$. 2) $500 = 16 \times 30 + 20$ (Calculez!)

Définition

Soit a, $b \neq 0 \in \mathbb{Z}$. Le nombre maximal positif qui divise a et b est appelé *le plus grand commun diviseur* de a et b, noté $\operatorname{pgcd}(a, b)$ ou $a \wedge b$.

Si $\operatorname{pgcd}(a, b) = 1$, on dit que a et b sont *premiers entre eux*.

Exemples

1) $\mathrm{pgcd}\ (\mathbf{2},\mathbf{3}) = \mathbf{1}$. 2) $\mathrm{pgcd}\ (\mathbf{5},\mathbf{10}) = \mathbf{5}$
3) Quelques soient des nombres positifs $\boldsymbol{a}$, $\boldsymbol{m}$ on a
$\mathrm{pgcd}\ (\boldsymbol{a},\boldsymbol{am}) = \boldsymbol{a}$.
En effet, $\boldsymbol{a}$ est évidemment un diviseur commun de $\boldsymbol{a}$ et $\boldsymbol{am}$. Tout diviseur $\boldsymbol{d}$ de $\boldsymbol{a}$ vérifie $\boldsymbol{d} \leqslant \boldsymbol{a}$ donc $\boldsymbol{a}$ est bien le plus grand commun diviseur de $\boldsymbol{a}$ et $\boldsymbol{am}$.

Lemme

Soit $\boldsymbol{a} = \boldsymbol{bx} + \boldsymbol{c}$, $(\boldsymbol{a},\boldsymbol{x},\boldsymbol{b},\boldsymbol{c} \in \mathbb{Z})$. *Alors* $\mathrm{pgcd}\ (\boldsymbol{a},\boldsymbol{x}) = \mathrm{pgcd}\ (\boldsymbol{x},\boldsymbol{c})$.

Démonstration. Soit $\boldsymbol{d} = \mathrm{pgcd}\ (\boldsymbol{a},\boldsymbol{x})$ alors $\boldsymbol{d} \mid \boldsymbol{a}$, $\boldsymbol{d} \mid \boldsymbol{x}$, donc $\boldsymbol{d} \mid (\boldsymbol{a} - \boldsymbol{bx})$, et $\boldsymbol{d} \mid \boldsymbol{c}$. Cela veut dire que $\boldsymbol{d}$ divise $\boldsymbol{x}$ et $\boldsymbol{c}$, donc $\boldsymbol{d} \leqslant \mathrm{pgcd}\ (\boldsymbol{c},\boldsymbol{x})$. Notons $\boldsymbol{d}' = \mathrm{pgcd}\ (\boldsymbol{c},\boldsymbol{x})$; on vient de démontrer que $\boldsymbol{d} \leqslant \boldsymbol{d'}$. On a $\boldsymbol{d}' \mid \boldsymbol{x}$ et $\boldsymbol{d}' \mid \boldsymbol{c}$, donc $\boldsymbol{d}' \mid (\boldsymbol{bx} + \boldsymbol{c})$, d'où $\boldsymbol{d}' \mid \boldsymbol{a}$ et $\boldsymbol{d}' \leqslant \mathrm{pgcd}\ (\boldsymbol{a},\boldsymbol{x}) = \boldsymbol{d}$.
Alors $\boldsymbol{d'} \leqslant \boldsymbol{d}$ et $\boldsymbol{d} \leqslant \boldsymbol{d'}$, ce qui implique $\boldsymbol{d} = \boldsymbol{d'}$. □

Exemple

$\text{pgcd}\ (\mathbf{200}, \mathbf{201}) = \mathbf{1}$, car $\mathbf{201} = \mathbf{1} \cdot \mathbf{200} + \mathbf{1}$, donc
$\text{pgcd}\ (\mathbf{200}, \mathbf{201}) = \text{pgcd}\ (\mathbf{200}, \mathbf{1}) = \mathbf{1}$.

Il existe un moyen efficace et universel pour trouver le pgcd de deux entiers a, b, notamment:

Algorithme d'Euclide.

Soit a, b des entiers positifs. On recherche $\mathrm{pgcd}\ (a, b)$. Posons $a_0 = a$, $a_1 = b$.
1) On effectue la division euclidienne de a_0 par a_1:

$$a_0 = a_1 b_1 + a_2, \quad 0 \leqslant a_2 < a_1.$$

Si $a_2 = 0$, on dit que la procédure est terminée et on pose $R = a_1$. Si $a_2 \neq 0$ on passe à l'étape 2).

2) On effectue la division euclidienne de a_1 par a_2:

$$a_1 = a_2 b_2 + a_3, \quad 0 \leqslant a_3 < a_2.$$

Si $a_3 = 0$, on dit que la procédure est terminée, et on pose $R = a_2$. Si $a_3 \neq 0$ on passe à l'étape 3). Et ainsi de suite... . . . . .

A l'étape numéro n on effectue la division euclidienne de a_{n-1} par a_n:

$$a_{n-1} = a_n b_n + a_{n+1}, \quad 0 \leqslant a_{n+1} < a_n.$$

Si $a_{n+1} = 0$, on dit que la procédure est terminée, et on pose $R = a_n$.
Si $a_{n+1} \neq 0$ on continue en divisant a_n par a_{n+1}.
.....
.....

Remarquons que la procédure va terminer à un moment car $a_1 > a_2 > \ldots > a_n > \ldots$, et a_i sont des entiers positifs, donc pour certain k on aura $a_{k+1} = 0$, c'est-à-dire

$$a_{k-1} = b_k a_k.$$

A cet étape-la on aura le nombre entier positif $R = a_k$.

Proposition

$R = \text{pgcd}\ (a, b)$.

Démonstration. On va montrer que

$$\text{pgcd}\ (a_{n-1}, a_n) = \text{pgcd}\ (a_0, a_1) \qquad (*)$$

par récurrence sur n.
Initialisation. $n = 1$. $a_{n-1} = a_0, a_n = a_1$; rien à démontrer.

Hérédité. Supposons que l'on a démontré $(*)$ au rang n et on va le faire au rang $n + 1$.

