ALGÈBRE ET ARITHMÉTIQUE
UNIVERSITÉ DE ROUEN
2021–2022

PAUL LESCOT
PAUL.LESCOT@UNIV-ROUEN.FR

Sommaire

Date: 30 Novembre 2021.

NB : sauf précision contraire, "entier" signifiera entier relatif, *i.e.* élément de $\mathbf{Z}$.

Pour p premier et $n \geq 1$, $v_p(n)$ désignera la **valuation p–adique** de n, c'est–à–dire le plus grand entier k tel que p^k divise n.

L'ordre de l'élément x d'un groupe G sera noté $\omega(x)$.

Conformément aux conventions du programme, "corps" signifiera "corps commutatif"; une structure algébrique satisfaisant à tous les axiomes des corps autres que la commutativité de la multiplication sera dite "anneau à division".

Ce texte reprend une partie du contenu d'un cours fait à l'ISMANS en 2007-2008. Une première version en avait été rédigée en 2009 avec la collaboration d'Aziz El Kaabouchi.

1. Pgcd, Théorème de Bachet–Bezout, ppcm. Théorème de Sylvester.

Théorème 1.1. ***(Algorithme d'Euclide)***
Soient a et b deux entiers ≥ 1, avec $a \geq b$. Posons $a_0 = a$, $a_1 = b$, et, pour $n \geq 0$ tel que $a_{n+1} \geq 1$, a_{n+2}:= le reste de la division de a_n par a_{n+1}, c'est–à–dire

$$\begin{aligned} a_n &= q_{n+1}a_{n+1} + a_{n+2} \\ &0 \leq a_{n+2} < a_{n+1} \ , \end{aligned}$$

avec $q_{n+1} \in \mathbf{Z}$.
Alors il existe un plus petit entier $m \geq 2$ tel que $a_m = 0$, le plus grand commun diviseur de a et b ($\mathrm{pgcd(a, b)}$*) vaut a_{m-1}, et il est divisible par tout diviseur commun de a et b.*

Démonstration. Par définition de la division euclidienne, on a $0 \leq a_{n+2} < a_{n+1}$, donc la suite des a_n ($n \geq 1$) est une suite strictement décroissante d'entiers ≥ 0 ; elle est donc de longueur finie, c'est–à–dire qu'il existe $m \geq 2$ tel que $a_m = 0$. Alors un entier k divise a et b si et seulement s'il divise a_0 et a_1, c'est–à–dire si et seulement s'il divise a_1 et $q_1a_1 + a_2$, c'est–à–dire si et seulement s'il divise a_1 et a_2 (car $k|a_1$ entraîne $k|q_1a_1$). En itérant ce raisonnement, on voit que k divise a et b si et seulement s'il divise à la fois a_{m-1} et $a_m = 0$, c'est–à–dire si et seulement s'il divise a_{m-1}. Donc le plus grand commun diviseur de a et b vaut a_{m-1}, et il possède la propriété requise. □

Corollaire 1.2. ***(Théorème de Bachet–Bezout)*** *Pour tout $(a, b) \in \mathbf{Z}^2 \backslash \{(0, 0)\}$,* $\mathrm{pgcd(a, b)}$ *est bien défini, et il existe $(x, y) \in \mathbf{Z}^2$ tel que* $\mathrm{pgcd(a, b)} = \mathrm{ax + by}$.

Remarque 1.3. Ce Théorème est dû à Bachet de Méziriac (1581–1638) : cf. [2], Note II, p. 227. Bezout (1730–1783) en démontra l'analogue pour les polynômes à coefficients dans un corps.

Démonstration. Il est facile de se ramener au cas où $a \geq b \geq 1$; on a alors

$$a_2 = a_0 - q_1a_1 = a - q_1b = 1 \cdot a + (-q_1) \cdot b \ ,$$

$$a_3 = a_1 - q_2a_2 = b - q_2(a - bq_1) = (-q_2)a + (1 + q_1q_2)b \ ,$$

et ainsi de suite : on voit que chaque a_k, et en particulier $a_{m-1} = \mathrm{pgcd(a, b)}$, est de la forme $ax + by$ ($(x, y) \in \mathbf{Z}^2$). □

L'algorithme d'Euclide est constructif, et d'ailleurs programmable. Par exemple, soient $a = 1729$ et $b = 923$; on a

$$\begin{aligned} 1729 &= 1 \cdot 923 + 806 \\ 923 &= 1 \cdot 806 + 117 \\ 806 &= 6 \cdot 117 + 104 \\ 117 &= 1 \cdot 104 + 13 \\ 104 &= 8 \cdot 13 + 0, \end{aligned}$$

d'où $\mathrm{pgcd}(1729, 923) = 13$.

Le calcul permet en outre de déterminer des entiers x et y satisfaisant à la conclusion du Théorème de Bachet–Bezout :

$$\begin{aligned} 13 &= 117 + (-1)\cdot 104 = 117 + (-1)\cdot(806 - 6\cdot 117) \\ &= 7\cdot 117 + (-1)\cdot 806 = 7(923 + (-1)\cdot 806) + (-1)\cdot 806 \\ &= 7\cdot 923 + (-8)\cdot 806 = 7\cdot 923 + (-8)\cdot(1729 + (-1)\cdot 923) \\ &= 15\cdot 923 + (-8)\cdot 1729 \end{aligned}$$

soit

$$13 = \mathrm{pgcd}(1729, 923) = 15\cdot 923 + (-8)\cdot 1729.$$

On déduit du Corollaire 1.2 le

Lemme 1.4. ***(Lemme de Gauss)*** *Si a et b sont premiers entre eux et a divise bc, alors a divise c.*

Démonstration. Par hypothèse, on peut écrire $bc = ad$ pour un certain entier d.

D'après le Théorème de Bachet–Bezout, il existe $(x, y) \in \mathbf{Z}^2$ tel que $ax + by = 1$. Mais alors

$$\begin{aligned} c &= 1\cdot c \\ &= (ax + by)\cdot c \\ &= axc + byc \\ &= a(xc) + (bc)y \\ &= a(xc) + (ad)y \\ &= a(xc + dy)\ , \end{aligned}$$

donc a divise c. □

Corollaire 1.5. *Si p est premier et p divise bc, alors p divise b ou p divise c.*

Démonstration. Supposons que p ne divise pas b, et soit $d = \mathrm{pgcd(p, b)}$; alors d divise p et $d \neq p$, donc $d = 1$, c'est–à–dire que p et b sont premiers entre eux. Mais alors le Lemme de Gauss entraîne que p divise c. □

De ce corollaire, on va déduire l'unicité de la décomposition d'un nombre entier en facteurs premiers :

Théorème 1.6. *Pour tout entier $n \geq 2$, il existe une et une seule décomposition (à permutation près des p_j):*

$$n = p_1^{a_1} \dots p_m^{a_m}$$

où $m \geq 1$, les p_j sont des nombres premiers deux à deux distincts et les $a_i \geq 1$.

Démonstration. L'existence est facile à établir par récurrence sur n : supposons le résultat exact pour tous les entiers $< n$, et soit p le plus petit diviseur > 1 de n. Alors p est premier et $\dfrac{n}{p} < n$. Si $\dfrac{n}{p} = 1$, alors $n = p$ et $m = 1$, $p_1 = 1$ et $a_1 = 1$ conviennent. Dans le cas contraire, $\dfrac{n}{p} \geq 2$; en vertu de l'hypothèse de récurrence, $\dfrac{n}{p}$ est alors un produit de facteurs premiers, donc $n = p.\dfrac{n}{p}$ l'est aussi.

Afin d'établir l'unicité, raisonnons par l'absurde, et soit n le plus petit nombre entier ≥ 2 possédant deux décompositions essentiellement distinctes. Ecrivons

$$n = p_1^{a_1} \dots p_m^{a_m} = q_1^{b_1} \dots q_{m'}^{b_{m'}} .$$

On a nécessairement $m \geq 1$; vu que p_1 divise $q_1^{b_1} ... q_{m'}^{b_{m'}} = n$, par une application immédiate du Corollaire 2.5, il apparaît que p_1 divise l'un des q_i, par exemple q_1. Mais alors $p_1 = q_1$, donc

$$\frac{n}{p_1} = p_1^{a_1 - 1} ... p_m^{a_m} = q_1^{b_1 - 1} ... q_{m'}^{b_{m'}}$$

possède deux décompositions essentiellement distinctes, et $\dfrac{n}{p_1} < n$, ce qui est absurde. □

Exemple : $1729 = 13 \cdot 133 = 7 \cdot 13 \cdot 19$.

Les considérations précédentes mènent naturellement à une démonstration constructive de l'existence du plus petit commun multiple (ppcm) de deux entiers.

Conservons les notations ci–dessus (avec $a \geq 1$, $b \geq 1$ et $(a, b) \neq (0, 0)$) ;

$d = \text{pgcd(a, b)}$ divise a et b, donc on peut écrire $a = da'$ et $b = db'$; vu que $ax + by = d$, on a $d = (da')x + (db')y = d(a'x + b'y)$, d'où $a'x + b'y = 1$.

Un diviseur commun > 0 de a' et b' doit donc diviser 1, donc être égal à 1, c'est–à–dire que a' et b' sont premiers entre eux.

Posons $m = da'b' = ab' = a'db' = a'b$; alors m est à la fois multiple de $a = da'$ et de $b = db'$. Soit maintenant n un multiple commun de a et b. On peut écrire $n = an'$; mais alors $db' = b$ divise $da'n' = an' = n$, i.e. b' divise $a'n'$. Vu que a' et b' sont premiers entre eux, le Lemme de Gauss entraîne que b' divise n' : $n' = b'u$, d'où

$$n = an' = ab'u = da'b'u = mu,$$

donc m divise n. On a bien établi l'existence de $\text{ppcm(a, b)} = \text{m}$. De plus, on obtient que

$$dm = dda'b' = (da')(db') = ab,$$

d'où le

Théorème 1.7. *Pour tout $(a, b) \in \mathbf{N}^2 \setminus \{(0, 0)\}$ on a*

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

Dans l'exemple ci–dessus ($a = 1729$ et $b = 923$), on a vu que $d = 13$, d'où $a' = 133$ et $b' = 71$; il s'ensuit que $m = da'b' = 13 \cdot 133 \cdot 71 = 122759$, et que

$$\text{ppcm}(1729, 923) = 122759 .$$

Théorème 1.8. ***(Théorème de Sylvester)*** *Soient a et b deux entiers ≥ 1 premiers entre eux. Alors le plus grand entier $N(a, b)$ ne pouvant pas être représenté sous la forme $ax + by$ avec $(x, y) \in \mathbf{N}^2$ est*

$$N(a, b) = ab - a - b .$$

Démonstration. Tout d'abord, $ab - a - b$ n'est pas représentable de cette façon. Supposons en effet que $ab - a - b = xa + yb$ avec $x \geq 0$ et $y \geq 0$. Alors

$$(y + 1)b = yb + b = a(b - 1 - x),$$

d'où $a \mid (y+1)b$; en vertu du Lemme de Gauss, $a|(y+1)$, soit $y+1 = \lambda a$; vu que $y+1 \geq 1 > 0$, on a $\lambda > 0$ d'où $\lambda \geq 1$. Symétriquement $x+1 = \mu b$ avec $\mu \geq 1$; mais alors

$$ab - a - b = xa + yb = (\mu b - 1)a + (\lambda a - 1)b = (\mu + \lambda)ab - a - b$$

et $1 = \mu + \lambda \geq 1 + 1 = 2$, une contradiction.

Soit maintenant M un entier au moins égal à $ab - a - b + 1$, et posons

$$x_0 = M - (ab - a - b) \geq 1 \ .$$

D'après le Théorème de Bachet–Bezout, il existe $(u, v) \in \mathbf{Z}^2$ tel que $au + bv = 1$. Soit alors r l'unique entier relatif tel que $rb < ux_0 \leq (r+1)b$; posons

$$x := ux_0 - 1 - rb \geq 0$$

et

$$y := vx_0 - 1 + (1 + r)a.$$

Alors, vu que $ux_0 \leq (r+1)b$, il suit

$$\begin{aligned} by &= bvx_0 - b + ba + rba \\ &= (1 - au)x_0 - b + ba + rba \\ &= x_0 - aux_0 - b + ba + rba \\ &\geq x_0 - a(r+1)b - b + ba + rba \\ &= x_0 - b \\ &> -b, \end{aligned}$$

d'où $b(y+1) = by + b > 0$, $y + 1 > 0$, $y + 1 \geq 1$ et $y \geq 0$. Il s'avère maintenant que

$$\begin{aligned} ax + by &= a(ux_0 - 1 - rb) + b(vx_0 - 1 + a(r+1)) \\ &= (au + bv)x_0 - a - arb - b + bar + ba \\ &= x_0 + ab - a - b \\ &= M \ . \end{aligned}$$

On a donc $N(a, b) = ab - a - b$. □

Exemple : au moyen de pièces de 2 euros et de billets de 5 euros, il est possible de régler toute somme entière supérieure ou égale à 4 euros, mais pas une somme de 3 euros ($a = 2$, $b = 5$ et $ab - a - b = 3$).

