Jacobienne des courbes de genre 2
Applications à la cryptographie

Damien Robert
Directeur de thèse: Guillaume Hanrot

8 octobre 2009

Table des matières

1 Logarithme discret dans un groupe

Définition 1: Soit G un groupe abélien fini. $g \in G$ un élément du groupe d'ordre n, et $y \in \langle g \rangle$. On note $\log_g(y)$ l'élément $x \in \mathbf{Z}/n\mathbf{Z}$ tel que $y = g^x$. C'est le logarithme de y en base g.

1.1 Logarithme discret en cryptographie

Le logarithme discret dans un groupe est a priori difficile à calculer, alors que sa fonction réciproque l'exponentiation est rapide ($g \mapsto g^m$ est polynomiale en $\log_2(m)$). A l'instar du couplage puissance modulaire et racine modulaire dans $\mathbf{Z}/p\mathbf{Z}$ qui donne RSA, le problème du logarithme discret nous fournit une cryptographie asymétrique.

Ainsi, supposons que Alice et Bob veulent converser sur un canal public. S'ils ont beaucoup de données à échanger, utiliser un protocole à base de clé publique pour l'ensemble de l'échange est coûteux, de tels algorithmes étant environ 100 fois plus longs que les algorithmes à clé secrète. Le meilleur moyen est d'arriver à échanger une clé secrète de manière sécurisée.

Définition 2 (Protocole d'échange de clé de Diffie-Hellmann): Alice choisit un groupe G[1] et un élément $g \in G$ d'ordre n, qu'elle rend publique. Alice choisit ensuite un secret $a \in \mathbf{Z}/n\mathbf{Z}$, et publie $p_a := g^a$. Bob choisit de même $b \in \mathbf{Z}/n\mathbf{Z}$ et publie $p_b := g^b$. Alice et Bob calculent ensuite la clé secrète commune $s := g^{ab} = p_a^b = p_b^a$.

Un attaquant (Eve) qui voudrait retrouver la clé secrète commune doit trouver g^{ab} à partir de g^a et g^b. Il s'agit du problème de Diffie-Hellman calculatoire pour le couple p_a, p_b. En pratique, on ne sait résoudre le problème de Diffie-Hellman calculatoire qu'en calculant le log discret de p_a ou p_b.

La même idée conduit à un algorithme de cryptographie à clé publique reposant sur le problème de Diffie-Hellmann calculatoire.

Définition 3 (Algorithme d'ElGamal): Alice choisit un groupe G et un élément $g \in G$. Elle choisit une clé secrète $a \in \mathbf{Z}$ et publie $(G, g, p_a := g^a)$. Bob veut envoyer un message $m \in G$ à Alice, sans que Eve qui écoute sur le canal ne puisse le connaître. Il choisit $b \in \mathbf{Z}$ et envoie $(p_b := g^k, s := p_a^k m)$. Alice calcule alors $m = s/p_b^a$.

Eve connaît g^a, g^k et $g^{ak}m$. Retrouver m revient encore une fois à un problème de Diffie-Hellmann calculatoire sur le couple g^a, g^b.

Remarque 4: Bob doit faire attention à changer k à chaque message qu'il envoie, car à partir de $g^k m_1$ et $g^k m_2$, Eve connaît m_1/m_2, ce qui lui permettrait de retrouver m_1 si elle arrive à faire envoyer par Bob un message m_2 qu'elle connaît.

Comme d'habitude, en magouillant ce protocole de cryptographie asymétrique on arrive à un algorithme de signature de message :

Définition 5 (Algorithme de signature d'ElGamal): Alice a toujours $(G, g, p_a := g^a)$ comme clé publique, où cette fois on suppose que $G = \mathbf{Z}/p\mathbf{Z}^\star$ et g est un de ses générateurs. Elle envoie un message m à Bob. Le canal étant non sécurisé, Bob veut vérifier que le message provient bien d'Alice. Alice choisit alors $k \in (\mathbf{Z}/p\mathbf{Z})^\star$ au hasard puis publie

[1] En pratique on prend $G = (\mathbf{Z}/pZ)^\star$ pour p un grand nombre premier

$(r := g^k, s := (m - ar)/k)$[1]. Si $s = 0$, Alice recommence le calcul avec un autre k . Bob n'a plus qu'à vérifier que $g^m = p_a^r r^s$.

