TP Maple 7 | Arithmétique dans $\mathbb{Z}$. Résidus quadratiques de $\mathbb{Z}/p\mathbb{Z}$.

Les résidus quadratiques apparaissent naturellement lors de la résolution des équations du second degré sur un corps K (voir l'introduction du paragraphe 2. de ce TP). Nous exposerons dans cette séance quelques résultats sur les résidus quadratiques de $\mathbb{Z}/p\mathbb{Z}$ (p étant un nombre premier) permettant de les déterminer et d'en calculer une « racine carrée ». Une excellente référence en la matière est le **cours d'algèbre (primalité, divisibilité, codes) de Michel Demazure** *publié aux éditions Cassini et synthèse d'un cours que l'auteur a enseigné à plusieurs promotions de l'Ecole Polytechnique.*

1. Arithmétique dans $\mathbb{Z}$ sous Maple

Maple peut manipuler des nombres comportant un très grand nombre de chiffres mais néanmoins limité. Le nombre maximal de chiffres, *maxdigits*, dépend du matétiel utilisé. On y aura accès par la commande **kernelopts(maxdigits)**.

```
> kernelopts(maxdigits);

                              268435448
```

Voici un aperçu des différentes opérations possibles sur les nombres entiers :

► *La fonction factorielle* : pour tout $n \in \mathbb{N}$, $n!$ se calcule au moyen de la commande **factorial** ou à l'aide du symbole **!**.

```
> factorial(12), 12!;
```

$$479001600, 479001600$$

► *Division euclidienne* : rappelons rapidement le principe de la division euclidienne : pour tous entiers naturels n et $m \neq 0$, il existe un unique couple d'entiers naturels (q, r) vérifiant

$$n = m \cdot q + r \quad et \quad 0 \leqslant r < m$$

On dit que q et r sont respectivement le quotient et le reste dans la division euclidienne de n par m (ou encore *de n modulo m*). On utilise les commandes **irem** et **iquo** pour calculer *le* reste et *le* quotient de la division euclidienne [1].

```
> irem(23,3);
```

$$2$$

```
> irem(-3,2);
```

$$-1$$

```
> -3 mod 2;
```

$$1$$

```
> iquo(23,3);
```

$$7$$

► *Test de primalité* : la fonction **isprime** permet de tester si un entier est premier [2] ou non.

```
> isprime(23);
```

$$true$$

1. **irem** et **iquo** sont les abréviations respectives de *integer remainder* et *integer quotient*.
2. Un nombre entier est dit premier s'il est ditinct de 1 et si ses seuls diviseurs sont 1 et lui-même.

► *Décomposition en produit de facteurs premiers*[3] : la fonction **ifactor** calcule la décomposition en produit de facteur(s) premier(s) d'un entier donné.

```
> ifactor(561);
```

$$(3)(11)(17)$$

On a donc $561 = 3 \times 11 \times 17$.

On rappelle rapidement les principales fonctions arithmétiques offertes par Maple.

Arithmétique élémentaire sous Maple

- **irem(n,m)** : renvoie un reste de n dans la division euclidienne par m.
- **iquo(n,m)** : renvoie un quotient de n dans la division euclidienne par m.
- **igcd(n,m)** : renvoie $\text{pgcd}(n,m)$.
- **igcdex(a,b,'u','v')** : affecte aux variables u et v deux entiers relatifs vérifiant $a \wedge b = u \cdot a + v \cdot b$.
- **ilcm(n,m)** : renvoie $\text{ppcm}(n,m)$.
- **ithprime(n)** : renvoie le n-ième nombre premier.
- **isprime(n)** : renvoie *true* si n est premier, *false* sinon.
- **ifactor(n)** : renvoie la décomposition en produit de facteur(s) premier(s) de n.

2. Retour sur les algorithmes essentiels

Cette partie expose les algorithmes élémentaires de l'arithmétique. On n'utilisera pas les commandes de Maple telles que `igcd`, `irem`, `iquo`, etc. Le principe est de redéfinir ces procédures au moyen des algorithmes.

