ACCQ 207 - Cryptographie

1 Introduction

1.1 Historique

Les premiers usages étaient pour les militaires. Les exemples les plus connus sont :
- chiffrement par décalage, ou de Jules César,
- chiffrement par substitution, on applique une fonction de permutation sur les lettres,
- chiffrement par permutation : on divise le texte en groupes de lettres de même taille et à chaque groupe on applique une permutation entre les lettres.

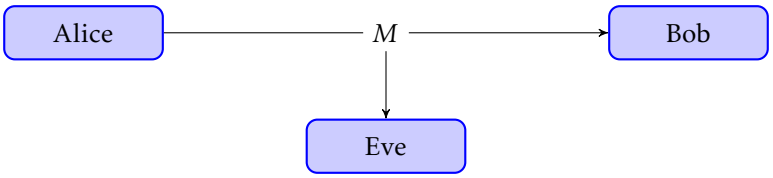
La plupart des systèmes actuels peuvent se voir comme combinaisons de ces transformations élémentaires.

Principe de Kerckhoff : quasiment toutes les caractéristiques du système doivent être publiques, mais le chiffrement dépend juste d'un paramètre secret, la clé.

Intérêt :
- déploiement à grande échelle,
- ne compromet pas toute la sécurité du système si une seule clé s'ébruite,
- permet d'analyser la sécurité par des tiers.

Peut-on prouver qu'un système est sûr, mesurer sa sécurité ? Deux approches possibles :
- sécurité informationnelle → théorie de l'information (Shannon).
  1948 : *A mathematical theory of communications*
  1949 : *Communication theory of secrecy systems*
- sécurité computationnelle → théorie de la complexité.

1.2 Sécurité informationnelle



Modèle : A veut envoyer un message clair $M \in \mathcal{M}$. M est vu comme une variable aléatoire de loi donnée.

Définition. Fonction de chiffrement : $E : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ où $\mathcal{K}$ est l'espace des clés et $\mathcal{C}$ est l'espace des chiffrés.

Au préalable Alice et Bob se sont mis d'accord sur une clé $K \in \mathcal{K}$. K est également vue comme une v.a de loi donnée.

Alice envoie à Bob le chiffré $C = E_K(M)$. Eve voit donc passer C. Quelle information peut-elle en déduire sur M ?

1.3 Les systèmes parfaits

Définition. Dans un **système parfait au sens de Shannon**, la connaissance de C n'apporte aucune info sur M.

Deux variantes :
- *en moyenne* : $H(M \mid C) = H(M)$,
- *dans tous les cas* : égalité des lois, $\forall M, \forall C, p(M \mid C) = p(M)$.

Exemple. On a les données suivantes :

$$\mathcal{M} = \{\text{oui}, \text{non}\}, \quad p(\text{oui}) = \frac{3}{4}, p(\text{non}) = \frac{1}{4}, \quad \mathcal{K} = \{K_1, K_2, K_3\}, \quad p(K_1) = p(K_2) = p(K_3) = \frac{1}{3}, \quad \mathcal{C} = \{x, y, z\}$$

et le chiffrage donné par

	oui	non
K_1	x	y
K_2	y	x
K_3	z	y

.

Eve voit C et en déduit que Alice a envoyé M avec probabilité $p(M \mid C)$. Par formule de Bayes il vient $p(\text{oui} \mid x) = \frac{p(x|\text{oui})p(\text{oui})}{p(x)}$, avec $p(x) = p(x \mid \text{oui})p(\text{oui}) + p(x \mid \text{non})p(\text{non})$ et idem avec y et z ou $M = \text{oui}$.

On trouve $p(x) = \frac{1}{3}$, $p(y) = \frac{5}{12}$ et $p(z) = \frac{1}{4}$.

Supposons $C = x$. Alors $p(\text{oui} \mid x) = \frac{3}{4}$ et $p(\text{non} \mid x) = \frac{1}{4}$ donc Eve n'a rien appris de plus que ce qu'elle connaissait déjà.

Supposons $C = y$. Alors $p(\text{oui} \mid y) = \frac{3}{5}$ et $p(\text{non} \mid y) = \frac{2}{5}$. L'incertitude est plus grande, en un sens Eve a appris quelque chose de nouveau par rapport à ce qu'elle estimait précedemment.

Supposons $C = z$. Alors $p(\text{oui} \mid z) = 1$ et $p(\text{non} \mid z) = 0$. Donc le clair se déduit du chiffré.

En conclusion ce système n'est pas parfait.

Exemple (Un système parfait : le one-time pad, ou masque jetable). On prend $\mathcal{M} = \{0,1\}^n$, $\mathcal{K} = \{0,1\}^n$ avec une distribution uniforme des clés et $\mathcal{C} = \{0,1\}^n$. On prend $E_K(M) := M \oplus K$. Alors $\forall M, \forall C, p(M \mid C) = p(M)$. Cette méthode est lourde : clé de même longueur que le message.

Théorème. Dans un système parfait on a nécessairement $\text{Card}(\mathcal{K}) \geqslant \text{Card}(\mathcal{C})$.

Démonstration. Pour un M donné on a

$$\forall C, p(C \mid M) = \frac{p(C,M)}{p(M)} = \frac{p(C \mid M)}{p(M \mid C)} = p(C) > 0$$

donc il existe une clé K telle que $C = E_K(M)$, d'où le résultat. □

Remarque. On a toujours $\text{Card}(C) \geqslant \text{Card}(M)$ pour pouvoir opérer un décodage (fonction E injective). Le cas le plus économique en sytème parfait est donc $\text{Card}(\mathcal{K}) = \text{Card}(\mathcal{C}) = \text{Card}(\mathcal{M})$ et alors $\forall M, \forall C, \exists! K, C = E_K(M)$.

On peut ensuite en déduire que la distribution de K doit être uniforme → c'est le one-time pad.

1.4 Distance d'unicité

Scénario : réutilisation d'une même clé pour chiffrer plusieurs messages.

Exemple (Chiffrement par substitution). On prend $\mathcal{M} = \mathcal{C} = \{\text{A}, \text{B}, \text{C}, \ldots, \text{Z}\}$ et $\mathcal{K}$ l'ensemble des permutations de $\mathcal{M}$. La réutilisation d'une clé permet d'étendre $E : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ en $E : \mathcal{M}^n \times \mathcal{K} \to \mathcal{C}^n$.

Ce système s'attaque par analyse des fréquences dès lors qu'on sait que le clair est restreint à un certain sous-ensemble de $\mathcal{M}^n$, e.g texte en français qui n'est pas une suite de lettres "très aléatoire".

Question : à partir de quelle longueur de chiffré peut-on retrouver la permutation clé ?

Prenons un alphabet $\mathcal{A}$. Alors $\mathcal{M} = \mathcal{A}^n$ avec une certaine redondance (non uniformité dans $\mathcal{A}$).

Définition. Entropie du langage : $h = \lim_{n\to\infty} \frac{1}{n} H(M)$.

