

I Division euclidienne

1° Énoncé

Théorème. Soient a et b deux entiers, b non nul. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que

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

Démonstration. On commence par l'unicité. Soient q, r, q', r' quatre entiers tels que $a = bq + r = bq' + r'$, $0 \leq r < |b|$ et $0 \leq r' < |b|$. On en déduit : $-|b| < r - r' < |b|$. Or, on a d'autre part : $r - r' = b(q' - q)$. Si on avait $q \neq q'$, il en résulterait : $|r - r'| = |b(q' - q)| \geq |b|$, ce qui est contradictoire. Par suite : $q = q'$ et $r = a - bq = r'$.

Pour l'existence, on suppose d'abord a et b positifs. Soit $A = \{n \in \mathbb{N} : bn > a\}$. Comme $b \geq 1$, on a : $b(a + 1) > a$, c'est-à-dire : $a + 1 \in A$. Ainsi, A est une partie non vide de \mathbb{N} : elle a donc un plus petit élément que l'on note p . Comme $0 \times n \leq a$, on a : $0 \notin A$, de sorte que $p \geq 1$. Soit $q = p - 1$ - c'est bien un entier naturel. Par minimalité de p , cet entier q n'est pas un élément de A , de sorte que l'on a : $bq \leq a$. En revanche, $q + 1 = p$ appartient à A , ce qui donne : $b(q + 1) > a$. On réécrit ces inégalités sous la forme : $0 \leq a - bq < b$. Autrement dit, en posant $r = a - bq$, on a : $a = bq + r$ et $0 \leq r < b$.

On suppose a négatif et b positif. On écrit la division euclidienne de $-a$ par b sous forme : $-a = bq' + r'$ avec $0 \leq r' < b$. Si $r' = 0$, on pose $q = -q'$ et $r = 0$, ce qui donne $a = bq + r$ et $0 \leq r < b$. Sinon, on écrit : $a = b(-q' - 1) + b - r'$; on pose $q = -q' - 1$ et $r = b - r'$, on a : $a = bq + r$ et $0 < r < b$ comme souhaité.

Enfin, on suppose b négatif. On écrit la division euclidienne de a par $-b$ sous forme : $a = -bq' + r'$ avec $0 \leq r' < -b$. On pose $q = -q'$ et $r = r'$ et c'est gagné. \square

Exemple. Soit N le numéro INSEE d'une personne (à 13 chiffres, le premier étant le genre, puis l'année de naissance, etc.). La clé de ce numéro est $97 - r$, où r est le reste de la division de N par 97. L'intérêt de cette clé est qu'elle est facile à calculer et permet de détecter une erreur sur un chiffre : si deux numéros INSEE N et N' diffèrent en un seul chiffre, alors les clés sont différentes. Saurez-vous le montrer ?

2° Écriture en base quelconque

Proposition. Soit b un entier, $b \geq 2$. Pour tout $n \in \mathbb{N}^*$, il existe un unique $r \in \mathbb{N}$ et une unique $(r + 1)$ -liste $(a_0, \dots, a_r) \in \{0, \dots, b - 1\}^{r+1}$ tels que

$$n = \sum_{k=0}^r a_k b^k \quad \text{et} \quad a_r \neq 0. \quad (\S)$$

Démonstration. On procède par récurrence sur n . On initialise la récurrence pour n tel que $1 \leq n < b$. Pour l'unicité, on voit que si $r \geq 1$, alors $\sum_{k=0}^r a_k b^k \geq a_r b^r \geq b$, ce qui est absurde. D'où nécessairement $r = 0$ et donc : $n = a_0$. Et cette écriture convient.

Soit n un entier supérieur ou égal à b . On suppose que tout entier $< n$ admet une unique écriture en base b . Supposons que n admette une écriture (§) et prouvons-en l'unicité. D'abord, on constate que a_0 est nécessairement le reste de la division de n par b ; par suite, on a :

$(n - a_0)/b = \sum_{k=0}^{r-1} a_{k+1}b^k$: par unicité de l'écriture en base b de $n' = (n - a_0)/b$, r et a_1, \dots, a_r sont uniquement déterminés.

