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

Chapitre II - Loi de Réciprocité quadratique

Table des matières

1. Symbole de Legendre

Soient m et n des entiers ≥ 1. On dit que m est un résidu quadratique modulo n si $m + n\mathbb{Z}$ est un carré dans $\mathbb{Z}/n\mathbb{Z}$, autrement dit, s'il existe $a \in \mathbb{Z}$ tel que l'on ait

$$m \equiv a^2 \text{ mod. } n.$$

Dans ce cas, on dit aussi que m est un carré modulo n.

Définition 2.1. *Soient p un nombre premier et n un entier relatif. On note $\left(\frac{n}{p}\right)$ l'entier défini comme suit. On a :*
1) $\left(\frac{n}{p}\right) = 0$ si p divise n.
2) $\left(\frac{n}{p}\right) = 1$ si p ne divise pas n et si n est un résidu quadratique modulo p.
3) $\left(\frac{n}{p}\right) = -1$ si n n'est pas un résidu quadratique modulo p.

L'expression $\left(\frac{n}{p}\right)$ s'appelle le symbole de Legendre. L'entier $\left(\frac{n}{p}\right)$ ne dépend que de la classe de n modulo p.

Exemples 2.1.

1) On a $\left(\frac{n}{2}\right) = 1$ si n est impair et $\left(\frac{n}{2}\right) = 0$ si n est pair. On a ainsi $\left(\frac{n}{2}\right) \equiv n$ mod. 2.

2) Vérifions la congruence

$$\left(\frac{n}{3}\right) \equiv n \text{ mod. } 3.$$

Si 3 divise n, on a $\left(\frac{n}{3}\right) = 0$. Si $n \equiv 1$ mod. 3 on a $\left(\frac{n}{3}\right) = 1$. Si $n \equiv -1$ mod. 3, vu que -1 n'est pas un carré modulo 3, on obtient $\left(\frac{n}{3}\right) = \left(\frac{-1}{3}\right) = -1$, d'où la formule annoncée.

Proposition 2.1. *Soit p un nombre premier impair. On a*

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

Ainsi, -1 est un carré modulo p si et seulement si on a $p \equiv 1$ mod. 4.

Démonstration : Supposons $\left(\frac{-1}{p}\right) = 1$. Il existe $n \in \mathbb{Z}$ tel que l'on ait $-1 \equiv n^2$ mod. p. Le sous-groupe de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ engendré par la classe de n est d'ordre 4, d'où $p \equiv 1$ mod. 4. Inversement, si 4 divise $p-1$, le groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ étant cyclique, il possède un sous-groupe cyclique d'ordre 4. Si x est un générateur de ce sous-groupe, on a $x^2 = -1$, d'où $\left(\frac{-1}{p}\right) = 1$. Par suite, on a $\left(\frac{-1}{p}\right) = 1$ si et seulement si p est congru à 1 modulo 4, ce qui entraîne (1).

2. Le critère d'Euler

Il permet de calculer le symbole de Legendre.

Théorème 2.1 (Critère d'Euler). *Soit p un nombre premier impair. Pour tout entier relatif n, on a*

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

Démonstration : Commençons par établir le lemme suivant :

Lemme 2.1. *Soit p un nombre premier impair. L'ensemble des carrés de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ est un sous-groupe de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ d'ordre $\frac{p-1}{2}$.*

Démonstration : L'application $\left(\mathbb{Z}/p\mathbb{Z}\right)^* \to \left(\mathbb{Z}/p\mathbb{Z}\right)^*$qui à x associe x^2 est un morphisme de groupes. Son noyau est $\{\pm 1\}$. Il est d'ordre 2 car $p \neq 2$. L'image de ce morphisme, qui est le sous-groupe des carrés de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$, est donc d'ordre $\frac{p-1}{2}$.

Le théorème 2.1 se déduit comme suit. Soit n un entier relatif. La congruence (2) est vraie si p divise n. Supposons que p ne divise pas n. On a $n^{p-1} \equiv 1$ mod. p. Puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, on a donc

$$n^{\frac{p-1}{2}} \equiv \pm 1 \text{ mod. } p. \tag{3}$$

Par ailleurs, le polynôme $X^{\frac{p-1}{2}} - 1 \in \left(\mathbb{Z}/p\mathbb{Z}\right)[X]$ a au plus $\frac{p-1}{2}$ racines. On déduit du lemme 2.1 que ses racines sont exactement les $\frac{p-1}{2}$ carrés de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$. On obtient l'équivalence

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

La condition (3) entraîne alors le résultat.

