CRYPTA
Chapitre 2 : Factorisation

1 Primalité

1.1 Certificats de primalité (non traité en cours)

Notons $\mathbb{P}$ l'ensemble des nombres premiers. Étant donné un entier $n \in \mathbb{N} \setminus \mathbb{P}$, exhiber un facteur de n donne une preuve facilement vérifiable que n n'est pas premier (nous utiliserons le mot *composé*). L'ensemble $\mathbb{N} \setminus \mathbb{P}$ définit donc un langage décidable en temps polynomial par une machine de Turing non déterministe (*i.e* un langage de la classe de complexité NP). En 1975, V. Pratt a montré que c'est également le cas du langage défini par l'ensemble $\mathbb{P}$ en montrant que si n est un nombre premier, il existe une preuve (appelée *certificat de primalité* de n) qui peut être vérifiée en temps polynomial en la longueur de l'entier n.

Lemme 1. *Un entier n est premier si et seulement s'il existe un entier $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv 1 \bmod n$ mais $a^{(n-1)/q} \not\equiv 1 \bmod n$ pour tout diviseur premier q de $n-1$.*

Démonstration. L'entier n est premier si et seulement si le groupe $\mathbb{Z}_n^*$ est cyclique d'ordre $n-1$ donc si et seulement s'il existe un élément $a \in \mathbb{Z}_n^*$ d'ordre $n-1$, c'est-à-dire un entier $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv 1 \bmod n$ mais $a^{(n-1)/q} \not\equiv 1 \bmod n$ pour tout diviseur premier q de $n-1$. □

Théorème 1 (V. Pratt)**.** *Tout nombre premier admet un certificat de primalité polynomial (en sa longueur binaire).*

Démonstration. D'après le lemme précédent, la liste d'entiers $(a, q_1, \ldots, q_t)$ est un certificat de primalité de n si

- $a^{n-1} \equiv 1 \pmod n$;
- $a^{(n-1)/q_i} \not\equiv 1 \pmod n$ pour tout $i \in \{1, \ldots, t\}$;
- $n - 1 = q_1 \ldots q_t$.
- q_i est un nombre premier pour tout $i \in \{1, \ldots, t\}$;

Le lemme précédent montre que tout nombre premier possède un certificat de primalité et il est immédiat que la vérification des trois premières propriétés précédentes peut se réaliser en temps polynomial. Pour prouver la primalité de n, il suffit donc de fournir par récurrence un certificat de primalité des q_i pour $i \in \{1, \ldots, t\}$.

Par récurrence, nous pouvons montrer qu'un certificat de primalité complet pour n nécessite moins de $(6 \log n - 4)$ entiers inférieurs à n. Cette propriété est vérifiée pour $n = 2$ et $n = 3$. Supposons la propriété vérifiée pour tout nombre premier $p < n$ pour $n > 3$ impair. Avec les notations précédentes, nous avons $n - 1 = q_1 \ldots q_t$ avec $t \geq 2$. Un certificat de primalité de n est formé des t entiers q_i pour $i \in \{1, \ldots, t\}$, de l'entier a et des certificats de primalité des q_i pour $i \in \{1, \ldots, t\}$. Il est donc formé d'au plus

$$\sum_{k=1}^{t} (6 \log(q_i) - 4) + t + 1 = 6 \log(n-1) - 3t + 1 \leq 6 \log(n) - 4$$

entiers inférieurs à n. La vérification d'un certificat de primalité (complet) pour n peut donc se faire en temps polynomial. □

1.2 Test de Fermat (non traité en cours)

Rappelons le « petit théorème de Fermat » qui est à la base de tous les tests de primalité que nous allons voir dans ce cours :

Théorème 2 (Petit théorème de Fermat)**.** *Si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} \equiv 1 \bmod p$.*

En particulier, si pour un entier n, il existe un entier a inférieur à n tel que $a^{n-1} \not\equiv 1 \bmod n$ alors n est un nombre composé. Le *test de primalité de Fermat* (*cf.* Algorithme (1)) repose sur cette idée simple.

Algorithme 1 Test de primalité de Fermat

Entrée: $n \in \mathbb{N}$, $a \in \mathbb{N}$.
Sortie: Composé ou Probablement premier
  $b \leftarrow a^{n-1} \bmod n$ ▷ par exponentiation dichotomique
  si $b = 1$ **alors**
    retourner Probablement premier
  sinon
    retourner Composé
  fin si

Ce test de primalité est malheureusement insuffisant car pour tout entier $a \geq 1$, il existe des entiers composés n tels que $a^{n-1} \equiv 1 \bmod n$ (et l'algorithme peut retourner Probablement premier alors que l'entrée n est un nombre composé). Un tel nombre composé est appelé un nombre *pseudo-premier de Fermat en base a*. Les premiers nombres pseudo-premiers de Fermat en base 2 sont 341, 561, 645, 1105, 1387, 1729, 1905 ...
Nous pouvons même montrer qu'il existe une infinité de tels nombres pour toute base $a \geq 2$.