2. Congruences ; $\frac{\mathbf{Z}}{n\mathbf{Z}}$.

Soient $n \geq 1$ un entier, et a et b deux entiers relatifs. On dira que a **est congru à** b modulo n, et on notera $a \equiv b[n]$, si n divise $a - b$. Il s'agit (exercice!) d'une relation d'équivalence sur $\mathbf{Z}$.

On notera $\bar{a}$ la classe de l'élément a de $\mathbf{Z}$ pour cette relation, et $\frac{\mathbf{Z}}{n\mathbf{Z}}$ l'ensemble de ces classes d'équivalence.

En termes plus algébriques, il s'agit de l'ensemble quotient de $\mathbf{Z}$ par la relation de congruence modulo n. Cet ensemble est naturellement muni d'opérations dérivées de celles de $\mathbf{Z}$:

$$\bar{a} + \bar{b} = \overline{a+b}$$

et

$$\bar{a}\bar{b} = \overline{ab} \ .$$

Ces opérations font de $\frac{\mathbf{Z}}{n\mathbf{Z}}$ un **anneau commutatif unitaire**, de zéro $\bar{0}$ et d'unité $\bar{1}$; en termes simplifiés, on peut dire que l'on calcule sur les classes de congruence modulo n comme sur les entiers usuels, en assimilant les multiples de n à 0. On notera

$$\begin{aligned} \pi_n : \quad \mathbf{Z} &\to \frac{\mathbf{Z}}{n\mathbf{Z}} \\ a &\mapsto \bar{a} \end{aligned}$$

la **projection canonique** .

Soit $a \in \mathbf{Z}$; en effectuant la division euclidienne de a par n, on obtient une expression de la forme

$$a = nq + r$$

avec $0 \leq r \leq n-1$; en particulier, n divise $a - r = nq$, d'où $\bar{a} = \bar{r}$.

Par ailleurs, lorsque $0 \leq i < j \leq n-1$, on a $0 < j - i < n$, donc n ne divise pas $j - i$ et $\bar{i} \neq \bar{j}$. Il apparaît que

$$\frac{\mathbf{Z}}{n\mathbf{Z}} = \{\bar{0}, ..., \overline{n-1}\} ;$$

en particulier, $\frac{\mathbf{Z}}{n\mathbf{Z}}$ a pour cardinal n.

Vu que $\bar{0} = \bar{n}$, on a aussi

$$\frac{\mathbf{Z}}{n\mathbf{Z}} = \{\bar{1}, ..., \bar{n}\}.$$

Remarquons qu'un élément $\bar{a}$ de $\frac{\mathbf{Z}}{n\mathbf{Z}}$ est inversible si et seulement s'il existe $\bar{x} \in \frac{\mathbf{Z}}{n\mathbf{Z}}$ tel que $\bar{a}\bar{x} = \bar{1}$. Mais cette égalité équivaut à :

$$\overline{ax} = \bar{1},$$

soit :

$$ax \equiv 1[n] \ ,$$

c'est–à–dire qu'il existe $y \in \mathbf{Z}$ tel que $1 - ax = ny$, soit

$$\exists (x,y) \in \mathbf{Z}^2 \ \ ax + ny = 1 \ .$$

Pour cela, il est nécessaire que pgcd(a, n) = 1 ; la condition est suffisante en vertu du Théorème de Bachet–Bezout. Donc, pour chaque $a \in \mathbf{Z}$, $\bar{a}$ est inversible dans $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ si et seulement si a est premier avec n.

En particulier, on a la

Proposition 2.1. *Lorsque p est premier, $\dfrac{\mathbf{Z}}{p\mathbf{Z}}$ est un corps.*

Démonstration. Soit $\bar{a}$ un élément $\neq 0$ de $\dfrac{\mathbf{Z}}{p\mathbf{Z}}$. Alors $p \nmid a$, donc pgcd(p, a) $\neq$ p ; mais p est premier et pgcd(p, a)|p, donc pgcd(p, a) = 1 et a et p sont premiers entre eux. Par suite $\bar{a}$ est inversible dans $\dfrac{\mathbf{Z}}{p\mathbf{Z}}$. □

On notera dorénavant ce corps $\mathbf{F}_p = \dfrac{\mathbf{Z}}{p\mathbf{Z}}$.

La Proposition 2.1 admet une réciproque.

Théorème 2.2. *Pour n un entier ≥ 1, les propositions suivantes sont équivalentes*

1) *n est premier*
2) $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ *est un corps*
3) $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ *est intègre.*

Remarque 2.3. L'équivalence entre 2) et 3) est un cas particulier d'un résultat plus général: tout anneau intègre fini est un corps.

Démonstration. 1) ⇒ 2) vient d'être vu.

2) ⇒ 3) est évident.

3) ⇒ 1)

Supposons $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ intègre ; alors $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ a au moins deux éléments, donc $n \geq 2$. Si n pouvait s'écrire comme un produit $n = ab$ avec $1 < a < n$ et $1 < b < n$, on aurait, dans $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$:

$$\bar{a} \neq \bar{0} \ , \ \bar{b} \neq \bar{0}, \text{et } \bar{a}\bar{b} = \bar{a}\bar{b} = \bar{n} = \bar{0} \ ,$$

contredisant l'intégrité de $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$. □

Théorème 2.4. ***(Théorème de Wilson)*** *Soit p un nombre premier ; alors*

$$(p-1)! \equiv -1[p] \ .$$

Démonstration. Notons $\bar{x}$ la classe d'un entier x modulo p. Pour $p = 2$ le résultat est évident ; supposons donc $p \geq 3$. Vu que

$$(p-1)! = \Pi_{j=1}^{p-1} j \ ,$$

on a

$$\overline{(p-1)!} = \Pi_{j=1}^{p-1} \bar{j} \ ,$$

donc $\overline{(p-1)!}$ est égal au produit des éléments non nuls de $\mathbf{F}_p$. Mais l'équation $u = u^{-1}$ dans $\mathbf{F}_p$ équivaut à $u^2 = \bar{1}$ et donc, $\mathbf{F}_p$ étant un corps, à $u \in \{\bar{1}, -\bar{1}\}$. Les éléments de $\mathbf{F}_p \setminus \{0, \bar{1}, -\bar{1}\}$ se répartissent donc en paires (u, u^{-1}) de produit 1. Le produit des éléments non nuls de $\mathbf{F}_p$ est donc $\bar{1} \cdot (-\bar{1}) = -\bar{1}$. □

Remarque 2.5. On peut exprimer ce résultat en disant que le dernier chiffre de l'écriture de $(p-1)!$ en base p est $p-1$.

Remarque 2.6. L'argument utilisé dans la preuve du Théorème de Wilson s'applique dans n'importe quel groupe abélien fini possédant un et un seul élément d'ordre 2.

3. Fonction indicatrice d'Euler.

Théorème 3.1. *(Théorème des Restes Chinois)*
Soient m et n deux entiers ≥ 1 premiers entre eux; alors

$$\frac{\mathbf{Z}}{mn\mathbf{Z}} \simeq \frac{\mathbf{Z}}{m\mathbf{Z}} \times \frac{\mathbf{Z}}{n\mathbf{Z}}$$

en tant qu'anneaux.

Démonstration. Soit

$$\begin{aligned} \psi \quad : \quad & \mathbf{Z} \to \frac{\mathbf{Z}}{m\mathbf{Z}} \times \frac{\mathbf{Z}}{n\mathbf{Z}} \\ & a \mapsto (\pi_m(a), \pi_n(a)) \ . \end{aligned}$$

Il est clair que ψ est un morphisme d'anneaux. On a évidemment $\ker(\psi) = m\mathbf{Z} \cap n\mathbf{Z}$, lequel contient $mn\mathbf{Z}$; mais si $u \in m\mathbf{Z} \cap n\mathbf{Z}$, on peut écrire $u = mx$, d'où $n|mx$, puis, en vertu du Lemme de Gauss (car m et n sont premiers entre eux) $n|x$, *i.e* $x = ny$ et $u = mx = m(ny) = (mn)y \in mn\mathbf{Z}$. Donc $m\mathbf{Z} \cap n\mathbf{Z} \subset mn\mathbf{Z}$, $mn\mathbf{Z} = m\mathbf{Z} \cap n\mathbf{Z}$ et $\ker \psi = mn\mathbf{Z}$. On a donc

$$\frac{\mathbf{Z}}{mn\mathbf{Z}} = \mathbf{Z}/\ker \psi \simeq Im(\psi) \ ,$$

et il suffit d'établir la surjectivité de ψ. Soient donc

$$\alpha = \pi_m(a) \in \frac{\mathbf{Z}}{m\mathbf{Z}}$$

et

$$\beta = \pi_n(b) \in \frac{\mathbf{Z}}{n\mathbf{Z}} \ ;$$

d'après le Théorème de Bachet–Bezout, il existe $(x, y) \in \mathbf{Z}^2$ tel que $mx + ny = 1$.

Posons $z = nya + mxb$; alors

$$z = (1 - mx)a + mxb = a + mx(b - a) \equiv a[m]$$

et

$$z = nya + (1 - ny)b = b + ny(a - b) \equiv b[n] \ ,$$

donc $\pi_m(z) = \pi_m(a) = \alpha$ et $\pi_n(z) = \pi_n(b) = \beta$, c'est–à–dire que $\psi(z) = (\alpha, \beta)$. Nous avons bien établi la surjectivité de ψ. □

Remarque 3.2. Afin de conclure, nous aurions également pu comparer les cardinaux des deux ensembles : l'image $Im(\psi) \simeq \dfrac{\mathbf{Z}}{mn\mathbf{Z}}$ est de cardinal mn et est contenue dans $\dfrac{\mathbf{Z}}{m\mathbf{Z}} \times \dfrac{\mathbf{Z}}{n\mathbf{Z}}$, également de cardinal mn, d'où l'égalité.

Définition 3.3. On appelle *fonction indicatrice d'Euler* , et on note ϕ, l'application $\phi : \mathbf{N}^* \to \mathbf{N}^*$ définie par :

$$\forall n \in \mathbf{N}^* \ \ \phi(n) = |\{k \in \{1, ..., n\} | \text{pgcd(k, n)} = 1\}|$$

(*i.e.* $\phi(n)$ est le nombre d'entiers strictement positifs inférieurs ou égaux à n et premiers avec n).

Les premières valeurs en sont faciles à calculer : $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, et $\phi(6) = 2$.