Remarque 6:
- Si Bob retrouve a à partir de l'information donnée par Alice, c'est qu'il connaît k et donc connaît le log discret de r.
- Si Eve répond à la place d'Alice, elle doit trouver $r := g^k$ et s tels que $p_a^r r^s = g^m$, c'est à dire que $ar + ks \cong m$, mais alors elle connaît a.
- L'algorithme de signature DSA est basé sur un schéma de même type.

Enfin, le logarithme discret peut aussi servir comme protocole Zero-Knowledge. Alice a un secret s. Elle veut prouver à Bob qu'elle connaît s, mais sans lui révéler.

Définition 7 (Zero-Knowledge): Alice choisit un groupe G et un élément $g \in G$ d'ordre n. Bob veut vérifier que Alice connaît bien $s \in \mathbf{Z}/n\mathbf{Z}$. Alice ne veut pas révéler s à Bob. Le protocole est le suivant : Alice publie $p = g^s$. Puis elle choisit un $x \in \mathbf{Z}/n\mathbf{Z}$ au hasard, et envoie $q = g^x$ à Bob. Bob à deux choix : soit il demande x à Alice et vérifie que $q = g^x$, soit il demande $s + x$ et vérifie que $qp = g^{x+s}$. On recommence un nombre suffisant de fois jusqu'à ce que Bob soit convaincu que Alice connaît bien s.

Remarque 8: Si Alice ne connaît pas s mais connaît le choix de Bob à l'avance, elle peut le tromper ainsi : si Bob va vérifier que $qp = g^{x+s}$, Alice envoie g^x/p au lieu d'envoyer g^x. Mais si Bob demande x, Alice doit alors renvoyer $x - s$, ce qui n'est pas possible si elle ne connaît pas s.

1.2 Difficulté du logarithme discret

Pour toute la suite du texte, p représentera un nombre premier, et q une puissance de p.

Pour que les algorithmes précédents soient sûrs, il faut vérifier que le logarithme discret est effectivement difficile à calculer. On se place dans un groupe $G = \langle g \rangle$ générique, c'est à dire un groupe où l'on utilisera que les opérations suivantes :
- Calculer ab et a^{-1} si l'on se donne $a, b \in G$.
- Tester si $a = b$.
- On suppose que l'on a une bonne représentation informatique de G, c'est à dire en gros que l'on peut trier/hacher/chercher efficacement des éléments dans G.

On se demande alors combien de calculs un attaquant doit faire s'il veut espérer trouver x à partir de g^x. Soit N l'ordre de G. L'algorithme trivial donne un algorithme d'inversion en $O(N)$[2] opérations. On peut toutefois faire un peu mieux en utilisant une méthode de type « diviser pour régner ».

Algorithme 9 (Pas de bébés, pas de géants): *Soit $u \approx \sqrt{N} \in \mathbf{N}$. On écrit x en base u : $x = x_0 + x_1 u$. Alors $hg^{-x_0} = (g^u)^{x_1}$. Ainsi on construit la liste $\{h, hg^-1, \ldots, hg^{-u}\}$ et on calcule $g^u, (g^u)^2, \ldots, (g^u)^u$ jusqu'à tomber sur un élément de la liste.*

L'algorithme à un coût en complexité en $O(\sqrt{N})$ et en mémoire en $O(\sqrt{N})$, ainsi on a cassé le problème de taille N en $\sqrt{N}$ problèmes de tailles $\sqrt{N}$.

[1] En pratique pour la signature on remplace m par un hachage de m

[2] Comme les algorithmes qu'on va présenter dans cette partie sont typiquement exponentiels ou sous-exponentiels (en $\log(N)$), on omettra les polynômes en $\log(N)$ dans les $O(.)$.

Ensuite, le théorème des restes chinois conjugué à un lemme de Hensel trivial permettent de se ramener à un nombre premier divisant N.

