24

Nombres premiers

L'ensemble $\mathcal{D}_n$ des diviseurs dans $\mathbb{N}^*$ d'un entier $n \geq 2$ contient toujours 1 et n, il est donc de cardinal supérieur ou égal à 2. On s'intéresse ici aux entiers $p \geq 2$ tels que $\mathcal{D}_p$ soit de cardinal minimal, à savoir 2.

24.1 L'ensemble $\mathcal{P}$ des nombres premiers

Définition 24.1 *On dit qu'un entier naturel p est premier s'il est supérieur ou égal à 2 et si les seuls diviseurs positifs de p sont 1 et p.*

Remarque 24.1 *0 et 1 ne sont pas premiers et 2 est le seul nombre pair qui est premier.*

On note $\mathcal{P}$ l'ensemble de tous les nombres premiers.

Exemple 24.1 *$n = 111111$ est non premier (la somme des chiffres de n est égale à 6, donc n est divisible par $3 < n$).*

Exemple 24.2 *Les nombres de Fermat sont les entiers de la forme $F_n = 2^{2^n} + 1$ où n est un entier naturel.*
Ces entiers sont premiers pour $n = 0, 1, 2, 3, 4$, mais pas pour $n = 5$ ou $n = 6$.
L'instruction Maple :
for n from 1 to 6 do factorset(2^(2^n)+1) od;
nous donne :
{5}, {17}, {257}, {65537}, {6700417, 641}, {67280421310721, 274177}
soit pour $n = 5$ et $n = 6$:

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417 = \left(2^7 \cdot 5 + 1\right)\left(2^7 \cdot 3 \cdot 17449 + 1\right),$$

$$\begin{aligned} F_6 &= 2^{2^6} + 1 = 18446744073709551617 = 274177 \times 67280421310721 \\ &= \left(2^8 \cdot 3^2 \cdot 7 \cdot 17 + 1\right)\left(2^8 \cdot 5 \cdot 47 \cdot 373 \cdot 2998279 + 1\right). \end{aligned}$$

Euler (sans l'aide de Maple) avait montré que F_5 n'est pas premier.

Le résultat qui suit se déduit du fait que toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Théorème 24.1 (Euclide) *Tour entier n supérieur ou égal à 2 a au moins un diviseur premier.*

Démonstration. Pour tout entier $n \geq 2$ l'ensemble $\mathcal{D}_n$ des diviseurs strictement positifs de n a au moins deux éléments, 1 et n, donc $\mathcal{D}_n \setminus \{1\}$ est non vide dans $\mathbb{N} \setminus \{0,1\}$ et il admet un plus petit élément p qui est nécessairement premier. En effet si p n'est pas premier il admet un diviseur q tel que $2 \leq q < p$ avec q qui divise n, ce qui contredit le caractère minimal de p. ∎

Corollaire 24.1 *Tout entier relatif $n \in \mathbb{Z} \setminus \{-1,0,1\}$ a au moins un diviseur premier.*

Démonstration. Tout diviseur premier de $|n| \geq 2$ convient. ∎

Un entier naturel non premier s'écrit donc $n = pq$ avec $p \geq 2$ premier et $q \geq 2$. On dit alors qu'il est composé.

Exercice 24.1 *Soit $b \geq 3$ une base de numération. Montrer que $n = \overline{12\cdots21}^b$, où le chiffre 2 est répété $p \geq 2$ fois, est non premier.*

Solution 24.1 *On a :*

$$\begin{aligned} n &= 1 + 2b + \cdots + 2b^p + b^{p+1} \\ &= 1 + 2b\frac{b^p - 1}{b-1} + b^{p+1} \\ &= \frac{b^{p+2} + b^{p+1} - b - 1}{b-1} = \frac{(b^{p+1}-1)(b+1)}{b-1} \\ &= (b+1)\left(1 + b + \cdots + b^{p-1} + b^p\right) \end{aligned}$$

les deux termes de ce produit étant ≥ 2, donc n n'est pas premier.

Exercice 24.2 *Soient $a \geq 2$ et $m \geq 2$ deux entiers et $p = a^m - 1$. Montrer que si p est premier alors $a = 2$ et m est premier. La réciproque est-elle vraie ? On appelle nombre de Mersenne tout entier de la forme $2^m - 1$. Le plus grand nombre premier connu à ce jour (16 septembre 2006) est le nombre premier de Mersenne : $2^{32582657} - 1$.*

Solution 24.2 *Supposons que p soit premier. On a :*

$$p = a^m - 1 = (a-1)\sum_{k=0}^{m-1} a^k = (a-1)\,q$$

Si $a > 2$, on a $a - 1 \geq 2$ et $q \geq 2$ puisque $m \geq 2$ et p ne peut être premier. On a donc nécessairement $a = 2$ et $p = 2^m - 1$. Si m n'est pas premier, il s'écrit $m = ab$ avec $a \geq 2$, $b \geq 2$ et :

$$p = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)\sum_{k=0}^{b-1} (2^a)^k = (2^a - 1)\,q$$

avec $2^a - 1 \geq 2$ (puisque $2^a \geq 4$) et $q \geq 2$ (puisque $b \geq 2$) et p ne peut être premier. L'entier m est donc nécessairement premier.
Pour $m = 2, 3, 5, 7$, on a $p = 3, 7, 31, 127$ qui sont premiers et pour $m = 11$, on a $p = 2^{11} - 1 = 2047 = 23 \times 89$. La réciproque est donc fausse.

Un diviseur premier de $n \geq 2$ est nécessairement inférieur ou égal à n. En fait, pour n non premier, on peut toujours en trouver un qui est inférieur ou égal à $\sqrt{n}$, c'est $p = \min(\mathcal{D}_n \setminus \{1\})$.

Théorème 24.2 *Tout entier n supérieur ou égal à 2 qui est composé a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.*

Démonstration. En supposant n composé et en gardant les notations de la démonstration du théorème précédent, on a vu que $p = \min(\mathcal{D}_n \setminus \{1\})$ est un diviseur premier de n. On a donc $n = pq$ avec $2 \leq q \leq n$ (on a $q \neq 1$ puisque n n'est pas premier) et $q \in \mathcal{D}_n \setminus \{1\}$, ce qui implique que $p \leq q$ et $p^2 \leq pq = n$, soit $p \leq \sqrt{n}$.

On peut aussi montrer ce résultat par récurrence sur $n \geq 4$.

$p = 2$ divise $n = 4$.

Supposons le résultat acquis pour tous les entiers composés compris entre 2 et $n-1 \geq 4$. Si n est premier, il n'y a rien à montrer, sinon il existe deux entiers a et b compris entre 2 et $n-1$ tels que $n = ab$ et comme ces deux entiers jouent des rôles symétriques, on peut supposer que $a \leq b$. Si a est premier, c'est alors un diviseur premier de n tel que $a^2 \leq ab \leq n$, sinon il admet un diviseur premier $p \leq \sqrt{a}$ et p divise aussi n avec $p \leq \sqrt{n}$. ∎

Le théorème précédent nous donne un premier algorithme, relativement simple, permettant de savoir si un entier $n \geq 2$ est premier ou non : on effectue successivement la division euclidienne de n par tous les entiers $p \leq \sqrt{n}$: si l'une de ces divisions donne un reste nul, alors n n'est pas premier, sinon, n est premier.

Une petite amélioration peut être apportée à cet algorithme en remarquant que si 2 ne divise pas n, il est inutile de tester les divisibilités par les entiers $p \leq \sqrt{n}$ pairs.

Pour tester la divisibilité de n par les nombres premiers $p \leq \sqrt{n}$, on doit disposer de la liste de tous ces nombres premiers. Le crible d'Eratosthène nous permet d'obtenir une telle liste. Le principe est le suivant :

- on se donne la liste de tous les entiers compris entre 2 et m (m est la partie entière de $\sqrt{n}$ pour l'algorithme précédent) ;
- on garde 2 et on supprime tous les autres multiples de 2 de cette liste ;
- le premier entier strictement supérieur à 2 est 3 et comme il ne possède pas de diviseur strict, il est premier, on le garde et on supprime tous les autres multiples de 3 de la liste ;
- on continue ainsi de suite et on s'arrête dès que l'on tombe sur un nombre premier strictement plus grand que $\sqrt{m}$. La liste finale contient alors tous les nombres premiers inférieurs à m.

Par exemple pour $m = 25$, on a la séquence suivante :

- $L_0 = (2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25)$;
- 2 est premier et on supprime de L_0 tous les multiples de 2 qui sont différents de 2, ce qui donne la liste $L_1 = (\mathbf{2}, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25)$;
- 3 est nécessairement premier et en supprimant de L_1 tous les multiples de 3 qui sont différents de 3, on obtient la liste $L_2 = (\mathbf{2}, \mathbf{3}, 5, 7, 11, 13, 17, 19, 23, 25)$;
- 5 est nécessairement premier et en supprimant de L_2 tous les multiples de 5 qui sont différents de 5, on obtient la liste $L_3 = (\mathbf{2}, \mathbf{3}, \mathbf{5}, 7, 11, 13, 17, 19, 23)$;
- 7 est nécessairement premier et en supprimant de L_3 tous les multiples de 7 qui sont différents de 7, on obtient la liste $L_4 = (\mathbf{2}, \mathbf{3}, \mathbf{5}, \mathbf{7}, \mathbf{11}, \mathbf{13}, \mathbf{17}, \mathbf{19}, \mathbf{23})$. Tous les éléments de cette liste sont premiers puisque $7 > \sqrt{25}$.

Les résultats qui suivent sont élémentaires, mais souvent utiles.

Lemme 24.1 *Soit p un entier naturel premier. Pour tout entier naturel non nul n, on a soit p qui divise n, soit p qui est premier avec n.*

Démonstration. Comme $\delta = p \wedge n$ divise p, on a soit $\delta = p$ et p divise n, soit $\delta = 1$ et p est premier avec n. ∎

Lemme 24.2 *Deux nombres premiers distincts sont premiers entre eux.*

Démonstration. Soient p, q deux nombres premiers. Si $\delta = p \wedge q \neq 1$, le lemme précédent nous dit que p divise q et q divise p, donc $p = q$. ∎

Lemme 24.3 *Un entier $p \geq 2$ est premier si, et seulement si, il est premier avec tout entier compris entre 1 et $p-1$.*

Démonstration. Si p est premier, comme il ne divise pas $k \in \{1, \cdots, p-1\}$, il est premier avec k.

Réciproquement si p n'est pas premier, il s'écrit alors $p = ab$ avec $a \geq 2$, $b \geq 2$ et p n'est pas premier avec $a \in \{2, \cdots, p-1\}$. ■

Le théorème de Gauss nous donne le résultat suivant qui nous sera utile pour prouver l'unicité (à l'ordre près) de la décomposition en facteurs premiers d'un entier $n \geq 2$.

Lemme 24.4 *Soit p un nombre premier et r un entier naturel supérieur ou égal à 2. Si p divise le produit $n_1 n_2 \cdots n_r$ de r entiers naturels non nuls, alors p divise l'un des n_k.*

Démonstration. On procède par récurrence sur $n \geq 2$.

Si p divise $n_1 n_2$, on a soit p qui divise n_1, soit p qui est premier avec n_1 et il va alors diviser n_2 (théorème de Gauss).

Supposons le résultat acquis au rang $n-1 \geq 2$. Si p divise $n_1 n_2 \cdots n_r$, on a soit p qui divise n_1, soit p qui est premier avec n_1 et il va alors diviser $n_2 \cdots n_r$ et l'un des n_k où k est compris entre 2 et n. ■

Dans le cas où tous les n_k sont égaux à un même entier n, on a :

$$(p \text{ premier divise } n^r) \Rightarrow (p \text{ divise } n)$$

Exercice 24.3 *Soient $p \geq 2$ un nombre premier et n, m des entiers naturels non nuls. Montrer que p divise n ou p^m est premier avec n.*

Solution 24.3 *Si p divise n c'est fini. Sinon p est premier avec n et le théorème de Bézout nous dit qu'il existe deux entiers relatifs u et v tels que $up + vn = 1$. On a alors $1 = (up + vn)^m = u^n p^n + v_n n$, ce qui signifie que p^n et n sont premiers entre eux.*

Exercice 24.4 *Soient a et b deux entiers relatifs non nuls. Montrer que :*

$$\left(a^2 + b^2\right) \wedge (ab) = (a \wedge b)^2 .$$

Solution 24.4 *Soient $\delta = a \wedge b$ et p, q premiers entre eux tels que $a = \delta p$ et $b = \delta q$. On a :*

$$\begin{aligned} \delta' &= \left(a^2 + b^2\right) \wedge (ab) = \left(\delta^2 \left(p^2 + q^2\right)\right) \wedge \left(\delta^2 (pq)\right) \\ &= \delta^2 \left(\left(p^2 + q^2\right) \wedge (pq)\right) . \end{aligned}$$

Il s'agit alors de montrer que $\delta' = (p^2 + q^2) \wedge (pq) = 1$ si $p \wedge q = 1$ (on s'est ramené en fait au cas où a et b sont premiers entre eux). Supposons que $\delta' \geq 2$, il admet alors un diviseur premier $d \geq 2$ et d qui divise pq (pq est multiple de δ') va diviser p ou q. Mais d divise p entraîne d divise p^2 avec d diviseur de $p^2 + q^2$ ($p^2 + q^2$ est multiple de δ'), donc d premier divise q^2, il divise donc q, ce qui est impossible (p et q premiers entre eux ne peuvent avoir $d \geq 2$ comme diviseur commun). Comme p et q jouent des rôles analogues, d ne divise pas q. On a donc nécessairement $\delta' = 1$.