Proposition 3.4. *On a :*

$$\forall n \geq 2 \quad \phi(n) \leq n-1 \ ,$$

et

$$\phi(n) = n-1 \iff n \text{ est premier} \ .$$

Démonstration. Si $n \geq 2$, alors, parmi $\{1, ..., n\}$ il y a au moins un élément non premier avec n (n lui-même), d'où (i). On a $\phi(n) = n-1$ si et seulement si $1, ..., n-1$ sont premiers avec n, ce qui est le cas si n est premier ; réciproquement, soit $n > 1$ non premier, et soit p le plus petit diviseur > 1 de n. Alors p est premier et $p \neq n$; il y a donc parmi $1, ..., n$ au moins deux entiers non premiers avec n (n lui–même et p), d'où $\phi(n) \leq n-2$. □

Plus généralement :

Théorème 3.5. *Si p est premier et $m \geq 1$, alors*

$$\phi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1) = p^m \left(1 - \frac{1}{p}\right) \ .$$

Démonstration. Un entier compris entre 1 et p^m n'est pas premier avec p^m si et seulement s'il a avec ce dernier un diviseur premier commun, lequel ne peut être que p. Les éléments de $\{1, ..., p^m\}$ non premiers avec p sont donc exactement les multiples de p contenus dans cet intervalle, c'est–à–dire les pk pour $1 \leq k \leq p^{m-1}$; il y en a donc p^{m-1}, d'où en effet

$$\phi(p^m) = p^m - p^{m-1} \ .$$

□

D'après les remarques du §2, on a le

Corollaire 3.6. *Pour chaque $n \geq 1$, $\phi(n)$ est égal au nombre d'éléments inversibles dans $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$.*

Théorème 3.7. *Lorsque m et n sont premiers entre eux, alors*

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

Démonstration. Il résulte du théorème des Restes Chinois (Théorème 3.1) que le groupe multiplicatif $U\left(\dfrac{\mathbf{Z}}{mn\mathbf{Z}}\right)$ des éléments inversibles de $\dfrac{\mathbf{Z}}{mn\mathbf{Z}}$ est isomorphe au groupe des éléments inversibles de $\dfrac{\mathbf{Z}}{m\mathbf{Z}} \times \dfrac{\mathbf{Z}}{n\mathbf{Z}}$ donc à

$$U\left(\frac{\mathbf{Z}}{m\mathbf{Z}}\right) \times U\left(\frac{\mathbf{Z}}{n\mathbf{Z}}\right).$$

Comparant les cardinaux de ces deux ensembles, on obtient le résultat annoncé. □

Soit alors $n = p_1^{a_1}...p_m^{a_m}$ la décomposition d'un entier n en facteurs premiers (les p_i étant deux à deux distincts, et les $a_i \geq 1$) ; il suit des Théorèmes 3.5 et 3.7 que

$$\begin{aligned}
\phi(n) &= \prod_{i=1}^{m} \phi(p_i^{a_i}) \\
&= \prod_{i=1}^{m} p_i^{a_i-1}(p_i - 1) \\
&= \prod_{i=1}^{m} p_i^{a_i}(1 - \frac{1}{p_i}) \\
&= \prod_{i=1}^{m} p_i^{a_i} \prod_{i=1}^{m}(1 - \frac{1}{p_i}) \\
&= n \prod_{p \text{ premier}, p|n} (1 - \frac{1}{p}) \ .
\end{aligned}$$

Carmichael a conjecturé (cf. [3], [4]) que toute valeur de ϕ était prise au moins deux fois

$$\forall n \geq 1 \ \exists m \neq n \ \ \phi(m) = \phi(n) \ .$$

Cela n'est toujours pas (Septembre 2020) établi.

Théorème 3.8. *Pour tout $n \geq 1$, on a :*

$$\sum_{d|n} \phi(d) = n \ .$$

Démonstration. Pour chaque $k \in \{1, ..., n\}$, $\text{pgcd}(k, n)$ est un diviseur de n. Pour d un diviseur fixé de n, cherchons donc le nombre de $k \in \{1, ..., n\}$ tels que $\text{pgcd}(k, n) = d$. Si $\text{pgcd}(k, n) = d$, on doit avoir $d|k$, d'où $k = dl$ avec $1 \leq l \leq \frac{n}{d}$. Alors

$$\text{pgcd}(k, n) = \text{pgcd}(dl, n) = d \, \text{pgcd}(l, \frac{n}{d})$$

et la condition $\text{pgcd}(k, n) = d$ équivaut à $\text{pgcd}\left(\text{l}, \frac{\text{n}}{\text{d}}\right) = 1$. Le nombre d'entiers $k \in \{1, ..., n\}$ tels que $\text{pgcd}(k, n) = d$ est donc égal au nombre d'entiers $l \in \{1, ..., \frac{n}{d}\}$ tels que $\text{pgcd}\left(\text{l}, \frac{\text{n}}{\text{d}}\right) = 1$, soit à $\phi(\frac{n}{d})$. On a donc

$$n = \sum_{d|n} \phi(\frac{n}{d}) \ .$$

Mais, lorsque d parcourt les diviseurs de n, $\frac{n}{d}$ fait de même, d'où

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$$

et le résultat. □

Théorème 3.9. ***(Euler)***
Soient $n \geq 1$ un entier, et $a \in \mathbf{Z}$ premier avec n. Alors

$$a^{\phi(n)} \equiv 1[n] \ .$$

Démonstration. $\phi(n)$ est l'ordre du groupe $U(\frac{\mathbf{Z}}{n\mathbf{Z}})$ des éléments inversibles de $\frac{\mathbf{Z}}{n\mathbf{Z}}$; en vertu d'une propriété bien connue des groupes finis, l'élément $\bar{a}$ de $U(\frac{\mathbf{Z}}{n\mathbf{Z}})$ vérifie donc :

$$\bar{a}^{\phi(n)} = \bar{1} \ ,$$

soit le résultat voulu. □

Corollaire 3.10. ***("Petit Théorème de Fermat")***
Soient p un nombre premier et a un entier. Alors

$$a^p \equiv a[p] \ .$$

Démonstration. Si p divise a, le résultat est clair ; dans le cas contraire, a est premier avec p (cf. §1, preuve du Corollaire 1.5), d'où

$$a^{p-1} = a^{\phi(p)} \equiv 1[p]$$

et

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

Une variante intéressante des deux derniers théorèmes est la suivante

Corollaire 3.11. *Soit $n \geq 1$ un entier sans facteur carré (par exemple le produit de deux nombres premiers distincts), et soient d et e deux entiers tels que $ed \equiv 1[\phi(n)]$. Alors, pour tout $a \in \mathbf{Z}$*

$$a^{ed} \equiv a[n] \ .$$

Démonstration. Nous traiterons uniquement le cas $n = pq$ (p et q étant deux nombres premiers distincts), seul utilisé en cryptographie ; le cas général n'en diffère pas sur le fond. Supposons $p \nmid a$. On a $p-1|(p-1)(q-1) = \phi(n)|ed-1$, donc, d'après la démonstration du Corollaire 3.10, $a^{ed-1} \equiv 1[p]$ et $a^{ed} = a.a^{ed-1} \equiv a.1 = a[p]$, *i.e.*

$$p|a^{ed} - a \ .$$

Ceci reste évidemment vrai si $p|a$.

De même

$$q|a^{ed} - a \ .$$

Soit $a^{ed} - a = px$; alors $q|a^{ed} - a = px$, et q et p, en tant que nombres premiers distincts, sont premiers entre eux. D'après le Lemme de Gauss, $q|x$, *i.e.* $x = qy$ et

$$a^{ed} - a = px = p(qy) = (pq)y = ny \ ,$$

d'où $a^{ed} \equiv a[n]$. □

Remarque 3.12. Ce Corollaire est à la base du système de cryptographie RSA ([6]) : on commence par représenter les données à chiffrer (lettres ou groupes de lettres) par des éléments de $\frac{\mathbf{Z}}{n\mathbf{Z}}$, où $n = pq$ est le produit de deux nombres premiers distincts assez grands (de l'ordre de 10^{50}). On choisit ensuite deux entiers d et e tels que $de \equiv 1[\phi(n)]$: d est la *clef de décodage* et e la *clef de chiffrement* ("encryption key"). On chiffre $M \in \frac{\mathbf{Z}}{n\mathbf{Z}}$ par $E(M) =_{\text{déf.}} M^e$, et on déchiffre $M \in \frac{\mathbf{Z}}{n\mathbf{Z}}$ par $D(M) =_{\text{déf.}} M^d$. Cela a un sens car

Théorème 3.13. *E et D sont inverses l'une de l'autre.*

Démonstration. On a, pour $M \in \dfrac{\mathbf{Z}}{n\mathbf{Z}}$:

$$E(D(M)) = E(M^d) = (M^d)^e = M^{de} = M$$

(d'après le Corollaire 3.11) et de même

$$D(E(M)) = M \ .$$

□

La *clef* e est publique ("public–key cryptography"); il n'est guère possible d'en déduire d car, par définition de d et e, calculer d connaissant e revient à calculer $\phi(n) = (p-1)(q-1) = pq-p-q+1 = n-p-q+1$ (cf. le calcul suivant le Théorème 3.7), soit à calculer $p+q$. Mais connaissant $pq = n$ et $p+q$, on déterminerait alors l'ensemble $\{p, q\}$; or, il n'existe pas de méthode de factorisation connue en temps raisonnable pour un nombre de l'ordre de 10^{100}, même sachant que ce nombre possède exactement deux facteurs premiers.

4. Résidus quadratiques, réciprocité quadratique.

Soit p un nombre premier ; recherchons les carrés de $\mathbf{F}_p$. Pour $p = 2$, on a $0^2 = 0$ et $1^2 = 1$, donc chaque élément de $\mathbf{F}_2$ est un carré. Soit donc p impair ; si $\alpha^2 = \beta^2$ dans $\mathbf{F}_p$, alors $\beta = \alpha$ ou $\beta = -\alpha$ ($\mathbf{F}_p$ étant un corps, les calculs usuels peuvent y être pratiqués). Pour $\alpha \neq 0$, il y a donc exactement deux éléments de $\mathbf{F}_p$ ayant le même carré que α : α lui–même et $-\alpha$. Le nombre de carrés non nuls dans $\mathbf{F}_p$ est donc $\dfrac{p-1}{2}$. Par ailleurs, si $\beta \in {\mathbf{F}_p}^*$ et $\alpha = \beta^2$, alors

$$\alpha^{\frac{p-1}{2}} = (\beta^2)^{\frac{p-1}{2}} = \beta^{p-1} = \overline{1}$$

comme il a été vu au §3. Mais l'équation $\alpha^{\frac{p-1}{2}} = \overline{1}$ possède **au plus** $\dfrac{p-1}{2}$ solutions dans $\mathbf{F}_p$ (l'argument habituel pour les polynômes complexes s'applique en effet dans n'importe quel corps), donc elle en possède **exactement** $\dfrac{p-1}{2}$, et ces solutions coïncident avec les carrés non nuls de $\mathbf{F}_p$. Vu que, pour chaque $\alpha \in {\mathbf{F}_p}^*$, on a

$$(\alpha^{\frac{p-1}{2}})^2 = \alpha^{p-1} = \overline{1} \ ,$$

on a $\alpha^{\frac{p-1}{2}} \in \{\overline{1}, -\overline{1}\}$. On a donc le

Théorème 4.1. *Soit a non multiple de p ; alors $\overline{a}$ est un carré dans $\mathbf{F}_p$ si et seulement si*

$$a^{\frac{p-1}{2}} \equiv 1[p] \ ;$$

dans le cas contraire,

$$a^{\frac{p-1}{2}} \equiv -1[p] \ .$$

Pour $a \in \mathbf{Z}$ non divisible par p, notons $(\dfrac{a}{p}) = 1$ si $\overline{a}$ est résidu quadratique modulo p, et -1 sinon (**symbole de Legendre**). Alors, d'après le Théorème 4.1, $(\dfrac{a}{p}) \equiv a^{\frac{p-1}{2}}[p]$. En particulier on a la

Proposition 4.2. *Le symbole de Legendre est multiplicatif, c'est–à–dire que*

$$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}) \ .$$

De plus

$$(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \ [p],$$

d'où il suit que

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} \ .$$

En particulier, pour p un nombre premier impair, $-\overline{1}$ est un carré dans $\mathbf{F}_p$ si et seulement si $p \equiv 1[4]$.

Lemme 4.3. ***(Gauss)*** *Soit a un entier premier à p ; pour chaque $x \in \{1, ..., \frac{p-1}{2}\}$, il existe un unique couple $(\epsilon_x(a), y_{x,a}) \in \{-1, 1\} \times \{1, ..., \frac{p-1}{2}\}$ tel que*

$$ax \equiv \epsilon_x(a) y_{x,a} [p] \ .$$

Alors

$$(\frac{a}{p}) = \prod_{x=1}^{\frac{p-1}{2}} \epsilon_x(a) \ .$$

Démonstration. Dans le cours de cette démonstration, $\equiv$ signifiera congruence modulo p.

