

Résidus quadratiques

# 1 Le symbole de Legendre

Soit  $p \in \mathbb{Z}$  un premier impair. On dit que  $n \in \mathbb{Z}$  est un **résidu quadratique modulo  $p$**  si  $n \pmod p$  est un carré dans  $\mathbb{F}_p$ , c'est-à-dire s'il existe  $m \in \mathbb{Z}$  tel que  $n \equiv m^2 \pmod p$ . On définit alors le **symbole de Legendre**  $\left(\frac{n}{p}\right)$  entre  $n$  et  $p$  comme suit :

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \mid n, \\ 1 & \text{si } p \text{ est premier à } n \text{ et si } n \text{ est résidu quadratique modulo } p, \\ -1 & \text{si } p \text{ est premier à } n \text{ et si } n \text{ est non résidu quadratique modulo } p. \end{cases}$$

Le critère d'Euler donne un moyen facile de calculer ce symbole.

**Proposition 1.1 (Critère d'Euler)** *Soit  $p$  un premier impair. Exactement  $\frac{p-1}{2}$  éléments de  $\mathbb{F}_p^*$  sont des carrés et on a la formule :*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod p$$

**Question 1.** Faire la preuve de ce critère.

**Question 2.** Quelle est la complexité de la vérification du fait qu'un élément de  $\mathbb{F}_p^*$  est un carré ou non ?

**Question 3.** Sait-on pour autant calculer explicitement une racine carrée ?

**Proposition 1.2** *Le symbole de Legendre satisfait les égalités suivantes.*

1. Pour tous  $m, n \in \mathbb{Z}$ , on a :

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \left(\frac{n}{p}\right), \quad \left(\frac{m^2n}{p}\right) = \left(\frac{n}{p}\right),$$

où pour la deuxième il faut de plus supposer  $m$  est premier à  $p$ .

2. On a :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{autrement dit} \quad \left[\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4\right].$$

3. On a :

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad \text{autrement dit} \quad \left[\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8\right].$$

**Question 4.** Seule la dernière assertion exige un peu de travail.

a. Traitons deux exemples. Dans  $\mathbb{F}_{13}$  et  $\mathbb{F}_{19}$ , écrivons :

dans  $\mathbb{F}_{13}$   $2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 = (2 \cdot 4 \cdot 6)(8 \cdot 10 \cdot 12)$

dans  $\mathbb{F}_{19}$   $2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdot 14 \cdot 16 \cdot 18 = (2 \cdot 4 \cdot 6 \cdot 8)(10 \cdot 12 \cdot 14 \cdot 16 \cdot 18)$

A gauche faites apparaître  $2^{\frac{p-1}{2}}$  et  $\frac{p-1}{2}!$ , à droite une certaine puissance de  $-1$  et encore  $\frac{p-1}{2}!$ .

b. En tentant de généraliser ce qui précède, montrer que si  $p \equiv 1 \pmod 4$  alors que  $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$  et si  $p \equiv 3 \pmod 4$  alors que  $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}$ . Puis conclure.

La première assertion montre que  $x \mapsto \left(\frac{x}{p}\right)$  définit un morphisme de  $\mathbb{F}_p^*$  dans  $\{\pm 1\}$  dont le noyau n'est rien d'autre que l'ensemble des carrés.

Enfin, on peut relier le comportement quadratique de  $p$  modulo  $q$  à celui de  $q$  modulo  $p$ . C'est ce que l'on appelle la **loi de réciprocité quadratique**. Il en existe beaucoup de preuves ; celle fournie ici s'inspire (fortement) de Demazure [Dem97] §5.2.

**Théorème 1.3 (Loi de réciprocité quadratique)** *Soit  $p$  et  $q$  deux nombres premiers impairs alors :*

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

Remarquons que la loi est évidente pour  $p = q$ , les deux membres de l'égalité étant nuls. Dans ce qui suit, on suppose que  $p \neq q$ . Pour établir cette loi, nous allons travailler dans l'anneau  $A = \mathbb{F}_p[X]/\langle \Phi_q(X) \rangle$ , où  $\Phi_q(X)$  désigne le  $q$ -ème polynôme cyclotomique :

$$\Phi_q(X) = \frac{X^q - 1}{X - 1} = X^{q-1} + X^{q-2} + \dots + X + 1.$$

Notons  $\zeta = X \bmod \Phi_q(X)$ . On a donc  $A = \mathbb{F}_p[\zeta]$  et  $\zeta^q = 1$ . Introduisons la **somme de Gauss** définie par :

$$\tau = \sum_{i \in \mathbb{F}_q} \left(\frac{i}{q}\right) \zeta^i.$$

**Question 5.** Pourquoi l'expression  $\zeta^i$  a-t-elle un sens pour  $i \in \mathbb{F}_q$  ?

Montrons le :

**Lemme 1.4 (Gauss)** *La somme de Gauss  $\tau$  vérifie les identités :*

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

**Preuve** — (i) Calculons :

$$(-1)^{\frac{q-1}{2}} \tau^2 = \left(\frac{-1}{q}\right) \left(\sum_{i \in \mathbb{F}_q} \left(\frac{i}{q}\right) \zeta^i\right)^2 = \sum_{i, j \in \mathbb{F}_q} \left(\frac{-ij}{q}\right) \zeta^{i+j} = \sum_{k \in \mathbb{F}_q} \left(\sum_{i \in \mathbb{F}_q} \left(\frac{i(i-k)}{q}\right)\right) \zeta^k. \quad (1)$$

Pour  $k \in \mathbb{F}_q$ , on s'est ramené à déterminer les sommes  $s_k \stackrel{\text{déf.}}{=} \sum_{i \in \mathbb{F}_q} \left(\frac{i(i-k)}{q}\right)$ .