2.1. La division euclidienne

Rappelons le théorème de la division euclidienne :

3. Il s'agit du théorème fondamental de l'Arithmétique : tout nombre entier distinct de 1 se décompose en produit de facteurs premiers.

La division euclidienne dans $\mathbb{N}$

Soient a et b deux entiers naturels tels que $0 < b$. Il existe un unique couple d'entiers naturels (q, r) tel que

$$a = b \cdot q + r \quad \text{et} \quad 0 \leqslant r < b$$

appelés respectivement *quotient* et *reste* dans la division euclidienne de a par b. On dit aussi que r et q sont respectivement *le reste et le quotient de a modulo b*.

L'algorithme de la division euclidienne de a par b le plus élémentaire est fondé sur des soustractions successives de b au nombre a.

Algorithme de la division euclidienne

Initialisation $\begin{cases} r \leftarrow a \\ q \leftarrow 0 \end{cases}$

Tant que $r \geqslant b$ **faire** $\begin{cases} r \leftarrow r - b \\ q \leftarrow q + 1 \end{cases}$

Renvoyer q et r.

A la sortie de la boucle **Tant que**, les entiers q et r sont respectivement égaux au quotient et au reste dans la division euclidienne de a par b.

Exercice 1. *Division euclidienne*

Ecrire une procédure `DivEuclide(a,b)` d'arguments $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$ renvoyant sous forme d'une liste $[q, r]$ le quotient et le reste dans la division euclidienne de a par b.

2.2. Les algorithmes d'Euclide

L'algorithme d'Euclide de calcul du pgcd de deux entiers naturels a et b est fondé sur la division euclidienne. On notera $a \wedge b$ le pgcd des entiers a et b. En voici le principe :

On note $r_0 = a$ et $r_1 = b$. Si $b = 0$, $r_0 \wedge r_1 = a$. Sinons, on effectue en cascade des divisions euclidiennes :

$$\begin{cases} r_0 = r_1 \cdot q_2 + r_2 & \text{où} \quad r_2 < r_1 \\ r_1 = r_2 \cdot q_3 + r_3 & \text{où} \quad r_3 < r_2 < r_1 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ r_i = r_{i+1} \cdot q_{i+2} + r_{i+2} & \text{où} \quad 0 < r_{i+2} < r_{i+1} < r_i < \cdots < r_1 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ r_{n_0-2} = r_{n_0-1} \cdot q_{n_0} + r_{n_0} & \text{où} \quad 0 = r_{n_0} < r_{n_0-1} < \cdots < r_2 < r_1 \end{cases}$$

Le processus s'arrête car les restes r_i forment une séquence strictement décroissante d'entiers naturels : il existe $n_0 \in \mathbb{N}$ tel que $r_{n_0} = 0$.

Venons-en à la remarque fondamentale : pour tout $0 \leqslant i \leqslant n_0 - 2$, l'ensemble des diviseurs de r_i et r_{i+1} étant égal à l'ensemble des diviseurs de r_{i+1} et r_{i+2}, on a

$$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{n_0-1} \wedge r_{n_0} = r_{n_0-1}$$

On retiendra que le pgcd de a et b est égal au dernier reste non nul dans l'algorithme d'Euclide.

Algorithme d'Euclide

Initialisation : $\begin{cases} r_0 = a \\ r_1 = b \end{cases}$

Tant que $r_1 \neq 0$ **faire** $\begin{cases} x \leftarrow r_0 \\ r_0 \leftarrow r_1 \\ r_1 \leftarrow \text{reste dans la division euclidienne de } x \text{ par } r_0 \end{cases}$

Renvoyer r_0

Exercice 2. *Algorithme d'Euclide*

Ecrire une procédure `Euclide(a,b)` d'arguments a et b dans $\mathbb{N}$ et renvoyant $a \wedge b$ par l'algorithme d'Euclide.

