Université Pierre et Marie Curie
Cours de cryptographie MM029 - 2009/10
Alain Kraus

Chapitre I - Arithmétique

Table des matières

1. Plus grand commun diviseur

La notion de « pgcd » de deux entiers joue un rôle très important en cryptographie. Rappelons ici ses principales propriétés. Soient $\mathbb{N}$ l'ensemble des entiers naturels et $\mathbb{Z}$ celui des entiers relatifs. Toute partie non vide $\mathbb{N}$ possède un plus petit élément.

Proposition 1.1 (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*

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

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

Démonstration : Considérons l'ensemble

$$A = \left\{ a - bk \;\middle|\; k \in \mathbb{Z} \right\} \cap \mathbb{N}.$$

C'est une partie non vide de $\mathbb{N}$. Par suite, A possède un plus petit élément r. Puisque r appartient à A, c'est un entier naturel et il existe $q \in \mathbb{Z}$ tel que $a - bq = r$. Vérifions que l'on a $r < |b|$. Supposons le contraire. On obtient

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

et l'inégalité $r - |b| < r$ contredit le caractère minimal de r, d'où l'assertion d'existence. Supposons qu'il existe (q, r) et (q', r') dans $\mathbb{Z} \times \mathbb{Z}$ 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 $|q - q'||b| = |r' - r|$. Puisque r et r' sont positifs, $|r - r'|$ est inférieur ou égal à r ou r', d'où $|r - r'| < |b|$. On obtient $|q - q'| < 1$, d'où $q = q'$ puis $r = r'$, ce qui établit l'unicité.

Afin de définir le plus grand commun diviseur de deux entiers, une façon de procéder est de décrire préalablement les sous-groupes de $\mathbb{Z}$. Pour tout $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$. Inversement :

Lemme 1.1. *Soit H un sous-groupe de $\mathbb{Z}$. Il existe un unique entier $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.*

Démonstration : Si $H = \{0\}$ l'entier $n = 0$ convient. Supposons $H \neq \{0\}$. L'ensemble $A = H \cap \mathbb{N}^*$ n'est pas vide, car si n est dans H, alors $-n$ l'est aussi. Soit n le plus petit élément de A. Vérifions que l'on a $H = n\mathbb{Z}$. Tout d'abord, H étant un sous-groupe de $\mathbb{Z}$, et n étant dans H, $n\mathbb{Z}$ est contenu dans H. Inversement, soit x un élément de H. On a $n \neq 0$. Il existe donc q et r dans $\mathbb{Z}$ tels que $x = nq + r$ avec $0 \leq r < n$ (prop. 1.1). Puisque x et nq appartiennent à H, il en est de même de r. Le caractère minimal de n entraîne $r = 0$, donc x appartient à $n\mathbb{Z}$. Par ailleurs, si l'on a $n\mathbb{Z} = m\mathbb{Z}$ avec m et n dans $\mathbb{N}$, alors m divise n et n divise m, d'où $m = n$.

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

$$a\mathbb{Z} + b\mathbb{Z} = \Big\{ au + bv \;\Big|\; u, v \in \mathbb{Z} \Big\},$$

est un sous-groupe de $\mathbb{Z}$. Il existe donc un unique entier $d \geq 1$ tel que l'on ait

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Définition 1.1. *L'entier d s'appelle le plus grand commun diviseur de a et b, ou en abrégé le pgcd de a et b. On note souvent $d = \mathrm{pgcd}(a, b)$.*

Avec cette définition, on a de fait la propriété de Bézout, à savoir qu'il existe des entiers relatifs u et v tels que l'on ait

$$d = au + bv. \tag{1}$$

On en déduit directement la caractérisation du pgcd de deux entiers :

Lemme 1.2. *Le pgcd de a et b est l'unique entier naturel satisfaisant les conditions suivantes :*

1) c'est un diviseur de a et b.

2) Il est multiple de tout diviseur commun de a et b.

Définition 1.2. *On dit que a et b sont premiers entre eux, ou que a est premier avec b, si l'on a* $\mathrm{pgcd}(a, b) = 1$.

Comme conséquence de (1), on obtient :

Lemme 1.3. *Les entiers a et b sont premiers entre eux si et seulement si il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$.*

Corollaire 1.1. *Les entiers $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.*

Corollaire 1.2 (Théorème de Gauss). *Soit c un entier relatif tel que a divise bc et que a soit premier avec b. Alors a divise c.*

Démonstration : Il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$. On obtient l'égalité $(ac)u + (bc)v = c$, d'où l'assertion.

Exemples 1.1.

1) Soient a et b des entiers naturels tels que $a > b$. On a

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, a - b).$$

En effet, un entier divise a et b si et seulement si il divise b et $a - b$. Cette égalité, utilisée récursivement, permet de calculer le pgcd de a et b. Par exemple, on a

$$\mathrm{pgcd}(48, 30) = \mathrm{pgcd}(30, 18) = \mathrm{pgcd}(18, 12) = \mathrm{pgcd}(12, 6) = \mathrm{pgcd}(6, 6) = 6.$$

Ce procédé est à la base de l'algorithme d'Euclide (voir ci-dessous).

2) Démontrons que tout entier $n \geq 7$ peut s'écrire sous la forme

$$n = a + b \quad \text{avec} \quad \mathrm{pgcd}(a, b) = 1 \quad \text{et} \quad a \geq 2,\ b \geq 2.$$

Si n est impair, la décomposition $n = a + b$ avec $a = 2$ et $b = n - 2$ convient. Supposons n multiple de 4. En posant $n = 4k$, on a $n = a + b$ avec $a = 2k - 1$ et $b = 2k + 1$. Deux nombres impairs consécutifs étant premiers entre eux, on obtient l'assertion dans ce cas. Supposons $n \equiv 2 \bmod. 4$. Posons $n = 4k + 2$. On a alors $n = a + b$ avec $a = 2k + 3$ et

$b = 2k - 1$. L'inégalité $n \geq 7$ entraîne $k \geq 2$, donc a et b sont au moins égaux à 2. On a $a - b = 4$, donc le pgcd de a et b divise 4. Puisque a et b sont impairs, ils sont donc premiers entre eux, d'où le résultat.

3) Soient a et b des entiers relatifs tels que $a > b$. Il existe une infinité d'entiers $n \in \mathbb{N}$ tels que $a + n$ et $b + n$ soient premiers entre eux. Tel est le cas des entiers n de la forme

$$n = (a - b)k + 1 - b,$$

où k est un entier plus grand que $\frac{b-1}{a-b}$. En effet, si d est un diviseur positif de $a + n$ et $b + n$, alors d divise $a - b$, et l'égalité $b + n = (a - b)k + 1$ implique $d = 1$.

4) Pour tout $n \in \mathbb{N}$, posons $F_n = 2^{2^n} + 1$. Un tel entier s'appelle un nombre de Fermat. Soient m et n deux entiers naturels distincts. Vérifions que F_m et F_n sont premiers entre eux. Supposons $n > m$. On a

$$F_n = \left(2^{2^m}\right)^{2^{n-m}} + 1 = \left(F_m - 1\right)^{2^{n-m}} + 1 \equiv 2 \text{ mod. } F_m.$$

Par suite, tout diviseur commun de F_m et F_n divise 2, d'où l'assertion vu que F_m et F_n sont impairs.

Remarque 1.1 (Plus petit commun multiple). Étant donnés des entiers relatifs a et b non nuls, l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. L'entier naturel m tel que

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \tag{2}$$

s'appelle le plus petit commun multiple de a et b. On écrit en abrégé $m = \text{ppcm}(a, b)$. Il est caractérisé par le fait que c'est un multiple de a et b et que tout multiple de a et b est un multiple de m. De plus, on a l'égalité

$$\text{pgcd}(a, b)\,\text{ppcm}(a, b) = |ab|. \tag{3}$$

En effet, si $d = \text{pgcd}(a, b)$, d'après (2) l'entier $\frac{m}{d}$ est le ppcm de $\frac{a}{d}$ et $\frac{b}{d}$. Puisque $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux, afin d'établir (3) on se ramène au cas où $d = 1$. Il s'agit donc de prouver que si a et b sont premiers entre eux, $|ab|$ est le ppcm de a et b. D'abord, $|ab|$ est multiple de a et b. Par ailleurs, si c est un multiple de a et b, il existe des entiers r et s tels que $c = ar = bs$, et d'après le théorème de Gauss a divise s, donc c est multiple de $|ab|$, d'où la formule (3).

2. L'algorithme d'Euclide

Soient a et b deux entiers naturels tels que

$$a > b \geq 1.$$

On va détailler ici l'algorithme d'Euclide étendu, qui permet de déterminer le pgcd de a et b, et de plus d'expliciter une relation de Bézout entre a et b, autrement dit, d'expliciter des entiers relatifs u et v tels que l'on ait $\mathrm{pgcd}(a,b) = au + bv$.