Pour l'existence d'une décomposition (§) pour n , on remonte ce qu'on vient de démontrer : on définit a_0 comme le reste de la division de n par b et n' comme le quotient, de sorte que $n' = (n - a_0)/b$; on écrit n' grâce à l'hypothèse de récurrence sous forme $n' = \sum_{k=0}^s a'_k b^k$ pour $s \in \mathbb{N}$ et $(a'_0, \dots, a'_s) \in \{0, \dots, b-1\}^{s+1}$; enfin, on a : $n = \sum_{k=0}^s a'_k b^{k+1} + a_0 = \sum_{k=1}^{s+1} a'_{k-1} b^k + a_0$, qui est de la forme souhaitée avec $r = s + 1$ et $a_k = a'_{k-1}$ si $1 \leq k \leq r$. \square

NOTATION. Lorsque b est entendu, on note $\overline{a_r \cdots a_1 a_0}$ ou $[a_r \cdots a_1 a_0]_b$ la somme $\sum_{k=0}^r a_k b^k = n$; si $b = 10$, on écrit simplement $a_r \cdots a_0$. On dit que les a_k sont les *chiffres* de n en base b .

Remarque. La preuve donne un algorithme itératif pour trouver les chiffres d'un nombre n en base b : effectuer la division euclidienne de n par b ; juxtaposer la suite des chiffres du quotient n' au reste a_0 .

Exemple. En base 2, les chiffres autorisés sont 0 et 1. Par exemple : $[10011] = 1 \times 2^4 + 1 \times 2 + 1 = 19$. Inversement, écrivons le nombre décimal 324 en base 2 :

- la division de 324 par 2 s'écrit : $324 = 2 \times 162 + 0$, le dernier chiffre est $a_0 = 0$;
- on a : $162 = 2 \times 81 + 0$, donc le dernier chiffre en base 2 de 162, qui est le chiffre a_1 de 324, est 0; on continue patiemment...
- on a : $81 = 2 \times 40 + 1$ donc $a_2 = 1$;
- on a : $40 = 2 \times 20 + 0$ donc $a_3 = 0$;
- on a : $20 = 2 \times 10 + 0$ donc $a_4 = 0$;
- on a : $10 = 2 \times 5 + 0$ donc $a_5 = 0$;
- on a : $5 = 2 \times 2 + 1$ donc $a_6 = 1$;
- on a : $2 = 2 \times 1 + 0$ donc $a_7 = 0$;
- on a : $1 = 2 \times 0 + 1$ donc $a_8 = 1$.

Au bilan : $324 = [101000100]_2 = 2^8 + 2^6 + 2^2$, formule que l'on vérifie aisément.

Exemple. En base $b = 2^4$ (seize), on a besoin de seize chiffres notés traditionnellement : $\{0, \dots, 2^4 - 1\} = \{0, 1, \dots, 9, A, B, C, D, E, F\}$, où A représente dix, B onze, etc. Un nombre à deux chiffres en base seize est compris entre $[00]_{2^4} = 0$ et $[FF]_{2^4} = (2^4 - 1) \times 2^4 + (2^4 - 1) = (2^4)^2 - 1$, nombre noté 255 en base dix.

Le code RGB d'une couleur est une suite de six chiffres en base seize : deux chiffres pour l'intensité de rouge (*red*), deux pour le vert (*green*), deux pour le bleu (*blue*). On peut donc décrire $(2^4)^6$ couleurs différentes (plus de seize millions). Par exemple, la couleur *salmon* est codée par $F A 8 0 7 2$, c'est-à-dire beaucoup de rouge ($[FA] = 250$), intensité moyenne de vert et de bleu ($[80] = 128$, $[72] = 114$).

II Divisibilité et congruences

1° Divisibilité

DEFINITION. Soient a et b deux entiers. On dit que b *divise* a ou que a est un *multiple* de b et on écrit $b|a$ s'il existe un entier k tel que $a = bk$.

Remarque. Si b est non nul, b divise a si et seulement si le reste de la division de a par b est nul. En effet, soient q et r le quotient et le reste de la division de a par b , de sorte que $a = bq + r$ et $0 \leq r < |b|$. Si b divise a , alors $a = bk$ pour k convenable et l'on a : $b(k - q) = r$, de sorte que r est un multiple de b compris entre 0 et $|b| - 1$: autrement dit, r est nul. Réciproquement, si $r = 0$, alors $a = bq$ et b divise a .

Exemple. Tout entier b divise 0 car $0 = b \times 0$. Tout entier a est multiple de 1 car $a = a \times 1$.

Exercice. En utilisant l'écriture en base dix d'un entier, (re)trouver les critères bien connus de divisibilité par 2 et par 5.