Exercice 24.5 *Soient a et b deux entiers relatifs non nuls et n un entier naturel non nul. Montrer que :*

$$a^n \wedge b^n = (a \wedge b)^n \quad \text{et} \quad a^n \vee b^n = (a \vee b)^n .$$

Solution 24.5 *Soient $\delta = a \wedge b$ et p, q premiers entre eux tels que $a = \delta p$ et $b = \delta q$. On a :*

$$a^n \wedge b^n = (\delta^n p^n) \wedge (\delta^n q^n) = \delta^n (p^n \wedge q^n)$$

et $(a \wedge b)^n = \delta^n$. Il s'agit alors de montrer que $\delta' = p^n \wedge q^n = 1$ si $p \wedge q = 1$ (on s'est ramené en fait au cas où a et b sont premiers entre eux). Supposons que $\delta' \geq 2$, il admet alors un diviseur premier $d \geq 2$ et d qui divise p^n et q^n va diviser p et q ce qui est impossible. On a donc nécessairement $\delta' = 1$.
Pour ce qui est du ppcm, *on a :*

$$a^n \vee b^n = \frac{|a|^n |b|^n}{a^n \wedge b^n} = \frac{(|a|\,|b|)^n}{(a \wedge b)^n} = (a \vee b)^n .$$

Par exemple, on a :

$$125 \wedge 27 = 5^3 \wedge 3^3 = 5 \wedge 3 = 1.$$

On peut déduire de l'exercice précédent que deux entiers relatifs non nuls a et b sont premiers entre eux si, et seulement si, a^n et b^n sont premiers entre eux, quel que soit l'entier $n \geq 1$.

Exercice 24.6 *Soient a, b, c, d des entiers relatifs non nuls. Montrer que si $a \wedge b = c \wedge d = 1$, alors $(ac) \wedge (bd) = (a \wedge d)(b \wedge c)$.*

Solution 24.6 *En notant $\delta_1 = a \wedge d$ et $\delta_2 = b \wedge c$, on a $a = \delta_1 p_1$, $d = \delta_1 q_1$, $b = \delta_2 p_2$ et $c = \delta_2 q_2$ avec $p_1 \wedge q_1 = p_2 \wedge q_2 = 1$, ce qui donne :*

$$(ac) \wedge (bd) = \delta_1 \delta_2 ((p_1 q_2) \wedge (p_2 q_1)) .$$

Si $\delta' = ((p_1 q_2) \wedge (p_2 q_1)) \geq 2$, il admet alors un diviseur premier p qui divise $p_1 q_2$ et $p_2 q_1$ et on a quatre possibilités :

- *soit p divise p_1 et q_1, ce qui est impossible puisque $p_1 \wedge q_1 = 1$;*
- *soit p divise q_2 et p_2, ce qui est impossible puisque $p_2 \wedge q_2 = 1$;*
- *soit p divise p_1 et p_2 et il divise alors a et b ce qui est impossible puisque $a \wedge b = 1$;*
- *soit p divise q_2 et q_1 et il divise alors c et d ce qui est impossible puisque $c \wedge d = 1$.*

La seule possibilité est donc $\delta' = 1$.

24.2 L'ensemble $\mathcal{P}$ des nombres premiers est infini

On peut montrer de nombreuses manières que l'ensemble $\mathcal{P}$ des nombres premiers est infini.

La démonstration élémentaire qui suit, conséquence de l'existence de diviseurs premiers pour $n \geq 2$, est due à Euclide.

Théorème 24.3 (Euclide) *L'ensemble $\mathcal{P}$ des nombres premiers est infini.*

Démonstration. On sait déjà que $\mathcal{P}$ est non vide (il contient 2). Supposons que $\mathcal{P}$ soit fini avec :

$$\mathcal{P} = \{p_1, \cdots, p_r\} .$$

L'entier $n = p_1 \cdots p_r + 1$ qui est supérieur 2 admet un diviseur premier $p_k \in \mathcal{P}$. L'entier p_k divise alors $n = p_1 \cdots p_r + 1$ et $p_1 \cdots p_r$, il divise donc la différence qui est égale à 1, ce qui est impossible. En conclusion $\mathcal{P}$ est infini. ∎

Remarque 24.2 *En rangeant les nombres premiers dans l'ordre croissant, on constate que les entiers* $n_r = p_1 \cdots p_r + 1$ *sont premiers pour* r *compris entre* 1 *et* 5 *(*$n_1 = 3$, $n_2 = 7$, $n_3 = 31$, $n_4 = 211$, $n_5 = 2311$*). Pour* $r = 6$, $n_6 = 30\,031 = 59 \times 509$ *n'est pas premier. On ne sait pas si la suite* $(n_r)_{r \geq 1}$ *contient une infinité de nombres premiers.*

Exercice 24.7 *Montrer que pour tout entier naturel* n*, on peut trouver un nombre premier* p *plus grand que* n*. Conclure.*

Solution 24.7 *Pour tout* $n \in \mathbb{N}$*, l'entier* $m = n! + 1 \geq 2$ *admet un diviseur premier* p_n*. Si* $p_n < n$ *alors* p_n *est un diviseur de* $n!$*, donc de* $1 = m - n!$*, ce qui est impossible. On peut donc construire une suite strictement croissante* $(p_n)_{n \in \mathbb{N}}$ *de nombres premiers, ce qui implique que* $\mathcal{P}$ *est infini.*

Exercice 24.8 *On note :*

$$\mathcal{P}_1 = \{p \in \mathcal{P} \mid \exists n \in \mathbb{N} \ ; \ p = 4n + 3\}$$
$$\mathcal{P}_2 = \{p \in \mathcal{P} \mid \exists n \in \mathbb{N} \ ; \ p = 6n + 5\}$$

Montrer, en s'inspirant de la démonstration du théorème d'Euclide, que $\mathcal{P}_1$ *[resp.* $\mathcal{P}_2$*] est infini et conclure.*

Solution 24.8 *On remarque qu'un nombre premier différent de* 2 *est nécessairement impair et son reste dans la division euclidienne par* 4 *[resp. par* 6*] ne peut être que* 1 *ou* 3 *[resp.* $1, 3$ *ou* 5*].*
Supposons que $\mathcal{P}_1$ *[resp.* $\mathcal{P}_2$*] soit fini et notons* $p_1 = 3$ *[resp.* $p_1 = 5$*]* $< p_2 < \cdots < p_r$ *tous ses éléments. L'entier :*

$$m = 4p_1 \cdots p_r - 1 = 4\left(p_1 \cdots p_r - 1\right) + 3$$
$$\textit{resp. } m = 6p_1 \cdots p_r - 1 = 6\left(p_1 \cdots p_r - 1\right) + 5$$

qui est de la forme $4n + 3$ *[resp.* $6n + 5$*] avec* $n \geq 2$ *n'est pas premier puisque strictement supérieur à tous les* p_k *pour* k *compris entre* 1 *et* r *(*$m > 4p_k - 1 > p_k$ *puisque* $p_k \geq 3$*) [resp.* $m > 6p_k - 1 > p_k$ *puisque* $p_k \geq 5$*]. Comme* m *est impair [resp. impair non multiple de* 3 *puisque congru à* 5 *modulo* 3*] ses diviseurs premiers sont de la forme* $4k + 1$ *avec* $k \in \mathbb{N}^*$ *ou* $4k + 3$ *avec* $k \in \mathbb{N}$ *[resp.* $6k + 1$ *avec* $k \in \mathbb{N}^*$ *ou* $6k + 5$ *avec* $k \in \mathbb{N}$*] et ils ne peuvent pas être tous de la forme* $4k + 1$ *[resp.* $6k + 1$*] sans quoi* m *serait aussi de cette forme, donc congru à* 1 *modulo* 4 *[resp. modulo* 6*] ce qui contredit le fait qu'il est congru à* 3 *[resp. à* 5*] (ou à* -1*) modulo* 4 *[resp. modulo* 6*]. L'entier* m *a donc un diviseur* p_k *dans* $\mathcal{P}_1$ *[resp. dans* $\mathcal{P}_2$*] et comme* p_k *divise* $p_1 \cdots p_r$*, il va aussi diviser* -1*, ce qui est impossible avec* p_k *premier. L'ensemble* $\mathcal{P}_1$ *[resp.* $\mathcal{P}_2$*] est donc infini.*
De $\mathcal{P}_1 \subset \mathcal{P}$ *[resp.* $\mathcal{P}_2 \subset \mathcal{P}$*] on déduit que* $\mathcal{P}$ *est infini.*

Remarque 24.3 *De manière plus générale on peut montrer que si* a *et* b *sont deux entiers premiers entre eux alors il existe une infinité de nombres premiers de la forme* $an + b$ *(théorème de Dirichlet).*

Pour tout réel $x \geq 2$, on désigne par $\pi(x)$ le cardinal de l'ensemble des nombres premiers contenus dans l'intervalle $[0, x]$, soit :

$$\pi(x) = \operatorname{card}\left(\mathcal{P} \cap [0, x]\right)$$

Du théorème d'Euclide on déduit que :

$$\lim_{x\to+\infty} \pi(x) = +\infty.$$

Le théorème des nombres premiers (conjecturé par Gauss, puis montré par Hadamard et de la Vallée-Poussin) nous dit plus précisément que :

$$\pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\ln(x)}.$$

En désignant par li la fonction logarithme intégral définie par :

$$\forall x \geq e,\ \mathrm{li}(x) = \int_e^x \frac{dt}{\ln(t)}$$

on a aussi :

$$\pi(x) \underset{x\to+\infty}{\sim} \mathrm{li}(x).$$

Exercice 24.9 *Montrer que* $\mathrm{li}(x) \underset{x\to+\infty}{\sim} \dfrac{x}{\ln(x)}$.

Solution 24.9 *Une intégration par parties donne :*

$$\mathrm{li}(x) = \left[\frac{t}{\ln(t)}\right]_e^x + \int_e^x \frac{dt}{\ln^2(t)} = \frac{x}{\ln(x)} - 1 + \int_e^x \frac{dt}{\ln^2(t)}$$

avec :

$$\begin{aligned}\varphi(x) = \int_e^x \frac{dt}{\ln^2(t)} &= \int_e^{\sqrt{x}} \frac{dt}{\ln^2(t)} + \int_{\sqrt{x}}^x \frac{dt}{\ln^2(t)} \\ &\leq \frac{\sqrt{x}-e}{\ln^2(e)} + 4\frac{x-\sqrt{x}}{\ln^2(x)} \leq \sqrt{x} + 4\frac{x}{\ln^2(x)}\end{aligned}$$

(pour $t \geq \sqrt{x}$*, on a* $\ln(t) \geq \ln(\sqrt{x}) = \dfrac{\ln(x)}{2}$*) et :*

$$0 < \frac{\varphi(x)}{\frac{x}{\ln(x)}} \leq \frac{\ln(x)}{\sqrt{x}} + \frac{4}{\ln(x)} \underset{x\to+\infty}{\to} 0$$

ce qui donne l'équivalence $\mathrm{li}(x) \underset{x\to+\infty}{\sim} \dfrac{x}{\ln(x)}$.

Les exercices qui suivent nous donne une première idée de la répartition des nombres premiers.

Exercice 24.10 *On note :*

$$2 = p_1 < p_2 < \cdots < p_n < p_{n+1} < \cdots$$

la suite infinie des nombres premiers rangée dans l'ordre croissant.

1. *Montrer que :*
$$\forall n \geq 1,\ 2n-1 \leq p_n \leq 2^{2^{n-1}}.$$
2. *En déduire que* $\pi(x) > \ln(\ln(x))$.