Lemme 2. *Soit $a \geq 2$ un entier. L'entier $n = (a^{2p} - 1)/(a^2 - 1)$ est un nombre entier composé si p est un nombre impair.*

Démonstration. Nous avons

$$n = \frac{a^{2p} - 1}{a^2 - 1} = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1}.$$

Puisque $a - 1$ divise $a^p - 1$ et $a + 1$ divise $a^p + 1$ (pour p impair), n est un nombre entier composé. □

Lemme 3. *Soient $a \geq 2$ un entier et $n = (a^{2p} - 1)/(a^2 - 1)$. Si p est un nombre premier ne divisant pas $a^2 - 1$, alors $2p$ divise $n - 1$.*

Démonstration. Si p un nombre premier impair, par le petit théorème de Fermat, nous avons $a^p \equiv a \bmod p$ et donc $a^{2p} \equiv a^2 \bmod p$. Donc p divise $a^{2p} - a^2$ mais ne divise pas $a^2 - 1$ par hypothèse. Donc p divise $n - 1 = (a^{2p} - a^2)/(a^2 - 1)$.
De plus $n - 1 = a^{2p-2} + a^{2p-4} + \cdots + a^2$ est la somme d'un nombre pair de termes de même parité. Donc 2 divise $n - 1$ et $2p$ divise $n - 1$. □

Théorème 3. *Soit $a \geq 2$ un entier. Il existe une infinité de nombres pseudo-premiers de Fermat en base a.*

Démonstration. D'après les lemmes précédents, si p est un nombre premier impair ne divisant pas a^2-1, $a^{2p}-1$ est un diviseur de $a^{n-1}-1$ mais $a^{2p}-1$ est un multiple de n, donc $a^{n-1} \equiv 1 \bmod n$. La suite des nombres premiers ne divisant pas a^2-1 étant infinie, nous obtenons une famille infinie de nombres pseudo-premiers de Fermat en base a. □

Un nombre de Carmichael est un entier composé tel que $a^{n-1} \equiv 1 \bmod n$ pour tout entier $a > 0$ premier avec n. Le théorème suivant montre que les nombres de Carmichael vérifient des conditions arithmétiques assez strictes connues sous le nom de *critère de Korselt*.

Théorème 4 (Nombres de Carmichael - Critère de Korselt)**.** *Les nombres de Carmichael sont les entiers impairs n composés sans facteur carré, et tel que pour tout entier p divisant n, $p-1$ divise $n-1$.*

Démonstration.

1. Pour un entier n pair, nous avons
$$(n-1)^n \equiv (-1)^n \equiv 1 \not\equiv n-1 \bmod n$$
et un nombre de Carmichael est donc nécessairement impair.
2. Soient n un nombre de Carmichael, p un facteur premier de n et $\ell \geq 1$ tel que $p^\ell \mid n$ mais $p^{\ell+1} \nmid n$. Pour montrer que $\ell = 1$ et donc que n est sans facteur carré, nous allons tout d'abord montrer qu'il existe un entier a tel que a est un générateur de $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ et a est premier avec n/p^ℓ.
Nous savons que le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique engendré par $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$. Nous allons construire à partir de α un entier γ tel que $\gamma \equiv \alpha \bmod p$ et γ est un générateur de $(\mathbb{Z}/p^\ell\mathbb{Z})^*$.
Notons m l'ordre de l'entier α dans $(\mathbb{Z}/p^\ell\mathbb{Z})^*$. Nous avons $\alpha^m \equiv 1 \bmod p^\ell$ et donc $\alpha^m \equiv 1 \bmod p$. Comme α est d'ordre $p-1$ modulo p, nous obtenons que $p-1$ divise m. L'élément $\alpha^{m/(p-1)}$ dans $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ est donc d'ordre exactement $p-1$.
Montrons que l'élément $\beta = 1+p$ est d'ordre $p^{\ell-1}$ dans $(\mathbb{Z}/p^\ell\mathbb{Z})^*$. En calculant les puissances p-ième successives de β, nous obtenons
$$\begin{aligned}
\beta &= 1+p \\
\beta^p &= (1+p)^p \equiv 1+p^2 \bmod p^3 \\
\beta^{p^2} &= (1+p)^{p^2} \equiv 1+p^3 \bmod p^4 \\
&\vdots \\
\beta^{p^{\ell-2}} &= (1+p)^{p^{\ell-2}} \equiv 1+p^{\ell-1} \bmod p^\ell \\
\beta^{p^{\ell-1}} &= (1+p)^{p^{\ell-1}} \equiv 1 \bmod p^\ell
\end{aligned}$$
Ces puissances p-ième sont donc toutes distinctes et l'ordre de β est exactement égal à $p^{\ell-1}$. En notant γ le produit de $\alpha^{m/(p-1)}$ et β, l'ordre de γ est égal au plus petit commum multiple des ordres de $\alpha^{(m/(p-1)}$ et β, soit $(p-1)p^{\ell-1}$ et nous avons donc montré que $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ est cyclique.

Par hypothèse, p^ℓ et n/p^ℓ sont premiers entre eux donc, par le théorème chinois des restes, il existe un entier a tel que $a \equiv \gamma \bmod p^\ell$ et $a \equiv 1 \bmod n/p^\ell$. Un tel entier a est premier avec n et est un générateur de $(\mathbb{Z}/p^\ell\mathbb{Z})^*$.

Puisque n est un nombre de Carmichael, nous avons

$$a^{n-1} \equiv 1 \bmod n \text{ donc } a^{n-1} \equiv 1 \bmod p^\ell.$$

L'ordre de a modulo p^ℓ est égal à $(p-1)p^{\ell-1}$, donc $(p-1)p^{\ell-1}$ divise $n-1$. En particulier si $\ell \geq 2$, p divise n et p divise $n-1$ et on obtient une contradiction. Donc $\ell = 1$ et on a bien que $(p-1)$ divise $(n-1)$.

