

Chapitre VIII - Arithmétique sur \mathbb{Z}

Table des matières

1. Division euclidienne	1
2. Nombres premiers	2
3. Valuation p -adique d'un entier relatif	7
4. Plus grand commun diviseur	9
5. L'algorithme d'Euclide	12
6. L'équation $ax + by = c$	14
7. Plus petit commun multiple	15
8. Numération en base b	16

1. Division euclidienne

Rappelons que toute partie non vide de \mathbb{N} possède un plus petit élément.

Théorème 8.1 (Division euclidienne). *Soient a et b des entiers relatifs avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que l'on ait*

$$a = bq + r \quad \text{et} \quad 0 \leq r < |b|.$$

On dit que q est le quotient et que r est le reste de la division euclidienne de a par b .

Démonstration : 1) Démontrons l'assertion d'unicité. Supposons pour cela qu'il existe des couples (q, r) et (q', r') d'entiers relatifs tels que l'on ait

$$a = bq + r = bq' + r' \quad \text{avec} \quad 0 \leq r < |b| \quad \text{et} \quad 0 \leq r' < |b|.$$

On a l'égalité

$$(1) \quad |q - q'| |b| = |r' - r|.$$

Par ailleurs, r et r' étant positifs, $|r - r'|$ est inférieur ou égal à r ou r' . On a donc

$$|r - r'| < |b|.$$

D'après (1) on obtient $|q - q'| < 1$, d'où $q = q'$ puis $r = r'$, ce qui établit l'unicité.

2) Démontrons l'assertion d'existence. Considérons l'ensemble

$$A = \{a - bk \mid k \in \mathbb{Z}\} \cap \mathbb{N}.$$

Vérifions que A n'est pas vide. Tel est le cas si $a \geq 0$, car dans ce cas a est dans A (on prend $k = 0$). Supposons $a < 0$. Si $b \geq 1$, on constate que $a(1 - b) \in A$ (prendre $k = a$) et si $b \leq -1$, alors $a(1 + b) \in A$ (prendre $k = -a$). Il en résulte que A possède un plus petit élément r . Puisque r appartient à A , on a $r \geq 0$ et il existe $q \in \mathbb{Z}$ tel que l'on ait $a - bq = r$. Il reste à vérifier que l'on a $r < |b|$. Supposons le contraire. On a alors

$$0 \leq r - |b| = a - b(q + \varepsilon) \in A \quad \text{avec} \quad \varepsilon = \pm 1,$$

et l'inégalité $r - |b| < r$ contredit le caractère minimal de r , d'où le résultat.

Définition 8.1. Soient a et b des entiers relatifs. On dit que b divise a ou que b est un diviseur de a , ou bien encore que a est un multiple de b (dans \mathbb{Z}) s'il existe $k \in \mathbb{Z}$ tel que $a = bk$. Si b est non nul, cette condition signifie que le reste de la division euclidienne de a par b est nul.

Exercice 1.

- 1) Quels sont le quotient et le reste de la division euclidienne de 56798 par 23 ?
- 2) Démontrer que 14443 est divisible par 101.
- 3) Déterminer tous les entiers naturels n tels que $n + 1$ divise $n^2 + 1$.

2. Nombres premiers

Définition 8.2. On appelle nombre premier tout entier $p \geq 2$ dont les seuls diviseurs positifs sont 1 et p .

Par exemple 2, 3, 5, 7, 11, 13, \dots sont des nombres premiers.

Lemme 8.1. Soit p un entier ≥ 2 . Alors, p est premier si et seulement si p n'est pas le produit de deux entiers strictement plus grands que 1.

Démonstration : Si l'on a $p = ab$ avec a et b strictement plus grands que 1, alors a divise p et a est distinct de 1 et p , autrement dit, p n'est pas premier. Inversement, si p n'est pas premier, il possède un diviseur positif a autre que 1 et p . On a alors $p = ab$, où a et b sont ≥ 2 .

Théorème 8.2. Tout entier $n \geq 2$ est un produit de nombres premiers. En particulier, tout entier $n \geq 2$ possède un diviseur premier.

Démonstration : On procède par récurrence sur n . Notons $P(n)$ la propriété : n est un produit de nombres premiers. D'abord $P(2)$ est vraie, car 2 est premier. Considérons

alors un entier $n \geq 3$ tel que $P(k)$ soit vraie pour tout entier k tel que $2 \leq k < n$. Il s'agit de démontrer que $P(n)$ est vraie. Tel est le cas si n est premier. Si n n'est pas premier, il existe deux entiers a et b strictement plus grands que 1 tels que $n = ab$ (lemme 8.1). Puisque l'on a $2 \leq a < n$ et $2 \leq b < n$, les propriétés $P(a)$ et $P(b)$ sont vraies, ce qui entraîne le résultat.

Notation. On notera désormais \mathbf{P} l'ensemble des nombres premiers.

Le résultat suivant est dû à Euclide qui vécut au III^e siècle avant J.-C. :

Théorème 8.3. *L'ensemble \mathbf{P} est infini.*

Démonstration : Supposons que \mathbf{P} soit fini de cardinal n . Soient p_1, \dots, p_n ses éléments. Posons $N = 1 + p_1 \cdots p_n$. On a $N \geq 2$, donc N possède un diviseur premier p . L'entier p divise $p_1 \cdots p_n$, d'où l'on déduit que p divise 1, ce qui conduit à une contradiction.

Théorème 8.4 (Lemme d'Euclide). *Soient a, b des entiers naturels et p un nombre premier tels que p divise ab . Alors, p divise l'un des entiers a et b .*

Démonstration. On peut supposer $ab \neq 0$. La démonstration qui suit est due à Gauss⁽¹⁾. Supposons que p ne divise pas a . Il s'agit de montrer que p divise b . Considérons pour cela l'ensemble

$$A = \{n \geq 1 \mid p \text{ divise } an\}.$$

Il est non vide, car par exemple p appartient à A . Soit m le plus petit élément de A . D'après l'hypothèse faite sur a , on a l'inégalité

$$(2) \quad m \geq 2.$$

Soit n un élément de A . Vérifions que m divise n . D'après le théorème de la division euclidienne, il existe des entiers q et r tels que l'on ait $n = mq + r$ avec $0 \leq r < m$. On a l'égalité $an - (am)q = ar$, d'où l'on déduit que p divise ar (car n et m sont dans A). Puisque l'on a $r < m$, r n'est pas dans A , d'où $r = 0$ et notre assertion. Les entiers p et b étant dans A , il en résulte que m divise p et b . L'inégalité (2) et le fait que p soit premier entraînent alors $p = m$. Par suite, p divise b .