Pour  $k = 0$ , c'est facile car :

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

Pour  $k \neq 0$ , on transforme encore la somme :

$$\begin{aligned} s_k &= \sum_{i \in \mathbb{F}_q} \left(\frac{i(i-k)}{q}\right) = \sum_{i \in \mathbb{F}_q^*} \left(\frac{i(i-k)}{q}\right) = \sum_{i \in \mathbb{F}_q^*} \left(\frac{i^2(1-ki^{-1})}{q}\right) = \sum_{i \in \mathbb{F}_q^*} \left(\frac{1-ki^{-1}}{q}\right) \\ &= \sum_{j \in \mathbb{F}_q \setminus \{1\}} \left(\frac{j}{q}\right) = \sum_{j \in \mathbb{F}_q^* \setminus \{1\}} \left(\frac{j}{q}\right) = -1 \end{aligned}$$

car quand  $i$  parcourt  $\mathbb{F}_q^*$  alors  $1-ki^{-1}$  parcourt  $\mathbb{F}_q \setminus \{1\}$ , puis car il y a autant de carrés que de non-carrés dans  $\mathbb{F}_q^*$  (et on a enlevé un carré).

Il n'y a plus qu'à ré-injecter ces expressions des sommes  $s_k$  dans (1) :

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

d'où le résultat.

(ii) Etant en caractéristique  $p$ , on sait que :

$$\tau^p = \left( \sum_{i \in \mathbb{F}_q} \left( \frac{i}{q} \right) \zeta^i \right)^p = \sum_{i \in \mathbb{F}_q} \left( \frac{i}{q} \right)^p \zeta^{pi} = \sum_{i \in \mathbb{F}_q} \left( \frac{i}{q} \right) \zeta^{pi},$$

donc :

$$\left( \frac{p}{q} \right) \tau^p = \sum_{i \in \mathbb{F}_q} \left( \frac{pi}{q} \right) \zeta^{pi} = \sum_{j \in \mathbb{F}_q} \left( \frac{j}{q} \right) \zeta^j = \tau,$$

car  $p$  est inversible modulo  $q$  donc  $i \mapsto pi$  définit une bijection de  $\mathbb{F}_q$ . □

**Question 6.** En continuant de raisonner dans l'anneau  $A$  montrer que la loi de réciprocité quadratique résulte des deux formules précédentes.

## 2 Le symbole de Jacobi

On généralise le symbole de Legendre en admettant les «dénominateurs impairs non premiers». C'est que l'on appelle le **symbole de Jacobi** : pour  $a, b \in \mathbb{Z}$ , avec  $b$  **impair** se factorisant sous la forme  $b = p_1^{e_1} \cdots p_r^{e_r}$ , on définit le symbole de Jacobi  $\left( \frac{a}{b} \right)$  par :

$$\left( \frac{a}{b} \right) = \left( \frac{a}{p_1} \right)^{e_1} \cdots \left( \frac{a}{p_r} \right)^{e_r}.$$

**Question 7.** a. Quelle est la valeur de  $\left( \frac{a}{b} \right)$  si  $\text{pgcd}(a, b) \neq 1$ .

b. Quelle est la valeur de  $\left( \frac{a}{b} \right)$  si  $a$  est un carré modulo  $b$ ?

c. Réciproquement, est-ce que  $\left( \frac{a}{b} \right) = 1$  implique  $a$  carré modulo  $b$ ?

Le symbole de Jacobi partage les propriétés suivantes avec le symbole de Legendre.

**Proposition 2.1** Pour  $a, b \in \mathbb{Z}$  avec  $a$  ou  $b$  impair dès lors qu'il apparaît au «dénominateur» d'un symbole, on a :

$$\begin{aligned} \left( \frac{a}{b} \right) &= \left( \frac{a'}{b} \right) \text{ si } a \equiv a' \pmod{b}, & \left( \frac{aa'}{b} \right) &= \left( \frac{a}{b} \right) \left( \frac{a'}{b} \right), & \left( \frac{a}{bb'} \right) &= \left( \frac{a}{b} \right) \left( \frac{a}{b'} \right), \\ \left( \frac{-1}{b} \right) &= (-1)^{\frac{b-1}{2}} \text{ autrement dit } & \left[ \left( \frac{-1}{b} \right) = 1 \Leftrightarrow b \equiv 1 \pmod{4} \right], \\ \left( \frac{2}{b} \right) &= (-1)^{\frac{b^2-1}{8}} \text{ autrement dit } & \left[ \left( \frac{2}{b} \right) = 1 \Leftrightarrow b \equiv \pm 1 \pmod{8} \right], \\ \left( \frac{a}{b} \right) &= (-1)^{\frac{(a-1)(b-1)}{4}} \left( \frac{b}{a} \right) \text{ (loi de réciprocité)}. \end{aligned}$$

**Question 8.** Vérifier cette proposition.

**Question 9.** En s'inspirant de l'algorithme d'Euclide, grâce à de simples divisions euclidiennes et à des vérifications de parité, calculer le symbole  $\left( \frac{713}{1009} \right)$ .

Toujours en prenant modèle sur l'algorithme d'Euclide, il est facile de généraliser ce qui précède afin d'obtenir un algorithme efficace du calcul d'un symbole de Jacobi. De la même façon que l'on sait calculer un pgcd sans factoriser, on sait donc calculer un symbole de Jacobi sans factoriser le dénominateur.