Une variante de cet algorithme permet, au-delà du calcul du pgcd d de a et b, d'obtenir les coefficients (u, v) dans $\mathbb{Z}$ d'une relation de Bezout :

$$u \cdot a + v \cdot b = d$$

En voici le principe en reprenant les notations précédentes. On prouve par une récurrence facile que, pour tout $0 \leqslant n \leqslant n_0$, il existe $(u_n, v_n) \in \mathbb{Z}^2$ tel que

$$r_n = u_n \cdot a + v_n \cdot b$$

En effet si cette propriété est vérifiée pour tout $k \leqslant n$, on a

$$\begin{cases} r_n = u_n \cdot a + v_n \cdot b \\ r_{n+1} = u_{n+1} \cdot a + v_{n+1} \cdot b \end{cases} \quad \text{et} \quad r_{n+2} = r_n - q_{n+2} \cdot r_{n+1}$$

ainsi

$$\begin{aligned} r_{n+2} = r_n - q_{n+2} \cdot r_{n+1} &= u_n \cdot a + v_n \cdot b - q_{n+2} \cdot (u_{n+1} \cdot a + v_{n+1} \cdot b) \\ &= \left(u_n - q_{n+2} \cdot u_{n+1}\right) \cdot a + \left(v_n - q_{n+2} \cdot v_{n+1}\right) \cdot b \end{aligned}$$

On peut donc définir une telle séquence de couple par les relations de récurrence suivantes :

$$\begin{cases} u_0 = 1 \\ v_0 = 0 \\ u_1 = 0 \\ v_1 = 1 \end{cases}, \quad \forall 0 \leqslant n \leqslant n_0 - 2, \quad \begin{cases} u_{n+2} = u_n - q_{n+2} \cdot u_{n+1} \\ v_{n+2} = v_n - q_{n+2} \cdot v_{n+1} \end{cases}$$

Le couple recherché est (u_{n_0-1}, v_{n_0-1}) puisque

$$a \wedge b = r_{n_0-1} = u_{n_0-1} \cdot a + v_{n_0-1} \cdot b$$

Cet algorithme est appelé *algorithme d'Euclide étendu* :

Algorithme d'Euclide étendu

Initialisation : $\begin{cases} r_0 \leftarrow a \\ r_1 \leftarrow b \end{cases}$, $\begin{cases} u_0 \leftarrow 1 \\ u_1 \leftarrow 0 \end{cases}$, $\begin{cases} v_0 \leftarrow 0 \\ v_1 \leftarrow 1 \end{cases}$

Tant que $r_1 \neq 0$ **faire** $\begin{cases} x \leftarrow r_0 \\ r_0 \leftarrow r_1 \\ r_1 \leftarrow \text{reste de } x \text{ modulo } r_0 \\ y \leftarrow u_0 \\ u_0 \leftarrow u_1 \\ u_1 \leftarrow y - u_0 \times \text{quotient de } x \text{ modulo } r_0 \\ y \leftarrow v_0 \\ v_0 \leftarrow v_1 \\ v_1 \leftarrow y - v_0 \times \text{quotient de } x \text{ modulo } r_0 \end{cases}$

Renvoyer (u_0, v_0)

Exercice 3. *Algorithme d'Euclide étendu*

Ecrire une procédure `EuclideEtendu(a,b)` d'arguments a et b dans $\mathbb{N}$ et renvoyant un couple $(u, v) \in \mathbb{Z}^2$ tel que $a \wedge b = u \cdot a + v \cdot b$.

3. Résidus quadratiques de $\mathbb{Z}/p\mathbb{Z}$

Soient K un corps de caractéristique différente de 2 et $(a, b) \in K^2$. Considérons l'équation

$$(E) \ : \ x^2 + ax + b = 0$$

Pour la résoudre, on utilise classiquement une mise sous forme canonique :

$$x^2 + ax + b = \left(x + 2^{-1} \cdot a\right)^2 - 2^{-2} \cdot a^2 + b = \left(x + 2^{-1} \cdot a\right)^2 - \left(2^{-1}\right)^2 \cdot \left(a^2 - 4b\right)$$

valable car, en caractéristique différente de 2, le nombre 2 (par définition égal à $1_K + 1_K$) est inversible car non nul. Résoudre (E) revient donc à résoudre

$$y^2 = a^2 - 4b$$

c'est-à-dire à trouver les racines carrées du discrimiant $\Delta = a^2 - 4b$. Si $\Delta \neq 0$, on a l'alternative suivante : soit Δ n'admet aucune racine carrée, soit Δ admet exactement deux racines carrées opposées. Cela découle immédiatement de la factorisation $X^2 - \delta^2 = (X+\delta)(X-\delta)$ pour tout δ dans K.