Observons que $a_{n-1} = a_n b_n + a_{n+1}$ et par le lemme qu'on a démontré juste avant la proposition on a

$$\text{pgcd}\ (a_{n-1}, a_n) = \text{pgcd}\ (a_n, a_{n+1})$$

et par l'hypothèse de récurrence on conclut que
$\text{pgcd}\ (a_{n+1}, a_n) = \text{pgcd}\ (a, b)$.

Au dernier étape de l'algorithme on a $a_{k+1} = 0$ et donc $a_{k-1} \vdots a_k$.

On obtient $\text{pgcd}\ (a_{k-1}, a_k) = \text{pgcd}\ (a, b)$. Or $a_{k-1} \vdots a_k$ donc $\text{pgcd}\ (a_{k-1}, a_k) = a_k = R$. Alors $R = \text{pgcd}\ (a, b)$ et la proposition est démontrée. □

Exemple

$a = a_0 = 262$, $b = a_1 = 230$,
$262 = 1 \times 230 + 32$,
$230 = 7 \times 32 + 6$,
$32 = 5 \times 6 + 2$,
$6 = 3 \times 2$.
$\text{pgcd}\ = (262, 230) = 2$.

2. Théorèmes de Gauss et de Bézout.

Théorème

(Théorème de Bézout.) Soient a, b *des entiers relatifs non-nuls, notons* d *leur* pgcd *. Alors il existe* $m, n \in \mathbb{Z}$ *tels que* $d = am + bn$.

Démonstration. $\mathrm{pgcd}\ (a, b)$ peut être calculé à l'aide de l'algorithme d'Euclide. En appliquant cet algorithme, on obtient une suite des nombres posiifs $a_0 = a,\ a_1 = b,\ a_2,\ \ldots,\ a_k$ dont le dernier terme a_k est égal à d. Pour chaque j le nombre a_{j+1} est le reste de la division euclidienne de a_j par a_{j+1}:

$$a_j = b_j a_{j+1} + a_{j+2} \quad \text{et} \quad 0 \leqslant a_{j+2} < a_{j+1}.$$

On va montrer par récurrence que chaque terme a_j de la suite est une combinaison linéaire de a et b aux coefficients entiers.
Initialisation. $a_0 = a,\ a_1 = b$ il n'y a rien à démontrer.

Hérédité. Supposons que notre assertion est vraie au rang $\leqslant k$, c'est-à-dire pour chaque $j \leqslant k$ on a $a_j = am_j + bn_j$ où $m_j, n_j \in \mathbb{Z}$.

Alors $a_{j-1} = b_j a_j + a_{j+1}$ donc

$$a_{j+1} = a_{j-1} - b_j a_j = am_{j-1} + bn_{j-1} - (am_j + bn_j)b_j = a(m_{j-1} - m_j b_j) + b(n_{j-1} - n_j b_j),$$

et l'hérédité est établie.
Alors le pgcd de a, b qui est le dernier terme de notre suite, lui aussi est une combinaison linéaire de a et b. □

Corollaire

Si $c \mid a$ et $c \mid b$ alors $c \mid \operatorname{pgcd}(a, b)$.

Démonstration.
$\operatorname{pgcd}(a, b) = am + bn$;
si $c \mid a$ et $c \mid b$ alors $c \mid (am + bn)$. □

Corollaire

$\mathrm{pgcd}\ (a, b) = 1$ *si et seulement s'il existe* $x, y \in \mathbb{Z}$ *tels que* $ax + by = 1$.

Démonstration. Si $\mathrm{pgcd}\ (a, b) = 1$ alors $\exists x, y \in \mathbb{Z}$ tels que $ax + by = 1$, c'est le contenu du théorème de Bézout.
Supposons maintenant qu'il existe x, y tels que $ax + by = 1$. Soit $d = \mathrm{pgcd}\ (a, b)$ alors $d \mid a$, $d \mid b$. On en déduit que $d \mid (ax + by)$ donc $d \mid 1$ et $d = 1$. □

Corollaire

(Théorème de Gauss). Si $p \mid ab$ *et* $\mathrm{pgcd}\ (p, a) = 1$ *alors* $p \mid b$.

Démonstration. Il existe x, y tels que $px + ay = 1$, donc $pxb + ayb = b$. Or $p \mid pxb$ et $p \mid ab$ donc $p \mid (pxb + ayb)$; cela veut dire $p \mid b$. □

Corollaire

Soit $a \mid x$, $b \mid x$. *Supposons que* a, b *sont premiers entre eux. Alors* $ab \mid x$.

Démonstration. Soit $x = ay = bz$. Alors $a \mid bz$ et par le théorème de Gauss on a $a \mid z$, car a et b sont premiers entre eux.
Donc $z = at$ et $x = bz = bat$. □

Exercice

Soit $\operatorname{pgcd}(a, b) = ax + by$. Démontrer, que $\operatorname{pgcd}(x, y) = 1$.

Définition

Soient $a \neq 0$, $b \neq 0 \in \mathbb{Z}$. Le nombre positif minimal m tel que $a \mid m$, $b \mid m$ est appelé *le plus petit commun multiple de* a, b, noté $\operatorname{ppcm}(a, b)$ ou encore $a \vee b$.

Exemple

$\text{ppcm}\ (4, 10) = 20$

Exercice

Montrer que $\text{ppcm}\ (ad, bd) = d \cdot \text{ppcm}\ (a, b)$.

Proposition

Soit $a > 0$, $b > 0$. *Alors* $\text{ppcm}\ (a, b) = \frac{a \cdot b}{\text{pgcd}\ (a,b)}$.

Démonstration. **1.** Supposons d'abord que $\text{pgcd}\ (a, b) = 1$. Dans ce cas-là il faut démontrer que $\text{ppcm}\ (a, b) = ab$.
ab est un commun multiple de a et de b donc $ab \geqslant \text{ppcm}\ (a, b)$.
Par définition $\text{ppcm}\ (a, b)$ est divisible par a et par b. Vu que a et b sont premiers entre eux, $\text{ppcm}\ (a, b)$ est divisible par ab, ce qui implique $\text{ppcm}\ (a, b) \geqslant ab$. Alors $\text{ppcm}\ (a, b) = ab$.