⁽¹⁾ Carl Friedrich Gauss, surnommé le prince des mathématiciens, est né à Brunswick en 1777 et décède à Göttingen en 1855. On lui doit une quantité massive de résultats en arithmétique, ainsi que dans d'autres domaines. Son ouvrage, *Disquisitiones Arithmeticae*, est resté célèbre en théorie des nombres. On pourra trouver les arguments de la démonstration du théorème 8.4 à la page 6 de ce livre. À dix ans, le maître d'école lui demanda de calculer la somme des cent premiers entiers naturels. Il donna de façon surprenante la réponse très rapidement, à savoir $50 \times 101 = 5050$. Quelle formule avait-il utilisée ?

Corollaire 8.1. *Si un nombre premier divise un produit d'entiers relatifs, il divise l'un de ces entiers. En particulier, si un nombre premier divise un produit de nombres premiers, il est égal à l'un d'eux.*

Démonstration : C'est une conséquence directe du théorème 8.4, en procédant par récurrence sur le nombre de facteurs du produit (exercice).

Le théorème suivant s'appelle parfois le théorème fondamental de l'arithmétique :

Théorème 8.5. *Tout entier $n \geq 2$ s'écrit de façon unique sous la forme*

$$(3) \quad n = p_1^{n_1} \cdots p_r^{n_r},$$

où les n_i sont des entiers naturels non nuls, et où les p_i sont des nombres premiers vérifiant $p_{i-1} < p_i$ pour $i = 2, \dots, r$. On dit que l'égalité (3) est la décomposition de n en produit de nombres premiers.

Démonstration : L'assertion d'existence provient du théorème 8.2 en regroupant les facteurs égaux par ordre croissant. Prouvons l'assertion d'unicité. Supposons que l'on ait

$$n = p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s},$$

où les p_i et q_i sont premiers tels que $p_1 < \cdots < p_r$, $q_1 < \cdots < q_s$ et où les n_i et m_i sont des entiers naturels non nuls. On déduit du corollaire 8.1 que l'on a

$$\{p_1, \dots, p_r\} = \{q_1, \dots, q_s\}.$$

Par suite, on a $r = s$. De plus, p_1 est le plus petit élément de $\{p_1, \dots, p_r\}$ et q_1 est le plus petit élément de $\{q_1, \dots, q_r\}$, d'où $p_1 = q_1$, puis $p_i = q_i$ pour tout i . Par ailleurs, s'il existe un indice i tel que $n_i \neq m_i$, par exemple $n_i < m_i$, alors p_i divise 1 ou bien un produit de nombres premiers tous distincts de lui-même, ce qui contredit le corollaire 8.1 et établit le résultat.

Exercice 2. (Petit théorème de Fermat⁽²⁾) Soient a un entier ≥ 1 et p un nombre premier.

- 1) Soit k un entier tel que $1 \leq k \leq p-1$. Montrer que p divise le coefficient binomial C_p^k .
- 2) En déduire, par récurrence sur a , que p divise $a^p - a$.

⁽²⁾ Pierre de Fermat est né près de Toulouse en 1601 et mourut à Castres en 1665. Bien qu'il consacra une partie de sa carrière à sa fonction de conseiller à la Cour de Toulouse, il restera comme l'un des grands mathématiciens de son temps, notamment pour ses travaux en théorie de nombres et en probabilité. Il existe aussi un «grand théorème de Fermat», qui en réalité n'est devenu un théorème qu'en 1994. Il s'agit de l'énoncé suivant : pour tout entier $n \geq 3$, il n'existe pas d'entiers relatifs x, y et z tels que $x^n + y^n = z^n$ avec $xyz \neq 0$. L'entier $n = 2$ doit évidemment être exclu vu que pour tous a et b dans \mathbb{Z} , on a l'égalité $(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2$, ce qui géométriquement signifie qu'il existe une infinité de triangles rectangles dont les longueurs des côtés sont des entiers. La recherche d'une démonstration, ne serait-ce que pour des valeurs particulières de l'exposant n , a par exemple donné naissance à la notion d'idéal d'un anneau, puis à toute la théorie algébrique des nombres.

Une problème naturel qui se pose est le suivant :

Problème. Soit n un entier ≥ 2 . Comment décider si n est un nombre premier ou non ?

Il existe de nombreux tests permettant parfois de reconnaître si un entier n est premier. Nous n'aborderons pas cette étude dans ce cours. C'est la théorie des tests de primalité. Signalons seulement à ce sujet le résultat ci-dessous :

Lemme 8.2. Soit n un entier ≥ 2 . Si n n'est pas premier, alors n possède un diviseur premier p vérifiant l'inégalité $p^2 \leq n$.

Démonstration : Si n n'est pas premier, il existe deux entiers a et b strictement plus grands que 1 tels que $n = ab$ (lemme 8.1). Supposons par exemple $a \leq b$. Puisque $a \geq 2$, a possède un diviseur premier p (th. 8.2). En particulier, p divise n et l'on a $p^2 \leq ap \leq ab = n$.

En utilisant ce résultat, on constate par exemple que 641 est premier. En effet, s'il ne l'était pas, il devrait exister un nombre premier $p < 25$ divisant 641. Les nombres premiers plus petits que 25 sont 2, 3, 5, 7, 11, 13, 17, 19 et 23. On vérifie alors qu'aucun de ces nombres ne divise 641 en utilisant le théorème de la division euclidienne.

Étant donné un entier N , il existe un procédé de criblage, appelé crible d'Ératosthène (il vécut au III^e siècle), qui permet de déterminer tous les nombres premiers inférieurs à N , en utilisant seulement l'opération de multiplication, et pas celle de division, ce qui est plus facile. Son principe est le suivant. On écrit d'abord dans un tableau tous les entiers jusqu'à N . On raye ensuite tous les multiples de 2, autres que 2, puis tous les multiples de 3, autres que 3, etc, autrement dit, à chaque étape on raye tous les multiples du plus petit entier qui n'a pas encore été rayé. Pour savoir si N est premier, il suffit d'après le lemme 8.2 d'examiner les multiples des entiers plus petits que \sqrt{N} .

Remarquons par ailleurs que le petit théorème de Fermat permet parfois de démontrer qu'un entier $n \geq 2$ n'est pas premier, si tel est le cas. Compte tenu de ce théorème, il suffit en effet d'explicitier un entier naturel a tel que n ne divise pas $a^n - a$. Cela étant, il existe des entiers n non premiers pour lesquels quel que soit $a \in \mathbb{Z}$, l'entier $a^n - a$ est divisible par n . Ces entiers s'appellent les nombres de Carmichael (1879-1967). Tel est par exemple le cas de $n = 561$ (c'est le plus petit) et de $n = 1105$ (c'est le suivant). On sait par ailleurs démontrer, depuis 1992, qu'il existe une infinité de nombres de Carmichael. La démonstration de ce résultat, qui dépasse de loin le niveau de ce cours, utilise la théorie analytique des nombres. Signalons qu'il est néanmoins assez facile de prouver que pour tout entier $n \geq 1$, si les trois nombres $p = 6n + 1$, $q = 12n + 1$ et $r = 18n + 1$ sont premiers, alors pqr est un nombre de Carmichael. Il en est ainsi avec $n = 1$, auquel cas $pqr = 1729$. La question de savoir s'il existe une infinité de tels entiers n est ouverte.