**Question 10.** Donner un tel algorithme et préciser sa complexité.

### 3 Application : le critère de primalité de Solovay et Strassen

Soit  $n$  un entier impair. On note  $\mathbb{Z}/n\mathbb{Z}^*$  le groupe des inversibles modulo  $n$ . On dispose de deux morphismes  $\chi_i : \mathbb{Z}/n\mathbb{Z}^* \rightarrow \mathbb{Z}/n\mathbb{Z}^*$ ,  $i = 1, 2$ , définis par :

$$\chi_1(x) = \left(\frac{x}{n}\right) \quad \text{et} \quad \chi_2(x) = x^{\frac{n-1}{2}}.$$

Grâce au critère d'Euler, on sait que si  $n$  est un premier impair alors  $\chi_1(x) = \chi_2(x)$  pour tout  $x \in \mathbb{Z}/n\mathbb{Z}^*$ . Dès lors, s'il existe  $x \in \mathbb{Z}/n\mathbb{Z}^*$  tel que  $\chi_1(x) \neq \chi_2(x)$ , nécessairement  $n$  n'est pas premier. Un tel  $x$  s'appelle un **témoin de Solovay** pour  $n$ .

**Question 11.** Donner des témoins de Solovay pour  $n = 6, 8, 9$  et  $21$ .

Sur le modèle du *critère de Miller-Rabin* déjà évoqué, Solovay et Strassen ont proposé un test probabiliste de primalité basé sur la recherche de témoins de Solovay.

**Question 12.** Donner cet algorithme et calculer la complexité de chacune de ses étapes après tirage au hasard.

Il nous reste à déterminer la proportion de témoins de Solovay si  $n$  est composé, en l'espérant aussi grande que possible. En fait, on peut se contenter de vérifier que si  $n$  est composé alors il existe au moins un témoin de Solovay. C'est déjà satisfaisant car l'ensemble des «faux témoins» :

$$\mathcal{S}_n = \{x \in \mathbb{Z}/n\mathbb{Z}^* \mid \chi_1(x) = \chi_2(x)\} = \left\{x \in \mathbb{Z}/n\mathbb{Z}^* \mid \left(\frac{x}{n}\right) = x^{\frac{n-1}{2}}\right\}.$$

forme clairement un sous-groupe de  $\mathbb{Z}/n\mathbb{Z}^*$ . Du coup, le simple fait qu'il ne soit pas  $\mathbb{Z}/n\mathbb{Z}^*$  tout entier si  $n$  n'est pas premier montre que la proportion de faux témoins est moindre que  $\frac{1}{2}$  ou encore que la proportion de témoins de Solovay est au moins égale à  $\frac{1}{2}$ . Montrons donc le :

**Proposition 3.1 (Solovay-Strassen)** *Soit  $n > 1$  un entier impair. Si  $n$  est composé alors il existe un témoin de Solovay, c-a-d un  $x \in \mathbb{Z}/n\mathbb{Z}^*$  tel que  $\chi_1(x) \neq \chi_2(x)$ .*

**Preuve** — Si  $n$  possède un facteur carré alors il existe  $p, m \in \mathbb{Z}$  et  $k \geq 2$  tels que  $n = p^k m$  et  $p \nmid m$ . Le noyau de la surjection canonique  $\mathbb{Z}/n\mathbb{Z}^* \twoheadrightarrow \mathbb{Z}/pm\mathbb{Z}^*$ , constitué des classes modulo  $n$  congrues à 1 modulo  $pm$ , est un groupe cyclique d'ordre  $p^{k-1}$  engendré par  $1 + pm \pmod n$  (comme dans la suite exacte  $1 \rightarrow \langle 1 + p \rangle \rightarrow \mathbb{Z}/p^k\mathbb{Z}^* \rightarrow \mathbb{Z}/p\mathbb{Z}^* \rightarrow 1$ ). Comme nous l'avons déjà remarqué, tout élément de ce groupe est un carré donc la restriction de  $\chi_1$  à ce sous groupe est triviale. En revanche,  $\chi_2$  ne l'est pas car tous les éléments de ce sous groupe sont d'ordre une puissance de  $p$  et  $p$  est premier à  $\frac{n-1}{2}$ .

Si  $n$  est sans facteur carré alors il s'écrit  $n = pm$  avec  $p \in \mathbb{Z}$  premier et  $m \in \mathbb{Z}$  premier à  $p$ . D'après le théorème chinois  $\mathbb{Z}/n\mathbb{Z}^* \simeq \mathbb{Z}/p\mathbb{Z}^* \times \mathbb{Z}/m\mathbb{Z}^*$ . Soit  $y \in \mathbb{Z}/p\mathbb{Z}^*$  un non résidu quadratique et  $x \in \mathbb{Z}/n\mathbb{Z}^*$  dont l'image par le théorème chinois satisfait  $(x \pmod p, x \pmod m) = (y, 1)$ . Par construction on a  $\chi_1(x) = -1$ . En revanche,  $\chi_2(x) \neq -1$  car, de nouveau par construction,  $\chi_2(x) \pmod m = 1$ .

Dans tous les cas, on a bien exhibé un témoin de Solovay. □

En résumé, si  $n$  est composé, parmi les  $\varphi(n)$  éléments de  $\mathbb{Z}/n\mathbb{Z}^*$ , au moins  $\frac{\varphi(n)}{2}$  sont des témoins de Solovay. C'est satisfaisant mais moins bien que la proportion des témoins de Miller-Rabin au moins égale à  $\frac{3\varphi(n)}{4}$ .