Remarque 2.1. Soit p un nombre premier impair. Parmi les entiers compris entre 1 et $p-1$, il y en a exactement la moitié qui sont des résidus quadratiques modulo p (lemme 2.1). On a donc la formule

$$\sum_{k=1}^{p-1}\Big(\frac{k}{p}\Big) = 0. \tag{4}$$

Exemple 2.2. Le critère d'Euler permet de calculer $\big(\frac{n}{p}\big)$ en utilisant le calcul « rapide » de la puissance d'un entier. Par exemple, on obtient que $\big(\frac{5}{23}\big) = -1$ en écrivant que l'on a

$$11 = 2^3 + 2 + 1 \quad \text{puis} \quad 5^{11} = 5^{2^3} \times 5^2 \times 5 \equiv -1 \text{ mod. } 23.$$

Corollaire 2.1. *Soit p un nombre premier. Quels que soient les entiers m et n, on a*

$$\Big(\frac{mn}{p}\Big) = \Big(\frac{m}{p}\Big)\Big(\frac{n}{p}\Big). \tag{5}$$

De plus, si n n'est pas divisible par p, on a

$$\Big(\frac{mn^2}{p}\Big) = \Big(\frac{m}{p}\Big). \tag{6}$$

Démonstration : Si $p = 2$, l'égalité (5) provient du fait que mn est pair si et seulement si m ou n l'est. Si $p \neq 2$, elle se déduit du critère d'Euler. Quant à l'égalité (6), elle résulte de (5) et de la définition du symbole de Legendre.

Remarque 2.2. On peut déduire de la formule (5) l'énoncé suivant :

Proposition 2.2. *Soit p un nombre premier impair. Soit n le plus petit entier naturel qui ne soit pas un résidu quadratique modulo p. On a*

$$n < 1 + \sqrt{p}.$$

Démonstration : Soit m le plus petit entier naturel tel que $mn > p$. Puisque p est premier, on a donc $n(m-1) < p$ i.e. $mn - p < n$. D'après le caractère minimal de n, on a donc avec la formule (5) les égalités

$$1 = \Big(\frac{mn-p}{p}\Big) = \Big(\frac{mn}{p}\Big) = \Big(\frac{m}{p}\Big)\Big(\frac{n}{p}\Big) = -\Big(\frac{m}{p}\Big).$$

Par suite, on a $m \geq n$. Le résultat s'ensuit vu que l'on a

$$(n-1)^2 < n(n-1) \leq n(m-1) < p.$$

Citons à ce propos la conjecture de Vinogradov :

Conjecture. *Soit ε un nombre réel > 0. Pour tout nombre premier p assez grand, le plus petit entier naturel qui ne soit pas un résidu quadratique modulo p est inférieur à p^{ε}.*

Par exemple, Hudson et Williams ont démontré en 1979 que si p est un nombre premier impair non congru à 1 modulo 8, le plus petit entier naturel n qui ne soit pas un résidu quadratique modulo p est inférieur à $p^{\frac{2}{5}} + 12p^{\frac{1}{5}} + 33$. On a ainsi $n < 1,54\ p^{\frac{2}{5}}$ dès que p (non congru à 1 modulo 8) est plus grand que 10^7.

Exemple 2.3. Soient p un nombre premier impair et n un entier non divisible par p. Afin de calculer le symbole $\left(\frac{n}{p}\right)$, on peut utiliser la méthode suivante. Posons $a = n + p\mathbb{Z}$. Supposons donné un anneau commutatif A, contenant le corps $\mathbb{Z}/p\mathbb{Z}$, dans lequel a soit un carré. Soit b un élément de A tel que $a = b^2$. Puisque a est inversible dans A, il en est de même de b. Par suite, on a

$$n^{\frac{p-1}{2}} + p\mathbb{Z} = a^{\frac{p-1}{2}} = \frac{b^p}{b}.$$

On a donc $b^p = \pm b$ et d'après le critère d'Euler on obtient

$$\left(\frac{n}{p}\right) = 1 \quad \text{si} \quad b^p = b \quad \text{et} \quad \left(\frac{n}{p}\right) = -1 \quad \text{si} \quad b^p = -b. \tag{7}$$

Tout revient alors à calculer b^p.
Voyons dans cette direction comment déterminer $\left(\frac{5}{p}\right)$. En suivant une démonstration de Gauss de la loi de réciprocité quadratique (voir après), l'idée est de prendre pour A l'anneau quotient

$$A = \big(\mathbb{Z}/p\mathbb{Z}\big)[X]/(\Phi_5) \quad \text{où} \quad \Phi_5 = \sum_{j=0}^{4} X^j \in \big(\mathbb{Z}/p\mathbb{Z}\big)[X].$$

(Φ_5 est le cinquième polynôme cyclotomique.) On identifie $\mathbb{Z}/p\mathbb{Z}$ à un sous-anneau de A, via la flêche $n + p\mathbb{Z} \mapsto n1_A$ où $1_A = 1 + (\Phi_5)$. Notons α la classe de X modulo Φ_5. On a $\alpha^5 = 1$. Considérons « la somme de Gauss »

$$b = \sum_{i=1}^{4} \Big(\frac{i}{5}\Big)\alpha^i.$$

Dans A, on vérifie que l'on a

$$b^2 = 5.$$

En tenant compte du fait que $p1_A = 0$, on constate que l'on a

$$b^p = b \quad \text{si} \quad p \equiv \pm 1 \text{ mod. } 5 \quad \text{et} \quad b^p = -b \quad \text{si} \quad p \equiv \pm 2 \text{ mod. } 5.$$