Lemme. Soient a, b et c trois entiers :

- (i) on a : $a|a$;
- (ii) si $a|b$ et $b|a$, alors $a = \pm b$;
- (iii) si $a|b$ et $b|c$ alors $a|c$.

2° Congruences

Dans toute cette partie, on fixe un entier naturel n .

DEFINITION. Soient a et b deux entiers. On dit que a est congru à b modulo n et on note $\ll a \equiv b [n] \gg$ si $a - b$ est un multiple de n , c'est-à-dire s'il existe un entier k tel que $a - b = kn$.

Exemple. Si $n = 0$, a est congru à b modulo 0 si et seulement si $a - b = 0 \times k$ pour k convenable, si et seulement si $a = b$. Pas nouveau.

On suppose désormais que n n'est pas nul.

Si $n = 1$, a est toujours congru à b modulo 1... Pas passionnant non plus.

Exemple. Soient a, a' des entiers et $\zeta = e^{2i\pi/n}$. Alors :

$$\zeta^a = \zeta^{a'} \Leftrightarrow e^{\frac{2i\pi a}{n}} = e^{\frac{2i\pi a'}{n}} \Leftrightarrow \exists k \in \mathbb{Z}, \frac{2i\pi a}{n} = \frac{2i\pi a'}{n} + 2\pi k \Leftrightarrow \exists k, a - a' = n \Leftrightarrow a \equiv a' [n].$$

Exemple. Soit b un entier, $b \geq 2$. Soit N un entier naturel non nul, on l'écrit en base b : $N = \sum_{k=0}^r a_k b^k$ avec $r \in \mathbb{N}$, $(a_0, \dots, a_r) \in \{0, \dots, b-1\}^{r+1}$ et $a_r \neq 0$. On note $S(N) = \sum_{k=0}^r a_k$ la somme des chiffres de N . Alors : $N \equiv S(N) [b-1]$. En effet :

$$N - S(N) = \sum_{k=0}^r a_k b^k - \sum_{k=0}^r a_k = \sum_{k=1}^r a_k (b^k - 1) = (b-1) \sum_{k=1}^r a_k (b^{k-1} + b^{k-2} + \dots + b + 1).$$

Exercice. Partant de l'exemple précédent, expliquer les critères bien connus (?) de divisibilité par 9 et par 3. En remplaçant $S(N)$ par $T(N) = \sum_{k=0}^r (-1)^k a_k$, (re)trouver un critère de divisibilité par 11. [À suivre.]

Lemme (Une relation d'équivalence). Soient a, b et c trois entiers. Alors :

- (i) on a : $a \equiv a [n]$;
- (ii) si $a \equiv b [n]$, alors $b \equiv a [n]$;
- (iii) si $a \equiv b [n]$ et $b \equiv c [n]$, alors $a \equiv c [n]$.

Démonstration. (i) On a : $a - a = n \times 0$. (ii) Si $a - b = kn$, alors $b - a = (-k)n$. (iii) Si $a - b = kn$ et $b - c = \ell n$, alors $a - c = (k + \ell)n$. □

Proposition. Soient a et a' deux entiers. Alors, $a \equiv a' [n]$ si et seulement si a et a' ont le même reste dans la division euclidienne par n .

Démonstration. Écrivons les divisions euclidiennes : $a = nq + r$ et $a' = nq' + r'$ avec $0 \leq r < n$ et $0 \leq r' < n$. On a donc : $a \equiv r [n]$ et $a' \equiv r' [n]$. Par suite, si $r = r'$, alors $a \equiv a' [n]$ (transitivité). Réciproquement, si $a \equiv a' [n]$, alors $r \equiv r' [n]$, c'est-à-dire : $r - r' = kn$ pour k convenable. D'autre part, vu que r et r' sont compris entre 0 et $n - 1$, on a comme dans la preuve de la division euclidienne : $|r - r'| < n$. Par suite, $k = 0$ et $r = r'$. □

Corollaire. Pour $r \in \{0, \dots, n-1\}$, notons $\pi(r)$ l'ensemble des entiers a dont le reste de la division euclidienne par n vaut r . Alors $\pi(r)$ et $\pi(s)$ sont disjoints si r et s sont deux éléments différents de $\{0, \dots, n-1\}$ et la réunion des $\pi(r)$ est \mathbb{Z} entier.