Solution 24.10

1. *On procède par récurrence sur $n \geq 1$.*
   Pour $n = 1$ et $n = 2$, le résultat est évident.
   On le suppose acquis pour tout entier k compris entre 1 et $n \geq 2$. Comme pour $n \geq 2$, p_n est impair, l'entier $p_n + 1$ est pair donc non premier et $p_{n+1} \geq p_n + 2$. Avec l'hypothèse de récurrence, on déduit donc que :

   $$p_{n+1} \geq p_n + 2 \geq 2n + 1.$$

   Si p est un diviseur premier du produit $p_1 \cdots p_n + 1$, on a nécessairement $p \geq p_{n+1}$ (sinon $p = p_k$ où k est compris entre 1 et n, donc p divise $p_1 \cdots p_n$ et 1, ce qui est impossible). On a donc :

   $$p_{n+1} \leq p \leq p_1 \cdots p_n + 1 \leq 2^1 \cdots 2^{2^{n-1}} + 1,$$

   soit :

   $$p_{n+1} \leq 2^{1+2+\cdots+2^{n-1}} + 1 = 2^{2^n-1} + 1 \leq 2^{2^n}.$$

2. *Pour tout réel $x \geq 2$, la partie entière m de $\ln(\ln(x))$ est telle que :*

   $$-1 \leq m \leq \ln(\ln(x)) < m + 1$$

   et l'entier naturel $n = m + 1$ est tel que :

   $$n - 1 \leq \ln(\ln(x)) < n$$

   ce qui équivaut à :

   $$e^{e^{n-1}} \leq x < e^{e^n}$$

   La fonction π étant croissante, on a :

   $$n = \pi(p_n) \leq \pi\left(2^{2^{n-1}}\right) \leq \pi\left(e^{2^{n-1}}\right) \leq \pi(x)$$

   soit :

   $$\pi(x) \geq n > \ln(\ln(x))$$

Exercice 24.11 *Montrer que pour tout entier naturel $n \geq 2$, on peut trouver n entiers naturels consécutifs non premiers (la distribution des nombres premiers n'est pas régulière).*

Solution 24.11 *Les n entiers $m_k = (n+1)! + k$ où k est compris entre 2 et $n + 1$ sont non premiers puisque m_k est divisible par k qui est compris entre 2 et $n + 1 < m_k$.*

24.3 Décomposition en facteurs premiers

Le théorème qui suit est parfois appelé « théorème fondamental de l'arithmétique ».

Théorème 24.4 *Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme :*

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha r}, \tag{24.1}$$

où les p_k sont des nombres premiers vérifiant :

$$2 \leq p_1 < p_2 < \cdots < p_r$$

et les α_k sont des entiers naturels non nuls.

Démonstration. On démontre tout d'abord l'existence d'une telle décomposition par récurrence sur $n \geq 2$.

Pour $n = 2$, on a déjà la décomposition.

Supposons le résultat acquis pour tout entier k compris entre 2 et $n \geq 2$. Si $n+1$ est premier, on a déjà la décomposition, sinon on écrit $n+1 = ab$ avec a et b compris entre 2 et n et il suffit d'utiliser l'hypothèse de récurrence pour a et b.

L'unicité d'une telle décomposition peut aussi se montrer par récurrence sur $n \geq 2$. Le résultat est évident pour $n = 2$. Supposons le acquis pour tout entier k compris entre 2 et $n \geq 2$. Si $n+1$ a deux décompositions :

$$n+1 = p_1^{\alpha_1} \cdots p_r^{\alpha r} = q_1^{\beta_1} \cdots q_s^{\beta s},$$

où les p_j [resp. q_i] sont premiers deux à deux distincts et les α_j [resp. β_i] entiers naturels non nuls. L'entier p_1 est premier et divise le produit $q_1^{\beta_1} \cdots q_s^{\beta s}$, il divise donc nécessairement l'un des q_k. L'entier q_k étant également premier la seule possibilité est $p_1 = q_k$. En simplifiant par p_1 on se ramène à la décomposition d'un entier inférieur ou égal à n et il suffit alors d'utiliser l'hypothèse de récurrence pour conclure. ∎

L'écriture (24.1) est la décomposition en facteurs premiers de l'entier n.

Le théorème précédent se traduit en disant que l'anneau $\mathbb{Z}$ des entiers relatifs est factoriel.

En fait, de manière plus générale, on peut montrer qu'un anneau euclidien (c'est le cas de $\mathbb{Z}$ ou de $\mathbb{K}[x]$) est principal et en conséquence factoriel.

L'unicité dans la décomposition en facteurs premiers peut être utilisée pour montrer que $\mathbb{Q}$ (ou $\mathbb{N}^2$) est dénombrable.

Exercice 24.12 *On désigne par f l'application définie sur $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ par :*

$$\forall\, (n,m) \in \mathbb{N}^2,\ f(n,m) = 2^n 3^m$$

Montrer que f est injective. Il résulte que $\mathbb{N}^2$ est dénombrable.

Solution 24.12 *L'égalité $f(n,m) = f(n',m')$ avec (n,m) et (n',m') dans $\mathbb{N}^2$ équivaut à $2^n 3^m = 2^{n'} 3^{m'}$ et l'unicité de la décomposition en facteurs premiers d'un entier naturel non nul nous dit que $(n,m) = (n',m')$. L'application f est donc injective de $\mathbb{N}^2$ dans $\mathbb{N}$ et bijective de $\mathbb{N}^2$ dans $f(\mathbb{N}^2) \subset \mathbb{N}$.*

Exercice 24.13 *Soient $p > q \geq 2$ deux nombres premiers. Montrer que $\dfrac{\ln(p)}{\ln(q)}$ est irrationnel.*

Solution 24.13 *Supposons que $\dfrac{\ln(p)}{\ln(q)} = \dfrac{\alpha}{\beta}$ avec α, β entiers naturels non nuls premiers entre eux. On a alors $\ln(p^\alpha) = \ln\left(q^\beta\right)$ et $p^\alpha = q^\beta$, ce qui est impossible du fait de l'unicité de la décomposition en facteurs premiers.*

Exercice 24.14 *Soient $p_1 < p_2 < \cdots < p_r$ des nombres premiers. Montrer que les réels $\ln(p_1), \ln(p_2), \cdots, \ln(p_r)$ sont $\mathbb{Q}$-libres dans $\mathbb{R}$.*

Solution 24.14 *Supposons qu'il existe des rationnels $\dfrac{\alpha_1}{\beta_1}, \cdots, \dfrac{\alpha_r}{\beta_r}$ tels que $\displaystyle\sum_{k=1}^{r} \frac{\alpha_k}{\beta_k} \ln(p_k) = 0$. En notant $\beta = \displaystyle\prod_{k=1}^{r} \beta_k$, on a $\displaystyle\sum_{k=1}^{r} \beta \frac{\alpha_k}{\beta_k} \ln(p_k) = 0$, soit $\displaystyle\sum_{k=1}^{r} \gamma_k \ln(p_k) = 0$, où les γ_k sont des entiers relatifs, ce qui équivaut à $\displaystyle\prod_{k=1}^{r} p_k^{\gamma_k} = 1$ et les γ_k sont nécessairement tous nuls puisque les p_k sont premiers distincts (unicité de la décomposition en facteurs premiers).*

Exercice 24.15 *Soit $n \geq 2$ un entier sans facteur carré, c'est-à-dire que n a une décomposition en facteurs premiers de la forme $n = \prod_{k=1}^{r} p_k$ où les p_k sont premiers deux à deux distincts. Montrer que $\sqrt{n}$ est irrationnel.*

Solution 24.15 *Si $\sqrt{n}$ est rationnel, il s'écrit alors $\sqrt{n} = \dfrac{a}{b}$, où a, b sont deux entiers naturels non nuls premiers entre eux. On a $a^2 = nb^2$ et si p est un diviseur premier de a (on a bien $a \geq 2$ puisque $\sqrt{n} > 1$), p^2 divise nb^2 en étant premier avec b^2 (a et b sont premiers entre eux), il divise n (théorème de Gauss), ce qui contredit le fait que n est sans facteur carré. Donc $\sqrt{n}$ est irrationnel.*

Exercice 24.16 *Soit n un entier de la forme $n = 2^m + 1$ avec $m \geq 0$. Montrer que si n est premier alors $m = 0$ ou m est une puissance de 2 (ce qui revient à dire que $n = 2^{2^p} + 1$ est un nombre de Fermat).*

Solution 24.16 *Si $m = 0$, alors $n = 2$ est premier.*
Si $m = 1 = 2^0$, alors $n = 3$ est premier.
On suppose que $m \geq 2$. La décomposition en facteurs premiers de m permet d'écrire que $m = 2^p(2q+1)$ où p et q sont des entiers naturels.
Si q est non nul, on a alors :

$$\begin{aligned} n &= \left(2^{2^p}\right)^{2q+1} + 1 = a^{2q+1} + 1 \\ &= (a+1) \sum_{k=0}^{2q} (-1)^k a^{2q-k} = (a+1)\, b \end{aligned}$$

avec $a + 1 = 2^{2^p} + 1 \geq 3$ et :

$$b = \frac{n}{a+1} = \frac{a \cdot a^{2q} + 1}{a+1} > 1$$

($a \geq 2$ et $q \geq 1$), donc n n'est pas premier.

Exercice 24.17 *Soit $p = 2^m - 1$ un nombre premier de* Mersenne *(donc m est premier). Montrer que $q = 2^{m-1}p$ est un nombre parfait, c'est-à-dire qu'il est égal à la somme de ses diviseurs stricts (i. e. différents de q).*

Solution 24.17 *L'entier $q = 2^{m-1}p$ est décomposé en facteurs premiers et ses diviseurs stricts sont les 2^k avec k compris entre 0 et $m-1$ et les $2^k p$ avec k compris entre 0 et $m-2$. La somme de ses diviseurs stricts est :*

$$\begin{aligned} S &= \sum_{k=0}^{m-1} 2^k + p \sum_{k=0}^{m-2} 2^k \\ &= 2^m - 1 + p\left(2^{m-1} - 1\right) = p + p\left(2^{m-1} - 1\right) = q \end{aligned}$$

Si $n = \prod_{k=1}^{r} p_k^{\alpha_k}$ est un entier décomposé en produit de facteurs premiers, alors les diviseurs de n sont de la forme $d = \prod_{k=1}^{r} p_k^{\gamma_k}$ où les γ_k sont des entiers naturels tels que $\gamma_k \leq \alpha_k$ pour tout k compris entre 1 et r. Il y a donc $\prod_{k=1}^{r} (\alpha_k + 1)$ diviseurs positifs possibles de n.

La décomposition en facteurs premiers peut être utilisée pour calculer le pgcd et le ppcm de deux entiers naturels supérieur ou égal à 2.

Tout est basé sur le lemme qui suit.

Lemme 24.5 *Soient n, m deux entiers naturels supérieur ou égal à 2 et :*

$$n=\prod_{k=1}^{r}p_k^{\alpha_k},\ m=\prod_{k=1}^{r}p_k^{\beta_k}$$

leurs décompositions en facteurs premiers avec les p_k premiers deux à deux distincts et les α_k, β_k entiers naturels (certains de ces entiers pouvant être nuls). On a alors :

$$(a\ \textit{divise}\ b)\Leftrightarrow\left(\forall k\in\{1,2,\cdots,r\},\ \alpha_k\leq\beta_k\right)$$

Démonstration. Dire que n divise m équivaut à dire qu'il existe un entier $q\geq 1$ tel que $m=qn$ et en écrivant $q=p_1^{\gamma_1}\cdots p_r^{\gamma_r}$ où les γ_k sont des entiers naturels, on a :

$$m=p_1^{\beta_1}\cdots p_r^{\beta r}=p_1^{\alpha_1+\gamma_1}\cdots p_r^{\alpha_r+\gamma_r}.$$

L'unicité de la décomposition en facteurs premiers de m nous dit alors que :

$$\forall k\in\{1,2,\cdots,r\},\ \beta_k=\alpha_k+\gamma_k\geq\alpha_k.$$

■

Théorème 24.5 *Soient n, m deux entiers naturels supérieur ou égal à 2 et :*

$$n=\prod_{k=1}^{r}p_k^{\alpha_k},\ m=\prod_{k=1}^{r}p_k^{\beta_k}$$

leurs décompositions en facteurs premiers avec les p_k premiers deux à deux distincts et les α_k, β_k entiers naturels (certains de ces entiers pouvant être nuls). On a alors :

$$n\wedge m=\prod_{k=1}^{r}p_k^{\min(\alpha_k,\beta_k)},\ n\vee m=\prod_{k=1}^{r}p_k^{\max(\alpha_k,\beta_k)}.$$

Démonstration. L'entier $\delta=\prod_{k=1}^{r}p_k^{\min(\alpha_k,\beta_k)}$ divise n et m d'après le lemme précédent.