3. Montrons que $p-1$ divise $n-1$. Soit a une racine primitive modulo p. Puisque n est un nombre de Carmichael, nous avons $a^{n-1} \equiv 1 \bmod n$ et puisque p divise n nous avons $a^{n-1} \equiv 1 \bmod p$. L'ordre de a modulo p divise donc $n-1$ et puisque a est d'ordre $p-1$ nous avons bien montré le résultat.
4. Montrons enfin la réciproque. Soit n un entier sans facteur carré tel que pour tout nombre premier p divisant n, $p-1$ divise $n-1$. Pour tout nombre premier p divisant n et tout entier a premier avec n, nous avons $a^{p-1} \equiv 1 \bmod p$ et donc $a^{n-1} \equiv 1 \bmod p$. Tout diviseur premier de n divise $a^{n-1}-1$ et comme n est sans facteur carré, nous en déduisons que n divise $a^{n-1}-1$, et donc que n est un nombre de Carmichael.

□

Corollaire 1. *Un nombre de Carmichael a au moins trois diviseurs premiers.*

Démonstration. Supposons que $n = pq$ avec p et q premiers impairs (et $p \neq q$). D'après le critère de Korselt, $p-1$ divise $n-1 = pq-1 = (p-1)q + q - 1$. Donc $p-1$ divise $q-1$ et de même $q-1$ divise $p-1$, donc $p = q$. Un nombre de Carmichael a donc nécessairement au moins trois diviseurs premiers. □

Même si les nombres de Carmichael sont rares, W. R. Alford, A. Granville et C. Pomerance ont démontré en 1994 qu'il en existe une infinité. Il est donc nécessaire d'utiliser des critères de primalité plus stricts que la « petit théorème de Fermat ».

1.3 Critère d'Euler et test de Solovay-Strassen (non traité en cours)

Soit n un entier positif. Un entier a est un *carré modulo n* (ou est un *résidu quadratique* modulo n) s'il existe $b \in \mathbb{N}$ tel que $a \equiv b^2 \bmod n$. Cette propriété dépend uniquement de la classe de a modulo n et lorsque n est un nombre premier impair p, le *critère d'Euler* donne une caractérisation simple des carrés modulo p.

Théorème 5 (Critère d'Euler)**.** *Si p est un nombre premier et si a est un entier non divisible par p, alors $a^{(p-1)/2} \equiv 1 \bmod p$ si a est un carré modulo p et $a^{(p-1)/2} \equiv -1 \bmod p$ sinon.*

Démonstration. Soit p un nombre premier et g un générateur de $\mathbb{Z}_p^*$. Pour tout élément $a \in \mathbb{Z}_p^*$, il existe un unique entier $x \in \mathbb{Z}_{p-1}$ tel que $a = g^x \bmod p$ et a est un carré modulo p si et seulement si x est pair. Nous avons donc

$$a^{(p-1)/2} \equiv g^{x(p-1)/2} \bmod p \equiv (-1)^x \bmod p \equiv \left(\frac{a}{p}\right).$$

□

Nous utiliserons le *symbole de Legendre* pour noter si a est un résidu quadratique modulo p.

Définition 1 (Symbole de Legendre)**.** *Soit p un nombre premier impair et $a \in \mathbb{Z}_p^*$. Le symbole de Legendre de a modulo p est défini par :*

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

Le critère d'Euler s'énonce alors, pour $n = p$ un nombre premier impair, sous la forme

$$\forall a \in \mathbb{Z}_n^*, \quad a^{(n-1)/2} = \left(\frac{a}{n}\right) \bmod n. \tag{1}$$

Le *symbole de Jacobi* est une extension formelle du symbole de Legendre dont les propriétés permettent de calculer plus facilement des symboles de Legendre.

Définition 2 (Symbole de Jacobi)**.** *Soit $n \geq 2$ un entier impair dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_k}\right)^{\alpha_k} \dots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

Si pour deux entiers a et n (avec n non premier), $\left(\frac{a}{n}\right) = -1$ nous assure que a n'est pas un résidu quadratique modulo n, nous ne pouvons pas déduire en général de $\left(\frac{a}{n}\right) = 1$ que a est un résidu quadratique modulo n.

Pour tout nombre premier p impair, nous avons

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \text{ et } \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

La valeur d'un symbole de Jacobi quelconque peut être calculée très efficacement (*i.e.* en temps quadratique) en utilisant de façon répétée la *loi de réciprocité quadratique.*

Théorème 6 (Loi de réciprocité quadratique)**.** *Soient m et n deux nombres premiers entre eux et impairs. Nous avons*

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{(n-1)(m-1)/4}.$$

En utilisant la relation (1), nous obtenons un nouveau critère de primalité vérifié pour tout nombre premier p.
Étant donné un entier a, un nombre composé peut vérifier cette égalité. Dans ce cas, il est appelé un nombre *pseudo-premier d'Euler en base a.*
Au contraire des nombres pseudo-premiers de Fermat, il n'existe pas de nombre pseudo-premier d'Euler en base a pour toute base a.