### 4 Calcul de racine carrée dans un corps fini

Il n'y a pas lieu ici de se limiter dans un corps premier. C'est pourquoi on considère  $q$  une puissance d'un premier  $p$  et  $\mathbb{F}_q$  le corps fini de cardinal  $q$ . On se place dans le groupe multiplicatif  $\mathbb{F}_q^*$ . On rappelle que ce groupe est cyclique de cardinal  $q - 1$  ; on écrit ce cardinal sous la forme  $q - 1 = 2^\alpha r$  avec  $\alpha \in \mathbb{N}$  et  $r \in \mathbb{N}$  impair. Alors le groupe  $\mathbb{F}_q^*$  se décompose sous la forme :

$$\begin{aligned} \mathbb{F}_q^* &\xrightarrow{\simeq} G_1 \times G_2 \\ h &\longmapsto (h_1, h_2) \end{aligned}$$

où  $G_1$  est cyclique de cardinal  $r$  et où  $G_2$  est cyclique de cardinal  $2^\alpha$ . Le groupe  $G_2$  est aussi le 2-syloew de  $\mathbb{F}_q^*$ .

**Question 13.** Donner la version explicite de cet isomorphisme.

Calculer la racine carré d'un élément  $h \in \mathbb{F}_q^*$  revient donc à calculer celles de  $h_1$  et  $h_2$ . Pour le premier, le calcul est évident puisque  $h_1 = \left(h_1^{\frac{r+1}{2}}\right)^2$ . Si  $\alpha = 1$ , c'est-à-dire si  $q \equiv 3 \pmod{4}$ , la partie  $G_2$ , isomorphe à  $\{\pm 1\}$ , ne pose aucun problème et, pour  $h$  carré, on a :

$$h = \left(h^{\frac{r+1}{2}}\right)^2.$$

**Question 14.** Le vérifier.

En revanche, dès que  $\alpha \geq 2$ , il faut bel et bien calculer une racine carrée dans  $G_2$ . Ceci est l'objet de la section suivante. Mais avant de passer à celle-ci remarquons que l'on peut éviter de décomposer  $h$  sous la forme  $(h_1, h_2)$  en écrivant :

$$h = \left(h^{\frac{r+1}{2}}\right)^2 \times (h^r)^{-1};$$

le calcul de la racine carré de  $h \in \mathbb{F}_q^*$  est donc ramené à celle de l'élément  $h^r$  qui appartient à  $G_2$ .

#### 4.1 Racine carrée dans le 2-syloew de $\mathbb{F}_q^*$

Commençons par établir le lemme :

**Lemme 4.1** *Dans un 2-groupe cyclique on a :*

1. *le produit  $xy$  de deux éléments  $x$  et  $y$  ayant le même ordre est d'ordre strictement plus petit;*
2. *les non carrés sont exactement les générateurs du groupe (ou les carrés sont exactement les éléments d'ordre strictement inférieur à l'ordre du groupe).*

**Question 15.** Le prouver.

Supposons que l'on connaisse un générateur  $g$  de  $G_2$  (on verra à la fin de cette section comment en produire facilement). Tout élément  $h$  de  $G_2$  s'écrit donc sous la forme  $h = g^\beta$  avec  $0 \leq \beta \leq 2^\alpha - 1$ ; on dit que  $\beta$  est le logarithme discret de  $h$  en base  $g$ . Les carrés ne sont rien d'autre que les éléments dont le logarithme discret est pair, auquel cas  $g^{\frac{\beta}{2}}$  est une racine carrée de  $h$ . Ainsi calculer une racine carrée de  $h$  revient à déterminer  $\beta$  le logarithme discret de  $h$ . Pour cela décomposons  $\beta$  en base 2 :

$$\beta = \beta_0 + 2\beta_1 + \dots + 2^{\alpha-1}\beta_{\alpha-1}, \quad \beta_i \in \{0, 1\}.$$

Remarquons que si  $\beta_i$  est le premier coefficient non nul, alors  $h$  est d'ordre  $2^{\alpha-i}$ . Autrement dit, le calcul de l'ordre de  $h$  donne les premiers coefficients. Pour continuer, on remarque qu'en vertu de lemme précédent, l'élément  $h \times g^{-2^i}$  est d'ordre strictement inférieur à  $2^{\alpha-i}$ . On peut donc itérer le processus jusqu'à ce que l'ordre vaille 1.

**Question 16.** Montrer les affirmations concernant les ordres et en déduire un algorithme de calcul de racine carré dans  $G_2$ .

Il ne reste plus qu'à montrer que l'on sait calculer un générateur de  $G_2$ . Pour cela, on tire au hasard un élément de  $g \in \mathbb{F}_q^*$  jusqu'à ce que  $g$  soit un non-résidu quadratique, c'est-à-dire jusqu'à ce que  $\left(\frac{g}{q}\right) = -1$ ; comme ces derniers occupent la moitié des éléments de  $\mathbb{F}_q^*$ , à chaque tirage, on a une chance sur deux d'obtenir un non-résidu quadratique. On vérifie ensuite que  $g^r$  est forcément un générateur de  $G_2$ .

## 5 Racine carrée dans $\mathbb{Z}/pq\mathbb{Z}$

Nous venons de voir que l'on sait efficacement calculer une racine carrée modulo un premier  $p$ . On peut légitimement se poser la question de savoir ce qu'il en est de la difficulté de ce problème quand le modulus  $N$  n'est plus premier. S'il est une puissance d'un premier  $p$ , le calcul d'une racine carrée se ramène à celui d'une racine carrée modulo  $p$ , grâce au lemme de Hensel. Si  $N = pq$  avec  $p$  et  $q$  deux premiers distincts (ou plus généralement si  $N$  se factorise en plusieurs premiers), le problème se ramène à celui d'une racine carrée modulo  $p$  et  $q$  grâce au théorème chinois. Malheureusement, cela suppose que l'on connaisse  $p$  et  $q$ , c'est-à-dire que l'on sache factoriser efficacement  $N$ . On sait bien qu'il n'en est rien à ce jour.

