Contrôle continu de cryptographie

— Partie I —

Résiduosité quadratique et symbole de Legendre-Jacobi

Si a et n sont deux entiers (avec $n > 1$), on dit que a est un *résidu quadratique* modulo n s'il existe $x \in \mathbb{Z}$ tel que $a = x^2 \bmod n$; de façon équivalente, la classe de a (encore notée a s'il n'y a pas d'ambiguïté) est un carré dans $\mathbb{Z}/n\mathbb{Z}$.

Le problème de la résiduosité quadratique consiste à déterminer si un entier est un résidu quadratique modulo n. Un outil pour l'étude de ce problème est le symbole de Jacobi (ou de Legendre-Jacobi), dont on donne la définition :

Définition. *Si p est un nombre premier impair, pour tout $a \in \mathbb{Z}$ le symbole de Jacobi est défini par*

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

Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ est un entier **impair** *composé, pour tout $a \in \mathbb{Z}$ on pose $\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i}$.*

Nonobstant cette définition, il est possible de calculer efficacement le symbole $\left(\frac{a}{n}\right)$ **sans passer par la factorisation de** n, ce qui en fait un outil très pratique.

1. Soit n un entier impair.
   (a) Montrer que si a et b sont congrus modulo n alors $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
   (b) Montrer que $\left(\frac{a}{n}\right) = 0$ si et seulement si a et n ne sont pas premiers entre eux.

Soit p un entier premier impair.

2. **Carrés modulo p**
   (a) En considérant le morphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$, $x \mapsto x^2$ dont on déterminera le noyau, montrer qu'il y a exactement $(p-1)/2$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$.
   (b) Montrer que pour tout $a \in \mathbb{Z}$,

   $$a \text{ est un résidu quadratique mod } p \iff p \mid a \text{ ou } a^{(p-1)/2} = 1 \bmod p.$$

   Indication : déterminer les racines du polynôme $X^{(p-1)/2} - 1$ dans $\mathbb{Z}/p\mathbb{Z}$.
   (c) En déduire l'égalité $\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$, pour tout $a \in \mathbb{Z}$.

3. **Carrés modulo p^α**
   (a) Soit $\alpha \geq 2$ un entier. Montrer que si a est un résidu quadratique modulo p^α, alors c'est un résidu quadratique modulo p.

(b) Soit $k \in \mathbb{N}^*$, et a un résidu quadratique modulo p^k tel que $p \nmid a$.
On note x un entier tel que $a = x^2 \bmod p^k$.

i. Justifier que $2x$ est inversible modulo p.

ii. Montrer qu'il existe $y \in \mathbb{Z}$ tel que $a = (x + p^k y)^2 \bmod p^{k+1}$, puis que a est un résidu quadratique modulo p^{k+1}.

(c) Montrer que si $p \nmid a$ et a est un résidu quadratique modulo p, alors a est un résidu quadratique modulo p^α.

(d) Montrer que p n'est pas un résidu quadratique modulo p^α.

4. **Carrés modulo n composé**
Soit $n = \prod_{i=1}^r p_i^{\alpha_i}$ un entier impair, avec p_i des nombres premiers distincts et $\alpha_i \in \mathbb{N}^*$.

(a) À l'aide de la question 2.(c), montrer la multiplicativité du symbole de Jacobi : pour tout $a, b \in \mathbb{Z}$, $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

(b) Montrer qu'un entier a est un résidu quadratique modulo n si et seulement si c'est un résidu quadratique modulo chacun des $p_i^{\alpha_i}$.

(c) Montrer que si $\left(\frac{a}{n}\right) = -1$ alors a n'est pas un résidu quadratique modulo n.

(d) Montrer que si $n = pq$ est un produit de deux facteurs premiers distincts, alors il existe $a \in \mathbb{Z}$ tel que $\left(\frac{a}{n}\right) = 1$ mais a n'est pas un résidu quadratique modulo n.

Ainsi, si $\left(\frac{a}{n}\right) = -1$ alors on sait que a n'est pas un résidu quadratique modulo n, mais la réciproque est fausse quand n est composé. Quand $\left(\frac{a}{n}\right) = 1$, on ne connait pas actuellement de méthode pour déterminer si a est un résidu quadratique modulo n sans passer par la factorisation de n.