Définition. Redondance du langage : $r = 1 - \frac{h}{\log_2(\text{Card}(\mathcal{A}))}$.

Intuitivement un texte de n symboles dans le langage peut se compresser en nh bits ($n \to \infty$).

En longueur n, parmi les $\text{Card}(A)^n$ suites de n symboles possibles, il y en a $\simeq 2^{nh}$ qui sont dans le langage. Les chiffrés doivent sembler aléatoires, on peut espérer en avoir $\text{Card}(A)^n$.

À chaque chiffré correspond $\frac{2^{nh+\log_2(\#\mathcal{K})}}{(\#\mathcal{A})^n}$ couples (M,K) possibles.

Une recherche exhaustive donne un déchiffrement unique dès lors que $\frac{2^{nh+\log_2(\#\mathcal{K})}}{(\#\mathcal{A})^n} \leqslant 1$, où $\frac{2^{nh+\log_2(\#\mathcal{K})}}{(\#\mathcal{A})^n} = 2^{n(h-\log_2\#\mathcal{A})+\log_2\#\mathcal{K}} = 2^{-rn\log_2\#\mathcal{A}+\log_2\#\mathcal{K}}$.

Définition. Distance critique : $n = \frac{\log_2 \#\mathcal{K}}{r \log_2 \#\mathcal{A}}$.

Exemple. Pour une substitution simple, en français, $\#\mathcal{K} = 26!$, donc $\log_2 \#\mathcal{K} \simeq 88$, $r \in [0{,}75\,;0{,}8]$ et $\#\mathcal{A} = 26$ donc $\log_2 \#\mathcal{A} \simeq 4{,}7$. Alors $n \simeq 25$. En pratique, à la main, on peut casser le chiffrement pour n jusqu'à 200 ou 250.

Autre exemple avec sécurité informationnelle : partage de secret à seuil.

Exemple (Le système de Shamir). Un "distributeur" dispose d'un secret $S \in \mathbf{F}_q$ et veut donner une part de ce secret à n participants de sorte que :

- t participants qui se concertent peuvent reconstruire le secret avec leurs parts,
- $t-1$ participants n'ont aucune info sur S.

On supposera $q > n$. Le distributeur choisit $t-1$ éléments $a_1, \ldots, a_{t-1} \in \mathbf{F}_q$ uniformément indépendants. Il prend le polynôme $P(X) = S = a_1 X + a_2 X^2 + \ldots + a_{t-1} X^{t-1}$.

Étant choisis $x_1, \ldots, x_n \in \mathbf{F}_q^\times$ distincts, on calcule $y_i = P(x_i)$. Au participant n°i est envoyé le couple (x_i, y_i). L'assignation des x_i peut être publique, la part de secret est contenue dans y_i.

Cela vérifie bien les propriétés voulues :

Alice	*Public*	Bob
	$\mathbf{F}_q$	
	$\alpha \in \mathbf{F}_q^\times$	
$r \in \mathbf{Z}$ aléatoire		$s \in \mathbf{Z}$ aléatoire
$\beta = \alpha^r$	$\xrightarrow{\beta}$	
	$\xleftarrow{\gamma}$	$\gamma = \alpha^s$
$\gamma^r = \alpha^{rs}$		$\beta^s = \alpha^{rs}$

- Si t participants se concertent P est déterminé de façon unique par interpolation de Lagrange : $P(X) = \sum_{i=1}^{t} y_i \prod_{j \neq i} \frac{X - x_i}{x_i - x_j}$ et alors $S = P(0)$.
- Si $t-1$ participants se concertent ils ne peuvent en déduire aucune information car toutes les valeurs de S sont compatibles par interpolation de Lagrange.

1.5 Sécurité computationnelle

En cryptographie symétrique, A et B possèdent une clé secrète commune. En cryptographie asymétrique on veut communiquer de façon sécurisée sans avoir eu la possibilité au préalable de se mettre d'accord sur un secret commun.

Historique : 1974, Merkle, projet de fin d'études *Énigmes*.

Bob prépare un grand nombre N de messages clairs qui disent « la clé n°i est k_i ». Il les chiffre de façon pas très sûre, cassable en temps T. Il publie ces chiffres (dans le désordre).

Alice choisit une devinette, elle la résout et apprend un couple (i, k_i). Elle dit à Bob « je connais la clé n°i ». Eve ne sait pas quelle devinette correspond à la clé i, elle doit les résoudre toutes → en moyenne temps $\frac{N}{2}T$.

Exemple (**Diffie-Hellman** (1976)). Système d'échange de clé (key agreement).

À la fin α^{rs} est leur secret commun. Eve voit passer q, α, β, γ. Elle doit en déduire un certain δ tel que $\exists r, s, \delta = \alpha^{rs}, \beta = \alpha^r, \gamma^s$. C'est le *problème de Diffie-Hellman*. Cela ressemble (mais n'est pas équivalent) au problème du log discret : connaissant q, α, β, trouver r tel que $\beta = \alpha^r$.

Exemple (**RSA**, 1978). Méthode de chiffrement et de signature.

Bob choisit p et q premiers secrets. Il calcule $N = pq$, alors $\varphi(N) = (p-1)(q-1)$. Il choisit $e \in \mathbf{N}$ premier à $\varphi(N)$ et d son inverse, i.e $ed = 1 \mod \varphi(N)$.

La clé publique de Bob est (N, e), où N est appelé *module RSA* et e est l'*exposant de chiffrement*. L'entier d sera appelé *exposant de déchiffrement* et constitue la clé secrète.

Alice veut envoyer un message clair à Bob encodé comme un élément $m \in (\mathbf{Z}/N\mathbf{Z})^\times$. Elle calcule $c = m^e$, le chiffré, et l'envoie à Bob. Bob déchiffre $c^d = m^{ed} = m$.

Eve peut vouloir :

1 - retrouver le secret primitif de Bob, i.e p et q, ensuite elle trouve $\varphi(N)$ puis $d = e^{-1}$ par Euclide,

2 - retrouver juste d à partir de (N, e),

3 - être capable de retrouver un m correspondant à un c,

4 - retrouver un bit d'information sur m à partir de c où m est vu comme un entier dans $[\![1 ; N-1]\!]$.

Remarque : en théorie de la complexité on appelle "faciles" les problèmes résolubles en temps polynomial en la taille des entrées. On appelle difficile les problèmes résolubles en tant exponentiel → sous classe NP.

En crypto on veut typiquement que le déchiffrement soit NP : facile si on connaît la clé et difficile si on ne la connaît pas.

Dans le cas de RSA :

1 → problème de factorisation donné N, trouver ses facteurs premiers p et q. Le problème est réputé NP, mais ni P ni NP-complet.

2 → on peut montrer que ça équivaut à 1.

3 → extraction de racine $e^{\text{ième}}$ dans $\mathbf{Z}/N\mathbf{Z}$, $m = \sqrt[e]{c} \mod N$. Si $e = 2$ on a vu que c'était équivalent à la factorisation de N. Mais lorsque e est impair (souvent $e = 3$), cela pourrait être plus facile quee la factorisation mais estimé non polynomial.