Exemple. Pour $n = 2$, $\pi(0)$ (resp. $\pi(1)$) est l'ensemble des nombres pairs (resp. impairs). Être congru modulo 2, c'est avoir la même parité.

Proposition (Compatibilité des congruences aux opérations). Soient a, b, a', b' quatre entiers. On suppose que $a \equiv a' [n]$ et que $b \equiv b' [n]$. Alors :

$$a + b \equiv a' + b' [n] \quad \text{et} \quad ab \equiv a'b' [n].$$

Démonstration. On a : $a - a' = kn$ et $b - b' = \ell n$ pour k et ℓ entiers convenables. Il vient : $a + b - (a' + b') = (k + \ell)n$, d'où la première congruence, et, pour la seconde :

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') = (kb + a'\ell)n. \square$$

Exercice. Soit $b \geq 2$. On reprend les notations d'un exemple précédent : on note $S(N)$ la somme des chiffres en base b d'un entier N . On rappelle que N et $S(N)$ sont congrus modulo $b - 1$. Prenant $b = 10$, expliquer la preuve par 9 des opérations arithmétiques.

Corollaire. Soient a et a' tels que $a \equiv a' [n]$ et k un entier naturel. Alors : $a^k \equiv a'^k [n]$.

Démonstration. Par récurrence sur k . Si $k = 0$, $a^k = 1 = a'^k$, rien à faire ; si $k = 1$ c'est évident aussi. Si la propriété est vraie pour k , on écrit $a^{k+1} = a \times a^k$, de même pour a' , et on applique l'hypothèse de récurrence (c'est-à-dire $a^k \equiv a'^k [n]$) et la proposition à $a, b = a^k, a'$ et $b' = a'^k$. \square

III Plus grand diviseur commun (PGCD), etc.

1° DEFINITION. Soient a et b deux entiers. Soit d un entier. On dit que d est un PGCD de a et b s'il divise a et b et s'il est multiple de tout diviseur commun à a et b :

$$\begin{cases} d|a \text{ et } d|b \\ \forall e \in \mathbb{Z}, \quad e|a \text{ et } e|b \implies e|d. \end{cases}$$

L'existence d'un PGCD ne résulte pas de la définition mais l'algorithme d'Euclide assure l'existence d'un PGCD. En revanche, on voit facilement que si d et d' sont deux PGCD de a et b , alors $d' = \pm d$. On peut éventuellement définir le PGCD comme étant, si on prouve son existence, le positif des deux. On le note souvent $\text{pgcd}(a, b)$ ou $a \wedge b$.

2° Algorithme d'Euclide

DEFINITION. Soient a et b deux entiers positifs. On pose $r_{-1} = a$ et $r_0 = b$. L'algorithme d'Euclide est défini par la suite $(r_i)_{i \geq -1}$ construite de la façon suivante. Pour $i \in \mathbb{N}$, supposant avoir défini r_{-1}, \dots, r_i , on distingue deux cas :

- si $r_i = 0$, on pose : $r_{i+1} = 0$;
- sinon, on définit r_{i+1} comme le reste de la division euclidienne de r_{i-1} par r_i , caractérisé par :

$$\begin{cases} r_{i-1} = q_i r_i + r_{i+1} \\ 0 \leq r_{i+1} < r_i. \end{cases}$$

Remarque. Si $0 < a < b$, les premières valeurs de la suite sont : $r_{-1} = a, r_0 = b, q_0 = 0, r_1 = a$, etc. Il n'est donc pas utile de commencer par ordonner a et b .

Proposition (Euclide). Soient a et b deux entiers et $(r_i)_{i \geq -1}$ la suite définie par l'algorithme d'Euclide. Alors, la suite (r_i) stationne en zéro et la dernière valeur non nulle est le PGCD de a et b : il existe i_{\max} tel que $r_{i_{\max}} \neq 0$ et $r_i = 0$ pour $i > i_{\max}$ et $r_{i_{\max}}$ est le PGCD de a et b .

Exemple. Soit $a = 2037$ et $b = 798$. On écrit la suite des divisions euclidiennes :

$$\begin{array}{rcl} 2037 & = & 2 \times 798 + 441 & r_1 = 441 \\ 798 & = & 441 + 357 & r_2 = 357 \\ 441 & = & 357 + 84 & r_3 = 84 \\ 357 & = & 4 \times 84 + 21 & r_4 = 21 \\ 84 & = & 4 \times 21 + 0 & r_5 = 0, \text{ etc.}, \end{array}$$

d'où : $2037 \wedge 798 = 21$.