D'après (7), on obtient

$$\left(\frac{5}{p}\right) = 1 \quad \text{si} \quad p \equiv \pm 1 \text{ mod. } 5 \quad \text{et} \quad \left(\frac{5}{p}\right) = -1 \quad \text{si} \quad p \equiv \pm 2 \text{ mod. } 5.$$

Pour tout p premier impair, on a ainsi la relation

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right). \tag{8}$$

La formule (8) est un cas particulier de la loi de réciprocité quadratique, qui affirme que pour tous nombres premiers impairs p et q distincts, on a

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

Il existe plus de deux cent vingt preuves connues de ce résultat. On en donnera deux. Une dans laquelle interviennent des sommes de racines l'unité, appelées sommes de Gauss, analogues à celle de l'exemple précédent. Une autre, due à Eisenstein, qui utilise un lemme de trigonométrie. Auparavant, on va établir la formule permettant de calculer le symbole $\left(\frac{2}{p}\right)$, et en donner des exemples d'applications.

3. Le symbole $\left(\frac{2}{p}\right)$

Proposition 2.3. *Soit p un nombre premier impair. On a*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{9}$$

Ainsi, 2 est un carré modulo p si et seulement si on a $p \equiv \pm 1$ mod. 8.

Démonstration : Posons

$$S = \left\{1, \cdots, \frac{p-1}{2}\right\}.$$

Étant donné $a \in \mathbb{Z}$ non divisible par p, pour tout $s \in S$ il existe un unique élément $s_a \in S$ tel que l'on ait

$$as \equiv e_s(a)s_a \text{ mod. } p \quad \text{avec} \quad e_s(a) = \pm 1.$$

Lemme 2.2 (Gauss). *Soit a un entier relatif non divisible par p. On a*

$$\left(\frac{a}{p}\right) = \prod_{s \in S} e_s(a).$$

Démonstration : Vérifions que l'application $f : S \to S$ définie par $f(s) = s_a$ est une bijection de S. Soient s et s' des éléments de S tels que $f(s) = f(s')$. On obtient

$e_s(a)s \equiv e_{s'}(a)s'$ mod. p, d'où $s \equiv \pm s'$ mod. p, ce qui implique $s = s'$. Par suite, f est injective, d'où l'assertion. Il en résulte que l'on a

$$a^{\frac{p-1}{2}} \prod_{s\in S} s = \prod_{s\in S}(as) \equiv \prod_{s\in S} e_s(a) \prod_{s\in S} s_a \text{ mod. } p,$$

d'où

$$a^{\frac{p-1}{2}} \prod_{s\in S} s \equiv \prod_{s\in S} e_s(a) \prod_{s\in S} s \text{ mod. } p,$$

puis la congruence

$$a^{\frac{p-1}{2}} \equiv \prod_{s\in S} e_s(a) \text{ mod. } p.$$

D'après le critère d'Euler, on obtient ainsi

$$\prod_{s\in S} e_s(a) \equiv \left(\frac{a}{p}\right) \text{ mod. } p,$$

d'où le résultat car les deux membres de cette congruence valent ± 1 et p est impair.

La proposition 2.3 se déduit comme suit. On utilise le lemme précédent avec $a = 2$. Pour tout $s \in S$, on a

$$e_s(2) = 1 \quad \text{si} \quad 2s \in S \quad \text{et} \quad e_s(2) = -1 \quad \text{sinon.}$$

Par suite, on a (lemme 2.2)

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

où $n(p)$ est le nombre d'entiers u tels que

$$\frac{p-1}{4} < u \leq \frac{p-1}{2}.$$

Supposons $p \equiv \pm 1$ mod. 8. On a $p = \pm 1 + 8k$ où $k \in \mathbb{N}$, et l'on vérifie que $n(p) = 2k$. Si l'on a $p = 3 + 8k$ où $k \in \mathbb{N}$, on obtient $n(p) = 2k + 1$. Si $p = -3 + 8k$ où $k \in \mathbb{N}$, on a $n(p) = 2k - 1$. Cela conduit à la formule (9).

Exemple 2.4. Démontrons qu'il existe une infinité de nombres premiers congrus à 7 modulo 8. Supposons le contraire. Soient $\{p_1, \cdots, p_n\}$ l'ensemble des nombres premiers congrus à 7 modulo 8. Posons

$$N = \left(4p_1 \cdots p_n\right)^2 - 2.$$

Soit p un diviseur premier impair de N. On a $2 \equiv \big(4p_1 \cdots p_n\big)^2$ mod. p, donc 2 est un carré modulo p. Par suite, on a $p \equiv \pm 1$ mod. 8 (prop. 2.3). Compte tenu de l'égalité

$$\frac{N}{2} = 8\big(p_1 \cdots p_n\big)^2 - 1,$$

il existe donc un diviseur premier q de N qui est congru à -1 modulo 8. Ainsi q est l'un des p_i, ce qui conduit à une contradiction.