4 → équivalent à 3. Plus précisément on a une réduction polynomiale de l'un à l'autre. Soit A une "boîte noire" qui nous dit si $m < \frac{N}{2}$ ou non à partir du chiffré c. Or on a $2^e c = (2m)^e$ le chiffré correspondant au clair $2m \mod N$. Si $m < \frac{N}{2}$, $2m \mod N = 2m$ pair et si $m > \frac{N}{2}$, $2m \mod N = 2m - N$ impair. Ensuite, par dichotomie, en $\log_2(N)$ appels à la boîte A on a complètement localisé m.

Exemple. Public : $\mathbf{F}_q$ et $\alpha \in \mathbf{F}_q^\times$. Clé publique de Bob : $\beta \in \mathbf{F}_q^\times$. Clé secrète : $r \in \mathbf{Z}$ tel que $\beta = \alpha^r$.

Alice veut envoyer le message en clair $m \in \mathbf{F}_q^\times$. Elle choisit $s \in \mathbf{Z}$ aléatoire et calcule $c_1 = \alpha^s$ et $c_2 = \beta^s m$. Elle envoie (c_1, c_2) à Bob qui déchiffre par $c_2 c_1^{-r} = \beta^s m \alpha^{-rs} = m$.

Eve peut vouloir :

1. retrouver la clé secrète à partir de la clé publique $\longrightarrow$ problème du logarithme discret,
2. retrouver m à partir de (c_1, c_2) où sont connus $F_q, \alpha, \beta = \alpha^r, c_1 = \alpha^s, c_2 = m\alpha^{rs}$. Alors retrouver m revient à retrouver α^{rs}. C'est le problème de DH.

DH et El Gamal utilisent la structure de groupe de $\mathbf{F}_q$. La sécurité repose essentiellement sur la difficulté du log discret dans ce groupe. De même que la factorisation on ne sait pas le résoudre en temps polynomial, mais on sait faire mieux que exponentiel.

Formule générale : $L_{\varepsilon,c}(t) = \exp\left(c \cdot t^\varepsilon \log(t)^{1-\varepsilon}\right)$. Si $\varepsilon = 0$ on est dans le cas polynomial : $L_{\varepsilon,c}(t) = t^c$. Si $\varepsilon = 1$ on est dans le cas exponentiel : $L_{\varepsilon,c}(t) = e^{ct}$.

On sait résoudre les problèmes de factorisation et de log discret en $\varepsilon = \frac{1}{3}$. En pratique, avec les puissances de calcul actuelles, cela veut dire que l'on doit prendre des clés de taille environ 2000 bits.

2 Courbes elliptiques

2.1 Définitions

Définition. Une **courbe elliptique** sur un corps K est

- soit la donnée d'une courbe algébrique E projective lisse de genre 1 sur K et d'un point $O_E \in E(K)$,
- soit la donnée d'une équation "de Weierstrass" de la forme $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ qui définit une courbe plane où les coefficients $a_1, a_2, a_3, a_4, a_6 \in K$ sont choisis pour que E soit lisse. La courbe admet alors un unique point à l'infini, noté O_E.

Remarque. Lorsque K est de caractéristique différente de 2 ou 3, on se ramène par changement de variable à une équation de la forme $y^2 = x^3 + ax + b$. La lissité équuivaut donc à ce que $x^3 + ax + b$ soit sans racine double, i.e $\Delta = 4a^3 + 27b^2 \neq 0$ dans K.

Plan projectif : $\mathbf{P}^2 = \mathbf{A}^2 \cup \mathbf{P}^1$ où $\mathbf{P}^2$ correspond à $(X : Y : Z)$, $\mathbf{A}^2$ est le plan affine $(X : Y : 1)$ et $\mathbf{P}^1$ est la droite à l'infini $Z = 0$, $(X : Y : 0)$.

2.2 Loi de groupe

Lemme. Soit $D \in \mathrm{Div}^0(E)$, alors $\exists! P \in E(K), D \sim (P) - (O_E)$.

On a donc une bijection $\begin{array}{ccc} E(K) & \xrightarrow{\sim} & Cl^0(E)_K \\ P & \mapsto & (P) - (O_E) \end{array}$ avec $Cl^0(E)_K$ le groupe des classes d'équivalence linéaire de diviseurs de degré 0 définis sur K.

Définition. On munit $E(K)$ d'une loi de groupe $+$ en transportant la loi de $Cl^0(E)_K$ par cette bijection.

Proposition. (i) L'élément neutre de $E(K)$ est O_E.

(ii) $\forall P, Q \in E(K)$, $P + Q$ dans $E(K)$ est l'unique point tel que $(P) - (O_E) + (Q) - (O_E) \sim (P + Q) - (O_E)$ dans $\mathrm{Div}^0(E)$, i.e. tel que $\exists f \in E(K), \mathrm{div}(f) = (P) + (Q) - (P + Q) - (O_E)$.

(iii) Soit $D = \sum_{P \in E(K)} n_P \cdot (P)$ un diviseur sur E. Alors D est principal si et seulement si $\deg(D) = \sum_P n_P = 0$ et $\sum_p n_P P = O_E$ dans $E(K)$.

(iv) En particulier $P + Q + R = O_E \iff (P) - (O_E) + (Q) - (O_E) + (R) - (O_E) \sim 0$ dans $\mathrm{Div}^0(E)$.

(v) $\forall P \in E(K)$, $-P \in E(K)$ est l'unique point tel que $\exists f, \mathrm{div}(f) = (P) + (-P) - 2(O_E)$.

Remarque. On a $P + Q + R = O_E$ si et seulement si P, Q, R sont les trois points d'intersection de E et d'une droite.

Remarque. Si P est un point de coordonnées affines (x_P, y_P) alors $-P$ a pour coordonnées $(x_P, -y_P)$.

Formule explicite : $x_{P+Q} = \lambda^2 - x_P - x_Q$ et $y_{P+Q} = -y_P + \lambda(x_P - x_{P+Q})$, avec $\lambda = \frac{y_Q - y_P}{x_Q - x_P} = \frac{3x_P^3 + a}{2y_P}$.

Définition. Soit E une courbe elliptique sur K et $n \in \mathbf{N}^*$. On note $E[n] = \{P \in E(\bar{K}) \mid n \cdot P = O_E\}$ où $n \cdot P = P + P + \ldots + P$ pour la loi de E. On dit que P est de n-torsion s'il vérifie $n \cdot P = O_E$;

Remarque. La loi est commutative donc $E[n]$ est un sous-groupe de $E(\bar{K})$. De même $E[n] \cap E(K)$ est un sous-groupe de $E(K)$.

Exemple. Les points de 2-torsion sont les P tels que $P + P = O_E$. Donc soit $P = O_E$, soit $P = (x, 0)$ avec $x^3 + ax + b = 0$. Ce polynôme a trois racines dans $\bar{K}$, donc $E[2] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

...

...

...