Si d est un diviseur de n et m, il s'écrit sous la forme $d=\prod_{k=1}^{r}p_k^{\gamma_k}$ où les γ_k sont des entiers naturels tels que $\gamma_k\leq\alpha_k$ et $\gamma_k\leq\beta_k$ pour tout k compris entre 1 et r, on a donc $\gamma_k\leq\min(\alpha_k,\beta_k)$ pour tout k compris entre 1 et r et d divise δ. Donc δ est bien le pgcd de n et m.

Pour ce qui est du ppcm, on a :

$$n\vee m=\frac{nm}{n\wedge m}=\prod_{k=1}^{r}p_k^{\alpha_k+\beta_k-\min(\alpha_k,\beta_k)}$$

avec :

$$\alpha_k+\beta_k-\min(\alpha_k,\beta_k)=\max(\alpha_k,\beta_k)$$

pour tout k compris entre 1 et r. ■

Le résultat précédent se généralise au calcul du pgcd et du ppcm de $p\geq 2$ entiers naturels.

Exercice 24.18 *On note $2=p_1<p_2<\cdots<p_n<\cdots$ la suite infinie des nombres premiers et on se propose de montrer la divergence de la série $\sum_{n=1}^{+\infty}\frac{1}{p_n}$. Pour ce faire, on introduit la suite $(u_n)_{n\geq 1}$ définie par :*

$$\forall n\geq 1,\ u_n=\frac{1}{\prod_{k=1}^{n}\left(1-\frac{1}{p_k}\right)}.$$

1. *Montrer que, pour tout* $n \geq 1$, *on a :*

$$u_n = \sum_{k \in E_n} \frac{1}{k}$$

où E_n *est l'ensemble des entiers naturels non nuls qui ont tous leurs diviseurs premiers dans* $\mathcal{P}_n = \{p_1, \cdots, p_n\}$.

2. *En déduire que, pour tout* $n \geq 1$, *on a :*

$$u_n \geq \sum_{k=1}^{p_n} \frac{1}{k}.$$

3. *En déduire que la série* $\sum \ln\left(1 - \frac{1}{p_n}\right)$ *est divergente et conclure.*

4. *Quelle est la nature de la série* $\sum \frac{1}{p_n^\alpha}$ *où* α *est un réel ?*

5. *Quelle est le rayon de convergence de la série entière* $\sum \frac{z^{p_n}}{p_n}$.

Solution 24.18

1. *Pour* $n \geq 1$, *on a :*

$$\begin{aligned} u_n &= \prod_{k=1}^{n} \frac{1}{1 - \frac{1}{p_k}} = \prod_{k=1}^{n} \left(\sum_{i=0}^{+\infty} \frac{1}{p_k^i} \right) = \sum_{i_1 \geq 0, i_2 \geq 0, \cdots, i_n \geq 0}^{+\infty} \frac{1}{p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n}} \\ &= \sum_{k \in E_n} \frac{1}{k}. \end{aligned}$$

2. *Résulte du fait que* E_n *contient* $\{1, 2, \cdots, p_n\}$, *la série étant à termes positifs.*

3. *La suite* $\left(\sum_{k=1}^{p_n} \frac{1}{k} \right)_{n \geq 1}$ *étant extraite de la suite divergente vers l'infini* $\left(\sum_{k=1}^{n} \frac{1}{k} \right)_{n \geq 1}$, *on a* $\lim_{n \to +\infty} \sum_{k=1}^{p_n} \frac{1}{k} = +\infty$, *donc* $\lim_{n \to +\infty} u_n = +\infty$ *et* $\lim_{n \to +\infty} \prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right) = 0$, *ce qui entraîne :*

$$\lim_{n \to +\infty} \ln \left(\prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right) \right) = \lim_{n \to +\infty} \sum_{k=1}^{n} \ln \left(1 - \frac{1}{p_k}\right) = -\infty$$

La série $\sum \ln\left(1 - \frac{1}{p_n}\right)$ *est donc divergente. Cette série étant à termes négatifs avec* $\ln\left(1 - \frac{1}{p_n}\right) \underset{+\infty}{\backsim} -\frac{1}{p_n}$, *on en déduit la divergence de* $\sum \frac{1}{p_n}$.
On a aussi la courte démonstration suivante :
Si $\sum_{n=1}^{+\infty} \frac{1}{p_n} < +\infty$ *il existe alors un entier* $r \geq 1$ *tel que :*

$$R_r = \sum_{n=r+1}^{+\infty} \frac{1}{p_n} < \frac{1}{2}.$$

On note $P = p_1 \cdots p_r$. *Pour tout* $n \geq 1$, *les diviseurs premiers de* $1 + nP$ *sont dans* $\{p_k \mid k \geq r+1\}$ *(pour* $1 \leq k \leq r$, *le nombre premier* p_k *divisant* P *ne peut diviser* $1+nP$*) et on a :*

$$1 + nP = p_{r+1}^{m_1} \cdots p_{r+s_n}^{m_{s_n}}$$

avec $s_n \geq 1$, $m_j \geq 0$ *pour* j *compris entre* 1 *et* s_n *et* $m_{s_n} \geq 1$. *On en déduit que pour tout* $N \geq 1$, *on a :*

$$\sum_{n=1}^{N} \frac{1}{1+nP} = \sum_{n=1}^{N} \prod_{k=1}^{s_n} \frac{1}{p_{r+k}^{m_k}} < \sum_{j=1}^{+\infty} \left(\sum_{k=1}^{+\infty} \frac{1}{p_{r+k}} \right)^j < \sum_{j=1}^{+\infty} \left(\frac{1}{2} \right)^j$$

en contradiction avec $\sum_{n=1}^{+\infty} \dfrac{1}{1+nP} = +\infty$.

4. *Pour* $\alpha \leq 0$, *on a* $\dfrac{1}{p_n^\alpha} \geq 1$ *et la série* $\sum \dfrac{1}{p_n^\alpha}$ *diverge puisque son terme général ne tend pas vers* 0.
Pour $0 < \alpha \leq 1$, *on a* $\dfrac{1}{p_n^\alpha} \geq \dfrac{1}{p_n}$ *et la série* $\sum \dfrac{1}{p_n^\alpha}$ *diverge.*
Pour $\alpha > 1$, *on a pour tout* $n \geq 1$ *:*

$$S_n = \sum_{k=1}^{n} \frac{1}{p_k^\alpha} \leq \sum_{k=1}^{p_n} \frac{1}{k^\alpha} < \sum_{k=1}^{+\infty} \frac{1}{k^\alpha} < +\infty$$

donc la suite des sommes partielles $(S_n)_{n\geq 1}$ *est majorée et la série* $\sum \dfrac{1}{p_n^\alpha}$ *converge.*

5. *La série* $\sum \dfrac{z^{p_n}}{p_n}$ *diverge pour* $z = 1$, *son rayon de convergence est donc* $R \leq 1$.
Pour $|z| < 1$ *et* $n \geq 1$, *on a* $p_n \geq n$ *et :*

$$\left| \frac{z^{p_n}}{p_n} \right| \leq |z^{p_n}| \leq |z^n|$$

avec $\sum_{n=1}^{+\infty} |z^n| < +\infty$, *donc* $\sum_{n=1}^{+\infty} \left| \dfrac{z^{p_n}}{p_n} \right| < +\infty$ *et* $R \geq 1$. *On a donc* $R = 1$.

Un théorème de Mertens nous dit que pour tout réel $x \geq 2$, on a :

$$\sum_{p_n \leq x} \frac{1}{p_n} = C + \ln(\ln(x)) + O\left(\frac{1}{\ln(x)} \right)$$

où $C \backsimeq 0.261$.

On a aussi :

$$\sum_{p_n \leq x} \frac{1}{p_n} = \ln(x) + O(1).$$

24.4 Valuation p-adique

Pour tout nombre premier p et tout entier naturel non nul n, on note $\nu_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers avec $\nu_p(n) = 0$ si p ne figure pas dans cette décomposition et $\nu_p(1) = 0$. Cet entier $\nu_p(n)$ est appelé la valuation p-adique de n.

On a donc :

$$\nu_p(n) = \max\left\{k \in \mathbb{N} \mid p^k \text{ divise } n\right\}$$

et :

$$\nu_p(n) \neq 0 \Leftrightarrow (p \text{ divise } n).$$

La décomposition en facteurs premiers de n peut donc s'écrire sous la forme :

$$n = \prod_{p \in \mathcal{D}_n \cap \mathcal{P}} p^{\nu_p(n)}$$

où $\mathcal{D}_n$ désigne l'ensemble des diviseurs positifs de n, ce qui peut aussi s'écrire $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$, le produit étant fini puisque $\nu_p(n) = 0$ si p ne divise pas n.

On peut remarquer que si m est le nombre de zéros qui terminent l'écriture décimale d'un entier $n \geq 2$, alors n est divisible par 10^m et pas par 10^{m+1} et en conséquence, $m = \min(\nu_2(n), \nu_5(n))$.

Théorème 24.6

1. *Si p est un nombre premier et n, m sont deux entiers naturels non nuls, alors :*

$$\begin{cases} \nu_p(nm) = \nu_p(n) + \nu_p(m) \\ \nu_p(n+m) \geq \min(\nu_p(n), \nu_p(m)) \end{cases}$$

l'égalité étant réalisée dans la deuxième formule si $\nu_p(n) \neq \nu_p(m)$.

2. *Soient n, m deux entiers naturels non nuls.*

   (a) *n divise m si, et seulement si, $\nu_p(n) \leq \nu_p(m)$ pour tout $p \in \mathcal{P}$.*

   (b) *Pour tout $p \in \mathcal{P}$, on a :*

$$\begin{cases} \nu_p(n \wedge m) = \min(\nu_p(n), \nu_p(m)) \\ \nu_p(n \vee m) = \max(\nu_p(n), \nu_p(m)) \end{cases}$$

Démonstration.

1. On a :

$$nm = \prod_{q \in \mathcal{P}} q^{\nu_q(n) + \nu_q(m)}$$

ce qui entraîne $\nu_p(nm) = \nu_p(n) + \nu_p(m)$ pour tout $p \in \mathcal{P}$ et en supposant que $\nu_p(n) \leq \nu_p(m)$:

$$\begin{aligned} n + m &= p^{\nu_p(n)} \prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(n)} + p^{\nu_p(m)} \prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(m)} \\ &= p^{\nu_p(n)} \left(\prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(n)} + p^{\nu_p(m) - \nu_p(n)} \prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(m)} \right) \end{aligned}$$

ce qui entraîne $\nu_p(n+m) \geq \nu_p(n) = \min(\nu_p(n), \nu_p(m))$. Si $\nu_p(n) \leq \nu_p(m)$, alors $\prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(n)} + p^{\nu_p(m) - \nu_p(n)} \prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(m)}$ ne peut pas être divisible par p et $\nu_p(n+m) = \nu_p(n)$.

2.

(a) C'est le lemme 24.5.

(b) C'est le théorème 24.5.

■

Exercice 24.19 *On se donne un entier $n \geq 2$ et un nombre premier p.*

1. *Déterminer, pour tout entier naturel non nul k, le nombre n_k de multiples de p^k compris entre 1 et n.*
2. *Montrer que :*
$$\nu_p(n!) = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k}\right]$$
(formule de Legendre).
3. *Donner un équivalent de $\nu_p(n!)$ quand n tend vers l'infini.*
4. *Déterminer le nombre de zéros qui terminent l'écriture décimale de 100!*

Solution 24.19

1. *Les multiples de p^k compris entre 1 et n sont les entiers $m = p^k q$ où q est un entier compris entre 1 et $\dfrac{n}{p^k}$, il y en a $n_k = \left[\dfrac{n}{p^k}\right]$. Pour $p^k > n$, on a $n_k = 0$.*
2. *L'ensemble $E_n = \{1, 2, \cdots, n\}$ peut être partitionné sous la forme :*
$$E_n = \bigcup_{k=0}^{+\infty} (P_k \cap E_n)$$
où P_0 est l'ensemble des entiers non multiples de p et, pour $k \geq 1$, P_k est l'ensemble des entiers multiples de p^k et non multiples de p^{k+1}. Pour tout $k \geq 0$ et tout $m \in P_k$, on a $\nu_p(m) = k$. De plus, pour $k \geq 1$, $P_k \cap E_n$ est formé de l'ensemble des entiers compris entre 1 et n qui sont multiples de p^k privé du sous-ensemble formé des multiples de p^{k+1} et donc $\operatorname{card}(P_k \cap E_n) = n_k - n_{k+1}$.
On en déduit que :
$$\begin{aligned}\nu_p(n!) &= \sum_{m=1}^{n} \nu_p(m) = \sum_{k=0}^{+\infty} \sum_{m \in P_k \cap E_n} \nu_p(m) \\ &= \sum_{k=0}^{+\infty} k \operatorname{card}(P_k \cap E_n) = \sum_{k=0}^{+\infty} k(n_k - n_{k+1})\end{aligned}$$

cette somme étant en réalité finie. Précisément on a $n_k = 0$ *dès que* $p^k > n$, *soit* $k > \dfrac{\ln(n)}{\ln(p)}$.