2. Maintenant soit $\text{pgcd}\ (a,b) = d \neq 1$. On a alors $a = a'd,\ b = b'd$. Remarquons que $\text{pgcd}\ (a',b') = 1$.
En effet, on a $ax + by = d$, donc $a'dx + b'dy = d$, et $a'x + b'y = 1$.
On a déjà démontré que cela implique $\text{pgcd}\ (a',b') = 1$.
Selon le point 1. ci-dessus, on déduit $\text{ppcm}\ (a',b') = a'b'$.
Il reste à remarquer que

$$\text{ppcm}\ (a,b) = d \cdot \text{ppcm}\ (a',b') = da'b' = \frac{(da')(db')}{d} = \frac{ab}{d}.$$

□

Exemple

$$\text{ppcm}\ (4,6) = 12 = 24/\text{pgcd}\ (4,6).$$

Définition

Soit $a_1, ..., a_m$ des nombres entiers relatifs non-nuls. Un nombre entier positif maximal d tel que $d \mid a_1$, $d \mid a_2$,..., $d \mid a_m$ est appelé *le plus grand commun diviseur des nombres* $a_1, ..., a_m$ et noté $\operatorname{pgcd}(a_1, ..., a_m)$.

Exercice

Montrer qu'il existe des nombres entiers $x_1, ..., x_m \in \mathbb{Z}$ tels que $\operatorname{pgcd}(a_1, ..., a_m) = a_1x_1 + ... + a_mx_m$.

Définition

Soit $a_1, ..., a_m \in \mathbb{Z}$. Le nombre positif minimal k tel que $a_i \mid k$ pour chaque i est appelé *le plus petit commun multiple des nombres* $a_1, ..., a_m$ et noté $\operatorname{ppcm}(a_1, ..., a_m)$.

Exercice

Est-ce que $\operatorname{ppcm}(a_1, ..., a_m) = \frac{a_1 \cdot a_2 \cdot ... \cdot a_m}{\operatorname{pgcd}(a_1, ..., a_m)}$?

3. Nombres premiers

Définition

Un nombre entier positif $\boldsymbol{p} > \mathbf{1}$ est dit *premier* s'il n'a pas de diviseurs entiers positif sauf 1 et $\boldsymbol{p}$.

Exemples

$\mathbf{2}$ est premier,
$\mathbf{6} = \mathbf{2} \cdot \mathbf{3}$ n'est pas premier,
$\mathbf{5}, \mathbf{7}, \mathbf{11}, \mathbf{13}$ sont premiers.

Proposition

Soit p un nombre premier, et n un nombre entier. Alors $p|n$ ou bien $\mathrm{pgcd}\ (p,n) = 1$.

Démonstration. Soit $k = \mathrm{pgcd}\ (p,n)$. Alors $k|p$ ce qui ne laisse que deux possibilités: $k = 1$ ou $k = p$. Dans le premier cas $\mathrm{pgcd}\ (p,n) = 1$, dans le deuxième cas $p|n$. □

Proposition

Soit p un nombre premier, et a, b des nombres entiers relatifs, tels que $p|ab$. Alors $p|a$ ou $p|b$.

Démonstration. Si $p \nmid a$ alors par la proposition précédente on a $\mathrm{pgcd}\ (p,a) = 1$. On en déduit par le théorème de Gauss que $p|b$. □

Remarque

Si p n'est pas premier, l'énoncé précédent n'est pas valide. Par exemple, $4|6 \cdot 2$ or $4 \nmid 2$ et $4 \nmid 6$.

Proposition

Soit $n > 1$. Alors il y a au moins un nombre premier p tel que $p \mid n$.

Démonstration.
Si n est premier, alors l'assertion est évidente car $n \mid n$.

Si n n'est pas premier alors n admet au moins un diviseur positif d tel que $1 < d < n$. Soit d_0 le *minimal* diviseur positif de n tel que $d_0 > 1$. Alors d_0 est premier.
(En effet, si d_0 n'est pas premier, alors $d_0 = d_1 d_2$ où $1 < d_1, d_2 < d_0$. Or $d_1 \mid n$, $d_2 \mid n$, ce qui contrédit la minimalité de d_0). On a donc trouvé un diviseur premier de n, notamment d_0. □

Proposition

L'ensemble des nombres premiers est infini.

Démonstration.
Supposons que l'ensemble P des nombres premiers est fini, $P = \{p_1, ..., p_k\}$ avec $p_1 < p_2 < ... < p_k$.
Soit $N = 1 + p_1 \cdot ... \cdot p_k$. Alors selon la proposition précédente N admet un diviseur premier, donc il existe i tel que $p_i \mid N$.
Or p_i divise le produit de tous les nombres $p_1, ..., p_k$, c'est-à-dire $p_i \mid (p_1 \cdot ... \cdot p_k)$ donc $p_i \mid (N - p_1 \cdot ... \cdot p_k)$ ce qui veut dire $p_i \mid 1$, et c'est impossible car un nombre premier est par définition > 1. Alors notre hypothèse que l'ensemble des nombres premiers est fini est fausse. □

Le théorème suivant est assez important, on l'appelle des fois *le théorème principal d'arithmétique*.

Théorème

(Décomposition en facteurs premiers.)
1) soit $n \in \mathbb{N}$, $n > 1$. *Alors il existe des nombres premiers* $p_1, \ldots, p_k$ *tel que*

$$n = p_1 p_2 \ldots p_k . \qquad (*)$$

2) La représentation $(*)$ *est unique à permutation près.*

Exemple

$200 = 2 \times 100 = 2 \times 2 \times 50 = 2 \times 2 \times 2 \times 5 \times 5$
on peut aussi permuter les termes dans le produit:
$200 = 5 \times 2 \times 2 \times 2 \times 5$.

Démonstration.
(1) On va d'abord démontrer qu'une présentation $(*)$ existe. On fait la récurrence sur n.

Initialisation. $n = 2$, alors n est premier lui-même et il n'y a rien à démontrer.
Hérédité. On suppose que le théorème est démontré pour tous les nombres strictment inférieurs à n et on va faire la démonstration pour n.

On peut supposer que n n'est pas premier, il admet donc un diviseur d tel que $1 < d < n$. On a $n = d \cdot c$ et $1 < c < n$.