L'existence des couples $(\epsilon_x(a), y_{x,a})$ est évidente car les classes $\neq 0$ de $\mathbf{F}_p$ sont $\overline{1}, ..., \overline{\frac{p-1}{2}}, \overline{\frac{p+1}{2}} = -\overline{\frac{p-1}{2}}, ..., \overline{p-1} = -\overline{1}$. De plus, de $y_{x,a} = y_{x',a}$ suit

$$\begin{aligned} ax \quad & \equiv \epsilon_x(a) y_{x,a} \\ & = \epsilon_x(a) y_{x',a} \\ & = \epsilon_x(a) \epsilon_{x'}(a)^{-1} \epsilon_{x'}(a) y_{x',a} \\ & = \alpha \epsilon_{x'}(a) y_{x',a} \\ & \equiv \alpha x' a [p] \end{aligned}$$

pour un $\alpha \in \{-1, 1\}$, d'où $p | a(x - \alpha x')$ soit $p | a(x - x')$ ou $p | a(x + x')$. Mais $p \nmid a$, donc $p | x - x'$ ou $p | x + x'$. Vu que $2 \leq x + x' \leq p - 1$, on a nécessairement $p | x - x'$, soit $x = x'$. Nous avons montré que l'application

$$\begin{array}{ccc} \{1, ... \frac{p-1}{2}\} & \to & \{1, ... \frac{p-1}{2}\} \\ x & \mapsto & y_{x,a} \end{array}$$

était injective ; elle est donc bijective, d'où :

$$\prod_{x=1}^{\frac{p-1}{2}} y_{x,a} = \prod_{x=1}^{\frac{p-1}{2}} x \ .$$

Mais alors

$$\begin{aligned} a^{\frac{p-1}{2}} \prod_{x=1}^{\frac{p-1}{2}} x \quad & = \quad \prod_{x=1}^{\frac{p-1}{2}} (ax) \\ & \equiv \quad \prod_{x=1}^{\frac{p-1}{2}} (\epsilon_x(a) y_{x,a}) \\ & = \quad \prod_{x=1}^{\frac{p-1}{2}} \epsilon_x(a) \prod_{x=1}^{\frac{p-1}{2}} y_{x,a} \\ & = \quad \prod_{x=1}^{\frac{p-1}{2}} \epsilon_x(a) \prod_{x=1}^{\frac{p-1}{2}} x \end{aligned}$$

d'où

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \equiv \prod_{x=1}^{\frac{p-1}{2}} \epsilon_x(a) \ .$$

Le résultat s'ensuit, vu que $(\frac{a}{p})$ et

$$\prod_{x=1}^{\frac{p-1}{2}} \epsilon_x(a)$$

appartiennent à $\{-1, 1\}$ et que p est impair. □

Théorème 4.4. *(Loi de Réciprocité Quadratique) Si p et q sont deux nombres premiers impairs distincts, alors*

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}} \ .$$

Ce résultat a été conjecturé par Euler, puis démontré par Gauss, après des tentatives presque concluantes de Legendre ; il s'agit de l'un des plus beaux théorèmes de l'Arithmétique. Une grande partie des recherches effectuées depuis deux siècles en théorie des nombres a eu pour objet de le généraliser : la théorie du corps de classes (Hilbert (1896), Takagi (1920), Artin (1923), Chevalley (1936)) et le programme de Langlands (Langlands (1967), Lafforgue (2002)) en sont directement issus.

Démonstration. D'après le Lemme 4.5, on a $(\frac{q}{p}) = (-1)^{N_p(q)}$, où $N_p(q)$ désigne le nombre de $x \in \{1, ..., \frac{p-1}{2}\}$ tels que le reste modulo p de qx soit $> \frac{p-1}{2}$, c'est–à–dire qu'existe $y \in \mathbf{Z}$ tel que

$$\frac{p+1}{2} \leq qx - py \leq p-1 \quad (*) \ .$$

Il est clair qu'à x fixé, il existe au plus un y tel que $(*)$ soit vérifiée ; $N_p(q)$ peut donc être défini comme le nombre de couples $(x, y) \in \mathbf{Z}^2$ tels que $1 \leq x \leq \frac{p-1}{2}$ et

$$\frac{p+1}{2} \leq qx - py \leq p-1 \quad (**) \ .$$

En posant $z = 1 + y$, $(**)$ devient

$$\frac{1-p}{2} \leq qx - pz \leq -1 \ ,$$

soit

$$1 \leq pz - qx \leq \frac{p-1}{2} \ .$$

Mais ceci entraîne

$$1 \leq z \leq \frac{q-1}{2} \ .$$

On a donc $N_p(q) = |E|$, où E est défini par :

$$E = \{(x, z) \in \mathbf{Z}^2 | 1 \leq x \leq \frac{p-1}{2}, 1 \leq z \leq \frac{q-1}{2}, 1 \leq pz - qx \leq \frac{p-1}{2}\}.$$

De même $N_q(p) = |E^{'}|$, avec

$$E^{'} = \{(x, z) \in \mathbf{Z}^2 | 1 \leq x \leq \frac{q-1}{2}, 1 \leq z \leq \frac{p-1}{2}, 1 \leq qz - px \leq \frac{q-1}{2}\}.$$

Mais

$$|E^{'}| = |E^{''}|$$

où

$$\begin{aligned} E^{''} &= \{(x,z) \in \mathbf{Z}^2 | 1 \leq x \leq \frac{p-1}{2}, 1 \leq z \leq \frac{q-1}{2}, 1 \leq qx - pz \leq \frac{q-1}{2}\} \\ &= \{(x,z) \in \mathbf{Z}^2 | 1 \leq x \leq \frac{p-1}{2}, 1 \leq z \leq \frac{q-1}{2}, -\frac{q-1}{2} \leq pz - qx \leq -1\}. \end{aligned}$$

Mais, pour $1 \leq z \leq \frac{q-1}{2}$, on a $q \nmid z$ donc $q \nmid pz$, $pz \neq qx$ et $pz - qx \neq 0$; il s'ensuit :

$$\begin{aligned} N_p(q) + N_q(p) &= |E| + |E^{''}| \\ &= |E \cup E^{''}| (\text{car } E \text{ et } E^{''} \text{ sont disjoints}) \\ &= |\{(x,z) \in \mathbf{Z}^2 | 1 \leq x \leq \frac{p-1}{2}, 1 \leq z \leq \frac{q-1}{2}, \\ &\quad -(\frac{q-1}{2}) \leq pz - qx \leq \frac{p-1}{2}\}| \\ &= |E^{'''}| \end{aligned}$$

où l'on a posé

$$E^{'''} := E \cup E^{''} = \{(x,z) \in \mathbf{Z}^2 | 1 \leq x \leq \frac{p-1}{2}, 1 \leq z \leq \frac{q-1}{2}, -(\frac{q-1}{2}) \leq pz - qx \leq \frac{p-1}{2}\}.$$

Il est facile de voir que

$$\begin{aligned} h &: \mathbf{Z}^2 \to \mathbf{Z}^2 \\ &\quad (x,z) \mapsto (\frac{p+1}{2} - x, \frac{q+1}{2} - z) \end{aligned}$$

est une involution laissant invariant $E^{'''}$. Lorsque $p \equiv 1[4]$ ou $q \equiv 1[4]$, h ne possède aucun point fixe, donc $h|_{E^{'''}}$ n'en a pas non plus, et $|E^{'''}|$ est pair ; dans le cas contraire ($p \equiv 3[4]$ et $q \equiv 3[4]$), h possède un unique point fixe ($\alpha = (\frac{p+1}{4}, \frac{q+1}{4})$) et il est facile de voir que $\alpha \in E^{'''}$, donc α est le seul point fixe de $h|_{E^{'''}}$, et $|E^{'''}|$ est impair. Mais nous avons vu que

$$\begin{aligned} (\frac{p}{q})(\frac{q}{p}) &= (-1)^{N_p(q)+N_q(p)} \\ &= (-1)^{|E^{'''}|}, \end{aligned}$$

donc le produit $(\frac{p}{q})(\frac{q}{p})$ vaut 1 si $p \equiv 1[4]$ ou $q \equiv 1[4]$ (auquel cas $\frac{(p-1)(q-1)}{4}$ est pair) et -1 si $p \equiv 3[4]$ et $q \equiv 3[4]$ (auquel cas $\frac{(p-1)(q-1)}{4}$ est impair), d'où le résultat. □

On a de plus le

Théorème 4.5. *(Formule complémentaire) Si p est un nombre premier impair, alors*

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}.$$

Démonstration. Si $p \equiv 1[4]$, écrivons $p = 4m + 1$; pour $1 \leq x \leq m$, on a $2x = 1.2x$ et $\epsilon_x(2) = 1$, $y_{x,2} = 2x$; pour $m + 1 \leq x \leq 2m$ on a

$$\frac{p+1}{2} = 2m + 1 \leq 2m + 2 \leq 2x \leq 4m = p - 1$$

d'où $\epsilon_x(2) = -1$ et $y_{x,2} = p - 2x$. Il s'ensuit que

$$\prod_{x=1}^{\frac{p-1}{2}} \epsilon_x(2) = (-1)^m \ ,$$

d'où

$$(\frac{2}{p}) = (-1)^m \ .$$

Mais $\frac{p^2-1}{8} = 2m^2 + m$ et $(-1)^{\frac{p^2-1}{8}} = (-1)^m$.

Dans le cas $p \equiv 3[4]$, posons $p = 4m + 3$; pour $1 \leq x \leq m$, on a $2x = 1.2x \leq 2m \leq 2m + 1 = \frac{p-1}{2}$ et $\epsilon_x(2) = 1$, $y_{x,2} = 2x$; pour

$$m + 1 \leq x \leq 2m + 1$$

on a $\frac{p+1}{2} = 2m + 2 \leq 2x \leq 4m + 2 = p - 1$ d'où $\epsilon_x(2) = -1$ et $y_{x,2} = p - 2x$. Mais alors

$$\prod_{x=1}^{\frac{p-1}{2}} \epsilon_x(2) = (-1)^{m+1} \ ,$$

donc $(\frac{2}{p}) = (-1)^{m+1}$. Vu que

$$\frac{p^2-1}{8} = 2m^2 + 3m + 1$$

et $(-1)^{\frac{p^2-1}{8}} = (-1)^{m+1}$, on obtient, dans l'un et l'autre cas, la conclusion du Théorème. □

Pour une autre démonstration, l'on peut consulter [7].

5. Nombres de Fermat.

On appelle nombres de Fermat les éléments de la suite

$$F_n = 2^{2^n} + 1 (n \in \mathbf{N}) \ .$$

Fermat observa que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ étaient tous premiers, et conjectura donc que tous les F_n étaient premiers. Euler trouva un contre–exemple : $F_5 = 2^{32} + 1 = 4294967297$ est divisible par 641. En effet,

$$4294967297 = 641 \cdot 6700417 \ .$$

Il est possible de "deviner" le facteur 641 au moyen du résultat suivant :

Lemme 5.1. *Soit p un diviseur premier de F_n ; alors*

$$p \equiv 1[2^{n+1}] \ .$$

Démonstration. Soit p un diviseur premier de F_n ; alors $p|2^{2^n} + 1$, donc

$$2^{2^n} \equiv -1[p] \ .$$

En particulier

$$2^{2^n} \not\equiv 1[p] \ ,$$

donc l'ordre (multiplicatif) m de $\overline{2}$ dans ${\mathbf{F}_p}^*$ ne divise pas 2^n. Mais

$$2^{2^{n+1}} = (2^{2^n})^2 \equiv (-1)^2 = 1[p] \ ,$$

donc m divise 2^{n+1}. On a donc $m = 2^k$ pour un $k \leq n+1$. Si l'on avait $k \leq n$, on aurait $m = 2^k|2^n$, une contradiction ; donc $m = 2^{n+1}$. Mais alors m, étant l'ordre d'un élément de ${\mathbf{F}_p}^*$, divise l'ordre de ${\mathbf{F}_p}^*$, soit $p-1$, c'est–à–dire que

$$p \equiv 1[2^{n+1}] \ .$$

□

Pour chercher le plus petit diviseur (premier) de F_5, on peut donc se limiter aux nombres premiers congrus à 1 modulo $2^6 = 64$; les quatre plus petits sont 193, 257, 449 et 577, lesquels ne conviennent pas (on peut d'ailleurs récuser $257 = F_3$ au moyen de la Proposition 5.3 ci–dessous). Le suivant, 641, s'avère diviser F_5 (cette démarche est essentiellement celle d'Euler).

Un critère de primalité pour les nombres de Fermat a été établi par Pépin :

Théorème 5.2. *Soit n un entier ≥ 1. L'entier F_n est premier si et seulement si*

$$3^{2^{2^n-1}} \equiv -1[F_n] \ .$$

Démonstration. Supposons que $3^{2^{2^n-1}} \equiv -1[F_n]$, et soit p un diviseur premier de F_n ; alors l'argument utilisé dans la preuve du Lemme 5.1 montre que 2^{2^n} est l'ordre multiplicatif de $\overline{3}$ dans $\mathbf{F}_p^*$. En particulier 2^{2^n} divise $p-1$, donc $p-1 \geq 2^{2^n}$, soit $p \geq 2^{2^n} + 1 = F_n$. Mais alors $F_n = p$ est premier.

