Symboles de Jacobi, primalité, applications

Septembre 2011

1 Le groupe $(\mathbb{Z}/N\mathbb{Z})^*$

On s'intéresse à la structure de groupe abélien de $(\mathbb{Z}/N\mathbb{Z})^*$. On se ramène au cas où $N = p^k$. Si $k = 1$ il n'y a pas de mystère (on a déjà vu que le groupe $\mathbb{F}_p^*$ est cyclique). On suppose donc que $k \geq 2$.

Le cardinal de $(\mathbb{Z}/p^k\mathbb{Z})^*$ est $p^{k-1}(p-1)$. Comme $p-1$ et p^{k-1} sont premiers entre eux, le groupe $(\mathbb{Z}/p^k\mathbb{Z})^*$ est produit direct de deux sous groupes de cardinaux respectifs $p-1$ et p^{k-1}. On peut être plus précis.

On a la suite exacte

$$1 \to \mathbf{U}_1 \to (\mathbb{Z}/p^k\mathbb{Z})^* \to \mathbb{F}_p^* \to 1 \tag{1}$$

où $\mathbf{U}_1$ est l'ensemble des $x \bmod p^k$ tels que $x \equiv 1 \bmod p$.

Soit $\mathbf{V}$ l'ensemble des solutions de l'équation $x^{p-1} = 1$. Le lemme de Hensel montre qu'il y a au moins $p-1$ telles racines distinctes et que la réduction modulo p est une bijection de $\mathbf{V}$ sur $\mathbb{F}_p^*$. L'intersection de $\mathbf{V}$ et $\mathbf{U}_1$ est triviale.

On définit pour tout $n \geq 1$ le groupe $\mathbf{U}_n \subset (\mathbb{Z}/N\mathbb{Z})^*$ formé des résidus congrus à 1 modulo p^n. Donc $\{1\} = \mathbf{U}_k \subset \mathbf{U}_{k-1} \subset \ldots \subset \mathbf{U}_1$.

Pour $1 \leq n \leq k-1$, le quotient $\mathbf{U}_n/\mathbf{U}_{n+1}$ est cyclique d'ordre p et engendré par $1 + p^n$. En effet l'application

$$1 + ap^n \bmod p^{n+1} \mapsto a \bmod p$$

est un isomorphisme de $(\mathbf{U}_n/\mathbf{U}_{n+1}, \times)$ sur $(\mathbb{Z}/p\mathbb{Z}, +)$.

Lemme 1 *Soit n tel que $1 \leq n \leq k-2$ si $p \geq 3$ et $2 \leq n \leq k-2$ si $p = 2$. Soit $x \in \mathbf{U}_n - \mathbf{U}_{n+1}$. Alors $x^p \in \mathbf{U}_{n+1} - \mathbf{U}_{n+2}$.*

En effet on a $x = 1 + ap^n$ et a premier avec p. Si $p \geq 3$ on calcule $x^p = (1+ap^n)^p = 1+ap^{n+1}+\sum_{2\leq m\leq p-1} \binom{p}{m} a^m p^{nm}+a^p p^{np} \equiv 1+ap^{n+1} \bmod p^{n+2}$ car $np \geq n+2$.

Si $p = 2$ et $n \geq 2$ on a $x^2 = (1 + a2^n)^2 = 1 + a2^{n+1} + a^2 2^{2n} \equiv 1 + a2^{n+1} \bmod 2^{n+2}$ car $2n \geq n+2$. □

On en déduit que si $p \geq 3$ alors $\mathbf{U}_1$ est cyclique d'ordre p^{k-1} et engendré par $1 + p$.

Pour $p = 2$, on a seulement que $\mathbf{U}_2$ est cyclique d'ordre 2^{k-2} et engendré par 5.

Si p est impair le groupe $(\mathbb{Z}/p^k\mathbb{Z})^*$ est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{k-1}\mathbb{Z}$.

Pour $p = 2$ on vérifie que $\mathbf{U}_1 = \{1, -1\} \times \mathbf{U}_2$ donc $\mathbb{Z}/2^k\mathbb{Z}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z})$.

2 Symbole de Legendre

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

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

Il existe de nombreuses preuves de ce théorème. Par exemple soit $\Phi_q(x) = 1 + x + \cdots + x^{q-1}$ et soit $A(x) \in \mathbb{F}_p[x]$ un facteur irréductible de $\Phi_q(x)$ modulo p. On pose $\mathbf{L} = \mathbb{F}_p[x]/A$ et soit $\zeta = x \bmod A(x) \in \mathbf{L}$ la classe de x. Donc ζ est une racine q-ième dans le corps $\mathbf{L}$.

Question 1 *Montrer que ζ est racine q-ième primitive, c'est-à-dire qu'elle est d'ordre exactement q dans le groupe multiplicatif.*

On définit la *somme de Gauss*

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

qui est un élément de $\mathbf{L}$.

