Niveau : 2 **Orange**

Extraire une racine carrée modulo n

1 Le problème

Soit $n > 1$ un entier. Nous nous plaçons dans $\mathbb{Z}/n\mathbb{Z}^*$. Nous dirons que $a \in \mathbb{Z}/n\mathbb{Z}^*$ est un résidu quadratique, s'il existe un $x \in \mathbb{Z}/n\mathbb{Z}^*$, tel que $x^2 = a$ (bien entendu dans $a \in \mathbb{Z}/n\mathbb{Z}^*$, c'est-à-dire modulo n). Nous renvoyons à la fiche « fichecrypto200 » pour des détails sur les résidus quadratiques. Le problème ici sera :

Soit a un résidu quadratique dans $\mathbb{Z}/n\mathbb{Z}^*$, trouver une racine carrée de a dans $\mathbb{Z}/n\mathbb{Z}^*$. Nous étudierons le problèmes dans les deux cas suivants :

1. n est un nombre premier $p > 2$
2. $n = pq$ est le produit de deux nombres premiers distincts > 2.

2 Cas d'un module premier

Soit p un nombre premier impair et soit a un entier qui est un carré dans $\mathbb{Z}/p\mathbb{Z}^*$. Dans ce cas, il y a deux racines carrées de a distinctes et deux seulement. En effet puisque a est un carré, $x^2 - a$ se factorise sous la forme :

$$x^2 - a = (x - x_1)(x + x_1),$$

et comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, il n'y a pas de diviseurs de zéro, ce qui fait que les solutions sont $\pm x_1$.

2.1 Si p est un nombre premier de Blum

Cest le cas où :

$$p \equiv 3 \quad (4).$$

Alors :

$$x_1 = a^{\frac{p+1}{4}} \mod p$$

est une racine carrée.
Preuve.

$$x_1^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}} \times a,$$

mais comme a est un carré :

$$a^{\frac{p-1}{2}} \equiv 1 \quad (p),$$

d'après le petit théorème de Fermat. Donc :

$$x_1^2 \equiv a \quad (p).$$

□

Remarquons que dans ce cas, parmi les deux racines carrées de a qui sont $\pm x_1$ l'une de deux et une seulement est elle-même un carré. Ceci découle tout de suite du fait que $(p-1)/2 = (4k+3-1)/2 = 2k+1$ est impair. Donc un et un seul des deux symboles de Legendre :

$$\left(\frac{\pm x_1}{p}\right) = (\pm x_1)^{\frac{p-1}{2}},$$

vaut 1.

2.2 Si p n'est pas un nombre premier de Blum

C'est le cas où $p \equiv 1 \quad (4)$. Alors dans ce cas, c'est moins simple. Il existe toutefois un algorithme probabiliste de Las Vegas qui calcule une racine carrée de a. C'est l'algorithme de Shank.
On suppose donc maintenant que p est de la forme $4k+1$. On écrit alors :

$$p - 1 = 2^s t,$$

avec t impair et $s \geq 2$.
Soit $a = b^2$ dans $\mathbb{Z}/p\mathbb{Z}^*$. On suppose qu'on connaît un m qui ne soit pas un résidu quadratique modulo p. Posons alors :

$$z = m^t.$$

Par suite :

$$z^{2^{s-1}} = m^{t2^{s-1}} = m^{\frac{p-1}{2}}.$$

Comme m n'est pas un carré on obtient :

$$z^{2^{s-1}} \equiv -1 \quad (p).$$

Posons :

$$B = a^t, \quad X = a^{\frac{t+1}{2}}, \quad Y = z, \quad R = s-1$$

et effectuons l'algorithme suivant :

Tant que $R \geq 1$ **faire**
  si $B^{2^{R-1}} \equiv 1 \ (p)$ **alors**
    $Y := Y^2$;
    $R := R - 1$;
  sinon
    $B := BY^2$;
    $X := XY$;
    $Y := Y^2$;
    $R := R - 1$;
  finsi
fintq ;

On vérifie qu'en sortie, X contient une racine carrée de a. Il suffit pour cela de vérifier que les conditions suivantes constituent un invariant de boucle :

$$\left\{\begin{array}{lcll} aB & = & X^2 & \\ Y^{2^R} & \equiv & -1 & (p) \\ B^{2^R} & \equiv & 1 & (p) \\ R & \geq & 0 & . \end{array}\right.$$

Remarquons que cet algorithme donne le résultat pourvu qu'on ait tiré au sort au début un m qui ne soit pas un résidu quadratique. Ceci donne naissance à un algorithme de Las Vegas.