On a donc, en posant $q = \left[\dfrac{\ln(n)}{\ln(p)}\right]$ *et en effectuant un changement d'indice :*

$$\begin{aligned}\nu_p(n!) &= \sum_{k=1}^{q} k(n_k - n_{k+1}) = \sum_{k=1}^{q} kn_k - \sum_{k=1}^{q} kn_{k+1} \\ &= \sum_{k=1}^{q} kn_k - \sum_{j=2}^{q+1} (j-1)\, n_j \\ &= n_1 + \sum_{k=2}^{q} (kn_k - (k-1)\, n_k) - qn_{q+1} \\ &= \sum_{k=1}^{q} n_k = \sum_{k=1}^{+\infty} n_k = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k}\right].\end{aligned}$$

3. *Avec les notations précédentes, on a pour tout entier* k *compris entre* 1 *et* $q_n = \left[\dfrac{\ln(n)}{\ln(p)}\right]$ *:*

$$\left[\frac{n}{p^k}\right] \leq \frac{n}{p^k} < \left[\frac{n}{p^k}\right] + 1$$

et :

$$\nu_p(n!) = \sum_{k=1}^{q_n} \left[\frac{n}{p^k}\right] \leq \sum_{k=1}^{q_n} \frac{n}{p^k} < \nu_p(n!) + q_n$$

ou encore :

$$\frac{\nu_p(n!)}{n} \leq \sum_{k=1}^{q_n} \frac{1}{p^k} < \frac{\nu_p(n!)}{n} + \frac{q_n}{n}$$

avec :

$$0 < \frac{q_n}{n} \leq \frac{1}{\ln(p)} \frac{\ln(n)}{n} \underset{n\to+\infty}{\to} 0$$

ce qui donne :

$$\lim_{n\to+\infty} \left(\sum_{k=1}^{q_n} \frac{1}{p^k} - \frac{\nu_p(n!)}{n} \right) = 0$$

et tenant compte de $\lim\limits_{n\to+\infty} q_n = +\infty$, *on a :*

$$\lim_{n\to+\infty} \sum_{k=1}^{q_n} \frac{1}{p^k} = \sum_{k=0}^{+\infty} \frac{1}{p^k} - 1 = \frac{1}{1-\frac{1}{p}} - 1 = \frac{1}{p-1}$$

et $\lim\limits_{n\to+\infty} \dfrac{\nu_p(n!)}{n} = \dfrac{1}{p-1}$, *soit* $\nu_p(n!) \underset{n\to+\infty}{\sim} \dfrac{n}{p-1}$.

4. *Si* m *est le nombre de zéros qui terminent l'écriture décimale de* $n!$ *où* $n = 100$, *alors* $n!$ *est divisible par* 10^m *et pas par* 10^{m+1} *et donc :*

$$m = \min(\nu_2(n!), \nu_5(n!)).$$

On a :

$$\nu_2(100!) = \sum_{k=1}^{+\infty} \left[\frac{100}{2^k}\right] = \sum_{k=1}^{q} \left[\frac{100}{2^k}\right]$$

avec $q = \left[\dfrac{\ln(100)}{\ln(2)}\right] = 6$ *et :*

$$\nu_5(100!) = \sum_{k=1}^{+\infty} \left[\frac{100}{5^k}\right] = \sum_{k=1}^{q'} \left[\frac{100}{5^k}\right]$$

avec $q' = \left[\dfrac{\ln(100)}{\ln(5)}\right] = 2$ *ce qui donne :*

$$\nu_5(100!) = \frac{100}{5} + \frac{100}{25} = 24 < \frac{100}{2} < \nu_2(100!)$$

et $m = 24$, *ce qui est confirmé par Maple :*

$$\begin{aligned} 100! = {} & 93\,326\,215\,443\,944\,152\,681\,699\,238\,856\,266\,700\,490\,715\,968\,264\,38 \\ & 621\,468\,592\,963\,895\,217\,599\,993\,229\,915\,608\,941\,463\,976\,156\,518 \\ & 286\,253\,697\,920\,827\,223\,758\,251\,185\,210\,916\,864 \\ & 000\,000\,000\,000\,000\,000\,000\,000 \end{aligned}$$

On peut remarquer que $\nu_2(100!) \backsimeq 100$ *et* $\nu_5(100!) \backsimeq 25$.

Exercice 24.20 *Pour tout entier naturel* n *supérieur ou égal à* 2, *on note* $H_n = \sum_{k=1}^{n} \dfrac{1}{k}$.

1. *Soit* p *un entier naturel non nul. Montrer que* $H_{2p} = \dfrac{1}{2}H_p + \dfrac{a}{2b+1}$ *où* a, b *sont des entiers naturels avec* a *non nul.*
2. *Montrer par récurrence que pour tout entier naturel non nul* H_n *est le quotient d'un entier impair par un entier pair et qu'en conséquence ce n'est pas un entier.*

Solution 24.20

1. *On a :*

$$H_{2p} = \sum_{k=1}^{p} \frac{1}{2k} + \sum_{k=0}^{p-1} \frac{1}{2k+1} = \frac{1}{2}H_p + \frac{N}{D}$$

avec $D = \text{ppcm}(1, 3, \cdots, 2p-1)$ *qui est impair et* N *entier naturel non nul.*

2. *On a* $H_2 = \dfrac{3}{2} \notin \mathbb{N}$. *Supposons le résultat acquis au rang* $n \geq 2$. *Si* $n = 2p$, *on a alors :*

$$\begin{aligned} H_{n+1} = H_n + \frac{1}{2p+1} &= \frac{2a+1}{2b} + \frac{1}{2p+1} \\ &= \frac{(2a+1)(2p+1)+2b}{2b(2p+1)} = \frac{2a'+1}{2b'} \end{aligned}$$

avec $a' = a + b + p + 2ap$ *et* $b' = b(2p+1)$. *Si* $n = 2p+1$, *on a alors :*

$$\begin{aligned} H_{n+1} = H_{2(p+1)} &= \frac{c}{2d+1} + \frac{1}{2}H_{p+1} \\ = \frac{c}{2d+1} + \frac{1}{2}\frac{2a+1}{2b} &= \frac{4bc + (2d+1)(2a+1)}{4b(2d+1)} = \frac{2a'+1}{2b'} \end{aligned}$$

avec $a' = a + d + 2ad + 2bc$ *et* $b' = b(2d+1)$.
Dans tous les cas, H_n *est le quotient d'un entier impair par un entier pair et en conséquence, ce n'est pas un entier.*

Exercice 24.21 *Soient* $m < n$ *deux entiers naturels non nuls et :*

$$H_{m,n} = \sum_{k=m}^{n} \frac{1}{k}.$$

1. *Montrer que :*
$$r = \max_{m \leq k \leq n} \nu_2(k) \neq 0.$$
2. *On veut montrer qu'il existe un unique entier* k *compris entre* m *et* n *tel que* $r = \nu_2(k)$. *Pour ce faire on raisonne par l'absurde en supposant que* $r = \nu_2(k_1) = \nu_2(k_2)$ *avec* $m \leq k_1 < k_2 \leq n$.
   (a) *Montrer que* $r = \nu_2(k_3)$ *avec* $k_1 < k_3 = \dfrac{k_1 + k_2}{2} < k_2$.
   (b) *Montrer que la suite* $(k_j)_{j \geq 2}$ *définie par* $k_{j+1} = \dfrac{k_1 + k_j}{2}$ *est une suite strictement décroissante d'entiers naturels non nuls vérifiant* $r = \nu_2(k_j)$ *pour tout* $j \geq 2$ *et conclure.*
3. *Montrer qu'il existe un entier impair* s *tel que :*
$$\operatorname{ppcm}(m, m+1, \cdots, n) = 2^r s.$$
4. *On désigne par* k *l'unique entier compris entre* m *et* n *tel que* $r = \nu_2(k)$.
   (a) *Montrer qu'il existe un entier impair* n_k *tel que :*
$$\frac{1}{k} = \frac{n_k}{2^r s}.$$
   (b) *Montrer que pour tout entier* j *compris entre* m *et* n *et différent de* k, *il existe un entier pair* n_j *tel que :*
$$\frac{1}{j} = \frac{n_j}{2^r s}.$$
   (c) *En déduire que* $H_{m,n}$ *s'écrit comme le quotient d'un entier impair par un entier pair et donc qu'il n'est pas entier.*

Solution 24.21

1. *Du fait que l'un des deux entiers* m *ou* $m+1$ *est pair, on déduit que pour* $m < n$ *on a* $r = \max_{m \leq k \leq n} \nu_2(k) \neq 0$.
2. *L'ensemble* $\{m, \cdots, n\}$ *étant fini il existe au moins un entier* k *compris entre* m *et* n *tel que* $r = \nu_2(k)$ *et il s'agit ici de montrer que cet entier est unique. On suppose donc qu'il existe deux entiers* $k_1 < k_2$ *compris entre* m *et* n *tels que* $r = \nu_2(k_1) = \nu_2(k_2)$. *On a alors* $k_1 = 2^r q_1$ *et* $k_2 = 2^r q_2$ *avec* q_1 *et* q_2 *impairs.*

(a) *L'entier* $k_3 = \dfrac{k_1+k_2}{2}$, *milieu de l'intervalle* $[k_1, k_2]$, *est compris entre* m *et* n *et il s'écrit :*

$$k_3 = 2^{r-1}(q_1+q_2),$$

avec q_1+q_2 *pair. On a donc* $\nu(k_3) \geq r$ *et comme on a aussi* $\nu_2(k_3) \leq r = \max_{m\leq k\leq n} \nu_2(k)$, *on a nécessairement* $\nu_2(k_3) = r$.

(b) *En itérant la construction précédente, on peut construire une suite strictement décroissante d'entiers* $(k_j)_{j\geq 2}$ *telle que* $k_{j+1} = \dfrac{k_1+k_j}{2}$, $m \leq k_1 < k_j \leq n$ *et* $r = \nu_2(k_1) = \nu_2(k_j)$, *ce qui est impossible. On peut donc conclure qu'il existe un unique entier* k *compris entre* m *et* n *tel que* $r = \nu_2(k)$.

3. *En utilisant les décompositions en facteurs premiers de tous les entiers compris entre* m *et* n, *on a :*

$$\operatorname{ppcm}(m, m+1, \cdots, n) = 2^r s,$$

où s *est un entier impair.*

4. *Pour tout entier* j *compris entre* m *et* n, *on peut écrire :*

$$\frac{1}{j} = \frac{1}{2^{\nu_2(j)} q_j},$$

où q_j *est impair et divise* s. *Soit en écrivant* $s = q_j p_j$ *avec* p_j *impair :*

$$\frac{1}{j} = \frac{2^{r-\nu_2(j)} p_j}{2^r s}.$$

(a) *Pour* $j = k$ *on a* $r = \nu_2(k)$ *et :*

$$\frac{1}{k} = \frac{n_k}{2^r s},$$

avec $n_k = p_k$ *impair.*

(b) *Pour* $j \neq k$, *on a* $\nu_2(j) < r$ *et :*

$$\frac{1}{j} = \frac{n_j}{2^r s},$$

avec $n_j = 2^{r-\nu_2(j)} p_j$ *pair.*

(c) *En écrivant que :*

$$H_{m,n} = \frac{1}{k} + \sum_{\substack{j=m \\ j\neq k}}^{n} \frac{1}{j} = \frac{n_k}{2^r s} + \frac{u}{2^r s} = \frac{n_k+u}{2^r s},$$

avec n_k *impair et* u *pair, on déduit que* $H_{m,n}$ *est le quotient d'un entier impair par un entier pair. En conséquence* $H_{m,n}$ *n'est pas un entier.*

Exercice 24.22 *Soit* $n \geq 3$ *un entier.*
Si $a < b$ *sont des réels strictement positifs, on notera* $\prod_{a\leq p\leq b} p$ *le produit des nombres premiers compris entre* a *et* b, *avec la convention que ce produit vaut* 1 *s'il n'y a pas de nombres premiers compris entre* a *et* b. *On utilise la même notation avec les inégalités* $a < p \leq b$, $a \leq p < b$ *ou* $a < p < b$.