Exemple 2.5. Voyons une illustration du critère d'Euler et de la proposition 2.3, concernant la primalité des nombres de Fermat

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

Prouvons que pour tout $n \geq 2$, les facteurs premiers de F_n sont congrus à 1 modulo 2^{n+2}. Soit p un facteur premier de F_n. On a

$$2^{2^n} \equiv -1 \text{ mod. } p \quad \text{et} \quad 2^{2^{n+1}} \equiv 1 \text{ mod. } p.$$

Par suite, l'ordre de 2 modulo p est 2^{n+1}. D'après le théorème de Lagrange, 2^{n+1} divise $p-1$. En particulier, on a $p \equiv 1$ mod. 8, d'où $\left(\frac{2}{p}\right) = 1$. D'après le critère d'Euler, on obtient

$$2^{\frac{p-1}{2}} \equiv 1 \text{ mod. } p,$$

donc 2^{n+1} divise $\frac{p-1}{2}$, d'où l'assertion. En testant les entiers congrus à 1 modulo 128, on constate par exemple que $2^{32} + 1$ est le produit de deux nombres premiers, avec l'égalité

$$2^{32} + 1 = 641 \times 6700417.$$

Exemple 2.6. Soit p un nombre premier. Supposons que p soit de la forme

$$p = 1 + 4q \quad \text{avec} \quad q \text{ premier.}$$

Vérifions que la classe de 2 est un générateur de $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$. Soit d l'ordre multiplicatif de 2 modulo p. Puisque q est premier, on $d \in \big\{1, 2, 4, q, 2q, 4q\big\}$. On a $p \neq 3$ et $p \neq 5$, d'où $d = q, 2q$ ou $4q$. Supposons $d \neq 4q$. Dans ce cas, on obtient la congruence

$$2^{\frac{p-1}{2}} \equiv 1 \text{ mod. } p.$$

D'après le critère d'Euler, 2 est donc un résidu quadratique modulo p. Cela conduit à une contradiction vu que p est congru à 5 modulo 8.

4. Sommes de Gauss

Soit q un nombre premier impair. Soient A un anneau commutatif, d'élément neutre multiplicatif $1 = 1_A$. Soit α un élément de A tels que

$$1 + \alpha + \cdots + \alpha^{q-1} = 0. \tag{10}$$

On a $\alpha^q = 1$, autrement dit α est une racine q-ième de l'unité. L'élément α^i et l'entier $\left(\frac{i}{q}\right)$ ne dépendent que de la classe de i modulo q. Considérons la somme de Gauss

$$\tau = \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \Big(\frac{i}{q}\Big)\alpha^i = \sum_{i=0}^{q-1} \Big(\frac{i}{q}\Big)\alpha^i.$$

Théorème 2.2. *1) On a l'égalité*

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

2) Soit p un nombre premier impair distinct de q. Supposons que l'on ait $p\alpha = 0$. On a

$$\tau^p = \Big(\frac{p}{q}\Big)\tau.$$

Commençons par établir le lemme suivant :

Lemme 2.3. *Soit k un entier non divisible par q. On a*

$$\sum_{i=1}^{q-1} \Big(\frac{i(i-k)}{q}\Big) = -1.$$

Démonstration : Pour tout i entre 1 et $q-1$, i est inversible modulo q. Notons i^{-1} son inverse modulo q compris entre 1 et $q-1$. On a (cor. 2.1)

$$\Big(\frac{i(i-k)}{q}\Big) = \Big(\frac{i^2(1-ki^{-1})}{q}\Big) = \Big(\frac{1-ki^{-1}}{q}\Big).$$

Par ailleurs, l'application $\big(\mathbb{Z}/q\mathbb{Z}\big)^* \to \mathbb{Z}/q\mathbb{Z} - \big\{1\big\}$ qui à la classe de i associe celle de $1 - ki^{-1}$ est une bijection. Par suite, on a

$$\sum_{i=1}^{q-1} \Big(\frac{i(i-k)}{q}\Big) = \sum_{\substack{i=0 \\ i\neq 1}}^{q-1} \Big(\frac{i}{q}\Big) = \sum_{i=1}^{q-1} \Big(\frac{i}{q}\Big) - \Big(\frac{1}{q}\Big).$$

La formule (4) entraîne alors le résultat.

Démonstration du théorème 2.2 : 1) On a (prop. 2.1)

$$(-1)^{\frac{q-1}{2}}\tau^2 = \Big(\frac{-1}{q}\Big)\tau^2 = \sum_{i,j}\Big(\frac{-1}{q}\Big)\Big(\frac{i}{q}\Big)\Big(\frac{j}{q}\Big)\alpha^i\alpha^j = \sum_{i,j}\Big(\frac{-ij}{q}\Big)\alpha^{i+j}.$$

Puisque $\mathbb{Z}/q\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$ est la réunion disjointe des ensembles

$$\Big\{(i,j)\in\mathbb{Z}/q\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}\;\Big|\; i+j=k+q\mathbb{Z}\Big\}\quad\text{pour}\quad k=0,\cdots,q-1,$$

on en déduit que

$$(-1)^{\frac{q-1}{2}}\tau^2 = \sum_{k=0}^{q-1} s_k\alpha^k \quad\text{avec}\quad s_k = \sum_{i=0}^{q-1}\Big(\frac{i(i-k)}{q}\Big).$$

On a $s_0 = q-1$. Si k n'est pas nul, on a $s_k = -1$ (lemme 2.3). D'après (10), on obtient

$$(-1)^{\frac{q-1}{2}}\tau^2 = (q-1) - \sum_{k=1}^{q-1}\alpha^k = q - \sum_{k=0}^{q-1}\alpha^k = q,$$

et l'égalité annoncée.