Proposition. Il existe deux fractions rationnelles $F_m(x)$ et $G_m(x)$ telles que $\forall P = \begin{bmatrix} x \\ y \end{bmatrix} \in E, m \cdot P = \begin{bmatrix} F_m(x) \\ yG_m(x) \end{bmatrix}$ et le dénominateur de $F_m(x)$ et $G_m(x)$ est une puissance d'un certain polynôme ψ_m, appelé polynôme de m-division, de degré $\deg \psi_m = \begin{cases} \frac{m^2-1}{2} \text{ si } m \text{ est impair} \\ 3 + \frac{m^2-4}{2} \text{ si } m \text{ est pair} \end{cases}$.

Principe de la preuve. On prouve la propriété par récurrence avec les formules pour $(m+1)P = mP+P$. □

Remarque. On a $-P = \begin{bmatrix} x \\ -y \end{bmatrix}$ et $m \cdot P = \begin{bmatrix} F_m(x) \\ -yG_m(x) \end{bmatrix} = m \cdot (-P)$. De plus P est de m-torsion ssi mP est le point O_E à l'infini, ssi x est un pôle de F_m (et de G_m), ssi x est racine de ψ_m.

Exemple. ...

Corrolaire. On a $|E[m]| \leqslant m^2$.

Démonstration. $E[m] = \{(x,y) \in E \mid \psi_m(x) = 0\} \cup \{O_E\}$. Si m est impair, ψ_m a au plus $\frac{m^2-1}{2}$ racines x et pour chaque tel x, au plus deux valeurs de ...

... □

Remarque. En réalité on sait dire mieux dans le cas $m = p^e$. Si $p \neq \text{Card}(K)$ alors $|E[m]| = m^2$ et si $p = \text{Card}(K)$ alors $|E[m]| = 1$ ou m.

Corrolaire. Soit $K = \mathbf{F}_q$ un corps fini. Alors $E(\mathbf{F}_q)$ est le produit d'au plus deux groupes cycliques, c'est-à-dire que ou bien $E(\mathbf{F}_q) \simeq \mathbf{Z}/N\mathbf{Z}$ est cyclique, ou bien $E(\mathbf{F}_q) \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, ...

Démonstration. On a $E(\mathbf{F}_q) \simeq Z/n_1\mathbf{Z} \times \cdots \times Z/n_r\mathbf{Z}$ où $n_{i+1} | n_i$. Soit l premier tel que $l | n_r$, donc $\forall i, l | n_i$. Alors

$$E(\mathbf{F}_q)[l] \subset E[l]$$
$$\simeq$$

□

Théorème (de Hasse). Soit $K = \mathbf{F}_q$ un corps fini et $E : y^2 = x^3+ax+b$. Alors $\left|E(\mathbf{F}_q)\right| \in \left[q+1-2\sqrt{q}; q+1+2\sqrt{q}\right]$, ou encore $\left|E(\mathbf{F}_q)\right| = q+1-t$ pour un entier $t \in \mathbf{Z}, |t| \leqslant 2\sqrt{q}$ (t la "trace").

Remarque. $E(\mathbf{F}_q) = \{O_E\} \cup \{(x,y) \in \mathbf{F}_q \times \mathbf{F}_q \mid y^2 = x^3 + ax + b\}$ et ce deuxième ensemble a pour cardinal q, le nombre de valeur possibles pour x. En effet, à x fixé il y a 0, 1 ou 2 valeurs possibles pour y. 0 si x^3+ax+b n'est pas carré dans $\mathbf{F}_q$, 1 si $x^3 + ax + b = 0$, donc $y = 0$ et 2 si $x^3 + ax + b \neq 0$ est un carré dans $\mathbf{F}_q$.

Il y a autant de carrés que de non carrés dans $\mathbf{F}_q$. On s'attend donc à ce que $x^3 + ax + b$ soit à peu près aussi souvent carré que non carré. Le théorèmme de Hasse dit que l'excès de l'un ou de l'autre est inférieur à $2\sqrt{q}$.

Exemple. Prenons $K = \mathbf{F}_5, |E[\mathbf{F}_5]| \in [2;10], E : y^2 = x^3 - x$, donc $a = -1$ et $b = 0$. Alors $\Delta = 4a^3 + 27b^2 = 1 \neq 0$ et $E(\mathbf{F}_5)$ contient les éléments suivants :

$$0_E, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 3 \end{bmatrix}, \begin{bmatrix} 4 \\ 0 \end{bmatrix}$$

d'où $\left|E(\mathbf{F}_(5)\right| = 8$. On veut l'identifier à un groupe abélien de cardinal 8 qui soit produit d'au plus deux groupes cycliques. Or il existe deux tels groupes : $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/8\mathbf{Z}$.

Remarquons alors que $E(\mathbf{F}_5)[2] = \left\{O_E, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 4 \\ 0 \end{bmatrix}\right\}$ et $\mathbf{Z}/8\mathbf{Z}[2] = 4\mathbf{Z}/8\mathbf{Z} = \{\bar{0}, \bar{4}\}$. Donc l'isomorphisme se fait nécessairement avec $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Rappel : expliciter un isomorphisme entre en groupe abélien donné et un produit de cycliques revient à trouver une "base" de ce groupe. Soit G donné. On veut un isomorphisme explicite $G \simeq \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$.

1. nécessairement $n_1 = \omega(G)$ et on cherche $x_1 \in G$ d'ordre maximal $\omega(G)$,
2. alors $G/\langle x_1 \rangle \simeq \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$ et l'on trouve récursivement $z_2, \ldots, z_r$ une "base" de ce quotient,

3. relever chaque $z_i \in G/\langle x_1\rangle$ en un $x_i \in G$ de sorte que $\langle x_1\rangle \cap \langle x_2,\dots,x_r\rangle = \{0\}$.

Dans ce cas :

(1) on cherche $P \in E(\mathbf{F}_5)$ d'ordre 4. Les éléments de $E(\mathbf{F}_5) \simeq \mathbf{Z}/4\mathbf{Z} \times Z/2\mathbf{Z}$ sont d'ordre 1, 2 ou 4. Tout élément qui n'est pas de 2-torsion est d'ordre 4. $P = \begin{bmatrix}2\\1\end{bmatrix}$ convient.

(2) Trouver Q d'ordre 2 tel que

$$\begin{aligned}\langle P\rangle \cap \langle Q\rangle = \{O_E\} &\iff Q \text{ d'ordre } 2, Q \notin \langle P\rangle = \{O_E, P, 2P, 3P\}\\ &\iff Q \text{ d'ordre } 2, Q \neq 2P\end{aligned}$$

Calcul de $2P$: $\lambda = \frac{3\cdot 2^2-1}{2\cdot 1} = -\frac{4}{2} = 3$ donc $2P = \begin{bmatrix}3^2-2-2\\3(2-0)-1\end{bmatrix} = \begin{bmatrix}0\\0\end{bmatrix}$. On peut prendre $Q = \begin{bmatrix}1\\0\end{bmatrix}$.

