AUTOUR DES NOMBRES PREMIERS

par

Julien Roques

Résumé. — Notes de cours autour des nombres premiers. Attention, notes fraiches (et travail en cours d'ailleurs). Des erreurs se sont sans doute glissées ici et là, ne pas hésiter à me les signaler.

Table des matières

1. L'anneau $\mathbb{Z}/n\mathbb{Z}$: rappels 2
2. Loi de récprocité quadratique 4
   2.1. Propriétés élémentaires des carrés de $\mathbb{F}_p$ 5
   2.2. Symbole de Legendre 5
   2.3. Loi de réciprocité quadratique 6
   2.4. Lois complémentaires 8
   2.5. Symbole de Jacobi 8
   2.6. Algorithme pour le calcul du symbole de Jacobi 9
   2.7. Une application aux entiers qui sont des résidus quadratiques pour presque tout nombre premier 9
3. Répartition des nombres premiers 10
   3.1. La série des inverse des nombres premiers 10
   3.2. Postulat de Bertrand 12
   3.3. Théorème des nombres premiers 12
   3.4. Théorème de la progression arithmétique 13
4. Gren-Tao : pour la culture 15
5. Une formule pour les nombres premiers ? 15
6. Primalité : soyons concrets 15
   6.1. Méthode naïve 16
   6.2. Application directe du petit théorème de Fermat 16
   6.3. Miller-Rabin 19

6.4. Solovay Strassen 20
6.5. Miller-Rabin vs Solovay-Strassen 21
6.6. Critères de primalité lorsque les facteurs premiers de $n-1$ ou $n+1$ sont connus 21
6.6.1. Critère de Lehmer. Nombres de Fermat 21
6.6.2. Suites de Lucas. Nombres de Mersenne 23
7. Leçon sur les nombres premiers 25
8. Quelques résultats supplémentaires 27
Références 28

1. L'anneau $\mathbb{Z}/n\mathbb{Z}$: rappels

Les références pour les résultats rappelés dans ce § sont si nombreuses que je n'en donne aucune : choisissez votre cours d'algèbre préféré.

Pour tout entier $n \geq 1$, on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe abélien fini formé par les inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. En utilisant le théorème de Bézout, on montre que

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{m \mod n \mid m \in [[0, n-1]], \mathrm{pgcd}(m,n) = 1\}. \tag{1}$$

L'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est noté $\varphi(n)$. La formule (1) montre que

$$\varphi(n) = \sharp\{m \in [[0, n-1]] \mid \mathrm{pgcd}(m,n) = 1\}.$$

L'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est appelée indicatrice d'Euler. Il s'agit d'une fonction arithmétique multiplicative i.e.

$$\forall m, n \in \mathbb{N}^*, \mathrm{pgcd}(m,n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n).$$

Cela résulte par exemple du fait que l'isomorphisme d'anneaux

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

donné par le théorème des restes chinois induit un isomorphisme de groupes

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Par ailleurs, si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de n alors

$$\begin{aligned} \varphi(n) &= p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1) \\ &= n \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

Compte tenu de la multiplicativité de φ, pour justifier cette formule, il suffit de montrer que $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ pour tout nombre premier p et tout entier $\alpha \geq 1$. Montrer cela revient à montrer que le nombre d'entiers $m \in [[0, p^\alpha - 1]]$

non premiers avec p^α, c'est-à-dire divisibles par p, est égal à $p^{\alpha-1}$, ce qui est évident.

Le théorème de Lagrange implique que

$$\forall a \in \mathbb{Z}, \mathrm{pgcd}(a,n) = 1 \Rightarrow a^{\varphi(n)} = 1 \mod n;$$

dans le cas particulier où $n = p$ est un nombre premier, on obtient le petit théorème de Fermat :

$$\forall a \in \mathbb{Z}, p \not| a \Rightarrow a^{p-1} = 1 \mod p$$

et donc

$$\forall a \in \mathbb{Z}, a^p = a \mod p.$$

Il résulte par exemple de (1) que :

Proposition 1. — *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

Pour tout nombre premier p, on notera $\mathbb{F}_p$ le corps fini $\mathbb{Z}/p\mathbb{Z}$. Le groupe $\mathbb{F}_p^\times$ est cyclique. Cette assertion est un cas particulier du :

Théorème 2. — *Pour tout corps fini K, le groupe $K^\times = K\backslash\{0\}$ est cyclique.*

Avant de prouver ce théorème, une digression sur la notion d'exposant est utile.

Définition 3. — *L'exposant d'un groupe fini G, noté $\omega(G)$, est le ppcm des ordres des éléments de G.*

Le théorème de Lagrange montre que :

Proposition 4. — *L'exposant $\omega(G)$ de tout groupe fini G divise l'ordre de G.*

Proposition 5. — *Tout groupe abélien fini G possède un élément d'ordre $\omega(G)$.*

Démonstration. — On considère la décomposition $\omega(G) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ de $\omega(G)$ en facteurs premiers. Pour tout $i \in [[1,r]]$, il existe un élément h_i de G dont l'ordre est divisible par $p_i^{\alpha_i}$. Alors $g_i := h_i^{o(h_i)/p_i^{\alpha_i}}$ est d'ordre $p_i^{\alpha_i}$. Puisque $g_1, ..., g_r$ commutent entre eux et que leurs ordres sont premiers entre eux deux à deux, l'élément $g = g_1 \cdots g_r$ de G est d'ordre $o(g_1) \cdots o(g_r) = \omega(G)$. □

Nous sommes à présent en mesure de prouver le théorème.

Preuve du Théorème 2. — Soit q le cardinal de K. Notons $\omega = \omega(K^\times)$. Il résulte de la définission de ω que le polynôme $X^{\omega+1} - X \in K[X]$ s'annule sur K. Donc $\omega + 1 = \deg X^{\omega+1} - X \geq \sharp K = q$. Puisque ω divise $|K^\times| = q - 1$, on en déduit que $\omega = q - 1$. Le résultat est maintenant une conséquence de la Proposition 5. □

Intéressons-nous de plus près au groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. Considérons la décomposition $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ de n en facteurs premiers. L'isomorphisme d'anneaux

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$$

donné par le théorème des restes chinois induit un isomorphisme de groupes

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times.$$

Le résultat suivant permet de décomposer $(\mathbb{Z}/n\mathbb{Z})^\times$ en un produit de groupes cycliques.

Proposition 6. — *Soient p un nombre premier et $\alpha \in \mathbb{N}^*$.*
i) Si p est impair alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.
ii) Si $p = 2$ et $\alpha \geq 2$ alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times = (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. De plus, $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$.

Démonstration. — Nous traitons seulement le cas p impair.

Il suffit de démontrer que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ possède des éléments a et b d'ordres respectifs $p-1$ et $p^{\alpha-1}$. En effet, puisque a et b commutent et que leurs ordres sont premiers entre eux, leur produit est d'ordre $o(a)o(b) = p^{\alpha-1}(p-1) = |(\mathbb{Z}/p^\alpha\mathbb{Z})^\times|$ et est donc un générateur de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

Notons que $a = 1 + p \mod p^\alpha$ est un élément d'ordre $p^{\alpha-1}$ de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Cela résulte du fait (dont nous laissons la preuve par récurrence au lecteur) que, pour tout $k \in \mathbb{N}$, il existe $\lambda_k \in \mathbb{N}^*$ premier avec p tel que $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$.

Par ailleurs, on note $u : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ le morphisme de groupes surjectif défini par $u(m \mod p^\alpha) = m \mod p$. Puisque $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, il possède un élément y d'ordre $p-1$. Soit $x \in u^{-1}(y)$. Il est clair que l'ordre de x est divisible par $p-1$. Alors $b = x^{o(x)/(p-1)}$ est d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. □

2. Loi de récprocité quadratique

Définition 7. — *On dit que $a \in \mathbb{Z}$ est un résidu quadratique modulo $n \in \mathbb{N}^*$ si $a \mod n$ est un carré de $\mathbb{Z}/n\mathbb{Z}$.*

La loi de réciprocité quadratique lie les prioriétés "p est un résidu quadratique modulo q" et "q est un résidu quadratique modulo p" pour des nombres premiers impairs p et q. Avant de l'énoncer, nous donnons des propriétés élémentaires des carrés dans les corps finis $\mathbb{F}_p$ et introduisons le symbole de Legendre.

Références : carrés des corps finis : [**Per**] ; carrés des corps finis, symbole de Legendre, loi de réciprocité quadratique, symbole de Jacobi : [**Dem, Zis**].

2.1. Propriétés élémentaires des carrés de $\mathbb{F}_p$. — On considère un nombre premier impair p. Nous nous intéressons ici aux carrés du corps fini $\mathbb{F}_p$. On pourrait sans difficulté étendre notre étude aux carrés des corps finis arbitraires.

Proposition 8. — *Il y a autant de carrés que de non carrés dans $\mathbb{F}_p^\times$, à savoir $\frac{p-1}{2}$.*

Démonstration. — Cela résulte du fait que l'endomorphisme de groupes ψ de $\mathbb{F}_p^\times$ défini par $\psi(x) = x^2$ a pour noyau $\{\pm 1\}$ et induit donc un isomorphisme de groupes entre le groupe quotient $\mathbb{F}_p^\times/\{\pm 1\}$ et le sous-groupe de $\mathbb{F}_p^\times$ formé des carrés. □

Proposition 9. — *On a :*

i) Un élément de x de $\mathbb{F}_p^\times$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.

ii) Un élément de x de $\mathbb{F}_p^\times$ n'est pas un carré si et seulement si $x^{\frac{p-1}{2}} = -1$.