Démonstration. Tout d'abord, on note que la suite $(r_i)_{i \geq 0}$ est une suite décroissante d'entiers naturels. Par conséquent, il existe i tel que $r_i = r_{i+1}$. Ceci ne peut se produire que si $r_i = 0$, sans quoi, par construction, on a : $r_{i+1} < r_i$. Ainsi, la suite (r_i) stationne en 0.

Pour deux entiers m et n , on note $D(m, n)$ l'ensemble des diviseurs commun à m et n . On prouve par récurrence finie sur $i \geq 0$ que si $r_i \neq 0$, alors : $D(r_{i-1}, r_i) = D(a, b)$. Pour $i = 0$, c'est évident puisque $r_{-1} = a$ et $r_0 = b$. Soit $i \in \mathbb{N}$, on suppose que $D(r_{i-1}, r_i) = D(a, b)$.

Montrons que l'on a : $D(r_{i-1}, r_i) = D(r_i, r_{i+1})$. Si e appartient à $D(r_{i-1}, r_i)$, on sait que e divise r_i mais e divise également r_{i+1} : en effet, $r_{i-1} = ek$ et $r_i = el$ pour k et l convenables donc $r_{i+1} = r_{i-1} - q_i r_i = e(k - q_i l)$. Inversement, si e appartient à $D(r_i, r_{i+1})$, alors e divise r_i et r_{i-1} : en effet, si $r_i = el$ et $r_{i+1} = em$, alors : $r_{i-1} = q_i r_i + r_{i+1} = e(q_i l + m)$. Ainsi, il vient : $D(a, b) = D(r_i, r_{i+1})$, ce qui permet de conclure la récurrence.

Soit $d = r_{i_{\max}}$. On a démontré la relation : $D(a, b) = D(r_{i_{\max}}, r_{i_{\max}}) = D(d, 0)$, qui est l'ensemble des diviseurs de d . On voit bien que d est un diviseur commun à a et b et que tout diviseur commun à a et b , c'est-à-dire tout élément de $D(a, b)$, est un diviseur de d . \square

Exercice. Soit r un rationnel : par définition, il existe a et b entiers, b non nul, tels que $r = a/b$. Montrer qu'il existe un unique couple (a, b) tel que $r = a/b$, a et b sont premiers entre eux et $b > 0$. Le couple (a, b) est alors appelé *représentant irréductible* de r .

3° Théorème de Bézout

Lemme. Si d est un PGCD de a et b , il existe u et v entiers tels que

$$au + bv = d.$$

Démonstration. On reprend les notations de la preuve de l'existence du PGCD. On prouve par récurrence finie sur $-1 \leq i \leq i_{\max}$ qu'il existe u_i et v_i tels que $r_i = au_i + bv_i$. Pour $i = -1$, on prend : $u_{-1} = 1$ et $v_{-1} = 0$; pour $i = 0$, on prend $u_0 = 0$ et $v_0 = 1$. Si la relation est vraie jusqu'au rang i et que $r_i \neq 0$, alors :

$$r_{i+1} = r_{i-1} - q_i r_i = au_{i-1} + bv_{i-1} - q_i(au_i + bv_i) = a(u_{i-1} - q_i u_i) + b(v_{i-1} - q_i v_i),$$

et on conclut la récurrence en posant : $u_{i+1} = u_{i-1} - q_i u_i$ et $v_{i+1} = v_{i-1} - q_i v_i$. \square

Mise en garde. En pratique, a et b étant donnés, il faut savoir trouver les « coefficients de Bézout » u et v . Voici un exemple, l'idée est de « remonter » à partir de l'algorithme d'Euclide.

Exemple. Soient $a = 2037$ et $b = 798$. On reprend la suite des divisions et on complète la colonne de droite de bas en haut.

$$\begin{array}{rcl} 2037 & = & 2 \times 798 + 441 & 21 & = & 5 \times 798 - 9 \times (2037 - 2 \times 798) = 23 \times 798 - 9 \times 2037 \\ 798 & = & 441 + 357 & 21 & = & 5 \times (798 - 441) - 4 \times 441 = 5 \times 798 - 9 \times 441 \\ 441 & = & 357 + 84 & 21 & = & 357 - 4 \times (441 - 357) = 5 \times 357 - 4 \times 441 \\ 357 & = & 4 \times 84 + 21 & 21 & = & 357 - 4 \times 84. \end{array}$$

On trouve ainsi : $21 = 23 \times 798 - 9 \times 2037$.