On montre que $\tau^2 = \left(\frac{-1}{q}\right) q \in \mathbf{L}$. Donc on a une formule pour la racine carrée de $\left(\frac{-1}{q}\right) q$ dans une clôture algébrique de $\mathbb{F}_p$. Cette racine est dans $\mathbb{F}_p$ si et seulement si $\tau^p = \tau$. On voit sans peine que $\tau^p = \left(\frac{p}{q}\right)\tau$. Donc $\left(\frac{-1}{q}\right) q$ est un carré si et seulement si $\left(\frac{p}{q}\right) = 1$. Cela termine la démonstration.

On aura aussi besoin de la formule suivante

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \tag{2}$$

si p est impair.

Notons déjà que si x est impair alors $x = 1 + 2k$ et $x^2 = 1 + 4k(k+1) = 1 + 8\binom{k+1}{2}$ est bien congru à 1 modulo 8. En outre $k(k+1)/2$ est pair si et seulement si k est congru à 0 ou 3 modulo 4 c'est-à-dire x congru à 1 ou 7 modulo 8.

Soit alors $A(x) \in \mathbb{F}_p[x]$ un facteur irréductible de $x^4 + 1$ modulo p et $\zeta = x \bmod A(x)$ la classe de x dans le corps $\mathbb{F}_p[x]/A$.

Question 2 *Montrer que ζ est une racine primitive huitième de* 1.

On vérifie que $(\zeta + \zeta^{-1})^2 = 2$. Donc on a trouvé une racine carrée de 2 dans une clôture algébrique de $\mathbb{F}_p$. Donc 2 est un carré si et seulement si cette racine est dans $\mathbb{F}_p$ c'est-à-dire si et seulement si $\alpha^p = \alpha$.

Or $\alpha^p = \zeta^p + \zeta^{-p}$ où les exposants p sont à voir modulo 8. Si p est congru à 1 ou -1 modulo 8 on en déduit que $\alpha^p = \alpha$. Si p est congru à 3 ou 5 modulo 8 on vérifie que $\alpha^p = -\alpha$. Ceci prouve la formule (**??**).

3 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 $2 \times 13 = 1 + 15$ 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.

Si N est un entier composé, comment calculer des racines carrées modulo N ? Pour $N = p^k$ on peut utiliser le lemme de Hensel. Pour N quelconque, on factorise N en produits de facteurs premiers et on se ramène au cas précédent. Malheureusement, celà suppose que l'on sache factoriser efficacement.

On ne connaît pas d'algorithme polynomial en temps pour factoriser des entiers. On considère donc qu'il est difficile de calculer des racines carrées modulo un nombre composé en général.

Si $N = pq$ est un produit de deux grands nombres premiers, la fonction $\gamma_N : x \mapsto x^2$ de $(\mathbb{Z}/N\mathbb{Z})^*$ est facile à évaluer mais il est difficile de trouver un antécédent d'un y donné dans $(\mathbb{Z}/N\mathbb{Z})^*$. En tout cas, on ne connaît pas d'algorithme polynomial pour résoudre ce problème. On dit que γ_N est une fonction *asymétrique*.

Noter que si l'on connaît p et q, alors il est facile de calculer des antécédents. On dit que γ_N est une fonction *trappe*.

Question 3 *On suppose qu'on dispose d'un oracle (une boîte noire) qui pour tout $y \in \mathbb{Z}/N\mathbb{Z}$ retourne une racine carrée de y modulo N s'il en existe une. Montrer qu'il est alors possible de factoriser N en temps polynomial en* $\log N$.

4 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 2 (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.

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.

5 Test de primalité de Solovay et Strassen

Soit N un entier impair. Soient $\chi_1 : (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N\mathbb{Z})^*$ et $\chi_2 : (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N\mathbb{Z})^*$ les deux homomorphismes de groupes définis par

$$\chi_1 : x \mapsto x^{\frac{N-1}{2}} \bmod N$$

et

$$\chi_2 : x \mapsto \left(\frac{x}{N}\right) \bmod N.$$

On note $\chi_0 = \chi_2/\chi_1$. Il est évident que χ_0 est trivial si N est premier. On a le

Lemme 2 *Si N est impair et n'est pas premier alors il existe un $x \bmod N$ dans $(\mathbb{Z}/N\mathbb{Z})^*$ tel que $\chi_0(x) \neq 1$.*

Supposons d'abord que N a un facteur carré. Donc il existe un premier impair p et un entier $k \geq 2$ tel que p^k divise exactement N. On pose $M = N/p^k$. Soit $G \subset (\mathbb{Z}/N\mathbb{Z})^*$ le sous-groupe formé des résidus congrus à 1 modulo Mp. C'est un groupe cyclique d'ordre p^{k-1}. La restriction du symbole de Jacobi à ce sous-groupe est triviale. La restriction de χ_1 n'est pas triviale car $\frac{N-1}{2}$ est premier à p.