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

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

Supposons construits $r_0, r_1, \cdots, r_i$ 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 $r_0, r_1, \cdots, r_{i-1}, r_i$. Il existe un unique entier $n \geq 1$ tel que la condition suivante soit satisfaite :

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

Proposition 1.2. *On a* $r_n = \mathrm{pgcd}(a,b)$.

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

$$r_{i-1} = q_i r_i + r_{i+1} \quad \text{avec} \quad 0 \leq r_{i+1} < r_i. \tag{4}$$

On a l'égalité

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

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

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

$$r_n = au + bv.$$

Le problème qui nous intéresse alors 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

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

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

où q_i est défini par l'égalité (4), autrement dit, où q_i est le quotient de la division euclidienne de r_{i-1} par r_i.

Proposition 1.3. *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	0
1	0	u_2	$\cdots$	u_{n-1}	u_n	
0	1	v_2	$\cdots$	v_{n-1}	v_n	

Exemple 1.2. Avec $a = 20825$ et $b = 455$, on obtient le tableau :

	45	1	3	3	
20825	455	350	105	35	0
1	0	1	-1	4	
0	1	-45	46	-183	

On a donc $\mathrm{pgcd}(a, b) = 35$ et l'on obtient la relation de Bézout

$$4 \times 20825 - 183 \times 455 = 35.$$

Avec les notations précédentes, l'entier n est le nombre de divisions euclidiennes à effectuer pour déterminer r_n. On dit que n est le nombre de pas nécessaires dans l'algorithme d'Euclide pour obtenir le pgcd de a et b. Donnons une majoration de n.

Théorème 1.1. *On a l'inégalité*

$$n \leq \frac{3}{2 \log 2} \log b + 1.$$

Afin de prouver cet énoncé, introduisons la suite de Fibonacci définie par les égalités

$$U_0 = 0, \quad U_1 = 1 \quad \text{et} \quad U_{k+1} = U_k + U_{k-1} \quad \text{pour } k \geq 1.$$

On vérifie par récurrence que pour tout $k \geq 1$, on a l'égalité matricielle

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} U_{k+1} & U_k \\ U_k & U_{k-1} \end{pmatrix}.$$

On en déduit par exemple l'égalité

$$U_{k+1} U_{k-1} - U_k^2 = (-1)^k,$$

qui entraîne que U_k et U_{k+1} sont premiers entre eux.

Proposition 1.4 (Lamé, 1845). *Posons* $d = \mathrm{pgcd}(a, b)$. *On a*

$$a \geq dU_{n+2} \quad et \quad b \geq dU_{n+1}. \tag{5}$$

Démonstration : Si $n = 1$, l'entier a est alors multiple de b et l'on a

$$d = b \quad \text{et} \quad a \geq 2b.$$

Vu que l'on a $U_2 = 1$ et $U_3 = 2$, les inégalités (5) sont donc vérifiées dans ce cas. Supposons $n \geq 2$ et l'énoncé vrai pour l'entier $n - 1$. Le premier pas de l'algorithme transforme le couple (a, b) en (b, c), où c est le reste de la division euclidienne de a par b (avec les notations utilisées précédemment on a $c = r_2$). Par définition, l'algorithme d'Euclide, partant du couple (b, c) pour obtenir d, s'arrête au bout de $n - 1$ pas. D'après l'hypothèse de récurrence, on obtient

$$b \geq dU_{n+1} \quad \text{et} \quad c \geq dU_n.$$

Puisque l'on a $a \geq b + c$, on en déduit l'inégalité

$$a \geq d\big(U_{n+1} + U_n\big) = dU_{n+2},$$

ce qui prouve la condition (5) pour l'entier n.

Remarque 1.2. Pour tout $k \geq 1$, le pgcd de U_{k+2} et U_{k+1} est 1, et sa détermination par l'algorithme d'Euclide nécessite k pas. Avec $a = U_{k+2}$ et $b = U_{k+1}$, les inégalités (5) sont donc des égalités.

Lemme 1.4. *Pour tout* $k \in \mathbb{N}$, *on a*

$$U_{k+1} \geq 2^{\frac{2(k-1)}{3}}.$$

Démonstration : C'est vrai pour $k = 0$ et $k = 1$. Soit k un entier ≥ 1 tel que cette inégalité soit vraie pour les entiers $k - 1$ et k. On a

$$U_{k+2} = U_{k+1} + U_k \geq 2^{\frac{2(k-1)}{3}} + 2^{\frac{2(k-2)}{3}}.$$

L'inégalité

$$2^{-\frac{2}{3}} + 2^{-\frac{4}{3}} \geq 1$$

entraîne alors le résultat.

Le théorème se déduit comme suit. D'après la proposition 1.4, on a $U_{n+1} \leq b$. Compte tenu du lemme 1.4, on obtient

$$2^{\frac{2(n-1)}{3}} \leq b,$$

et la majoration annoncée.

3. Nombres premiers

Définition 1.3. *On appelle nombre premier tout entier $p \geq 2$ dont les seuls diviseurs positifs sont* 1 *et* p.

Lemme 1.5. *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, donc p n'est pas premier. Inversement, si p n'est pas premier, il a un diviseur positif a autre que 1 et p. On a alors $p = ab$, où a et b sont ≥ 2.

Proposition 1.5. *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 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 des entiers a et b strictement plus grands que 1 tels que $n = ab$. Puisque l'on a $2 \leq a < n$ et $2 \leq b < n$, les propriétés $P(a)$ et $P(b)$ sont vraies, d'où le résultat.

Corollaire 1.3 (Euclide). *L'ensemble des nombres premiers est infini.*

Démonstration : Supposons que cet ensemble soit fini de cardinal n. Soient $p_1, \cdots, p_n$ 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.

Remarques 1.3.

1) Ce résultat peut aussi se déduire de la proposition 1.5 et du fait que deux nombres de Fermat distincts sont premiers entre eux (exemples 1.1).

2) Donnons une démonstration, due à Euler, du fait que la somme

$$\sum_p \frac{1}{p}$$

où p parcourt l'ensemble des nombres premiers, est infinie. Cela entraîne évidemment le corollaire 1.3. Soit N un entier ≥ 1. D'après la proposition 1.5, tout entier compris entre 2 et N s'écrit comme un produit de nombres premiers $p \leq N$, affectés d'exposants inférieurs ou égaux à la partie entière de $\frac{\log N}{\log p}$. Il en résulte l'inégalité

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{\substack{p \leq N \\ p \ premier}} \left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{t_p}}\right) \quad \text{où} \quad t_p = \left[\frac{\log N}{\log p}\right],$$

d'où

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{\substack{p \leq N \\ p \text{ premier}}} \sum_{k \geq 0} \frac{1}{p^k} = \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}}.$$

Pour tout nombre premier $p \leq N$, on a

$$-\log\Big(1 - \frac{1}{p}\Big) = \sum_{k \geq 1} \frac{1}{kp^k} \leq \frac{1}{p} + \frac{1}{p^2}\left(\frac{1}{1 - \frac{1}{p}}\right) \leq \frac{1}{p} + \frac{1}{(p-1)^2}.$$

On obtient

$$\log \sum_{n=1}^{N} \frac{1}{n} \leq \sum_{p \leq N} \frac{1}{p} + \sum_{p \leq N} \frac{1}{(p-1)^2} \leq \sum_{p \leq N} \frac{1}{p} + \sum_{n \leq N} \frac{1}{n^2}.$$

La série $\sum \frac{1}{n}$ étant divergente et la somme $\sum \frac{1}{n^2}$ étant finie, cela implique le résultat.

Lemme 1.6 (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. La démonstration qui suit est due à Gauss. Supposons que p ne divise pas a. Il s'agit de montrer que p divise b. Considérons l'ensemble

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

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

$$m \geq 2. \tag{6}$$

Soit n un élément de A. Vérifions que m divise n. 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 (6) et le fait que p soit premier entraînent alors $p = m$. Par suite, p divise b.

Corollaire 1.4. *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.*

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

Théorème 1.2. *Tout entier $n \geq 2$ s'écrit de façon unique sous la forme*

$$n = p_1^{n_1} \cdots p_r^{n_r}, \tag{7}$$

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 tout $i = 2, \cdots, r$. On dit que l'égalité (7) *est la décomposition de n en produit de nombres premiers.*

Démonstration : L'assertion d'existence résulte de la proposition 1.5. 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 1.4 que l'on a

$$\Big\{p_1, \cdots, p_r\Big\} = \Big\{q_1, \cdots, q_s\Big\}.$$

Par suite, on a $r = s$. De plus, p_1 est le plus petit élément de $\big\{p_1, \cdots, p_r\big\}$ et q_1 est le plus petit élément de $\big\{q_1, \cdots, q_r\big\}$, 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, d'où une contradiction (cor. 1.4).

Remarque 1.4. Soit n un entier ≥ 2. Si n n'est pas premier, alors n possède un diviseur premier p tel que $p^2 \leq n$. En effet, si n n'est pas premier, il existe deux entiers a et b strictement plus grands que 1 tels que $n = ab$. Supposons $a \leq b$. Puisque $a \geq 2$, a possède un diviseur premier p. En particulier, p divise n et l'on a $p^2 \leq ap \leq ab = n$.
Par exemple, 641 est premier, sinon il devrait exister un nombre premier $p < 25$ divisant 641. Or les nombres premiers plus petits que 25 sont $2, 3, 5, 7, 11, 13, 17, 19$ et 23, et aucun d'eux ne divise 641.