Par l'hypothèse de récurrence le théorème est vrai pour d et c donc $d = p_1 \cdot \ldots \cdot p_k$ et $c = p_{k+1} \cdot \ldots \cdot p_r$ où tous les nombres p_i sont premiers;

alors $n = cd = p_1 \cdot \ldots \cdot p_r$.

(2) Maintenant on va démontrer l'unicité de la présentation $(*)$.

Lemme

Soit $p, r_1, \ldots, r_s$ des nombres premiers tel que $p \mid r_1 r_2 \ldots r_s$.
Alors il existe i tel que $p = r_i$.

Démonstration.
Récurrence sur s.
$s = 1$: puisque $p | r_1$ et r_1 est premier, on a alors $p = r_1$.

$s \rightsquigarrow s + 1$

Soit $p \mid r_1 \ldots r_{s+1}$. On note $R = r_2 r_3 \ldots r_{s+1}$ alors $p \mid r_1 \cdot R$.
p étant premier on a $p \mid r_1$ ou bien $p \mid R$. Dans le premier cas $p = r_1$ et la démonstration est terminée.
Dans le deuxième cas, $p \mid R$ on a $p \mid r_2 r_3 \ldots r_{s+1}$ et l'hypothèse de récurrence implique que $p = r_i$ pour un nombre i entre 2 et $s + 1$. Le lemme est démontré. □

Procédons à la démonstration du théorème. Soit

$$n = p_1 \ldots p_k = r_1 \ldots r_s$$

deux décompositions en facteurs premiers du même nombre n. On va démontrer que $k = s$ et que quitte à permuter les nombres r_j on a $p_i = r_i$ pour chaque i. On procède par récurrence sur k.
Initialisation. Si $k = 1$ alors $p_1 = r_1 r_2 \ldots r_s$. Puisque p_1 est premier cela est possible uniquement si $s = 1$, et on a $p_1 = r_1$.

Hérédité. Le nombre premier p_1 divise le produit des nombres r_i, donc selon le Lemme il existe i tel que $p_1 = r_i$. Quitte à permuter les r_i, on peut supposer que $p_1 = r_1$ donc $p_1 p_2 \ldots p_k = p_1 r_2 \ldots r_s$ d'où $p_2 p_3 \ldots p_k = r_2 r_3 \ldots r_s$.
Le produit à gauche contient $k - 1$ facteurs, donc on peut appliquer l'hypothèse de récurrence et conclure que $k - 1 = s - 1$ et quitte à permuter les nombres r_j on a $p_i = r_i$ si $i \geqslant 2$.

Le théorème est démontré. □

Voici une autre version du même théorème (la démonstration sera omise.)

Théorème

Soit $n > 1$. *Alors il existe des nombres premiers* $p_1 < p_2 < \ldots < p_k$ *et des entiers strictement positifs* $r_1, r_2, \ldots, r_k$ *tel que*

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k}.$$

Cette présentation est unique.

Exemple

$200 = 2^3 5^2$.

Proposition

Soit p *un nombre premier et* $0 < n < p$.
Alors $C_p^n = \frac{p!}{n!(p-n)!}$ *est divisible par* p.

Démonstration. On a

$$p! = C_p^n \cdot n! \cdot (p-n)!$$

Le nombre p divise évidemment $p!$. Vu le théorème de Gauss il nous suffit de démontrer que

$$\text{pgcd}\ (p, n!) = \text{pgcd}\ \Big(p, (p-n)!\Big) = 1$$

Montrons par exemple que p et $n!$ sont premiers entre eux. Quel que soit un nombre $x < p$ on a $\text{pgcd}\ (x, p) = 1$, puisque p n'est divisible par aucun nombre entier positif apart lui-même et 1.
Par le théorème de Gauss on déduit que p et $n! = 1 \cdot 2 \cdot \ldots \cdot n$ sont premiers entre eux. De la même façon on montre que $\text{pgcd}\ (p, (p-n)!) = 1$, et notre proposition est démontrée. □

La proposition suivante a été découverte en Gréce antique.

Proposition

Soit p un nombre premier, alors $\sqrt{p}$ est irrationnel.

Démonstration. Supposons que $\sqrt{p}$ est un nombre rationnel: $\sqrt{p} = \frac{m}{n}, n > 0,\ m > 0$. En simplifiant la fraction si nécessaire, on peut toujours supposer que m et n sont premiers entre eux.

On a $p \cdot n^2 = m^2$, donc p divise m^2, et par le théorème de Gauss, p divise m; soit $m = p \cdot m'$.

On a donc $p \cdot n^2 = p^2 \cdot (m')^2$, ce qui implique $p \mid n^2$; on en déduit que $p \mid n$. C'est impossible car p divise m et $\mathrm{pgcd}\ (m, n) = 1$.

Notre hypothèse n'était donc pas correcte, et $\sqrt{p}$ n'est pas un nombre rationnel. □

Exercice

Démontrer la généralisation de la proposition précédente:

Soit n *un nombre entier positif, tel que* $n = m^2$*, où* m *est un nombre rationnel. Alors* m *est un nombre entier.*

Proposition

Soit n *non premier.*
Alors il existe p *premier tel que* $p \mid n$ *et* $p \leqslant \sqrt{n}$.

Démonstration. Il existe un diviseur d de n, tel que $1 < d < n$. Si $d \leqslant \sqrt{n}$, alors tout diviseur premier de d vérifie la conclusion de la proposition.
Si $d > \sqrt{n}$, alors $\frac{n}{d} < \frac{n}{\sqrt{n}} = \sqrt{n}$;

or $\frac{n}{d}$ lui aussi est un diviseur de n. On lui applique le raisonnement précédent. □

Cette proposition est souvent utilisée pour démontrer qu'un nombre donné est premier. Par exemple pour démontrer que **61** est premier il suffit de vérifier que **61** n'est pas divisible par les entiers premiers entre 1 et 7, c'est-à-dire 3,5,7 (car $\mathbf{8^2 = 64}$).

4.Congruences

Définition

Soit $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{n} \in \mathbb{Z}, \boldsymbol{n} \neq \mathbf{0}$. On dit que $\boldsymbol{a}, \boldsymbol{b}$, sont *congrus modulo* $\boldsymbol{n}$ si $\boldsymbol{a} - \boldsymbol{b}$ est divisible par $\boldsymbol{n}$. On écrit $\boldsymbol{a} \equiv \boldsymbol{b}\ (\boldsymbol{n})$ ou $\boldsymbol{a} \equiv \boldsymbol{b}\ \boldsymbol{mod}(\boldsymbol{n})$. La relation $\equiv$ est appelée *relation de congruence*.

