TP Maple Option Calcul Formel Agrégation.
Cryptosystème de Rabin

16 avril 2013

1 Racine carrée modulo un nombre premier

Soit p un nombre premier impair et soit a un entier tel que $\left(\frac{a}{p}\right) = 1$. Il existe un entier x tel que $x^2 \equiv a \pmod p$. Pour déterminer x, on peut faire une recherche exhaustive (*la programmer*) et cela prendrait $O(p)$ opérations.

Dans certains cas particuliers on peut donner une expression d'une racine carrée de a modulo p.

Si $p \not\equiv 1 \pmod 4$ alors $p \equiv 3 \pmod 4$. *Une solution est donnée par*

$$x = a^{(p+1)/4} \bmod p.$$

Si $p \equiv 1 \pmod 4$ et $p \not\equiv 1 \pmod 8$, alors $p \equiv 5 \pmod 8$ et $a^{(p-1)/4} \equiv \pm 1 \pmod p$. *Une solution est donnée par*

$$x = \begin{cases} a^{(p+3)/8} \bmod p & si \quad a^{(p-1)/4} \equiv 1 \pmod p \\ 2a(4a)^{(p-5)/8} \bmod p & si \quad a^{(p-1)/4} \equiv -1 \pmod p \end{cases}$$

L'algorithme de Tonelli Shanks est un algorithme probabiliste qui généralise les cas précédents.

Soient s et $t \in \mathbb{N}$ tels que $p-1 = 2^s t$ avec t impair. D'après le théorème de Sylow, $\mathbb{Z}/p\mathbb{Z}^*$ possède un sous-groupe G d'ordre 2^s. Soit z un générateur de G. Comme a est un carré modulo p, on a $a^{(p-1)/2} \equiv 1 \pmod p$ donc $(a^t)^{2^{s-1}} \equiv 1 \pmod p$, donc a^t est dans G et son ordre divise 2^{s-1}. En particulier, *il existe un entier pair* $m \in \{0, \ldots, 2^s - 1\}$ *tel que*

$$a^t z^m = 1.$$

Si l'on pose

$$x = a^{(t+1)/2} z^{m/2}$$

on a donc $x^2 \equiv a \pmod p$.

Deux questions se posent : comment trouver un générateur z de G ? comment trouver m ?

Pour trouver z, on cherche un non carré b dans $\mathbb{Z}/p\mathbb{Z}^*$ et on pose $z = b^t$. Alors $z^{2^{s-1}} = b^{t2^{s-1}} = b^{(p-1)/2} = -1 \bmod p$ et z est d'ordre 2^s. Il y a autant de carrés que de non carrés dans $\mathbb{Z}/p\mathbb{Z}^*$ donc la probabiblité d'échec est $1/2$.

Pour trouver m on procède comme suit : on construit les suites (m_i) et (a_i) définies par : $m_0 = 0$,

$$a_i = (a^t\, z^{m_i})^{2^{s-1-i}} \bmod p$$

$$m_{i+1} = \begin{cases} m_i + 2^i & \text{si } a_i = -1 \\ m_i & \text{sinon} \end{cases}$$

On montre que m_s *est pair et que* $a^t\, z^{m_s} \equiv 1 \pmod p$ *d'où l'on déduit que* $a^{\frac{t+1}{2}}\, z^{\frac{m_s}{2}}$ *est bien une racine carrée de* a *modulo* p.

Pour résumer on obtient donc l'algorithme suivant :

Entrée : p, nombre premier impair ; a carré modulo p
Sortie : une racine carrée de a modulo p

1: Trouver b entre 2 et $p-1$ tel que b ne soit pas un carré modulo p
2: Calculer s, t tels que $p-1 = 2^s t$ avec t impair et $s \in \mathbb{N}$
3: $z \leftarrow b^t$
4: $m \leftarrow 0$
5: **pour** i de 0 à $s-1$ **faire**
6: **si** $(a^t z^m)^{2^{s-1-i}} \equiv -1 \pmod{p}$ **alors**
7: $m \leftarrow m + 2^i$
8: **fin si**
9: **fin pour**
10: **rendre** $a^{(t+1)/2} z^{m/2}$

2 Cryptosystème de Rabin

Pour le cryptosystème RSA, si l'on sait factoriser le module RSA alors on peut casser le cryptosystème, mais la réciproque n'a pas été prouvée.

Le cryptosystème à clé publique de Rabin est un exemple de schéma prouvé sûr : retrouver le message à partir du cryptogramme est équivalent à factoriser le module.

Voici les trois étapes de ce crytposystème : la fabrication des clés, le chiffrement et le déchiffrement.

2.1 Génération des clés

A génère deux grands nombres premiers distincts p et q et calcule $n = pq$.

La clé publique est n, la clé privée est (p, q).

2.2 Chiffrement

B chiffre un message pour A :

- Il consulte l'annuaire des clés où il récupère la clé publique n de A ;
- il représente le message comme un entier m entre 0 et $n-1$;
- il calcule $c = m^2 \bmod n$;
- il envoie le cryptogramme c à A.

2.3 Déchiffrement

A reçoit c

- il calcule les racines carrées $\pm m_p$ de c modulo p et $\pm m_q$ de c modulo q à l'aide de l'algorithme de Tonelli-Shanks ;
- *à l'aide du théorème chinois*, il en déduit les racines $m_1, n-m_1, m_2, n-m_2$ de c modulo n.

Le message initial est l'une de ces quatre valeurs et A n'a aucun moyen de sélectionner le bon message parmi les quatre possibilités. Pour éviter ce problème, on peut ajouter de la redondance au message avant de le chiffrer (par exemple les derniers 64 bits du message peuvent être ajoutés).

Exemple 1

1. *Génération des clés*
   A choisit les nombres premiers $p = 277$ *et* $q = 331$ *et calcule* $n = pq = 91687$.
2. *Chiffrement*
   B souhaite envoyer le message binaire 1001111001*, il ajoute les* 6 *derniers bits et obtient* 1001111001111001 *qui converti, en base* 10 *donne* $m = 40569$.
   B calcule $c = m^2 \bmod n = 62111$ *et envoie* c *à A.*
3. *Déchiffrement*
   A reçoit c *et calcule les* 4 *racines carrées de* c *:* $69654, 22033, 40569, 51118$ *qui en binaires donnent*

$m1 = 10001000000010110, m2 = 101011000010001, m3 = 1001111001111001, m4 = 1100011110101110$

Comme $m3$ *est le seul message avec redondance, A choisit* $m3$ *et retrouve le message* 1001111001.

3 Suggestions

1. Un certain nombre de suggestions sont en italique dans le texte.
2. Vous pourrez démontrer un certain nombre d'affirmations en italique dans le texte.
3. Programmer l'algorithme de Tonelli-Shanks.
4. Ecrire des procédures Maple pour la génération des clés, le chiffrement et le déchiffrement dans le cryptosystème de Rabin.
5. Etant donné un nombre premier p et un entier a qui est un carré modulo p, comment résoudre l'équation $x^2 \equiv a \pmod{p^\alpha}$ où α est un entier > 1 ?