La fonction  $x \mapsto x^2$  de  $\mathbb{Z}/N\mathbb{Z}^*$  dans lui-même est donc facile à évaluer mais il est difficile de trouver un antécédent d'un élément  $y \in \mathbb{Z}/N\mathbb{Z}^*$  donné. On qualifie cette fonction **d'asymétrique**. En revanche, dès lors que  $p$  et  $q$  sont connus, le calcul de l'inverse devient à nouveau facile ; on dit que la fonction  $x \mapsto x^2$  de  $\mathbb{Z}/N\mathbb{Z}^*$  est une fonction **trappe**.

Ces fonctions sont très recherchées en cryptographie et plus généralement en théorie de l'information. On les aime d'autant plus que «casser leur asymétrie» est un problème aussi difficile qu'un autre problème réputé difficile.

### 5.1 Qui sait calculer une racine carrée modulo $N$ sait factoriser $N$

L'objet de cette section est de montrer que calculer un résidu quadratique modulo un entier  $N$  de la forme  $pq$  ( $p, q$  premiers distincts) est au moins aussi difficile que factoriser  $N$ . Pour cela, supposons que l'on dispose d'une «boîte noire» qui sait calculer un résidu quadratique modulo  $N$  en temps polynomial, et montrons que l'on est alors en mesure de factoriser  $N$  toujours en temps polynomial de façon probabiliste.

L'idée est simple : remarquons que dans  $\mathbb{Z}/N\mathbb{Z}^* \simeq \mathbb{Z}/p\mathbb{Z}^* \times \mathbb{Z}/q\mathbb{Z}^*$ , un carré n'a pas deux racines carrées comme à l'accoutumé mais quatre ! C'est dû au fait qu'il y a quatre racines carrées de 1, à savoir  $\pm 1$  et les éléments correspondant par le chinois aux couples  $(1 \bmod p, -1 \bmod q)$  et  $(-1 \bmod p, 1 \bmod q)$ . Si maintenant  $y^2 = y'^2 = x$  sont deux racines carrées de  $x$  telles que  $y' \neq \pm y$  alors  $\text{pgcd}(N, y - y') = p$  ou  $q$ .

**Question 17.** Le montrer.

En pratique, on tire au hasard  $y \in \mathbb{Z}/N\mathbb{Z}^*$ , on l'élève au carré  $x = y^2$  puis on détermine  $y'$  la racine carrée de  $x$  calculée grâce à la boîte noire. Avec en gros une chance sur deux on a  $y' \neq \pm y$  auquel cas  $N$  est factorisé. Si tel n'est pas le cas, libre à nous de recommencer en tirant au hasard un nouvel élément  $y \in \mathbb{Z}/N\mathbb{Z}^*$ .

### 5.2 Application : un protocole d'identification

Un problème central pour la sécurisation des communications est celui de l'identification. Il s'agit de s'assurer de l'identité d'un correspondant ou d'un interlocuteur.

Supposons que Dalva est membre d'une Organisation secrète et a reçu l'ordre de prendre contact avec Duane. Elle n'a jamais rencontré Duane et ne peut l'identifier à sa seule apparence physique (surtout si la prise de contact se fait par téléphone ou internet). De son côté, Duane ne connaît pas Dalva. Afin d'éviter une infiltration, Dalva et Duane recourent à un procédé d'identification. L'organisation a imposé le protocole suivant. Duane s'approche de Dalva et lui dit «Rivière». Dalva répond alors «Niobrara». Si tout se passe comme prévu Dalva et Duane savent qu'ils sont bien en présence l'un de l'autre. Cela suppose bien sûr que les deux mots de passe («Rivière» et «Niobrara») fournis par l'organisation n'ont pas été éventés avant la rencontre. En outre, ces mots de passe ne pourront être utilisés qu'une fois car un tiers, membre d'une organisation ennemie, pourrait surprendre l'échange des mots de passe entre Duane et Dalva. Pire encore, une fausse Dalva (baptisons la Calva) pourrait se présenter à Duane qui lui dévoilerait alors son mot de passe «Rivière» afin de s'identifier auprès d'elle. Elle pourrait alors communiquer ce mot de passe à un faux Duane qui pourrait à son tour se faire passer pour le vrai Duane auprès de la vraie Dalva...

Ces difficultés bien connues et bien réelles soulevées par les méthodes classiques d'identification résultent des deux principes contradictoires suivants.

- L'identité est définie par la connaissance d'une information (le mot de passe par exemple) qui doit rester secrète.
- La reconnaissance suppose que l'on dévoile au moins une partie de cette information (communication du mot de passe dans notre exemple).

Les techniques biométriques d'identification (empreintes digitales, observation de l'iris, reconnaissance de la voix) échappent à cette contradiction mais ce n'est pas le propos de ce texte de les présenter.

Nous définissons l'identité par la connaissance d'une information secrète et nous voulons montrer qu'il est possible à Duane de prouver à Dalva qu'il connaît un certain secret sans rien lui en dévoiler. Cette possibilité d'une preuve **sans apport d'information**<sup>1</sup> a été entrevue à la fin des années 80.

Nous sommes maintenant en mesure de décrire un protocole d'identification sans apport d'information basé sur les résidus quadratiques. On suppose que chaque membre  $X$  de l'organisation choisit deux grands nombres premiers  $p_X$  et  $q_X$  et forme leur produit  $N_X = p_X q_X$ . Il choisit aussi au hasard un résidu quadratique  $r_X$  modulo  $N_X$  avec distribution uniforme, et une racine carrée  $s_X$  telle que  $s_X^2 = r_X \pmod{N_X}$ . L'ensemble des triplets  $(X, N_X, r_X)$  est publié dans l'annuaire de l'organisation. En revanche, les facteurs premiers  $p_X$  et  $q_X$  et la racine carrée  $s_X$  sont connus de  $X$  seul. C'est la connaissance de  $s_X$  qui distingue  $X$ .