Exercice 3. Montrer que 3571 est un nombre premier (c'est le cinq centième nombre premier).

Exercice 4. Soit n un entier ≥ 1 .

1) Montrer que si $2^n - 1$ est un nombre premier, il en est de même de n .

Un nombre de la forme $2^n - 1$ s'appelle un nombre de Mersenne (c'était un moine français qui vécut de 1588 à 1648). On connaît « beaucoup » de nombres premiers de Mersenne, en fait quarante six,

$$2^2 - 1 = 3, 2^3 - 1 = 7, 2^5 - 1 = 31, \dots, 2^{19} - 1, \dots, 2^{61} - 1, \dots,$$

mais on ne sait pas prouver qu'il en existe une infinité. Le dernier a été découvert en septembre 2008, avec $n = 37.156.667$. Le plus grand nombre premier aujourd'hui connu est un nombre de Mersenne. Il s'agit de

$$2^{43.112.609} - 1,$$

découvert quinze jours avant, en août 2008. Il possède 12.978.189 chiffres décimaux (le vérifier). Les grands nombres premiers de Mersenne ont été détectés en utilisant un test de primalité qui leur est spécifique (test de Lucas). Notons que $2^{11} - 1 = 23 \times 89$ n'est pas premier. On ne sait pas non plus démontrer l'existence d'une infinité de nombres premiers p tels que $2^p - 1$ ne soit pas premier.

2) Montrer que si $2^n + 1$ est premier, alors n est une puissance de 2.

Un nombre de la forme $2^{2^n} + 1$ s'appelle un nombre de Fermat. On ne connaît que cinq nombres premiers de Fermat,

$$3, 5, 17, 257 \text{ et } 65537 = 2^{16} + 1.$$

On conjecture qu'il n'en existe qu'un nombre fini. En fait les nombres de Fermat croissent rapidement, et il est difficile de décider s'ils sont premiers ou non, y compris pour des petites valeurs de n .

Prouvons ici que $2^{32} + 1$ n'est pas premier en montrant qu'il est divisible par 641. L'argument qui suit est dû à Euler⁽³⁾. Posons $p = 641$. On écrit que l'on a

$$p = 5^4 + 2^4 \text{ et } p = 5 \cdot 2^7 + 1.$$

Il existe donc $k \in \mathbb{Z}$ tel que l'on ait $5^4 \cdot 2^{28} = (p - 1)^4 = 1 + kp$. On obtient l'égalité $p(2^{28} - k) = 2^{32} + 1$, d'où l'assertion.

Cela étant, on ne sait toujours pas démontrer l'existence d'une infinité de nombres de Fermat qui ne sont pas premiers.

⁽³⁾ Leonhard Euler était un mathématicien suisse. Il est né à Bâle en 1707 et décède à Saint-Petersbourg en 1783. Il apporta d'importantes contributions en théorie des nombres et en analyse. Il établit sa renommée en calculant la somme des inverses des carrés des entiers, en démontrant l'égalité $\sum \frac{1}{n^2} = \frac{\pi^2}{6}$.

Exercice 5. Déterminer tous les nombres premiers p tels que p divise $2^p + 1$ (utiliser le petit théorème de Fermat).

Exercice 6. Soit n un entier naturel. Posons $p = 2n + 1$. Démontrer que p est un nombre premier si et seulement si n ne figure pas dans le tableau infini suivant :

$$\begin{pmatrix} 4 & 7 & 10 & 13 & 16 & \dots \\ 7 & 12 & 17 & 22 & 27 & \dots \\ 10 & 17 & 24 & 31 & 38 & \dots \\ 13 & 22 & 31 & 40 & 49 & \dots \\ 16 & 27 & 38 & 49 & 60 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

dans lequel la première colonne est une suite arithmétique de premier terme 4 et de raison 3 et la k -ième ligne est une suite arithmétique de raison $2k+1$. (On vérifiera que le coefficient de la k -ième ligne et de la j -ième colonne de ce tableau est $2kj + k + j$).

Exercice 7. Démontrer que l'entier $1 + 2 + 2^2 + 2^3 + \dots + 2^{26}$ n'est pas premier.

3. Valuation p -adique d'un entier relatif

On considère dans ce paragraphe l'ensemble $\mathbb{N} \cup \{+\infty\}$ obtenu en adjoignant à \mathbb{N} un élément noté $+\infty$, que l'on munit de la structure d'ensemble ordonné qui induit l'ordre usuel sur \mathbb{N} et telle que $+\infty \geq n$ pour tout entier naturel n . On prolonge par ailleurs la loi additive de \mathbb{N} à cet ensemble en posant $(+\infty) + n = n + (+\infty) = +\infty$ et $(+\infty) + (+\infty) = +\infty$. Pour tout nombre premier p , on va définir ici une application, appelée valuation p -adique,

$$v_p : \mathbb{Z} \rightarrow \mathbb{N} \cup \{+\infty\}.$$

Définition 8.2. Soient n un entier relatif et p un nombre premier.

1) Si l'on a $n \geq 2$, alors $v_p(n)$ est l'exposant de p dans la décomposition de n en produit de nombres premiers. Autrement dit :

1.1) si p ne divise pas n , on a $v_p(n) = 0$.

1.2) Si $n = p_1^{n_1} \dots p_r^{n_r}$ est la décomposition de n en produit de nombres premiers ($n_i \geq 1$), on a

$$v_{p_i}(n) = n_i \quad \text{pour } i = 1, \dots, r.$$

2) On pose $v_p(0) = +\infty$ et $v_p(1) = 0$.

3) Pour tout $n \geq 1$, on pose $v_p(-n) = v_p(n)$.

On dit que $v_p(n)$ est la valuation p -adique de n .

Pour tout nombre premier p et tout entier $n \geq 1$, zéro est divisible par p^n , ce qui justifie l'égalité $v_p(0) = +\infty$.

Exemple 8.1. Posons $n = 539000$. On a $n = 2^3 \cdot 5^3 \cdot 7^2 \cdot 11$, de sorte que l'on a $v_2(n) = 3$, $v_5(n) = 3$, $v_7(n) = 2$, $v_{11}(n) = 1$ et pour tout nombre premier p distinct de 2, 5, 7 et 11, on a $v_p(n) = 0$.