Nous allons développer dans la suite de ce TP des outils permettant de savoir si un éléments de $K = \mathbb{Z}/p\mathbb{Z}$ (avec p premier) est un carré et, le cas échéant, d'en extraire une racine carrée.

3.1. Caractérisation et dénombrement

Le premier résultat est un classique de l'oral des concours.

Théorème 1. (Carrés de $\mathbb{Z}/p\mathbb{Z}^*$)
Soit p un nombre premier impair. Parmi les $p-1$ éléments de $\mathbb{Z}/p\mathbb{Z}^*$, la moitié exactement sont des carrés. Si $x \in \mathbb{Z}/p\mathbb{Z}^*$ est un carré, on a $x^{(p-1)/2} = 1$. Sinon, on a $x^{(p-1)/2} = -1$.

Ce résultat et sa démonstration se généralise sans peine au cas d'un corps fini K de cardinal q impair : K^* contient exactement $(q-1)/2$ carrés et $x \in K^*$ est un carré *si et seulement si* $x^{(q-1)/2} = 1$. Dans le cas contraire $x^{(q-1)/2} = -1$.

Exercice 4.

Carré de $\mathbb{Z}/p\mathbb{Z}$.

1. Prouver le théorème 1.

2. En déduire que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ *si et seulement si* $p \equiv 1[4]$.

3.2. Le symbole de Legendre

Soient p un nombre premier et $n \in \mathbb{N}$. On dit que n *est un résidu quadratique modulo* p si $\overline{n}$ est un carré dans le corps $\mathbb{Z}/p\mathbb{Z}$. On définit alors *le symbole de Legendre* :

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } p \wedge n = 1 \text{ et } n \text{ est un résidu quadratique modulo } p \\ 0 & \text{si } p \text{ divise } n \\ -1 & \text{si } n \text{ n'est pas un résidu quadratique modulo } p \end{cases}$$

Ce symbole permet donc de répondre à la question suivante : $\overline{n}$ est-il un carré dans $\mathbb{Z}/p\mathbb{Z}$?

Exercice 5.

Vérifier que $\left(\frac{n}{2}\right) \equiv n[2]$ et $\left(\frac{n}{3}\right) \equiv n[3]$

Une première approche du calcul du symbole de Legendre est donnée par la formule d'Euler :

Théorème 2. (Formule d'Euler)
Pour tout entier naturel n et tout nombre premier impaire p, on a

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

Sachant que le coût du calcul rapide des puissances [4] de la forme $a^{(p-1)/2}$ est de l'ordre de $\ell\mathrm{n}(p)$ et que celui de la réduction modulo p d'un nombre inférieur ou égal à p^2 s'élève à $\left(\ell\mathrm{n}(p)\right)^2$, le coût du calcul du symbôle de Legendre par la formule d'Euler (sans compter la première réduction modulo, i.e. celle de n) est en $O\left(\left(\ell\mathrm{n}(p)\right)^3\right)$. Il est possible d'abaisser ce coût en un $O\left(\left(\ell\mathrm{n}(p)\right)^2\right)$ en utilisant la loi de réciprocité quadratique et le symbole de Jacobi qui généralise celui de Legendre.

Exercice 6.

Calcul du symbole de Legendre par la formule d'Euler.

1. Prouver la formule d'Euler.

2. Ecrire une procédure `Legendre(p,n)` renvoyant $\left(\frac{n}{p}\right)$ par la formule d'Euler. On utilisera la commande `Power(a,n) mod p` afin d'optimiser les calculs modulaires.