Démonstration. — Chaque carré de $\mathbb{F}_p^\times$ est racine de $X^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[X]$ (d'après le théorème de Lagrange). Les carrés de $\mathbb{F}_p^\times$ étant au nombre de $\frac{p-1}{2}$, il s'en suit que

$$X^{\frac{p-1}{2}} - 1 = \prod_{\substack{x \in \mathbb{F}_p^\times \\ x \text{ carré}}} (X - x).$$

D'où la première assertion. La seconde en résulte compte tenu de ce que :

$$\prod_{x \in \mathbb{F}_p} (X - x) = X^p - X = X(X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1).$$

□

2.2. Symbole de Legendre. — On considère un nombre premier impair p. Pour tout entier relatif n, le symbole de Legendre $\left(\frac{n}{p}\right)$ est défini par

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ si } n \text{ est divisible par } p\,; \\ 1 \text{ si } n \text{ est un résidu quadratique modulo } p, \text{ non divisible par } p\,; \\ \text{-1 si } n \text{ n'est pas un résidu quadratique modulo } p. \end{cases}$$

La Proposition 9 se reformule de la manière suivante :

***Proposition 10* (Formule d'Euler)**. — *Pour tout entier relatif n,*

$$\left(\frac{n}{p}\right) = n^{\frac{p-1}{2}} \mod p.$$

On en déduit :

Proposition 11. — *Pour $m, n \in \mathbb{Z}$,*

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right).$$

On peut naturellement définir un symbole de Legendre $\left(\frac{\cdot}{p}\right)$ sur $\mathbb{F}_p$ de telle sorte que

$$\left(\frac{n \mod p}{p}\right) = \left(\frac{n}{p}\right).$$

La Proposition 11 montre qu'il induit un caractère de $\mathbb{F}_p^\times$. On pourra démontrer à titre d'exercice qu'il s'agit de l'unique caractère de $\mathbb{F}_p^\times$ d'ordre 2.

Remarque 12. — *Froebenuis-Zolotarev.*

2.3. Loi de réciprocité quadratique. —

***Théorème 13* (Loi de réciprocité quadratique)**. — *Soient p et q des nombres premiers impairs. On a*

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

Il existe d'innombrables démonstrations de ce théorème. Voici les grandes lignes d'une preuve classique reposant sur les sommes de Gauss que l'on trouvera par exemple dans [**Dem**]. D'autres démonstrations sont données dans [**Zis**, Chapitre 4].

Démonstration. — On suppose $p \neq q$ (le cas $p = q$ étant trivial). Notons que

$$(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right) = \epsilon(q)^{\frac{(p-1)}{2}} q^{\frac{(p-1)}{2}} = (\epsilon(q)q)^{\frac{p-1}{2}} \mod p$$

où $\epsilon(q) = (-1)^{\frac{q-1}{2}} = \left(\frac{-1}{q}\right)$. Ainsi, si τ est une racine carrée de $\epsilon(q)q \mod p$ dans une extension K de $\mathbb{F}_p$ alors

$$(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right) = \tau^{p-1}$$

et tout revient à vérifier que $\tau^{p-1} = \left(\frac{p}{q}\right)$ i.e.

$$\tau^p = \left(\frac{p}{q}\right)\tau. \tag{2}$$

Le point clé de la démonstration est la construction "explicite" de τ comme la somme de Gauss suivante :

$$\tau = \sum_{k=0}^{q-1}\left(\frac{k}{q}\right)\alpha^k = \sum_{x \in \mathbb{F}_q}\left(\frac{x}{q}\right)\alpha^x$$

où $\alpha \neq 1$ est une racine $q$ème de l'unité dans une extension de $\mathbb{F}_p$. Nous avons utilisé la notation $\alpha^{k \mod q} = \alpha^k$ qui est légitime puique $\alpha^q = 1$.

La validité de la formule (2) pour cette somme de Gauss ne présente pas de difficulté :

$$\left(\frac{p}{q}\right)\tau^p = \left(\frac{p}{q}\right)\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)^p \alpha^{px} = \left(\frac{p}{q}\right)\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\alpha^{px}$$
$$= \sum_{x\in\mathbb{F}_q}\left(\frac{px}{q}\right)\alpha^{px} = \sum_{y\in\mathbb{F}_q}\left(\frac{y}{q}\right)\alpha^{y} = \tau$$

où la première égalité résulte du fait qu'on travaille en caractéristique p et la dernière du fait que $x \mapsto px$ est une bijection de $\mathbb{F}_q$.

Il reste donc à vérifier que τ est une racine carrée de $\epsilon(q)q$. On a

$$\epsilon(q)\tau^2 = \sum_{x,y\in\mathbb{F}_q}\left(\frac{-xy}{q}\right)\alpha^{x+y} = \sum_{z\in\mathbb{F}_q} s_z\alpha^z$$

où, pour tout $z \in \mathbb{F}_q$,

$$s_z = \sum_{x\in\mathbb{F}_q^\times}\left(\frac{x(x-z)}{q}\right).$$

Or,

$$s_0 = \sum_{x\in\mathbb{F}_q^\times}\left(\frac{x^2}{q}\right) = \sum_{x\in\mathbb{F}_q^\times}\left(\frac{x}{q}\right)^2 = q-1.$$

De plus, pour $z \in \mathbb{F}_q^\times$, on a

$$s_z = \sum_{x\in\mathbb{F}_q^\times}\left(\frac{x^2(1-zx^{-1})}{q}\right) = \sum_{x\in\mathbb{F}_q^\times}\left(\frac{1-zx^{-1}}{q}\right) = \sum_{y\in\mathbb{F}_q\setminus\{1\}}\left(\frac{y}{q}\right) = -1,$$

l'avant-dernière égalité résultant du fait que l'application $\mathbb{F}_q^\times \to \mathbb{F}_q \setminus \{1\}$, $x \mapsto 1 - xz^{-1}$ est bijective et la dernière du fait que

$$\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right) = 0$$

car il y a autant de carrés non nuls que de non carrés dans $\mathbb{F}_p$. Il s'ensuit que

$$\epsilon(q)\tau^2 = (q-1) - \alpha - \cdots - \alpha^{q-1} = (q-1) + 1 = q$$

comme attendu. □

2.4. Lois complémentaires. — On considère un nombre premier impair p.

Proposition 14. — *On a*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ et } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

En d'autres termes, -1 *est un résidu quadratique modulo* p *si et seulement si* $p = 1 \mod 4$ *et* 2 *est un résidu quadratique modulo* p *si et seulement* $p = \pm 1 \mod 8$.

Démonstration. — La première formule est un cas particulier de la formule d'Euler.

La démonstration de la seconde formule est une légère variante de celle de la loi de réciprocité quadratique donnée plus haut (on va construire une racine carrée de 2 modulo p à partir d'une racine primitive 8ème de l'unité dans une extension de $\mathbb{F}_p$). On considère un corps de rupture K de $X^4+1 \in \mathbb{F}_p[X]$ et un racine α de X^4+1 dans K. Alors $\tau = \alpha + \alpha^{-1}$ est une racine carrée dans K de $2 \mod p$ ($\tau^2 = \alpha^2 + \alpha^{-2} + 2 = \alpha^{-2}(\alpha^4+1)+2 = 2$). Ainsi $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = \tau^p/\tau$. Puisque K est de caractéristique p, $\tau^p = \alpha^p + \alpha^{-p}$ d'où l'on déduit aisément que $\tau^p = \tau$ si $p = 1$ ou $7 \mod 8$ et que $\tau^p = -\tau$ si $p = 3$ ou $5 \mod 8$. □

2.5. Symbole de Jacobi. — Pour tout entier relatif n et tout entier naturel impair $m \geq 3$, le symbole de Jacobi $\left(\frac{n}{m}\right)$ est défini par

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)^{\alpha_1} \cdots \left(\frac{n}{p_r}\right)^{\alpha_r} \in \{0, \pm 1\}$$

où $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est la décomposition de m en facteurs premiers.

Il est immédiat que :

i) $\left(\frac{n}{m}\right) = 0$ si et seulement si $\text{pgcd}(m, n) \neq 1$;

ii) si $\left(\frac{n}{m}\right) = -1$ alors m n'est pas un résidu quadratique modulo l'un des facteurs premiers de m (et donc pas non plus modulo m) ;

iii) $\left(\frac{n}{m}\right)$ ne dépend que de la classe de n modulo m.

Attention, l'implication réciproque à ii) est en général fausse. En effet, il se peut que $\left(\frac{n}{m}\right) = 1$ alors que n n'est pas un résidu quadratique modulo m ; par exemple, $\left(\frac{-1}{3^2}\right) = \left(\frac{-1}{3}\right)^2 = 1$ mais -1 n'est pas un résidu quadratique modulo 3 donc pas non plus modulo 3^2.