1. *Montrer que, pour tout réel* $x > 0$, $[2x] - 2[x]$ *vaut* 0 *ou* 1.

2. *Montrer que tous les facteurs premiers de* C_{2n}^n *sont compris entre* 2 *et* $2n$.
3. *Calculer* $\nu_p\left(C_{2n}^n\right)$ *pour tout nombre premier* p.
4. *Montrer que si* p *est un nombre premier vérifiant* $\sqrt{2n} < p < 2n$, *alors* $\nu_p\left(C_{2n}^n\right)$ *vaut* 0 *ou* 1.
5. *Montrer que si* p *est un nombre premier vérifiant* $\frac{2}{3}n < p < n$, *alors* $\nu_p\left(C_{2n}^n\right) = 0$.
6. *Montrer que si* p *est un nombre premier vérifiant* $2 \leq p \leq \sqrt{2n}$, *on a alors, en notant* $m_p = \nu_p\left(C_{2n}^n\right)$, $p^{m_p} \leq 2n$.
7. *Déduire de ce qui précède que :*

$$C_{2n}^n \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \prod_{n<p\leq 2n} p$$

Solution 24.22

1. *Des encadrements :*

$$\begin{cases} [2x] \leq 2x < [2x] + 1 \\ [x] \leq x < [x] + 1 \end{cases}$$

on déduit que :

$$[2x] - 2[x] > 2x - 1 - 2x = -1$$

soit $[2x] - 2[x] \geq 0$ *et :*

$$[2x] - 2[x] < 2x - 2x + 2 = 2$$

soit $[2x] - 2[x] \leq 1$. *On a donc bien* $[2x] - 2[x] \in \{0, 1\}$.

2. *Si* p *est un diviseur premier de* C_{2n}^n, *il divise aussi* $(2n)! = (n!)^2 C_{2n}^n$ *et en conséquence il divise l'un des entiers* m *compris entre* 1 *et* $2n$, *il est donc nécessairement compris entre* 2 *et* $2n$.
3. *On a :*

$$\nu_p\left((2n)!\right) = \nu_p\left((n!)^2 C_{2n}^n\right) = 2\nu_p\left(n!\right) + \nu_p\left(C_{2n}^n\right)$$

et en utilisant la formule de Legendre (exercice précédent) :

$$\begin{aligned} \nu_p\left(C_{2n}^n\right) &= \nu_p\left((2n)!\right) - 2\nu_p\left(n!\right) \\ &= \sum_{k=1}^{+\infty} \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \right). \end{aligned}$$

4. *Si* p *est un nombre premier vérifiant* $\sqrt{2n} < p < 2n$, *on a alors pour tout* $k \geq 2$ *:*

$$0 < \frac{n}{p^k} < \frac{2n}{p^k} \leq \frac{2n}{p^2} < 1$$

et $\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] = 0$, *ce qui donne :*

$$\nu_p\left(C_{2n}^n\right) = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] \in \{0, 1\}$$

5. *Pour $n \geq 5$, on a $\sqrt{2n} < \dfrac{2}{3}n$ (c'est équivalent à $\sqrt{2n} > 3$ ou encore à $2n > 9$), donc si p est un nombre premier tel que $\dfrac{2}{3}n < p \leq n$, on a $\nu_p\left(C_{2n}^n\right) = \left[\dfrac{2n}{p}\right] - 2\left[\dfrac{n}{p}\right]$ avec :*

$$\begin{cases} 2 \leq \dfrac{2n}{p} < 3 \\ 1 \leq \dfrac{n}{p} < \dfrac{3}{2} \end{cases}$$

ce qui donne :

$$\nu_p\left(C_{2n}^n\right) = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 2 - 2 = 0.$$

Pour $n = 2$, le seul nombre premier vérifiant $\dfrac{2}{3}2 < p \leq 2$ est $p = 2$ et :

$$\nu_2\left(C_4^2\right) = \nu_2(6) = 1.$$

Pour $n = 3$, le seul nombre premier vérifiant $\dfrac{2}{3}3 < p \leq 3$ est $p = 3$ et :

$$\nu_3\left(C_6^3\right) = \nu_3(20) = 0.$$

Pour $n = 4$, le seul nombre premier vérifiant $\dfrac{2}{3}4 < p \leq 4$ est $p = 3$ et :

$$\nu_3\left(C_8^4\right) = \nu_3(65) = 0.$$

On peut aussi dire directement que si $\dfrac{2}{3}n < p \leq n$ avec $n \geq 3$, alors $p > \dfrac{2}{3}3 = 2$, soit $p \geq 3$, donc $p^2 \geq 3p > 2n$ et pour tout $k \geq 2$:

$$\frac{n}{p^k} < \frac{2n}{p^k} \leq \frac{2n}{p^2} < 1$$

ce qui donne $\left[\dfrac{2n}{p^k}\right] - 2\left[\dfrac{n}{p^k}\right] = 0$ et :

$$\nu_p\left(C_{2n}^n\right) = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 2 - 2 = 0$$

puisque $2 \leq \dfrac{2n}{p} < 3$ et $1 \leq \dfrac{n}{p} < \dfrac{3}{2}$.

6. *En notant, pour tout entier $k \geq 1$, $a_k = \left[\dfrac{2n}{p^k}\right] - 2\left[\dfrac{n}{p^k}\right]$, on a :*

$$m_p = \nu_p\left(C_{2n}^n\right) = \sum_{k=1}^{+\infty} a_k$$

cette somme étant finie et les a_k valant 0 ou 1. Si tous les a_k sont nuls, alors $m_p = 0$ et $p^{m_p} = 1 \leq 2n$. Sinon, il y en a seulement un nombre fini qui valent 1 et on désigne par r le grand indice tel que $a_r = 1$. On a alors :

$$m_p = \sum_{k=1}^{r} a_k \leq r.$$

Si $p^{m_p} > 2n$, *on a alors* $\dfrac{2n}{p^k} \leq \dfrac{2n}{p^{m_p}} < 1$ *pour tout* $k \geq m_p$ *et* $a_k = 0$, *ce qui impose* $r < m_p$ *(*$r \geq m_p$ *donnerait* $a_r = 0$, *alors que* $a_r = 1$*) en contradiction avec* $m_p \leq r$. *On a donc* $p^{m_p} \leq 2n$.

7. *Comme les facteurs premiers de* C_{2n}^n *sont compris entre* 2 *et* $2n$ *avec* $\nu_p\left(C_{2n}^n\right) \in \{0,1\}$ *pour* $\sqrt{2n} < p < 2n$, *on a :*

$$C_{2n}^n = \prod_{2\leq p\leq\sqrt{2n}} p^{m_p} \prod_{\sqrt{2n}<p\leq 2n} p^{m_p}$$

avec $m_p = \nu_p\left(C_{2n}^n\right)$ *et* $p^{m_p} \leq 2n$ *pour* $2 \leq p \leq \sqrt{2n}$, $m_p \in \{0,1\}$ *pour* $\sqrt{2n} < p \leq 2n$. *Comme il y a au plus* $\left[\sqrt{2n}\right]$ *nombres premiers entre* 2 *et* $\sqrt{2n}$ *avec* $\left[\sqrt{2n}\right] \leq \sqrt{2n}$, *on déduit que :*

$$C_{2n}^n \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n}<p\leq 2n} p^{m_p}.$$

De plus on a vu que $m_p = 0$ *pour* $\dfrac{2}{3}n < p \leq n$, *ce qui donne :*

$$C_{2n}^n \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p^{m_p} \prod_{n<p\leq 2n} p^{m_p} \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \prod_{n<p\leq 2n} p$$

24.5 Le postulat de Bertrand

On se propose ici de montrer le résultat suivant postulé par J. Bertrand en 1845 : si n est un entier supérieur ou égal à 2, il existe des nombres premiers compris entre n et $2n$.

La démonstration de ce lemme utilise la majoration :

$$\forall n \geq 2,\ C_{2n}^n \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \prod_{n<p\leq 2n} p$$

établie avec l'exercice 24.22 et les lemmes techniques qui suivent.

Lemme 24.6 *Pour tout entier* $r \geq 1$, *on a :*

$$\frac{2^{2r}}{2r} \leq C_{2r+1}^r \leq 2^{2r}$$

et $\displaystyle\prod_{r+2\leq p\leq 2r+1} p$ *divise* C_{2r+1}^r.

Démonstration. Pour $r \geq 1$, on a :

$$\begin{aligned} 2^{2r+1} = (1+1)^{2r+1} &= \sum_{k=0}^{2r+1} C_{2r+1}^k \\ &\geq C_{2r+1}^r + C_{2r+1}^{r+1} = 2C_{2r+1}^r \end{aligned}$$

et $C_{2r+1}^r \leq 2^{2r}$.

Pour k compris entre 1 et r, on a :

$$\begin{aligned} C_{2r}^k &= \frac{(2r)!}{k!\,(2r-k)!} = \frac{2r-k+1}{k} \frac{(2r)!}{(k-1)!\,(2r-(k-1))!} \\ &= \frac{2r-k+1}{k} C_{2r}^{k-1} \geq \frac{k+1}{k} C_{2r}^{k-1} > C_{2r}^{k-1} \end{aligned}$$

Il en résulte que $C_{2r}^r > C_{2r}^k$ pour tout k compris entre 1 et $r-1$, cette inégalité étant encore valable pour $k=0$. Et avec $C_{2r}^{r+k} = C_{2r}^{r-k}$ pour k compris entre 0 et r, on déduit que $C_{2r}^r > C_{2r}^k$ pour tout $k \neq r$ compris entre 0 et $2r$.

De ces inégalités, on déduit que :

$$\begin{aligned} 2^{2r} = (1+1)^{2r} &= C_{2r}^0 + C_{2r}^r + \sum_{\substack{k=1 \\ k\neq r}}^{2r} C_{2r}^k \\ &< C_{2r}^0 + C_{2r}^r + (2r-1)\, C_{2r}^r = 1 + 2rC_{2r}^r \end{aligned}$$

soit $2^{2r} \leq 2rC_{2r}^r$, ou encore $\dfrac{2^{2r}}{2r} \leq C_{2r}^r$.

S'il n'y a pas de nombres premiers compris entre $r+2$ et $2r+1$, alors $\prod_{r+2\leq p\leq 2r+1} p = 1$ divise C_{2r+1}^r. Sinon, soit p un nombre premier compris entre $r+2$ et $2r+1$. Cet entier p divise $(2r+1)! = r!\,(r+1)!C_{2r+1}^r$ et comme $p \geq r+2$, il ne peut diviser le produit $r!\,(r+1)!$ formé d'entiers tous strictement inférieurs à $r+2$ (sinon il diviserait l'un d'eux), il est donc premier avec $r!\,(r+1)!$ et va diviser C_{2r+1}^r (théorème de Gauss). L'entier C_{2r+1}^r est donc divisible par tous les nombres premiers compris entre $r+2$ et $2r+1$, en conséquence, il est divisible par leur produit. On a donc en particulier $\prod_{r+2\leq p\leq 2r+1} p \leq C_{2r+1}^r$. ■

Lemme 24.7 *Pour tout entier $m \geq 2$, on a :*

$$\prod_{2\leq p\leq m+1} p \leq 4^m.$$

Démonstration. On procède par récurrence sur $m \geq 2$. Pour $m=2$, on a :

$$\prod_{2\leq p\leq m+1} p = 2\cdot 3 < 4^2.$$

Supposons le résultat acquis jusqu'au rang $m-1 \geq 2$.