Voici les propriétés de la relation de congruence.

Proposition

1) $\boldsymbol{a} \equiv \boldsymbol{a}(\boldsymbol{n})$ *(réflexivité).*
2) Si $\boldsymbol{a} \equiv \boldsymbol{b}(\boldsymbol{n})$ *alors* $\boldsymbol{b} \equiv \boldsymbol{a}(\boldsymbol{n})$ *(symétricité).*
3) Si $\boldsymbol{a} \equiv \boldsymbol{b}(\boldsymbol{n})$ *et* $\boldsymbol{b} \equiv \boldsymbol{c}(\boldsymbol{n})$ *alors* $\boldsymbol{a} \equiv \boldsymbol{c}(\boldsymbol{n})$ *(transitivité).*

Démonstration. On ne fera que le point 3 en laissant 1 et 2 pour exercice. Si $\boldsymbol{a} - \boldsymbol{b} = \boldsymbol{nk}$, $\boldsymbol{b} - \boldsymbol{c} = \boldsymbol{nm}$ alors
$\boldsymbol{a} - \boldsymbol{c} = (\boldsymbol{a} - \boldsymbol{b}) + (\boldsymbol{b} - \boldsymbol{c}) = \boldsymbol{nk} + \boldsymbol{nm} = \boldsymbol{n}(\boldsymbol{k} + \boldsymbol{m})$. □

Proposition

Si $a \equiv b\ (n)$, $c \equiv d\ (n)$ *alors:*
1) $a + c \equiv b + d\ (n)$.
2) $ac \equiv bd\ (n)$.

Démonstration. 1) On a $a - b = nk$, et $c - d = nm$. Alors $(a + c) - (b + d) = n(k + m)$ donc $a + c \equiv b + d\ (n)$.

2) On a $ac = (b + nk)(d + nm) = bd + nkd + mnb + n^2mk$ donc $ac \equiv bd\,(n)$. □

Exemples

1) *Chaque nombre entier positif* n *est congru* **mod 3** *à la somme des chiffres de son écriture décimale.*

En effet, soit $n = a_k a_{k-1} \ldots a_0$ l'écriture décimale d'un nombre n, où $0 \leqslant a_i \leqslant 9$. Cela veut dire

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_0.$$

(Par exemple $231 = 2 \cdot 10^2 + 3 \cdot 10^1 + 1 \cdot 10^0$.)
Or $1 \equiv 1 \quad (3)$, $\quad 10 \equiv 1\ (3)$, $\quad 10^2 \equiv 1^2\ (3)$, . . . , $10^k \equiv 1\ (3)$ pour tout k.
Donc $n \equiv a_k + a_{k-1} + \ldots + a_0\ (3)$.
Cela veut dire en particulier qu'un nombre est divisible par **3** si et seulement si la somme des chiffres de son écriture décimale est divisible par **3**.

2) *Chaque nombre entier positif* n *est congru modulo* **11** *à la somme alternée des chiffres de son écriture décimale*,
c'est-à-dire si $n = a_k a_{k-1} \ldots a_0$ on a

$$n \equiv a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^k a_k \ (11).$$

En effet, $n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_0$ et
$1 \equiv 1(11)$,
$10 \equiv -1(11)$,
$100 = 10^2 \equiv (-1) \times (-1) = 1(11)$,
.....
.....
$10^k \equiv (-1)^k (11)$ pour tout k.
donc $n \equiv a_k (-1)^k + a_{k-1}(-1)^{k-1} + \ldots + a_0 \quad (11).$

Exercice

Etablir les critères de divisibilité par 9 et par 4.

Relations d'équivalence

Définition

Soit A un ensemble. Un sous-ensemble R de $A \times A$ est appelé *relation*, ou *relation binaire*.

Exemples

$A = \mathbb{Z}$, $R = \{(x, y) \mid x \leqslant y\}$ = relation d'ordre.
$A = \mathbb{Z}$, $R = \{(x, y) \mid x \equiv y (n)\}$ = relation de congruence.
A un ensemble quelconque, $R = \{(x, y) \mid x = y\}$ = relation d'égalité.

Définition

On dit que R est une *relation d'équivalence* si
1) $(x, x) \in R$ pour chaque $x \in A$,
2) si $(x, y) \in R$ alors $(y, x) \in R$,
3) si $(x, y) \in R$ et $(y, z) \in R$ alors $(x, z) \in R$.

Pour une relation d'équivalence R, on écrit souvent $x \sim y$ au lieu de $(x, y) \in R$.
Alors les propriétés 1) – 3) s'écrivent comme suit:
1) $x \sim x$ (réflexivité).
2) $(x \sim y) \Longrightarrow (y \sim x)$ (symétricité).
3) $(x \sim y)$ & $(y \sim z) \Longrightarrow x \sim z$ (transitivité).

Exemples

1) La relation d'ordre sur l'ensemble des entiers relatifs
$A = \mathbb{Z}, \quad R = \{(x, y) \mid x \leqslant y\}$
est réflexive $(x \leqslant x)$ et transitive car $(x \leqslant y)$ &$(y \leqslant z) \Longrightarrow (x \leqslant z)$.
Mais R n'est pas symétrique parce que $(x \leqslant y) \not\Rightarrow (y \leqslant x)$,
donc R n'est pas une relation d'équivalence.

2) La relation d'égalité:
$(x, y) \in R$ si et seulement si $x = y$
est évidemment une relation d'équivalence.

3) La relation de congruence modulo n est une relation d'équivalence sur l'ensemble $\mathbb{Z}$ (nous avons déjà vérifié les propriétés de reflexivité, symétricité et transitivité pour cette relation).

Etant donné un ensemble A et une relation d'équivalence R sur A nous allons maintenant construire un autre ensemble appelé *l'ensemble quotient de* A *par* R.

Définition

Soit A un ensemble, R une relation d'équivalence. Soit $x \in A$. L'ensemble de tous les $y \in A$ tels que $y \sim x$ est appelé *la classe d'équivalence de* x et noté $[x]$ ou $C_x = \{y \in A \mid y \sim x\}$.