Supposons donc maintenant que N est sans facteur carré. Soit p un facteur premier impair de N et soit $M = N/p$. Soit x un entier congru à 1 modulo M et qui ne soit pas un carré modulo p. Donc $\chi_2(x) = -1$ et $\chi_1(x) = 1 \bmod M$. Ainsi, $\chi_1(x) \neq \chi_2(x)$. □

Si N est impair et composé alors le noyau de χ_0 est un sous-groupe strict de $(\mathbb{Z}/N\mathbb{Z})^*$. Son cardinal est donc $\leq \frac{N-1}{2}$. On a donc une chance sur deux au moins de trouver $\chi_0(x) \neq 1$ si on choisit x au hasard uniformément dans $(\mathbb{Z}/N\mathbb{Z})^*$. Comme on dispose d'algorithmes polynomiaux pour calculer χ_1 et χ_2 on obtient un test probabiliste de primalité :

1. on s'assure d'abord que N est impair ;
2. on choisit x au hasard dans $(\mathbb{Z}/N\mathbb{Z})^*$ et on calcule $\chi_1(x)$ et $\chi_2(x)$;
3. si $\chi_1(x) \neq \chi_2(x)$, on sait que N est composé ;
4. si $\chi_1(x) = \chi_2(x)$, on ne peut conclure ... mais on peut recommencer !

Si N est impair et composé et si $x \in (\mathbb{Z}/N\mathbb{Z})^*$ vérifie $\chi_1(x) = \chi_2(x)$, on dit que x est un faux témoin.

La proportion de faux témoins dans $(\mathbb{Z}/N\mathbb{Z})^*$ est inférieure ou égale à $1/2$.

6 Test de primalité de Miller et Rabin

Si N est premier et si x est premier à N alors $x^{N-1} = 1 \bmod N$.

Une idée pour tester la primalité de N serait de choisir x premier à N et de calculer $x^{N-1} \bmod N$. Si le résultat est différent de 1 alors on sait que N est composé.

On dit qu'un entier N est *pseudo premier* de base x si x est premier à N et $x^{N-1} = 1 \bmod N$.

Si N est premier alors il est pseudo premier de base x pour tout x premier à N.

Malheureusement, N peut être pseudo premier de base x pour beaucoup de résidus x modulo N, même si N est composé.

Par exemple, pour $N = 561 = 3 \times 11 \times 17$ tous les x premiers à N vérifient $x^{N-1} = 1 \bmod N$. En effet le groupe $(\mathbb{Z}/N\mathbb{Z})^*$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$. Son exposant est donc $16 \times 5 = 80$. Or $N - 1 = 16 \times 5 \times 7$ est un multiple de 80.

Le test de Fermat peut donc être trompeur.

L'idée de Miller et Rabin (et de bien d'autres avant eux) est de raffiner la congruence de Fermat. On écrit $N - 1 = M \times 2^e$ avec M impair et on observe que le polynôme $x^{N-1} - 1$ se factorise

$$x^{N-1}-1=(x^{\frac{N-1}{2}}+1)(x^{\frac{N-1}{4}}+1)(x^{\frac{N-1}{8}}+1)...(x^{\frac{N-1}{2^{e-1}}}+1)(x^M+1)(x^M-1). \qquad (3)$$

On dit que la condition $\mathrm{MR}(x, N)$ est satisfaite si x est un entier premier à N et si l'un des facteurs du membre de droite de l'équation (**??**) est nul modulo N.

On dit aussi que N est *fortement pseudo premier* de base x. Si N est premier, il est fortement pseudo premier de base x pour tout x premier à N.

Un théorème de Rabin assure que si $N \geq 15$ est impair et composé, alors $\mathrm{MR}(x, N)$ n'est pas vraie pour plus du quart des résidus x dans $(\mathbb{Z}/N\mathbb{Z})^*$.

On obtient un deuxième test de primalité probabiliste

1. on s'assure d'abord que N est impair et ≥ 15 ; sinon il n'y a pas de mystère.
2. on choisit x au hasard dans $(\mathbb{Z}/N\mathbb{Z})^*$ et on calcule $x^M \bmod N$. On vérifie ensuite la condition $\mathrm{MR}(x, N)$;
3. si $\mathrm{MR}(x, N)$ n'est pas satisfaite, on sait que N est composé ;
4. si $\mathrm{MR}(x, N)$ est satisfaite alors on ne peut conclure ... mais on peut recommencer !

Dans le cas où N est composé, la proportion de faux témoins est $\leq 1/4$.

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 (conjecture ci-dessus) que cela n'est pas possible en temps polynomial.

8 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 apport 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 apport 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.