Exemple. $E : y^2 = x^3 + x$, $\Delta = 4 \neq 0$ et $E(\mathbf{F}_5) = \left\{O_E, \begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}2\\0\end{bmatrix}, \begin{bmatrix}3\\0\end{bmatrix}\right\}$, d'où $|E(\mathbf{F}_5)| = 4$ et $E(\mathbf{F}_5) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Exemple. $E : y^2 = x^3 + x + 2$, $E(\mathbf{F}_5) = \{O_E, \dots\}$ ...

2.3 Isogénies

Définition. Soit E et E' deux courbes elliptiques. Une isogénie $E \to E'$ est un morphisme de courbes algébriques $E \to E'$ qui envoie O_E sur $O_{E'}$.

Concrètement, si $E : y^2 = x^3 + ax + b$ et $E' : y^2 = x^3 + a'x + b'$, un morphisme de E dans E' est donné par des fonctions rationnelles $f(x,y)$ et $g(x,y)$ telles que

$$\forall x, y^2 = x^3 + ax + b \implies g(x,y)^2 = f(x,y)^3 + a'f(x,y) + b'$$

et le morphisme envoie $\begin{bmatrix}x\\y\end{bmatrix} \in E$ sur $\begin{bmatrix}f(x,y)\\g(x,y)\end{bmatrix} \in E'$.

Exemple. Soit $u \in K^\times$. $\begin{pmatrix}x\\y\end{pmatrix} \mapsto \begin{pmatrix}u^2x\\u^3y\end{pmatrix}$ définit une isogénie de $y^2 = x^3 + ax + b$ dans $y^2 = x^3 + u^4ax + u^6b$.

Cette isogénie est inversible (isomorphisme) d'inverse $\begin{pmatrix}x\\y\end{pmatrix} \mapsto \begin{pmatrix}u^{-2}x\\u^{-3}y\end{pmatrix}$.

On peut montrer que tout isomorphisme entre deux courbes elliptiques est de cette forme. Par ailleurs, remplacer la courbe $y^2 = x^3 + ax + b$ par $y^2 = x^3 + u^4ax = u^6b$ laisse invariant $j = \frac{4a^3}{4a^3+27b^2}$.

Théorème. Deux courbes sont isomorphes (sur $\bar{K}$) ssi elles ont le même j-invariant. De plus pour tout choix de $j \in K$, il existe $a, b \in K$ tels que la courbe $y^2 = x^3 + ax + b$ est une courbe elliptique de j-invariant égal à j.

Démonstration. Prouvons la deuxième partie. On cherche a, b tels que $A = 4a^3$ et $B = 27b^2$. De la sorte $j = \frac{A}{A+B} = \frac{1}{1+B/A}$.

Dans le cas $j \neq 0$, $1 + \frac{B}{A} = \frac{1}{j}$,...

...

□

Exemple. Supposons que K contient un élément i tel que $i^2 = -1$, comme $i = 2$ dans $K = \mathbf{F}_5$. Alors $\begin{pmatrix}x\\y\end{pmatrix} \mapsto \begin{pmatrix}-x\\iy\end{pmatrix}$ définit une isogénie, et même un isomorphisme de le courbe $y^2 = x^3 - x$ dans elle-même.

Exemple. Soit E une courbe elliptique et m un entier. Alors $\begin{array}{ccc}E & \to & E\\ P & \mapsto & mP\end{array}$ est une isogénie de E.

Exemple. Soit $K = \mathbf{F}_p$, $E : y^2 = x^3 + ax + b$. Le Frobenius $\varphi(x,y) = (x^p, y^p)$ définit une isogénie de E. En effet, $\forall x, y \in \bar{\mathbf{F}}_p$,

$$y^2 = x^3 + ax + b \implies (y^p)^2 = (y^2)^p = (x^3 + ax + b)^p = (x^p)^3 + ax^p + b\,.$$

Théorème. Si $E \to E'$ est une isogénie, alors elle définit un morphisme de groupes $E(K) \to E'(K)$.

Démonstration. Les lois de $E(K)$ et $E'(K)$ sont celles de leurs groupes de classes de diviseurs. □

Exemple. Cas $K = \mathbf{F}_5$, $E : y^2 = x^3 - x$ et les points de $E(\mathbf{F}_5)$ sont

$$O_E, \underbrace{\begin{pmatrix}0\\0\end{pmatrix}}_{2P}, \underbrace{\begin{pmatrix}1\\0\end{pmatrix}}_{Q}, \underbrace{\begin{pmatrix}2\\1\end{pmatrix}}_{P}, \underbrace{\begin{pmatrix}2\\4\end{pmatrix}}_{3P}, \underbrace{\begin{pmatrix}3\\2\end{pmatrix}}_{3P+Q}, \underbrace{\begin{pmatrix}3\\3\end{pmatrix}}_{P+Q}, \underbrace{\begin{pmatrix}4\\0\end{pmatrix}}_{2P+Q}$$

On le munit de l'isogénie $\begin{pmatrix}x\\y\end{pmatrix} \mapsto \begin{pmatrix}-x\\2y\end{pmatrix}$. Elle respecte la structure de groupe et induit un isomorphisme de groupes de $E(\mathbf{F}_5) \simeq \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ dans lui-même.

...

Remarque. ...

Exercice. On prend $y^2 = x^3 - x$. Ses zéros sont $P_1 = \begin{pmatrix}-1\\0\end{pmatrix}$, $P_2 = \begin{pmatrix}0\\0\end{pmatrix}$ et $P_3 = \begin{pmatrix}1\\0\end{pmatrix}$.

On veut montrer $\mathrm{div}(x) = 2(P_2) - 2(O_E)$ et $\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(O_E)$.

On a $K[x,y]/(y^2 - (x^3 - x), x) = K[y]/(y^2)$. Si on veut formaliser : il s'agit d'une courbe plane lisse donnée par une équation $F(x,y) = 0$. On se donne une fonction $h(x,y)$ qui n'est pas multiple de F (sinon h est identiquement nulle sur la courbe) et de dimension finie. On veut trouver l'ordre d'annulation de h en un point P de la courbe, i.e l'anneau quotient $K[x,y]/(F,h)$.

On a $K[x,y]/(F,h) \simeq A_1 \times \cdots \times A_r$ produit fini d'anneaux de dimensions finies. r est le nombre de points d'intersection de $F = 0$ et $h = 0$ et chaque A_i correspond à un P_i point d'intersection. De plus $\dim A_i$ est l'ordre de h en P_i.

Pour garder uniquement le A_i qui correspond à P il faut en plus trouver une autre fonction ψ telle que ψ s'annule en P avec une grande multiplicité (convient si supérieure à $\deg(F) \cdot \deg(h)$) et $\psi \neq 0$ sur les autres P_i. Alors $K[x,y]/(F,h,\psi) = A_{i_0}$ où i_0 est l'indice de P.

Souvent on aura pas besoin de tout ça et on pourra conclure plus rapidement par un simple argument de degré.

