Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Pierre Le Scornet

mars 2020

Résumé

L'objet de ce mémoire est la leçon 220 *Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.* La philosophie de ce plan est de partir de généralités sur ces anneaux, avec les aspects de théorie des groupes, des anneaux et des corps associés à $\mathbb{Z}/n\mathbb{Z}$. Elle continue avec les théorèmes chinois, décrivant la structure des anneaux produits des anneaux $\mathbb{Z}/n\mathbb{Z}$. Elle devient plus pratique avec des résultats d'arithmétique modulaire et de tests de primalité, avant d'appliquer ces résultats à des situations réelles comme la recherche de grand nombres premiers ou la cryptographie.

Table des matières

1 Groupes, anneaux et corps $\mathbb{Z}/n\mathbb{Z}$

Cette première partie va définir $\mathbb{Z}/n\mathbb{Z}$ en tant que groupe, anneau et corps. Elle va notamment présenter en quoi ces structures se trouvent au coeur des groupes abéliens finis, et développer sur les inversibles de cet anneau.

1.1 Le groupe $\mathbb{Z}/n\mathbb{Z}$

Définition 1.1. Pour un groupe G abélien et un sous-groupe H de G, on note G/H le *groupe quotient de G par H*, défini par l'ensemble des gH pour $g \in G$ muni de la loi $g_1H, g_2H \in G/H \to g_1g_2H$.

Définition 1.2. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est le groupe quotient de $\mathbb{Z}$ par $n\mathbb{Z}$, pour $n \in \mathbb{N}^*$.

Les éléments de ce groupe sont exactement les classes $n\mathbb{Z} + k$ pour $k \in [\![0; n-1]\!]$. Ainsi, $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n.
Ces groupes représentent exactement les groupes cycliques, dans le sens où :

Proposition 1.1. *Si un groupe G est cyclique et de cardinal n, alors il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

L'isomorphisme de cette propriété est entièrement déterminé par $\phi : g \to \overline{1}$, avec g engendrant G. Il est surjectif puisque G est monogène (engendré par un élément), et donc bijectif par égalité des cardinaux. On peut aussi caractériser les générateurs de ces groupes, ce qui permet d'introduire l'indicatrice d'Euler :

Proposition 1.2. *Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\overline{k}, k \in \mathbb{Z}$ tels que k est premier avec n. On note $\varphi(n)$ le nombre de ces générateurs. Cette fonction φ est nommée* indicatrice d'Euler.

On peut aussi étudier les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

Proposition 1.3. *Pour d diviseur de n, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$, qui est le sous-groupe engendré par la classe de $\frac{n}{d}$. Ce sont les seuls sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.*

Exemple. Les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ sont $\{0\}, 2\mathbb{Z}/6\mathbb{Z}, 3\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$.

Les groupes $\mathbb{Z}/n\mathbb{Z}$ sont au coeur de la théorie des groupes abéliens finis, comme le montre le théorème de structure :

Théorème 1.1 (de structure)**.** *Soit G un groupe abélien fini. Alors, il existe un unique $r \in \mathbb{N}^*$ et une unique famille $(n_1, ...n_r)$ d'entiers tel que $n_r|...|n_1 > 1$ et :*

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z}$$

Les n_i sont appelés invariants *de G.*

Corollaire 1.1.1. Ce théorème se généralise aux groupes abéliens de type fini. Si G est de ce type, alors il existe des uniques $k, r \in \mathbb{N}^*$ et une unique famille $(n_1, ...n_r)$ d'entiers tel que $n_r|...|n_1 > 1$ et :

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z} \times \mathbb{Z}^k$$

On peut appeler k le rang de G.

Exemple. Puisque $600 = 2^3 \times 5^2 \times 3$, il y a 6 groupes abéliens d'ordre 600 à isomorphisme près. Leurs invariants sont : $(600), (5, 120), (2, 300), (10, 60), (2, 2, 150), (2, 10, 30)$.

1.2 Anneaux $\mathbb{Z}/n\mathbb{Z}$

De la même façon qu'avec les groupes, on peut définir le quotient d'un anneau par un idéal de cet anneau.

Définition 1.3. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'anneau quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.

Le groupe additif associé à cet anneau est exactement le groupe $\mathbb{Z}/n\mathbb{Z}$, d'où la même notation. On peut étudier les éléments de cet anneau.