La formule d'Euler ne s'étend en général pas non plus au symbole de Jacobi [1]. En effet, $\left(\frac{2}{3^2}\right) = \left(\frac{2}{3}\right)^2 = 1 \neq 7 = 2^{\frac{3^2-1}{2}} \mod 3^2$.

1. Ceci peut être précisé et est à l'origine du test de primalité de Solovay Strassen ; voir § 6.4.

Il résulte de la définission du symbole de Jacobi que, si n est un entier relatif et si $m, m' \geq 3$ sont des entiers impairs, alors :

$$\left(\frac{n}{mm'}\right) = \left(\frac{n}{m}\right)\left(\frac{n}{m'}\right).$$

La Proposition 11 montre la :

Proposition 15. — *Si n, n' sont des entiers relatifs et si $m \geq 3$ est un entier impair, alors :*

$$\left(\frac{nn'}{m}\right) = \left(\frac{n}{m}\right)\left(\frac{n'}{m}\right).$$

Enfin, la loi de réciprocité quadratique et les lois complémentaires conduisent au résultat suivant :

Théorème 16. — *Si $n, m \geq 3$ sont des entiers impairs, alors :*

$$\left(\frac{n}{m}\right) = (-1)^{\frac{(n-1)(m-1)}{4}}\left(\frac{m}{n}\right).$$

De plus,

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} \text{ et } \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$

2.6. Algorithme pour le calcul du symbole de Jacobi. — Le Théorème 16 conduit à un algorithme pour le calcul du symbole de Jacobi. Voir par exemple [**Dem**] (ou, mieux, le faire en exercice).

2.7. Une application aux entiers qui sont des résidus quadratiques pour presque tout nombre premier. —

Proposition 17. — *Supposons qu'un entier relatif n est un résidu quadratique modulo p pour presque tout nombre premier p* [2]*. Alors n est un carré dans $\mathbb{Z}$.*

Démonstration. — Raisonnons par l'absurde : supposons qu'il existe un entier relatif n qui est un résidu quadratique modulo presque tout nombre premier mais qui n'est pas un carré dans $\mathbb{Z}$.

Soit m l'unique diviseur de n sans facteur carré tel que n/m est un carré. Il est clair que m est un résidu quadratique modulo presque tout nombre premier mais n'est pas un carré dans $\mathbb{Z}$. Soient $q_1, ..., q_s$ les nombres premiers modulo lesquels m n'est pas un résidu quadratique.

Pour aboutir à une contradiction, on va montrer que m n'est pas un résidu quadratique modulo un certain nombre premier distinct de $q_1, ..., q_s$.

2. "pour presque tout nombre premier" signifie "pour tout nombre premier sauf peut-être un nombre fini".

On traite directement les cas $m = -1, \pm 2$ à l'aide des lois complémentaires (elles montrent que m n'est pas un résidu quadratique modulo une infinité de nombres premiers).

On suppose à présent $m \neq -1, \pm 2$. On décompose m sous la forme $m = p_0 p_1 \cdots p_r$ où $p_0 \in \{\pm 1, \pm 2\}$ et $p_1, ..., p_r$ sont des nombres premiers impairs. On a $r \geq 1$. Pour aboutir à la contradiction annoncée plus haut, il suffit de montrer qu'il existe un entier impair $\kappa \geq 3$ premier avec $q_1, ..., q_s$ tel que $\left(\frac{m}{\kappa}\right) = -1$. Considérons à cette fin un entier (nécessairement impair) $\kappa \geq 3$ tel que $\kappa = 1 \mod 8 \frac{m}{p_0 p_r} q_1 \cdots q_s$ et $\kappa = u \mod p_r$ (son existence est garantie par le théorème des restes chinois) où u est un entier tel que $\left(\frac{u}{p_r}\right) = -1$. On a $\left(\frac{m}{\kappa}\right) = \left(\frac{p_0}{\kappa}\right)\left(\frac{p_1}{\kappa}\right) \cdots \left(\frac{p_r}{\kappa}\right)$. Or, d'une part, $\left(\frac{p_0}{\kappa}\right) = 1$ (appliquer la deuxième partie du Théorème 16 en exploitant le fait que $\kappa = 1 \mod 8$). D'autre part, pour tout $i \in \{1, ..., r\}$, $\left(\frac{p_i}{\kappa}\right) = \left(\frac{\kappa}{p_i}\right)$ (car $\kappa = 1 \mod 8$) ; ainsi, pour tout $i \in \{1, ..., r\} \setminus \{r\}$, $\left(\frac{p_i}{\kappa}\right) = 1$ (car $\kappa = 1 \mod p_i$) et $\left(\frac{p_r}{\kappa}\right) = -1$ (car $\kappa = u \mod p_r$). Par suite, $\left(\frac{m}{\kappa}\right) = -1$ comme attendu. □

3. Répartition des nombres premiers

On sait depuis Euclide que l'ensemble des nombres premiers est infini. On peut en effet toujours trouver un nombre premier strictement plus grand qu'un nombre premier p donné, à savoir n'importe quel facteur premier de $p! + 1$.

Dans ce chapitre, nous affinons ce résultat fondamental.

On peut déjà mentionner le résultat suivant :

Proposition 18. — *Il existe des intervalles d'entiers arbitrairement longs ne contenant aucun nombre premier.*

Démonstration. — Considérons un entier $n > 1$ et posons $N = (n+1)! + 1$. Pour tout $k \in [[1, n]]$, $k+1$ divise $N-1$ et donc aussi $N-1+k+1 = N+k$. Ainsi, l'intervalle d'entiers $[[N+1, N+n]]$ ne contient aucun nombre premier. □

Notation 19. — *On notera $(p_k)_{k \geq 1}$ la suite croissante des nombres premiers.*

Par ailleurs, pour tout réel x, on utilisera le symbole $\sum_{k \leq x}$ pour désigner une somme sur les entiers strictement positifs et inférieurs ou égaux à x.

3.1. La série des inverse des nombres premiers. — Le résultat d'Euclide au sujet de l'infinitude de l'ensemble des nombres premiers a été précisé par Euler :

Proposition 20. — *La série des inverses des nombres premiers est divergente (voir* [**FGNb**, Exercice 3.18]*).*

Démonstration. — Il suffit de démontrer que le produit $\prod_{k=1}^{\infty} \frac{1}{1-\frac{1}{p_k}}$ tend vers $+\infty$ (vérifiez que vous comprenez pourquoi). Ceci résulte de l'égalité

$$\prod_{k=1}^{r} \frac{1}{1-\frac{1}{p_k}} = \prod_{k=1}^{r} \sum_{l=0}^{\infty} \frac{1}{p_k^l} = \sum_{j \in E_r} \frac{1}{j}$$

où E_r désigne l'ensemble des entiers dont les facteurs premiers appartiennent à $\{p_k \mid k \in [[1,r]]\}$ et de la divergence de la série harmonique. □

On peut préciser le résultat précédent :

Proposition 21. — *On a :*

$$\sum_{\substack{p \leq x \\ p \text{ premier}}} \frac{1}{p} \geq \ln\ln x - \ln 2.$$

(voir [**TMF**, Chapitre 1, §7]*)*

Démonstration. — On abrégera "sans facteur carré [3]" par "s.f.c.". Le résultat découle des inégalités suivantes :

$$\ln(x) \leq \sum_{j \leq x} \frac{1}{j} = \sum_{\substack{q \leq x \\ q \text{ s.f.c.}}} \frac{1}{q} \sum_{m \leq \sqrt{x/q}} \frac{1}{m^2} \leq \sum_{\substack{q \leq x \\ q \text{ s.f.c.}}} \frac{1}{q} \sum_{m \geq 1} \frac{1}{m^2}$$

$$\leq 2 \sum_{\substack{q \leq x \\ q \text{ s.f.c.}}} \frac{1}{q} \leq 2 \prod_{\substack{p \leq x \\ p \text{ premier}}} \left(1 + \frac{1}{p}\right) \leq 2 \exp\left(\sum_{\substack{p \leq x \\ p \text{ premier}}} \frac{1}{p} \right).$$

La première inégalité s'obtient classiquement par une comparaison série/intégrale, la troisième provient de :

$$\sum_{m \geq 1} \frac{1}{m^2} \leq 1 + \sum_{m \geq 2} \frac{1}{m(m-1)} = 1 + \sum_{m \geq 2} \frac{1}{m-1} - \frac{1}{m} = 2$$

et la dernière est une application de l'inégalité $1 + u \leq \exp(u)$ valable pour $u \geq 0$ qui résulte par exemple de la convexité de l'exponentielle. □

En utilisant le théorème des nombres premiers (difficile ; voir § 3.3) et l'équivalent suivant pour les sommes partielles d'une série de Bertrand

$$\sum_{k=2}^{n} \frac{1}{k \ln k} \sim \ln\ln n,$$

3. Un entier est dit sans facteur carré s'il n'est pas divisible par le carré d'un nombre premier.

on peut démontrer que

$$\sum_{p\leq x}\frac{1}{p}\sim \ln\ln x.$$

3.2. Postulat de Bertrand. — On doit a Tchébychev une démonstration [4] d'une conjecture connue sous le nom de postulat de Bertrand :

***Théorème 22* (Postulat de Bertrand).** — *Pour tout entier $n > 3$, il existe un nombre premier strictement compris entre n et $2n-2$.*

Nous renvoyons à [**Gou**, Chapitre 1, § 5, Sujet d'Etude 1] pour une démonstration.