Lemme 4. *Si $n \geq 3$ n'est pas premier alors pour (au moins) la moitié des $a \in \mathbb{Z}_n^*$, nous avons*

$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \bmod n.$$

Algorithme 2 Test de primalité d'Euler

Entrée: $n \in \mathbb{N}$, $a \in \mathbb{N}$.
Sortie: Composé ou Probablement premier

$b_1 \leftarrow a^{(n-1)/2} \bmod n$ ▷ par exponentiation dichotomique
$b_2 \leftarrow \left(\frac{a}{n}\right)$ ▷ par la loi de réciprocité quadratique
si $b_1 = b_2$ **alors**
  retourner Probablement premier
sinon
  retourner Composé
fin si

Démonstration. Soit $n \geq 3$ un nombre composé. Posons

$$J_n = \left\{ a \in \mathbb{Z}_n^*, \left(\frac{a}{n}\right) \equiv a^{(p-1)/2} \bmod n \right\}.$$

J_n est un sous-groupe de $\mathbb{Z}_n^*$ et il suffit de montrer que c'est un sous-groupe propre de $\mathbb{Z}_n^*$ pour montrer le résultat. Supposons par l'absurde que $J_n = \mathbb{Z}_n^*$ (en particulier n est un nombre de Carmichael, et donc n est sans facteur carré).
Soit p un diviseur premier de n et notons $g \in \mathbb{Z}_p^*$ un générateur. Soit $a \in \mathbb{Z}_n^*$ tel que

$$\begin{cases} a & \equiv & g \bmod p \\ a & \equiv & 1 \bmod n/p \end{cases}$$

qui existe d'après le théorème des restes chinois (puisque p et n/p sont premiers entre eux). Nous avons

$$\begin{aligned} \left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{n/p}\right) &= \left(\frac{a \bmod p}{p}\right)\left(\frac{a \bmod n/p}{n/p}\right) \\ &= \left(\frac{g}{p}\right)\left(\frac{1}{n/p}\right) \\ &= \left(\frac{g}{p}\right) = -1. \end{aligned}$$

Puisque $a \in J_n$ nous avons $a^{(n-1)/2} \equiv -1 \bmod n$ et comme (n/p) divise n, nous avons $a^{(n-1)/2} \equiv -1 \bmod n/p$ ce qui contredit $a \equiv 1 \bmod (n/p)$.
Donc J_n est un sous-groupe propre de $\mathbb{Z}_n^*$, donc de cardinal au plus $(n-1)/2$, donc pour au moins la moitié des $a \in \mathbb{Z}_n^*$, nous avons

$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \bmod n.$$

□

Nous obtenons, pour tout entier T, un algorithme qui, prenant en entrée un entier n, retourne Composé ou Premier en $O(T \log^3 n)$ opérations binaires, de sorte que

— si l'algorithme retourne Composé, alors n est toujours un nombre composé ;
— si l'algorithme retourne Premier, alors la probabilité que n soit composé est inférieure à 2^{-T}.

L'algorithme consiste simplement à itérer le test de primalité d'Euler (*cf.* Algorithme (2)) T fois en tirant uniformément aléatoirement une nouvelle base a pour chaque itération. L'algorithme obtenu est le test de primalité de Solovay-Strassen qui a été proposé en 1977 par R. Solovay et V. Strassen.

Algorithme 3 Test de primalité de Solovay-Strassen

Entrée: $n \in \mathbb{N}$, $a \in \mathbb{N}$.
Sortie: Composé ou Probablement premier

```
pour i de 1 à T faire
  a ←R Z*_n
  b1 ← a^((n−1)/2) mod n          ▷ par exponentiation dichotomique
  b2 ← (a/n)                      ▷ par la loi de réciprocité quadratique
  si b1 ≠ b2 alors
    retourner Composé
  fin si
fin pour
retourner Premier
```

Le test de primalité de Fermat repose sur le fait que $a^{p-1} \equiv 1 \bmod p$ pour tout nombre premier p. Le test de primalité de Solovay-Strassen utilise le fait que $a^{(p-1)/2} \equiv \pm 1 \bmod p$. Il existe également le *test de primalité de Miller-Rabin* qui utilise de façon itérée l'idée que si $x^2 \equiv 1 \bmod p$ alors $x \equiv \pm 1 \bmod p$.

Le test de primalité de Solovay-Strassen (ou de Miller-Rabin) montre que l'ensemble $\mathbb{P}$ définit donc un langage décidable en temps polynomial par une machine de Turing probabiliste avec une probabilité d'erreur inférieure à $1/3$ pour toutes les instances (*i.e* un langage de la classe de complexité BPP). Pendant très longtemps, le problème de savoir si l'ensemble $\mathbb{P}$ définit un langage décidable en temps polynomial par une machine de Turing déterministe (*i.e* un langage de la classe de complexité P) a été ouvert. En 2002, M. Agrawal, N. Kayal et N. Saxena ont montré que c'est effectivement le cas.

2 Factorisation

2.1 Méthodes exponentielles de factorisation

La méthode de factorisation par divisions successives est la technique la plus simple pour factoriser de nombres entiers. Étant donné un entier n, elle consiste à essayer de diviser n par chaque nombre premier inférieur ou égal à $\sqrt{n}$. Si aucun diviseur n'est trouvé, l'entier n est premier. La complexité de l'algorithme dans le pire des cas est exponentielle (puisqu'elle demande $\sqrt{n}$ divisions), néanmoins cette méthode est toujours la première à tester car elle permet de trouver les petits facteurs de l'entier n.