La démonstration de la réciproque est moins élémentaire. Supposons que F_n soit premier, posons $p = 3$ et $q = F_n$, et appliquons la Loi de Réciprocité Quadratique

(Théorème 4.6). On obtient

$$\begin{aligned}(\frac{3}{q})(\frac{q}{3}) &= (-1)^{\frac{(3-1)(q-1)}{4}} \\ &= (-1)^{\frac{q-1}{2}} \\ &= (-1)^{2^{2^n}-1} \\ &= 1\ ,\end{aligned}$$

donc

$$(\frac{3}{q}) = (\frac{q}{3})\ .$$

Mais $q = F_n \equiv (-1)^{2^n} + 1 = 2[3]$, d'où

$$(\frac{q}{3}) = (\frac{2}{3}) = -1$$

et

$$(\frac{3}{q}) = -1\ .$$

Il s'ensuit que $3^{\frac{q-1}{2}} \equiv -1[q]$, soit $3^{2^{2^n}-1} \equiv -1[F_n]$. □

A ce jour (Septembre 2020), les seuls nombres de Fermat premiers connus sont toujours F_0,...,F_4; on sait des $(F_n)_{5\leq n\leq 32}$ qu'ils sont composés.

Néanmoins on a la

Proposition 5.3. *Si $m \neq n$, F_m et F_n sont premiers entre eux.*

Démonstration. On peut supposer que $m < n$; alors

$$\begin{aligned}F_n &= 2^{2^n} + 1 \\ &= 2^{2^m \cdot 2^{n-m}} + 1 \\ &= (2^{2^m})^{2^{n-m}} + 1 \\ &= (F_m - 1)^{2^{n-m}} + 1 \\ &\equiv (-1)^{2^{n-m}} + 1 \\ &\equiv 2\,[F_m]\ .\end{aligned}$$

Il existe donc un entier k tel que $F_n = kF_m + 2$. Si un entier d divise F_m et F_n, il divise $F_n - kF_m = 2$, donc $d = 1$ ou $d = 2$. Mais F_m est impair, d'où $d = 1$. □

D'où le

Corollaire 5.4. *L'ensemble* $\mathbf{P}$ *des nombres premiers est infini.*

Démonstration. Pour chaque $n \in \mathbf{N}$, soit q_n le plus petit diviseur strictement supérieur à 1 de F_n ; alors chaque q_n est premier, et, d'après la Proposition 5.3, les $(q_n)_{n\in\mathbf{N}}$ sont deux à deux distincts. □

6. Sommes de deux carrés

Fermat, suite à des essais numériques, conjectura que chaque nombre premier de la forme $4m+1$ était somme de deux carrés d'entiers ; par exemple $29 = 5^2 + 2^2$, $61 = 6^2 + 5^2$, etc.. Euler démontra le premier ce résultat, ouvrant ainsi l'ère moderne de la Théorie des Nombres.

Théorème 6.1. *Soit p un nombre premier de la forme $4m+1$; alors il existe $(a,b) \in \mathbf{N}^2$ tel que $p = a^2 + b^2$.*

Démonstration. Nous établirons tout d'abord l'existence d'un entier $x \geq 0$ tel que p divise $x^2 + 1$. Utilisons pour cela le Théorème de Wilson (Théorème 2.4): $(4m)! = (p-1)! \equiv -1[p]$, et

$$(4m)! = 1 \cdot 2 \cdot \ldots \cdot 2m \cdot (2m+1) \cdot \ldots \cdot 4m \ .$$

Mais $2m+1 \equiv -2m[p]$, $\ldots$, $4m \equiv -1[p]$, d'où :

$$(2m+1) \cdot \ldots \cdot 4m \equiv (-2m) \ldots (-1) = (-1)^{2m}(2m)! \equiv (2m)! \ [p] \ .$$

On a donc

$$(4m)! \equiv (2m)!^2 [p] \ ,$$

soit

$$(2m)!^2 \equiv -1[p] \ ,$$

et $x = (2m)!$ convient.

En utilisant des concepts introduits au §4, l'on peut justifier autrement

l'assertion : d'après la remarque précédant Théorème 4.3, $-\overline{1}$ est un carré dans $\mathbf{F}_p$, donc il existe $\overline{x} \in \mathbf{Z}/p\mathbf{Z}$ tel que $\overline{x}^2 = -\overline{1}$, soit $p|x^2+1$.

L'entier $x^2 + 1^2$ est donc divisible par p. Parmi tous les entiers strictement positifs de la forme $a^2 + b^2$(a et b premiers entre eux) qui sont divisibles par p, choisissons alors le plus petit

$$a^2 + b^2 = np \ .$$

Si $n = 1$, on a bien $p = a^2 + b^2$ et le théorème est démontré.

Supposons donc $n \geq 2$, et divisons a par p : on obtient $a = pl + r$, avec

$0 \leq r < p$; si $r > \frac{p}{2}$, on peut écrire $a = p(l+1) - (p-r)$ avec $0 \leq p - r < p/2$; remplaçant alors r par $p - r$, on obtient, dans les deux cas, $a = pl + \varepsilon_1 r$ avec $\varepsilon_1 = 1 \,\text{ou}\, -1$ et $0 \leq r \leq p/2$, d'où $0 \leq r < p/2$ car p est impair. De même, $b = pk + \varepsilon_2 s$ avec $0 \leq s < p/2$ et $\varepsilon_2 = 1 \,\text{ou}\, -1$. On a alors

$$r^2 + s^2 \equiv a^2 + b^2 = np \equiv 0[p] \ ,$$

d'où $p|r^2 + s^2$. Vu que a et b sont premiers entre eux, on a $r \neq 0$ ou $s \neq 0$ (en fait $r \neq 0$ et $s \neq 0$), d'où $r^2 + s^2 \neq 0$. Soit alors $d = \text{pgcd(r, s)}$, et posons $r = du$, $s = dv$. Alors $r^2 + s^2 = d^2(u^2 + v^2)$ et $p \nmid d$, donc $p|u^2 + v^2$. Vu le choix de n, on a $a^2 + b^2 \leq u^2 + v^2$ d'où

$$\begin{aligned} np &= a^2 + b^2 \\ &\leq u^2 + v^2 \\ &\leq r^2 + s^2 \\ &< 2(p/2)^2 \\ &= p^2/2, \end{aligned}$$

et

$$n < p/2 \ .$$

Divisons maintenant a par n (c'est l'idée cruciale de la démonstration). Par le même raisonnement que ci–dessus, remplaçant p par n, on obtient $a = nq + \varepsilon x$ avec $\varepsilon = 1$ ou -1 et $0 \leq x \leq n/2$, et de même $b = nq' + \varepsilon' y$ avec $\varepsilon' = 1$ ou -1 et $0 \leq y \leq n/2$

Mais alors

$$x^2 + y^2 \equiv a^2 + b^2 = np \equiv 0[n] \ ,$$

c'est–à–dire que n divise $x^2 + y^2$; autrement dit, $x^2 + y^2 = nw$ pour un w entier. Si l'on avait $w = 0$, on aurait $x = y = 0$ donc $n|a$ et $n|b$, d'où $n^2|a^2 + b^2 = np$, $n|p$, et $n = 1$ ou $n = p$, contredisant l'encadrement déjà établi : $2 \leq n < p/2$. On a donc $w \geq 1$; en outre

$$\begin{aligned} n^2pw &= np(x^2 + y^2) \\ &= (a^2 + b^2)((\epsilon\epsilon' x)^2 + y^2) \\ &= (ay - b\epsilon\epsilon' x)^2 + (a\epsilon\epsilon' x + by)^2 \ . \end{aligned}$$

Mais $ay - b\epsilon\epsilon' x = (nq + \epsilon x)y - (nq' + \epsilon' y)\epsilon\epsilon' x = n(qy - q'\epsilon\epsilon' x)$ est divisible par n, donc n^2 divise

$$(a\epsilon\epsilon' x + by)^2 = n^2pw - (ay - b\epsilon\epsilon' x)^2 \ ,$$

i.e. n divise $a\epsilon\epsilon' x + by$. Posons maintenant $|ay - b\epsilon\epsilon' x| = nf$ et $|a\epsilon\epsilon' x + by| = ng$; alors $n^2pw = np(x^2 + y^2) = (nf)^2 + (ng)^2 = n^2(f^2 + g^2)$, donc $f^2 + g^2 = pw$. Mais

$$nw = x^2 + y^2 \leq 2(n/2)^2 = n^2/2,$$

d'où $w \leq n/2 < n$, et aussi $w \leq p/4 < p$; en particulier, $p \nmid w$. Soit $d' = \mathrm{pgcd(f, g)}$, et soient $f = d'h$, $g = d'i$. Alors $(d')^2(h^2 + i^2) = f^2 + g^2 = pw$; vu que $p \nmid t$, $p^2 \nmid pw$ donc $p \nmid d'$. Mais alors $p|h^2 + i^2$ et $h^2 + i^2 = pj$ avec $(d')^2pj = pw$, $(d')^2j = w$ et donc $1 \leq j \leq w \leq \frac{n}{2} < n$, ce qui contredit la définition de n. □

Seconde démonstration du Théorème 6.1. Nous allons maintenant donner une démonstration élémentaire de ce résultat, due à Zagier ([8] ; cf.aussi [1]).

Soit S l'ensemble des triplets $(x, y, z) \in (\mathbf{N}^*)^3$ tels que $x^2 + 4yz = p$; cet ensemble est bien évidemment fini. Si $(x, y, z) \in S$, on ne peut avoir $x = y - z$ (car on aurait alors $p = (y - z)^2 + 4yz = (y + z)^2$, contredisant la primalité de p), ni $x = 2y$ (car on aurait alors $p = (2y)^2 + 4yz = 4y(y + z)$ et la même contradiction).

L'ensemble S est donc la réunion disjointe des ensembles S_1, S_2 et S_3 respectivement définis par :

$$S_1 = \{(x, y, z) \in (\mathbf{N}^*)^3, \ x^2 + 4yz = p \text{ et } x < y - z\} \ ,$$

$$S_2 = \{(x, y, z) \in (\mathbf{N}^*)^3, \ x^2 + 4yz = p \text{ et } y - z < x < 2y\} \ ,$$

et

$$S_3 = \{(x, y, z) \in (\mathbf{N}^*)^3, \ x^2 + 4yz = p \ \text{ et } 2y < x\} \ .$$

Soit l'application f définie sur S par

$$f(x, y, z) = \begin{cases} (x + 2z, z, y - x - z) \text{ si } (x, y, z) \in S_1 \\ (2y - x, y, x - y + z) \text{ si } (x, y, z) \in S_2 \\ (x - 2y, x - y + z, y) \text{ si } (x, y, z) \in S_3. \end{cases}$$

Il est facile de vérifier que $f(S_1) \subseteq S_3$, $f(S_2) \subseteq S_2$ et $f(S_3) \subseteq S_1$; en particulier, $f(S) \subseteq S$. Un calcul simple montre alors que

$$\forall (x,y,z) \in S^3 \quad f(f(x,y,z)) = (x,y,z) \ .$$

En particulier f est une involution de S, d'où $f(S) = S$, $f(S_1) = S_3$, $f(S_2) = S_2$ et $f(S_3) = S_1$. Il est clair que f n'a de point fixe ni dans S_1 ni dans S_3, et que son unique point fixe dans S_2 est $(1,1,\frac{p-1}{4}) = (1,1,m)$; en particulier f a au total un point fixe dans S, donc le cardinal $|S|$ de S est impair.

Mais alors l'involution évidente

$$\begin{array}{rcl} g & : & S \to S \\ & & (x,y,z) \mapsto (x,z,y) \end{array}$$

possède au moins un point fixe, c'est–à–dire qu'il existe $(x,y,z) \in S$ tel que $y = z$, d'où $p = x^2 + 4yz = x^2 + 4y^2 = x^2 + (2y)^2$, et le résultat en découle, avec $a = x$ et $b = 2y$.