Si m est impair, alors $m+1$ est pair différent de 2 et :

$$\prod_{2\leq p\leq m+1} p = \prod_{2\leq p\leq m} p \leq 4^{m-1} < 4^m.$$

Si m est pair, il s'écrit $m=2r$ avec $r \geq 2$ (puisque $m \geq 3$) et :

$$\begin{aligned} \prod_{2\leq p\leq m+1} p = \prod_{2\leq p\leq 2r+1} p &= \prod_{2\leq p\leq r+1} p \prod_{r+2\leq p\leq 2r+1} p \\ &\leq 4^r C_{2r+1}^r \leq 4^r 2^{2r} = 4^{2r} = 4^m. \end{aligned}$$

■

Lemme 24.8 *Pour tout entier $n \geq 3$, on a :*

$$C_{2n}^n \leq (2n)^{\sqrt{2n}}\, 4^{\frac{2n}{3}} \prod_{n<p\leq 2n} p$$

et :

$$2^{\frac{2n}{3}} \leq (2n)^{1+\sqrt{2n}} \prod_{n<p\leq 2n} p. \tag{24.2}$$

Démonstration. Pour $n \geq 3$, en notant $m = \left[\frac{2n}{3}\right]$, on a $m \leq \frac{2n}{3} < m+1$ et :

$$\prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \leq \prod_{2\leq p\leq m+1} p \leq 4^m \leq 4^{\frac{2n}{3}}$$

ce qui donne :

$$C_{2n}^n \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \prod_{n<p\leq 2n} pC_{2n}^n \leq (2n)^{\sqrt{2n}} 4^{\frac{2n}{3}} \prod_{n<p\leq 2n} p$$

En utilisant l'inégalité $\frac{2^{2n}}{2n} \leq C_{2n}^n$, on en déduit que :

$$2^{2n} = 4^n \leq (2n)^{1+\sqrt{2n}} 4^{\frac{2n}{3}} \prod_{n<p\leq 2n} p$$

et :

$$4^{\frac{n}{3}} = 2^{\frac{2n}{3}} \leq (2n)^{1+\sqrt{2n}} \prod_{n<p\leq 2n} p.$$

■

Lemme 24.9 *En désignant par f et g les fonctions définies pour $x \geq 3$ par :*

$$f(x) = \frac{\ln(x)}{x} \text{ et } g(x) = \frac{\ln(2)}{6}\frac{x}{1+x}.$$

il existe un entier $n_0 > 3$ tel que $f(x) < g(x)$ pour tout $x \geq n_0$.

Démonstration. Comme $\lim_{x\to+\infty} \frac{\ln(x)}{x} = 0$ et $\lim_{x\to+\infty} g(x) = \frac{\ln(2)}{6} > 0$, l'existence de x_0 tel que $f(x_0) = g(x_0)$ est assurée. En dessinant les graphes de f et g sur $[3, 35]$, on voit que x_0 est unique et localisé entre 30 et 31.

La fonction $h = g - f$ est dérivable sur $]0, +\infty[$ avec :

$$h'(x) = \frac{\ln(2)}{6}\frac{1}{(1+x)^2} + \frac{1}{x^2}(\ln(x) - 1) > 0$$

pour $x \geq 3$. Cette fonction est donc strictement croissante sur $[3, +\infty]$ et avec :

$$h(30) \backsimeq -1.575\,3 \times 10^{-3} < 0,\ h(31) \backsimeq 1.140\,6 \times 10^{-3} > 0$$

on déduit du théorème des valeurs intermédiaires que h s'annule en un point $x_0 \in]30, 31[$ et $h(x) > 0$ pour tout $x > x_0$. La valeur $n_0 = 31$ convient. ■

Théorème 24.7 (Bertrand) *Si n est un entier supérieur ou égal à 2, il existe alors des nombres premiers compris entre n et $2n$.*

Démonstration. Pour $n = 2$, c'est clair.

Supposons que, pour $n \geq 3$, il n'existe pas de nombres premiers compris entre n et $2n$. A fortiori, il n'en existe pas entre $n+1$ et $2n$ et $\prod_{n<p\leq 2n} p = 1$. De l'inégalité (24.2), on déduit alors que $2^{\frac{2n}{3}} \leq (2n)^{1+\sqrt{2n}}$, ce qui entraîne :

$$\frac{2n}{3}\ln(2) \leq \left(1 + \sqrt{2n}\right)\ln(2n)$$

ou encore :

$$\frac{2n}{6}\ln(2) \leq \left(1+\sqrt{2n}\right)\ln\left(\sqrt{2n}\right)$$

encore équivalent à :

$$g\left(\sqrt{2n}\right) = \frac{\ln(2)}{6}\frac{\sqrt{2n}}{1+\sqrt{2n}} \leq f\left(\sqrt{2n}\right) = \frac{\ln\left(\sqrt{2n}\right)}{\sqrt{2n}}$$

et nécessairement $\sqrt{2n} < n_0 = 31$, soit $2n < 31^2 = 961$ ou encore $n \leq \dfrac{960}{2} = 480$.

On donc ainsi montré que pour tout entier $n > 480$, il existe des nombres premiers entre n et $2n$.

Pour les entiers compris entre 2 et 480, il n'est pas nécessaire de considérer tous les cas. On peut remarquer que la suite strictement croissante de nombres premiers :

$$(p_k)_{1\leq k\leq 11} = (2,3,5,7,13,23,43,83,163,317,631)$$

est telle que $p_k < p_{k+1} < 2p_k$. Il en résulte que tout intervalle $]n,2n]$ avec $2 \leq n \leq 480$ contient l'un de ces nombres premiers. En effet, en désignant pour $n \geq 2$, par k le plus grand indice tel que $p_k \leq n$, on a $p_k \leq n < p_{k+1} < 2p_k \leq 2n$ et $p_{k+1} \in]n,2n]$. ■

24.6 Les théorèmes de Fermat et de Wilson

Le lemme qui suit nous donne une démonstration relativement simple du « petit » théorème de Fermat.

Lemme 24.10 *Un entier naturel $p \geq 2$ est premier si, et seulement si, pour tout entier k compris entre 1 et $p-1$, p divise $C_p^k = \dfrac{p!}{k!\,(p-k)!}$.*

Démonstration. Si $p \geq 2$ est premier, comme il divise $p! = k!\,(p-k)!C_p^k$ et est premier avec $k!\,(p-k)!$ (sinon il diviserait ce produit et donc l'un des entiers j compris entre 1 et $p-1$, ce qui est impossible), il divise C_p^k (théorème de Gauss).

Réciproquement, supposons que p divise C_p^k pour tout entier k compris entre 1 et $p-1$.

Pour tout k compris entre 1 et $p-1$, on a :

$$C_{p-1}^{k-1} + C_{p-1}^k = C_p^k$$

(triangle de Pascal) et avec $C_p^k \equiv 0$ modulo p, on déduit que $C_{p-1}^k \equiv -C_{p-1}^{k-1}$ modulo p et par récurrence finie sur k compris entre 1 et $p-1$, on déduit que C_{p-1}^k est congru à $(-1)^k$ modulo p. En effet, pour $k=1$, on a $C_{p-1}^1 \equiv -C_{p-1}^0 = -1$ modulo p et en supposant le résultat acquis pour $k-1$ compris entre 1 et $p-2$, on a $C_{p-1}^k \equiv -C_{p-1}^{k-1} \equiv -(-1)^{k-1} = (-1)^k$.

Si p n'est pas premier, il admet un diviseur d compris entre 2 et $p-1$ et on a :

$$C_p^d = \frac{p}{d}C_{p-1}^{d-1} = qC_{p-1}^{d-1}$$

où q est un entier compris entre 2 et $p-1$, avec $C_p^d \equiv 0$ modulo p et $C_{p-1}^{d-1} \equiv (-1)^{d-1}$ modulo p, ce qui donne $q(-1)^{d-1} \equiv 0$ modulo p, encore équivalent à dire que p divise $q(-1)^{d-1}$ avec $2 \leq \left|q(-1)^{d-1}\right| \leq p-1$, ce qui est impossible.

Donc p est premier. ■

Théorème 24.8 (Fermat) *Soit p un entier naturel premier. Pour tout entier relatif n on a :*

$$n^p \equiv n \ (p)\,.$$

Démonstration. On démontre tout d'abord ce résultat sur les entiers naturels par récurrence sur $n \geq 0$. Pour $n = 0$ le résultat est évident. On le supposant acquis pour $n \geq 0$, on a :

$$(n+1)^p = n^p + \sum_{k=1}^{p-1} C_p^k n^k + 1 \equiv n^p + 1 \equiv n + 1 \ (p)\,.$$

Pour $n < 0$, on a $(-n)^p \equiv -n$ modulo p. Si $p = 2$ alors $-n \equiv n$ modulo 2 et $(-n)^2 = n^2$. Pour $p \geq 3$, p est impair et $(-n)^p = -n^p$ est congru à $-n$ modulo p, donc n^p est congru à n modulo p. ∎

On peut aussi déduire du lemme 24.10 que si p est premier, alors pour tout couple (a, b) d'entiers relatifs, on a :

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} C_p^k a^{p-k} b^k + b^p \equiv a^p + b^p \ (p)\,.$$

Par récurrence sur l'entier $n \geq 1$, on déduit alors que pour tout n-uplet $(a_1, \cdots, a_n)$ d'entiers relatifs, on a :

$$(a_1 + \cdots + a_n)^p \equiv a_1^p + \cdots + a_n^p \ (p)\,.$$

Prenant tous les a_k égaux à 1, on en déduit que n^p est congru à n modulo p. Ce résultat est encore valable pour $n = 0$ et $n < 0$.

Théorème 24.9 (Fermat) *Soit p un entier naturel premier. Pour tout entier relatif n non multiple de p, on a :*

$$n^{p-1} \equiv 1 \ (p)\,.$$

Démonstration. L'entier premier p divise $n^p - n = n\,(n^{p-1} - 1)$ et est premier avec n si n n'est pas un multiple de p, il divise donc $n^{p-1} - 1$. ∎

Remarque 24.4 *Connaissant les anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et le théorème de Lagrange pour les groupes finis, on peut donner la démonstration suivante du théorème de Fermat : pour p premier, $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps, donc $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times} = \dfrac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{0\}$ est un groupe d'ordre $p-1$ et tout élément de ce groupe a un ordre qui divise $p-1$, ce qui entraîne $a^{p-1} = 1$ dans ce groupe.*

Si p est un entier pour lequel il existe un entier n compris entre 1 et $p-1$ tel que n^{p-1} ne soit pas congru à 1 modulo p, alors p n'est pas premier puisque n^{p-1} est congru à 1 modulo p pour p premier et $1 \leq n \leq p-1$ d'après le théorème de Fermat.

La réciproque du théorème de Fermat est fausse. On peut en fait montrer que pour $p \geq 2$, la condition $n^{p-1} \equiv 1 \pmod{p}$ pour tout n premier avec p est équivalente à p premier ou $p = \prod_{k=1}^{r} p_k$ avec $r \geq 3$, $3 \leq p_1 < \cdots < p_r$ premiers tels que pour tout k compris entre 1 et r, $p_k - 1$ divise $p-1$ (un tel entier est appelé nombre de Carmichaël ou nombre pseudo-premier). Par exemple 561, 1105, 1729, sont des nombres de Carmichaël.

En 1999, Alford, Granville et Pomerance ont montré qu'il y a une infinité de nombres de Carmichaël.

Exercice 24.23 *Calculer le reste dans la division euclidienne de* 5^{2008} *par* 11.

Solution 24.23 *Comme* 11 *est premier le théorème de Fermat nous dit que* 5^{10} *est congru à* 1 *modulo* 11. *On effectue alors la division euclidienne de* 2008 *par* 10, *soit* $2008 = 200 \times 10 + 8$ *et on déduit que* 5^{2008} *est congru à* 5^8 *modulo* 11. *Enfin avec* $5^2 \equiv 3$, $5^4 \equiv 9 \equiv -2$, $5^8 \equiv 4$ *modulo* 11, *on déduit que* $5^{2008} \equiv 4$ *modulo* 11, *ce qui signifie que* 4 *est le reste dans la division euclidienne de* 5^{2008} *par* 11.

Le principe de l'exercice précédent est le suivant.

On cherche le reste dans la division euclidienne de a^b par p, où $p \geq 3$ est premier.

On effectue la division euclidienne de b par $p-1$, soit $b = q\,(p-1) + r$ avec $0 \leq r \leq p-2$ et on a $a^b = (a^{p-1})^q\, a^r$ avec $a^{p-1} \equiv 1 \ (p)$ si p ne divise pas a, ce qui donne $a^b \equiv a^r \ (p)$ (on a diminué b). Ensuite $a \equiv s \ (p)$ avec $1 \leq s \leq p-1$ (on a diminué a) et $a^b \equiv s^r \ (p)$. On se débrouille pour construire un exercice où s^r est facile à calculer.

Exercice 24.24 *Soit* $p \geq 7$ *un nombre premier. Montrer que* $p^4 - 1$ *est divisible par* 240.