L'algorithme de Fermat est une méthode de factorisation des entiers qui tente de factoriser un entier impair n en l'écrivant comme la différence de deux carrés $n = a^2 - b^2$. En notant $n = \alpha\beta$ avec α le plus grand diviseur de n inférieur à $\sqrt{n}$, le nombre d'opérations arithmétiques est de l'ordre de $(\sqrt{n}-\alpha)^2/2\alpha$. En particulier si n possède un diviseur proche de $\sqrt{n}$, la méthode de Fermat est plus rapide que la méthode des divisions successives mais

Algorithme 4 Méthode de factorisation de Fermat

Entrée: $n \in \mathbb{N}$
Sortie: PREMIER ou $a \in \mathbb{N}$, $a \mid n$, $a \neq 1, n$
  pour α de $\lceil \sqrt{n} \rceil$ à $(n+9)/6$ **faire**
    $\beta \leftarrow \sqrt{\alpha^2 - n}$
    si $\beta \in \mathbb{N}$ **alors**
      retourner $\alpha - \beta$
    fin si
  fin pour
  retourner PREMIER

dans le pire des cas, elle peut demander jusqu'à n opérations arithmétiques. L'efficacité de la méthode de Fermat pour factoriser un entier n est optimale lorsque l'un des facteurs de n est proche de $\sqrt{n}$.
Nous allons présenter une autre méthode exponentielle de factorisation des entiers due à J. M. POLLARD. Il s'agit d'une méthode spécifique qui est efficace pour les entiers dont au moins l'un des diviseurs p est tel que $p-1$ est friable.
Soit n un entier impair et soit $B > 0$ une borne fixée. Supposons qu'il existe un nombre premier p divisant n tel que toute puissance d'un nombre premier q^α divisant $p-1$ est inférieure à B.
Soit a l'entier $2^{B!}$. L'algorithme d'exponentiation dichotomique permet de calculer $a' \equiv a \bmod n$ en $O(B \log B)$ multiplications modulaires modulo n. Puisque $p-1$ divise $B!$, nous avons $a' \equiv 1 \bmod p$ et le plus grand diviseur commun de $a'-1$ et n est un facteur non trivial de n sauf si $a' = 1$.
L'algorithme de factorisation consiste simplement à calculer itérativement la valeur a' en (faisant grandir la valeur de B) et à tester si le plus grand diviseur commun révèle un facteur non trivial de n.

Algorithme 5 Méthode $p-1$ de Pollard

Entrée: $n \in \mathbb{N}$, B
Sortie: $r \in \mathbb{N}$, $r \mid n$
  Trouver la suite des nombres premiers $p_1 < p_2 < \ldots < p_m \leq B$
  Trouver pour tout $i \in \{1, \ldots, m\}$, l'entier k_i maximal tel que $p_i^{k_i} \leq B$
  $a \leftarrow 2$
  pour i de 1 à m **faire**
    pour j de 1 à k_i **faire**
      $a \leftarrow a^{p_i}$
    fin pour
  fin pour
  $r \leftarrow \text{pgcd}(a-1, n)$
  retourner r

Si la valeur r retournée est égale à 1, cela indique généralement que n n'a pas de diviseur premier p tel que $p-1$ soit suffisamment friable alors que si la valeur retournée est $r = n$, cela signifie généralement que tous les facteurs le sont. Il existe de nombreuses variantes de cet algorithme comme la méthode $p+1$ de Williams ou la méthode ECM de Lenstra (qui utilise des courbes elliptiques). En raison de cette attaque, pendant longtemps

les standards cryptographiques préconisaient de vérifier qu'un module RSA n'était pas constitué de nombres premiers ayant pas cette propriété. En raison du développement de la méthode ECM, cette condition n'est plus réellement pertinente de nos jours.

En 1975, J. Pollard a introduit un nouvel algorithme de factorisation des entiers. En considérant une fonction $F : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ et s_0 un élément de $\mathbb{Z}_n$, l'algorithme construit une suite définie par la récurrence $s_{i+1} = F(s_i)$ pour $i \in \mathbb{N}$. Comme l'algorithme ρ de Pollard pour le logarithme discret (vu dans le TD1), la méthode utilise peu de mémoire.

Algorithme 6 Algorithme ρ de Pollard (pour la factorisation)

Entrée: $n \in \mathbb{N}$
Sortie: $d \in \mathbb{N}$, $d \mid n$, $d \neq 1, n$ ou Échec

```
x ← 2
y ← 2
d ← 1
tant que d = 1 faire
    x ← F(x)
    y ← F(y)
    y ← F(y)
    d ← pgcd(|x − y|, n)
fin tant que
si d = n alors
    retourner Échec
sinon
    retourner d
fin si
```