On obtient alors $\mathrm{div}\left(\frac{x}{y}\right) = \mathrm{div}(x) - \mathrm{div}(y) = (P_2) + (O_E) - (P_1) - (P_3)$. Si l'on veut dérouler l'algo jusqu'au bout, par exemple pour trouver $v_{P_2}(y)$, on cherche une fonction ψ qui s'annule en P_2 à l'ordre 3 et non nul en P_1 et P_3. Par exemple $\psi = x^3$ convient. On obtient $K[x,y]/(y^2 - (x^3 - x), y, x^3) \simeq K[x]/(x)$ de dimension 1.

Lemme. Soient P et Q deux points de E et $l_{P,Q} : \lambda x + \mu y + \nu$ l'équation affine de la droite (PQ) (ou bien de la tangente à la courbe en P si $P = Q$). Alors $\mathrm{div}(l_{P,Q}) = (P) + (Q) + (-P - Q) - 3(O_E)$.

On se donne $D = \sum_P n_P(P)$ tel que $\sum n_P = 0$ et $\sum n_P P = O_E$.

Problème : trouver f tel que $D = \mathrm{div}(f)$.

Quitte à réécrire les points autant de fois que leur multiplicité $D = (P_1) + \ldots + (P_n) - (Q_1) - \ldots - (Q_n)$ avec $P_1 + \ldots + P_n = Q_1 + \ldots + Q_n$ dans E. On procède par récurrence sur n.

Pour $n = 0$ et $D = 0$, $f = 1$ convient. Pour $n = 1$, $D = (P_1) - (P_1) = 0$ et on retombe sur $n = 0$.

On suppose $n \geqslant 2$ et qu'on sait faire jusqu'à $n - 1$.

...

...

2.4 Les courbes algébriques en crypto

Les courbes algérbriques ont été introduites pour la factorisation → généralisation de l'algo $p - 1$ de Pollard qui permet de trouver facilement les diviseurs premiers p d'un entier N tel que $p - 1$ soit friable. On doit donc éviter ce type de facteur.

Cela repose sur $N = pq \implies (\mathbf{Z}/N\mathbf{Z})^\times \simeq (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times$. L'algorithme $p - 1$ de Pollard fonctionne si $\mathbf{F}_p^\times$ est friable.

Lenstra généralise cela avec des courbes elliptiques. Soit $a, b \in \mathbf{Z}/N\mathbf{Z}$ et $E : y^2 = x^3 + ax + b$. On a $E(\mathbf{Z}/N\mathbf{Z}) = E(\mathbf{F}_p) \times E(\mathbf{F}_q)$ (avec des bizarreries pour O_E). Quand a et b varient, $\left|E(\mathbf{F}_q)\right|$ varie et on arrive toujours à tomber sur un friable.

Plus tard les courbes algébriques ont été utilisées pour fabriquer des cryptosystèmes en remplaçant $\mathbf{F}_p^\times$ par $E(\mathbf{F}_p)$ où le log discret est plus difficile.

2.5 Couplages

Les couplages ont été introduits pour la cryptanalyse pour ramener certaines instances du log discret elliptique au log discret classique. On fabrique ensuite des cryptosystèmes avec des propriétés spéciales.

Définition. Soient A, B, G trois groupes abéliens, avec une loi notée additivement pour A et B, et multiplicativement pour G. Un **couplage** e: $A \times B \to G$ est une application bilinéaire, i.e telle que $e(a + a', b) = e(a,b)e(a',b)$ et $e(a, b + b') = e(a,b)e(a,b')$.

Dans le cas particulier $A = B$:

- le couplage est dit **symétrique** si $e(a,b) = e(b,a)$,
- le couplage est dit **alterné** si $\forall a, e(a,a) = 1$, ce qui implique l'antisymétrie $e(b,a) = e(a,b)^{-1}$.

Construction d'un couplage alterné sur les groupes de m-torsion d'une courbe elliptique. On travaille sur $K = \mathbf{F}_q$ où $q = p^n$ avec p premier et on note $\bar{K}$ la cloture algébrique de K. Soit $m \in \mathbf{N}$ tel que $p \nmid m$. Soit $\mu_m \subset \bar{K}^\times$ le groupe des racines m-ièmes de l'unité. μ_m forme un groupe cyclique d'ordre m, donc $\mu_m \simeq \mathbf{Z}/m\mathbf{Z}$.

Remarque. $X^m - 1$ est bien à racines simples dans $\bar{K}$ car sa dérivée est mX^{m-1} et $\operatorname{pgcd}(X^m - 1, mX^{m-1}) = 1$.

Soit E une courbe elliptique sur K. $E[m] \subset E(\bar{K})$ est le produit de deux groupes cycliques d'ordre m.

On va construire le couplage de Weil $e_m \colon E[m] \times E[m] \to \mu_m$. Soient $P, Q \in E[m]$ et $D_{P,Q} = (P) + (P+Q) + (P+2Q) + \ldots + (P+(m-1)Q) - (O_E) - (Q) - (2Q) - \ldots - ((m-1)Q)$. Ce diviseur est principal (puisque $mP = O_E$ par définition de $P \in E[m]$)..

On construit effectivemet une fonction f_{PQ} telle que $\operatorname{div}(f_{PQ}) = D_{PQ}$.

Soit maintenant $\tau_Q \colon \begin{array}{ccc} E & \to & E \\ R & \mapsto & Q+R \end{array}$ l'application de translation par Q. C'est un morphisme algébrique de E dans lui-même.

Si f est une fonction de E, $\tau_Q^* f$ est la fonction telle que $\tau_Q^* f(R) = f(Q+R)$. Donc $\operatorname{div}(\tau_Q^* f)$ est translatée de $\operatorname{div}(f)$ par $-Q$.

En particulier, pour $f = f_{P,Q}$, $\div(\tau_Q^* f_{P,Q}) = \operatorname{div}(f_{P,Q}) = D_{PQ}$ invariant par translation par Q. Donc $\tau_Q^* f_{P,Q} = c \cdot f_{P,Q}$ pour une certaine constante $c \in \bar{K}^*$.

$$\tau_{2Q}^* f_{P,Q} = \tau_Q^* \tau_Q^* f_{P,Q} = \tau_Q^*(c \cdot f_{P,Q}) = c \cdot \tau_Q^* f_{P,Q} = c^2 f_{P,Q}$$

Par suite il vient $\tau_{mQ}^* f_{P,Q} = c^m f_{P,Q}$. Or $mQ = O_E$ car $Q \in E[m]$, donc $\tau_{mQ}^* f_{P,Q} = f_{P,Q}$, d'où $c \in \mu_m$.

Définition. $e_m(P,Q) = \frac{\tau_Q^* f_{P,Q}}{f_{P,Q}}$.

Théorème. (i) $e_m(P+P',Q) = e_m(P,Q) e_m(P',Q)$,

(ii) $e_m(P,Q+Q') = e_m(P,Q) = e_m(P,Q')$,

(iii) $e_m(P,P) = 1$,

(iv) si $P, Q \in E[m](K)$ alors $e_m(P,Q) \in K$,

(v) $e_m \colon E[m] \times E[m] \to \mu_m$ est surjective.