2.3 Cas d'un module produit de deux nombres premiers distincts > 2

On suppose donc que $n = pq$ (p et q deux nombres premiers distincts) et que a est un carré modulo n premier avec n.
Alors a est un carré non nul modulo p et modulo q. Comme on sait chercher des racines carrés modulo un nombre premier, on peut trouver u et v (qui sont aussi non nuls) tels que :

$$u^2 \equiv a \quad (p),$$

$$v^2 \equiv a \quad (q).$$

Pour trouver les racines carrées de a modulo pq on est donc amené à résoudre les 4 systèmes de congruences :

$$\left\{\begin{array}{l} x_1 \equiv u \quad (p), \\ x_1 \equiv v \quad (q). \end{array}\right.$$

$$\left\{\begin{array}{l} x_2 \equiv u \quad (p), \\ x_2 \equiv -v \quad (q). \end{array}\right.$$

$$\left\{\begin{array}{l} x_3 \equiv -u \quad (p), \\ x_3 \equiv v \quad (q). \end{array}\right.$$

$$\left\{\begin{array}{l} x_4 \equiv -u \quad (p), \\ x_4 \equiv -v \quad (q). \end{array}\right.$$

D'après le théorème des restes chinois, nous obtenons une solution (modulo n) pour chaque système. Ces systèmes sont tous distincts puisque u et v ne sont pas nuls. Les solutions x_1, x_2, x_3, x_4 constituent les 4 racines carrées de a modulo n.
Remarque : on peut aussi donner les résultats dans les cas particuliers ; si $a \equiv 0 \quad (n)$ on a évidemment 0 comme seule racine carrée ; si a est multiple de p ou de q sans être multiple de n, alors on obtient deux racines carrées.

Supposons maintenant que p et q soient deux nombres premiers de Blum. Alors une et une seulement des 4 racines carrées de a est elle-même un carré. En effet si u et v sont tels que :

$$u^2 \equiv a \quad (p),$$

$$v^2 \equiv a \quad (q),$$

alors des deux nombres $\pm u$ un seul est un carré modulo p, suppopsons que ce soit u, des deux nombres $\pm v$ un seul est un carré modulo q, supposons que ce soit v. Dans ces conditions, seul le système de congruence :

$$\begin{cases} x_1 \equiv u \quad (p), \\ x_1 \equiv v \quad (q). \end{cases}$$

donne une solution qui est un carré modulo pq, les 3 autres systèmes donnent des solutions qui ne sont pas des carrés modulo pq.

2.4 Difficulté du problème de l'extraction

Soit $n = pq$ le produit de deux grands nombres premiers. On a vu que si on sait factoriser n, c'est-à-dire si on connait p et q on peut calculer les racines carrées d'un carré a dans $\mathbb{Z}/n\mathbb{Z}^*$. En revanche si on ne sait pas factoriser n, le problème de l'extraction d'une racine carrée d'un carré est un problème difficile. En fait il est calculatoirement aussi difficile que factoriser n. Plus précisément :

Il existe un algorithme polynomial de Las Vegas qui factorise n en utilisant un oracle qui donne une racine carrée dans $\mathbb{Z}/n\mathbb{Z}^*$ de tout nombre carré qu'on lui propose.
Preuve. On tire un x au sort, on calcule $x^2 \mod n$, on le soumet à l'oracle qui fournit y tel que $y^2 \mod n = x^2$. Il y a une probabilité $1/2$ pour que le y retouné par l'oracle soit $\neq \pm x$. Dans ce cas, $\gcd(x - y, n) = p$ ou q. Si l'oracle retourne $\pm x$ on tire un autre nombre au sort. □