3.3. Théorème des nombres premiers. — Pour tout réel positif x, on note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x. Le théorème des nombres premiers conjecturé par Gauss et démontré indépendamment par Hadamard et La Vallée-Poussin [5] est :

***Théorème 23* (Théorème des nombres premiers)**
On a :

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

Le jury insiste sur le fait que les candidats devraient connaître l'énoncé de ce résultat compte tenu de son importance historique, tout en précisant que sa démonstration (complexe) n'est pas exigible au niveau de l'agrégation.

Notons le :

Corollaire 24. — *On a :*

$$p_k\sim k\ln k.$$

Démonstration. — L'équivalent $k=\pi(p_k)\sim\frac{p_k}{\ln p_k}$ se réécrit $\ln p_k-\ln\ln p_k=\ln k+o(1)$ d'où $\frac{\ln k}{\ln p_k}=1-\frac{\ln\ln p_k}{\ln p_k}+o(1)$. Ainsi $\ln p_k\sim\ln k$. Par conséquent $k=\pi(p_k)\sim\frac{p_k}{\ln p_k}\sim\frac{p_k}{\ln k}$. □

4. Plus précisément, Tchébychev a prouvé une forme faible du théorème des nombres premiers (énoncé plus bas) : il a déterminé des constantes $c_1,c_2>0$ telles que, lorsque $x\to\infty$,

$$(c_1+o(1))\frac{\ln x}{x}\leq\pi(x)\leq(c_2+o(1))\frac{\ln x}{x}$$

où $\pi(x)$ désigne le nombre de nombres premiers inférieurs ou égaux à x. C'est ce qui lui a permis de démontrer le postulat de Bertrand.

5. Les démonstrations de Hadamard et de La Vallée-Poussin reposent sur la célèbre fonction zêta de Riemman et l'analyse complexe. Ultérieurement, des démonstrations utilisant des outils élémentaires (ce qui ne veut pas dire qu'elles sont *simples*!) ont été trouvées par Erdös et Selberg.

3.4. Théorème de la progression arithmétique. — Le théorème suivant, dont on doit la démonstration à Dirichlet, est mentioné pour culture générale : son énoncé est simple mais sa démonstration (voir [**Ser**]) beaucoup moins !

***Théorème 25* (Théorème de la progression arithmétique [7])**
Si a et $b \geq 1$ sont des entiers premiers entre eux alors il existe une infinité de nombres premiers congrus à a modulo b.

Cependant, des cas particuliers du théorème de la progression arithmétique ont des preuves abordables.

Le cas particulier $a = 3$ et $b = 4$ n'est guère plus compliqué que le résultat fondamental d'Euclide.

Proposition 26. — *Il existe une infinité de nombres premiers congrus à* 3 *modulo* 4 *(voir* [**FGNa**, Exercice 4.16]*).*

Démonstration. — Supposons au contraire qu'il n'y a qu'un nombre fini de nombres premiers congrus à 3 modulo 4. Notons les $p_1, ..., p_r$. Considérons $N = 4p_1 \cdots p_r - 1 \geq 2$. Les diviseurs premiers de N sont impairs (car N est impair) et donc congrus à 1 ou 3 modulo 4. Ils sont congrus à 1 modulo 4 puisqu'ils sont clairement distincts de $p_1, ..., p_r$. On en déduit que N lui-même est congru à 1 modulo 4, d'où une contradiction. □

Traitons le cas particulier $a = 1$ et $b = 4$ en utilisant la caractérisation des nombres premiers modulo lesquels -1 est un résidu quadratique.

Proposition 27. — *Il existe une infinité de nombres premiers congrus à* 1 *modulo* 4 *(voir* [**Per**, p.76]*).*

Démonstration. — Le résultat découle du fait que, pour tout entier $n > 1$, les diviseurs premiers de $(n!)^2 + 1$ sont supérieurs à n et congrus à 1 modulo 4 puisque, pour chaque diviseur premier p (forcément impair) de $(n!)^2 + 1$, -1 est un carré modulo p. □

7. On a en fait un énoncé plus précis : *l'ensemble des nombres premiers congrus à a modulo b a pour densité analytique $1/\varphi(b)$ où φ désigne l'indicatrice d'Euler.* On dit qu'une partie A de l'ensemble des nombres premiers a pour densité analytique $k \in \mathbb{R}$ si

$$\sum_{p \in A} \frac{1}{p^s} \underset{\substack{s \to 1 \\ s > 1}}{\sim} k \cdot \log \frac{1}{s-1}.$$

On montre aussi (et c'est plus fort) que cet ensemble de nombres premiers a pour densité naturelle $1/\varphi(b)$ c'est-à-dire que :

$$\lim_{n \to \infty} \frac{\sharp\{p \text{ premier } \leq n \mid p = a \mod b\}}{\sharp\{p \text{ premier } \leq n\}} = 1/\varphi(b).$$

Pour tout cela, on renvoit à [**Ser**].

Le résultat suivant, plus général que les deux précédents, a une jolie démonstration reposant sur les polynômes cyclotomiques.

Théorème 28. — *Soit b un entier ≥ 2. Il existe une infinité de nombres premiers congrus à 1 modulo b.*

La preuve donnée ici est essentiellement celle de [**Goz**, Proposition VII.13]. Une variante est proposée dans [**FGNa**, Exercice 4.17].

Démontrons d'abord la

Proposition 29. — *Soit $P(X) \in \mathbb{Z}[X]$ de degré ≥ 1. Il existe une infinité de nombres premiers p tels que $P(X) \mod p \in \mathbb{F}_p[X]$ admet une racine dans $\mathbb{F}_p$.*

Démonstration. — Si $P(0) = 0$, le résultat est clair. Supposons donc $a_0 := P(0) \neq 0$. Quitte à remplacer $P(X)$ par $P(a_0X)/a_0$, on peut supposer que $P(0) = 1$. Soit n un entier. Puisque $P(n!X)$ est un élément de $\mathbb{Z}[X]$ de degré ≥ 1, il prend sur $\mathbb{Z}$ une valeur distincte de $0, \pm 1$ qui est donc divisible par un nombre premier p. Ainsi $P(n!X) \mod p$, et donc $P(X) \mod p$ lui-même, admet une racine dans $\mathbb{F}_p$. On a $p > n$ car, pour tout entier naturel $m \leq n$, $P(n!X) = P(0) = 1 \mod m$. Puisque n peut être choisi arbitrairement grand, le résultat est prouvé. □

Rappelons que le $n$ème polynôme cyclotomique $\Phi_n(X)$ est défini par :

$$\Phi_n(X) = \prod_{\xi \in \mathrm{Prim}_n} (X - \xi)$$

où ξ parcourt l'ensemble Prim_n des racines primitives $n$èmes de l'unité dans $\mathbb{C}$ et que l'on a $\prod_{d|n} \Phi_d(X) = X^n - 1$ et $\Phi_n(X) \in \mathbb{Z}[X]$.

Proposition 30. — *Soit p est un nombre premier ne divisant pas n. Si $\Phi_n(X) \mod p$ a une racine dans $\mathbb{F}_p$ alors $p = 1 \mod n$.*

Démonstration. — Soit $x \in \mathbb{F}_p$ une racine de $\Phi_n(X) \mod p$. Puisque $\Phi_n(X)$ divise $X^n - 1$ dans $\mathbb{Z}[X]$, on a $x^n = 1$ et donc l'ordre d de x dans $\mathbb{F}_p^\times$ divise n. Supposons que c'est un diviseur strict de n. On a $x^d = 1$. Or $X^d - 1 = \prod_{d'|d} \Phi_{d'}(X)$, donc x est racine de $\Phi_{d'} \mod p$ pour un certain diviseur strict d' de d. De la formule $X^n - 1 = \prod_{k|n} \Phi_k(X)$, on en déduit que $X^n - 1 \mod p$ a une racine multiple ce qui est faux car $X^n - 1 \mod p$ est premier avec son polynôme dérivé $nX^{n-1} \mod p$ (car p ne divise pas n). Ainsi $d = n$. Le théorème de Lagrange montre que $d = n$ divise $|\mathbb{F}_p^\times| = p - 1$ i.e. $p = 1 \mod n$. □

Preuve du théorème 28. — Combiner les deux résultats précédents ! □

4. Gren-Tao : pour la culture

Le résultat suivant dû à Green et Tao est très récent (et sa démonstration bien difficile !).

***Théorème 31* (Green-Tao).** — *La suite des nombres premiers contient des progressions arithmétiques arbitrairement longues.*

Il s'agit d'un cas particulier d'une conjecture formulée par Erdos (non démontrée à ce jour) :

Conjecture 32. — *Soit $(x_n)_{n\in\mathbb{N}}$ une suite d'entiers strictement positifs. Si la série $\sum_{n\geq 0}\frac{1}{x_n}$ diverge alors on peut extraire de $(x_n)_{n\in\mathbb{N}}$ des progressions arithmétiques arbitrairement longues.*

5. Une formule pour les nombres premiers ?

On peut naïvement se demander s'il existe une formule engendrant les nombres premiers. Un premier résultat négatif :

Proposition 33. — *Soit $P \in \mathbb{Z}[X]$ non constant. Une infinité de valeurs prisent par $P(X)$ sur $\mathbb{N}$ ne sont pas des nombres premiers.*

Démonstration. — Soit $n \in \mathbb{N}$ tel que $|P(n)| \geq 2$. Si p est un facteur premier de $|P(n)|$ alors, pour tout entier k, $|P(n+kp)|$ est divisible par p et tend vers l'infini avec k, il est donc composé pour tout k assez grand. □

Cependant, on sait qu'il existe un polynôme de degré 25 en 26 variables dont l'ensemble des valeurs positives est l'ensemble des nombres premiers. Il existe bien d'autres "formules", pas forcément polynômiales ; nous renvoyons par exemple au court article [**Inf**].

