LES CARRÉS DE $\mathbb{Z}/N\mathbb{Z}$

RÉSUMÉ ET QUESTIONS

1. LES CARRÉS DE $\mathbb{Z}/p\mathbb{Z}$

Considérons à titre d'exemple le numbre premier $p = 13$. Écrire la liste des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$. Combien sont ils ? Pourquoi ?

Soit p un nombre premier impair. Pour tout entier x on définit $\left(\frac{x}{p}\right)$ de la façon suivante :

(1) $\left(\frac{x}{p}\right) = 0$ si p divise x,

(2) $\left(\frac{x}{p}\right) = 1$ si x est un carré non nul modulo p,

(3) $\left(\frac{x}{p}\right) = -1$ si x n'est pas un carré modulo p.

L'application $x \mapsto \left(\frac{x}{p}\right)$ induit un morphisme de groupes de $\mathbb{F}_p^*$ dans $\{1, -1\}$. On dit que c'est un caractère.

En fait $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \bmod p$. Cela donne une première méthode pour calculer efficacement ce symbole.

On a la fameuse loi de réciprocité quadratique

Théorème 1.1. *Si p et q sont des premiers impairs positifs et distincts, alors*

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

On pourra vérifier ce théorème sur quelques exemples. Par exemple avec $p = 5$ et $q = 7$. Puis avec $p = 5$ et $q = 3$.

2. CALCUL DE RACINES CARRÉES DANS $\mathbb{Z}/p\mathbb{Z}$

Prenons $p = 103$ et $x = 46$. On vérifie que $46^{51} \equiv 1 \bmod 103$ donc 46 est un carré modulo 103.

Comme p est congru à 3 modulo 4 on a $51 = \frac{p-1}{2}$ impair. L'inverse de 2 modulo 51 est donné par l'algorithme d'Euclide étendu et c'est 26. On a bien en effet (et on aurait pu s'en appercevoir plus vite)

$$26 \times 2 = 1 + 51.$$

Posons $y = x^{26} \bmod 103$. On a $y^2 = x^{1+51} = x$ donc y est une racine de x. Le calcul de $y = x^{26}$ se fait sans difficulté par exponentiation rapide et on trouve $y = 46 \bmod 103$.

Cette méthode est très efficace si p est un nombre premier congru à 3 modulo 4.

Supposons maintenant que $p = 101$ et $x = 13 \bmod 101$. On vérifie que $x^{50} \equiv 1 \bmod 101$ donc x est un carré modulo 101. En outre l'ordre de x dans le groupe $(\mathbb{Z}/101\mathbb{Z})^*$ est un diviseur de 50. Le plus grand diviseur impair de 50 est 25 mais $x^{25} \equiv -1 \bmod 101$. Donc l'ordre de x est pair. Il est donc exclu de procéder comme dans l'exemple précédent puisque 2 n'est pas inversible modulo l'ordre de x.

Pour contourner cet obstacle on suppose que z est un non-résidu quadratique modulo 101 (c'est-à-dire que z n'est pas un carré). De tels z sont nombreux puisque la moitié des éléments non-nuls de $\mathbb{Z}/p\mathbb{Z}$ ne sont pas des carrés. On prends un entier z au hasard entre 2 et $p-1$ et on calcule $z^{50} \bmod 101$. Avec probabilité $\frac{1}{2}$ le résultat est -1 et on a trouvé notre non-résidu quadratique.

Par exemple $z = 46$ convient car $z^{50} = -1 \bmod 101$. Multiplions x par $z^2 = 96 \bmod 101$. On obtient $X = xz^2 = 36 \bmod 101$. Et cette fois $X^{25} = x^{25}z^{50} = 1 \bmod 101$ donc X a un ordre impair. On calcule aisément une racine carrée de X en inversant 2 modulo 25. On trouve que $2 \times 13 = 1 + 25$ donc X^{13} est une racine carrée de X. Posons alors $y = X^{13}z^{-1}$. On vérifie que y est une racine carrée de x.