De la formule d'Euler, on déduit la multiplicativité du symbole de Legendre :

Proposition 3. (Propriétés du symbole de Legendre)
Pour tout nombre premier p impair et tous entiers naturels n et n', on a

$$\left(\frac{n\cdot n'}{p}\right)=\left(\frac{n}{p}\right)\cdot\left(\frac{n'}{p}\right)$$

De plus, pour tous entiers naturels n et n' tel que $p\wedge n=1$, on a $\left(\frac{n^2\cdot n'}{p}\right)=\left(\frac{n'}{p}\right)$.

De cette propriété, on déduit un fait qui n'était pas évident auparavant : le produit de deux non-carrés est un carré.

4. Calcul des résidus quadratiques de $\overline{n}$ dans $\mathbb{Z}/p\mathbb{Z}$

La formule d'Euler permet de savoir si un nombre n est un résidu quadratique modulo p mais ne permet pas *dans le cas général*[5] de trouver une racine carrée de $\overline{n}$ dans $\mathbb{Z}/p\mathbb{Z}$. Nous allons exposer dans ce paragraphe un algorithme de calcul d'un résidu quadratique de n dans $\mathbb{Z}/p\mathbb{Z}$ dans le cas où $\left(\frac{n}{p}\right)=1$. La méthode est dûe à Shanks et repose sur la connaissance d'un non-résidu quadratique modulo p.

4.1. Détermination d'un non-résidu quadratique

L'idée est simple : en choisissant au hasard un élément de $\mathbb{Z}/p\mathbb{Z}$, on déduit du théorème 1 que l'on a une chance sur deux de trouver un non-résidu quadratique. En itérant ce processus N fois, on a donc une probabilité égale à $1-2^{-N}$ de trouver un non-résidu quadratique modulo p.

4. Voir l'algorithme de calcul rapide des puissances au programme de MPSI.
5. Elle n'est intéressante de ce point de vue que dans le cas où $p\equiv 3$ [4] comme nous le verrons ci-dessous.

Exercice 7.

Ecrire une procédure `NonResidu(p)` renvoyant un non-résidu modulo p par la méthode décrite ci-dessus. On pourra utiliser la bibliothèque `RandomTools` de Maple (cf. l'aide en ligne).

4.2. L'algorithme de Shanks (1973)

Commençons par remarquer que si $p \equiv 3\ [4]$ et $\left(\frac{n}{p}\right) = 1$, on déduit de la formule d'Euler que

$$n \equiv n \cdot \left(\frac{n}{p}\right) \equiv n \cdot n^{(p-1)/2} \equiv n^{(p+1)/2} \equiv \left(n^{(p+1)/4}\right)^2 \ [p]$$

L'entier $n^{(p+1)/4}$ est donc une racine carrée de n modulo p : nul besoin d'un algorithme pour calculer une racine carrée de n modulo p dans ce cas.

Dans le cas où $p \not\equiv 3\ [4]$, écrivons p sous la forme $p = 1 + 2^s \cdot t$ avec t impair. On a alors

$$\forall n \in \mathbb{N}, \quad \left(\frac{n}{p}\right) \equiv n^{2^{s-1} \cdot t}\ [p]$$

Soit z un entier tel que

$$z^{2^{s-1}} \equiv -1\ [p]$$

Pour trouver un tel entier z, il suffit de déterminer un non-résidu quadratique m modulo p (voir le paragraphe précédent pour un algorithme) et de poser $z = m^t$.

Algorithme de Shanks pour le calcul d'un résidu quadratique modulo $p \not\equiv 3\ [4]$

Initialisation : $\begin{cases} m \leftarrow s \\ x \leftarrow n^{(t+1)/2} \\ b \leftarrow n^t \end{cases}$

Tant que $b \not\equiv 1\ [p]$ **faire** $\begin{cases} \text{Trouver le plus petit entier } 0 < i < m \text{ tel que } b^{2^i} \equiv 1\ [p] \\ \begin{cases} y \leftarrow z^{2^{m-i-1}} \\ z \leftarrow y^2 \\ b \leftarrow bz \\ x \leftarrow xy \end{cases} \\ m \leftarrow i \end{cases}$

Renvoyer x

Exercice 8.