Lorsque Dalva prépare sa rencontre avec Duane elle consulte l'annuaire et prend connaissance du triplet  $(\text{Duane}, N_{\text{Duane}}, r_{\text{Duane}})$  correspondant. Au moment de la rencontre, pour s'assurer qu'elle est bien en présence de Duane elle doit se convaincre que son interlocuteur connaît une racine de  $r_{\text{Duane}}$  modulo  $N_{\text{Duane}}$ . Elle procède de la façon suivante :

1. Duane choisit un résidu quadratique  $r = s^2 \pmod{N_{\text{Duane}}}$  aléatoire (avec distribution uniforme) et calcule  $t = r r_{\text{Duane}} \pmod{N_{\text{Duane}}}$ . Il transmet  $t$  à Dalva.
2. Dalva choisit un élément  $\varepsilon$  au hasard (avec distribution uniforme) dans  $\{\pm 1\}$  et le transmet à Duane.
3. Si  $\varepsilon = 1$  Duane transmet  $s$  à Dalva. Sinon il transmet une racine carrée de  $t$  modulo  $N_{\text{Duane}}$ , à savoir  $u = s s_{\text{Duane}}$ .
4. Si  $\varepsilon = 1$ , Dalva calcule  $r = t / r_{\text{Duane}} \pmod{N_{\text{Duane}}}$  et vérifie que  $r = s^2 \pmod{N_{\text{Duane}}}$ . Si  $\varepsilon = -1$ , Dalva vérifie que  $t = u^2 \pmod{N_{\text{Duane}}}$ .

On vérifie sans peine que ce protocole s'exécute en temps polynomial en  $\log(N_{\text{Duane}})$ . Ce protocole est reproduit un grand nombre de fois (par exemple 1000 fois). Si les conditions vérifiées par Dalva à la dernière étape sont satisfaites à chaque fois, alors Dalva reconnaît Duane en son interlocuteur. Sinon elle l'accuse d'imposture.

Si un ennemi (appelons le Mickael) veut se faire passer pour Duane auprès de Dalva sans connaître une racine de  $r_{\text{Duane}}$  il ne peut pas connaître à la fois un  $s$  et un  $u$  tels que  $u^2 = t$  et  $s^2 = r$  donc il est pris en défaut avec probabilité  $\frac{1}{2}$  à chaque exécution du protocole.

Si c'est bien Duane qui se présente à Dalva, il sait répondre à toutes ses questions. En outre, Dalva n'apprend rien sur le secret de Duane car elle observe seulement une suite aléatoire de résidus quadratiques modulo  $N_{\text{Duane}}$ . Mais elle peut aussi bien fabriquer une telle suite elle-même sans le secours de Duane. Elle n'apprend donc rien.

### 5.3 Le problème de résiduosit  quadratique

On vient de voir que si  $N$  n'est pas la puissance d'un premier, le calcul d'une racine carr e dans  $\mathbb{Z}/N\mathbb{Z}^*$  est difficile d s lors que la factorisation de  $N$  est inconnue. On peut se demander si le probl me — a priori plus simple — de d cider si un  l ment  $x \in \mathbb{Z}/N\mathbb{Z}^*$  est un carr  ou non reste difficile. Cette question n'a d'int r t que si on la restreint au noyau du symbole de Jacobi,

$$\mathcal{J}_1 \stackrel{\text{d f.}}{=} \left\{ x \in \mathbb{Z}/N\mathbb{Z}^* \mid \left( \frac{x}{N} \right) = 1 \right\},$$

<sup>1</sup>C'est le «zero-knowledge proof» en anglais.

car si  $\left(\frac{x}{N}\right) = -1$  alors  $x$  n'est pas un carré. En revanche, la question reste pertinente restreinte à  $\mathcal{J}_1$  car ce n'est pas parce que  $\left(\frac{x}{N}\right) = 1$  que  $x$  est un carré modulo  $N$ .

**Question 18.** Vérifier ces affirmations.

Un élément de  $\mathcal{J}_1$  qui n'est pas un carré s'appelle un **faux carré**. Le **problème de résiduosit  quadratique** est celui de distinguer les faux carrés des vrais. De la m me fa on qu'il est commun ment admis qu'il n'existe pas d'algorithmes polynomiaux permettant de factoriser un entier  $N$ , on pense qu'il n'existe pas d'algorithmes polynomiaux permettant de distinguer les faux carrés des vrais ayant une bonne probabilit  de succ s. M me si on ne sait pas prouver ce genre de r sultat   ce jour, tout le monde s'accorde cependant   faire l'hypoth se suivante :

**Hypoth se 5.1 (Difficult  de la r siduosit  quadratique)** *Tout algorithme probabiliste polynomial de d cision de la r siduosit  quadratique dans  $\mathbb{Z}/N\mathbb{Z}^*$  a une probabilit  de succ s de la forme  $\frac{1}{2} + \varepsilon$  avec  $\varepsilon$  n gligeable devant toute puissance de  $\log(N)$ .*

## 5.4 Application : un g n rateur de bits al atoires

Le probl me que l'on se pose dans cette section est le suivant : «comment apprendre   un ordinateur   tirer au hasard?». Le caract re intrins quement «d terministe» d'un ordinateur ne facilite pas la r solution d'un tel probl me. En fait, on va plut t montrer un proc d  qui partant d'une courte cha ne de bits tir e au hasard permet de produire des cha nes beaucoup plus longues dont la distribution ne peut pas  tre distingu e d'une distribution al atoire. En anglais on dit parfois que l'on a «boost  le hasard»<sup>2</sup>. Voici la d finition pr cise d'un g n rateur pseudo-al atoire de bits.