Attention : cette méthode est probabiliste. On ne connaît pas de bonne méthode déterministe pour calculer des racines carrées modulo p ni pour factoriser des polynômes sur un corps fini.

3. RESTES CHINOIS

Si $N_1 \geq 2$ et $N_2 \geq 2$ sont deux entiers premiers entre eux. L'application $\rho : (\mathbb{Z}/N_1N_2\mathbb{Z}) \to (\mathbb{Z}/N_1\mathbb{Z}) \times (\mathbb{Z}/N_2\mathbb{Z})$ définie par $\rho(x \bmod N_1N_2) = (x \bmod N_1, x \bmod N_2)$ est bien définie et compatible avec l'addition et le produit. C'est un morphisme d'anneaux. C'est en fait une bijection. On montre par exemple que c'est une injection à l'aide du lemme de Gauss. On en déduit que c'est une bijection car les deux ensembles de départ et d'arrivée ont même cardinal. On cherche maintenant à calculer l'application inverse de ρ. C'est le problème des restes Chinois.

On pose $M_2 = 1/N_1 \bmod N_2$ et $M_1 = 1/N_2 \bmod N_1$. On note que M_2N_1 est congru à 0 modulo N_1 et à 1 modulo N_2. Et M_1N_2 est congru à 0 modulo N_2 et à 1 modulo N_1. Donc $x_1M_1N_2 + x_2M_2N_1$ est congru à x_1 modulo N_1 et à x_2 modulo N_2.

On a donc une formule explicite et un algorithme pour l'application réciproque de ρ. On pourra illustrer cette formule sur l'exemple $N_1 = 6$ et $N_2 = 5$.

On pourra aussi généraliser au cas d'un nombre plus grand de modules. Soit $I \geq 2$ un entier et $(N_i)_{1 \leq i \leq I}$ des entiers plus grands que 1 et premiers deux à deux. On pose $U_i = \prod_{j \neq i} N_i$ et $M_i = 1/U_i \bmod N_i$. Montrez que ces entiers sont bien définis. Donnez la formule pour inverser l'application ρ dans ce cas. Donnez un exemple avec $N_1 = 5$, $N_2 = 7$, $N_3 = 6$. On détaillera la décomposition de $(\mathbb{Z}/210\mathbb{Z}, +)$ en produit direct de trois sous-groupes de cardinaux 5, 7 et 6.

4. LES CARRÉS DANS $\mathbb{Z}/N\mathbb{Z}$

Soit $N \geq 2$ un entier. On écrit sa décomposition en facteurs premiers $N = \prod_i p_i^{e_i}$. L'isomorphisme ρ de la section précédente assure que x est un carré modulo N si et seulement s'il est carré modulo chaque $p_i^{e_i}$. On peut calculer une racine carrée de $x \bmod N$ en calculant séparément les racines des $x \bmod p_i^{e_i}$ puis en recollant les résultats avec les restes chinois. On utilise donc la factorisation de N.

On pourra traiter l'exemple $N = 11 \times 13$ et calculer les racines de $x = 3$. On en trouve quatre. Pourquoi ?

En général, si N est impair et a I facteurs premiers on trouve 2^k racines carrées pour tout carré de $(\mathbb{Z}/N\mathbb{Z})^*$.

Réciproquement, si l'on dispose d'une boîte noire qui calcule des racines carrées, alors on peut facilement factoriser N. Pourquoi ? On dit qu'il existe une **réduction** de la factorisation au calcul des racines carrées. La réciproque est vraie aussi. Donc ces deux problèmes ont des complexités similaires. Comme la factorisation est supposée difficile, le calcul des racines carrées modulo un nombre composé est supposé difficile aussi. C'est la raison pour laquelle le système de Rabin est supposé sûr contre une attaque passive. Donnez une **attaque à chiffré choisi** pour ce cryptosystème.