Le principe est similaire à l'algorithme ρ de Pollard pour le logarithme discret vu en TD. La suite $(s_i)_{i\in\mathbb{N}}$ prend ses valeurs dans un ensemble fini $\mathbb{Z}_n$. Elle est définie par récurrence et elle est donc ultimement périodique. Soit p un diviseur premier de n, la suite $(s_i \bmod p)_{i\in\mathbb{N}}$ est également une suite ultimement périodique. Il existe donc un indice $j < k$ pour lequel $s_j = s_k \bmod p$ pour $k < j$. La suite $(s_i)_{i\in\mathbb{N}}$ étant définie par la récurrence $s_{i+1} = F(s_i)$ pour tout entier i, nous avons $s_{j+t} = s_{k+t}$ pour tout entier $t \geq 0$ et la suite $(s_i)_{i\in\mathbb{N}}$ peut être représentée comme sur la figure (1).
Si nous trouvons deux valeurs j et k telles que $s_j = s_k \bmod p$ et $s_j \neq s_k \bmod n$, alors le plus grand diviseur commun de $(s_j - s_k)$ et n produit une factorisation non triviale de n. Contrairement à la méthode ρ de Pollard pour le problème du logarithme discret, il est impossible de chercher directement une collision de la forme $s_\ell = s_{2\ell} \bmod p$, puisque calculer les valeurs de la suite $(s_i \bmod p)_{i\in\mathbb{N}}$ est impossible sans la connaissance de p. L'algorithme calcule donc en parallèle s_i et s_{2i} pour $i \in \mathbb{N}$ et recherche une collision par le calcul de plus grand diviseur commun.
Si la fonction F est une fonction aléatoire de $\mathbb{Z}_n^*$, le nombre espéré d'éléments de la suite $(s_i \bmod p)_{i\in\mathbb{N}}$ pour obtenir deux valeurs communes modulo p est de l'ordre de $j \sim \sqrt{\pi p/2}$. La complexité de l'algorithme pour trouver un facteur p de n est en $O(\sqrt{p})$ applications de la fonction F et donc de l'ordre de $O(n^{1/4})$ si le plus petit facteur premier de n est de l'ordre $\sqrt{n}$.

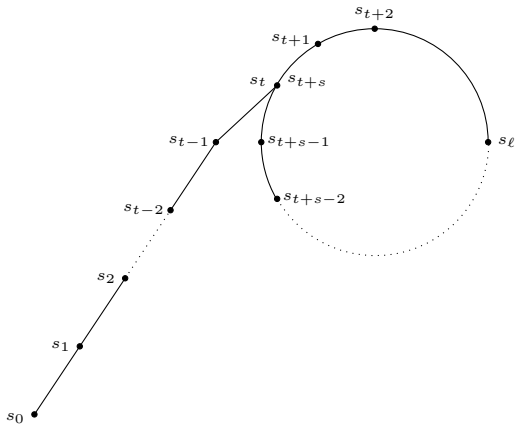

FIGURE 1 – Représentation de la suite $(s_n)_{n\in\mathbb{N}}$ dans l'algorithme ρ de Pollard

2.2 Racine carrée modulaire et factorisation

Nous avons utilisé les propriétés du symbole de Legendre pour tester la primalité d'un entier. Dans cette section, nous allons étudier le problème calculatoire associé (*i.e.* l'extraction de racines carrées modulaires) pour proposer notamment un algorithme de factorisation en temps sous-exponentiel.

Racine carrée modulo un nombre premier (survolé en cours)

Nous allons tout d'abord voir qu'il existe un algorithme polynomial probabiliste pour calculer une racine carrée modulo un nombre premier p.

Lemme 5. *Si $p \equiv 3 \bmod 4$, il existe un algorithme de complexité $O(\log^3 p)$ opérations binaires qui, étant donné $\alpha \in \{1,\dots,p-1\}$ tel que $\left(\frac{\alpha}{p}\right) = 1$, retourne $\beta \in \{1,\dots,p-1\}$ tel que $\beta^2 \equiv \alpha \bmod p$.*

Démonstration. Par hypothèse, nous avons $p \equiv 3 \bmod 4$. Par le critère d'Euler, nous savons que tout élément α de $\mathbb{Z}_p^*$ tel que $\left(\frac{\alpha}{p}\right) = 1$ vérifie

$$\alpha^{(p-1)/2} \equiv 1 \bmod p \quad \text{soit} \quad \alpha^{(p+1)/2} = \alpha^{(p-1)/2} \cdot \alpha \equiv \alpha \bmod p.$$

Comme $(p+1)$ est divisible par 4 par hypothèse, nous obtenons alors

$$\left(\alpha^{(p+1)/4}\right)^2 = \alpha^{(p+1)/2} = \alpha \bmod p,$$

et $\beta = \alpha^{(p+1)/4}$ est une racine carrée de α que l'on peut calculer en $O(\log p)$ multiplications dans $\mathbb{Z}_p$ en appliquant l'algorithme d'exponentiation dichotomique (et donc $O(\log^3 p)$ opérations binaires). □

Nous supposons désormais que $p \equiv 1 \bmod 4$. Posons $p = 2^h m + 1$ avec m impair.

Lemme 6. *Il existe un algorithme probabiliste qui étant donné p retourne un élément γ de $\{1,\dots,p-1\}$ tel que $\left(\frac{\gamma}{p}\right) = -1$ en temps espéré $O(\log^2 p)$ opérations binaires. Pour un tel γ, l'élément $\delta = \gamma^m$ engendre l'unique sous-groupe d'ordre 2^h de $\mathbb{Z}_p^*$.*

Démonstration. L'algorithme probabiliste consiste simplement à tirer γ uniformément aléatoirement dans $\mathbb{Z}_p^*$ et à vérifier que $\left(\frac{\gamma}{p}\right) = -1$. Le calcul du symbole de Legendre en utilisant la loi de réciprocité quadratique est de complexité quadratique et le nombre de γ à tester avant de trouver un non-résidu quadratique est égal à 2 (puisque $\mathbb{Z}_p^*$ contient $(p-1)/2$ non-résidus quadratiques).
Un tel γ vérifie $\gamma^{(p-1)/2} \equiv -1 \bmod p$ par le critères d'Euler, donc

$$(\gamma^m)^{2^{h-1}} \equiv \gamma^{2^{h-1}m} \equiv -1 \bmod p.$$

et γ^m est donc un générateur de l'unique sous-groupe d'ordre 2^h de $\mathbb{Z}_p^*$.