Avec cette définition, le théorème 8.5 s'écrit comme suit :

Théorème 8.6. *Tout entier relatif n non nul s'écrit de manière unique, à l'ordre près des facteurs, sous la forme*

$$(4) \quad n = \varepsilon \prod_{p \in \mathbf{P}} p^{v_p(n)} \quad \text{avec} \quad \varepsilon = \pm 1.$$

On a $\varepsilon = 1$ si $n \geq 1$ et $\varepsilon = -1$ si $n \leq -1$. Contrairement à ce que laisse supposer cette formule, il s'agit d'un produit fini car on a $v_p(n) = 0$ pour presque tout $p \in \mathbf{P}$ (au sens tous sauf un nombre fini). De plus, pour tout $n \in \mathbb{Z}$, on a l'équivalence

$$(5) \quad v_p(n) \geq 1 \iff p \text{ divise } n.$$

Pour tous x et y dans \mathbb{Z} , on note dans la suite $\text{Min}(x, y)$ le plus petit d'entre eux.

Proposition 8.1. *Soient a et b des entiers relatifs et p un nombre premier.*

- 1) *On a $v_p(ab) = v_p(a) + v_p(b)$.*
- 2) *On a $v_p(a + b) \geq \text{Min}(v_p(a), v_p(b))$. De plus, si $v_p(a) \neq v_p(b)$, alors on a l'égalité $v_p(a + b) = \text{Min}(v_p(a), v_p(b))$.*
- 3) *Pour que a divise b , il faut et il suffit que l'on ait $v_p(a) \leq v_p(b)$ pour tout $p \in \mathbf{P}$.*

Démonstration : On vérifie directement que ces assertions sont vraies si $ab = 0$. Supposons donc $ab \neq 0$.

- 1) Il résulte du théorème 8.6 que l'on a les égalités

$$ab = \varepsilon \prod_{p \in \mathbf{P}} p^{v_p(ab)} = \varepsilon \prod_{p \in \mathbf{P}} p^{v_p(a) + v_p(b)} \quad \text{avec} \quad \varepsilon = \pm 1.$$

L'unicité de la décomposition d'un entier sous la forme (4) entraîne alors l'égalité annoncée.

- 2) Il existe des entiers r et s , qui ne sont pas divisibles par p , tels que l'on ait

$$a = p^{v_p(a)} r \quad \text{et} \quad b = p^{v_p(b)} s.$$

Supposons par exemple $v_p(a) \geq v_p(b)$. On a

$$(6) \quad a + b = p^{v_p(b)} (p^{v_p(a) - v_p(b)} r + s),$$

d'où l'on déduit, d'après la première assertion, que l'on a

$$v_p(a+b) = v_p(b) + v_p(p^{v_p(a)-v_p(b)}r+s) \geq v_p(b) = \text{Min}(v_p(a), v_p(b)).$$

Supposons de plus $v_p(a) > v_p(b)$. Dans ce cas, p ne divise pas $p^{v_p(a)-v_p(b)}r+s$. D'après (6), cela conduit à l'égalité $v_p(a+b) = v_p(b)$.

3) Supposons que a divise b . Il existe $k \in \mathbb{Z}$ tel que $b = ak$. Pour tout nombre premier p , on a $v_p(b) = v_p(a) + v_p(k)$, d'où $v_p(b) \geq v_p(a)$. Inversement, d'après l'hypothèse faite, pour tout $p \in \mathbf{P}$ il existe $t_p \geq 0$ tel que l'on ait $v_p(b) = v_p(a) + t_p$. Pour presque tout p , on a $v_p(a) = v_p(b) = t_p = 0$. Posons

$$t = \prod_{p \in \mathbf{P}} p^{t_p}.$$

Pour tout $p \in \mathbf{P}$, on a donc $v_p(b) = v_p(at)$, d'où $b = \pm at$ et a divise b .

Exercice 8. Calculer $v_2(1056)$. Pour tout $p \in \mathbf{P}$ calculer $v_p(196000)$.

Définition 8.3. Soient a et b des entiers relatifs. On dit que a et b sont premiers entre eux s'il n'existe pas de nombres premiers divisant à la fois a et b , autrement dit, si pour tout nombre premier p , on a $\text{Min}(v_p(a), v_p(b)) = 0$. Dans ce cas, on dit aussi que a est premier avec b .

Théorème 8.7 (Lemme de Gauss). Soient a, b, c des entiers relatifs tels que a divise bc et que a soit premier avec b . Alors, a divise c .

Démonstration : Soit p un nombre premier. Compte tenu de l'assertion 3 de la proposition 8.1, il s'agit de démontrer que l'on a l'inégalité $v_p(a) \leq v_p(c)$. Elle est évidente si $v_p(a) = 0$. Supposons $v_p(a) \geq 1$ i.e. que p divise a . L'entier a étant premier avec b , on a alors $v_p(b) = 0$. Puisque a divise bc , on a $v_p(a) \leq v_p(bc)$, d'où $v_p(a) \leq v_p(c)$ et le résultat.

Corollaire 8.2. Soient a un entier relatif et r, s des entiers premiers entre eux. Si a est divisible par r et s , alors a est divisible par rs .

Démonstration : Il existe u et v dans \mathbb{Z} tels que l'on ait les égalités $a = ur = vs$. D'après le lemme de Gauss, r divise donc v , d'où l'assertion.

Exercice 9. Soient p et q des nombres premiers distincts. Montrer que pq divise $p^{q-1} + q^{p-1} - 1$.

4. Plus grand commun diviseur

Soient a et b des entiers relatifs non tous les deux nuls.

Théorème 8.8. Il existe un unique entier $d \geq 1$ vérifiant les deux conditions suivantes :

- 1) l'entier d est un diviseur commun à a et b .

2) Tout diviseur commun à a et b divise d .

On a l'égalité

$$(7) \quad d = \prod_{p \in \mathbf{P}} p^{\min(v_p(a), v_p(b))}.$$

Définition 8.4. L'entier d défini par l'égalité (7) est appelé le plus grand commun diviseur de a et b , ou en abrégé le pgcd de a et b . On le note $\text{pgcd}(a, b)$ ou $a \wedge b$.

Démonstration : Considérons l'entier d défini par l'égalité (7) (d est bien défini car a et b ne sont pas tous les deux nuls). Pour tout nombre premier p , $v_p(a)$ et $v_p(b)$ sont plus grands que $\min(v_p(a), v_p(b))$, donc d est un diviseur commun à a et b (assertion 3 de la prop. 8.1). Par ailleurs, si c est un diviseur commun à a et b , alors pour tout nombre premier p on a $v_p(c) \leq v_p(a)$ et $v_p(c) \leq v_p(b)$, d'où $v_p(c) \leq \min(v_p(a), v_p(b))$, donc c divise d (*loc. cit.*). Ainsi d vérifie les conditions 1 et 2. Par ailleurs, si d' est un entier naturel non nul vérifiant ces conditions, alors d divise d' et d' divise d , d'où $d = d'$.