Nous retiendrons que ces formules n'ont **aucun intérêt pratique** : les temps de calculs sont bien trop élevés !

6. Primalité : soyons concrets

Comment décider qu'un nombre donné n est premier (ou pas) ? Comment trouver de grands nombres premiers ? Telles sont les questions motivant ce chapitre. Nous cherchons des méthodes utilisables sur machine, nécessitant des temps de calcul raisonnables (typiquement, de l'ordre de $\ln^k$). Cette recherche d'un bon rapport qualité/prix conduit notamment à considérer des tests de primalité probabilistes assurant seulement qu'un entier donné est "probablement premier" (c'est souvent suffisant en pratique). Nous verrons cependant qu'il y a des tests de primalité déterministes efficaces pour certains nombres, dont ceux de Fermat et de Mersennes. Ces derniers (ou des variantes proches)

donnent les exemples des plus grands nombres premiers connus mais ne sont cependant pas utilisés pour crypter des données car ils sont trop spéciaux.

Nous ne rentrons pas dans le détail du calcul des coûts dans ces notes ; nous renvoyons pour cela à [**Dem**]. Insistons : cet aspect est primordial et justifie ce qui suit donc ne faites pas l'impasse.

Référence principale : [**Dem**].

6.1. Méthode naïve. — La définission des nombres premiers conduit au cirtère naïf suivant :

Proposition 34. — *Un entier n est composé si et seulement s'il existe un entier $a \in [[2, \sqrt{n}]]$ non premier à n (ce que l'on teste grâce à l'algorithme d'Euclide).*

Obstruction à l'utilité pratique de ce résultat : les entiers a permettant de conclure à la non primalité de l'entier n via le résultat précédent sont rares et souvent grands (penser au produit de deux grands nombres premiers).

Il existe des cirtères plus pertinents, utilisant le calcul modulaire, qui sont l'objet des chapitres suivants. Il faut garder en tête l'intérêt pratique d'un contexte modulaire : cela permet de travailler avec des nombres "pas trop grands". Nous aurons fréquemment à calculer des puissances d'un entier a modulo un entier n. Il existe pour cela des algorithmes plus performants que l'algorithme naïf consistant à poser $a_0 = a \mod n$ puis à faire $a_{k+1} := a_k * a \mod n$ pour $k \geq 0$. Nous ne traiterons pas ces importantes questions pratiques ici ; nous renvoyons à [**Dem**, Chapitre 1].

En parlant de calcul modulaire, on pourrait imaginer utiliser le théorème de Wilson : on ne le fait pas en raison du coût élevé du calcul des factorielles.

6.2. Application directe du petit théorème de Fermat. — Le petit théorème de Fermat conduit à la

Proposition 35. — *Un entier $n > 0$ est composé si et seulement si il existe $a \in [[1, n-1]]$ tel que $a^{n-1} \neq 1 \mod n$.*

Démonstration. — Compte tenu du petit théorème de Fermat, il reste simplement à démontrer que si n est composé alors il existe $a \in [[1, n-1]]$ tel que $a^{n-1} \neq 1 \mod n$. Considérer pour cela n'importe quel $a \in [[1, n-1]]$ non premier avec n. □

Donnons les mauvaises nouvelles avant les bonnes : pour certains entiers n, ce critère n'apporte rien de nouveau relativement au critère naïf :

Définition 36. — *Un entier composé n tel que, pour tout a premier à n, on a $a^{n-1} = 1 \mod n$ est appelé nombre de Carmichael. En d'autres termes, un*

entier composé n est de Carmichael si l'exposant du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ divise $n-1$.

Il existe une infinité de nombres de Carmichael ; les premiers sont :

$$\begin{aligned} 561 &= 3\cdot 11\cdot 17 \\ 1105 &= 5\cdot 13\cdot 17 \\ 1729 &= 7\cdot 13\cdot 19 \\ 2465 &= 5\cdot 17\cdot 29 \\ 2821 &= 7\cdot 13\cdot 31 \\ 6601 &= 7\cdot 23\cdot 41 \\ 8911 &= 7\cdot 19\cdot 67. \end{aligned}$$

En fait, les nombres de Carmichael peuvent être caractérisés par leurs décompositions en facteurs premiers. Soit n un entier et considérons $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. Si n est impair l'exposant de $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal à :

$$\mathrm{ppcm}(p_1^{\alpha_1-1}(p_1-1),...,p_r^{\alpha_r-1}(p_r-1)).$$

Si n est pair, on peut supposer que $p_1=2$ et l'exposant de $(\mathbb{Z}/n\mathbb{Z})^\times$ est alors donné par :

$$\begin{cases} \mathrm{ppcm}(2^{\alpha-1},p_2^{\alpha_2-1}(p_2-1),...,p_r^{\alpha_r-1}(p_r-1)) \text{ si } \alpha\in\{1,2\}; \\ \mathrm{ppcm}(2^{\alpha-2},p_2^{\alpha_2-1}(p_2-1),...,p_r^{\alpha_r-1}(p_r-1)) \text{ si } \alpha\geq 3. \end{cases}$$

Ces assertions résultent clairement de la décomposition de $(\mathbb{Z}/n\mathbb{Z})^\times$ en produit de groupes cycliques donnée au § 1. Si n est de Carmichael, alors l'exposant de $(\mathbb{Z}/n\mathbb{Z})^\times$ divise $n-1$ et donc, pour chaque $i\in[[1,r]]$, on a $\alpha_i=1$ (car $n-1$ n'est pas divisible par p_i) et p_i-1 divise $n-1$. En d'autres termes, n est sans facteur carré et, pour tout diviseur premier p de n, $p-1$ divise $n-1$. En reprenant les formules ci-dessus on constate que tout entier vérifiant ses conditions est de Carmichael.

Proposition 37. — *Soit n un entier ≥ 2. Les assertion suivantes sont équivalentes :*

i) n est de Carmichael ;

ii) n est sans facteur carré et, pour tout diviseur premier p de n, $p-1$ divise $n-1$;

iii) pour tout entier a, $a^n = a \mod n$.

Démonstration. — L'équivalence entre i) et ii) a déjà été prouvée [8].

Prouvons que ii) implique iii). Soit $n = p_1 \cdots p_r$ la décomposition en facteurs premiers de n. Compte tenu de l'isomorphisme d'anneaux

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r\mathbb{Z}$$

donné par le théorème des restes chinois, il s'agit de démontrer que, pour tout $a \in \mathbb{Z}$, pour tout $i \in [[1, r]]$, $a^n = a \mod p_i$. Cette égalité résulte facilement de ce que $n = 1 \mod (p_i - 1)$ et du fait que $a^{p_i} = a \mod p_i$.

Le fait que iii) implique i) est clair (si a est premier avec n alors $a \mod n$ est un inversible de $\mathbb{Z}/n\mathbb{Z}$). □

On a aussi ([**Dem**]) :

Proposition 38. — *Tout nombre de Carmichael n est le produit de nombres premiers impairs distincts en nombre au moins* 3.

Et maintenant, les bonnes nouvelles. Quels sont les progrès relativement au critère naïf ? Les nombres de Carmichael sont rares : les entiers composés n sont fréquemment tels que les entiers $a \in [[1, n-1]]$ non premiers avec n ne sont pas les seuls à satisfaire $a^{n-1} \neq 1 \mod n$. Il en existe fréquemment de « petits »(au moins lorsque n n'est pas trop grand). A titre d'illustration, nous encourageons le lecteur à vérifier à l'aide de son logiciel préféré que le 1200ème nombre premier est $p_{1200} = 9733$ (ce qui est un petit nombre premier !) et que :

- il y a 22 entiers naturels composés $n \leq p_{1200}$ tels que $2^{n-1} = 1 \mod n$;
- il y a 7 entiers naturels composés $n \leq p_{1200}$ tels que $2^{n-1} = 1 \mod n$ et $3^{n-1} = 1 \mod n$;
- il y a 4 entiers naturels composés $n \leq p_{1200}$ tels que $2^{n-1} = 1 \mod n$, $3^{n-1} = 1 \mod n$ et $5^{n-1} = 1 \mod n$.

Combien existe-t-il d'entiers $a \in [[1, n-1]]$ tels que $a^{n-1} \neq 1$ lorsque n n'est pas de Carmichael ? Un élément de réponse est donné par :

Proposition 39. — *Si n est un entier qui n'est pas de Carmichael alors* $\sharp\{a \in [[1, n-1]] \mid a^{n-1} = 1 \mod n\} \leq \varphi(n)/2$.