Voici un énoncé plus complet.

Proposition (Théorème de Bézout). *Soient a et b deux entiers et d leur PGCD. Pour tout e , il est équivalent de dire :*

- (i) e est un multiple de d : $\exists k \in \mathbb{Z}, e = kd$;
- (ii) $\exists (u, v) \in \mathbb{Z}^2, au + bv = e$.

Démonstration. (i) \Rightarrow (ii) : On suppose que $e = kd$ pour k convenable. Par la première version de la relation de Bézout, on peut trouver u_0 et v_0 tels que $au_0 + bv_0 = d$. En multipliant par k tel que $e = kd$, il vient : $au_0k + bv_0k = kd = e$.

(ii) \Rightarrow (i) : On suppose qu'existent u et v tels que $au + bv = e$. Soient k et ℓ tels que $a = kd$ et $b = \ell d$, alors : $e = au + bv = kdu + \ell dv = (ku + \ell v)d$. \square

Remarque (L'équation $ax + by = c$). Soient $a, b, c \in \mathbb{Z}$. On note d le PGCD de a et b et on définit a' et b' par : $a = da'$ et $b = db'$. On cherche tous les $x, y \in \mathbb{Z}$ tels que $ax + by = c$. D'après la proposition, il existe une solution si et seulement si d divise c . On suppose que c'est le cas, c'est-à-dire que $c = dd'$ pour d' convenable. On commence par trouver (u_0, v_0) tel que $au_0 + bv_0 = d$ par l'algorithme d'Euclide, d'où, en posant $x_0 = d'u_0$ et $y_0 = d'v_0$, une solution : $ax_0 + by_0 = dd' = c$.

Soit $(x, y) \in \mathbb{Z}^2$. C'est une solution SSI $ax + by = ax_0 + by_0$ SSI $a(x - x_0) = -b(y - y_0)$. Grâce au lemme de Gauss, on montre plus bas qu'alors, il existe k tel que $x = x_0 + kb'$ et il vient : $y = y_0 - ka'$. Réciproquement, on vérifie que les couples $(x_0 + kb', y_0 - ka')$ sont solutions, ce qui résulte de : $ab' = ab/d = a'b$.

4° Nombres premiers entre eux

DEFINITION. On dit que a et b sont premiers entre eux si leur PGCD est 1 (ou -1). On note alors : $a \wedge b = 1$.

Lemme. *Soient a et b deux entiers. Alors a et b sont premiers entre eux si et seulement s'il existe u et v entiers tels que*

$$au + bv = 1.$$

Démonstration. Si a et b sont premiers entre eux, leur PGCD est 1 et l'on peut trouver u et v par le théorème de Bézout. Réciproquement, supposons qu'existent u et v tels que $au + bv = 1$ et soit d un diviseur commun à a et b . Alors on peut écrire $a = kd$ et $b = \ell d$ pour k et ℓ convenables, d'où : $1 = au + bv = kdu + \ell dv = (ku + \ell v)d$. Ainsi, d divise 1 et donc : $d = \pm 1$. \square

Corollaire. *Soient n et a deux entiers. Alors : $a \wedge n = 1$ SSI $\exists u \in \mathbb{Z}, au \equiv 1 [n]$.*

Démonstration. Si a et n sont premiers entre eux, on peut trouver u et v tels que $au + nv = 1$, de sorte que l'on a bien : $au \equiv 1 [n]$. Réciproquement, s'il existe u tel que $au \equiv 1 [n]$, alors il existe v tel que $au - 1 = nv$, donc a et n sont premiers entre eux par le lemme de Bézout. \square

5° Lemme de Gauss

Le résultat suivant est fondamental, en particulier pour l'unicité dans la factorisation d'un entier.

Lemme (Gauss). *Soient a, b, c des entiers. Si $a|bc$ et $a \wedge b = 1$, alors $a|c$.*

Démonstration. Supposons que a divise bc . Alors il existe k tel que $bc = ak$. Par réflexe, on écrit qu'il existe u et v tels que $au + bv = 1$. Multiplions cette égalité par c , il vient : $c = acu + bcv = acu + akv = a(cu + kv)$, ce qui prouve que a divise c . \square

Exercice. Démontrer proprement que si p est un nombre premier, alors \sqrt{p} n'est pas rationnel.