Remarque 1.5. Soient a et b des entiers ≥ 2. Supposons connues leurs décompositions en facteurs premiers. Dans ce cas, il est immédiat de déterminer leur pgcd d. Pour tout nombre premier p, l'exposant de p dans la décomposition en facteurs premiers de d est le minimum des exposants de p intervenant dans celles de a et b. Cela étant, on ne parvient pas en général à factoriser un entier, ayant plus de deux cent cinquante chiffres décimaux, en produit de nombres premiers. L'efficacité de certains cryptosystèmes est précisément basée sur cette difficulté.

4. La fonction de comptage des nombres premiers

Notons, comme il est d'usage, π la fonction de comptage des nombres premiers. Pour tout réel x positif, $\pi(x)$ est le nombre des nombres premiers inférieurs ou égaux à x. Par exemple, on a

$$\pi(2) = 1, \quad \pi(100) = 25, \quad \pi(10^5) = 9592, \quad \pi(10^8) = 5761455, \quad \pi(10^9) = 50847534.$$

La plus grande valeur connue de la fonction π se situe aujourd'hui aux environs de 10^{23}. Il importe en cryptographie de connaître le comportement de $\pi(x)$ quand x tend vers l'infini, notamment dans l'étude des tests de primalité et des méthodes de factorisation. En analysant des tables de nombres premiers, Gauss et Legendre à la fin du dix-huitième siècle ont observé que si x est « assez grand », la probabilité pour qu'un entier proche de x soit premier semblait être $\frac{1}{\log x}$. Cela les a conduit à conjecturer, sous une forme ou une autre, que $\frac{x}{\log x}$ devait être une bonne approximation asymptotique de $\pi(x)$. Cela s'est avéré exact. J. Hadamard et C. de la Vallée Poussin ont démontré indépendamment en 1896 le résultat suivant.

Théorème 1.3 (Théorème des nombres premiers). *Quand x tend vers l'infini, on a*

$$\pi(x) \sim \frac{x}{\log x}.$$

Sa démonstration relève de la théorie analytique des nombres. La fonction logarithme-intégral

$$\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\log t}$$

est intimement liée à ce théorème. Lorsque x tend vers l'infini, on vérifie par exemple avec une intégration par parties que l'on a

$$\mathrm{Li}(x) \sim \frac{x}{\log x}.$$

Les fonctions $\mathrm{Li}(x)$ et $\pi(x)$ sont donc équivalentes quand x tend vers l'infini. C'est d'ailleurs sous cette forme que Gauss avait formulé sa conjecture sur $\pi(x)$. En fait, $\mathrm{Li}(x)$ est une bien meilleure approximation de $\pi(x)$ que $\frac{x}{\log x}$. Par exemple, on a

$$\pi\big(10^{21}\big) = 21127269486018731928, \quad \mathrm{Li}\big(10^{21}\big) \simeq 21127269486616126181,3,$$

$$\frac{10^{21}}{\log 10^{21}} \simeq 20680689614440563221,4.$$

Le terme d'erreur $\pi(x) - \mathrm{Li}(x)$ a été l'objet de recherches intensives durant le vingtième siècle, et est encore loin d'avoir livré tous ses secrets. La différence $\pi(x) - \mathrm{Li}(x)$ est liée à l'hypothèse de Riemann concernant les zéros de la fonction zéta. Rappelons que la fonction ζ de Riemann est une fonction holomorphe sur $\mathbb{C}\backslash\{1\}$, ayant un pôle simple en 1, où le résidu est 1, telle que

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} \quad \text{pour } \mathrm{Re}(s) > 1.$$

Dans le demi-plan $\mathrm{Re}(s) > 0$ privé de 1, on a l'égalité

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{+\infty} \frac{\{u\}}{u^{1+s}}\mathrm{d}u \quad \text{avec } \{u\} = u - [u],$$

où $[u]$ est la partie entière de u. Riemann à proposé cette conjecture, qui est centrale en mathématiques :

Conjecture (Hypothèse de Riemann). *Tous les zéros de la fonction ζ dans la bande critique $0 < \mathrm{Re}(s) < 1$ sont sur la droite $\mathrm{Re}(s) = \frac{1}{2}$.*

Signalons qu'il est relativement facile de démontrer que l'on a $\zeta(s) \neq 0$ pour tout s dans le demi-plan $\mathrm{Re}(s) \geq 1$. Von Koch a établi en 1901 que l'hypothèse de Riemann est équivalente à l'estimation suivante :

$$\pi(x) - \mathrm{Li}(x) = O\big(\sqrt{x}\log x\big)^{(1)}.$$

Plus précisément, l'hypothèse de Riemann équivaut à l'énoncé suivant :

Conjecture. *Pour tout $x \geq 2,01$, on a*

$$|\pi(x) - \mathrm{Li}(x)| \leq \sqrt{x}\log x.$$

P. Chebyshev, vers le milieu du dix-neuvième siècle, est le premier à avoir établi des résultats importants concernant l'estimation asymptotique de fonction $\pi(x)$. Il a démontré que $\frac{x}{\log x}$ est effectivement le bon ordre de grandeur de $\pi(x)$, en prouvant les inégalités,

$$0,9\frac{x}{\log x} \leq \pi(x) \leq 1,2\frac{x}{\log x} \quad \text{pour tout } x \geq 30.$$

Cela implique au passage l'existence d'un nombre premier entre n et $2n$ pour tout entier $n \geq 1$, ce résultat étant connu sous le nom de postulat de Bertrand. De plus, il avait prouvé que si $\frac{\pi(x)\log x}{x}$ possède une limite à l'infini, alors cette limite est 1. Cela étant, la difficulté essentielle du théorème des nombres pemiers est d'établir que la limite de $\frac{\pi(x)\log x}{x}$ existe quand x tend vers l'infini. On va se limiter ici à démontrer un énoncé qui ne permet pas de retrouver le postulat de Bertrand, mais qui néanmoins met en évidence l'ordre de grandeur de $\pi(x)$.

---

(1) Étant données des fonctions f et g définies sur un intervalle de la forme $[a, +\infty[$ à valeurs réelles, la relation

$$f(x) = O\big(g(x)\big) \quad \text{quand } x \text{ tend vers } +\infty,$$

signifie qu'il existe un nombre $M > 0$, tel que pour tout x assez grand, on ait

$$|f(x)| \leq M|g(x)|.$$

Théorème 1.4. *Pour tout nombre réel $x \geq 2$, on a*

$$\left(\frac{\log 2}{2}\right)\frac{x}{\log x} \leq \pi(x) \leq (9\log 2)\frac{x}{\log x}.$$

Considérons les fonctions arithmétiques traditionnellement notées Λ, ψ et θ. La fonction Λ de von Mangolt est définie sur $\mathbb{N}$ par

$$\Lambda(n) = \begin{cases} \log p & \text{si } \ n = p^\alpha \text{ avec } p \text{ premier et } \alpha \geq 1 \\ 0 & \text{sinon.} \end{cases}$$

Les fonctions ψ et θ sont définies sur $\mathbb{R}$ par

$$\psi(x) = \sum_{n \leq x} \Lambda(n) \quad \text{et} \quad \theta(x) = \sum_{\substack{p \leq x \\ p \ premier}} \log p.$$

Pour tout entier $N \geq 1$, on vérifie directement que l'on a

$$\exp\big(\psi(N)\big) = \text{ppcm}(1, \cdots, N), \tag{8}$$

où $\text{ppcm}(1, \cdots, N)$ est le plus petit commun multiple des entiers naturels non nuls inférieurs ou égaux à N.