Proposition

1) Pour chaque $x \in A$*, sa classe d'équivalence* C_x *n'est pas un ensemble vide.*
2) La réunion de toutes les classes d'équivalence est égale à A*.*
3) Si $x, y \in A$ *alors* $C_x \cap C_y = \emptyset$ *ou bien* $C_x = C_y$*.*

Démonstration. 1) $x \sim x$ donc $x \in C_x$ et $C_x \neq \emptyset$.
2) Chaque x est dans sa classe d'équivalence C_x donc la réunion de toutes les classes d'équivalence est bien A.
3) Deux cas sont possibles:

a) $x \sim y$.

Dans ce cas $C_x \subset C_y$. En effet, si $z \in C_x$ alors $z \sim x$ et puisque $x \sim y$ on a $z \sim y$ (par transitivité) donc $z \in C_y$. Le même argument montre que $C_y \subset C_x$. Donc $C_x = C_y$.

b) $x \nsim y$.

Dans ce cas $C_x \cap C_y = \varnothing$. En effet, si $z \in C_x$ et $z \in C_y$ alors $z \sim x$ et $z \sim y$ donc $x \sim y$ (par transitivité). Cela contrédit a notre hypothèse $x \nsim y$, donc les deux sous-ensembles C_x, C_y n'ont pas d'éléments communs.

La proposition est démontrée. □

On obtient donc une présentation de A comme réunion des sous-ensembles qui ne s'intersectent pas l'un avec l'autre.
Une telle réunion est appelée *réunion disjointe*, et une telle présentation est dite *une partition de* A.

Définition

Soit A un ensemble, R une relation d'équivalence sur A. L'ensemble des classes d'équivalence modulo R est appelé *l'ensemble quotient de* A *modulo* R et noté A/R, ou $A/\sim$.

Exemples

1) Deux points sont équivalents s'ils sont de même couleur. (faire le dessin!)
On a 3 classes d'équivalence chacune comportant 3 éléments:
$A/\sim$ c'est l'ensemble des couleurs; $\mathrm{card}\ (A/\sim) = 3$.

2) Soit A un ensemble $R = \{(x, x) \mid x \in A\}$ c'est-à-dire $x \sim y \iff x = y$.
Pour chaque x il y a un seul élément équivalent à x, notamment lui-même. Donc $C_x = [x] = \{x\}$ et A/R est l'ensemble des sous-ensembles de A de cardinalité **1**, il est en bijection naturelle avec A.

3) $A = \mathbb{Z}$, $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y(n)\}$ (la relation de congruence modulo n).
Considérons d'abord le cas le plus simple: $n = 2$. Deux nombres entiers x, y sont équivalents si et seulement si $x - y$ est divisible par **2**. C'est-à-dire les deux sont pairs ou les deux sont impairs. Donc on a deux classes d'équivalence.
La première classe contient tous les nombres pairs. Ils sont tous équivalents à **0**.
La deuxième classe contient tous les nombres impairs. Ils sont tous équivalents à **1**.
L'ensemble $\mathbb{Z}/\sim$ contient donc deux éléments: **[0]** et **[1]**.

Pour un entier positif $n \geqslant 2$, il y a n classes d'équivalence, comme dit la proposition suivante.

Proposition

Soit $n > 1$. Chaque $x \in \mathbb{Z}$ est congru modulo n à un unique nombre dans $[[0, n-1]] = \{0, 1, ..., n-1\}$.

Démonstration. La proposition dit que chaque $x \in \mathbb{Z}$ s'écrit

$$x = r + kn \text{ où } \quad 0 \leqslant r \leqslant n-1$$

et le nombre r est unique.
Cela découle immédiatement du théorème sur la division euclidienne.
□

Définition

L'ensemble quotient $\mathbb{Z}/\sim = \left\{[0], [1], ..., [n-1]\right\}$ est noté $\mathbb{Z}/n\mathbb{Z}$.

Théorème chinois des restes.

Le théorème suivant a été découvert en Chine il y a au moins 1000 ans.

Théorème

Soit $n, k \in \mathbb{N}_*$ des nombres premiers entre eux. Soit $a, b \in \mathbb{Z}$. Alors il existe $x \in \mathbb{Z}$ tel que $x \equiv a\ (n)$ et $x \equiv b\ (k)$.

Démonstration.

Par le théorème de Bézout il existe r, s tels que $nr + ks = 1$.
On pose $x = aks + bnr$. Alors

$$x \equiv aks\ (n) \equiv a(1 - nr)\ (n) \equiv a\ (n)$$

et

$$x \equiv bnr\ (k) \equiv b(1 - ks)\ (k) \equiv b\ (k).$$

□

Petit théoréme de Fermat

Le théorème suivant a été découvert par Pierre de Fermat en 1640.

Théorème

Soit p un nombre premier et $x \in \mathbb{Z}$. Alors $x^p \equiv x\,(p)$.

Démonstration. Supposons d'abord que x est positif et démontrons le théorème par récurrence sur x.
1) $x = 1$, alors $x^p = x$ quelque soit p, donc notre assertion est vraie.

2) $x \rightsquigarrow x + 1$

Par la formule du binôme de Newton on obtient:

$$(x+1)^p = x^p + C_p^{p-1}x^{p-1} + \ldots + C_p^2 x^2 + C_p^1 x + 1.$$

Or $C_p^k \vdots p$ pour $1 \leqslant k \leqslant p-1$ alors $(x+1)^p \equiv x^p + 1\,(p)$.
Rappelons que $x^p \equiv x\,(p)$ par l'hypothèse de récurrence, donc $(x+1)^p \equiv x + 1(p)$, ce qu'il fallait démontrer. □

Exercice

Déduire le petit théorème de Fermat pour $x < 0$.

Corollaire

Soit p un nombre premier, soit $x \in \mathbb{Z}$ tel que $p \nmid x$. Alors $x^{p-1} \equiv 1(p)$.