5. LE SYMBOLE DE JACOBI

Supposons maintenant que $N \geq 3$ est un entier naturel impair et $N = \prod_i p_i^{e_i}$ sa décomposition en produit de facteurs premiers. On définit pour tout entier x le symbole de Jacobi comme une généralisation du symbole de Legendre en posant

$$\left(\frac{x}{N}\right) = \prod_i \left(\frac{x}{p_i}\right)^{e_i}.$$

Le symbole de Jacobi $\left(\frac{x}{N}\right)$ ne dépend que de la classe de congruence de x modulo N. Le symbole de Jacobi satisfait de nombreuses propriétés multiplicatives évidentes, héritées de sa définition et des propriétés du symbole de Legendre. Par exemple $\left(\frac{a}{b}\right) = 0$ si et seulement si a et b ne sont pas premiers entre eux.

La *loi de réciprocité quadratique* s'étend au symbole de Jacobi.

Théorème 5.1 (Gauss)**.** *Soient M et N deux entiers naturels impairs différents de 1 et premiers entre eux. On a $\left(\frac{-1}{M}\right) = (-1)^{\frac{M-1}{2}}$, $\left(\frac{2}{M}\right) = (-1)^{\frac{M^2-1}{8}}$, et*

$$\left(\frac{M}{N}\right)\left(\frac{N}{M}\right) = (-1)^{\frac{(M-1)(N-1)}{4}}.$$

Ce théorème permet de calculer très efficacement le symbole de Jacobi en procédant comme dans l'algorithme d'Euclide. On pourra par exemple l'utiliser pour calculer $\left(\frac{107}{211}\right)$.

Si N n'est pas premier, le symbole de Jacobi ne suffit pas à distinguer les résidus quadratiques des autres résidus. Par exemple si $N = pq$ est produit de deux premiers impairs distincts et x premier à N alors $\left(\frac{x}{N}\right) = 1$ signifie soit que x est un carré modulo p et modulo q soit qu'il n'est un carré ni modulo p ni modulo q. Dans ce dernier cas on dit que x est un *faux carré*.

On considère qu'il est difficile de distinguer les vrais carrés des faux en général. La sécurité du cryptosystème présenté à la section 7 repose sur cette observation.

6. 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 Carole est membre d'une Organisation secrète et a reçu l'ordre de prendre contact avec James. Elle n'a jamais rencontré James et ne peut l'identifier à sa seule apparence physique (surtout si la prise de contact se fait par téléphone). De son coté, James ne connaît pas Carole. Afin d'éviter une infiltration, Carole et James recourrent à un procédé d'identificaion. L'Organisation a imposé le protocole suivant. James s'approche de Carole et lui dit "JARDIN". Carole répond alors "ANGLAIS". Si tout se passe comme prévu Carole et James savent qu'ils sont bien en présence l'un de l'autre. Cela suppose bien sûr que les deux mots de passe (JARDIN et ANGLAIS) 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 James et Carole. Pire encore, une fausse Carole (baptisons la Karole) pourrait se présenter à James qui lui devoilerait alors son mot de passe JARDIN afin de s'identifier auprès d'elle. Elle pourrait alors communiquer ce mot de passe à un faux James qui pourrait à son tour se faire passer pour le vrai James auprès de la vraie Carole...

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

(1) L'identité est définie par la connaissance d'une information (le mot de passe par exemple) qui doit rester secrète
(2) 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 James de prouver à Carole qu'il connaît un certain secret sans rien lui en dévoiler. Cette possibilité d'une *preuve sans divulgation d'information* (zero-knowledge proof en anglais) a été entrevue à la fin des années 80.

Nous sommes maintenant en mesure de décrire un protocole d'identification sans divulgation d'information. 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 f_X telle

que $f_X^2 = r_X \bmod N_X$. 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 f_X sont connus de X seul. C'est la connaissance de f_X qui distingue X.

Lorsque Carole prépare sa rencontre avec James elle consulte l'annuaire et prend connaissance du triplet (J, N_J, r_J) correspondant.