□

Lemme 7. *Soit $\alpha \in \{1, \ldots, p-1\}$ tel que $(\alpha|p) = 1$. L'élément α^m appartient au sous-groupe engendré par δ.*

Démonstration. Nous avons $(\alpha^m)^{2^h} \equiv \alpha^{(p-1)} \equiv 1 \bmod p$, donc α^m appartient à l'unique sous-groupe d'ordre 2^h de $\mathbb{Z}_p^*$. Il existe donc un élément $x \in \{0, \ldots, 2^h - 1\}$ tel que $\alpha^m = \delta^x \bmod p$. □

Une fois la valeur de δ construire, il suffit de calculer le logarithme discret x ce qui peut être fait soit en appliquant l'algorithme de Pohlig-Hellman en $O(h(\log(2)+\log(p)) = O(\log(p)^3)$ opérations de groupe dans $\mathbb{Z}_p^*$. Nous obtenons ensuite un algorithme pour calculer une racine carré de α^m modulo p. En effet, nous avons

$$1 = \left(\frac{\alpha}{p}\right) = \left(\frac{\alpha^m}{p}\right) = \left(\frac{\delta^x}{p}\right) = \left(\frac{\delta}{p}\right)^x = (-1)^x,$$

donc ce x est nécessairement pair.
Lorsque cette valeur x est connue, nous avons $\alpha^{(m+1)} \equiv \delta^x \alpha \bmod p$ et

$$(\alpha^{(m+1)/2}\delta^{-x/2})^2 = (\delta^x\alpha)\delta^{-x} \equiv \alpha \bmod p.$$

Donc $\beta = \alpha^{(m+1)/2}\delta^{-x/2} \bmod p$ est une racine carrée de α.

Algorithme 7 Algorithme de Tonelli-Shanks

Entrée: $p = 2^h m + 1 \in \mathbb{P}$, $\alpha \in \mathbb{Z}_p^*$ avec $\left(\frac{\alpha}{p}\right) = 1$, $\gamma \in \mathbb{Z}_p^*$ avec $\left(\frac{\gamma}{p}\right) = -1$.
Sortie: $\beta \in \mathbb{Z}_p^*$ tel que $\beta^2 \equiv \alpha \bmod p$

```
δ ← γ^m
β ← α^m
t ← 0
pour i de 0 à h − 1 faire
  si (βδ^t)^{2^{h−1−i}} ≡ −1 mod p alors
    t ← t + 2^i
  fin si
fin pour
retourner α^{(m+1)/2} δ^{t/2} mod p
```

Nous verrons en TD qu'il existe également un algorithme polynomial probabiliste pour calculer une racine carrée modulo une puissance d'un nombre premier.

Racine carré modulaire et factorisation

Nous allons voir que le problème de la factorisation d'un entier N et l'extraction de racines carrées modulo N sont de difficulté équivalente.
Soit N un entier dont la décomposition en facteur premier est $N = q_1^{f_1} \dots q_d^{f_d}$ où $q_i \in \mathbb{P}$ sont des nombres premiers et $f_i \geq 1$ pour $i \in \{1, \dots, d\}$).

Lemme 8. *Un entier x est un carré modulo N dès que tous les symboles de Legendre $\left(\frac{x}{q_j}\right)$ sont égaux à 1 pour $j \in \{1, \dots, d\}$. Un tel carré modulo N a exactement 2^d racines carrées.*

Démonstration. Si x est un carré modulo N, alors en réduisant modulo chacun de ses diviseurs premiers, x est un carré modulo q_i pour $i \in \{1, \dots, d\}$ et tous les symboles de Legendre $\left(\frac{x}{q_j}\right)$ sont égaux à 1.
D'après l'exercice du TD, x est un carré modulo $q_i^{f_i}$ si et seulement si x est un carré modulo q_i, c'est-à-dire si et seulement le symbole de Legendre $\left(\frac{x}{q_j}\right) = 1$. Si tous les symboles de Legendre $\left(\frac{x}{q_j}\right)$ sont égaux à 1 pour $j \in \{1, \dots, d\}$, il existe donc $y_i \in \mathbb{Z}_{q_i^{f_i}}$ pour $i \in \{1, \dots, d\}$ tels que $x \equiv y_i^2 \bmod q_i^{f_i}$. Par le théorème des restes chinois, il existe un entier y tel que $y \equiv y_i \bmod q_i^{f_i}$ pour tout $i \in \{1, \dots, d\}$. Cet élément vérifie $y^2 \equiv x \bmod q_i^{f_i}$ pour tout $i \in \{1, \dots, d\}$ et donc $y^2 \equiv x \bmod N$.