L'algorithme de Shanks.

1. Justifier la validité et la terminaison de cet algorithme.

2. Ecrire une procédure `FactoDeux(a)` renvoyant l'unique couple d'entiers naturels (s,t) tels que $a = 2^s \cdot t$ avec t impair pour tout $a \in \mathbb{N}^*$.

3. Ecrire une procédure `Shanks(n,p)` renvoyant une racine carrée de n modulo p par l'algorithme de Shanks dans le cas où $\left(\frac{n}{p}\right) = 1$. On utilisera les procédures `FactoDeux` et `NonResidu` écrites précédemment.

5. La loi de réciprocité quadratique

L'objet de ce paragraphe est d'établir la loi de réciprocité quadratique.

Théorème 4. (Loi de réciprocité quadratique, Gauss)
Pour tous nombres premiers p et q différents de 2, on a

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

De ce théorème, nous déduirons un algorithme de calcul du symbole de Legendre plus efficace que celui exposé précédemment. Pour les besoins de la démonstrations, nous commencerons par quelques résultats élémentaires sur les quotients de $\mathbb{K}[X]$.

5.1. Quotients de $\mathbb{K}[X]$

On considère un corps K et l'algèbre $\mathbb{K}[X]$ des polynômes à coefficients dans K. On sait que $\mathbb{K}[X]$ muni des opérations usuelles de somme et de produit a une structure d'anneau euclidien commutatif. Il est donc principal et tout idéal I de $\mathbb{K}[X]$ est de la forme $I = (\Gamma) = \Gamma \cdot \mathbb{K}[X]$ où Γ est unique si on impose qu'il soit unitaire.

Pour tout idéal I de $\mathbb{K}[X]$, on considère la relation d'équivalence $\mathscr{R}$ définie sur $\mathbb{K}[X]$ par :

$$P \mathscr{R} Q \text{ si et seulement si } P - Q \in I$$

On prouve sans peine que $\mathscr{R}$ est une relation d'équivalence sur $\mathbb{K}[X]$. On démontre également que cette relation est compatible avec les opérations + et × sur $\mathbb{K}[X]$, c'est-à-dire que

$$\forall (P,Q,P',Q') \in \mathbb{K}[X]^4, \quad \begin{cases} P \mathscr{R} P' \\ Q \mathscr{R} Q' \end{cases} \Rightarrow \begin{cases} P+Q \mathscr{R} P'+Q' \\ PQ \mathscr{R} P'Q' \end{cases}$$

Dès lors, on démontre facilement que les égalités suivantes

$$\forall (P,Q) \in \mathbb{K}[X]^2, \quad \begin{cases} \overline{P} + \overline{Q} = \overline{P+Q} \\ \overline{P} \times \overline{Q} = \overline{PQ} \end{cases}$$

définissent deux lois de composition internes sur l'ensemble quotient $\mathbb{K}[X]/\mathscr{R}$ faisant de cet ensemble un anneau commutatif noté $\mathbb{K}[X]/I$: *le quotient de* $\mathbb{K}[X]$ *par l'idéal* I. Le neutre 0_A pour l'addition de cet anneau est clairement égal à $\overline{0_{\mathbb{K}[X]}}$, la classe d'équivalence du polynôme nul.

En considérant l'injection

$$\begin{array}{rcl} j : K & \longrightarrow & A = K[X]/I \\ x & \longmapsto & \overline{x} \end{array}$$

on identifier K et $j(K)$ et ainsi considérer que A est un anneau contenant K. On dit que l'anneau A est une extension de K. On peut alors définir $P(a)$ pour tout couple $(P,a) \in K[X] \times A$. Etant donnés un corps K et $P \in K[X]$ non constant, cette méthode permet de plonger un corps K dans un anneau A dans lequel P admet une racine. Soit $P \in \mathbb{K}[X]$ unitaire et $A = \mathbb{K}[X]/(P)$. En posant $\alpha = \overline{X}$ (la classe d'équivalence de X modulo l'idéal (P)), on a $P(\alpha = 0)$. En effet,

$$P(\alpha) = P\left(\overline{X}\right) = \overline{P(X)} = \overline{0_{\mathbb{K}[X]}} = 0_A$$

d'après la définition des lois de l'anneau A. C'est un principe très puissant en algèbre et en choisissant P irréductible sur $\mathbb{K}$, on peut prouver que $A = K[X]/(P)$ est un corps.