Test de primalité de Solovay-Strassen

Si n est un nombre premier impair, alors pour tout a non divisible par n on a $\left(\frac{a}{n}\right) = a^{(n-1)/2} \bmod n$. Cette remarque est à la base du test de primalité de Solovay-Strassen : pour tester un entier n impair,
— choisir $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ au hasard ;
— calculer $a^{(n-1)/2} \bmod n$ par un algorithme d'exponentiation rapide ;
— calculer $\left(\frac{a}{n}\right)$;
— si $\left(\frac{a}{n}\right) \neq a^{(n-1)/2} \bmod n$, répondre que n n'est pas premier (sinon, n est peut-être premier).

En pratique si n n'est pas premier, la plupart du temps $a^{(n-1)/2}$ sera différent de $\pm 1 \bmod n$: c'est le principe du test de primalité de Fermat, dont Solovay-Strassen est donc un raffinement.

Soit $G = \left\{ a \in (\mathbb{Z}/n\mathbb{Z})^\times : \left(\frac{a}{n}\right) = a^{(n-1)/2} \bmod n \right\}$.

5. Montrer que G est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.

On va montrer que ce sous-groupe est strict si n n'est pas premier, en distinguant deux cas.

6. Premier cas : $n = p_1 \dots p_s$ est un produit de nombres premiers distincts, avec $s \geq 2$.

(a) Justifier l'existence de $x \in \mathbb{Z}$ tel que $x = 1 \bmod p_2 \dots p_s$ et x non résidu quadratique modulo p_1.

(b) Montrer que $x^{(n-1)/2} \neq -1 \bmod n$, et en déduire que $x \in (\mathbb{Z}/n\mathbb{Z})^\times \setminus G$.

7. Deuxième cas : $n = p^\alpha m$ avec p premier, $\alpha \geq 2$, $p \nmid m$.

(a) On pose $y = 1 + p$. Montrer que $y^{p-1} \neq 1 \bmod p^\alpha$.

(b) Montrer que l'ordre de y^{p-1} dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est égal à p^k avec $1 \leq k \leq \alpha - 1$. En déduire que $y^{(n-1)/2} \neq \pm 1 \bmod p^\alpha$.

(c) Exhiber finalement un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times \setminus G$.

8. Déduire des questions précédentes que ce test permet de détecter, avec une probabilité supérieure à $1/2$, qu'un entier n n'est pas premier.
Donner une borne supérieure de la probabilité qu'un entier n non premier passe k fois le test avec succès.

9. Proposer une variante du test où l'entier a est choisi au hasard uniformément dans $\{1, \ldots, n-1\}$.

Pile ou face à distance

Le problème de la résiduosité quadratique permet de construire un protocole de pile ou face à distance entre deux participants Alice et Bob :

— (Mise en place) Alice choisit un nombre impair $n = pq$, avec p, q deux nombres premiers distincts, et tel que $\left(\frac{-1}{n}\right) = 1$ et le transmet à Bob.
— Bob choisit $x \in \mathbb{Z}/n\mathbb{Z}$ et transmet $c = x^2$ à Alice.
— Alice doit deviner le symbole de Jacobi de x ; elle envoie $\epsilon = 1$ ou -1 à Bob.
— Bob dévoile x ; Alice vérifie que $x^2 = c$.
— Alice gagne si $\left(\frac{x}{n}\right) = \epsilon$ ou 0, et perd sinon.

On peut rejouer en recommençant à la deuxième étape.

Pour tout $a \in \mathbb{Z}/n\mathbb{Z}$, on note a' l'unique élément de $\mathbb{Z}/n\mathbb{Z}$ tel que $a' = a \bmod p$ et $a' = -a \bmod q$.

10. Montrer que pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, les seuls éléments de $\mathbb{Z}/n\mathbb{Z}$ dont le carré vaut x^2 sont x, x', $-x$ et $-x'$.

11. Montrer que si Bob connaît dans $\mathbb{Z}/n\mathbb{Z}$ deux éléments x_1 et x_2 tels que $x_1^2 = x_2^2 = c$ et $x_1 \neq \pm x_2$, alors il peut facilement trouver un facteur non trivial de n.