Remarque 6.2. Cette décomposition est d'ailleurs unique, à interversion près de a et b : supposons en effet $p = a^2 + b^2 = c^2 + d^2$; on peut alors écrire, en vertu de l'identité de Lagrange :

$$\begin{array}{rcl} p^2 & = & (a^2+b^2)(c^2+d^2) \\ & = & (ad+bc)^2 + (ac-bd)^2 \quad (\mathcal{E}_1) \end{array}$$

et de même

$$p^2 = (ad-bc)^2 + (ac+bd)^2 \quad (\mathcal{E}_2) \ .$$

Mais

$$\begin{array}{rcl} (ad-bc)(ad+bc) & = & a^2d^2 - b^2c^2 \\ & = & (a^2+b^2)d^2 - b^2(c^2+d^2) \\ & = & p(d^2-b^2) \\ & \equiv & 0[p] \end{array}$$

d'où $p|ad-bc$ ou $p|ad+bc$. Si $p|ad-bc$, alors $p^2|(ad-bc)^2$, d'où, d'après $(\mathcal{E}_2)$ et du fait que $a,b,c,d \geq 1$, $ad-bc = 0$ et $ac+bd = p$. Mais alors

$$\begin{array}{rcl} pc & = & (a^2+b^2)c \\ & = & -b(ad-bc) + a(ac+bd) \\ & = & -b \cdot 0 + a \cdot p \\ & = & pa \ , \end{array}$$

d'où $c = a$ et donc $d = b$.

De même, si p divise $ad+bc$, il suit de $(\mathcal{E}_1)$ que $ad+bc = p$ et $ac-bd = 0$, d'où

$$\begin{array}{rcl} pd & = & (a^2+b^2)d \\ & = & a(ad+bc) - b(ac-bd) \\ & = & a \cdot p - b \cdot 0 \\ & = & pa \end{array}$$

et maintenant $d = a$, d'où $c = b$. □

Nous sommes pouvons maintenant caractériser les entiers sommes de deux carrés.

Théorème 6.3. *Pour tout entier $n \geq 1$, les propositions suivantes sont équivalentes*

(1) *Il existe $(x, y) \in \mathbf{N}^2$ tel que $n = x^2 + y^2$.*
(2) *Pour chaque nombre premier $q \equiv 3[4]$ la valuation q–adique $v_q(n)$ de n est paire.*

Démonstration. (1) $\Rightarrow$ (2)

Soit $q \equiv 3[4]$, et procédons par récurrence sur n, en supposant le résultat établi pour tous les entiers strictement inférieurs à n. Si $v_q(n) = 0$ il n'y a rien à démontrer. Supposons donc $v_q(n) \geq 1$; alors q divise $n = a^2 + b^2$. Dans $\dfrac{\mathbf{Z}}{q\mathbf{Z}}$ on peut donc écrire

$$(\bar{a})^2 + (\bar{b})^2 = a^2 \bar{+} b^2 = \bar{n} = \bar{0}.$$

Si l'on avait $\bar{a} \neq \bar{0}$, il s'ensuivrait $(\bar{b})^2 = -(\bar{a})^2$ et

$$(\frac{\bar{b}}{\bar{a}})^2 = -\bar{1}$$

et $-\bar{1}$ serait un carré dans $\dfrac{\mathbf{Z}}{q\mathbf{Z}}$, contredisant la remarque suivant la démonstration de la Proposition 4.2. On a donc $\bar{a} = \bar{0}$, d'où $(\bar{b})^2 = -(\bar{a})^2 = \bar{0}$ et $\bar{b} = \bar{0}$: q divise a et b. On peut donc écrire $a = qc$ et $b = qd$ avec c et d entiers. Mais alors

$$n = a^2 + b^2 = (qc)^2 + (qd)^2 = q^2(c^2 + d^2).$$

Il en résulte que q^2 divise n et que

$$\frac{n}{q^2} = c^2 + d^2.$$

Mais $\dfrac{n}{q^2} < n$, donc, en vertu de l'hypothèse de récurrence, $v_q(\dfrac{n}{q^2})$ est pair ; mais alors $v_q(n) = 2 + v_q(\dfrac{n}{q^2})$ l'est.

(2) $\Rightarrow$ (1)

Remarquons tout d'abord que tout produit de sommes de deux carrés d'entier en est une. Il suffit de l'établir pour deux facteurs, auquel cas cela résulte de l'Identité de Lagrange :

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2,$$

déjà utilisée à plusieurs reprises.

Soient $p_1, ..., p_r$ les diviseurs premiers de n congrus à 3 modulo 4, et $p_{r+1}, ..., p_{r+s}$ les autres diviseurs premiers de n. Ecrivons

$$n = p_1^{\alpha_1} ... p_{r+s}^{\alpha_{r+s}}.$$

Pour chaque $i \geq r + 1$, p_i est soit égal à $2 = 1^2 + 1^2$, soit est congru à 1 modulo 4, donc, d'après le Théorème 6.1, est somme de deux carrés d'entiers.

Pour $i \leq r$, α_i est pair par hypothèse : $\alpha_i = 2\beta_i$, d'où

$$p_i^{\alpha_i} = p_i^{2\beta_i} = (p_i^{\beta_i})^2 = (p_i^{\beta_i})^2 + 0^2$$

est somme de deux carrés d'entiers.

Donc

$$n = p_1^{\alpha_1} ... p_r^{\alpha_r} p_{r+1} ... p_{r+1} ... p_{r+s} ... p_{r+s}$$

est un produit de sommes de deux carrés, donc en est une. □

7. Corps finis.

Soit K un corps fini ; définissons

$$\begin{aligned} \theta \quad : \quad & \mathbf{Z} \to K \\ & n \mapsto n.1_K \ . \end{aligned}$$

Alors θ est un morphisme d'anneaux, et $\dfrac{\mathbf{Z}}{\ker(\theta)}$ est isomorphe à $Im(\theta)$, un sous–anneau de K ; en particulier, il est fini et intègre. De sa finitude résulte que $\ker(\theta) \neq \{0\}$. Mais $\ker(\theta)$ est un idéal de $\mathbf{Z}$, donc de la forme $a\mathbf{Z}$ pour un (unique) $a \geq 1$. Vu que

$$\theta(1) = 1_K \neq 0 \ ,$$

on a $1 \notin \ker(\theta)$, donc $a \geq 2$; $\dfrac{\mathbf{Z}}{a\mathbf{Z}}$ étant intègre, a est premier (Théorème 3.2). Nous noterons dorénavant $p = a$; K contient le sous–anneau

$$K_0 := Im(\theta) \simeq \frac{\mathbf{Z}}{p\mathbf{Z}} \ ,$$

c'est–à–dire un sous–anneau isomorphe au corps $\mathbf{F}_p$. On appelle p la *caractéristique* de K.

Le corps K peut être considéré comme un espace vectoriel sur son sous–corps K_0 ; en tant que tel, il est isomorphe à une puissance K_0^n ($n \geq 1$), d'où

$$|K| = |K_0^n| = |K_0|^n = p^n \ .$$

En résumé, nous venons d'établir la

Proposition 7.1. *Soit K un corps fini ; alors il existe un nombre premier p et un entier $n \geq 1$ tels que*

$$|K| = p^n \ .$$

Réciproquement, on a le

Théorème 7.2. ***(Galois** [5]**)** Pour tout nombre premier p et tout entier $n \geq 1$, il existe un corps fini de cardinal p^n, unique à isomorphisme près.*

Ce corps sera noté $\mathbf{F}_{p^n}$ (parfois $GC(p^n)$ ou $GF(p^n)$).

Remarque 7.3. Attention à ne pas confondre ce corps avec l'anneau $\dfrac{\mathbf{Z}}{p^n\mathbf{Z}}$ (ils ne sont isomorphes que pour $n = 1$).

Remarque 7.4. En fait, tout anneau à division fini est commutatif (Théorème de Wedderburn) ; il s'agit donc d'un corps.

Proof. Par abus de langage, nous noterons 1 l'élément unité de chacun des corps considérés.

Supposons que K soit un corps de cardinal p^n. Comme vu ci–dessus, K contient un sous–corps $K_0 \simeq \mathbf{F}_p$, que nous identifierons dorénavant à $\mathbf{F}_p$ lui–même.

Chaque élément non nul α de K vérifie $\alpha^{p^n-1} = 1$ (car K^* est un groupe (multiplicatif) d'ordre $p^n - 1$) donc $\alpha^{p^n} = \alpha$. Cette dernière équation est trivialement satisfaite pour $\alpha = 0$; elle l'est donc pour tout $\alpha \in K$.

Pour chaque $\alpha \in K$, $X - \alpha$ divise donc (dans $K[X]$) le polynôme

$$Q(X) := X^{p^n} - X \in K[X],$$

donc

$$\prod_{\alpha\in K}(X-\alpha)$$

divise $Q(X)$. Mais ces deux polynômes sont unitaires et de même degré p^n, donc ils coïncident :

$$X^{p^n}-X=\prod_{\alpha\in K}(X-\alpha).$$

Il en résulte que $X^{p^n}-X$ est scindé sur K et que le corps engendré par ses racines sur $\mathbf{F}_p$ est

$$\mathbf{F}_p(\alpha|\alpha\in K)=K.$$

En particulier, K est un **corps de décomposition** de $X^{p^n}-X$ sur $\mathbf{F}_p$, d'où l'unicité à isomorphisme près de K.

Réciproquement, soit M un corps de décomposition de $X^{p^n}-X$ sur $\mathbf{F}_p$, et posons

$$L:=\{x\in M|x^{p^n}=x\}\ .$$

Tout d'abord, le polynôme $Q(X)=X^{p^n}-X\in\mathbf{F}_p[X]$ est scindé sur M ; par ailleurs, son polynôme dérivé est

$$Q^{'}(X)=p^nX^{p^n-1}-1=-1\ ,$$

lequel est premier avec Q. Toutes les racines de Q sont donc simples, d'où $|L|=p^n$. Soit

$$\begin{aligned}F\quad:\quad & M\to M\\ & x\mapsto x^p\ .\end{aligned}$$

J'affirme que F est un endomorphisme du corps M (l'*endomorphisme de Frobenius*). Il est en effet clair que $F(0)=0$, $F(1)=1$, et que, pour tout $(a,b)\in M^2$

$$F(ab)=F(a)F(b)\ .$$

De plus

$$\begin{aligned}F(a+b)&=(a+b)^p\\ &=\sum_{k=0}^{p}\binom{p}{k}a^kb^{p-k}\\ &=a^p+b^p+\sum_{k=1}^{p-1}\binom{p}{k}a^kb^{p-k}\\ &=F(a)+F(b)+\sum_{k=1}^{p-1}\binom{p}{k}a^kb^{p-k}\ .\end{aligned}$$

Mais, pour $1\leq k\leq p-1$, p divise $p.(p-1)!=p!=k!(p-k)!\binom{p}{k}=1...k.1...(p-k).\binom{p}{k}$.

p étant premier, il ne divise aucun de 1,...,k,1,..., $p-k$, donc, en vertu du Lemme de Gauss, $p|\binom{p}{k}$ et

$$\forall y\in K\ \binom{p}{k}y=0\text{ (vu que }M\text{ est de caractéristique }p).$$

Il s'ensuit que

$$F(a+b)=(a+b)^p=F(a)+F(b)\ ,$$

et donc que F est un endomorphisme du corps M. Mais

$$\forall x \in M \ F^n(x) = x^{p^n} \ ;$$

L est donc l'ensemble des points fixes de l'endomorphisme F^n du corps M, donc est un sous–corps de M, et on a

$$|L| = p^n,$$

d'où l'existence d'un corps à p^n éléments (en fait, il apparaît que $L = M$). □

Nous aurons besoin d'un lemme de pure théorie des groupes.