Si K est de caractéristique p, on prouve sans peine que A est aussi de caractéristique p. On rappelle que dans un anneau commutatif de caractéristique p, on a

$$\forall (x,y) \in A,\ \ (x+y)^p = x^p + y^p$$

5.2. Application au calcul du symbole de Legendre

On peut déduire de ce qui précède une méthode de calcul de $\left(\frac{n}{p}\right)$ lorsque $p \wedge n = 1$. L'idée est la suivante : on plonge $\mathbb{Z}/p\mathbb{Z}$ dans un anneau A commutatif de caractéristique p dans lequel il existe a tel que $\overline{n} = a^2$. On a alors que

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

car a est inversible dans l'anneau A puisque son carré $a^2 = \overline{n} \neq 0$ est inversible dans $K \subset A$. Ainsi,

$$a^p = \begin{cases} a & \text{si } \left(\frac{n}{p}\right) = 1 \\ -a & \text{si } \left(\frac{n}{p}\right) = -1 \end{cases}$$

Il s'agit donc de calculer a^p. Le principe est alors d'exprimer a comme combinaison linéaire de racines de l'unité dans A et d'appliquer la règle de calcul $(x+y)^p = x^p + y^p$ valable en caractéristique p.

Illustrons cette méthode par le calcul de $\left(\frac{2}{p}\right)$ pour tout nombre premier impair p. Considérons $A = \mathbb{Z}/p\mathbb{Z}[X]/(X^4+1)$ et notons $u = \overline{X}$. On a $u^4 = -1$ et $u^{-1} = -u^3$. Posons alors $a = u + u^{-1}$, de sorte que

$$a^2 = \left(u + u^{-1}\right)^2 = u^2 + u^{-2} + 2 = u^{-2} \cdot \left(u^4 + 1\right) + 2 = 2$$

On remarque alors que

$$a^p = u^p + u^{-p} = \begin{cases} a & \text{pour } p \equiv 1\ [8] \\ a & \text{pour } p \equiv 7\ [8] \\ -a & \text{pour } p \equiv 3\ [8] \\ -a & \text{pour } p \equiv 5\ [8] \end{cases}$$

On peut résumer ces calculs de la manière suivante :

Théorème 5. (Calcul du symbole de Lengendre dans le cas où $n = 2$)
Pour tout nombre premier impair p, on a

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

5.3. Preuve de la loi de réciprocité quadratique

Afin d'alléger les calculs, on notera

$$\varepsilon(n) = (-1)^{(n-1)/2}$$

pour tout entier impair n. Soient p et q deux nombres premiers impairs distincts. Considérons

$$\Phi_q = X^{q-1} + X^{q-2} + \cdots + X + 1 \quad \text{et} \quad A = \mathbb{Z}/p\mathbb{Z}[X]/(\Phi_q)$$

Posons $u = \overline{X}$ de sorte que $u^q = 1$. Notons alors

$$\tau = \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i}{q}\right) \cdot u^i$$

Cette somme [6] est bien définie puisque $u^q = 1$. On a alors :

$$\varepsilon(q) \cdot \tau^2 = \sum_{i,j \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{-1}{q}\right) \cdot \left(\frac{i}{q}\right) \cdot \left(\frac{j}{q}\right) \cdot u^i \cdot u^j = \sum_{i,j \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{-ij}{q}\right) \cdot u^{i+j} = \sum_{k \in \mathbb{Z}/q\mathbb{Z}} \left(\sum_{i \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i(i-k)}{q}\right)\right) \cdot u^k$$