Lemme 8.3. Les entiers $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.

Démonstration : Pour tout $p \in \mathbf{P}$, $v_p(d)$ est égal à $v_p(a)$ ou $v_p(b)$. Par ailleurs, on a $v_p(a/d) = v_p(a) - v_p(d)$ et $v_p(b/d) = v_p(b) - v_p(d)$, donc le minimum de $v_p(a/d)$ et $v_p(b/d)$ est nul, d'où le lemme.

Lemme 8.4. Les entiers a et b sont premiers entre eux si et seulement si leur pgcd est 1.

Démonstration : Les entiers a et b sont premiers entre eux si et seulement si pour tout $p \in \mathbf{P}$, on a $\min(v_p(a), v_p(b)) = 0$. D'après (7), cela est équivalent à l'égalité $\text{pgcd}(a, b) = 1$.

Exercice 10. Déterminer le pgcd de 2800 et 120.

Exercice 11. Soient a et m des entiers tels que $a \geq 2$ et $m \geq 1$. Montrer que l'on a

$$\text{pgcd}\left(\frac{a^m - 1}{a - 1}, a - 1\right) = \text{pgcd}(a - 1, m).$$

Exercice 12. Déterminer l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ pour lesquels on a l'égalité $x + y - 1 = \text{pgcd}(x, y)$.

Exercice 13. Soient a, b et c des entiers relatifs non nuls. Montrer que l'on a

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

Théorème 8.9 (Théorème de Bézout⁽⁴⁾). *Il existe des entiers relatifs u et v tels que l'on ait*

$$\text{pgcd}(a, b) = au + bv.$$

Démonstration : Considérons l'ensemble

$$A = \{au + bv \mid u, v \in \mathbb{Z}\} \cap (\mathbb{N} - \{0\}).$$

C'est une partie non vide de \mathbb{N} . Soit c son plus petit élément. On a $c \geq 1$. Vérifions que l'on a

$$(8) \quad A = \{ck \mid k \geq 1\}.$$

D'abord, c étant dans A , les éléments de la forme ck , avec $k \geq 1$, sont aussi dans A . Inversement, soit n un élément de A . D'après le théorème de la division euclidienne, il existe $q, r \in \mathbb{Z}$ tels que l'on ait $n = cq + r$ avec $0 \leq r < c$. Supposons $r \neq 0$. On a alors $r = n - cq \geq 1$. Les entiers n et c étant dans A , $n - cq$ est aussi de la forme $a\alpha + b\beta$ avec $\alpha, \beta \in \mathbb{Z}$, donc r appartient à A . Le caractère minimal de c conduit alors à une contradiction. Par suite, on a $r = 0$, puis $n = cq$ avec $q \geq 1$, d'où l'égalité (8). Démontrons alors que l'on a

$$(9) \quad \text{pgcd}(a, b) = c,$$

ce qui entraînera le résultat. Si $ab \neq 0$ les entiers $|a|$ et $|b|$ sont dans A , et d'après (8), c divise donc a et b . On a la même conclusion si $ab = 0$. Ainsi, c est un diviseur commun à a et b . Par ailleurs, il existe u et v dans \mathbb{Z} tels que $c = au + bv$, de sorte que tout diviseur commun à a et b divise c . L'égalité (9) en résulte, car c vérifie les deux conditions du théorème 8.8.

On en déduit l'énoncé suivant :

Corollaire 8.3. *Les entiers a et b sont premiers entre eux si et seulement si il existe u et v dans \mathbb{Z} tels que l'on ait $1 = au + bv$.*

Exercice 14. Pour tout $n \in \mathbb{Z}$, montrer que les entiers $5n + 2$ et $12n + 5$ sont premiers entre eux.

Remarque 8.1. On peut généraliser la notion de pgcd au cas d'une famille finie d'entiers relatifs non tous nuls, et les résultats de ce paragraphe s'étendent à cette situation.

⁽⁴⁾ Étienne Bézout fut un mathématicien français qui vécut de 1730 à 1783. Il fut chargé de l'enseignement des élèves du corps de l'artillerie. Il publia une théorie générale des équations algébriques à Paris en 1779. Outre le théorème 8.9, un autre théorème célèbre porte son nom concernant l'intersection de deux « courbes algébriques ».

Si $(x_i)_{1 \leq i \leq n}$ est une famille d'entiers relatifs non tous nuls, le pgcd des x_i est l'unique entier $d \geq 1$ tel que d divise tous les x_i et que tout diviseur commun aux x_i divise d . Pour tout nombre premier p , on vérifie que l'on a (avec la notation évidente)

$$v_p(d) = \text{Min}(v_p(x_1), \dots, v_p(x_n)).$$

On démontre que d peut s'écrire sous la forme $d = u_1x_1 + \dots + u_nx_n$ pour des entiers u_i convenablement choisis. On dit que les x_i sont premiers entre eux dans leur ensemble s'ils n'ont pas de diviseurs premiers communs, ce qui signifie que leur pgcd vaut 1. Il convient de noter que cela ne signifie pas qu'ils soient premiers entre eux deux à deux. En pratique, le calcul du pgcd d'une famille d'entiers se ramène à des calculs de pgcd de deux entiers. Par exemple, le pgcd de trois entiers non nuls a, b, c n'est autre que $(a \wedge b) \wedge c$.

5. L'algorithme d'Euclide

Considérons des entiers naturels non nuls a et b tels que $a \geq b$. On va détailler ici un algorithme, qui utilise seulement le théorème de la division euclidienne, permettant d'une part de déterminer le pgcd de a et b , et d'autre part d'expliciter une relation de Bézout entre a et b , autrement dit, de déterminer deux entiers relatifs u et v tels que l'on ait $\text{pgcd}(a, b) = au + bv$.