Remarque. On revient à $a(x - x_0) = -b(y - y_0)$ de l'équation $ax + by = c$. En divisant par d , il vient : $a'(x - x_0) = -b'(y - y_0)$. Alors, b' divise $a'(x - x_0)$ et b' est premier avec a' donc b' divise $x - x_0$. Autrement dit, il existe k tel que $x - x_0 = b'k$.

IV Nombres premiers

1° Définition

DEFINITION. Soit $p \in \mathbb{Z}$. On dit que p est *premier* si ses seuls diviseurs sont ± 1 et $\pm p$.

Exemple. Les premiers nombres premiers sont : $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23$, etc.

Voici une version faible de la factorisation qui n'utilise essentiellement pas d'arithmétique.

Lemme. *Tout entier non nul peut s'écrire d'au moins une façon comme produit de facteurs premiers. En particulier, tout entier supérieur ou égal à 2 possède un diviseur premier.*

Démonstration. Voici ce qu'il faut montrer : pour $n \in \mathbb{N}^*$, il existe un naturel r et des nombres premiers p_1, \dots, p_r tels que $n = p_1 \cdots p_r$. On procède par récurrence « forte » sur n . Pour $n = 1$, c'est clair : on prend $r = 0$, de sorte qu'il n'y a aucun nombre premier à trouver (un produit sur zéro facteurs est 1 par convention). Pour $n = 2$, on prend $r = 1$ et $p_1 = 2$. Soit n un entier supérieur à 2, on suppose que tout entier $k < n$ peut s'écrire comme produit de facteurs premiers. De deux choses l'une. Si n est un nombre premier, on prend $r = 1$ et $p_1 = n$ et c'est gagné. Sinon, n possède un diviseur k strictement compris entre 1 et n ; on pose $\ell = n/k$, strictement compris entre 1 et n aussi. On écrit $k = p_1 \cdots p_r$ et $\ell = q_1 \cdots q_s$ pour $p_1, \dots, p_r, q_1, \dots, q_s$ premiers, d'où : $n = p_1 \cdots p_r q_1 \cdots q_s$. Ainsi, n est un produit de nombres premiers et on conclut la récurrence. \square

Proposition (Euclide). *Il y a une infinité de nombres premiers.*

Démonstration. Il existe au moins un nombre premier – par exemple, 2 en est un. Soit $\mathcal{P} = \{p_1, \dots, p_r\}$ un ensemble fini de nombres premiers. On pose alors : $P = 1 + \prod_{i=1}^r p_i$. Aucun des p_i ne divise P . Pourtant, P admet un diviseur premier p_{r+1} (voir ci-dessus). On a ainsi – depuis Euclide! – une méthode pour fabriquer une suite infinie de nombres premiers. \square

2° Factorisation unique

Théorème. *Tout nombre entier s'écrit comme produit de nombres premiers, de façon unique à l'ordre et aux signes des facteurs près.*

On formule plus précisément...

Théorème. *Soit n un entier non nul.*

- (i) *Il existe $\varepsilon \in \{-1, 1\}$, $r \in \mathbb{N}$ et (p_1, \dots, p_r) premiers positifs tels que $n = \varepsilon p_1 \cdots p_r$.*
- (ii) *Si $\varepsilon' \in \{-1, 1\}$, $s \in \mathbb{N}$ et (q_1, \dots, q_s) sont des nombres premiers positifs tels que $n = \varepsilon' q_1 \cdots q_s$, alors : $\varepsilon = \varepsilon'$, $r = s$ et il existe une bijection σ de $\{1, \dots, r\}$ sur lui-même telle que $q_i = p_{\sigma(i)}$ pour tout i .*

On commence par un lemme : il étend le lemme de Gauss à plusieurs facteurs en utilisant le fait évident qu'un nombre premier qui ne divise pas un entier est premier avec cet entier.