Démonstration du théorème 1.4 : 1) Démontrons la minoration. Vérifions que l'on a

$$\psi(2n+1) \geq 2n\log 2 \quad \text{pour tout } n \in \mathbb{N}. \tag{9}$$

Considérons pour cela l'intégrale

$$I = \int_0^1 x^n(1-x)^n \mathrm{d}x.$$

D'après la formule du binôme de Newton, I est une somme de nombres rationnels dont les dénominateurs sont tous plus petits que $2n+1$. De plus, on a $I > 0$ (une fonction continue positive sur $[0,1]$, d'intégrale nulle sur $[0,1]$, est nulle). Compte tenu de (8), il en résulte que $\exp\big(\psi(2n+1)\big)I$ est un entier naturel non nul. Par ailleurs, on a $4x^2-4x+1 = (2x-1)^2 \geq 0$, d'où $x(1-x) \leq \frac{1}{4}$ pour tout $x \in [0,1]$. On en déduit que l'on a

$$I \leq \frac{1}{4^n}.$$

On obtient ainsi les inégalités

$$1 \leq \exp\big(\psi(2n+1)\big)I \leq \frac{\exp\big(\psi(2n+1)\big)}{4^n},$$

ce qui entraîne (9). Soit alors x un nombre réel au moins 6. Soit n l'entier naturel tel que

$$2n-1 \leq x < 2n+1.$$

La fonction ψ étant croissante, on a $\psi(x) \geq \psi(2n-1)$. D'après (9), on obtient

$$\psi(x) \geq 2(n-1)\log 2 > (x-3)\log 2.$$

Puisque $x \geq 6$, on a $x - 3 \geq \frac{x}{2}$, d'où l'inégalité

$$\psi(x) \geq \frac{x \log 2}{2}.$$

Par ailleurs, dans la somme des $\Lambda(n)$ pour $n \leq x$, la contribution relative à chaque nombre premier $p \leq x$ est $r_p \log p$, où p^{r_p} est la plus grande puissance de p inférieure à x. Cette contribution est donc inférieure à $\log x$, ce qui implique

$$\psi(x) \leq \pi(x)\log x,$$

d'où la minoration annoncée pour $x \geq 6$. Elle vaut en fait dès que $x \geq 2$, car la fonction $f(x) = \frac{x}{\log x}$ est décroissante sur $[2, e]$, croissante sur $[e, +\infty[$, et l'on a

$$\pi(x) = 1 = \frac{\log 2}{2} f(2) \quad \text{si } x \in [2, e], \qquad \pi(x) = 1 \geq \frac{\log 2}{2} f(3) \quad \text{si } x \in [e, 3[,$$

$$\pi(x) \geq 2 \geq \frac{\log 2}{2} f(6) \quad \text{si } x \in [3, 6].$$

2) Passons à la majoration. Vérifions que l'on a

$$\theta\big(2^r\big) \leq 2^{r+1}\log 2 \quad \text{pour tout } r \in \mathbb{N}. \tag{10}$$

On a $(2n)! = (n!)^2 C_{2n}^n$, donc pour tout $n \in \mathbb{N}$,

$$\prod_{\substack{n<p\leq 2n \\ p \text{ premier}}} p \quad \text{divise} \quad C_{2n}^n.$$

D'après l'égalité $(1+1)^{2n} = 2^{2n}$, on a $C_{2n}^n \leq 2^{2n}$. Il en résulte que l'on a

$$\theta(2n) - \theta(n) = \sum_{n<p\leq 2n} \log p \leq 2n \log 2.$$

On obtient alors (10) par récurrence. Soit t la partie entière de $\frac{\log x}{\log 2}$. Par définition, on a

$$2^t \leq x < 2^{t+1}.$$

En utilisant (10), on en déduit les inégalités

$$\theta(x) \leq \theta\big(2^{t+1}\big) \leq 2^{t+2} \log 2 \leq 4x \log 2.$$

En particulier, on a

$$\sum_{\sqrt{x}<p\leq x} \log p \leq 4x \log 2.$$

Cela implique

$$\big(\pi(x) - \pi(\sqrt{x})\big) \frac{\log x}{2} \leq 4x \log 2,$$

d'où, vu que $\pi(\sqrt{x})$ est plus petit que $\sqrt{x}$,

$$\pi(x) \leq \frac{8x \log 2}{\log x} + \sqrt{x}.$$

En étudiant les variations de la fonction qui à x associe $\sqrt{x} \log 2 - \log x$, on constate que l'on a

$$\sqrt{x} \leq \frac{x \log 2}{\log x} \quad \text{dès que } x \geq 16,$$

d'où le résultat dans ce cas. Par ailleurs, pour tout $x \in [2, 16]$, on a

$$\pi(x) \leq \pi(16) = 6 \leq 9 \log 2 \quad \text{et} \quad 1 \leq \frac{x}{\log x}.$$

Cela termine la démonstration du théorème.

5. Numération en base b

Considérons un entier $b \geq 2$.

Théorème 1.5. *Soit x un entier naturel non nul. On peut écrire x de manière unique sous la forme*

$$x = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0, \tag{11}$$

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

Démonstration : Démontrons l'assertion d'existence. Notons pour cela $P(x)$ la propriété : x possède une écriture de la forme (11) 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 (11). 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 $q = a_n b^{n-1} + \cdots + a_2 b + a_1$, 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 (11) 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

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

Il en résulte que n est la partie entière de $\frac{\log x}{\log b}$. 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.

Remarque 1.6. Pour tout entier $x \geq 1$, le nombre de chiffres intervenant dans l'écriture de x en base b est un plus la partie entière de $\frac{\log x}{\log b}$.

Exemple 1.3. On vérifie que l'on a $101 = 2^6 + 2^5 + 2^2 + 1$, de sorte que l'écriture de 101 en base 2 est 1100101 i.e. on a $101 = (1100101)_2$.

Donnons une application de ce théorème.

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

$$\frac{2 \log n}{\log 2}$$

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 $0 \leq j \leq k$. On peut donc calculer x^n avec $i_k + k$ multiplications. Par ailleurs, on a

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

On obtient

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

d'où notre assertion.

Exemple 1.4. 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.

6. Le théorème chinois

Pour tout entier $n \geq 1$, rappelons que $\mathbb{Z}/n\mathbb{Z}$ désigne l'anneau des entiers modulo n.

Théorème 1.6 (Théorème chinois). *Soient m et n des entiers naturels non nuls premiers entre eux. L'application*

$$f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

définie pour tout $a \in \mathbb{Z}$ par l'égalité

$$f(a) = \big(a + m\mathbb{Z}, a + n\mathbb{Z}\big),$$

est un morphisme d'anneaux surjectif, de noyau $mn\mathbb{Z}$. En particulier, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes, via l'application qui à tout élément $a + mn\mathbb{Z}$ de $\mathbb{Z}/mn\mathbb{Z}$ associe le couple $\big(a + m\mathbb{Z}, a + n\mathbb{Z}\big)$.

Remarque 1.7. Le contenu essentiel de cet énoncé réside dans le fait que f soit une application surjective de $\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Autrement dit, étant donnés des entiers relatifs a et b, il existe $c \in \mathbb{Z}$ tel que l'on ait

$$c \equiv a \text{ mod. } m \quad \text{et} \quad c \equiv b \text{ mod. } n. \tag{12}$$

Démonstration : Il résulte directement de la définition de la structure d'anneau produit sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (exemples 0.10) que f est un morphisme d'anneaux. Vérifions que l'on a

$$\mathrm{Ker}(f) = mn\mathbb{Z}.$$

Si a est un élément de $\mathrm{Ker}(f)$, on a $\big(a+m\mathbb{Z}, a+n\mathbb{Z}\big) = (m\mathbb{Z}, n\mathbb{Z})$, autrement dit, on a $a \equiv 0$ mod. m et $a \equiv 0$ mod. n. Puisque m et n sont premiers entre eux, on en déduit que mn divise a, i.e. que $a \in mn\mathbb{Z}$. Inversement, si a est dans $mn\mathbb{Z}$, alors a est divisible par m et n, donc a est dans $\mathrm{Ker}(f)$, d'où l'assertion
Prouvons que f est surjectif. Considérons pour cela un élément $\big(a+m\mathbb{Z}, b+n\mathbb{Z}\big)$ de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Puisque m et n sont premiers entre eux, il existe des entiers u et v tels que l'on ait

$$mu + nv = 1. \tag{13}$$

Posons alors

$$c = b(mu) + a(nv). \tag{14}$$

On vérifie que l'on a les congruences $c \equiv a$ mod. m et $c \equiv b$ mod. n, autrement dit que l'on a $f(c) = \big(a+m\mathbb{Z}, b+n\mathbb{Z}\big)$, d'où l'assertion, et le résultat (th. 0.6).

Remarque 1.8. La démonstration précédente est effective, au sens où si a et b sont deux entiers relatifs donnés, elle permet d'expliciter un entier c vérifiant les congruences (12). En effet, il suffit pour cela de déterminer des entiers u et v vérifiant l'égalité (13), ce que l'on peut faire en utilisant par exemple l'algorithme d'Euclide. On peut alors prendre comme entier c celui défini par l'égalité (14). Il est unique modulo $mn\mathbb{Z}$.