Lemme 7.5. *Soit G un groupe fini d'ordre $|G| = n$ et d'élément neutre noté e, ayant la propriété que, pour chaque diviseur d de n, le nombre d'éléments x de G tels que $x^d = e$ soit au plus d. Alors G est cyclique.*

Proof. Pour $x \in G$, notons $\omega(x)$ l'ordre de x. Pour d diviseur de n, définissons

$$a_d = |\{x \in G | \omega(x) = d\}| \ .$$

Alors

$$\sum_{d|n} a_d = |G| = n \ .$$

Si $a_d \neq 0$, il existe un élément y de G tel que $\omega(y) = d$. Mais alors les y^k $(1 \leq k \leq d)$ sont deux à deux distincts et vérifient $(y^k)^d = y^{kd} = y^{dk} = (y^d)^k = e^k = e$, d'où

$$\{y^k | 1 \leq k \leq d\} \subset \{x \in G | x^d = e\} \ ,$$

et

$$d = |\{y^k | 1 \leq k \leq d\}| \leq |\{x \in G | x^d = e\}| \leq d \ .$$

Donc

$$\{y^k | 1 \leq k \leq d\} = \{x \in G | x^d = e\} \ .$$

En particulier, si l'élément x de G est d'ordre d, on a $x^d = e$ et il existe donc $k \in \{1, ..., d\}$ tel que $x = y^k$. Mais alors

$$\omega(x) = \omega(y^k) = \frac{\omega(y)}{\mathrm{pgcd}(\omega(\mathrm{y}), \mathrm{k})} = \frac{d}{\mathrm{pgcd}(\mathrm{d}, \mathrm{k})}$$

et la condition $\omega(x) = d$ équivaut à $\mathrm{pgcd}(\mathrm{d}, \mathrm{k}) = 1$; il y a donc $\phi(d)$ possibilités pour k.

Nous avons établi que, si $a_d \neq 0$, alors $a_d = \phi(d)$; en particulier, pour chaque d divisant n, $a_d \leq \phi(d)$. Mais

$$\sum_{d|n} a_d = n = \sum_{d|n} \phi(d) \ .$$

Il en résulte que, pour chaque d divisant n, $a_d = \phi(d)$; en particulier,

$$a_n = \phi(n) \neq 0.$$

G possède donc au moins un élément y d'ordre n. Le sous–groupe $< y >$ de G engendré par y est alors d'ordre $n = |G|$; de ce fait il coïncide avec G, lequel est donc cyclique. □

Corollaire 7.6. *Si K est un corps fini, le groupe multiplicatif $K \setminus \{0\}$ est cyclique*

Proof. Soit $G = K \setminus \{0\}$; pour chaque diviseur d de l'ordre $|G|$ de G, le polynôme $X^d - 1$ a au plus d racines dans K ; en particulier, le nombre de $x \in K$ avec $x^d = 1$ est au plus d. Le résultat suit alors du Lemme 7.5. □

Corollaire 7.7. *Le groupe multiplicatif* $\mathbf{F}_p \setminus \{0\}$ *est cyclique.*

Un entier a tel que $\overline{a}$ engendre $\mathbf{F}_p \setminus \{0\}$ est dit *racine primitive* modulo p.

Exemple 7.8. L'exemple suivant provient de l'article d'origine sur la théorie des corps finis (Galois [5]) ; il s'agit de la construction du corps $\mathbf{F}_{7^3}$ à $7^3 = 343$ éléments.

Il est très facile de voir que 2 n'est pas un cube dans $\mathbf{F}_7$; le polynôme

$$X^3 - 2 \in \mathbf{F}_7[X] \ ,$$

étant de degré 3 sur $\mathbf{F}_7$, est donc irréductible. Soit

$$K := \frac{\mathbf{F}_7[X]}{(X^3-2)\mathbf{F}_7[X]} \ .$$

Alors K est un corps de degré 3 sur $\mathbf{F}_7$, donc isomorphe à $\mathbf{F}_{7^3}$; nous l'y identifierons dorénavant. Soit $\alpha = \overline{X}$ la classe de X dans $\dfrac{\mathbf{F}_7[X]}{(X^3-2)\mathbf{F}_7[X]}$; alors $K = \mathbf{F}_7[\alpha]$.

On peut déterminer explicitement un générateur du groupe multiplicatif

$$K^* = K \setminus \{0\} :$$

de $\alpha^3 = 2$ suit que

$$\alpha^9 = (\alpha^3)^3 = 2^3 = 8 = 1$$

(nous travaillons présentement en caractéristique 7), et $\alpha^3 \neq 1$. Il en résulte que l'ordre de α dans K^* est $9 = 3^2$. L'ordre de -1 dans K^* est évidemment 2. De plus,

$$(\alpha-1)^7 = \alpha^7 - 1 = 4\alpha - 1$$

et

$$(\alpha-1)^{21} = ((\alpha-1)^7)^3 = (4\alpha-1)^3 = 64\alpha^3 - 48\alpha^2 + 12\alpha - 1 = \alpha^2 - 2\alpha + 1 = (\alpha-1)^2$$

d'où

$$(\alpha-1)^{19} = 1 \ .$$

Vu que $\alpha - 1 \neq 1$, $\alpha - 1$ est d'ordre 19. Les nombres 2, 9 et 19 étant premiers entre eux, il suit d'une propriété bien connue des groupes commutatifs finis que

$$j := \alpha(-1)(\alpha-1) = \alpha - \alpha^2$$

est d'ordre $9 \cdot 2 \cdot 19 = 342 = 7^3 - 1$, et j engendre donc le groupe multiplicatif

$$\mathbf{F}_{7^3} \setminus \{0\} \ .$$

En particulier

$$\mathbf{F}_{7^3} = \mathbf{F}_7[j] \ .$$

8. La structure du groupe des unités de $\frac{\mathbf{Z}}{n\mathbf{Z}}$.

Nous avons vu au cours de la démonstration du Théorème 3.7 que, pour m et n premiers entre eux,

$$U\left(\frac{\mathbf{Z}}{mn\mathbf{Z}}\right)$$

était isomorphe à

$$U\left(\frac{\mathbf{Z}}{m\mathbf{Z}}\right) \times U\left(\frac{\mathbf{Z}}{n\mathbf{Z}}\right).$$

On en déduit aisément que, si $n = n = p_1^{\alpha_1}...p_r^{\alpha_r}$, alors

$$U\left(\frac{\mathbf{Z}}{n\mathbf{Z}}\right)$$

est isomorphe à

$$\prod_{i=1}^{r} U\left(\frac{\mathbf{Z}}{p_i^{\alpha_i}\mathbf{Z}}\right).$$

Il suffit donc de déterminer la structure de $U\left(\frac{\mathbf{Z}}{p^k\mathbf{Z}}\right)$ (p premier, $k \geq 1$).

Celle-ci est donnée par le

Théorème 8.1. (1) *Si p est impair, $U\left(\frac{\mathbf{Z}}{p^k\mathbf{Z}}\right)$ est isomorphe à $\frac{\mathbf{Z}}{p^{k-1}(p-1)\mathbf{Z}}$ (en d'autres termes, il est cyclique).*

(2)

$$U\left(\frac{\mathbf{Z}}{2^k\mathbf{Z}}\right)$$

est d'ordre 1 si $k = 1$, est isomorphe à $\frac{\mathbf{Z}}{2\mathbf{Z}}$ si $k = 2$, et est isomorphe à $\frac{\mathbf{Z}}{2^{k-1}\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}$ si $k \geq 3$.

Démonstration. (1)

Le Corollaire 7.7 nous donne le résultat pour $k = 1$; nous supposerons donc dorénavant $k \geq 2$.

Soit $z = \overline{1+p}$; nous allons faire voir que l'ordre multiplicatif de z dans

$$U\left(\frac{\mathbf{Z}}{p^k\mathbf{Z}}\right)$$

est p^{k-1}.

A cette fin, établissons par récurrence sur l'entier $m \geq 0$ que

$$(1+p)^{p^m} \equiv 1 + p^{m+1}[p^{m+2}].$$

Cest évident pour $m = 0$; en fait, dans ce cas, les deux termes de la congruence sont égaux. Supposons le résultat établi au rang m ; on a donc

$$(1+p)^{p^m} = 1 + p^{m+1} + \lambda p^{m+2}$$

pour un $\lambda \in \mathbf{Z}$. Soit

$$x := p^{m+1} + \lambda p^{m+2};$$

alors

$$\begin{aligned}(1+p)^{p^{m+1}} &= ((1+p)^{p^m})^p \\ &= (1+x)^p \\ &= \sum_{k=0}^{n}\binom{p}{k}x^k \\ &= 1+px+\sum_{k=2}^{p-1}\binom{p}{k}x^k+x^p.\end{aligned}$$

Mais, pour chaque k avec $1 \leq k \leq p-1$, p divise $\binom{p}{k}$; donc, lorsque $2 \leq k \leq p-1$, px^2 divise $\binom{p}{k}x^k$; mais $x = p^{m+1}(1+\lambda p)$ est un multiple de p^{m+1} , donc

$$p(p^{m+1})^2 = p^{2m+3}$$

divise px^2, donc aussi $\binom{p}{k}x^k$; en particulier p^{m+3} divise $\binom{p}{k}x^k$. Quant au dernier terme x^p, il est divisible par x^3, donc par $(p^{m+1})^3 = p^{3m+3}$, *a fortiori* par p^{m+3}. On a donc

$$\begin{aligned}(1+p)^{p^{m+1}} &\equiv 1+px \\ &= 1+p(p^{m+1}+\lambda p^{m+2}) \\ &= 1+p^{m+2}+\lambda p^{m+3} \\ &\equiv 1+p^{m+2}\ [p^{m+3}],\end{aligned}$$

et le résultat au rang $m+1$ sensuit.

Prenant $m = k-1$, on trouve que

$$(1+p)^{p^{k-1}} \equiv 1+p^k\ [p^{k+1}],$$

d'où

$$(1+p)^{p^{k-1}} \equiv 1+p^k \equiv 1\ [p^k],$$

soit

$$(\bar{z})^{p^{k-1}} = \bar{1}.\ (*)$$

Prenant maintenant $m = k-2$, on trouve

$$(1+p)^{p^{k-2}} \equiv 1+p^{k-1}[p^k],$$

en particulier

$$(1+p)^{p^{k-2}} \equiv 1+p^{k-1} \not\equiv 1[p^k].\ (**)$$

Daprès $(*)$, lordre $\omega(z)$ de z divise p^{k-1} ; c'est donc une puissance de p : p^l avec $l \leq k-1$. Mais il suit de $(**)$ que l'ordre de z ne divise pas p^{k-2}. On a donc $\omega(z) = p^{k-1}$.

Soit

$$\begin{aligned}\varphi\ :\ \mathbf{U}\left(\frac{\mathbf{Z}}{p^k\mathbf{Z}}\right) &\to U\left(\frac{\mathbf{Z}}{p\mathbf{Z}}\right) \\ \pi_{p^k}(a) &\mapsto \pi_p(a)\ .\end{aligned}$$

Supposons $\pi_{p^k}(a) = \pi_{p^k}(b)$; alors p^k divise $a-b$, donc p divise $a-b$ et $\pi_p(a) = \pi_p(b)$; φ est donc bien défini.

Il est en outre clair que

$$\varphi(\pi_{p^k}(a)\pi_{p^k}(b)) = \varphi(\pi_{p^k}(ab)) = \pi_p(ab) = \pi_p(a)\pi_p(b) = \varphi(\pi_{p^k}(a))\varphi(\pi_{p^k}(b)),$$

donc φ est un morphisme de groupes.

On peut aussi remarquer que φ n'est autre que la restriction au groupe des éléments inversibles de $U\left(\frac{\mathbf{Z}}{p^k\mathbf{Z}}\right)$ du morphisme naturel d'anneaux unitaires de $\frac{\mathbf{Z}}{p^k\mathbf{Z}}$ dans $\frac{\mathbf{Z}}{p\mathbf{Z}}$; à ce titre il est bien défini, c'est un morphisme de groupes, et son image est contenue dans $U\left(\frac{\mathbf{Z}}{p\mathbf{Z}}\right)$.

Soit $x \in U\left(\frac{\mathbf{Z}}{p\mathbf{Z}}\right)$; alors $x = \pi_p(a)$ pour un a premier avec p. Mais alors a est premier avec p^k, donc $\pi_{p^k}(a) \in U\left(\frac{\mathbf{Z}}{p^k\mathbf{Z}}\right)$ et

$$\varphi(\pi_{p^k}(a)) = \pi_p(a) = x$$

donc φ est surjectif.

On a vu (Corollaire 7.7) que $U\left(\frac{\mathbf{Z}}{p\mathbf{Z}}\right)$ est cyclique ; il contient donc un élément y d'ordre $p-1$. φ étant surjectif, il existe $x \in U\left(\frac{\mathbf{Z}}{p^k\mathbf{Z}}\right)$ tel que $\varphi(x) = y$; mais alors

$$p-1 = \omega(y) = \omega(\varphi(x))$$

divise $\omega(x)$: $\omega(x) = (p-1)k$ (k entier).