Démonstration. — Il revient au même de montrer que le cardinal de l'ensemble des $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ tels que $x^{n-1} = 1$ est inférieur ou égal à $\varphi(n)/2$. Cela résulte du fait que cet ensemble est un sous-groupe strict de $(\mathbb{Z}/n\mathbb{Z})^\times$ dont le cardinal est donc un diviseur strict de l'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$. □

On peut imaginer le test de primalité probabiliste suivant. On itère un certain nombre N de fois ce qui suit :

8. L'utilisation du calcul explicite de l'exposant de $(\mathbb{Z}/n\mathbb{Z})^\times$ rend cette équivalence naturelle et triviale. Pour une démonstration plus pédestre (reprenant tout de même des arguments utilisés pour étudier la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$), nous renvoyons à [**Dem**].

On choisit un entier $a \in [[2, n-1]]$.

Si $a^{n-1} \neq 1 \mod n$ alors n est composé et c'est terminé sinon on recommence.

Si n n'a pas été déclaré composé à l'issu des N itérations, on le déclare probablement premier.

Nous n'en disons pas davantage sur ce test : le test de Miller-Rabin décrit plus bas en est une amélioration.

6.3. Miller-Rabin. — Le résultat suivant est basé sur le petit théorème de Fermat mais un peu plus élaboré. Il est à la base d'un test de primalité probabiliste efficace.

***Théorème 40* (Miller).** — *Soit n un entier impair. Soit $s \in \mathbb{N}$ tel que $n-1 = 2^s t$ avec t impair. Alors n est composé si et seulement s'il existe $a \in [[2, n-1]]$ tel que :*

- $a^t \neq 1 \mod n$;
- $\forall k \in [[0, s-1]]$, $a^{2^k t} \neq -1 \mod n$.

Démonstration. — Supposons n premier. D'après le petit théorème de Fermat, on a $a^{2^s t} = a^{n-1} = 1 \mod n$. Donc, si $a^t \neq 1 \mod n$, il exsite $k \in [[0, s-1]]$ tel que $a^{2^k t} \neq 1 \mod n$ et $\left(a^{2^k t}\right)^2 = a^{2^{k+1} t} = 1 \mod n$. Puisque $\mathbb{Z}/n\mathbb{Z}$ est un corps, on en déduit que $a^{2^k t} = -1 \mod n$.

Réciproquement, si n est composé, il suffit de considérer $a \in [[2, n-1]]$ non premier à n. □

L'un des intérêts du critère de Miller réside dans la quantité peu importante d'entiers a ne satisfaisant pas les propriétés du Théorème 40 lorsque n est composé :

***Théorème 41* (Rabin).** — *Soit n un entier impair composé > 9. Soit $s \in \mathbb{N}$ tel que $n-1 = 2^s t$ avec t impair. Les entiers $a \in [[2, n-1]]$ tels que $a^t = 1 \mod n$ ou, pour un certain $k \in [[0, s-1]]$, $a^{2^k t} = -1 \mod n$ sont en nombre au plus $\varphi(n)/4 \leq (n-2)/4$.*

Pour la preuve, voir [**Dem**].

Puisque le nombre d'entiers $a \in [[2, n-1]]$ premiers avec n est $\varphi(n) - 1$ et que pour n composé $\varphi(n) - 1 > \varphi(n)/4$, le théorème précédent montre :

Corollaire 42. — *Pour chaque entier composé $n > 9$, il existe $a \in [[1, n-1]]$ premier avec n tel que :*

- $a^t \neq 1 \mod n$;
- $\forall k \in [[0, s-1]]$, $a^{2^k t} \neq -1 \mod n$.

Ainsi, on s'est débarassé des nombres de Carmichael !

Le test de primalité probabiliste suivant est connu sous le nom de test de Miller-Rabin. On itère un certain nombre N de fois ce qui suit :

On choisit un entier $a \in [[2, n-1]]$.

Si $a^t \neq 1 \mod n$ et, $\forall k \in [[0, s-1]]$, $a^{2^k t} \neq -1 \mod n$ alors n est composé et c'est terminé sinon on recommence.

Si à l'issu de ces N itérations, n n'est pas déclaré composé alors on le déclare probablement premier.

Le Théorème 41 montre que la probabilité que le résultat soit erroné est $\leq 4^{-N}$.

6.4. Solovay Strassen. — Le critère suivant peut être considéré comme une amélioration de celui issu du petit théorème de Fermat. Il repose sur le fait que la formule d'Euler pour les résidus quadratiques ne s'étend en général pas au symbole de Jacobi.

Proposition 43. — *Soit $n \geq 3$ un entier impair tel que, pour tout a premier avec n, $\left(\frac{a}{n}\right) = a^{(n-1)/2} \mod n$. Alors n est premier.*

Démonstration. — Supposons au contraire que n est composé. Il s'agit d'un nombre de Carmichael car, pour tout a premier avec n, on a $1 = \left(\frac{a}{n}\right)^2 = a^{n-1} \mod n$. Ainsi $n = p_1 \cdots p_r$ avec des entiers premiers impairs $p_1, ..., p_r$ deux à deux distincts et $r \geq 3$.

Puisque $\left(\frac{a}{n}\right)$ ne peut prendre que les valeurs 0 ou ± 1 et qu'il est congru à $a^{(n-1)/2}$ modulo p_1 (car il l'est modulo n), il ne dépend que de la classe de congruence de a modulo p_1. Nous aboutirons donc à une contradiction si l'on montre l'existence d'un entier b premier avec n et congru à a modulo p_1 tel que $\left(\frac{b}{n}\right) = -\left(\frac{a}{n}\right)$.

Considérons un entier β tel que $\left(\frac{\beta}{p_r}\right) = -\left(\frac{a}{p_r}\right)$. Le théorème des restes chinois assure l'existence d'un entier b tel que, pour tout $i \in [[1, r-1]]$, $b = a \mod p_i$ et tel que $b = \beta \mod p_r$. On a alors $a = b \mod p_1$ et

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right) \cdots \left(\frac{b}{p_r}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_{r-1}}\right) \left(\frac{\beta}{p_r}\right) = -\left(\frac{a}{n}\right).$$

D'où une contradiction. □

Par ailleurs,

Proposition 44. — *Soit $n \geq 3$ un entier impair composé. Alors l'ensemble des $a \in [[1, n-1]]$ premiers avec n tels que $\left(\frac{a}{n}\right) = a^{(n-1)/2} \mod n$ a au plus $\varphi(n)/2$ éléments.*

Démonstration. — Cela résulte du théorème de Lagrange compte tenu du fait que l'ensemble des $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ tels que $\left(\frac{x}{n}\right) = 1$ est un sous-groupe strict de $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Le test de primalité probabiliste suivant est connu sous le nom de test de Solovay-Strassen. On itère un certain nombre N de fois ce qui suit :

On choisit un entier $a \in [[2, n-1]]$.

Si ($\text{pgcd}(a,n) \neq 1$ ou $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \mod n$) alors n est composé et c'est terminé sinon on recommence.

Si à l'issu de ces N itérations, n n'est pas déclaré composé alors on le déclare probablement premier.

La Proposition 44 montre que la probabilité que le résultat soit erroné est $\leq 2^{-N}$.

6.5. Miller-Rabin vs Solovay-Strassen. — L'algorithme de Miller-Rabin est meilleur que celui de Solovay-Strassen : voir [**Dem**, § 5.3.5.].

6.6. Critères de primalité lorsque les facteurs premiers de $n-1$ ou $n+1$ sont connus. — Nous donnons des critères de primalité pour des entier n tels que la factorisation en produit de nombres premiers de $n-1$ ou de $n+1$ est connue. Nous les appliquons aux nombres de Fermat et à ceux de Mersenne.

6.6.1. Critère de Lehmer. Nombres de Fermat. —

***Théorème 45* (Critère de Lehmer).** — *Soit n un entier impair > 2. Alors n est premier si et seulement si il existe un entier a tel que $a^{(n-1)/2} = -1 \mod n$ et, pour tout facteur premier impair q de $n-1$, $a^{(n-1)/q} \neq 1 \mod n$.*

Démonstration. — Si n est un premier alors il existe un entier a avec les propriétés escomptées : considérer n'importe quel entier dont la classe modulo n engendre le groupe cyclique formé par les inversibles du corps $\mathbb{Z}/n\mathbb{Z}$.

Réciproquement s'il existe un entier a avec les proriétés annoncées alors $a \mod n$ est un élément d'ordre $n-1$ de $(\mathbb{Z}/n\mathbb{Z})^\times$ et donc $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z}\backslash\{0\}$. Par conséquent, $\mathbb{Z}/n\mathbb{Z}$ est un corps et n est donc premier. □

Appliquons cela aux nombres de Fermat. On définit le $n$ème nombre de Fermat par

$$Ferm_n = 2^{2^n} + 1.$$

Le critère de Lehmer conduit à :

- Le $n$ème nombre de Fermat $Ferm_n$ est premier si et seulement si il existe un entier a tel que $a^{(Ferm_n - 1)/2} = -1 \mod Ferm_n$.

Si $n > 1$, on peut en fait se limiter à tester l'égalité $a^{(Ferm_n-1)/2} = -1 \mod Ferm_n$ pour $a = 3$ sans rien perdre !