Exemple 1.5. Soit n un entier naturel impair. Notons r le nombre de ses diviseurs premiers. Soit S l'ensemble des solutions dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ de l'équation

$$x^2 = 1.$$

En notant $|S|$ le cardinal de S, vérifions que l'on a

$$|S| = 2^r. \tag{15}$$

Soit $n = p_1^{n_1} \cdots p_r^{n_r}$ la décomposition de n en produit de nombres premiers. Soit

$$f : \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/p_i^{n_i}\mathbb{Z},$$

le morphisme d'anneaux défini par $f(x+n\mathbb{Z}) = (x+p_1^{n_1}\mathbb{Z}, \cdots, x+p_r^{n_r}\mathbb{Z})$. D'après le théorème chinois, c'est un isomorphisme. Posons

$$T = \Big\{ \big(\varepsilon_1 + p_1^{n_1}\mathbb{Z}, \cdots, \varepsilon_r + p_r^{n_r}\mathbb{Z}\big) \;\Big|\; \varepsilon_i = \pm 1 \quad \text{pour} \quad i = 1, \cdots, r \Big\}.$$

Vérifions que l'on a

$$S = f^{-1}(T). \tag{16}$$

Soit $x + n\mathbb{Z}$ un élément de S. Pour tout $i = 1, \cdots, r$, on a $x^2 \equiv 1$ mod. $p_i^{n_i}$. Le pgcd de $x-1$ et $x+1$ est 1 ou 2. Puisque n est impair, $p_i^{n_i}$ divise donc $x-1$ ou bien $x+1$. Par suite, $f(x+n\mathbb{Z})$ est dans T, et S est contenu dans $f^{-1}(T)$. Inversement, si $x+n\mathbb{Z}$ est dans $f^{-1}(T)$, on a $x^2 \equiv 1$ mod. $p_i^{n_i}$ pour tout i. Cela implique $x^2 \equiv 1$ mod. n, autrement dit, $x + n\mathbb{Z}$ est dans S, d'où (16). Puisque T est de cardinal 2^r (les p_i sont impairs), il en est de même de S. Cela établit l'égalité (15).

Afin d'expliciter S, on est donc amené à résoudre les systèmes de r congruences

$$x \equiv \varepsilon_1 \text{ mod. } p_1^{n_1}, \quad \cdots \quad , x \equiv \varepsilon_r \text{ mod. } p_r^{n_r},$$

pour les 2^r systèmes de signes $(\varepsilon_1, \cdots, \varepsilon_r)$. Il suffit en fait d'en résoudre 2^{r-1} par un choix convenable de systèmes de signes, en prenant ensuite les solutions opposées à celles déjà obtenues.
Par exemple, si $n = 735$, l'ensemble S est formé des classes modulo n des entiers ± 1, ± 146, ± 244 et ± 344.

Il convient de remarquer que la résolution de l'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$ nécessite, a priori, la connaissance de la factorisation de n en produit de nombres premiers. Si l'on savait résoudre cette équation sans utiliser cette factorisation, il serait alors facile de trouver la factorisation de n. En effet, si a est un entier tel que $a^2 \equiv 1$ mod. n et $a \not\equiv \pm 1$ mod. n, le calcul du pgcd de $a+1$ (ou $a-1$) avec n fournit un diviseur non trivial de n. Le problème de la factorisation des entiers serait ainsi résolu, et la sécurité de nombreux cryptosystèmes serait complètement remise en cause. On aura l'occasion de revenir sur ce problème.

7. La fonction indicatrice d'Euler

Il s'agit de la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}$ définie comme suit.

Définition 1.4 (Fonction indicatrice d'Euler). *Pour tout $n \geq 1$, l'entier $\varphi(n)$ est le nombre des entiers compris entre 1 et n, et premiers avec n. Autrement dit, $\varphi(n)$ est le nombre des entiers k pour lesquels on a*

$$1 \leq k \leq n \quad et \quad \text{pgcd}(k, n) = 1.$$

Par exemple, on a $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, et pour tout nombre premier p, on a $\varphi(p) = p - 1$. Plus généralement :

Lemme 1.7. *Pour tout nombre premier p et tout entier $r \geq 1$, on a*

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

Démonstration : Il y a p^{r-1} entiers multiples de p entre 1 et p^r, d'où l'assertion.

Explicitons $\varphi(n)$ pour tout $n \geq 1$. On va voir en particulier que $\frac{\varphi(n)}{n}$ ne dépend que de l'ensemble des diviseurs premiers de n. Considérons pour cela le groupe $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ formé des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Rappelons d'abord l'énoncé suivant :

Lemme 1.8. *Soit n un entier ≥ 1. Soient a un entier et $\overline{a}$ sa classe modulo $n\mathbb{Z}$. Alors, $\overline{a}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a et n sont premiers entre eux. Autrement dit, on a*

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \left\{\overline{a} \;\middle|\; 1 \leq a \leq n \text{ et } \operatorname{pgcd}(a,n) = 1\right\}.$$

Démonstration : Supposons $\overline{a}$ inversible. Il existe $b \in \mathbb{Z}$ tel que l'on ait $ab \equiv 1$ mod. n, autrement dit, il existe $c \in \mathbb{Z}$ tel que $ab + nc = 1$, ce qui prouve que a et n sont premiers entre eux. Inversement, il existe des entiers u et v tels que l'on ait $au + nv = 1$. Ainsi $\overline{a}$ est inversible, d'inverse la classe de u modulo n.

Corollaire 1.5. *L'ordre de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ est $\varphi(n)$.*

Corollaire 1.6. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

Démonstration : L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si tous ses éléments non nuls sont inversibles. Par suite, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $\varphi(n) = n - 1$, ce qui implique l'assertion.

Corollaire 1.7. *Soient m et n des entiers naturels non nuls premiers entre eux. On a*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Démonstration : Les entiers m et n étant premiers entre eux, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes (th. 1.6). Les groupes des éléments inversibles de ces anneaux ont donc le même ordre. Le corollaire 1.5 et le lemme 0.7 entraînent alors le résultat.

Théorème 1.7. *Soit n un entier ≥ 1. On a l'égalité*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \tag{17}$$

où p parcourt l'ensemble des diviseurs premiers de n.

Démonstration : On peut supposer $n \geq 2$. Soit $\left\{p_1, \cdots, p_r\right\}$ l'ensemble des diviseurs premiers de n. Soit

$$n = \prod_{i=1}^{r} p_i^{n_i},$$

la décomposition en facteurs premiers de n. D'après le corollaire 1.7, on a

$$\varphi(n) = \prod_{i=1}^{r} \varphi\big(p_i^{n_i}\big).$$

Par ailleurs, on a (lemme 1.7)

$$\varphi\big(p_i^{n_i}\big) = p_i^{n_i}\left(1 - \frac{1}{p_i}\right),$$

d'où l'égalité (17).

Indiquons quelques propriétés de la fonction φ.

Corollaire 1.8. *Pour tout $n \geq 3$, l'entier $\varphi(n)$ est pair.*

Démonstration : Compte tenu de l'égalité (17), si n possède un diviseur premier impair p, alors $p-1$ est pair, et il en est donc de même de $\varphi(n)$. Si n est une puissance de 2, disons $n = 2^r$ avec $r \geq 2$, alors $\varphi(n) = 2^{r-1}$.

Corollaire 1.9. *Soient m et n des entiers naturels non nuls tels que m divise n. Alors $\varphi(m)$ divise $\varphi(n)$.*

Démonstration : Soit P_m (resp. P_n) l'ensemble des diviseurs premiers de m (resp. de n). On a les égalités (th. 1.7)

$$\frac{\varphi(n)}{\varphi(m)} = \frac{n}{m} \prod_{p \in P_n - P_m} \left(1 - \frac{1}{p}\right). \tag{18}$$

Pour tout nombre premier $p \in P_n - P_m$, p divise n sans diviser m, donc p divise $\frac{n}{m}$. Il en résulte que le second membre de l'égalité (18) est un entier.

L'implication réciproque de ce corollaire est fausse, comme le montre les égalités $\varphi(3) = \varphi(4) = 2$. Remarquons que l'énoncé précédent peut aussi se déduire du résultat suivant, qui est une conséquence du théorème chinois :

Lemme 1.9. *Soient m et n des entiers naturels non nuls tels que m divise n. L'application $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ définie par $f(a + n\mathbb{Z}) = a + m\mathbb{Z}$, est un morphisme de groupes surjectif de $(\mathbb{Z}/n\mathbb{Z})^*$ sur $(\mathbb{Z}/m\mathbb{Z})^*$.*

Démonstration : On remarque d'abord que f est bien définie. Le fait que f soit un morphisme de groupes résulte directement de la définition. On écrit ensuite n sous la forme $n = m'r$, où m et m' ont les mêmes facteurs premiers et où r est premier à m'. L'entier m

divise m' et r est premier à m. Soit $d + m\mathbb{Z}$ un élément de $(\mathbb{Z}/m\mathbb{Z})^*$. D'après le théorème chinois, il existe un entier a tel que

$$a \equiv d \text{ mod. } m \quad \text{et} \quad a \equiv 1 \text{ mod. } r.$$

Vérifions que a est premier à n. Supposons qu'il existe un nombre premier p qui divise a et n. Alors, p ne divise pas r, donc p divise m'. Par suite, p divise m et d, ce qui contredit le fait que d et m sont premiers entre eux. On a ainsi $f(a + n\mathbb{Z}) = d + m\mathbb{Z}$, d'où l'assertion.

Lemme 1.10. *Pour tout $n \geq 1$, on a l'égalité*

$$n = \sum_{d|n} \varphi(d),$$

où d parcourt l'ensemble des diviseurs de n.

Démonstration : Considérons l'ensemble $F = \left\{\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n-1}{n}, \frac{n}{n} = 1\right\}$. Pour tout diviseur d de n, posons $F_d = \left\{\frac{a}{d} \mid 1 \leq a \leq d \text{ et } \operatorname{pgcd}(a, d) = 1\right\}$. L'ensemble F est la réunion disjointe des F_d, d'où le résultat vu que le cardinal de F est n et que celui de F_d est $\varphi(d)$.