2) Compte tenu du fait que $p\alpha = 0$, on a

$$\tau^p = \left(\sum_{i\in\mathbb{Z}/q\mathbb{Z}}\Big(\frac{i}{q}\Big)\alpha^i\right)^p = \sum_{i\in\mathbb{Z}/q\mathbb{Z}}\Big(\frac{i}{q}\Big)^p\alpha^{ip} = \sum_{i\in\mathbb{Z}/q\mathbb{Z}}\Big(\frac{i}{q}\Big)\alpha^{ip}.$$

Par ailleurs, p est inversible modulo q, donc l'application qui à i associe ip est une bijection de $\mathbb{Z}/q\mathbb{Z}$. Il en résulte que l'on a

$$\Big(\frac{p}{q}\Big)\tau^p = \sum_{i\in\mathbb{Z}/q\mathbb{Z}}\Big(\frac{ip}{q}\Big)\alpha^{ip} = \sum_{j\in\mathbb{Z}/q\mathbb{Z}}\Big(\frac{j}{q}\Big)\alpha^j = \tau,$$

ce qui entraîne le résultat.

Exemple 2.7. Vérifions que l'on a

$$\tau = \sum_{i=0}^{q-1}\alpha^{i^2}. \tag{11}$$

Notons R l'ensemble des carrés de $\big(\mathbb{Z}/q\mathbb{Z}\big)^*$. On a les égalités

$$\tau = \sum_{i\in(\mathbb{Z}/q\mathbb{Z})^*}\Big(\frac{i}{q}\Big)\alpha^i = \sum_{i\in R}\alpha^i - \sum_{i\in(\mathbb{Z}/q\mathbb{Z})^*-R}\alpha^i.$$

Compte tenu de (10), on obtient

$$\tau = 2\sum_{i\in R}\alpha^i + 1.$$

Par ailleurs, on a

$$\sum_{i\in R}\alpha^i = \sum_{i=1}^{\frac{q-1}{2}}\alpha^{i^2} = \sum_{i=\frac{q+1}{2}}^{q-1}\alpha^{i^2},$$

d'où la formule (11).

5. La loi de réciprocité quadratique

Elle a été conjecturée par Euler en 1783, et a été démontrée par Gauss en 1796.

Théorème 2.3 (Gauss). *Soient p et q deux nombres premiers impairs distincts. On a*

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

Autrement dit, on a

$$\Big(\frac{p}{q}\Big) = \Big(\frac{q}{p}\Big) \quad \textit{si } p \textit{ ou } q \textit{ est congru à } 1 \textit{ modulo } 4,$$

$$\Big(\frac{p}{q}\Big) = -\Big(\frac{q}{p}\Big) \quad \textit{sinon.}$$

Démonstration : Posons

$$A = \big(\mathbb{Z}/p\mathbb{Z}\big)[X]/(\Phi_q) \quad \text{où} \quad \Phi_q = 1 + X + \cdots + X^{q-1}.$$

Rappelons que $\mathbb{Z}/p\mathbb{Z}$ s'identifie à un sous-anneau de A, via la flêche $n + p\mathbb{Z} \mapsto n1_A$ où $1_A = 1 + (\Phi_q)$. Soit α la classe de X modulo Φ_q. On a

$$1 + \alpha + \cdots + \alpha^{q-1} = 0.$$

Posons

$$\tau = \sum_{i\in\mathbb{Z}/q\mathbb{Z}}\Big(\frac{i}{q}\Big)\alpha^i.$$

On a (th. 2.2)

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

D'après le critère d'Euler, on a

$$\left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right) \equiv \Big((-1)^{\frac{q-1}{2}}q\Big)^{\frac{p-1}{2}} \text{ mod. } p.$$

On en déduit que l'on a dans A les égalités

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

Puisque $p = 0$ dans A, on a (*loc. cit.*)

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

Par ailleurs, q étant distinct de p, τ^2 est inversible dans A, donc τ l'est aussi, d'où l'égalité

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

Vu que p est impair, on obtient dans $\mathbb{Z}$ l'égalité

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

autrement dit,

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

ce qui entraîne le résultat car $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Exemples 2.8.

1) Vérifions que l'on a

$$\left(\frac{101}{641}\right) = -1.$$

En utilisant la loi de réciprocité, on obtient

$$\left(\frac{101}{641}\right) = \left(\frac{641}{101}\right) = \left(\frac{35}{101}\right) = \left(\frac{5}{101}\right)\left(\frac{7}{101}\right) = \left(\frac{101}{5}\right)\left(\frac{101}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -1.$$

2) Soit p un nombre premier congru à ± 2 modulo 5. Vérifions que l'équation

$$x^2 + py^2 = 5z^2$$

n'a pas de solutions dans $\mathbb{Z}^3$, autres que $(0, 0, 0)$. Soit (x, y, z) une solution non triviale. On peut supposer x, y et z premiers entre eux dans leur ensemble. Par suite, p ne divise pas z, donc 5 est un carré modulo p. On obtient une contradiction car

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1.$$

6. Symbole de Jacobi et réciprocité

Le symbole de Jacobi est une généralisation du symbole de Legendre.