Proposition 1.4. *Pour $\overline{s} \in \mathbb{Z}/n\mathbb{Z}$, alors $\overline{s}$ est inversible si et seulement si s est premier avec n, si et seulement si $\overline{s}$ engendre l'anneau $\mathbb{Z}/n\mathbb{Z}$. Ainsi, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.*

Cette propriété prolonge les équivalences sur les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$, et sont donc au nombre de $\varphi(n)$. On notera donc $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif des inversibles de $\mathbb{Z}/n\mathbb{Z}$. On peut donc caractériser le fait pour $\mathbb{Z}/n\mathbb{Z}$ d'être un corps.

Théorème 1.2. *$\mathbb{Z}/n\mathbb{Z}$ est un corps (i) si et seulement si n est premier (ii) si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est intègre (iii). Dans ce cas, on le note $\mathbb{F}_n$*

Corollaire 1.2.1. Pour n premier, on aura donc $\varphi(n) = n - 1$ puisque $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$.

Nous pouvons aussi étudier les idéaux de cet anneau. Les idéaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$, avec $d|n$. De plus, nous avons :

Proposition 1.5. *Les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $p\mathbb{Z}/n\mathbb{Z}$, avec $p|n$ premier.*

Exemple. Les idéaux de $\mathbb{Z}/8\mathbb{Z}$ sont $\{0\}, 2\mathbb{Z}/8\mathbb{Z}, 4\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}$ et son seul idéal maximal est $2\mathbb{Z}/8\mathbb{Z}$.

Enfin, nous pouvons étudier les automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$:

Théorème 1.3. *Pour $n \geq 2$, on a $((\mathbb{Z}/n\mathbb{Z})^\times, .) \simeq (Aut(\mathbb{Z}/n\mathbb{Z}), \circ)$. Cet automorphisme est réalisé par $\sigma : x \to (\sigma(x) :\to xy)$.*

Démonstration. Soit $x_1, x_2 \in (\mathbb{Z}/n\mathbb{Z})^\times$, et $y \in (\mathbb{Z}/n\mathbb{Z})$. On a :

$$\sigma(x_1x_2)(y) = x_1(x_2y) = \sigma(x_1) \circ \sigma(x_2)(y)$$

Donc σ est bien un morphisme de groupe. Ainsi pour $x \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\sigma(x) = 1 \Longrightarrow \sigma(x)(\overline{1}) = 1 \Longrightarrow x\overline{1} = \overline{1} \Longrightarrow x = \overline{1}$$

Ce morphisme est donc injectif. Montrons qu'il est surjectif : si $\phi \in Aut(\mathbb{Z}/n\mathbb{Z})$ et $\overline{k} = u(\overline{1})$ alors pour tout $\overline{j} \in \mathbb{Z}/n\mathbb{Z}$:

$$\phi(\overline{j}) = \phi(j\overline{1}) = j\phi(\overline{1}) = j\overline{k} = \overline{jk} = \sigma(\overline{k})(\overline{j})$$

Ainsi, ϕ est bien dans l'image de σ, donc σ est surjective. On a bien σ isomorphisme. □

2 Théorèmes chinois

Les théorèmes chinois étudient les solutions de systèmes de congruence. Elle nous donne notamment l'existence et l'unicité (dans des anneaux $\mathbb{Z}/n\mathbb{Z}$) de solutions à ces systèmes dans le cas premier entre eux deux à deux, et des conditions sur l'existence de solutions dans le cas général.

2.1 Théorème chinois

On commence par introduire les morphismes d'anneaux :

Définition 2.1. Un morphisme d'anneaux de l'anneau A à l'anneau B est une application $f : A \to B$ tels que $f(1_A) = 1_B$ et f compatible avec les lois de A, i.e. :

$$\forall x, y \in A, f(x + y) = x + y, f(xy) = f(x)f(y)$$

Proposition 2.1 (lemme chinois)**.** *Soient n, m deux entiers positifs premiers entre eux. Alors :*

$$\mathbb{Z}/_{nm\mathbb{Z}} \simeq \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}$$

qui est réalisé par l'isomorphisme $f : \overline{s} \in \mathbb{Z}/_{nm\mathbb{Z}} \to (\overline{s}, \overline{s}) \in \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}$.