On a donc

$$\begin{aligned}\omega(x^k) &= \frac{\omega(x)}{pgcd(\omega(x),k)}\\ &= \frac{(p-1)k}{pgcd((p-1)k,k)}\\ &= \frac{(p-1)k}{k}\\ &= p-1.\end{aligned}$$

Vu que p^{k-1} et $p-1$ sont premiers entre eux, il résulte d'une propriété bien connue des groupes abéliens que l'élément $u := zx^k$ est d'ordre $p^{k-1}(p-1)$. Mais

$$|U\left(\frac{\mathbf{Z}}{p^k\mathbf{Z}}\right)| = \phi(p^k) = p^{k-1}(p-1),$$

donc u engendre $U\left(\frac{\mathbf{Z}}{p^k\mathbf{Z}}\right)$: $U\left(\frac{\mathbf{Z}}{p^k\mathbf{Z}}\right)$ est cyclique.

(2)

Le résultat est clair pour $k \in \{1,2,3\}$. Soit donc $k \geq 4$; la première partie du raisonnement sera assez semblable à la démonstration de (1) : nous ferons voir que l'ordre multiplicatif de la classe $\bar{5}$ de 5 dans

$$U\left(\frac{\mathbf{Z}}{2^k\mathbf{Z}}\right)$$

est 2^{k-2}.

A cette fin, établissons par récurrence sur l'entier $m \geq 0$ que

$$5^{2^m} \equiv 1 + 2^{m+2}[2^{m+3}].$$

Cest évident pour $m = 0$; en fait, dans ce cas, les deux termes de la congruence sont égaux. Supposons le résultat établi au rang m ; on a donc

$$5^{2^m} = 1 + 2^{m+2} + \lambda 2^{m+3}$$

pour un $\lambda \in \mathbf{Z}$. Soit

$$x := 2^{m+2} + \lambda 2^{m+3};$$

alors

$$\begin{aligned} 5^{2^{m+1}} &= (5^{2^m})^2 \\ &= (1+x)^2 \\ &= 1 + 2x + x^2 \end{aligned}$$

Mais 2^{m+2} divise x, donc 2^{2m+4} divise x^2, à plus forte raison 2^{m+4} divise x^2 ; et $2x = 2^{m+3} + \lambda 2^{m+4} \equiv 2^{m+3}[2^{m+4}]$. On a donc

$$\begin{aligned} 5^{2^{m+1}} &= 1 + 2x + x^2 \\ &\equiv 1 + 2^{m+3}[2^{m+4}], \end{aligned}$$

et le résultat au rang $m+1$ s'ensuit.

Prenant $m = k-2$, on trouve que

$$5^{2^{k-2}} \equiv 1 + 2^k[2^{k+1}]$$

d'où

$$5^{2^{k-2}} \equiv 1 + 2^k[2^k]$$

et

$$5^{2^{k-2}} \equiv 1[2^k]$$

soit

$$(\bar{5})^{2^{k-2}} = \bar{1}. \ (***)$$

Prenant maintenant $m = k-3$, on trouve

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \not\equiv 1[2^k],$$

soit

$$(\bar{5})^{2^{k-3}} \neq \bar{1}. \ (****)$$

Daprs $(***)$, l'ordre $\omega(\bar{5})$ de $\bar{5}$ divise 2^{k-2} : cest donc une puissance 2^l avec $l \leq k-2$; mais il suit de $(****)$ que l'ordre de $\bar{5}$ ne divise pas 2^{k-3}. On a donc $\omega(\bar{5}) = 2^{k-2}$.

Le sous–groupe $< -\bar{1} >= \{\bar{1}, -\bar{1}\}$ est évidemment d'ordre 2.

Or le groupe $< \bar{5} >$, car cyclique, contient un unique sous–groupe d'ordre 2, donc un unique élément d'ordre 2 : $(\bar{5})^{2^{k-3}}$. Mais l'on vient de voir que

$$5^{2^{k-3}} \equiv 1 + 2^{k-1}[2^k]$$

donc

$$5^{2^{k-3}} \not\equiv -\bar{1}[2^k]$$

et

$$(\bar{5})^{2^{k-3}} \neq -\bar{1}$$

Il en résulte que

$$< \bar{5} > \cap < -\bar{1} >= \{\bar{1}\}$$

donc les sous–groupes $< \bar{5} >$ et $< -\bar{1} >$ engendrent un produit direct

$$< \bar{5} > \times < -\bar{1} > \simeq \frac{\mathbf{Z}}{2^{k-2}\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}.$$

Mais ce groupe est d'ordre $2^{k-2}.2 = 2^{k-1}$, donc coïncide avec $U\left(\frac{\mathbf{Z}}{2^k\mathbf{Z}}\right)$ et le résultat s'ensuit. □

Exercice 8.2. $U\left(\frac{\mathbf{Z}}{n\mathbf{Z}}\right)$ est cyclique si et seulement si n vaut 1, 2, 4, p^k (p premier impair, $k \geq 1$) ou $2p^k$ (p premier impair, $k \geq 1$).

9. Les Sommes de Gauss

Nous allons faire voir comment les concepts du paragraphe précédent permettent de donner une autre démonstration de la loi de réciprocité quadratique.

Commençons par redémontrer la *formule complémentaire* (Théorème 5.5). Soit K un corps de décomposition de X^8-1 sur $\mathbf{F}_p$; dans K, soit ζ une racine primitive 8–ième de l'unité, *i.e.* une racine de X^8-1 non racine de X^4-1. Alors $\zeta^4=-1$. Posons $G=\zeta+\zeta^{-1}$; alors

$$G^2=\zeta^2+\zeta^{-2}+2=2\ ;$$

en particulier, $G\neq 0$. De plus

$$(\frac{2}{p})=2^{\frac{p-1}{2}}=(G^2)^{\frac{p-1}{2}}=G^{p-1}\ .$$

En outre,

$$G^p=(\zeta+\zeta^{-1})^p=\zeta^p+\zeta^{-p}\ .$$

Si $p\equiv 1$ ou $7[8]$, $\zeta^p=\zeta$ ou ζ^{-1}, donc $G^p=G$ et $G^{p-1}=1$, d'où $(\frac{2}{p})=1$.

Si $p\equiv 3$ ou $5[8]$, $\zeta^p=\zeta^3=-\zeta^{-1}$ ou $\zeta^p=\zeta^{-3}=-\zeta$, donc $G^p=-G$, d'où $G^{p-1}=-1$ et $(\frac{2}{p})=-1$. On retrouve bien le résultat du §5.

Passons maintenant à la loi de réciprocité quadratique elle-même (Théorème 5.4).

Soient donc p et q deux nombres premiers impairs, distincts, et soit L un corps de décomposition de X^p-1 sur $\mathbf{F}_q$.

Soit alors $\zeta\in L$ avec $\zeta^p=1$ et $\zeta\neq 1$. Il apparaît que ζ^n ne dépend que de la classe $\overline{n}$ de n modulo p ; par abus de langage, nous noterons donc, pour $n\in\mathbf{Z}$, $\zeta^{\overline{n}}=\zeta^n$. De même, pour $n\in\mathbf{Z}$ non divisible par p, nous noterons

$$(\frac{\overline{n}}{p}):=(\frac{n}{p}).$$

Définissons la *Somme de Gauss*

$$G=\sum_{x\in{\mathbf{F}_p}^*}(\frac{x}{p})\zeta^x\in L\ ,$$

et procédons maintenant à un calcul dans L :

$$\begin{aligned}
G^2 &= \sum_{x\in{\mathbf{F}_p}^*}\sum_{y\in{\mathbf{F}_p}^*}(\frac{x}{p})\zeta^x(\frac{y}{p})\zeta^y\\
&= \sum_{x\in{\mathbf{F}_p}^*}\sum_{y\in{\mathbf{F}_p}^*}(\frac{xy}{p})\zeta^{x+y}(\text{d'après la Proposition 5.2})\\
&= \sum_{x\in{\mathbf{F}_p}^*}\sum_{z\in{\mathbf{F}_p}^*}(\frac{x^2z}{p})\zeta^{x(1+z)}(\text{on a posé } y=xz)\\
&= \sum_{z\in{\mathbf{F}_p}^*}(\frac{z}{p})(\sum_{x=0}^{p-1}(\zeta^{(1+z)})^x-1)\\
&= -\sum_{z\in{\mathbf{F}_p}^*}(\frac{z}{p})+\sum_{z\in{\mathbf{F}_p}^*}(\frac{z}{p})(\sum_{x=0}^{p-1}(\zeta^{(1+z)})^x)\ .
\end{aligned}$$

Mais

$$\sum_{x=0}^{p-1}(\zeta^{(1+z)})^x$$

vaut p si $\zeta^{1+z}=1$, et $\dfrac{(\zeta^{1+z})^p-1}{\zeta^{1+z}-1}=0$ sinon (car $\zeta^p=1$); or $\zeta^{1+z}=1$ si et seulement si $1+z=0$ dans $\mathbf{F}_p$, soit $z=-\bar{1}$. Par ailleurs, $\sum_{z\in{\mathbf{F}_p}^*}(\dfrac{z}{p})=0$ car il y a dans ${\mathbf{F}_p}^*$ autant de résidus quadratiques que de non–résidus (cf. §5). On a donc

$$G^2=p(\frac{-1}{p})=p(-1)^{\frac{p-1}{2}}\ ;$$

en particulier, $G\neq 0$.

Soit $\overline{r}$ l'inverse de $\overline{q}$ dans $\dfrac{\mathbf{Z}}{p\mathbf{Z}}$; on a

$$\begin{aligned}
G^q &= \sum_{x\in{\mathbf{F}_p}^*}(\frac{x}{p})^q\zeta^{xq}\\
&= \sum_{x\in{\mathbf{F}_p}^*}(\frac{x}{p})\zeta^{xq}\\
&= \sum_{x\in{\mathbf{F}_p}^*}(\frac{x}{p})\zeta^{x\bar{q}}\\
&= \sum_{y\in{\mathbf{F}_p}^*}(\frac{\bar{r}y}{p})\zeta^{\bar{q}\bar{r}y}(\text{on a posé } x=\bar{r}y)\\
&= (\frac{r}{p})\sum_{y\in{\mathbf{F}_p}^*}(\frac{y}{p})\zeta^{y}\\
&= (\frac{r}{p})G\\
&= (\frac{q}{p})G\ .
\end{aligned}$$

Du fait que $G\neq 0$, il vient

$$G^{q-1}=(\frac{q}{p})\ .$$

Mais alors

$$\begin{aligned}
(\frac{q}{p}) &= G^{q-1}\\
&= (G^2)^{\frac{q-1}{2}}\\
&= (p(-1)^{\frac{p-1}{2}})^{\frac{q-1}{2}}\\
&= (p^{\frac{q-1}{2}})(-1)^{\frac{(p-1)(q-1)}{4}}\\
&= (\frac{p}{q})(-1)^{\frac{(p-1)(q-1)}{4}}.
\end{aligned}$$

Vu que $(\dfrac{p}{q})(\dfrac{q}{p})\in\{-1,1\}$, on obtient le résultat. □

References

[1] M. Aigner and G.M.Ziegler *Proofs from The Book*, Springer-Verlag, 1999.

[2] Claude-Gaspar Bachet, Sieur de Méziriac *Problèmes plaisants et délectables qui se font par les nombres*, Albert Blanchard, Paris, 1959.

[3] R. D. Carmichael *On Euler's ϕ–function*, Bull. Amer. Math. Soc. 13, 1907, pp. 241–243.

[4] R. D. Carmichael *Note on Euler's ϕ–function*, Bull. Amer. Math. Soc. 28, 1922, pp. 109–110.

[5] E. Galois *Sur la théorie des nombres*, Bulletin des Sciences Mathématiques de Férussac, XIII, §218 (Juin 1830), repris dans *Ecrits et Mémoires Mathématiques* (éd. R. Bourgne et J.–P. Azra), Gabay, Paris, 1997, pp. 113–127.

[6] R. L. Rivest, A. Shamir, L. Adleman *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM 21(2), 1978, pp. 120–126.

[7] T. J. Stieltjes *Sur le caractère quadratique du nombre* 2, Annales de la faculté des sciences de Toulouse 1re série, tome 11, n^o1(1897), pp. A5-A8.

[8] D. Zagier *A one–sentence proof that every prime $p \equiv 1[4]$ is a sum of two squares*, American Mathematical Monthly 97(2), 1990, p.144.