On suppose désormais que p et q sont deux grands nombres premiers, de telle sorte que l'entier n est impossible à factoriser en pratique.

12. Pourquoi faut-il que $\left(\frac{-1}{n}\right) = 1$?

13. Alice, elle, connaît la factorisation de n ; on verra dans la partie suivante qu'elle peut alors calculer les quatre racines carrées de c dans $\mathbb{Z}/n\mathbb{Z}$.
Montrer que cette information lui permet de gagner à tous les coups si $\left(\frac{-1}{p}\right) = \left(\frac{-1}{q}\right) = 1$.

14. En déduire qu'Alice ne peut pas tricher si p et q congrus à 3 mod 4.

15. Bob peut-il vérifier que cette condition est satisfaite ? Le cas échéant, proposer une modification du protocole permettant à Bob de s'assurer qu'Alice n'a pas triché dans le choix de n.

— Partie II —

Calcul de racines carrées dans $\mathbb{F}_p$: algorithme de Tonelli–Shanks

Soient p un nombre premier impair et $s, t \in \mathbb{N}^*$ tels que $p - 1 = 2^s t$ avec $2 \nmid t$. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

L'algorithme de Tonelli-Shanks utilise le fait que le groupe multiplicatif de $\mathbb{F}_p^*$ est **cyclique** : il existe un élément $g \in \mathbb{F}_p^*$ tel que $\mathbb{F}_p^* = \langle g \rangle$. Soit G_{2^s} le sous-groupe engendré par g^t, c'est un sous-groupe cyclique d'ordre 2^s.

Soient a un carré dans $\mathbb{F}_p^*$ et b un non-carré dans $\mathbb{F}_p^*$.

1. Montrer qu'il existe $x \in G_{2^s}$ tel que $a^t = x^2$. Exprimer les racines carrées de a en fonction de a et de x. *Indication : calculer le carré de* $a^{(t+1)/2}$.
2. Montrer que b^t est un générateur de G_{2^s}. *Indication : écrire* b *sous la forme* g^k *et utiliser en le justifiant le fait que* k *est alors impair.*
3. Écrire un programme `find_generator(p)` qui choisit des éléments aléatoires dans $\mathbb{Z}/p\mathbb{Z}$ jusqu'à trouver un non-carré b, puis qui renvoie (s, t, b^t).
   On pourra créer le corps $F = \mathbb{Z}/p\mathbb{Z}$ avec l'instruction `F=Zmod(p)` et tirer des éléments aléatoires dans A en appelant la fonction `F.random_element()`.
4. Soit u un générateur de G_{2^s}. Montrer que le logarithme discret k de a^t en base u est pair, et que $x = u^{k/2}$ est une racine carrée de a^t.

On rappelle le principe de l'algorithme de Pohlig-Hellman : on note $c_0 + c_1 2 + \cdots + c_{s-1} 2^{s-1}$ l'écriture en base 2 du logarithme discret d'un élément h en base u, avec u d'ordre 2^s. Connaissant $c_0, \ldots, c_{i-1}$, on peut alors obtenir c_i comme le logarithme de discret de $\left(h.u^{-(c_0+c_1 2+\cdots+c_{i-1}2^{i-1})}\right)^{2^{s-1-i}}$ en base $u^{2^{s-1}}$.

5. Ici, que vaut $u^{2^{s-1}}$? Comment simplifier le calcul de c_i en conséquence ?
6. Écrire un programme `DLP_2s(h,u,s)` qui prend en entrée un élément u d'ordre 2^s, un élément h dans le groupe engendré par u, et renvoie le logarithme discret de h en base u en utilisant l'algorithme de Pohlig-Hellman.
   Challenge : calculer le logarithme discret de $h = 25184$ en base $u = 61204$ dans $\mathbb{Z}/65537\mathbb{Z}$. On pourra utiliser l'instruction `F=Zmod(65537); u=F(61204);` pour définir l'entier u modulo p.
7. Écrire enfin un programme qui calcule les racines carrées modulo un nombre premier impair p. Estimer sa complexité.
   Challenge : calculer les racines carrées de -12346 dans $\mathbb{Z}/p\mathbb{Z}$ avec $p = 97.2^{400} + 1$.