Démonstration. Montrons que l'on a bien un isomorphisme. D'abord, c'est un morphisme car :

$$\forall x, y \in \mathbb{Z}, f(x+y) = (\overline{x+y}, \overline{x+y})) = (\overline{x} + \overline{y}, \overline{x} + \overline{y}) = f(x) + f(y)$$

$$f(xy) = (\overline{xy}, \overline{xy}) = (\overline{xy}, \overline{xy}) = f(x)f(y)$$

et $f(\overline{1}) = (\overline{1}, \overline{1})$.
Pour $x \in \mathbb{Z}$, supposons $f(x) = (\overline{0}, \overline{0})$, i.e. m et n divisent x. Or m et n sont premiers entre eux, donc x est divisible par mn et $x = 0$. Donc f est injective.
On conclut par l'égalité des cardinaux que f est un isomorphisme. □

Théorème 2.1 (théorème chinois général)**.** *Soient $n_1..n_k \in \mathbb{N}$ premiers entre eux deux à deux, et $n = n_1...n_k$. Alors :*

$$\mathbb{Z}/_{n\mathbb{Z}} \simeq \mathbb{Z}/_{n_1\mathbb{Z}} \times ... \times \mathbb{Z}/_{n_k\mathbb{Z}}$$

qui est réalisé par le même genre d'isomorphisme que pour le lemme chinois.

2.2 Systèmes de congruence

Application 2.1.1. On peut réécrire ces théorèmes en terme de systèmes de congruences. Il existe une unique solution modulo mn à $\left\{ \begin{array}{rcll} x & \equiv & a & [n] \\ x & \equiv & b & [m] \end{array} \right.$ pour m et n premiers entre eux.

Exemple. $\left\{ \begin{array}{rcll} x & \equiv & 4 & [15] \\ x & \equiv & 3 & [4] \end{array} \right.$ si et seulement si $x \equiv 19[60]$

On peut généraliser ce résultat :

Corollaire 2.1.1. Le système

$$\left\{ \begin{array}{rll} x \equiv & a_1 & [n_1] \\ \vdots & & \\ x \equiv & a_k & [n_k] \end{array} \right.$$

admet une solution modulo $ppcm(n_1, ...n_k)$ si et seulement si $\forall i, j, a_1 \equiv a_j[pgcd(n_i, n_j)]$.

Ces théorèmes nous donnent une méthode générale de calcul de l'indicatrice d'Euler :

Application 2.1.2. — Si p premier, alors $\varphi(p^k) = (p-1)p^{k-1}$.

— Si $p_1...p_r$ premiers distincts, alors $\varphi(p_1^{k_1}...p_r^{k_r}) = \prod_{i=1}^{r}(p_i-1)p_i^{k_i-1}$.

Ainsi, on peut calculer l'indicatrice d'Euler pour tout entier grâce à sa décomposition en facteur premier. Il n'existe pas encore de méthode générale et efficace de calcul de l'indicatrice d'Euler, ce qui assure en principe la sécurité du cryptosystème RSA (en partie IV).

3 Résultats arithmétiques

Nous pouvons maintenant appliquer nos résultats à l'arithmétique, notamment en arithmétique modulaire, qui a des applications en cryptographie ou encore dans les codes correcteurs d'erreurs. Nous nous intéresseront notamment aux théorèmes de test de primalité, permettant de vérifier si un nombre est premier.

Théorème 3.1 (petit théorème de Fermat)**.** *Pour $a, p \in \mathbb{N}$ avec p premier, alors on a $a^p \equiv a[p]$.*

Corollaire 3.1.1. Ce théorème nous donne un test de primalité, sur p : si on trouve un a tel que $a^p \not\equiv a[p]$, alors p n'est pas premier. Les p non premiers qui passent cependant ce test sont appelés nombre de Carmichaël, ou pseudo-premier de Fermat.

Théorème 3.2 (d'Euler)**.** *On peut généraliser le petit théorème de Fermat à $n \in \mathbb{N}^*$ avec $a^{\varphi(n)} \equiv 1[n]$. Dans le cas p premier, nous avons donc $a^{p-1} \equiv 1[p]$.*

Si l'on veut montrer que p est premier, il nous faut un test de primalité parfait, dans le sens où si p passe le teste, alors il est premier. Le théorème de Wilson nous donne un exemple de test parfait :

Théorème 3.3 (de Wilson)**.** *Pour $p > 1$, p est premier si et seulement si $(p-1)! \equiv -1[p]$.*

par Gauss. Dans la factorielle, on regroupe les facteurs par paire élément-inverse dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Puisque les deux seuls éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ étant leur propre inverse sont $\overline{1}$ et $\overline{-1}$, on a donc $\overline{(p-1)!} = \overline{-1}\ \overline{1}\ \overline{1}^{\frac{p-3}{2}} = \overline{-1}$, d'où $(p-1)! \equiv -1[p]$. □

Remarque 3.3.1. Cependant, ce test est impraticable en terme de complexité algorithmique, puisque le calcul de la fonction factorielle est de complexité linéaire en nombre de produits.