Il est possible de construire une racine carrée de x à partir des y_i pour $i \in \{1, \dots, d\}$. Pour tout suite $\alpha = (\alpha_1, \dots, \alpha_d) \in \{-1, 1\}^d$, notons $y_\alpha \in \mathbb{Z}_N$ tel que $y_\alpha \equiv \alpha_i y_i \bmod q_i^{f_i}$ pour tout $i \in \{1, \dots, d\}$. Ces 2^d éléments sont deux à deux distincts (puisque distincts modulo $q_i^{f_i}$ pour au moins une valeur de $i \in \{1, \dots, d\}$) et sont tous des racines carrées de x modulo N. □

Lemme 9. *S'il existe un algorithme $\mathcal{A}$ capable d'extraire des racines carrées dans $\mathbb{Z}_N$ en temps τ, alors il existe un algorithme $\mathcal{B}$ qui retourne un diviseur propre de N en temps espéré $O(\tau \cdot (1 - 2^{1-d}))$.*

Démonstration. L'algorithme $\mathcal{B}$ consiste simplement à tirer uniformément aléatoirement un élément $y \in \mathbb{Z}_N$ et à calculer $x^2 \bmod N$ et à rechercher une racine carrée de x modulo N en appliquant l'algorithme $\mathcal{A}$. L'algorithme $\mathcal{A}$ va retourner une valeur $z \in \mathbb{Z}_N$ tel que $z^2 \equiv x \bmod N$.
Puisque $z^2 \equiv y^2 \bmod N$, N divise $(z - y)(z + y)$. S'il existe un diviseur de N qui divise $(z \pm y)$ mais pas $(z \mp y)$, alors $\text{pgcd}(N, z \pm y)$ est un diviseur propre de N. Nous avons $z \equiv \pm y \bmod q_i^{f_i}$ pour tout $i \in \{1, \dots, d\}$ si et seulement si $z \equiv \pm y \bmod N$. La probabilité que $z \equiv \pm y \bmod N$ est égal à 2^{1-d} puisque x possède 2^d racines carrés modulo N.
En calculant les deux plus grand diviseurs communs $\text{pgcd}(N, z - y)$ et $\text{pgcd}(z + y)$, l'algorithme obtient donc un diviseur propre de N avec probabilité 2^{1-d}. En répétant cette méthode jusqu'à obtenir un diviseur, nous obtenons un algorithme $\mathcal{B}$ qui retourne un diviseur propre de N en temps espéré $O(\tau \cdot (1 - 2^{1-d}))$. □

De nombreuses méthodes modernes de factorisation d'un entier N reposent sur la recherche d'une congruence de carrés. Une méthode naïve de recherche d'une telle congruence est de tirer aléatoirement des valeurs $x \in \mathbb{Z}_N$ et d'espérer obtenir une collision de la forme :

$$x^2 \equiv y^2 \bmod N, \qquad x \not\equiv \pm y \bmod N.$$

Cette méthode naïve est inefficace mais il est possible d'accélérer (par un calcul d'indice) la recherche de cette congruence de carrés en construisant des carrés modulaires *friables*. La méthode utilise une base de facteurs $\mathcal{B} = \{2, 3, 5, \ldots, p_k\}$ constitués des k premiers nombres premiers comme dans l'algorithme de calcul d'indice de Kraitchik pour le problème du logarithme discret. L'idée générale (due à J. D. Dixon est la suivante :

— dans une première étape, l'algorithme recherche des relations de la forme

$$x_i^2 \equiv p_1^{e_{i,1}} \ldots p_m^{e_{i,m}} \bmod N \tag{2}$$

avec $x_i \in \mathbb{Z}_N$

— dans une seconde étape, l'algorithme cherche à combiner ces relations (en appliquant des techniques d'algèbre linéaire modulo 2) pour obtenir une relation de la forme $x^2 \equiv y^2 \bmod N$ et ainsi trouver un diviseur non trivial de N avec une probabilité supérieure à $1/2$ d'après l'exercice précédent.

L'analyse de la complexité de la méthode de Dixon est similaire à celle de la méthode de Kraitchik, la seule différence est de calculer le nombre d'éléments x_i vérifiant la relation (2).

Algorithme 8 Méthode de Dixon

Entrée: $N \in \mathbb{N}$ et une base de facteur $\mathcal{B} = \{2, 3, 5, \ldots, p_m\}$
Sortie: $d \in \{2, \ldots, N-1\}$ tel que $d \mid N$ ou ÉCHEC

```
L ← ∅
i ← 0
répéter
    i ← i + 1
    répéter
        x_i ←R Z_N
        y_i ← x_i^2 mod N
    jusqu'à y_i est p_m-friable        ▷ y_i = p_1^{e_{i,1}} ... p_m^{e_{i,m}} par divisions successives
    e_i ← (e_{i,1}, ..., e_{i,m})
    L ← L ∪ {(x_i, e_i)}
jusqu'à i = m + 1
Trouver v ∈ Z^{m+1} tel que v_1 e_1 + v_2 e_2 + ··· + v_{m+1} e_{m+1} ∈ (2 · Z)^m.
                                                    ▷ par élimination gaussienne
x ← ∏_{i=1}^{m+1} x_i^{v_i} mod N
y ← ∏_{i=1}^{m+1} ∏_{j=1}^{m} p_j^{e_{i,j} v_i / 2} mod N          ▷ x^2 ≡ y^2 mod N
si pgcd(x − y, N) ∉ {1, N} alors
    retourner pgcd(x − y, N)
sinon
    si pgcd(x + y, N) ∉ {1, N} alors
        retourner pgcd(x + y, N)
    fin si
sinon
    retourner ÉCHEC
fin si
```