Définition 2.2. *Soient m un entier relatif et n un entier naturel impair. On note $\left(\frac{m}{n}\right)$ l'entier défini comme suit.*

1) On a $\left(\frac{m}{1}\right) = 1$.

2) Supposons $n \geq 3$. Soit $n = p_1 \cdots p_r$ la décomposition de n en produit de nombres premiers, les facteurs n'étant pas nécessairement distincts. On pose

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

L'expression $\left(\frac{m}{n}\right)$ s'appelle le symbole de Jacobi. On peut aussi définir le symbole de Jacobi si n est pair. Le cas où n est impair nous suffira pour la suite, notamment en ce qui concerne les critères de primalité.

Proposition 2.4. *Soient m un entier relatif et n un entier naturel impair.*

1) On a $\left(\frac{m}{n}\right) = -1, 0$ ou 1.

2) On a $\left(\frac{m}{n}\right) = 0$ si et seulement si m et n ne sont pas premiers entre eux.

3) L'entier $\left(\frac{m}{n}\right)$ ne dépend que la classe de m modulo n.

4) Soient m' un entier relatif et n' un entier naturel impair. On a

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

5) Si m et n sont premiers entre eux, on a

$$\left(\frac{m^2}{n}\right) = 1 \quad et \quad \left(\frac{m}{n^2}\right) = 1.$$

Démonstration : Les trois premières assertions sont des conséquences directes des définitions des symboles de Legendre et de Jacobi. Soit $n = p_1 \cdots p_r$ la décomposition de n en produit de nombres premiers (éventuellement répétés). On a

$$\left(\frac{mm'}{n}\right) = \prod_{i=1}^{r} \left(\frac{mm'}{p_i}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right)\left(\frac{m'}{p_i}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right).$$

Quant à la seconde égalité de l'assertion 4, on l'obtient en considérant les décompositions en facteurs premiers de n et n'. La dernière assertion se déduit des assertions 1, 2 et 4.

Remarques 2.3.

1) L'égalité $\left(\frac{m}{n}\right) = 1$ n'implique pas que m soit un carré modulo n. Par exemple, on a

$$\left(\frac{14}{51}\right) = \left(\frac{14}{3}\right)\left(\frac{14}{17}\right) = \left(\frac{-1}{3}\right)\left(\frac{-3}{17}\right) = 1,$$

pour autant 14 n'est pas un carré modulo 51, vu que ce n'est déjà pas un carré modulo 3. Cela étant, l'égalité $\left(\frac{m}{n}\right) = -1$ entraîne que m n'est pas un carré modulo n.

2) Si n est un nombre premier impair, on a $\left(\frac{m}{n}\right) \equiv m^{\frac{n-1}{2}}$ mod. n (critère d'Euler). Ce n'est plus vrai si n n'est pas premier. Par exemple, on a

$$\left(\frac{14}{51}\right) = 1 \quad \text{et} \quad 14^{25} \equiv 20 \text{ mod. } 51.$$

Vérifions cette congruence. On a $14^{25} \equiv -1$ mod. 3 (en particulier $14^{25} \not\equiv 1$ mod. 51) et $14^{25} \equiv (-3)^{25}$ mod. 17. D'après le petit théorème de Fermat, on a $(-3)^{16} \equiv 1$ mod. 17, d'où $14^{25} \equiv -3^9$ mod. 17. Par ailleurs, on a

$$\left(\frac{-3}{17}\right) \equiv 3^8 \text{ mod. } 17 \quad \text{et} \quad \left(\frac{-3}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = -1.$$

On obtient $14^{25} \equiv 3$ mod. 17, d'où l'assertion en utilisant le théorème chinois.
Il n'y a donc pas de rapport en général entre le symbole de Jacobi $\left(\frac{m}{n}\right)$ et l'entier $m^{\frac{n-1}{2}}$. Cette remarque est à la base du test de primalité de Solovay-Strassen (voir le chapitre V).

La loi de réciprocité quadratique s'étend aux symboles de Jacobi.

Théorème 2.4. *Soient m et n des entiers naturels impairs. On a*

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

Autrement dit, on a

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \quad \textit{si } m \textit{ ou } n \textit{ est congru à } 1 \textit{ modulo } 4,$$

$$\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right) \quad \textit{sinon.}$$

Démonstration : Si m et n ne sont pas premiers entre eux, on a $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = 0$. Si m ou n vaut 1, on a $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = 1$. Dans ces deux cas, on a l'égalité annoncée.
Supposons m et n au moins égaux à 3 et premiers entre eux. Soient

$$m = p_1 \cdots p_r \quad \text{et} \quad n = q_1 \cdots q_s$$

les décompositions de m et n en produits de nombres premiers. On a (prop. 2.4)

$$\Big(\frac{m}{n}\Big) = \prod_{i,j}\Big(\frac{p_i}{q_j}\Big) \quad \text{et} \quad \Big(\frac{n}{m}\Big) = \prod_{i,j}\Big(\frac{q_j}{p_i}\Big).$$