Enfin, on peut appliquer la théorie des anneaux $\mathbb{Z}/_{n\mathbb{Z}}$ pour montrer une version affaiblie du théorème de Fermat. En effet, à propos du grand théorème de Fermat, une direction de recherche était le principe de Hasse, consistant à montrer l'existence de solutions dans un sens plus faible et remonter ce résultat pour montrer le résultat fort. Depuis 1994, on sait que le grand théorème de Fermat est vrai grâce à la preuve de Andrew Wiles.

Théorème 3.4 (de Fermat modulaire)**.** *Pour tout $r > 0$, il existe $N_r > 0$ tel que pour tout $p > N_r$ premier, $x^r + y^r = z^r$ admet une solution non triviale ($xyz \neq 0$) dans $\mathbb{Z}/_{p\mathbb{Z}}$.*

Démonstration. Ce théorème est un lemme de Schur déguisé, qui est :

Lemme 3.1. Soit $r \in \mathbb{N}^*$, il existe N_r tel que pour tout $n > N_r$ et toute application $\sigma : [\![1; n]\!] \to \{c_1, ...c_r\}$, il existe $x, y, z \in [\![1; n]\!]$ tels que $x + y = z$ et $\sigma(x) = \sigma(y) = \sigma(z)$.

□

Théorème 3.5 (des deux carrés)**.** *p premier impair est somme de deux carrés d'entiers si et seulement si $p \equiv 1[4]$.*

4 Applications

Nous allons appliquer les résultats des trois premières parties ici. D'abord, nous étudierons les résidus quadratiques modulo p, puis nous les utiliserons pour étudier la primalité des nombres de Mersenne, avant de parler de cryptographie asymétrique.

4.1 Résidus quadratiques

Le problème de savoir si un nombre est le carré d'un autre est appelé problème de résidualité quadratique (ou résiduosité). C'est un problème réputé difficile, qui est souvent utilisé comme hypothèse de complexité de problèmes. Nous allons présenter les outils nécessaires à ce calcul en se basant sur la factorisation de notre nombre.

Définition 4.1. Pour p premier, on appelle symbole de Legendre le nombre

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } p|a \\ 1 \text{ si } \exists k \in \mathbb{Z}, a \equiv k^2[p] \\ -1 \text{ sinon.} \end{cases}$$

Proposition 4.1 (Critère d'Euler)**.**

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$$

pour $p > 2$ premier.

Lemme 4.1. Il y a $\frac{p-1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.

Démonstration du lemme. Il y en a déjà moins de $\frac{p-1}{2}$, puisque $\overline{x}^2 = \overline{-x}^2$. De plus, si $\overline{x}^2 = \overline{y}^2$, alors $(\overline{x} - \overline{y})(\overline{x} + \overline{y}) = 0$ d'où $\overline{x} = \pm\overline{y}$. Ainsi, nos $\frac{p-1}{2}$ carrés sont distincts. □

Démonstration. Soit $c = a^{\frac{p-1}{2}}$. Alors :

- Si $p|a$, alors $p|c$.
- Si $a \equiv b^2 \not\equiv 0$, alors $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1$ par le petit théorème de Fermat.
- Supposons que a n'est pas un carré modulo p. Puisque l'on a déjà traité le cas des $\frac{p-1}{2}$ carrés modulo p, a ne peut pas être racine de $X^{\frac{p-1}{2}} - 1$. Or a est racine de $X^{p-1} - 1$, par le théorème de Fermat, et $(X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1) = X^{p-1} - 1$. Ainsi, $a^{\frac{p-1}{2}} \equiv -1$.

□

Théorème 4.1 (loi de réciprocité quadratique)**.** *Soient p et q deux entiers impairs distincts. Alors :*

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

On admet pour ce théorème la classification des formes quadratiques dans un corps fini, qui dit qu'il y a deux classes d'équivalence de formes quadratiques non dégénérées, de matrices $\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \alpha \end{pmatrix}$ où α n'est pas un carré.

Démonstration. On peut le démontrer par un lemme de dénombrement montrant que :

$$\left|\{x \in \mathbb{F}_p, ax^2 + 1 \equiv 0[p]\}\right| = 1 + \left(\frac{a}{p}\right)$$

qui est juste une étude de cas. Ensuite, on va dénombrer X la boule unité de la forme quadratique canonique sur $(\mathbb{F}_q)^p$, notée $\phi : x \to x_1^2 + ... + x_p^2$, et la boule unité d'une autre forme quadratique, et enfin nous montrerons qu'elles seront de même taille.