On construit pour cela une suite finie d'entiers naturels $(r_i)_{i \geq 0}$, que l'on appelle la suite des restes (associée à a et b), par le procédé suivant : on pose d'abord

$$r_0 = a \quad \text{et} \quad r_1 = b.$$

Supposons construits r_0, r_1, \dots, r_i où $i \geq 1$. Si $r_i \neq 0$, on définit alors r_{i+1} comme étant le reste de la division euclidienne de r_{i-1} par r_i . Si $r_i = 0$, le procédé s'arrête et la suite des restes est alors formée des entiers $r_0, r_1, \dots, r_{i-1}, r_i = 0$. Il existe un unique indice $n \geq 1$ tel que la condition suivante soit satisfaite :

$$0 < r_n < r_{n-1} < \dots < r_1 \leq r_0 \quad \text{et} \quad r_{n+1} = 0.$$

Proposition 8.2. *On a $r_n = \text{pgcd}(a, b)$.*

Démonstration : Soit i un entier tel que $1 \leq i \leq n$. Il existe $q_i \in \mathbb{Z}$ tel que l'on ait

$$(10) \quad r_{i-1} = q_i r_i + r_{i+1} \quad \text{avec} \quad 0 \leq r_{i+1} < r_i.$$

Il résulte directement du théorème 8.8 que l'on a

$$\text{pgcd}(r_{i-1}, r_i) = \text{pgcd}(r_i, r_{i+1}).$$

Par suite, on a $\text{pgcd}(a, b) = \text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2) = \dots = \text{pgcd}(r_{n-1}, r_n) = r_n$.

On a ainsi démontré que le pgcd de a et b est le dernier reste non nul r_n dans la suite des restes que l'on a construite. Il existe donc u et v dans \mathbb{Z} tels que l'on ait

$$r_n = au + bv.$$

Le problème qui nous intéresse maintenant est d'expliciter un tel couple (u, v) . On construit pour cela deux suites d'entiers $(u_i)_{0 \leq i \leq n}$ et $(v_i)_{0 \leq i \leq n}$ en posant

$$u_0 = 1, \quad u_1 = 0 \quad \text{et} \quad v_0 = 0, \quad v_1 = 1,$$

$$u_{i+1} = u_{i-1} - u_i q_i \quad \text{et} \quad v_{i+1} = v_{i-1} - v_i q_i \quad \text{pour tout } i = 1, \dots, n-1,$$

où q_i est défini par l'égalité (10), autrement dit, où q_i est le quotient de la division euclidienne de r_{i-1} par r_i .

Proposition 8.3. *On a $r_n = au_n + bv_n$.*

Démonstration : Il suffit de vérifier que pour tout i tel que $0 \leq i \leq n$, on a l'égalité $r_i = au_i + bv_i$. Elle est vraie si $i = 0$ et $i = 1$. Considérons un entier k vérifiant les inégalités $1 \leq k < n$ tel que l'on ait $r_i = au_i + bv_i$ pour tout $i \leq k$. On a alors

$$r_{k+1} = r_{k-1} - q_k r_k = (u_{k-1}a + v_{k-1}b) - q_k(u_k a + v_k b) = au_{k+1} + bv_{k+1},$$

d'où l'égalité annoncée.

Il peut être commode de présenter les étapes de calculs sous la forme du tableau suivant :

	q_1	q_2	\cdots	q_{n-1}	q_n
$r_0 = a$	$r_1 = b$	r_2	\cdots	r_{n-1}	r_n
1	0	u_2	\cdots	u_{n-1}	u_n
0	1	v_2	\cdots	v_{n-1}	v_n

Exemple 8.2. Appliquons ce qui précède au calcul du pgcd des entiers $a = 17640$ et $b = 525$. On obtient le tableau :

	33	1	1	2
17640	525	315	210	105
1	0	1	-1	2
0	1	-33	34	-67

Ainsi $105 = \text{pgcd}(a, b)$ et l'on obtient la relation de Bézout

$$2 \times 17640 - 67 \times 525 = 105.$$

Bien entendu, on peut aussi expliciter les décompositions de a et b en produit de nombres premiers. On trouve $a = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$ et $b = 3 \cdot 5^2 \cdot 7$, d'où $\text{pgcd}(a, b) = 3 \cdot 5 \cdot 7 = 105$ comme attendu (th. 8.8).

Exercice 15. Soit n un entier ≥ 1 . Déterminer le pgcd de $9n + 4$ et $2n - 1$.

Exercice 16. Soient a et b deux entiers ≥ 1 . Déterminer le pgcd de $2^a - 1$ et $2^b - 1$.

Exercice 17. Déterminer les entiers n de quatre chiffres tels que les restes des divisions euclidiennes de 21685 et 33509 par n soient respectivement 37 et 53.

6. L'équation $ax + by = c$

Soient a, b et c des entiers relatifs non nuls. On va décrire ici l'ensemble S des couples $(x, y) \in \mathbb{Z}^2$ tels que l'on ait

$$(11) \quad ax + by = c.$$

Proposition 8.4. Soit d le pgcd de a et b . Posons $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$.

- 1) L'ensemble S est non vide si et seulement si d divise c .
- 2) Supposons que d divise c . Soit (x_0, y_0) un élément de \mathbb{Z}^2 tel que $ax_0 + by_0 = c$. On a

$$S = \left\{ (x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z} \right\}.$$

Démonstration : 1) S'il existe des entiers x et y vérifiant (11), d doit diviser c vu que d est un diviseur de a et b . Inversement, supposons que d divise c . Il existe c' dans \mathbb{Z} tel que $c = dc'$. Puisque a' et b' sont premiers entre eux (lemme 8.3), il existe u et v dans \mathbb{Z} tels que $a'u + b'v = 1$ (cor. 8.3). On obtient alors l'égalité $c = a(c'u) + b(c'v)$, ce qui prouve que S n'est pas vide.

- 2) Soit (x, y) un élément de S . On a l'égalité

$$a'(x - x_0) = b'(y_0 - y).$$

Puisque a' est premier avec b' , on déduit du lemme de Gauss que a' divise $y - y_0$. Il existe donc $k \in \mathbb{Z}$ tel que l'on ait $y = y_0 - ka'$, puis $x = x_0 + kb'$. Inversement, pour tout $k \in \mathbb{Z}$, on a $a(x_0 + kb') + b(y_0 - ka') = c$, d'où le résultat.

Exercice 18. Déterminer les couples $(x, y) \in \mathbb{Z}^2$ tels que $47x + 111y = 1$.

7. Plus petit commun multiple

Soient a et b des entiers relatifs non nuls. Pour tous $x, y \in \mathbb{Z}$, notons $\text{Max}(x, y)$ le plus grand d'entre eux.

Théorème 8.10. *Il existe un unique entier $m \geq 1$ vérifiant les deux conditions suivantes :*

- 1) *l'entier m est un multiple commun à a et b .*
- 2) *Tout multiple commun à a et b est un multiple de m .*

On a l'égalité

$$(12) \quad m = \prod_{p \in \mathbf{P}} p^{\text{Max}(v_p(a), v_p(b))}.$$

Définition 8.5. *L'entier m défini par l'égalité (12) est appelé le plus petit commun multiple de a et b , ou en abrégé le ppcm de a et b . On le note $\text{ppcm}(a, b)$ ou $a \vee b$.*

Démonstration : Considérons l'entier m défini par l'égalité (12). Pour tout $p \in \mathbf{P}$, on a $\text{Max}(v_p(a), v_p(b)) \geq v_p(a), v_p(b)$. Ainsi, m est un multiple commun à a et b (prop. 8.1). Par ailleurs, si c est un multiple commun à a et b , on a pour tout $p \in \mathbf{P}$ les inégalités $v_p(c) \geq v_p(a)$ et $v_p(c) \geq v_p(b)$, d'où $v_p(c) \geq \text{Max}(v_p(a), v_p(b))$, donc c est un multiple de m (*loc. cit.*). L'entier m vérifie donc les conditions 1 et 2. Si m' est un entier ≥ 1 vérifiant ces conditions, alors m' est un multiple de m et m est un multiple de m' , d'où $m = m'$.