En appliquant la loi de réciprocité quadratique rs fois, on en déduit l'égalité

$$\Big(\frac{m}{n}\Big) = (-1)^t\Big(\frac{n}{m}\Big),$$

où t est le nombre de couples (i,j) tels que p_i et q_j soient congrus à 3 modulo 4. Il en résulte que l'on a $\big(\frac{m}{n}\big) = -\big(\frac{n}{m}\big)$ si et seulement si il y a un nombre impair de nombre premiers congrus à 3 modulo 4 dans chacune des factorisations de m et n. Par ailleurs, un produit de nombres premiers impairs est congru à 3 modulo 4 si et seulement si il y a un nombre impair de nombres premiers congrus à 3 modulo 4 dans ce produit. Ainsi, $\big(\frac{m}{n}\big) = -\big(\frac{n}{m}\big)$ si et seulement si m et n sont congrus à 3 modulo 4, d'où le résultat.

Exemples 2.9.

1) Calculons $\big(\frac{323}{1443}\big)$. On a

$$\Big(\frac{323}{1443}\Big) = -\Big(\frac{1443}{323}\Big) = -\Big(\frac{151}{323}\Big) = \Big(\frac{323}{151}\Big) = \Big(\frac{21}{151}\Big) = \Big(\frac{151}{21}\Big) = \Big(\frac{4}{21}\Big) = 1.$$

2) Pour tout entier naturel impair n, on a les formules

$$\Big(\frac{-1}{n}\Big) = (-1)^{\frac{n-1}{2}} \quad \text{et} \quad \Big(\frac{2}{n}\Big) = (-1)^{\frac{n^2-1}{8}}. \tag{12}$$

Ces égalités sont vraies si $n = 1$. Supposons $n \geq 3$. Soit f l'application définie sur l'ensemble des entiers naturels impairs par l'égalité

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

Pour tous a et b impairs, on vérifie, en examinant les classes de a et b modulo 4, que l'on a

$$f(ab) = f(a)f(b).$$

Soit $n = p_1^{n_1}\cdots p_r^{n_r}$ la décomposition en facteurs premiers de n. On a ainsi

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

Par ailleurs, pour tout $i = 1, \cdots, r$, on a $f(p_i) = \big(\frac{-1}{p_i}\big)$, d'où l'égalité $f(n) = \big(\frac{-1}{n}\big)$ par définition du symbole de Jacobi.

On procède de même pour l'autre égalité, en posant pour tout m impair

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

Pour tous a et b impairs, on vérifie, en examinant les classes de a et b modulo 8, que l'on a $g(ab) = g(a)g(b)$, et l'on conclut comme ci-dessus.

3) Soient m un entier relatif et n un entier naturel impair. Vérifions que $\left(\frac{m}{n}\right)$ ne dépend que de la classe de n modulo $4|m|$, autrement dit, que si n' est un entier naturel, on a l'implication

$$n \equiv n' \text{ mod. } 4|m| \implies \left(\frac{m}{n}\right) = \left(\frac{m}{n'}\right). \tag{13}$$

Supposons m impair positif. Si m ou n est congru à 1 modulo 4, on a $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$. Puisque $\left(\frac{n}{m}\right)$ ne dépend que de la classe de n modulo m, on a $\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right)$. On a $n \equiv n'$ mod. 4, d'où $\left(\frac{n'}{m}\right) = \left(\frac{m}{n'}\right)$, puis $\left(\frac{m}{n}\right) = \left(\frac{m}{n'}\right)$. Supposons $m \equiv n \equiv 3$ mod. 4. Dans ce cas, on a $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right) = -\left(\frac{n'}{m}\right)$. Puisque m et n' sont congrus à 3 modulo 4, on a $\left(\frac{n'}{m}\right) = -\left(\frac{m}{n'}\right)$, d'où l'assertion dans ce cas.
Si m est impair négatif, en posant $m = -t$, on a (première égalité de (12))

$$\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{t}{n}\right),$$

ce qui, d'après le cas déjà traité, entraîne (13).
Supposons m pair. Posons $m = 2^r t$, avec t impair. On a

$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^r\left(\frac{t}{n}\right).$$

La congruence $n \equiv n'$ mod. $4|m|$ implique $n \equiv n'$ mod. 8, d'où (seconde égalité de (12))

$$\left(\frac{2}{n}\right)^r = \left(\frac{2}{n'}\right)^r.$$

Puisque $n \equiv n'$ mod. $4|t|$, on a

$$\left(\frac{t}{n}\right) = \left(\frac{t}{n'}\right),$$

d'où l'implication (13).

7. Autre démonstration de la loi de réciprocité quadratique

On présente ici une preuve, due d'Eisenstein en 1845, de la loi de réciprocité quadratique. Elle repose sur une formule de trigonométrie et le lemme de Gauss (lemme 2.2).