— Faisons agir $\mathbb{F}_p$ sur X par rotation :

$$\psi : \left\{ \begin{array}{ccc} \mathbb{F}_p \times X & \to & X \\ \alpha, x & \mapsto & (x_{1+\alpha}, ...x_{p+\alpha}) \end{array} \right.$$

La relation orbite stabilisateur nous dit que $p = |Orb(x)||Stab(x)|$ pour $x \in X$. Or, puisque p est premier, on a deux cas :

— $|Orb(x)| = 1$ et $|Stab(x)| = p$. Alors $Stab(x) = \mathbb{F}_p$, et donc $x_1 = ... = x_p$. Or $\psi(x) = px_1^2$, on en a donc $1 + \left(\frac{p}{q}\right)$.

— $|Orb(x)| = p$ et $|Stab(x)| = 1$.

Puisque $X = \sqcup Orb(x)$, on a $|X| \equiv 1 + \left(\frac{p}{q}\right)\ [p]$.

— Définissons une nouvelle forme quadratique $\phi' : x \to 2(x_1x_2 + x_3x_4 + ... + x_{p-2}x_{p-1}) + (-1)^{\frac{p-1}{2}}x_p^2$, et notons X' sa boule unité. $det(\phi) = 1$, et la matrice de cette forme quadratique dans la base canonique est :

$$A = \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & \ddots & & \\ & & & & (-1)^{\frac{p-1}{2}} \end{pmatrix}$$

Donc $det(\phi') = (-1)^{\frac{p-1}{2}} \times (-1)^{\frac{p-1}{2}} = 1 = det(\phi)$. Par le théorème de classification des formes quadratiques dans $\mathbb{F}_p$, ces deux formes sont équivalentes, donc leurs boules unités sont en bijection. Ainsi, $|X| = |X'|$.

— Enfin, déterminons la taille de $|X'|$. Distinguons les cas de $x \in X'$.

— Si $x_1, x_3...x_{p-2} = 0$, alors on peut choisir arbitrairement $x_2, ...x_{p-1}$ et on a $(-1)^{\frac{p-1}{2}}x_p^2 = 1$. On a donc $q^{\frac{p-1}{2}}(1 + \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right))$.

— Sinon, choisissons arbitrairement x_p et les $x_1, x_3...x_{p-2}$ non tous nuls. Alors les $(x_2, x_4, ...x_{p-1})$ sont exactement les éléments d'un hyperplan affine de $\mathbb{F}_q^p$, de cardinal $q^{\frac{p-1}{2}-1}$. Ainsi, on a $q(q^{\frac{p-1}{2}} - 1)q^{\frac{p-1}{2}-1}$ cas.

On a donc :

$$\begin{aligned} |X'| &= |X| \\ &\equiv 1 + \left(\frac{p}{q}\right) [p] \end{aligned}$$

D'où :

$$q^{\frac{p-1}{2}}(1 + \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)) + q(q^{\frac{p-1}{2}} - 1)q^{\frac{p-1}{2}-1} \equiv 1 + \left(\frac{p}{q}\right) [p]$$

Par le critère d'Euler :

$$\left(\frac{q}{p}\right)(1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}) + q^{p-1} - q^{\frac{p-1}{2}} \equiv 1 + \left(\frac{p}{q}\right) [p]$$

Par le critère d'Euler et le petit théorème de Fermat :

$$\left(\frac{q}{p}\right) + \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} + 1 - \left(\frac{q}{p}\right) \equiv 1 + \left(\frac{p}{q}\right) [p]$$

$$\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) [p]$$

Cette relation est vraie modulo p, or les deux termes sont égaux dans $\mathbb{Z}$ à ± 1, et $p > 2$, donc l'égalité est aussi vraie dans $\mathbb{Z}$:

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

□

Proposition 4.2. *La loi de réciprocité quadratique nous donne un critère pour que 3 soit un carré modulo p, ce qui nous servira pour déterminer la primalité des nombres de Mersenne dans la prochaine partie.*

4.2 Recherche de nombre premiers

Puisqu'il n'existe pas de plus grand nombre premier, on peut toujours chercher des nombres premiers de plus en plus grand. Ils servent notamment à tester des propriétés sur les nombres premiers n'ayant pas été formellement vérifiées. Les records de plus grands nombres premiers sont depuis 30 ans des nombres de Mersenne, de la forme $2^n - 1$. Le record actuel est d'ailleurs $M_{82589933} = 2^{82589933} - 1$. Nous pouvons donner un critère de primalité des nombres de Mersenne utilisant nos anneaux $\mathbb{Z}/_{n\mathbb{Z}}$.

Définition 4.2. Un nombre de Mersenne est un nombre entier de la forme $M_n = 2^n - 1$.

Remarque 4.2.1. Si $n = ab$ n'est pas premier, alors $M_n = (2^a - 1)(2^{a(b-1)} + ... + 2^a + 1)$. Donc une condition nécessaire pour que M_n soit premier est que n soit premier. Dans la suite, nous prendrons q premier impair.