Démonstration. On vient de démontrer que $x^p - x = x \cdot (x^{p-1} - 1)$ est divisible par p.
Or x et p sont premiers entre eux, donc en fait c'est $x^{p-1} - 1$ qui est divisible par p. □

5. Equations diophantiennes

Une équation dont les coefficients sont entiers, et les solutions recherchées sont aussi les nombres entiers est appelée *une équation diophantienne.*

Voici le premier exemple:
$ax = b$, où a, b sont des nombres entiers, $a \neq 0$.
Ici a, b sont des coefficients, et x est inconnue.
Il est clair que cette équation admet une solution si et seulement si $a \mid b$ auquel cas $x = \frac{b}{a}$.

Voici un exemple plus compliqué:

$$ax + by = c \qquad (*)$$

Ici a, b, c sont des nombres entiers (on suppose que $a \neq 0,\ b \neq 0$) et on cherche les couples (x, y) des nombres entiers vérifiant $(*)$.
On va d'abord traiter le cas $c = 0$. L'équation $(*)$ est appelée *homogène* dans ce cas.
Soit $d = \text{pgcd}\ (a, b)$. On pose $a' = a/d,\ b' = b/d$. Alors a' et b' sont premiers entre eux. L'équation $ax + by = 0$ est équivalente à l'équation

$$a'x + b'y = 0 \qquad (**)$$

Proposition

1) Soit $t \in \mathbb{Z}$. Alors le couple $(x, y) = (b't, -a't)$ est une solution de l'équation $(**)$.
2) Toute solution de $(**)$ s'obtient ainsi.

Démonstration. 1) $a' \cdot (b't) + b' \cdot (-a't) = 0$ donc le couple $(b't, -a't)$ est une solution de $(**)$.
2) Si $a'x + b'y = 0$, alors $b' | a'x$; vu que a' et b' sont premiers entre eux cela implique que $b' | x$. Soit $x = b't$; alors $a'b't + b'y = 0$, d'où $y = -a't$. La proposition est démontrée. □

Maintenant on va considérer l'équation

$$ax + by = c \qquad (*)$$

où $c \neq 0$.

Proposition

Soit $d = \operatorname{pgcd}(a, b)$. *Alors* $(*)$ *a des solutions si et seulement si* $d \mid c$.

Démonstration. 1) Si $(*)$ a des solutions, soit (x, y) une des solutions, alors on a $ax + by = c$. Or $d | ax$ et $d | by$ d'où $d | c$.
2) Si $d | c$, posons $c' = c/d$. Par le théorème de Bézout il existe x, y tels que $ax + by = d$. Alors $a(c'x) + b(c'y) = dc' = c$, donc le couple $(c'x, c'y)$ est une solution de $(*)$. □

Pour trouver une solution de l'équation $(*)$ on peut utiliser l'algorithme d'Euclide.

Exemple

On considère l'équation $262x + 230y = 2$. On a déjà appliqué l'algorithme d'Euclide pour trouver le pgcd de ces deux nombres: $a_0 = 262,\ a_1 = 230$.

$$\begin{aligned} 262 &= 1 \times 230 + 32 & a_0 &= a_1 + a_2; \\ 230 &= 7 \times 32 + 6 & a_1 &= 7a_2 + a_3; \\ 32 &= 5 \times 6 + 2 & a_2 &= 5a_3 + a_4; \\ 6 &= 3 \times 2 & a_3 &= 3a_4; \end{aligned}$$

Le $\mathrm{pgcd}\ (262, 230)$ est donc 2. On peut utiliser cet algorithme aussi pour trouver des solutions de l'équation $262x + 230y = 2$, en exprimant successivement a_i en fonction de a_{i-1} et a_{i-2} (comme on a fait dans la démonstration du théorème de Bézout).

Voici la procédure:

$$a_2 = a_0 - a_1$$

$$a_3 = a_1 - 7a_2 = a_1 + 7(a_1 - a_0) = 8a_1 - 7a_0$$

$$a_4 = a_2 - 5a_3 = a_0 - a_1 - 5(8a_1 - 7a_0) = 36a_0 - 41a_1$$

Il ne reste qu'à substituer $a_0 = 230,\ a_1 = 262, a_4 = 2$:

$36 \times 262 - 41 \times 230 = 2$,

donc on a trouver une solution de notre équation: $(x, y) = (36, -41)$.

Cette méthode permet de trouver une solution d'une équation $ax + by = c \quad (*)$ (si le pgcd de a et b divise c).

La proposition suivante explique comment trouver *toutes les solutions* de $(*)$ à partir d'une solution particulière.

Proposition

Soit (x_0, y_0) une solution de $(*)$. Alors chaque solution de $(*)$ est de la forme $(x_0 + x, y_0 + y)$ où (x, y) est une solution de l'équation homogène $ax + by = 0$.

Démonstration. Soit (X, Y) une solution de $(*)$. Alors $aX + bY = c$. On a aussi $ax_0 + by_0 = c$. D'oú

$$a(X - x_0) + b(Y - y_0) = 0$$

cela veut dire que le couple $(X - x_0, Y - y_0)$ est une solution de l'équation homogène. □

Exemple

Trouvons toutes les solutions de l'équation diophantienne:

$$\mathbf{262}x + \mathbf{230}y = \mathbf{2} \qquad (E)$$

On a trouvé une solution particuliére $(\mathbf{36}, -\mathbf{41})$ de cette équation. Les solutions de l'équation homogène

$$\mathbf{262}x + \mathbf{230}y = \mathbf{0}$$

sont donnée par la formule

$$x = \mathbf{115}t, \qquad y = -\mathbf{131}t$$

donc voici toutes les solutions de l'équation (E):

$$x = \mathbf{36} + \mathbf{115}t, \qquad y = -\mathbf{41} - \mathbf{131}t \qquad \text{où} \qquad t \in \mathbb{Z}$$

On va considérer un exemple d'une équation diophantienne du *second degré*:

$$x^2 + y^2 = z^2 \qquad (*)$$

On cherche les triples (x, y, z) des nombres entiers relatifs vérifiant l'équation $(*)$, un tel triple est appelée *un triple pythagoréen*.
Certaines solutions de cette équation étaient connues par de Babyloniens, et la solution générale et due à Euclide. En divisant par z on obtient l'équation suivante:

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

où $\frac{x}{z}, \frac{y}{z}$ sont de nombres *rationnels*.
Nous allons d'abord résoudre l'équation $u^2 + v^2 = 1$ où $u, v \in \mathbb{Q}$. En fait il s'agit de trouver tous le points sur le cercle unité, dont les deux coordonnées sont rationnelles.
On a 4 solution évidentes $u = \pm 1, v = 0$ et $u = 0, v = \pm 1$. On cherchera des solutions pour lesquelles $u \neq -1$.