***Proposition 46* (Critère de Pepin).** — *Le nème nombre de Fermat $Ferm_n$, pour $n > 1$, est premier si et seulement si $3^{(Ferm_n-1)/2} = -1 \mod Ferm_n$.*

Démonstration. — Compte tenu des résultats précédents, il suffit de montrer que si $Ferm_n$ est premier alors $3^{(Ferm_n-1)/2} = -1 \mod Ferm_n$. Puisque les nombres de Fermat $Ferm_n$ sont congrus à 5 modulo 12 pour $n > 1$, il suffit de montrer que, plus généralement, si p est un nombre premier congru à 5 modulo 12 alors $3^{(p-1)/2} = -1 \mod p$. Cela résulte de la loi de réciprocité quadratique, qui donne $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$, et du fait que p n'est pas un résidu quadratique modulo 3 (puisque $p = -1 \mod 3$). □

On peut vérifier que $Ferm_n$ est premier pour $0 \leq n \leq 4$. Fermat le savait mais pensait à tort que tous les nombres de Fermat étaient premiers. Le cinquième nombre $Ferm_5$ est composé ! A l'heure actuelle, on ne connait pas de nombre de Fermat $Ferm_n$ premier pour $n \geq 5$...

Pour terminer, nous donnons une autre preuve de la primalité de $Ferm_4$ et nous exhibons un facteur premier explicite de $Ferm_5$.

Proposition 47. — *On a :*

1) *si m est un entier non nul tel que $2^m + 1$ est premier alors m est une puissance de 2 et donc $2^m + 1$ est un nombre de Fermat.*
2) *$\forall n \in \mathbb{N}, Ferm_{n+1} = Ferm_0 \cdots Ferm_n + 2$; en particulier, les nombres de Fermat sont deux à deux premiers entre eux.*
3) *si $n \geq 2$ et si p est un diviseur premier strict de $Ferm_n$ alors $p = k2^{n+2} + 1$ où k est un entier qui n'est pas une puissance de 2.*

Démonstration. — Les preuves de 1) et 2) sont laissées au lecteur. Prouvons 3). On a $2^{2^n} = -1 \mod p$ donc 2 est d'ordre 2^{n+1} dans $\mathbb{F}_p^\times$; le théorème de Lagrange implique que $2^{n+1} | p - 1$ i.e. $p = h2^{n+1} + 1$ pour un certain entier h. Par conséquent, $p = 1 \mod 8$ et donc $2^{h2^n} = 2^{(p-1)/2} = \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = 1 \mod p$. Ainsi $2^{n+1} | h2^n$ et $h = 2k$ est pair. Puisque p est un diviseur strict de $Ferm_n$, 2) implique que p n'est pas un nombre de Fermat ; on déduit de 1) que k n'est pas une puissance de 2. □

Donnons une nouvelle preuve de la primalité de $Ferm_4$. Supposons $Ferm_4 = 65537$ composé et considérons le plus petit facteur premier p de $Ferm_4$. On a $p \leq \sqrt{Ferm_4}$ donc $p \leq 256$. La proposition précédente montre que nécessairement $p = 3 \cdot 2^6 + 1 = 193$ qui n'est pas un diviseur de 65537 : contradiction.

Exhibons un facteur premier p de F_5. On a $3 \cdot 2^7 + 1 = 3 \cdot 128 + 1 = 0 \mod 5$ donc le plus petit candidat est $p = 5 \cdot 2^7 + 1 = 641$ qui est bien premier. On a $p = 5 \cdot 2^7 + 1 = 5^4 + 2^4$. Donc $5 \cdot 2^7 = -1 \mod p$ et $5^4 \cdot 2^{28} = 1 \mod p$.

Par ailleurs, $2^4 = -5^4 \mod p$ donc $2^{32} = 2^4 2^{28} = -5^4 2^{28} = -1 \mod p$. Donc $p = 641$ divise $Ferm_5$.

6.6.2. Suites de Lucas. Nombres de Mersenne. — Considérons un élément a d'un anneau intègre A. L'unique suite à valeurs dans A telle que

$$\begin{cases} V_0 = 2, \\ V_1 = a, \\ \forall k \in \mathbb{N}^*, V_{k+1} = aV_k - V_{k-1}. \end{cases}$$

est donnée par :

$$\forall k \in \mathbb{N}, V_k = \alpha^k + \alpha^{-k}$$

où α est une racine de

$$P(X) = X^2 - aX + 1 \in A[X]$$

dans un corps de rupture K. Notons que

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

En d'autres termes, α est un élément non nul d'une extension de $\mathrm{Frac}(A)$ tel que $a = \alpha + \alpha^{-1}$.

Proposition 48 **(Critère de primalité de Lucas-Lehmer)**
Soit $n > 1$ un entier impair. Soit a un entier relatif tel que $\mathrm{pgcd}(n, a^2 - 4) = 1$ *et considérons la suite de Lucas $(V_k)_{k \geq 0}$ à valeurs dans $\mathbb{Z}$ définie par*

$$\begin{cases} V_0 = 2, \\ V_1 = a, \\ \forall k \in \mathbb{N}^*, V_{k+1} = aV_k - V_{k-1}. \end{cases}$$

Si $V_{n+1} = 2 \mod n$ et si $\mathrm{pgcd}(V_{(n+1)/q} - 2, n) = 1$ *pour tout facteur premier q de $n + 1$, alors n est premier.*

Démonstration. — Considérons un facteur premier (nécessairement impair) p de n. Il s'agit de montrer que $p = n$.

On note $(v_k)_{k \geq 0}$ la réduction de $(V_k)_{k \geq 0}$ modulo p. Ainsi $(v_k)_{k \geq 0}$ est la suite d'éléments de $\mathbb{F}_p$ définie par

$$\begin{cases} v_0 = 2 \mod p, \\ v_1 = a \mod p, \\ \forall k \in \mathbb{N}^*, v_{k+1} = av_k - v_{k-1}. \end{cases}$$

On a vu que si α est une racine de

$$P(X) = X^2 - aX + 1 \mod p \in \mathbb{F}_p[X].$$

dans un corps de rupture K alors $P(X) = (X - \alpha)(X - \alpha^{-1})$ et, pour tout $k \in \mathbb{N}$, $v_k = \alpha^k + \alpha^{-k}$.

Les hypothèses impliquent que

$$\alpha^{-(n+1)}(\alpha^{n+1}-1)^2 = \alpha^{n+1} + \alpha^{-(n+1)} - 2 = v_{n+1} - 2 = 0$$

et que, pour tout facteur premier q de $n+1$,

$$\alpha^{-(n+1)/q}(\alpha^{(n+1)/q}-1)^2 = \alpha^{(n+1)/q} + \alpha^{-(n+1)/q} - 2 = v_{(n+1)/q} - 2 \neq 0$$

donc $\alpha^{n+1} = 1$ et, pour tout facteur premier q de $n+1$, $\alpha^{(n+1)/q} \neq 1$. Ainsi l'ordre de α dans $K^\times$ est $n+1$.

Or, puisque que K est de caratéristique p et que $P(X)$ est à coefficients dans le sous-corps premier $\mathbb{F}_p$, la puissance $p$ème de toute racine de $P(X)$ dans K est à nouveau une racine de $P(X)$ dans K. Par conséquent, α^p coïncide avec α ou α^{-1} i.e. $\alpha^{p-1} = 1$ ou $\alpha^{p+1} = 1$. L'ordre de α dans $K^\times$ divise donc $p-1$ ou $p+1$.

On en déduit que $n+1$ divise $p-1$ ou $p+1$. Il s'en suit que $n+1 = p+1$ et donc $n = p$ est premier. □

Remarque 49. — *On peut se demander en quoi l'hypothèse* $\mathrm{pgcd}(n, a^2-4) = 1$ *est utile (elle n'a pas été utilisée). En fait elle n'est pas nécessaire, mais si elle n'est pas vérifiée les conditions d'applicabilité du théorème ne le sont pas non plus ! En effet, supposons que* $\mathrm{pgcd}(n, a^2-4) \neq 1$. *Soit* p *un facteur premier de* n *divisant* a^2-4. *On a donc* $a = \pm 2 \mod p$. *Si* $a = 2 \mod p$ *alors, pour tout* $k \in \mathbb{N}$, $V_k = 2 \mod p$ *donc* $\mathrm{pgcd}(V_k - 2, n) \neq 1$. *Si* $a = -2 \mod p$ *alors, pour tout* $k \in \mathbb{N}$, $V_k = (-1)^k 2 \mod p$ *donc, pour tout entier pair* k, $\mathrm{pgcd}(V_k - 2, n) \neq 1$ *; puisque* $n+1$ *est pair* ≥ 4, $n+1$ *admet un facteur premier* q *tel que* $(n+1)/q$ *est pair et donc tel que* $\mathrm{pgcd}(V_{(n+1)/q} - 2, n) \neq 1$.

A présent quelques remarques pratiques. Le critère de Lucas-Lehmer ne mettant en jeu que des propriétés modulo n, il suffit en pratique de calculer la suite de Lucas modulo n. Par ailleurs, la proposition suivante permet un calcul rapide des valeurs des suites de Lucas ; voir [**Dem**] pour les détails.