**D finition 5.2** *Soient  $k \in \mathbb{N}^*$  et  $l > k$  un polyn me en  $k$ . Un  $(k, l)$ -g n rateur pseudo-al atoire de bits<sup>3</sup> est une fonction  $f : \{0, 1\}^k \rightarrow \{0, 1\}^l$  qui peut  tre calcul e en temps polynomial en  $k$ . L'entr e  $s_0 \in \{0, 1\}^k$  s'appelle le terme initial ou la graine et l'image  $f(s_0)$  s'appelle la cha ne al atoire de bits.*

Blum, Blum et Shub ont propos  un mod le de g n rateur pseudo-al atoire bas  sur les r sidus commun ment appel  g n rateur BBS. On part de deux premiers  $p, q$  tels que  $p, q \equiv 3 \pmod{4}$  et dont le produit  $N = pq$  est de taille  $k$ . Les graines sont tir es parmi les carr s de  $\mathbb{Z}/N\mathbb{Z}^*$ . Si  $s_0$  est l'une d'entre elles, on note  $(s_i)_i$  la suite de  $\mathbb{Z}/N\mathbb{Z}^*$  d finie par la r currence  $s_{i+1} = s_i^2 \pmod{N}$  — dans toute la suite,  $x \pmod{N}$  d signe le repr sentant de  $x$  modulo  $N$  appartenant    $[0..N - 1]$  —. Le g n rateur est alors d fini par :

$$f(s_0) = (s_1 \pmod{2}, \dots, s_l \pmod{2}).$$

Autrement dit les bits al atoires g n r s ne sont rien d'autre que les bits initiaux des termes de la suite  $(s_i)_i$  ou encore les bits de parit  de ces termes.

**Question 19.** Impl menter ce g n rateur en `maple`.

Il convient maintenant de d finir ce qui fait la qualit  d'un g n rateur. Plusieurs points de vue sont envisageables. Nous ne traiterons ici que de la qualit  cryptographique d'un g n rateur qui n'a de sens qu'asymptotiquement lorsque  $k$  tend vers l'infini.

L'id e derri re la d finition de la qualit  d'un g n rateur  $f$  est que ce dernier ne doit pas alt rer le hasard. Plus pr cis ment, avec des moyens de calcul raisonnables (i.e. polynomiaux en  $k$  ou  $l$ , ce qui revient au m me), on souhaite qu'il soit impossible de distinguer une s rie de cha nes de bits de  $\{0, 1\}^l$  «vraiment» tir e au hasard d'une s rie de cha nes de bits  $f(s_0)$  de  $\{0, 1\}^l$  o  la s rie des graines  $s_0 \in \{0, 1\}^k$  a  t  tir e au hasard. Cette id e peut  tre formalis e plus rigoureusement en termes de probabilit s (cf. [Sti03], §12.2).

Cependant, nous ne nous  tendrons pas l -dessus car cette d finition, qui colle   l'intuition, peut  tre rendue plus maniable en montrant qu'elle est  quivalente au fait qu'il n'existe pas d'algorithme efficace qui, connaissant une portion non n gligeable de la cha ne al atoire, permet de deviner, avec

<sup>2</sup>Boosting randomness.

<sup>3</sup>En anglais, on dit « $(k, l)$ -pseudo-random bit generator» et on l'abr ge souvent PRBG.

une probabilité significativement plus grande que  $\frac{1}{2}$ , le bit suivant ou précédent. On peut par exemple s'intéresser à l'efficacité d'un **algorithme de prédiction du bit précédent** pour le générateur  $f$  qui est un algorithme polynomial et probabiliste prenant en entrée une chaîne de bits  $(b_1, \dots, b_l) \in \{0, 1\}^l$  provenant de l'application de  $f$  à une graine (inconnue)  $s_0 \in \{0, 1\}^k$  et qui prédit la parité de la graine (ou le bit initial), à savoir  $s_0 \bmod 2$ . On souhaite que la probabilité de succès d'un tel algorithme ne soit pas significativement plus grande que  $\frac{1}{2}$  :

**Définition 5.3** *Un  $(k, l)$ -générateur pseudo-aléatoire de bits est dit **cryptographiquement sûr** si tout algorithme de prédiction du bit précédent a une probabilité de succès de la forme  $\frac{1}{2} + \varepsilon$  avec  $\varepsilon$  négligeable devant  $k$  quand celui-ci tend vers l'infini.*

On va établir la sécurité du générateur BBS en deux étapes :

– **Etape 1** : s'il existe un algorithme polynomial de prédiction du bit précédent avec une probabilité de succès au moins égale à  $\frac{1}{2} + \varepsilon$ , alors il existe un algorithme de décision de la résiduosit  quadratique modulo  $N$  ayant une probabilité de succès au moins  gale    $\frac{1}{2} + \varepsilon$ .

– **Etape 2** : s'il existe un algorithme polynomial de d cision de la r siduosit  quadratique modulo  $N$  ayant une probabilit  de succ s au moins  gale    $\frac{1}{2} + \varepsilon$ , alors il existe de algorithme Monte Carlo de d cision de la r siduosit  quadratique ayant une probabilit  d'erreur aussi petite que voulue.

Comme l'existence d'un tel algorithme contredirait l'hypoth se 5.1, il est admis que le g n rateur BBS est cryptographiquement s r.

**Etape 1** : supposons que l'on dispose d'un algorithme  $\mathcal{A}$  qui pr dise la parit  de la graine   partir de la cha ne de bits qui lui est associ e (sans conna tre la graine  videmment).