Solution 24.24 *Comme* $240 = 2^4 \cdot 3 \cdot 5$, *il suffit de montrer que* $p^4 - 1$ *est multiple de* 2^4, 3 *et* 5.
Comme p est premier différent de 3 *et* 5, *le petit théorème de Fermat nous dit que* $p^4 - 1$ *est congru à* 0 *modulo* 5 *et* p^3 *congru à p, modulo* 3, *donc* p^4 *est congru à* p^2 *qui est lui même congru à* 1 *modulo* 3. *L'entier* $p^4 - 1$ *est donc multiple de* 3 *et* 5.
D'autre part, on a $p^4 - 1 = (p-1)\,(p^3 + p^2 + p + 1)$ *avec p congru à* 1 *ou* 3 *modulo* 4, *puisque p est premier différent de* 2.
Si p est congru à 1 *modulo* 4, *alors* $p - 1$ *est congru à* 0 *modulo* 4, *donc multiple de* 4, *et* $p^3 + p^2 + p + 1$ *est congru à* 0, *modulo* 4, *donc lui aussi multiple de* 4 *et* $p^4 - 1$ *est multiple de* 16.
Si p est congru à 3 *modulo* 4, *il s'écrit alors* $p = 3 + 4q$ *avec* $q \geq 1$ *et :*

$$p^4 - 1 = 432q + 864q^2 + 768q^3 + 256q^4 + 80$$

chaque coefficient de ce polynôme étant multiple de 16, *il en résulte que* $p^4 - 1$ *est multiple de* 16. *D'où le résultat annoncé.*

Exercice 24.25 *Soit* $n \geq 2$. *Montrer que* $n^5 - n$ *est divisible par* 30.

Solution 24.25 *Comme* $n\,(n-1)$ *est pair et* $n\,(n-1)\,(n+1)$ *est multiple de* 3 *(n est congru à* $-1, 0$ *ou* 1 *modulo* 3*)* $m = n^5 - n = n\,(n-1)\,(n+1)\,(n^2+1)$ *est divisible par* 2 *et* 3, *donc par* 6. *Le théorème de Fermat nous dit que* $m = n^5 - n$ *est divisible par* 5, *donc m est divisible par* $30 = 6 \times 5$ *puisque* 6 *est premier avec* 5.

Lemme 24.11 *Soit* $p \geq 5$ *un nombre premier. Pour tout entier k compris entre* 1 *et* $p-1$, *il existe un unique entier r compris entre* 1 *et* $p-1$ *tel que kr soit congru à* 1 *modulo p.*

Démonstration. Pour $k = 1$, on peut prendre $r = 1$.

Tout entier k compris entre 2 et $p-1$ étant premier avec p, il existe deux entiers relatifs u et v tels que $ku + pv = 1$ et ku est congru à 1 modulo p (on peut aussi utiliser le théorème de Fermat : comme k est premier avec p, k^{p-1} est congru à 1 modulo p et $u = k^{p-2}$ convient). En effectuant la division euclidienne de u par p, on a $u = qp + r$ avec r compris entre 0 et $p-1$ et kr est congru à ku, donc à 1, modulo p, ce qui exclu la valeur $r = 0$.

Supposons que l'on ait trouvé un autre entier $s \neq r$ vérifiant la même condition que r. On peut supposer que $s > r$. On a alors $kr \equiv ks \equiv 1$ modulo p avec r, s compris entre 1 et $p-1$, ce qui implique que $k(s-r) \equiv 0$ modulo p, donc p divise $k(s-r)$ en étant premier avec k et en conséquence il doit diviser $s-r$ avec $1 \leq s-r \leq p-1$, ce qui est impossible. L'entier r est donc unique. ∎

Dans le lemme précédent, on aura $k = r$, si, et seulement si, $k^2 - 1 = (k-1)(k+1)$ est divisible par p, donc p doit diviser $k-1$ ou $k+1$, ce qui n'est possible que si $k = 1$ ou $k = p-1$.

Théorème 24.10 (Wilson) *Un entier p supérieur ou égal à 2 est premier si, et seulement si, $(p-1)!$ est congru à -1 modulo p.*

Démonstration. Si p n'est pas premier il s'écrit $p = ab$ avec a et b entiers compris entre 2 et $p-1$. L'entier a est alors un diviseur de $(p-1)!$ et de p qui divise $(p-1)!+1$, donc a divise $(p-1)!+1$ et a divise 1, ce qui est impossible.

Soit $p \geq 2$ un nombre premier. Pour $p = 2$, $(p-1)!+1 = 2$ est congru à 0 modulo 2 et pour $p = 3$, $(p-1)!+1 = 3$ est congru à 0 modulo 3.

Pour $p \geq 5$, en utilisant le lemme précédent, on partitionne l'ensemble $E = \{2, 3, \cdots, p-2\}$ en deux sous-ensembles E_1 et E_2 à $\dfrac{p-3}{2}$ éléments de sorte que :

$$\forall k \in E_1,\ \exists r \in E_2 \mid kr \equiv 1 \mod p$$

et on a alors :

$$(p-1)! = 1 \cdot \left(\prod_{k \in E_1} k\right)\left(\prod_{r \in E_2} r\right)(p-1) \equiv p-1 \equiv -1 \mod p$$

∎

Exercice 24.26 *Montrer qu'un entier p supérieur ou égal à 2 est premier si, et seulement si, $(p-2)!$ est congru à 1 modulo p.*

Solution 24.26 *Pour $p \geq 2$, on a $(p-1)! = (p-1)(p-2)! \equiv -(p-2)!$ modulo p, avec la convention $0! = 1$. Le résultat se déduit alors du théorème de Wilson.*

24.7 Les anneaux $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et la fonction indicatrice d'Euler

Les démonstrations des propositions qui suivent sont faites au paragraphe 25.3.

Théorème 24.11 *Pour $n \geq 2$ il y équivalence entre :*

1. *n est premier ;*
2. *$\mathbb{Z}_n$ est un corps ;*
3. *$\mathbb{Z}_n$ est un intègre.*

Ce résultat nous permet de retrouver le petit théorème de Fermat.

On peut également en déduire le théorème de Wilson.

Le résultat qui suit donne une généralisation du petit théorème de Fermat.

Définition 24.2 *On dit que deux polynômes* P *et* Q *à coefficients entiers sont congrus modulo un nombre premier* p *s'ils sont de mêmes degré et tous leurs coefficients sont égaux modulo* p *(ce qui se traduit aussi par* $P = Q$ *dans l'anneau* $\mathbb{Z}_p[X]$ *des polynômes à coefficients dans le corps* $\mathbb{Z}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$*).*

Théorème 24.12 *p est premier si, et seulement si, il existe un entier relatif n premier avec p tel que $(X+n)^p$ soit congru à $X^p + n$ modulo p.*

Démonstration. On sait que si p est premier, alors pour tout entier k compris entre 1 et $p-1$, p divise $C_p^k = \dfrac{p!}{k!\,(p-k)!}$ (lemme 24.10), ce qui implique en utilisant la formule du binôme de Newton que, que pour tout $n \in \mathbb{Z}$, $(X+n)^p$ est congru à $X^p + n^p$ modulo p et le théorème de Fermat nous dit que n^p est congru à n modulo p.

Si $(X+n)^p$ est congru à $X^p + n$ modulo p, on a alors $C_p^k n^k \equiv 0$ modulo p pour tout k compris entre 1 et $p-1$ et $n^p \equiv n$ modulo p. Comme p est premier avec n et divise $C_p^k n^k$, pour k compris entre 1 et $p-1$, il va diviser C_p^k (théorème de Gauss). On déduit alors du lemme 24.10 que p est premier. ■

Le calcul de $\varphi(n)$ pour $n \geq 2$, où φ est la fonction indicatrice d'Euler, peut se faire en utilisant la décomposition de n en facteurs premiers grâce au théorème chinois.

Théorème 24.13 (chinois) *Les entiers n et m sont premiers entre eux si, et seulement si, les anneaux $\mathbb{Z}_{nm}$ et $\mathbb{Z}_n \times \mathbb{Z}_m$ sont isomorphes.*

Corollaire 24.2 *Si n et m sont deux entiers naturels non nuls premiers entre eux, alors* $\varphi(nm) = \varphi(n)\,\varphi(m)$.

Lemme 24.12 *Soient p un nombre premier et α un entier naturel non nul. On a :*

$$\varphi(p^\alpha) = (p-1)\,p^{\alpha-1}.$$

Théorème 24.14 *Si $n \geq 1$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $2 \leq p_1 < \cdots < p_r$ premiers et les α_i entiers naturels non nuls, alors :*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

De ce résultat on déduit que pour tout $n \geq 3$, $\varphi(n)$ est un entier pair. On déduit également que $\varphi(n)$ est compris entre 1 et n.

Exercice 24.27 *Soient p et q deux nombres premiers distincts et $n = pq$. Montrer que si a et b sont deux entiers naturels tels que $ab \equiv 1 \pmod{\varphi(n)}$, alors pour tout entier relatif c, on a $c^{ab} \equiv c \pmod{n}$. Ce résultat est à la base du système cryptographique R.S.A.*

Solution 24.27 *Si $ab \equiv 1 \pmod{\varphi(n)}$, il existe alors un entier relatif k tel que :*

$$ab = 1 + k\varphi(n) = 1 + k\,(p-1)\,(q-1).$$

Si c est un entier relatif premier avec p, on a alors $c^{p-1} \equiv 1 \pmod{p}$ (théorème de Fermat) et :

$$c^{ab} = cc^{k(p-1)(q-1)} \equiv c \pmod{p}.$$

Si l'entier relatif c n'est pas premier avec p, c'est nécessairement un multiple de p (qui est premier) et :

$$c^{ab} \equiv 0 \equiv c \pmod{p}.$$

De manière analogue, on a $c^{ab} \equiv c \pmod{q}$ et avec p et q premiers entre eux il en résulte que $c^{ab} \equiv c \pmod{pq}$.

Exercice 24.28 *Soit p un nombre premier impair.*

1. *En utilisant l'application $x \mapsto x^2$ de $\mathbb{Z}_p^\times$ dans $\mathbb{Z}_p^\times$, montrer qu'il y a exactement $\dfrac{p-1}{2}$ carrés dans $\mathbb{Z}_p^\times$.*
2. *Montrer que l'ensemble des carrés de $\mathbb{Z}_p^\times$ est l'ensemble des racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \overline{1}$.*
3. *En déduire que $\overline{(-1)}$ est un carré dans $\mathbb{Z}_p$ si, et seulement si, p est congru à 1 modulo 4.*
4. *En déduire qu'il existe une infinité de nombres premiers de la forme $4n+1$.*

Solution 24.28

1. *L'application $\varphi : x \mapsto x^2$ est un morphisme de groupes de $\mathbb{Z}_p^\times$ dans $\mathbb{Z}_p^\times$ de noyau $\ker(\varphi) = \left\{\overline{(-1)}, \overline{1}\right\}$ ($x^2 = 1 \Leftrightarrow (x-1)(x+1) = 0$ et $-1 \neq 1$ dans le corps $\mathbb{Z}_p$ pour $p \geq 3$ premier). On a donc $\operatorname{card}(\operatorname{Im}(\varphi)) = \operatorname{card}\left(\mathbb{Z}_p^\times / \left\{\overline{(-1)}, \overline{1}\right\}\right) = \dfrac{p-1}{2}$, ce qui signifie qu'il y a exactement $\dfrac{p-1}{2}$ carrés dans $\mathbb{Z}_p^\times$ (comme $\overline{0}$ est un carré, il y a exactement $\dfrac{p+1}{2}$ carrés dans $\mathbb{Z}_p$).*
2. *Si $x \in \mathbb{Z}_p^\times$ est un carré, il existe $y \in \mathbb{Z}_p^\times$ tel que $x = y^2$ et $x^{\frac{p-1}{2}} = y^{p-1} = \overline{1}$. Donc les carrés de $\mathbb{Z}_p^\times$ sont racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \overline{1}$. Comme il y a $\dfrac{p-1}{2}$ carrés et au plus $\dfrac{p-1}{2}$ racines du polynôme P dans $\mathbb{Z}_p^\times$, on en déduit l'ensemble $\operatorname{Im}(\varphi)$ des carrés de $\mathbb{Z}_p^\times$ est l'ensemble des racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \overline{1}$.*
3. *On a :*

$$\left(\overline{(-1)} \in \operatorname{Im}(\varphi)\right) \Leftrightarrow \left(\overline{(-1)}^{\frac{p-1}{2}} = \overline{1}\right) \Leftrightarrow \left(\frac{p-1}{2} \equiv 0 \pmod{2}\right)$$
$$\Leftrightarrow (p \equiv 1 \pmod{4})$$

4. *Supposons qu'il y a un nombre fini d'entiers premiers de la forme $4n+1$. On désigne par m le plus grand de ces entiers et par $p \geq 3$ un diviseur premier de $N = (m!)^2 + 1$, on a alors $p > m$ et $\overline{(m!)}^2 = \overline{(-1)}$, donc $\overline{(-1)}$ est un carré dans $\mathbb{Z}_p$ et est premier de la forme $4n+1$, ce qui contredit $p > m$.*