Terminons ce paragraphe en citant l'une des nombreuses conjectures concernant la fonction φ. Celle-ci a été proposée par Carmichael en 1922 :

Conjecture. *Quel que soit $n \geq 1$, il existe un entier $m \neq n$ tel que $\varphi(m) = \varphi(n)$.*

C'est évident si n est impair, vu que l'on a dans ce cas $\varphi(2n) = \varphi(n)$, ou bien si $n = 2m$ avec m impair, car on a alors $\varphi(n) = \varphi(m)$. Toute la difficulté concerne les entiers n divisibles par 4. On sait que s'il existe un entier n contredisant cette conjecture, il doit avoir plus de 10^7 chiffres décimaux. Signalons cependant qu'il existe des entiers n pour lesquels il n'existe pas d'entiers impairs m tels que $\varphi(m) = \varphi(n)$. Tel est par exemple le cas de $n = 2^9 \times 257^2$. Notons par ailleurs, qu'un entier $a \geq 1$ étant donné, il n'existe qu'un nombre fini d'entiers m tels que $\varphi(m) = a$ (c'est une conséquence du théorème 1.7). En fait, sans en faire la liste, très peu de résultats ont été démontrés sur cette conjecture.

8. Le théorème d'Euler

Euler a démontré cet énoncé en 1760 :

Théorème 1.8. *Soit n un entier naturel non nul. Pour tout entier a premier avec n, on a*

$$a^{\varphi(n)} \equiv 1 \text{ mod. } n. \tag{19}$$

Pour le vérifier, on peut utiliser directement le théorème 0.3, ou bien le cas particulier « abélien » de ce théorème dont la démonstration se simplifie alors notablement.

Proposition 1.6. *Soit G un groupe abélien fini d'ordre n, d'élément neutre e. Pour tout $x \in G$, on a $x^n = e$.*

Démonstration : Soit x un élément de G. L'application qui à $g \in G$ associe gx est une bijection de G. On en déduit l'égalité

$$\prod_{g \in G} gx = \prod_{g \in G} g.$$

Il convient ici de noter que les produits ne dépendent pas de l'ordre choisi des éléments car G est abélien. On obtient

$$x^n \prod_{g \in G} g = \prod_{g \in G} g,$$

ce qui conduit à l'égalité $x^n = e$.

On obtient alors la congruence (19), en prenant $G = \left(\mathbb{Z}/n\mathbb{Z}\right)^*$, qui est d'ordre $\varphi(n)$.

Corollaire 1.10 (Petit théorème de Fermat). *Soit p un nombre premier. Pour tout entier a non divisible par p, on a*

$$a^{p-1} \equiv 1 \text{ mod. } p.$$

En particulier, pour tout entier a, on a $a^p \equiv a$ mod. p.

Démonstration : Cela résulte de l'égalité $\varphi(p) = p - 1$.

Exemples 1.6.

1) Vérifions que l'écriture décimale de 3^{1000}, qui possède quatre cent soixante dix huit chiffres, se termine par 01. Il s'agit de déterminer l'entier a compris entre 0 et 99 tel que $3^{1000} \equiv a$ mod. 100. On a $\varphi(100) = 40$. D'après le théorème d'Euler, on obtient $3^{40} \equiv 1$ mod. 100. Puisque $1000 = 40 \times 25$, on a donc $3^{1000} \equiv 1$ mod. 100, d'où $a = 1$.

2) Vérifions que l'écriture décimale de 2^{1000}, qui possède trois cent deux chiffres, se termine par 76. Le raisonnement précédent ne s'applique pas directement (car 2 n'est pas premier avec 100). On a $2^{1000} \equiv 0$ mod. 4. L'idée est alors de déterminer la congruence de 2^{1000} modulo 25 et d'utiliser le théorème chinois. On a $2^{20} \equiv 1$ mod. 25 (théorème d'Euler), d'où $2^{1000} \equiv 1$ mod. 25. Il en résulte que $2^{1000} \equiv -24$ mod. 100 (cf. le théorème chinois), d'où l'assertion.

Les applications du théorème d'Euler sont innombrables, on en verra notamment en cryptographie. Donnons ici une illustration de ce théorème, en prouvant un résultat concernant la non primalité des entiers de la forme $2^{2^n} + k$ où k est un entier.

Proposition 1.7 (Schinzel). *Soit k un entier relatif distinct de 1. Il existe une infinité d'entiers n tels que $2^{2^n}+k$ ne soit pas un nombre premier.*

Démonstration : On peut supposer k impair. Soit a un entier naturel. Il suffit de prouver l'existence d'un entier n tel que $2^{2^n}+k$ ne soit pas premier et que $2^{2^n}+k>a$. Puisque k est distinct de 1, il existe $s\in\mathbb{N}$ et un entier impair h tels que

$$k-1=2^s h.$$

Soit t un entier naturel tel que l'on ait

$$p=2^{2^t}+k>a \quad \text{et} \quad t>s.$$

On peut supposer que p est un nombre premier. Il existe un entier impair h_1 tel que

$$p-1=2^s h_1.$$

D'après le théorème d'Euler, on a

$$2^{\varphi(h_1)}\equiv 1 \text{ mod. } h_1,$$

d'où l'on déduit la congruence

$$2^{s+\varphi(h_1)}\equiv 2^s \text{ mod. } p-1.$$

Puisque l'on a $t>s$, on obtient

$$2^{t+\varphi(h_1)}\equiv 2^t \text{ mod. } p-1.$$

L'entier p étant premier impair, on a $2^{p-1}\equiv 1$ mod. p. Il en résulte que

$$2^{2^{t+\varphi(h_1)}}+k\equiv 0 \text{ mod. } p.$$

L'entier $2^{2^{t+\varphi(h_1)}}+k$, qui est strictement plus grand que p, n'est donc pas premier. Il est plus grand que a, d'où le résultat.

On conjecture que cet énoncé est aussi vrai si $k=1$, mais on ne sait pas le démontrer. Pour autant, les seuls entiers n connus tels que F_n soit premier sont ceux inférieurs ou égaux à 4, et on pense qu'il n'y a qu'un nombre fini d'entiers F_n premiers. Par exemple, F_5 est divisible par 641. On le constate en écrivant que l'on a

$$641=5^4+2^4=5.2^7+1,$$

d'où $5.2^7\equiv -1$ mod. 641, puis $5^4.2^{28}\equiv 1$ mod. 641 et $2^{32}+1\equiv 0$ mod. 641.

9. Groupes cycliques

Les groupes cycliques sont utilisés en cryptographie notamment en ce qui concerne le problème du logarithme discret. Rappelons leurs principales propriétés.

Soit G un groupe fini d'ordre n, d'élément neutre e. Il est dit cyclique s'il possède un élément d'ordre n. Dans ce cas, un tel élément s'appelle un générateur de G. Un groupe cyclique est en particulier abélien. Si x est un générateur de G, on a

$$G = \left\{e, x, \cdots, x^{n-1}\right\}.$$

Par exemple, pour tout $n \geq 1$, le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n. La classe de 1 en est un générateur. À isomorphisme près, c'est le seul groupe cyclique d'ordre n.
On utilisera le fait que pour tout entier k, et tout élément y de G (cyclique ou non) d'ordre m, l'ordre de y^k est

$$\frac{m}{\mathrm{pgcd}(m,k)}.$$

En effet, si $d = \mathrm{pgcd}(m,k)$, on a $(y^k)^{\frac{m}{d}} = (y^m)^{\frac{k}{d}} = e$. Par ailleurs, si u est un entier tel que $(y^k)^u = e$, alors m divise uk, donc $\frac{m}{d}$ divise $\frac{uk}{d}$. Les entiers $\frac{m}{d}$ et $\frac{k}{d}$ étant premiers entre eux, $\frac{m}{d}$ divise u, d'où l'assertion.

Théorème 1.9. *Soit G un groupe cyclique d'ordre n.*

1) Tout sous-groupe de G est cyclique.

2) Pour tout diviseur $d \geq 1$ de n, l'ensemble

$$H_d = \left\{a \in G \mid a^d = e\right\}$$

est un sous-groupe de G d'ordre d.

3) L'application qui à d associe H_d est une bijection entre l'ensemble des diviseurs de n et l'ensemble des sous-groupes de G. En particulier, pour tout diviseur d de n, H_d est l'unique sous-groupe d'ordre d de G.

Démonstration : Soit x un générateur de G.

1) Soit H un sous-groupe de G. Considérons le plus petit entier $\delta \geq 1$ tel que x^δ appartienne à H. Le sous-groupe de G engendré par x^δ est contenu dans H. Montrons qu'il est égal à H. Soit y un élément de H. Il existe un entier m tel que l'on ait $y = x^m$. Par ailleurs, il existe des entiers q et r tels que l'on ait $m = \delta q + r$, avec $0 \leq r < \delta$. On en déduit que x^r est dans H, et donc que r est nul. D'où $m = \delta q$, et $y = (x^\delta)^q$ appartient au sous-groupe de G engendré par x^δ, d'où l'assertion.