Il s'agit donc de calculer les sommes

$$s_k = \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i(i-k)}{q}\right) = \sum_{i \in \mathbb{Z}/q\mathbb{Z}^*} \left(\frac{i(i-k)}{q}\right)$$

- Si $k = 0$, on a $\left(\frac{i(i-k)}{q}\right) = \left(\frac{i^2}{q}\right) = 1$ d'où

$$s_0 = q - 1$$

- Si $k \neq 0$, en notant i^{-1} l'inverse de i modulo q, on a

$$\left(\frac{i(i-k)}{q}\right) = \left(\frac{i^2\left(1 - k \cdot i^{-1}\right)}{q}\right) = \left(\frac{1 - k \cdot i^{-1}}{q}\right)$$

Or $i \mapsto 1 - k \cdot i^{-1}$ réalise une bijection de $\mathbb{Z}/q\mathbb{Z}^*$ sur $\mathbb{Z}/q\mathbb{Z} \setminus \{1\}$. Ainsi

$$s_k = \sum_{i \in \mathbb{Z}/q\mathbb{Z}^*} \left(\frac{i(i-k)}{q}\right) = \sum_{i \in \mathbb{Z}/q\mathbb{Z} \setminus \{1\}} \left(\frac{i}{q}\right) = \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i}{q}\right) - 1 = -1$$

car il y a autant de carré que de non-carrés dans $\mathbb{Z}/q\mathbb{Z}^*$ d'après le théorème 1.

6. appelée somme de Gauss.

On a donc

$$\varepsilon(q)\cdot\tau^2 = s_0 + \sum_{k\in\mathbb{Z}/q\mathbb{Z}^*} s_k\cdot u^k = q-1-\sum_{k\in\mathbb{Z}/q\mathbb{Z}^*} u^k = q-\sum_{k\in\mathbb{Z}/q\mathbb{Z}} u^k = q$$

Ainsi, puisque l'on calcule dans un anneau de caractéristique p,

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

d'où

$$\left(\frac{p}{q}\right)\cdot\tau^p = \sum_{i\in\mathbb{Z}/q\mathbb{Z}}\left(\frac{pi}{q}\right)\cdot u^{ip} = \sum_{j\in\mathbb{Z}/q\mathbb{Z}}\left(\frac{j}{q}\right)\cdot u^j = \tau$$

car $i\mapsto ip$ est bijective puisque p est inversible modulo q. On a donc

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

mais on a aussi

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

d'où

$$\left(\frac{p}{q}\right)\cdot\tau = \left(\frac{\varepsilon(q)\cdot q}{p}\right)\cdot\tau$$

et comme τ est inversible dans A puisque son carré l'est (en effet, $q\wedge p = 1$), on a bien

$$\left(\frac{p}{q}\right) = \left(\frac{\varepsilon(q)\cdot q}{p}\right) = \varepsilon(p)\cdot\varepsilon(q)\cdot\left(\frac{q}{p}\right)$$

ce qui achève la preuve de la loi de réciprocité quadratique de Gauss.

5.4. Application au calcul du symbole de Legendre

En appliquant les propriétés du symbole de Legendre (définition, multiplicativité, réciprocité), on ramène tout calcul à la détermination d'un résidu de -1 ou 2 modulo un nombre premier impair. Voyons cela sur un exemple :

$$\left(\frac{541}{2011}\right) = \left(\frac{2011}{541}\right) = \left(\frac{97}{541}\right) = \left(\frac{541}{97}\right) = \left(\frac{56}{97}\right) = \left(\frac{2}{97}\right)\cdot\left(\frac{7}{97}\right) = \left(\frac{2}{97}\right)\cdot\left(\frac{97}{7}\right) = \left(\frac{2}{97}\right)\cdot\left(\frac{-1}{7}\right) = -1$$

L'inconvénient de cette méthode est d'utiliser la décomposition en facteur premier des entiers dont on sait qu'elle est très coûteuse à obtenir. Pour remédier à ce problème, Jacobi a introduit une généralisation du symbole de Legendre.