Exercice 19. Calculer le ppcm de 1080 et de 3600.

Proposition 8.5. *On a l'égalité $\text{pgcd}(a, b) \text{ppcm}(a, b) = |ab|$.*

Démonstration : Pour tout $p \in \mathbf{P}$, on a

$$v_p(ab) = v_p(a) + v_p(b) = \text{Max}(v_p(a), v_p(b)) + \text{Min}(v_p(a), v_p(b)).$$

Les théorèmes 8.8 et 8.10 entraînent alors le résultat.

Exercice 20.

1) Trouver tous les couples d'entiers naturels (a, b) pour lesquels on a $\text{pgcd}(a, b) = 5$ et $\text{ppcm}(a, b) = 8160$.

2) Trouver le ppcm de 666952 et de 394108.

Remarque 8.2. On peut, comme pour le pgcd, généraliser la notion de ppcm au cas d'une famille finie d'entiers. Étant donnés des entiers non nuls x_1, \dots, x_n , leur ppcm est l'unique entier $m \geq 1$ multiple des x_i , tel que tout multiple des x_i soit multiple de m . Pour tout $p \in \mathbf{P}$, on a comme attendu

$$v_p(m) = \text{Max}(v_p(x_1), \dots, v_p(x_n)).$$

Cela étant, on notera que la proposition 8.5 est fausse dans ce cadre général, ce qui s'explique par le fait que l'entier $\text{Min}(v_p(x_1), \dots, v_p(x_n)) + \text{Max}(v_p(x_1), \dots, v_p(x_n))$ n'est pas en général la somme des $v_p(x_i)$: prendre par exemple $(x_1, x_2, x_3) = (2, 3, 4)$ et $p = 2$. Le pgcd des x_i est 1, leur ppcm est 12 et leur produit vaut 24.

Exercice 21. Soient a, b et c des entiers naturels non nuls. Montrer que l'on a

$$abc = \text{pgcd}(a, b, c) \text{ ppcm}(a, b, c)$$

si et seulement si a, b et c sont premiers entre eux deux à deux.

8. Numération en base b

Considérons un entier $b \geq 2$.

Théorème 8.11. Soit x un entier naturel non nul. On peut écrire x de manière unique sous la forme

$$(13) \quad x = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0,$$

où n est un entier naturel, où a_0, \dots, a_n sont des entiers tels que $0 \leq a_i \leq b - 1$ et où a_n est non nul. On dit que $x = a_n a_{n-1} \dots a_1 a_0$ est l'écriture de x en base b et l'on écrit parfois $x = (a_n \dots a_0)_b$.

Démonstration : Démontrons l'assertion d'existence. Notons pour cela $P(x)$ la propriété : x possède une écriture de la forme (13) comme indiquée dans l'énoncé. La propriété $P(1)$ est vraie, avec $n = 0$ et $a_0 = 1$. Considérons alors un entier $x \geq 2$ et supposons que la propriété $P(k)$ soit vraie pour tout entier k tel que $1 \leq k < x$. Il s'agit de démontrer que $P(x)$ est vraie. Tel est le cas si l'on a $x < b$, en prenant $n = 0$ et $a_0 = x$ dans (13). Supposons donc $x \geq b$. Il existe des entiers q et a_0 tels que l'on ait $x = bq + a_0$ avec $0 \leq a_0 < b$. L'inégalité $x \geq b$ entraîne $q \geq 1$. Par suite, on a $q < bq \leq x$. La propriété $P(q)$ étant vraie, il existe un entier $n \geq 1$ tel que l'on ait $q = a_n b^{n-1} + \dots + a_2 b + a_1$, où les a_i sont entiers vérifiant les inégalités $0 \leq a_i \leq b - 1$ et où $a_n \neq 0$. L'égalité $x = bq + a_0$ entraîne alors que $P(x)$ est vraie, d'où l'assertion d'existence.

Prouvons l'assertion d'unicité. On remarque pour cela que l'entier n intervenant dans (13) vérifie les inégalités

$$b^n \leq x < b^{n+1}.$$

En effet, la première inégalité est immédiate et le fait que les a_i soient compris entre 0 et $b - 1$ entraîne que l'on a

$$x \leq (b - 1)(b^n + b^{n-1} + \dots + b + 1) = b^{n+1} - 1 < b^{n+1}.$$

Il en résulte que n est la partie entière de $\frac{\text{Log } x}{\text{Log } b}$. Tout revient donc à démontrer que si l'on a

$$x = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0,$$

avec $a_n c_n \neq 0$ et $0 \leq a_i, c_i \leq b-1$, alors $a_i = c_i$ pour tout i . Vu le caractère d'unicité du reste de la division euclidienne de x par b , on a $a_0 = c_0$. On obtient ensuite l'assertion en procédant par récurrence finie sur les indices des coefficients.

Exemple 8.3. On vérifie que l'on a $101 = 1 + 2^2 + 2^5 + 2^6$, de sorte que l'écriture de 101 en base 2 est 1100101 i.e. on a $101 = (1100101)_2$.

Exercice 22. Déterminer l'écriture en base 3 de 7456.

Exercice 23. Soit n un entier naturel.

- 1) Trouver une condition nécessaire et suffisante simple pour que n soit divisible par 3, respectivement par 9.
- 2) Soit $n = (a_k a_{k-1} \cdots a_1 a_0)_{10}$ l'écriture de n en base 10. Montrer l'équivalence

$$n \text{ est divisible par } 11 \iff \sum_{i=0}^k (-1)^i a_i \equiv 0 \pmod{11}.$$

Exercice 24. Déterminer les nombres de deux chiffres qui s'écrivent uv en base 10 et vu en base 7.

Donnons deux applications de ce théorème.