Commen ons par quelques remarques sur le contexte du g n rateur BBS. Comme  $p$  et  $q$  sont congrus   3 modulo 4,  $-1$  n'est ni un carr  modulo  $p$  ni modulo  $q$ . Pour  $x \in \mathbb{Z}/p\mathbb{Z}^*$ , on a donc l' quivalence :  $x$  est un carr  si et seulement si  $-x$  n'en est pas un ; autrement dit  $x \mapsto -x$  d finit une bijection des carr s de  $\mathbb{Z}/p\mathbb{Z}^*$  vers les non carr s de  $\mathbb{Z}/p\mathbb{Z}^*$ . On a  videmment le m me ph nom ne modulo  $q$ .

Raisonnons modulo  $N = pq$  maintenant. Tout d'abord  $-1$  est un faux carr , c'est- -dire qu'il appartient    $\mathcal{J}_1$  sans  tre un carr . D'autre part, parmi les quatre racines carr es d'un carr   $x$  de  $\mathbb{Z}/N\mathbb{Z}^*$ , deux exactement appartiennent    $\mathcal{J}_1$  et une seule parmi ces deux est elle aussi un carr  ; on la note  $\sqrt{x}$ . Enfin  $x \mapsto -x$  d finit   nouveau une bijection des carr s de  $\mathcal{J}_1$  vers les non carr s de  $\mathcal{J}_1$ .

Partons de  $x \in \mathcal{J}_1$ . Alors  $\sqrt{x^2} = \pm x$  et on a les  quivalences :

$$x \text{ est un carr } \iff x = \sqrt{x^2} \iff x \bmod N \text{ et } \sqrt{x^2} \bmod N \text{ ont m me parit }$$

car les repr sentants  $x \bmod N$  et  $-x \bmod N$  (dans  $[0..N - 1]$ ) sont forc ment de parit s distinctes. Remarquons que la cha ne al atoire de bits  $f(\sqrt{x^2}) = (b_1, \dots, b_l)$  associ e   la graine  $\sqrt{x^2}$  se calcule, sans conna tre  $\sqrt{x^2}$ ,   partir de  $x$  puisque  $b_i = s_i \bmod 2$  et  $s_{i+1} = s_i^2 \bmod N$ ,  $s_1 = x^2 \bmod N$ . Le r sultat  $\mathcal{A}(b_1, \dots, b_l)$  nous donne la parit  de  $\sqrt{x^2}$ . Cela nous permet imm diatement de d cider si  $x$  est un carr  ou non. Voici l'algorithme qui d coule de ce qui pr c de ; nommons le  $\mathcal{B}$ .

---

Entr e :  $x \in \mathcal{J}_1$

Sortie :  $\{x \text{ est un carr , } x \text{ n'est pas un carr }\}$

Calculer la cha ne  $f(\sqrt{x^2}) = (b_1, \dots, b_l)$    partir de  $x$  ;

Si  $\mathcal{A}(b_1, \dots, b_l) = x \bmod 2$  alors Retourner( $x$  est un carr ) ;

sinon Retourner( $x$  n'est pas un carr ) ;

Fin si ;

---

**Etape 2** : On souhaite pour finir introduire de l'al a dans l'algorithme pr c dent afin d'en d duire un algorithme Monte Carlo r solvant le probl me de r siduosit  quadratique. L'id e, simple, consiste   modifier  $x$  par un carr  ou l'oppos  d'un carr  puis de tester la r siduosit  quadratique avec l'algorithme pr c dent.

---

Entrée :  $x \in \mathcal{J}_1$  et  $B \in \mathbb{N}^*$  une borne  
Sortie :  $\{x \text{ est un carré}, x \text{ n'est pas un carré}\}$

$c := 0$  ; # nombre de fois où  $x$  est décrété carré

Répéter  $B$  fois

Tirer au hasard  $r \in \mathbb{Z}/N\mathbb{Z}^*$  et  $s \in \{\pm 1\}$  ;

Poser  $y = s \times r^2 \times x$  ;

Déterminer si  $y$  est un carré avec l'algorithme  $\mathcal{B}$  ;

# on incrémente  $c$  quand  $x$  est décrété carré

Si  $[(y \text{ carré}) \text{ et } (s = 1)]$  ou

$[(y \text{ non carré}) \text{ et } (s = -1)]$  alors  $c := c + 1$  ; Fin si ;

Fin répéter ;

# On retourne la réponse la plus fréquente

Si  $c > B/2$  alors Retourner( $x$  est un carré) ;

sinon Retourner( $x$  n'est pas un carré) ;

Fin si ;

---

## 5.5 Suggestion de développements

Voici quelques pistes de développements :

- Implémenter une «boîte noire» permettant de calculer une racine carrée modulo  $N = pq$  en connaissant la factorisation  $p \times q$  et basée sur le théorème chinois. Vérifier qu'elle permet de refactoriser  $N$ .
- Infinité de premiers congrus à 3 modulo 4 ?
- Etude statistique de caractère aléatoire des bits fournis par le générateur BBS :
  - équité entre le nombre de zéros et de uns ;
  - équité entre le nombre de blocs 00, 01, 10 et 11 ;
  - pas de répétition de chaînes trop longues.
- Etudier le caractère périodique du générateur BBS. Trouver des premiers  $p$  et  $q$  maximisant cette périodicité.

## Références

- [Dem97] Michel Demazure. *Cours d'Algèbre — Primalité, Divisibilité, Codes*, volume 1 of *Nouvelle Bibliothèque mathématique*. Cassini, 1997.
- [Sti03] Douglas Stinson. *Cryptographie — Théorie et pratique*. Vuibert, 2003.