Lemme 2.4. *Soit m un entier naturel impair. Pour tout x dans $\mathbb{R} - \pi\mathbb{Z}$, on a*

$$\frac{\sin mx}{\sin x} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \Big(\sin^2 x - \sin^2 \frac{2\pi j}{m}\Big).$$

Démonstration : Posons $m = 2n+1$ où $n \in \mathbb{N}$. Soit x un nombre réel qui n'est pas dans $\pi\mathbb{Z}$. On a

$$(\cos x + i \sin x)^{2n+1} = \sum_{k=0}^{2n+1} C_{2n+1}^k i^k (\sin x)^k (\cos x)^{2n+1-k}.$$

D'après la formule de De Moivre, en séparant les parties réelles et imaginaires, on obtient

$$\sin(2n+1)x = \sum_{j=0}^{n} C_{2n+1}^{2j+1} (-1)^j (\sin x)^{2j+1} (\cos x)^{2(n-j)},$$

d'où

$$\frac{\sin(2n+1)x}{\sin x} = \sum_{j=0}^{n} C_{2n+1}^{2j+1} (-1)^j (\sin^2 x)^j (1 - \sin^2 x)^{n-j}.$$

Considérons le polynôme $P \in \mathbb{Z}[X]$ défini par

$$P = \sum_{j=0}^{n} C_{2n+1}^{2j+1} (-1)^j X^j (1-X)^{n-j}.$$

On a

$$P(\sin^2 x) = \frac{\sin mx}{\sin x}. \tag{14}$$

Les éléments

$$\sin^2 \frac{2\pi j}{m} \quad \text{pour} \quad j = 1, \cdots n,$$

sont distincts deux à deux, et sont des racines de P. Puisque P est de degré au plus n, son degré est donc n et ce sont toutes ses racines. Ainsi, il existe $\lambda \in \mathbb{R}$ tel que l'on ait

$$P = \lambda \prod_{j=1}^{\frac{m-1}{2}} \Big(X - \sin^2 \frac{2\pi j}{m}\Big).$$

D'après (14), on obtient

$$\frac{\sin mx}{\sin x} = \lambda \prod_{j=1}^{\frac{m-1}{2}} \Big(\sin^2 x - \sin^2 \frac{2\pi j}{m}\Big).$$

Il reste à déterminer λ. Celui-ci vaut

$$(-1)^n r \quad \text{où} \quad r = \sum_{j=0}^{n} C_{2n+1}^{2j+1}.$$

On a l'égalité

$$2^{2n+1} = \Big(C_{2n+1}^1 + C_{2n+1}^3 + \cdots + C_{2n+1}^{2n+1}\Big) + \Big(C_{2n+1}^0 + C_{2n+1}^2 + \cdots + C_{2n+1}^{2n}\Big).$$

Par ailleurs, on a

$$C_{2n+1}^1 + C_{2n+1}^3 + \cdots + C_{2n+1}^{2n+1} = C_{2n+1}^0 + C_{2n+1}^2 + \cdots + C_{2n+1}^{2n},$$

d'où $2r = 2^{2n+1}$ i.e. $r = 4^n$ et le lemme.

Démonstration de la loi de réciprocité : Soient p et q deux nombres premiers impairs distincts. Posons

$$S = \Big\{1, \cdots, \frac{p-1}{2}\Big\}.$$

Pour tout $s \in S$, il existe un unique élément $s_q \in S$ tel que l'on ait

$$qs \equiv e_s(q) s_q \text{ mod. } p \quad \text{avec} \quad e_s(q) = \pm 1.$$

On a donc

$$\sin\Big(\frac{2\pi}{p} qs\Big) = e_s(q) \sin\Big(\frac{2\pi}{p} s_q\Big).$$

Puisque $s \mapsto s_q$ est une bijection de S, on a ainsi (lemme de Gauss)

$$\Big(\frac{q}{p}\Big) = \prod_{s\in S} e_s(q) = \prod_{s\in S} \frac{\sin\big(\frac{2\pi qs}{p}\big)}{\sin\big(\frac{2\pi s}{p}\big)}.$$

Notons T l'ensemble des entiers compris entre 1 et $\frac{q-1}{2}$. D'après le lemme 2.4, utilisé avec $m = q$ et $x = \frac{2\pi s}{p}$, on obtient

$$\Big(\frac{q}{p}\Big) = \prod_{s\in S} (-4)^{\frac{q-1}{2}} \prod_{t\in T} \Big(\sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{q}\Big),$$

d'où l'égalité

$$\Big(\frac{q}{p}\Big) = (-4)^{\frac{(q-1)(p-1)}{4}} \prod_{s\in S, t\in T} \Big(\sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{q}\Big).$$

En permutant les rôles de p et q, on a aussi

$$\Big(\frac{p}{q}\Big) = (-4)^{\frac{(q-1)(p-1)}{4}} \prod_{s\in S, t\in T} \Big(\sin^2 \frac{2\pi s}{q} - \sin^2 \frac{2\pi t}{p}\Big),$$

de sorte que $\big(\frac{q}{p}\big)$ et $\big(\frac{p}{q}\big)$ sont égaux au signe près. Le cardinal de $S \times T$ étant $\frac{(p-1)(q-1)}{4}$, il en résulte l'égalité cherchée

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