(Faire le dessin) Les deux triangles sur le dessin: ABC et $A'B'C'$, sont homothétiques, d'où

$$\frac{v}{1+u} = \frac{t}{1} = t, \quad v = t(1+u)$$

(ici t est un nombre rationnel, et $u \neq -1$). Notre équation donne

$$u^2 + t^2(1+u)^2 = 1, \quad (1+u)^2 t^2 = 1 - u^2$$

en divisant par $1+u$ on aura $(1+u)t^2 = 1-u$ et on trouve u en fonction de t:

$$u(1+t^2) = 1 - t^2, \qquad u = \frac{1-t^2}{1+t^2}$$

En ce qui concerne v on a

$$v = t(1+u) = t\left(1 + \frac{1-t^2}{1+t^2}\right) = \frac{2t}{1+t^2}$$

Donc

$$(u, v) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right) \quad \text{où} \quad t \in \mathbb{Q}.$$

Il est facile à vérifier que chaque couple $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ vérifie l'équation $u^2 + v^2 = 1$, donc en fait on a trouvé toutes les solutions rationnelles de cette équation.

Remarque

La méthode que l'on vient d'utiliser constitue le premier pas vers la *géométrie algébrique*, le domaine des mathématiques qui utilise les techniques géométriques pour résoudre les problèmes algébriques et vice versa.

Revenons maintenant à notre équation du départ:

$$x^2 + y^2 = z^2 \qquad (*),$$

où on cherche des solutions $(x, y, z) \in \mathbb{Z}^3$.
Soit (x, y, z) est une telle solution, alors le couple $(\frac{x}{z}, \frac{y}{z}) \in \mathbb{Q}^2$ vérifie l'équation $u^2 + v^2 = 1$, et on a

$$\frac{x}{z} = \frac{1 - t^2}{1 + t^2}, \quad \frac{y}{z} = \frac{2t}{1 + t^2}.$$

Ici t est un nombre rationnel; $t = \frac{r}{p}$, autrement dit

$$\frac{x}{z} = \frac{p^2 - r^2}{p^2 + r^2}, \qquad \frac{y}{z} = \frac{2pr}{p^2 + r^2},$$

ou encore

$$\begin{cases} x(p^2 + r^2) = z(p^2 - r^2); \\ y(p^2 + r^2) = z(2pr) \end{cases}$$

On peut supposer que p, r sont premiers entre eux.

1^{et} cas: l'un des nombres p, r est pair et l'autre impair.
Remarquons que p et $p^2 + r^2$ sont premiers entre eux. (En effet, supposons qu'il existe d un diviseur premier de p et de $p^2 + r^2$. Alors d divise r^2, et puisque d est premier il divise aussi r. Cela est impossible car p et r sont premiers entre eux.)
De la même façon on montre que $\text{pgcd}\,(r, p^2 + r^2) = 1$.
La deuxième équation dit $y(p^2 + r^2) = 2prz$, donc $p \mid y$, $\quad r \mid y$.
Puisque p et r sont premiers entre eux cela implique
$pr \mid y$, $\quad$ donc $y = kpr$. D'où $k(p^2 + r^2) = 2 \cdot z$.

$p^2 + r^2$ est impair, donc k doit être divisible par 2, soit $k = 2m$ alors $z = m(p^2 + r^2)$. La première équation dit $x(p^2 + r^2) = z(p^2 - r^2)$ donc $x = m(p^2 - r^2)$.
En résumé

$$\begin{cases} x = m(p^2 - r^2); \\ y = 2mpr; \\ z = m(p^2 + r^2). \end{cases}$$

Ceci forme la première classe des solutions de l'équation $x^2 + y^2 = z^2$.

2^{eme} cas: p, r sont tous les deux impairs.
Soit

$$p' = \frac{p+r}{2}, \quad r' = \frac{p-r}{2},$$

alors $p = p' + r', \quad r = r' - p'$

et on aura pour p', r' le système des équations suivant:

$$\frac{x}{z} = \frac{2p'r'}{(p')^2 + (r')^2}, \qquad \frac{y}{z} = \frac{(p')^2 - (r')^2}{(p')^2 + (r')^2}$$

Or l'un des p', r' est impair et l'autre est pair (si ce n'etait pas le cas, alors p et r seraient tous les deux divisible par 2 ce qui est impossible car p et r sont premiers entre eux). En remplaçant (x, y) par (y, x) on revient au premier cas, et on obtient la deuxième famille des solutions de notre équation diophantienne:

$$\begin{cases} x = 2mp'r' \\ y = m(p'^2 - r'^2) \\ z = m(p'^2 + r'^2). \end{cases}$$

(on peut remarquer que ces solutions sont les mêmes que les solutions de la 1ère famille quitte à permuter x et y.)
On a obtenu toutes les solutions de l'équation diophantienne $x^2 + y^2 = z^2$.

Les équations diophantiennes du degré supérieur à deux sont en général plus difficile à résoudre. On peut démontrer que l'équation diophantienne $x^3 + y^3 = z^3$ n'a pas de solution non-triviales (c'est-à-dire les solutions où $x \neq 0, y \neq 0, z \neq 0$), l'argument est beaucoup plus compliqué que la solution de l'équation $x^2 + y^2 = z^2$.

En général, pour $n \geqslant 3$ l'équation diophantienne

$$x^n + y^n = z^n \qquad (**)$$

n'a pas de solution non-triviales non plus. Cela a été annoncé pas Pierre de Fermat, mais il n'a pas donné la preuve. L'équation $(**)$ est devenu l'un des problèmes les plus célèbres des mathématiques sous le nom du *grand théorème de Fermat*. Vers le milieu du 20me siècle le théorème a été démontré pour tous les n inférieur à un million.

La solution finale a éte obtenu par A. Wiles, un mathématicien américain à la fin de XXème siècle. La démonstration complète date de 1995.