Théorème 4.2 (critère de primalité des nombres de Mersenne)**.** *M_q est premier si et seulement si* $(2+\sqrt{3})^{2^{q-1}} \equiv -1[M_q]$.

Remarque 4.2.1. Si 3 est un carré modulo M_q, cette égalité se place naturellement dans $\mathbb{Z}/M_q\mathbb{Z}$. Sinon, on peut simplement se placer dans $\mathbb{Z}/M_q\mathbb{Z}[X]/\langle X^2 - 3\rangle$.

Démonstration. Prouvons les deux sens de cet implication. Pour le sens direct, la stratégie de notre démonstration va être d'abord de déterminer dans quel cas de la remarque nous sommes, puis on utilise le morphisme de Frobenius et le critère d'Euler. Pour le sens réciproque, on va prendre un diviseur premier de M_q et montrer qu'il est égal à M_q en étudiant l'ordre de $\alpha = 2 + \sqrt{3}$.

— D'abord, supposons que q est premier impair et M_q premier. Montrons d'abord un lemme :
Lemme 4.2. Si 3 est un carré modulo $p > 3$ premier, alors $p \equiv \pm 1[12]$.

Démonstration du lemme. Par la loi de réciprocité quadratique, on a $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$. Supposons donc que 3 est un carré modulo p. Alors on a $(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right)$. Or seul 1 est un carré modulo 3 (puisque $2^2 \equiv 1[3]$). Ainsi, on a deux cas :
— Si $p \equiv 1[3]$, alors $(-1)^{\frac{p-1}{2}} = 1$ et donc $\frac{p-1}{2}$ pair, i.e. $p \equiv 1[4]$. Par le lemme chinois, $p \equiv 1[12]$.
— Sinon, $p \equiv -1[4]$ (car p est supposé impair), donc $(-1)^{\frac{p-1}{2}} = -1$ i.e. $p \equiv -1[4]$. Par le lemme chinois, $p \equiv -1[12]$.
On a donc bien $p \equiv \pm 1[12]$. □

Montrons donc par récurrence que $M_q \not\equiv \pm 1[12]$. Notons $\mathcal{P}(\backslash)$ la propriété "$M_n \equiv 7[12]$, et montrons la sur les impairs.
— Pour $n = 3$, $M_3 = 7 \equiv 7[12]$.

— Supposons $\mathcal{P}(n)$, $n > 1$ impair. Alors :

$$\begin{aligned} M_{n+2} &= 2^{n+2} - 1 \\ &= (2^n - 1)2^2 + 2^2 - 1 \\ &\equiv 7 * 4 + 3[12] \\ &\equiv 7[12] \end{aligned}$$

Ainsi, 3 n'est pas un carré modulo M_q. Si l'on veut donner sens à la deuxième équation, nous devons donc nous placer dans le corps de rupture $\mathbb{F}_p[X]/\langle X^2 - 3\rangle$, et choisissons $\sqrt{3} = \overline{X}$. Remarquons d'ailleurs que 2 est un carré modulo M_q, puisque $2M_q = 2^{q+1} - 2 \equiv 0[M_q]$, et $q + 1$ pair. On peut donc noter $\sqrt{2} = \overline{2}^{\frac{q+1}{2}}$.

— Notons $\rho = \frac{1+\sqrt{3}}{\sqrt{2}}, \overline{\rho}\frac{1-\sqrt{3}}{\sqrt{2}}$. On a $\rho^2 = \frac{1+2\sqrt{3}+3}{2} = 2 + \sqrt{3}$, d'où :

$$\begin{aligned} (2+\sqrt{3})^{2^{q-1}} &= (\rho^2)^{2^{q-1}} \\ &= \rho \left(\frac{1+\sqrt{3}}{\sqrt{2}}\right)^{M_q} \\ &= \rho \left(\left(\frac{1}{\sqrt{2}}\right)^{M_q} + \left(\frac{\sqrt{3}}{\sqrt{2}}\right)^{M_q}\right) \\ &\quad \text{car } \mathbb{F}_{M_q}[X]/\langle X^2 - 3\rangle \text{ est de caractéristique } M_q \end{aligned}$$

Or par le critère d'Euler, puisque 2 est un carré modulo M_q et pas 3, on a $\sqrt{2}^{M_q} = 2^{\frac{M_q-1}{2}} * \sqrt{2} = \sqrt{2}$ et $\sqrt{3}^{M_q} = 3^{\frac{M_q-1}{2}}\sqrt{3} = -\sqrt{3}$. Ainsi,

$$(2+\sqrt{3})^{2^{q-1}} = \rho\frac{1-\sqrt{3}}{\sqrt{2}} = \frac{1-3}{2} = -1$$

dans $\mathbb{F}_{M_q}[X]/\langle X^2 - 3\rangle$.