Démonstration. *(ii)* et *(v)* sont admises (difficiles).

Pour *(i)* : on peut choisir $f_{P+P',Q} = f_{P,Q} \cdot \tau_{-P}^* f_{P',Q}$ et alors

$$\frac{\tau_Q^* f_{P+P',Q}}{f_{P+P',Q}} = \frac{\tau_Q^* f_{P,Q}}{f_{P,Q}} \cdot \frac{\tau_Q^* \tau_{-P}^* f_{P',Q}}{\tau_{-P}^* f_{P',Q}} = \frac{\tau_Q^* f_{P,Q}}{f_{P,Q}} \cdot \tau_{-P}\left(\frac{\tau_Q^* f_{P',Q}}{f_{P',Q}}\right)$$

Pour *(iii)* : $D_{P,P} = 0$, $f_{P,P} = 1$.

Pour *(iv)* : $f_{P,Q}$ diviseur de $D_{P,Q}$ est construite par récurrence. □

3 Carré modulaire

Rappel : on travaille sur un corps premier $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ avec $p > 2$.

On étudie la fonction $x \mapsto x^2$ dans $\mathbf{F}_p^\times$. C'est un morphisme de noyau $\{\pm 1\}$ de cardinal 2. Son image est donc de cardinal $\frac{p-1}{2} = \frac{\varphi(p)}{2}$, i.e dans $(\mathbf{Z}/p\mathbf{Z})^\times$ il y a $\frac{p-1}{2}$ résidus quadratiques et $\frac{p-1}{2}$ non-résidus.

Soit N composé sans facteur carré, $N = p_1 \cdots p_r$, $\forall i, p_i > 2$. Regardons alors $\begin{array}{ccc} (\mathbf{Z}/N\mathbf{Z})^\times & \to & (\mathbf{Z}/N\mathbf{Z})^\times \\ x & \mapsto & x^2 \end{array}$. C'est un morphisme de groupes de noyau $\{x \in (\mathbf{Z}/N\mathbf{Z})^\times \mid \forall i, x \equiv \pm 1 \mod p_i\}$, de cardinal 2^r. L'image est donc de cardinal $\frac{\varphi(N)}{2^r} = \prod_i \frac{p_i - 1}{2}$ et est égale à $\{x \in (\mathbf{Z}/N\mathbf{Z})^\times \mid \forall i, x \text{ est carré } \mod p_i\}$.

Disgression : dans un corps, tout polynôme P de degré d admet au plus d racines :

(1) si x_1 est racine de P, alors $P(X) = (X - x_1)Q(X)$ (marche dans n'importe quel anneau),

(2) si $x_2 \neq x_1$ est une autre racine de P alors $0 = P(x_2) = (x_2 - x_1)Q(x_2)$ donc $Q(x_2) = 0$ car on est dans un corps ou anneau intègre, et on conclut par récurrence.

Exemple. Cas de $X^2 - 1$ dans $\mathbf{Z}/15\mathbf{Z}$. Le polynôme admet 4 racines : $\pm 1 \mod 3$ et $\pm 1 \mod 5$. Qu'est ce qui se passe si l'on déroule la preuve précédente ?

(1) $x_1 = 1$ est racine de $P(X) = X^2 - 1$ d'où $P(X) = (X-1)(X+1)$,

(2) $x_2 = 4$ est une autre racine : $0 = P(4) = \underbrace{(4-1)}_{\neq 0}\underbrace{(4+1)}_{\neq 0}$.

Symbole de Legendre : soit $a \in \mathbf{Z}$ et $p > 2$ premier,

$$\left(\frac{a}{b}\right) = a^{\frac{p-1}{2}} \mod p = \begin{cases} 0 & \text{si } p \mid a \\ 1 & \text{si } a \text{ est un résidu quadratique modulo } p \\ -1 & \text{si } a \text{ n'est pas résidu} \end{cases}$$

Symbole de Jacobi : $\left(\frac{m}{n}\right)$ avec $m \in \mathbf{Z}$ et $n > 0$ un entier impair. Si $n = \prod_{i=1}^{r} p_i^{e_i}$ alors $\left(\frac{m}{n}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right)^{e_i}$. Pour simplifier on suppose n sans facteur carré, i.e $\forall i, e_i = 1$.

On suppose $(m,n) = 1$. Alors

$$m\text{est un carré} \mod n \iff \forall i, m\text{est un carré} \mod p_i \iff \forall i, \left(\frac{m}{p_i}\right) = 1 \implies \left(\frac{m}{n}\right) = 1$$

On remarque qu'il y a $\frac{\varphi(n)}{2^r}$ valeurs m telles que m est un carré modulo n, et $\frac{\varphi(n)}{2}$ tels que $\left(\frac{m}{n}\right) = 1$.

Jacobi (et Legendre) se calcule en temps $O(\log n)$:

- $\left(\frac{m}{n}\right) = \left(\frac{m \pmod n}{n}\right)$
- $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right)$
- $\left(\frac{2m}{n}\right) = (-1)^{\frac{n^2-1}{8}} \left(\frac{m}{n}\right)$.

Le Jacobi $\begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^\times & \to & \{\pm 1\} \\ x & \mapsto & \left(\frac{x}{n}\right) \end{array}$ est un morphisme de groupes.

En effet $\left(\frac{xy}{n}\right) = \left(\frac{x}{n}\right)\left(\frac{y}{n}\right)$ car $\forall i, \left(\frac{xy}{p_i}\right) = \left(\frac{x}{p_i}\right)\left(\frac{y}{p_i}\right)$.

Il est surjectif : soit a non résidu modulo p_1 : $a = a \mod p_1$ et $a = 1 \mod p_i$ pour $i \in [\![2; r]\!]$. Alors $\left(\frac{x}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{1}{p_2}\right)\cdots\left(\frac{1}{p_r}\right) = -1$.

Donc il est de noyau de cardinal $\frac{\varphi(x)}{2}$.

Souvent dans les applications cryptographiques on prend $N = pq$ (entier RSA).

Soit $m \in (\mathbf{Z}/N\mathbf{Z})^\times$.

- $\left(\frac{m}{N}\right) = -1$ se produit $\frac{\varphi(N)}{2}$ fois. m n'est pas carré modulo N et, en fait, ou bien m est carré modulo p et non carré modulo q, ou l'inverse.
- $\left(\frac{m}{N}\right) = +1$ signifie que, ou bien $\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right) = +1$ et m est carré modulo N, ce qui se produit $\frac{\varphi(N)}{4}$ fois, ou bien $\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right) = -1$ et on dit que m est pseudo-carré modulo N ce qui se produit $\frac{\varphi(N)}{4}$ fois.