1. Calcul «rapide» de la puissance d'un entier

L'existence de l'écriture en base 2 des entiers permet d'accélérer le calcul de la puissance d'un entier. Plus précisément, considérons deux entiers $x \geq 1$ et $n \geq 1$. Afin de calculer x^n , il faut a priori effectuer $n-1$ multiplications. En fait, la détermination de l'écriture de n en base 2 permet de calculer x^n en effectuant au plus la partie entière de

$$\frac{2 \text{Log } n}{\text{Log } 2}$$

multiplications. En effet, soit

$$n = 2^{i_k} + 2^{i_{k-1}} + \cdots + 2^{i_1} + 2^{i_0},$$

le développement de n en base 2 avec $i_0 < i_1 < \cdots < i_k$. On a l'égalité

$$x^n = x^{2^{i_k}} \times x^{2^{i_{k-1}}} \times \cdots \times x^{2^{i_1}} \times x^{2^{i_0}}.$$

On peut effectuer le calcul de $x^{2^{i_k}}$ avec i_k multiplications, ce qui fournit aussi le calcul des autres termes $x^{2^{i_j}}$ pour $0 \leq j \leq k$. Il en résulte que l'on peut calculer x^n avec $i_k + k$ multiplications. Par ailleurs, on a

$$k \leq i_k \quad \text{et} \quad 2^{i_k} \leq n \quad \text{i.e.} \quad i_k \leq \frac{\text{Log } n}{\text{Log } 2}.$$

Par suite, on a

$$i_k + k \leq \frac{2 \text{Log } n}{\text{Log } 2},$$

d'où notre assertion.

Exemple 8.4. On a vu plus haut que l'on a $101 = 2^6 + 2^5 + 2^2 + 1$. Le calcul de x^{101} peut donc se faire avec neuf multiplications, au lieu de cent a priori.

2. Formule de Legendre⁽⁵⁾ donnant $v_p(n!)$

Soient n un entier naturel non nul et p un nombre premier. On se propose de déterminer ici la valuation p -adique de $n!$. On va démontrer le résultat suivant, qui a été obtenu par Legendre en 1808 :

Théorème 8.12. Soit $n = (a_k \cdots a_0)_p$ l'écriture de n en base p . On a

$$(14) \quad v_p(n!) = \frac{n - S}{p - 1} \quad \text{où} \quad S = \sum_{i=0}^k a_i.$$

Démonstration : Pour tout $x \in \mathbb{R}$, notons $[x]$ la partie entière de x .

Lemme 8.5. Soient a et b des entiers ≥ 1 . On a

$$\left[\frac{a+1}{b} \right] - \left[\frac{a}{b} \right] = \begin{cases} 1 & \text{si } b \text{ divise } a+1 \\ 0 & \text{sinon.} \end{cases}$$

Démonstration : Il existe des entiers q et r tels que l'on ait

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b.$$

On a en particulier

$$\left[\frac{a}{b} \right] = q \quad \text{et} \quad a+1 = bq + (r+1) \quad \text{avec} \quad r+1 \leq b.$$

⁽⁵⁾ Adrien-Marie Legendre est né à Paris en 1752 et décède en 1833. Il fut professeur à l'École Militaire de Paris de 1775 à 1780. Il apporta sa contribution mathématique dans de nombreux domaines, notamment au calcul intégral, à la théorie des fonctions elliptiques ainsi qu'à la théorie des nombres.

On en déduit que b divise $a + 1$ si et seulement si $b = r + 1$. Si b divise $a + 1$, on a donc $a + 1 = b(q + 1)$, d'où

$$\left[\frac{a + 1}{b} \right] = q + 1,$$

et l'on obtient dans ce cas l'égalité annoncée. Si b ne divise pas $a + 1$, on a $r + 1 < b$, d'où

$$\left[\frac{a + 1}{b} \right] = q.$$

et le résultat.

Pour tout entier $N \geq 1$, posons

$$S_N = \sum_{i \geq 1} \left[\frac{N}{p^i} \right].$$

Il s'agit d'une somme finie car $\left[\frac{N}{p^i} \right]$ est nul dès que i est assez grand.

Corollaire 8.4. *Pour tout entier $N \geq 1$, on a $v_p(N!) = S_N$.*

Démonstration : On procède par récurrence sur N . Le résultat est vrai si $N = 1$. Supposons que ce soit le cas pour un entier $N \geq 1$. D'après le lemme 8.5, on a

$$\left[\frac{N + 1}{p^i} \right] - \left[\frac{N}{p^i} \right] = \begin{cases} 1 & \text{si } i \leq v_p(N + 1) \\ 0 & \text{sinon.} \end{cases}$$

On obtient les égalités

$$(15) \quad S_{N+1} - S_N = \sum_{1 \leq i \leq v_p(N+1)} 1 = v_p(N + 1).$$

Par ailleurs, on a

$$v_p((N + 1)!) = \sum_{j=1}^{N+1} v_p(j) = v_p(N!) + v_p(N + 1).$$

En utilisant l'hypothèse de récurrence, on obtient ainsi

$$v_p((N + 1)!) = S_N + v_p(N + 1),$$

qui d'après (15) implique $v_p((N + 1)!) = S_{N+1}$.

Fin de la démonstration du théorème : On a l'égalité

$$n = a_k p^k + \cdots + a_1 p + a_0 \quad \text{avec} \quad 0 \leq a_i < p.$$

Considérons un entier j tel que $1 \leq j \leq k$. On a

$$\frac{n}{p^j} = a_k p^{k-j} + \cdots + a_j + \frac{a_{j-1} p^{j-1} + \cdots + a_1 p + a_0}{p^j}.$$

Par ailleurs, on a

$$a_{j-1} p^{j-1} + \cdots + a_1 p + a_0 \leq (p-1)(p^{j-1} + \cdots + 1) = p^j - 1 < p^j.$$

Il en résulte que l'on a

$$(16) \quad \left[\frac{n}{p^j} \right] = a_k p^{k-j} + \cdots + a_j.$$

L'inégalité $n < p^{k+1}$ entraîne

$$\left[\frac{n}{p^i} \right] = 0 \quad \text{pour tout } i \geq k+1.$$

D'après le corollaire 8.4, on a donc

$$v_p(n!) = \sum_{j=1}^k \left[\frac{n}{p^j} \right].$$

On déduit alors de (16) l'égalité

$$v_p(n!) = a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots + a_k(p^{k-1} + p^{k-2} + \cdots + p + 1),$$

autrement dit,

$$v_p(n!) = \frac{1}{p-1} \left(a_1(p-1) + a_2(p^2-1) + a_3(p^3-1) + \cdots + a_k(p^k-1) \right) = \frac{n-S}{p-1},$$

ce qui établit la formule (14).

Exemple 8.5. On a $100 = 2^2 + 2^5 + 2^6 = 4.5^2$, autrement dit, $100 = (1100100)_2$ et $100 = (400)_5$. On a donc $v_2(100!) = 97$ et $v_5(100!) = 24$. Il en résulte que $100!$ se termine par vingt-quatre zéros dans son écriture en base 10.