— Montrons maintenant le sens réciproque. Supposons donc que $(2 + \sqrt{3})^{2^{q-1}} = -1$. Ici, $\sqrt{3}$ sera une racine de 3 s'il est un carré modulo M_q, la classe de X dans $\mathbb{Z}/_{M_q\mathbb{Z}}[X]/\langle X^2 - 3\rangle$, et notons $\mathcal{A}$ cet anneau. Soit p un facteur premier de M_q. Alors p est un diviseur de 0 dans $\mathcal{A}$. Notons donc $\mathcal{M}$ un idéal maximal de $\mathcal{A}$ contenant p. Cet idéal existe puisque l'anneau est fini, il suffit de partir de la famille p, puis y ajouter des éléments hors de l'idéal engendré tant qu'il en existe et que l'idéal engendré n'est pas $\mathcal{A}$ tout entier. Alors, puisque $\mathcal{M}$ est maximal, $\mathcal{A}/_{\mathcal{M}}$ est un corps. Ce corps est de caractéristique p, puisque

p est premier et $\overline{p} = \overline{0}$ dans $\mathcal{A}/\mathcal{M}$.
Posons donc $\alpha = 2 + \sqrt{3}, \beta = 2 - \sqrt{3}$. On a $\alpha^{2^{q-1}} = -1$ dans $\mathcal{A}$ donc aussi dans $\mathcal{A}/\mathcal{M}$. Puisque $\alpha^{2^q} = 1$, $o(\alpha)|2^q$ donc l'ordre est une puissance de 2. Or $\alpha^{2^{q-1}} \neq 1$, donc α est d'ordre 2^q.
Notons $Q(X) := (X-\alpha)(X-\beta) = X^2-(\alpha+\beta)X+\alpha\beta = X^2-4X+1$. Puisque α est racine de Q et que p est caractéristique de $\mathcal{A}/\mathcal{M}$, on a α^p aussi racine de Q. Or les deux racines de Q sont α et β, donc $\alpha^p = \alpha$ ou $\alpha = \beta$.

— Si $\alpha^p = \alpha$, puisque α est inversible (car $-1 = \alpha^{2^{q-1}}$ est inversible, $\alpha^{p-1} = 1$. Or α est d'ordre 2^q, donc $2^q|p-1$. Or $p|M_q = 2^q - 1$, on a donc une contradiction.

— On a donc $\alpha^p = \beta$. Or, $\alpha\beta = 4 - 3 = 1$, donc $\alpha^{p+1} = 1 = \alpha^{2^q}$, d'où $\alpha^p = \alpha^{M_q}$. Ainsi, $\alpha^{M_q - p} = 1$. On a donc $2^q|(M_q - p) < 2^q$, donc $M_q = p$.

Ainsi, $M_q = p$ et donc M_q premier.

□

Remarque 4.2.2. Cette méthode nous donne un test de primalité parfait sur les nombres de Mersenne. Il est cependant de complexité temporelle élevée, à cause de la taille de l'exposant. On peut le ramener à un algorithme de test de primalité de complexité cubique.

Théorème 4.3 (test de Lehmer-Lucas)**.** *Soit la suite L_n définie par :*

$$\begin{cases} L_0 & = 4 \\ L_{n+1} & = L_n^2 - 2[M_q] \end{cases}$$

Alors M_q est premier si et seulement si $L_{q-2} \equiv 0[M_q]$.

Démonstration. Gardons la notation $\alpha = 2 + \sqrt{3}$ et $\beta = 2 - \sqrt{3}$. Montrons par récurrence sur n que $\alpha^{2^n} + \beta^{2^n}$ est dans $\mathbb{Z}/M_q\mathbb{Z}$, c'est à dire que les termes en $\sqrt{3}$ s'annulent, et qu'il est égal à L_n modulo M_q.

— Pour $n = 0$, $\alpha^{2^0} + \beta^{2^0} = \alpha + \beta = 4 = L_0 \in \mathbb{Z}/M_q\mathbb{Z}$.

— Supposons la propriété vraie en $n >= 0$. Alors $\alpha^{2^{n+1}} + \beta^{2^{n+1}} = \left(\alpha^{2^n} + \beta^{2^n}\right)^2 - 2\alpha^{2^n}\beta^{2^n}$. Or $\alpha\beta = 1$, donc $\alpha^{2^{n+1}} + \beta^{2^{n+1}} = L_n^2 - 2 \in \mathbb{Z}/M_q\mathbb{Z}$.