Au moment de la rencontre, pour s'assurer qu'elle est bien en présence de James elle doit se convaincre que son interlocuteur connaît une racine de r_J modulo N. Elle procède de la façon suivante :

(1) James choisit un résidu quadratique $z = u^2 \bmod N_J$ aléatoire (avec distribution uniforme) et calcule $t = zr_J \bmod N_J$. Il transmet t à Carole.
(2) Carole choisit un élément ϵ au hasard (avec distribution uniforme) dans $\{1, -1\}$ et le transmet à James.
(3) Si $\epsilon = 1$ James transmet u à Carole. Sinon il transmet une racine carrée s modulo N_J de t (il sait calculer une telle racine carrée $s = uf_J$ car il connaît une racine de r_J et une racine de z.)
(4) Si $\epsilon = 1$, Carole calcule $z = t/r_J \bmod N_J$ et vérifie que $z = u^2 \bmod N_J$.
(5) Si $\epsilon = 0$, Carole vérifie que $s^2 = t \bmod N_J$.

On vérifie sans peine que ce protocole s'exécute en temps polynomial en $\log N_J$. Ce protocole est reproduit un grand nombre de fois (par exemple 1000 fois).

Si les conditions vérifiées par Carole à la dernière étape sont satisfaites à chaque fois, alors Carole reconnaît James en son interlocuteur. Sinon elle l'accuse d'imposture.

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

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

7. JOUER À PILE OU FACE AU TÉLÉPHONE

On veut jouer à pile ou face à distance. Les deux joueurs communiquent par téléphone ou par le truchement d'un ordinateur (le tirage télévisé du LOTO en est un exemple puisque le téléspectateur n'est pas *présent*). On veut reproduire dans ce contexte les conditions d'un tirage aléatoire équitable c'est-à-dire uniforme pour chacun des deux joueurs. On peut imaginer que le premier joueur (appelé Alice et noté A) tire à pile ou face et fait part du résultat au second joueur (appelé Bob et noté B). Mais Bob peut douter de l'honnêteté d'Alice et la soupçonner d'avoir choisi le tirage à sa convenance. On peut recourir à un témoin assermenté (huissier de justice) mais sa bonne foi pourra toujours être mise en cause par un mauvais perdant. En outre, cette solution est coûteuse et complexe.

La suite de calculs et d'échanges décrite ci-dessus est appelée *protocole cryptographique*.

(1) Bob choisit deux grands nombres premiers p et q. Il calcule leur produit $N = pq$ et le transmet à Alice (il ne transmet pas p et q). Bob choisit aussi un résidu x modulo N tel que $\left(\frac{x}{N}\right) = 1$ (avec distribution uniforme) et il transmet x à Alice.

(2) Alice reçoit N et x mais ignore p et q. Elle ignore donc si x est un vrai ou un faux carré. Elle choisit un élément ϵ au hasard (avec distribution uniforme) dans $\{1, -1\}$ et le transmet à Bob.

(3) Bob compare ϵ et $\left(\frac{x}{p}\right)$. S'ils sont égaux alors le résultat du tirage au sort est *pile* et s'ils sont différents le résultat du tirage au sort est *face*. Bob fait part de sa conclusion à Alice et la justifie en lui transmettant p et q.

(4) Alice vérifie que p et q sont premiers et que les symboles de Legendre $\left(\frac{x}{p}\right)$ et $\left(\frac{x}{q}\right)$ sont conformes aux affirmations de Bob.

On vérifie sans peine que ce protocole s'exécute en temps polynomial en $\log N$ et qu'il produit une distribution uniforme de probabilité si Alice et Bob sont honnêtes (c'est-à-dire s'ils exécutent fidèlement le protocole).

Si Bob est malhonnête et si Alice est honnête alors la distribution est encore uniforme car la stratégie de Bob ne modifie pas la distribution de probabilité du résultat.

Si Alice est malhonnête elle peut essayer d'influencer le résultat mais elle doit pour cela deviner si le x qu'on lui transmet est ou non un carré. On admet que cela n'est pas possible en temps polynomial.