Problème algorithmique :

	calculer Legendre/Jacobi	décider si un élément est un carré	extraire une racine carrée
mod p premier	facile	facile	facile
mod N composé	facile	difficile (mais pas pire que factoriser)	difficile (équivalent à factorise

Extraire une racine carrée $\mod p$ Cas facile : $p \equiv 3 \mod 4$. Soit x un carré $\mod p$. Alors $x^{\frac{p+1}{4}}$ est une racine de x (où $x^{\frac{p+1}{4}}$ s'obtient par exponentiation rapide, donc complexité polynomiale en le nombre de chiffres de p). En effet

$$\left(x^{\frac{p+1}{2}}\right)^2 = x^{\frac{p+1}{2}} = x \cdot x^{\frac{p-1}{2}} = x$$

...

TODO

...

Extraire une racine carrée $\mod p$ Difficulté : un carré admet deux racines, donc tout algo d'extraction de racine suppose de privilégier l'une des deux.

Algo 1 : Adleman-Manders-Miller $p-1 = u2^v$ avec u impair et $v = v_2(p-1)$. $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'ordre $p-1$. Pour tout $k \in [O;v]$ il admet un unique s-g d'ordre $u2^k$, en l'occurrence c'est le s-g formé des puissances 2^{v-k}-ièmes.

En notation additive, $(\mathbf{Z}/p\mathbf{Z})^\times \simeq \mathbf{Z}/(p-1)\mathbf{Z} = \mathbf{Z}/u2^v\mathbf{Z}$ admet pour s-g $2^{v-k}\mathbf{Z}/u2^v\mathbf{Z} \simeq \mathbf{Z}/u2^k\mathbf{Z}$.

Exemple. $p = 13$, $u = 3$, $v = 2$ et $12 = 3 \cdot 2^2$. Alors $(\mathbf{Z}/13\mathbf{Z})^\times = \{1,2,4,8,3,6,12,11,9,5,10,7\}$ (engendré par 2), $k = 2$. Il inclut les carrés : $\{1,4,3,12,9,10\}$, $k = 1$, qui inclut les puissances 4^e : $\{1,3,9\}$, $k = 0$. L'élévation au carré n'est bijective dans aucun de ces s-g sauf dans le dernier $k = 0$.

Si x est une puissance 2^v-ième, alors x appartient à ce dernier s-g, d'ordre u, dans lequel l'élévation au carré est inversible car 2 est inversible modulo u : $2^{-1} \mod u = \frac{u+1}{2}$ (dans le cas $p \equiv 3 \mod 4$, $u = \frac{p-1}{2}$, $v = 1$ et $2^{-1} \mod u = \frac{p+1}{4}$). Alors $y = x^{\frac{u+1}{2}}$ est une racine de x.

L'entrée de l'algorithme est $x \in (\mathbf{Z}/p\mathbf{Z})^\times$, réputé être carré. La sortie est une racine de x. Sont donnés : $p-1 = n2^v$ et b un non-résidu modulo p (par exemple b primitif).

Par récurrence on va construire des indices k_i : $v > k_1 > k_2 > \dots$ comme suit :

- $a_1 = x$
- étape i :
  - soit k_i e plus petit entier $k \geqslant 0$ tel que $a_i^{u2^k} = 1$. Remarque : alors $a_i^{u2^{k_i-1}} = -1$. On a $k_{i+1} \leqslant k_i - 1$.
  - on pose $a_{i+1} = a_i b^{v-k_i}$
- À l'étape N : $k_N = 0$ et $a_N^u = 1$
  - a_N appartient à l'unique s-g d'ordre u,
  - $r_N = a_N^{\frac{u+1}{2}}$ est racine de a_N, car $r_N^2 = a_N^{u+1} = a_N$.
- On remonte : si r_{i+1} est racine de a_{i+1} alors $r_i = r_{i+1} \cdot (b^{2^{v-k_i-1}})^{-1}$ est racine de a_i.

Algo 2 : probabiliste Entrée : x un carré. Sortie : y une racine de x.

À un moment il faut bien choisir entre y et $-y$: si $p \equiv 3 \mod 4$ il y a un carré et un non-carré parmi y et $-y$, si $p \equiv 1 \mod 4$ ça ne marche plus...

Remarque. Si a est aléatoire $\neq \pm y$ alors parmi $a+y$ et $a-y$, avec proba $\geqslant \frac{1}{2}$ il y aura un carré et un non-carré, ce qui équivaut à avoir $\frac{a+y}{a-y}$ non-carré.

L'application $\begin{array}{ccc} \mathbf{Z}/p\mathbf{Z} \setminus \{\pm y\} & \to & \mathbf{Z}/p\mathbf{Z} \setminus \{0,1\} \\ a & \mapsto & \frac{a+y}{a-y} \end{array}$ est bijective, touche $\frac{p-1}{2}$ non-carrés et $\frac{p-1}{2} - 1$ carrés.

On choisit a aléatoire et on calcule $\operatorname{pgcd}\left(X^{\frac{p-1}{2}} - 1, (X-a)^2 - x\right)$. Alors, avec proba $\simeq \frac{1}{2}$, ce pgcd est de la forme $X - c$. En effet : les racines de $X^{\frac{p-1}{2}} - 1$ sont les carrés de $(\mathbf{Z}/p\mathbf{Z})^\times$ et les racines de $(X-a)^2 - x$ sont $\{a+y, a-y\}$. Le pgcd est $X - c$ où ...

TODO

...

3.1 Extraction de racine modulo N où $N = pq$ est un entier RSA

...

TODO

...

Sécurité :

RSA		
attaque à chiffré seul	extraire une racine e-ième, pas plus difficile que factoriser	extrair
attaque à chiffré choisi	Bob est une boîte noire qui extrait les racines e-ième	Bob est une boîte noire qui extra

3.2 Un protocole de tirage à pile ou face

Alice choisit N un entier de Blum et $x_0 \in (\mathbf{Z}/N\mathbf{Z})^\times$. Elle calcule $x_1 = x_0^2$ et $x_2 = x_1^2 = x_0^4$. Elle publie N et x_2.

Bob choisit un bit au hasard, "pair" ou "impair". Alice révèle tout (x_0, p et q facteurs de N). Bob gagne si son choix est la parité de x_1.

Alice ne peut pas tricher car on vérifie tout a posteriori. Bob ne gagne pas avec proba $\geqslant \frac{1}{2}$ sauf s'il sait distinguer carrés de pseudo-carrés (difficile).

x_1 est une des quatres racines de x_2 et en fait c'est la racine principale. Imaginons que Bob sache gagner avec proba $\geqslant \frac{1}{2}$. Soit y tel que $\left(\frac{y}{N}\right) = 1$. On pose $x = y^2$.

On demande à Bob de choisir “pair” ou “impair” en lui soumettant $x_2 = x$. x admet 4 racines dont 2 de symbole de Jacobi -1 et 2 de symbole de Jacobi $+1$ qui sont y et $N - y$, une des deux est la racine principale (carrée), l'autre est un pseudo-carré et sont de parité différentes.

Pour Bob, distinguer les parités est équivalent à décider si y est carré ou pseudo-carré.