On a donc :

$$\begin{aligned} L_{q-2} = 0[M_q] &\Leftrightarrow \alpha^{2^{q-2}} + \beta^{2^{q-2}} = 0 \\ &\Leftrightarrow \alpha^{2^{q-2}} = -\alpha^{-2^{q-2}} \\ &\Leftrightarrow \alpha^{2^{q-1}} = -1 \\ &\Leftrightarrow M_q \text{ premier par le critère de primalité précédent.} \end{aligned}$$

□

Application 4.3.1. Le test de Lehmer-Lucas se généralise au test de Lehmer-Lucas-Riesel, qui vérifie la primalité de $N = k * 2^{n-1}$, pour $k < 2^n$. Ce test est le même que Lehmer-Lucas à l'exception de L_0, qui va dépendre de k.

Remarque 4.3.1. Dans le cas général, on sait depuis 2002 que le problème de primalité est polynomial en la taille de l'entrée par le test de Agrawal–Kayal–Saxena. Dans la pratique, quand on a besoin de trouver un grand nombre premier, on utilise des techniques probabilistes, comme celle de Miller-Rabin.

4.3 Cryptographie à clé publique : le système RSA

Définition 4.3. Soient p, q premiers distincts, et $n = pq$. L'objectif est d'avoir une fonction à sens unique, qui est facile à calculer dans un sens mais difficile dans le sens opposé. Ainsi, muni de la clé publique (représentant la fonction), n'importe qui peut envoyer un message que seul le possesseur de la clé privée (représentant la fonction inverse). Pour cela, nous allons utiliser le théorème d'Euler.

Proposition 4.3. *Choisissons e inversible modulo $\varphi(n) = (p-1)(q-1)$, d'inverse d. La fonction de chiffrement est alors $M \in \mathbb{Z}/n\mathbb{Z} \to M^e[n]$. Alors, la fonction de déchiffrement est $C \in \mathbb{Z}/n\mathbb{Z} \to C^d[n]$.*

Remarque 4.3.1. On peut donc représenter :
- la clé publique par (n, e),
- la clé privée par (d, n).

Dans la pratique, on utilisera des algorithmes d'exponentiation modulaire (au lieu de calculer M^e puis le passer au modulo, on effectue l'exponentiation directement dans $\mathbb{Z}/n\mathbb{Z}$). De plus, au lieu d'effectuer le déchiffrement dans $\mathbb{Z}/n\mathbb{Z}$, on peut faire l'exponentiation dans $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ avant de calculer le message chiffré grâce au théorème chinois.

Remarque 4.3.2. En pratique, p, q doivent être très grand pour résister à des attaques directes. Pour trouver nos nombre premier à n bits (en pratique entre 1024 et 2048 bits), on génère des nombres aléatoires uniformément à n bits jusqu'à en trouver un passant un test de primalité (si ce test n'est pas parfait, ce sera un nombre pseudo-premier, ou premier de qualité industrielle). Il doit être suffisament grand pour que $n = pq$ soit difficile à factoriser sans connaître p et q. D'autres conditions sont nécessaires sur p, q et e, notamment pour résister à des attaques ρ ou $\rho - 1$ de Pollard.

Remarque 4.3.3. La sécurité de ce système n'est sans doute pas encore mise à mal du côté mathématiques. Ce sont plutôt les implémentations qui peuvent être faibles, comme les algorithmes de générations de grands premiers (1989 - Wiener), ou les algorithmes de restes chinois (2003, Boneh - Brumley). Par ailleurs, l'algorithmique quantique donne des algorithmes permettant de casser RSA (dans l'hypothèse où l'on a un ordinateur quantique raisonnablement puissant) comme l'algorithme de Shor (cubique en nombre de bits en temps, et linéaire en nombre de bits en espace). Il existe déjà des pistes de cryptosystème asymétrique supposés résistant à l'algorithmique quantique, qui remplace l'anneau $\mathbb{Z}/_{n\mathbb{Z}}$ par des courbes elliptiques.

Remarque 4.3.4. Les applications de ce système sont nombreuses en terme de sécurité : on peut citer le problème de signature électronique (transmettre un message en le chiffrant de manière à cacher le contenu du message aux attaquants et de manière à assurer au destinataire de son identité), ou encore dans un protocole d'échange de clés (on échange des clés d'un protocole de chiffrement symétrique, nettement moins coûteux que le chiffrement asymétrique, de manière à ce qu'un attaquant ne puisse pas y avoir accès).

Références