2) Soit d un diviseur ≥ 1 de n. L'ensemble H_d est un sous-groupe de G. En effet, e appartient à H_d, et pour tous $a, b \in H_d$, on a

$$(ab)^d = a^d b^d = e \quad \text{et} \quad (a^{-1})^d = (a^d)^{-1} = e,$$

de sorte que ab et a^{-1} sont dans H_d. On a

$$\left(x^{\frac{n}{d}}\right)^d = x^n = e,$$

donc $x^{\frac{n}{d}}$ appartient à H_d. L'élément $x^{\frac{n}{d}}$ étant d'ordre d, l'ordre de H_d est divisible par d. Par ailleurs, H_d est cyclique (assertion 1). Si y est un générateur de H_d, on a $y^d = e$, donc l'ordre de H_d, qui est celui de y, divise d. Ainsi, H_d est d'ordre d.

3) Soit H un sous-groupe de G. Vérifions que l'on a $H = H_d$ où d est l'ordre de H, ce qui prouvera que l'application considérée est une surjection. Pour tout $z \in H$ on a $z^d = e$, donc H est contenu dans H_d. Puisque H_d est d'ordre d, on a donc $H = H_d$. Il reste à montrer que cette application est une injection : si d et d' sont deux diviseurs de n tels que $H_d = H_{d'}$, vu que H_d et $H_{d'}$ ont le même ordre, on a $d = d'$.

Corollaire 1.11. *Soit G un groupe cyclique d'ordre n. Pour tout entier $k \geq 1$, l'ensemble*

$$\left\{a \in G \mid a^k = e\right\}$$

est un sous-groupe de G d'ordre $\mathrm{pgcd}(k, n)$.

Démonstration : Soit k un entier naturel non nul. Posons $H = \left\{a \in G \mid a^k = e\right\}$ et $d = \mathrm{pgcd}(k, n)$. Le fait que H soit un sous-groupe de G se vérifie comme ci-dessus. Par ailleurs, en utilisant le propriété de Bézout, on constate directement que $H = H_d$, d'où le résultat (th. 1.9).

Exemple 1.7. Tout groupe fini d'ordre un nombre premier est cyclique. Ses éléments autres que l'élément neutre en sont des générateurs.

Une question importante concerne la description des générateurs d'un groupe cyclique. En particulier, combien y a-t-il de générateurs dans un groupe cyclique d'ordre n ?

Théorème 1.10. *Soient G un groupe cyclique d'ordre n et x un générateur de G.*
1) L'ensemble des générateurs de G est

$$\left\{x^k \mid 1 \leq k \leq n \text{ et } \mathrm{pgcd}(k, n) = 1\right\}.$$

En particulier, G possède exactement $\varphi(n)$ générateurs.
2) Pour tout diviseur d de n, il y a exactement $\varphi(d)$ éléments d'ordre d dans G.

Démonstration : 1) On a $G = \left\{x, \cdots, x^{n-1}, x^n\right\}$. Pour tout k compris entre 1 et n, l'ordre de x^k est $\frac{n}{\mathrm{pgcd}(n,k)}$. Par suite, x^k est d'ordre n si et seulement si on a $\mathrm{pgcd}(n, k) = 1$.

2) Il existe un unique sous-groupe H_d d'ordre d de G, à savoir l'ensemble des $a \in G$ tels que $a^d = e$ (th. 1.9). L'ensemble des éléments d'ordre d de G est donc contenu dans

H_d, et cet ensemble est formé des générateurs de H_d. Puisque H_d est cyclique (*loc. cit.*), il a exactement $\varphi(d)$ générateurs.

Exemple 1.8. Pour tout $n \geq 1$, l'ensemble des générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$ est formé des classes d'entiers premiers avec n.

Vérifions le lemme suivant que l'on utilisera plus loin.

Lemme 1.11. *Soient H et K des groupes cycliques. Le groupe produit $H \times K$ est cyclique si et seulement si les ordres de H et K sont premiers entre eux.*

Démonstration : Notons m et n les ordres de H et K respectivement. Pour tout $(a, b) \in H \times K$, l'ordre de (a, b) est le plus petit commun multiple des ordres de a et b. Supposons m et n premiers entre eux. Si x est un générateur de H et y un générateur de K, l'ordre de (x, y) est donc mn et $H \times K$ est cyclique. Inversement, supposons $H \times K$ cyclique. Soit (a, b) un de ses générateurs. Les éléments a et b sont alors respectivement des générateurs de H et K. Par suite, a est d'ordre m et b est d'ordre n. Il en résulte que mn est le plus petit commun multiple de m et n, d'où $\text{pgcd}(m, n) = 1$.

10. Le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ où p est premier impair

On va démontrer qu'il est cyclique pour tout $n \geq 1$. Commençons par traiter le cas où $n = 1$, autrement dit, par établir que $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ est un groupe cyclique.

Lemme 1.12. *Soit G un groupe fini d'ordre m, d'élément neutre e. Supposons que pour tout diviseur d de m, l'ensemble des éléments $x \in G$ tels que $x^d = e$ soit de cardinal au plus d. Alors G est cyclique.*

Démonstration : Soient d un diviseur de m et A_d l'ensemble des éléments de G d'ordre d. Vérifions que le cardinal de A_d est 0 ou $\varphi(d)$. Supposons pour cela qu'il existe un élément $x \in G$ d'ordre d. Soit H le sous-groupe de G engendré par x. Il est d'ordre d. D'après l'hypothèse faite, tout élément $y \in G$ tel que $y^d = e$ appartient donc à H. En particulier, les éléments d'ordre d de G sont ceux de H. Puisque H est cyclique d'ordre d, il y en a $\varphi(d)$ (th. 1.10), d'où l'assertion. Par ailleurs, G est la réunion disjointe des A_d où d parcourt l'ensemble des diviseurs de m. S'il existait un diviseur d de m tel que A_d soit vide, on aurait ainsi (lemme 1.10)

$$|G| < \sum_{d|m} \varphi(d) = m,$$

d'où une contradiction. En particulier, G a un élément d'ordre m i.e. G est cyclique.

Proposition 1.8. *Pour tout nombre premier p, le groupe $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$ est cyclique.*

Démonstration : Si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif. Pour tout entier $d \geq 1$, le polynôme $X^d - 1 \in \big(\mathbb{Z}/p\mathbb{Z}\big)[X]$ a donc au plus d racines dans $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$. Le lemme précédent entraîne alors le résultat.

On ne connaît pas de procédé, autre que la recherche exhaustive, permettant de déterminer un générateur de $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$. Citons à ce propos la conjecture d'Artin :

Conjecture. *Soit a un entier relatif distinct de -1 qui n'est pas un carré. Il existe une infinité de nombres premiers p tels que la classe de a soit un générateur de $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$.*

Signalons que conjecturalement, pour tout nombre premier $p \geq 3$ il existe un entier naturel $a < 2(\log p)^2$ tel que $a + p\mathbb{Z}$ soit un générateur de $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$.

Avant de démontrer le résultat annoncé établissons le lemme suivant.

Lemme 1.13. *Soient p un nombre premier impair et a un entier. Pour tout $n \in \mathbb{N}$, on a*

$$(1 + pa)^{p^n} \equiv 1 + p^{n+1}a \text{ mod. } p^{n+2}.$$

Démonstration : On procède par récurrence sur n. Cette congruence est vraie si $n = 0$. Supposons qu'elle le soit pour un entier $n \in \mathbb{N}$. Puisque p divise C_p^j pour $j = 1, \cdots, p-1$, on obtient

$$(1 + pa)^{p^{n+1}} \equiv \big(1 + p^{n+1}a\big)^p \text{ mod. } p^{n+3}.$$

Par ailleurs, on a

$$\big(1 + p^{n+1}a\big)^p \equiv 1 + p^{n+2}a + C_p^2 p^{2n+2}a^2 \text{ mod. } p^{n+3}.$$

On a $p \neq 2$, donc p divise C_p^2 et $C_p^2 p^{2n+2}a^2$ est divisible par p^{n+3} (y compris si $n = 0$). Cela entraîne le résultat.

Théorème 1.11. *Soient p un nombre premier impair et n un entier ≥ 1. Le groupe $\big(\mathbb{Z}/p^n\mathbb{Z}\big)^*$ est cyclique d'ordre $p^{n-1}(p-1)$. Plus précisément, soit a un entier naturel tel que $a + p\mathbb{Z}$ soit un générateur de $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$.*

1) Si $a^{p-1} \not\equiv 1$ mod. p^2, alors $a + p^n\mathbb{Z}$ est un générateur de $\big(\mathbb{Z}/p^n\mathbb{Z}\big)^*$.

2) Si $a^{p-1} \equiv 1$ mod. p^2, alors $(a + p) + p^n\mathbb{Z}$ est un générateur de $\big(\mathbb{Z}/p^n\mathbb{Z}\big)^*$.