Proposition 50. — *On a, pour tout* $k \in \mathbb{N}^*$,

$$\begin{aligned} V_{2k-1} &= V_k V_{k-1} - a \\ V_{2k} &= V_k^2 - 2 \\ V_{2k+1} &= aV_k^2 - V_n V_{k-1} - a. \end{aligned}$$

Démonstration. — On sait que, pour tout $k \in \mathbb{N}$, $V_k = \alpha^k + \alpha^{-k}$ où α est une racine de $X^2 - aX + 1$. Le résultat suit par des calculs directs. □

Appliquons ce qui précède aux nombres de Mersenne. On s'intéresse à la primalité des entiers de la forme

$$n = 2^s - 1$$

où $s > 1$ est un entier. Notons que si un tel entier est premier alors s est impair (mais la réciproque est fausse !).

Corollaire 51. — *Considérons $n = 2^s - 1$ où $s > 1$ est un entier impair. Soit a un entier relatif tel que* $\text{pgcd}(a^2 - 4, n) = 1$. *Considérons la suite $(L_i)_{i \geq 1}$ définie par*

$$\begin{cases} L_1 = a, \\ \forall i \in \mathbb{N}^*, L_{i+1} = L_i^2 - 2. \end{cases}$$

Si $L_{s-1} = 0 \mod n$ alors n est premier.

Démonstration. — La proposition 50 montre que

$$\forall i \in \mathbb{N}^*, L_i = V_{2^{i-1}}.$$

Par hypothèse, on a $V_{2^{s-2}} = 0 \mod n$ donc $V_{(n+1)/2} = V_{2^{s-1}} = 0^2 - 2 = -2 \mod n$ puis $V_{n+1} = V_{2^s} = (-2)^2 - 2 = 2 \mod n$. La Proposition 48 conduit au résultat. □

En fait, on a mieux : on peu se contenter de considérer $a = 4$.

Théorème 52. — *Considérons $n = 2^s - 1$ où $s > 1$ est un entier impair. Considérons la suite $(L_i)_{i \geq 1}$ définie par*

$$\begin{cases} L_1 = 4, \\ \forall i \in \mathbb{N}^*, L_{i+1} = L_i^2 - 2. \end{cases}$$

Pour que n soit premier il faut et il suffit que $L_{s-1} = 0 \mod n$.

Nous renvoyons pour la preuve à [**Dem**].

7. Leçon sur les nombres premiers

Quelques idées pour la leçon sur les nombres premiers :
- Définition et propriétés élémentaires des nombres premiers (dont le théorème fondamental de l'arithmétique bien entendu). Applications.
- Répartition des nombres premiers.
- Loi de réciprocité quadratique.
- Critères et tests de (non) primalité. Applications aux nombres de Fermat et à ceux de Mersennes.
- Méthode RSA.
- Et aussi : irréductibilité des polynômes dans $\mathbb{Z}[X]$, nombres premiers et théorie des groupes, polygones constructibles, etc.

Il faut bien entendu mentionner tôt dans le plan le fondamental
- lien nombres premiers/corps finis.

qui est utilisé dans bien des thèmes ci-dessus !

Poursuivons avec des extraits de rapports du jury qui vous aideront à construire votre plan.

Rapport du jury 2005 : *Certaines identifications rendent les exposés confus, voire faux : $\mathbb{Z}/n\mathbb{Z}$ identifié au sous-ensemble $\{0, 1, 2, ..., n-1\} \subset \mathbb{Z}$. Dans ces leçons, la loi de réciprocité quadratique est souvent proposée, mais les candidats ne proposent aucune application et ne savent pas calculer le symbole $\left(\frac{2}{p}\right)$. Par ailleurs il faut faire très attention à l'extension dans laquelle on travaille. En bref, on assiste souvent à une suite de calculs incompréhensibles. Il faudrait connaître les idéaux de $\mathbb{Z}/n\mathbb{Z}$. Il serait bon de ne pas donner des résultats tels que la caractérisation des nombres de Carmichael si l'on ne peut :*

- en exhiber un,

- savoir (au moins) qu'il en existe une infinité.

A l'enoncé d'un résultat, il est toujours utile de se poser la question de la réciproque. Ainsi, certains candidats ont retrouvé (découvert ?) avec l'aide du jury le plus souvent que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z} \Rightarrow m \wedge n = 1$. Par ailleurs, sur ces leçons, le jury attend que les candidats apportent des éléments du niveau de l'agrégation.

Rapport du jury 2007 : *Cette leçon est classique et bien balisé, encore faut-il l'organiser de façon cohérente. Il est absurde de vouloir déduire que l'ensemble des nombres premiers est infini de la divergence de la série $\sum \frac{1}{p}$. Il peut être intéressant de consacrer une section à la répartition des nombres premiers, à des exemples de nombres premiers, à la recherche de nombres premiers, aux applications en algèbre, en géométrie. Par contre le choix du développement doit être bien réfléchi ; le candidat ne peut se contenter de proposer un théorème de Sylow sous prétexte qu'un nombre premier apparaît en cours de route, ou le critère d'Eisenstein.*

Rapport du jury 2009 : *La répartition des nombres premiers est un résultat historique important. Sa démonstration n'est bien-sûr pas exigible au niveau de l'Agrégation. Il faut savoir si 89 est un nombre premier ! Attention aux choix des développements, ils doivent être pertinents.*

Rapport du jury 2010 : *Il faut savoir si 113 est un nombre premier ! Attention aux choix des développements, ils doivent être pertinents (l'apparition d'un nombre premier n'est pas suffisant !). La réduction modulo p n'est pas hors-sujet et constitue un outil puissant pour résoudre des problèmes arithmétiques*

simples. La répartition des nombres premiers est un résultat historique important, qu'il faudrait citer. Sa démonstration n'est bien-sûr pas exigible au niveau de l'Agrégation.

8. Quelques résultats supplémentaires

En utilisant le théorème fondamental de l'arithmétique, on montre facilement la :

Proposition 53. — *Soient a, b deux entiers naturels premiers entre eux. Soit $k \geq 2$ un entier. Si ab est une puissance $k$ème dans $\mathbb{Z}$ alors c'est aussi le cas de a et b*

Elle est utilisée dans [**FGNa**, Exercice 4.21] pour démontrer le résultat suivant :

Proposition 54. — *Soit $k \geq 2$ un entier. Le produit de trois entiers consécutifs n'est pas un puissance $k$ème.*

On utilise souvent le théorème fondamental de l'arithmétique pour ramener un énoncé sur des entiers arbitraires à un énoncé sur les nombres premiers. C'est par exemple la démarche adoptée dans [**FGNa**, Exercice 4.35] pour démontrer le

Théorème 55. — *Tout entier naturel est somme des quatre carrés.*

En effet, une identité remarquable montre que l'ensemble des entiers sommes de quatre carrés est stable par multiplication ; le théorème fondamental de l'arithmétique montre alors qu'il suffit de traiter le cas des nombres premiers.

Une fois cette réduction faite, un ingrédient de la démonstration est le fait que tout nombre premier impair p divise un nombre de la forme $1 + a^2 + b^2$ avec $a, b \in \mathbb{N}$ i.e. que l'équations $x^2 + y^2 = -1$ admet une solution dans $\mathbb{F}_p$. Ce résultat classsique s'établit habituellement par l'argument combinatoire suivant : les sous-ensembles $\{x^2 \mid x \in \mathbb{F}_p\}$ et $\{-1 - y^2 \mid y \in \mathbb{F}_p\}$ de $\mathbb{F}_p$ ont pour cardinal $\frac{p+1}{2}$ et ont donc une intersection non vide.

Rappelons au passage qu'on sait décrire les nombres premier sommes de deux carrés :

Proposition 56. — *Un nombre premier impair est somme de deux carrés si et seulement si il est congru à 1 modulo 4.*

J'invite le lecteur à jeter un coup d'oeil au théorème de Sophie Germain [**FGNa**, Exercice 4.38].

Références

[Dem] M. Demazure. Cours d'algèbre. Primalité. Divisibilité. Codes. *Cassini*.

[FGNa] S. Francinou, H. Gianella, and S. Nicolas. Exercices de mathématiques des oraux de l'Ecole polytechnique et des Ecoles normales supérieures : Algèbre Tome 1. *Cassini*.

[FGNb] S. Francinou, H. Gianella, and S. Nicolas. Exercices de mathématiques des oraux de l'Ecole polytechnique et des Ecoles normales supérieures : Analyse Tome 1. *Cassini*.

[Gou] X. Gourdon. Algèbre. *Ellipses*.

[Goz] Y. Gozard. Théorie de Galois. *Ellipses*.

[Inf] CNRS Info. Formules et nombres premiers. Il existe des formules qui donnent tous les nombres premiers, mais... `http://www.cnrs.fr/Cnrspresse/math2000/html/math10.htm♯image`.

[Per] D. Perrin. Cours d'algèbre. *Ellipses*.

[Ser] J.-P. Serre. Cours d'arithmétique. *Presses Universitaires de France*.

[TMF] G. Tenenbaum and M. Mendès France. Les nombres premiers, entre l'ordre et le chaos. *Dunond*.

[Zis] M. Zisman. Mathématiques pour l'agrégation. *Dunod*.

---

26 avril 2012

Julien Roques, Institut Fourier, Université Grenoble 1, CNRS UMR 5582, 100 rue des Maths, BP 74, 38402 St Martin d'Hères • *E-mail :* `Julien.Roques@ujf-grenoble.fr`