Lemme. *Soit p un nombre premier, r un entier et q_1, \dots, q_r des entiers. Si p divise le produit $q_1 \cdots q_r$, alors p divise l'un des facteurs q_i ($1 \leq i \leq r$).*

Démonstration. On procède par récurrence sur r . Si $r = 1$, il n'y a rien à démontrer. Si $r = 2$, c'est le lemme de Gauss. Supposons la propriété vraie pour $r - 1$ facteurs et supposons que p divise $q_1 \dots q_r$. De deux choses l'une. Soit p divise q_r , auquel cas c'est gagné. Soit p est premier avec q_r ; par le lemme de Gauss, p divise alors $q_1 \dots q_{r-1}$; par hypothèse de récurrence, p divise alors l'un des q_i et c'est gagné aussi. \square

Démonstration (du théorème). L'existence a déjà été vue, reste à voir l'unicité. On remarque d'abord que $\varepsilon = \varepsilon'$, c'est le signe de n . On reste avec des nombres positifs. On procède par récurrence sur r , l'hypothèse de récurrence étant : si un entier n admet une décomposition avec r facteurs premiers, alors elle est unique, c'est-à-dire que pour toute autre décomposition avec s facteurs premiers, on a $r = s$ et les facteurs sont égaux à l'ordre près. Dire que $r = 0$, cela signifie que $n = 1$ et donc n n'admet pas de diviseur premier, de sorte que $s = 0$ aussi.

Soit $r \in \mathbb{N}^*$, on suppose la propriété vraie pour toute factorisation de longueur $r - 1$. Soit n un entier admettant deux factorisations : $n = p_1 \dots p_r = q_1 \dots q_s$. Le nombre premier p_r divise n donc il divise le produit $q_1 \dots q_s$. Par le lemme, il divise donc q_i pour i convenable. Mais comme q_i est lui-même premier, c'est que l'on a : $p_r = q_i$. On peut simplifier et il vient : $p_1 \dots p_{r-1} = q_1 \dots q_{i-1} q_{i+1} \dots q_s$. On peut appliquer l'hypothèse de récurrence : $r - 1 = s - 1$ et l'ensemble $\{p_1, \dots, p_{r-1}\}$ coïncide avec l'ensemble $\{q_1, \dots, q_{i-1}, q_{i+1}, \dots, q_s\}$. On peut conclure. \square

On reformule derechef.

Théorème. Soit n un entier non nul. Il existe $\varepsilon \in \{-1, 1\}$, $s \in \mathbb{N}$, (p_1, \dots, p_s) des nombres premiers positifs tels que $p_1 < p_2 < \dots < p_s$ et (v_1, \dots, v_s) entiers naturels non nuls, tous uniques, tels que : $n = \varepsilon p_1^{v_1} \dots p_s^{v_s}$.

Dans cette écriture, la recherche du PGCD est facile.

Corollaire. Avec des notations évidentes : $\text{PGCD}(\prod_{i=1}^s p_i^{v_i}, \prod_{i=1}^s p_i^{w_i}) = \prod_{i=1}^s p_i^{\min(v_i, w_i)}$.

3° Congruences modulo un nombre premier

Proposition. Soit p premier. Pour tout a non divisible par p , il existe $u \in \mathbb{Z}$ tel que $au \equiv 1 [p]$.

Démonstration. Dire que a n'est pas divisible par p , c'est dire que a est premier avec p . On a donc déjà vu cette propriété comme corollaire du lemme de Bézout.

Lemme. Soit p un nombre premier et $k \in \{1, \dots, p - 1\}$. Alors : $\binom{p}{k} \equiv 0 [p]$.

Démonstration. On a : $k!(p - k)! \binom{p}{k} = p!$. On sait que p divise $p!$. Or, p est premier avec chaque facteur de $k!$ et de $(p - k)!$ donc, par le lemme de Gauss (étendu à plus de deux facteurs pour être précis), p est premier avec $k!(p - k)!$. Par suite, p divise $\binom{p}{k}$.

Théorème (Petit théorème de Fermat). Soit p premier et a non divisible par p . Alors :

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

Démonstration. On commence par montrer par récurrence sur $a \in \mathbb{N}$ que l'on a : $a^p \equiv a [p]$. Pour $a = 0$, c'est clair. Si la propriété est vraie pour a , on calcule :

$$(a + 1)^p \equiv \sum_{k=0}^p \binom{p}{k} a^k \equiv a^p + 1 \equiv a + 1 [p].$$

Ainsi, on a : $a(a^{p-1} - 1) \equiv 0 [p]$ pour tout a . Si a n'est pas divisible par p , on trouve u tel que $au \equiv 1 [p]$ et on multiplie par u la congruence précédente : il vient : $a^{p-1} - 1 \equiv u \times 0 \equiv 0 [p]$. \square