Démonstration : Vérifions d'abord que l'on a

$$a^{p-1} \not\equiv 1 \text{ mod. } p^2 \quad \text{ou bien} \quad (a+p)^{p-1} \not\equiv 1 \text{ mod. } p^2. \tag{20}$$

Supposons pour cela $a^{p-1} \equiv 1 \text{ mod. } p^2$. On a

$$(a+p)^{p-1} \equiv a^{p-1} + p(p-1)a^{p-2} \text{ mod. } p^2,$$

d'où la congruence

$$(a+p)^{p-1} \equiv 1 + p(p-1)a^{p-2} \text{ mod. } p^2.$$

Puisque p ne divise pas a, on en déduit que $(a+p)^{p-1} - 1$ n'est pas divisible par p^2, d'où la condition (20). Soit alors x l'un des entiers a et $a+p$ pour lequel on a

$$x^{p-1} \not\equiv 1 \text{ mod. } p^2. \tag{21}$$

Tout revient à démontrer que $x + p^n\mathbb{Z}$ est un générateur de $\big(\mathbb{Z}/p^n\mathbb{Z}\big)^*$. Soit r l'ordre de $x + p^n\mathbb{Z}$. D'après l'hypothèse faite sur a, l'ordre de x modulo p est $p-1$. La congruence

$$x^r \equiv 1 \text{ mod. } p$$

entraîne que $p-1$ divise r. Par ailleurs, r divise $\varphi(p^n) = p^{n-1}(p-1)$. Il existe donc un entier s tel que

$$r = p^s(p-1) \quad \text{avec} \quad 0 \leq s \leq n-1. \tag{22}$$

D'après la condition (21), il existe un entier k tel que

$$x^{p-1} = 1 + kp \quad \text{avec} \quad k \not\equiv 0 \text{ mod. } p.$$

Puisque p est impair, on déduit alors du lemme 1.13 que l'on a

$$x^r \equiv 1 + p^{s+1}k \text{ mod. } p^{s+2}.$$

Parce que p^n divise $x^r - 1$, et que p ne divise pas k, on a donc $n \leq s+1$. Compte tenu de (22), on obtient $s = n-1$, d'où $r = \varphi(p^n)$ et le résultat.

Exemple 1.9. Pour tout $n \geq 1$, la classe de 2 est un générateur du groupe $\big(\mathbb{Z}/3^n\mathbb{Z}\big)^*$. En effet, $2 + 3\mathbb{Z}$ est un générateur de $\big(\mathbb{Z}/3\mathbb{Z}\big)^*$ et l'on a $2^2 \not\equiv 1 \text{ mod. } 9$.

11. Le groupe $\big(\mathbb{Z}/2^n\mathbb{Z}\big)^*$

Le groupe $\big(\mathbb{Z}/2\mathbb{Z}\big)^*$ est trivial et $\big(\mathbb{Z}/4\mathbb{Z}\big)^*$ est cyclique d'ordre 2.

Considérons un entier $n \geq 3$. On va établir que $\big(\mathbb{Z}/2^n\mathbb{Z}\big)^*$ est isomorphe au groupe $\big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}, +\big)$. Posons

$$U(n) = \Big\{ a + 2^n\mathbb{Z} \;\Big|\; a \equiv 1 \text{ mod. } 4 \Big\}.$$

C'est un sous-groupe de $\big(\mathbb{Z}/2^n\mathbb{Z}\big)^*$. On a $\big(\mathbb{Z}/2^n\mathbb{Z}\big)^* = \big\{\pm 1\big\}U(n)$ et l'application

$$f : \big\{\pm 1\big\} \times U(n) \to \big(\mathbb{Z}/2^n\mathbb{Z}\big)^*$$

définie par

$$f\big((\varepsilon, a + 2^n\mathbb{Z})\big) = \varepsilon a + 2^n\mathbb{Z} \quad \text{avec} \quad \varepsilon = \pm 1,$$

est un isomorphisme de groupes.

Proposition 1.9. *Le groupe $U(n)$ est cyclique, d'ordre 2^{n-2}, et il est engendré par la classe de 5.*

Démonstration : Vu ce qui précède, l'ordre de $U(n)$ est $\frac{\varphi(2^n)}{2} = 2^{n-2}$. Par ailleurs, la classe de 5 est dans $U(n)$. Tout revient à prouver que l'ordre de $5 + 2^n\mathbb{Z}$ dans $\big(\mathbb{Z}/2^n\mathbb{Z}\big)^*$ est 2^{n-2}. Pour cela, on vérifie par récurrence sur n que l'on a

$$5^{2^{n-3}} \equiv 1 + 2^{n-1} \text{ mod. } 2^n.$$

Par suite, l'ordre de $5 + 2^n\mathbb{Z}$ ne divise pas 2^{n-3}. Vu que l'on a (prop. 1.6)

$$5^{2^{n-2}} \equiv 1 \text{ mod. } 2^n,$$

l'ordre de la classe de 5 est donc 2^{n-2}.

On en déduit le résultat annoncé :

Théorème 1.12. *Pour tout $n \geq 3$, le groupe $\big(\mathbb{Z}/2^n\mathbb{Z}\big)^*$ est isomorphe au groupe produit $\big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}, +\big)$.*

Pour tout $n \geq 3$, les éléments de $\big(\mathbb{Z}/2^n\mathbb{Z}\big)^*$ sont d'ordre divisant 2^{n-2}, en particulier il n'est pas cyclique.

Comme conséquence des théorèmes 1.11 et 1.12, et du théorème chinois, on obtient la liste, établie par Gauss, des entiers $m \geq 1$ tels que le groupe $\big(\mathbb{Z}/m\mathbb{Z}\big)^*$ soit cyclique.

Théorème 1.13 (Gauss, 1801). *Les entiers $m \geq 1$ tels que $\big(\mathbb{Z}/m\mathbb{Z}\big)^*$ soit un groupe cyclique sont $1, 2, 4$, et ceux de la forme p^r et $2p^r$ où p est un nombre premier impair.*

Démonstration : Si p est premier impair, les groupes $\big(\mathbb{Z}/p^r\mathbb{Z}\big)^*$ et $\big(\mathbb{Z}/2p^r\mathbb{Z}\big)^*$ sont isomorphes. Pour tout entier m intervenant dans l'énoncé, $\big(\mathbb{Z}/m\mathbb{Z}\big)^*$ est donc un groupe cyclique (th. 1.11).
Inversement, soit m un entier ≥ 3 tel que $\big(\mathbb{Z}/m\mathbb{Z}\big)^*$ soit cyclique. Soit

$$m = \prod_{i=1}^{t} p_i^{n_i},$$

la décomposition de m en produit de nombres premiers p_i, avec $p_i \neq p_j$ si $i \neq j$ et $n_i \geq 1$. Les groupes

$$\left(\mathbb{Z}/m\mathbb{Z}\right)^* \quad \text{et} \quad \prod_{i=1}^{t} \left(\mathbb{Z}/p_i^{n_i}\mathbb{Z}\right)^*$$

sont isomorphes (cf. le théorème chinois). Compte tenu du lemme 1.11, il en résulte que m est de la forme $2^s p^r$ où p est un nombre premier impair. Si $r = 0$, le théorème 1.12 implique $s = 2$ (car $m \geq 3$). Si $r \geq 1$, on obtient $s = 0$ ou $s = 1$, d'où le résultat.

Exemple 1.10. Vérifions que $\left(\mathbb{Z}/4418\mathbb{Z}\right)^*$ est cyclique engendré par la classe de 5. Ce groupe est cyclique, d'ordre 2162, car $4418 = 2 \times 47^2$. Il suffit d'établir que $5 + 47^2\mathbb{Z}$ est un générateur de $\left(\mathbb{Z}/47^2\mathbb{Z}\right)^*$. Démontrons pour cela que la classe de 5 est un générateur de $\left(\mathbb{Z}/47\mathbb{Z}\right)^*$. Déterminons l'ordre multiplicatif de 2 modulo 47. On a

$$2^{16} = (2^8)^2 \equiv 21^2 \equiv 18 \text{ mod. } 47,$$

d'où l'on déduit que $2^{23} \equiv 1$ mod. 47, puis que 23 est l'ordre cherché. Par ailleurs, -1 est d'ordre 2 modulo 47. Il en résulte que la classe de -2 est un générateur de $\left(\mathbb{Z}/47\mathbb{Z}\right)^*$. Les générateurs de $\left(\mathbb{Z}/47\mathbb{Z}\right)^*$ sont donc les éléments $(-2)^k + 47\mathbb{Z}$ avec $\text{pgcd}(k, 46) = 1$ (il y en a vingt-deux). On a $2^8 \equiv 21$ mod. 47 puis

$$-2^9 \equiv 5 \text{ mod. } 47,$$

d'où l'assertion. On vérifie ensuite à l'aide d'une calculatrice que l'on a $5^{46} \not\equiv 1$ mod. 47^2. Le théorème 1.11 entraîne alors le résultat.