Algorithme 10 (Pohlig-Hellmann): *Soit $N = \prod p_i^{e_i}$ la décomposition de N en facteurs premiers. Par les restes chinois, il suffit de trouver $x \mod p_i^{e_i}$. On écrit alors $x = x_0 + px_1 + \cdots + x_{e-1}p^{e-1}$. Soit $\beta = g^{N/p}$. Alors $x_0 = \log_\beta(h^{N/p})$ (car $h^{N/p} = \beta^x = \beta^{x_0}$ puisque β est d'ordre p , $x_1 = \log_\beta (hg^{-x_0})^{N/p^2}$, ...*

Ainsi le problème du logarithme discret en taille N est de l'ordre de grandeur du problème du logarithme discret en taille p, où p est le plus grand nombre premier divisant N.

Enfin on peut se passer du coût en mémoire de $O(\sqrt{N})$ de l'algorithme « Pas de bébés, pas de géants » en adaptant la méthode ρ pour la factorisation d'un entier :

Algorithme 11 (Algorithme ρ de Pollard): *On choisit une fonction de hachage $H : \langle(\rangle G) \to [1;20]$, et des éléments $m_k = g^{\alpha_k}h^{\beta_k}$, $k \in [1;20]$ où les α_k, β_k sont choisis au hasard.*

On choisit a_0, b_0 au hasard et on calcule $s_0 = g^{a_0}h^{b_0}$. Puis on définit $s_{i+1} = s_i m_{H(s_i)}$, $a_{i+1} = a_i + \alpha_{H(s_i)}$ et $b_{i+1} = b_i + \beta_{H(s_i)}$.

On itère jusqu'à trouver une collision $s_i = s_j$, on a alors $h = g^{\frac{a_i - a_j}{b_i - b_j}}$ ce qui nous donne x sous réserve que $b_i \neq b_j$ (mais ce cas a une probabilité $1/N$ donc très faible de se produire). Le paradoxe des anniversaires montre que i et j sont en $O(\sqrt{N})$. Et on peut ne garder qu'un élément sur 2^k, quitte à itérer un peu plus (c'est à dire remplacer i par la plus petite puissance de deux qui le contient).

D'où un coût en $O(\sqrt{N})$ et essentiellement nul en mémoire.

Théorème 12: *Dans un groupe générique, l'algorithme ρ combiné à l'algorithme de Pohlig-Hellmann est à peu près optimal.*

Le graal de la cryptographie est donc de trouver des groupes suffisamment génériques pour que l'on ait pas d'autres moyens que les algorithmes précédents pour calculer un logarithme discret. Bien évidemment, le problème du logarithme discret étant *NP*, on ne peut espérer prouver qu'une famille de groupe est suffisamment générique (sous peine de prouver que $P \neq NP$).

Un exemple de groupe qui ne convient pas du tout est le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$, puisque le logarithme discret revient à calculer l'inverse par la loi multiplicative de x par g, ce qui se fait par un algorithme d'Euclide étendu et est très rapide (polynomial en $\log(n)$).

Le groupe $(\mathbf{Z}/p\mathbf{Z})^\star$, avec g un générateur de ce groupe, semble plus robuste et les premières applications du logarithme discret se faisaient dans ce groupe. Cependant en adaptant les idées du crible quadratique utilisée pour la factorisation on a des attaques plus efficaces. L'idée est de calculer des éléments g^r (que l'on voit dans $\mathbf{Z}$), de regarder ceux qui sont divisibles par des petits nombres premiers q_i (on dit que ce sont des nombres friables). Une fois que l'on a suffisamment de relations, on utilise de l'algèbre linéaire (avec des matrices très creuses) pour trouver les $\log(q_i)$. Enfin on prends des r au hasard jusqu'à ce que $h.g^r$ soit friable, ce qui permet de trouver le logarithme de h. Le coût de cet algorithme est $L_p(1/2, \sqrt{2})$ où $L_N(\alpha, C) = \exp(C(\log N)^\alpha(\log\log N)^{1-\alpha})$.

On peut même faire encore mieux en adaptant le crible algébrique : dans $(\mathbf{Z}/p\mathbf{Z})^\star$ on aboutit à des algorithems pour le logarithme discret en $L_p(1/3, (64/9)^{1/3})$.

Actuellement, on utilise du logarithme discret dans des courbes elliptiques.

2 Courbes elliptiques

Soit k un corps algébriquement clos de caractéristique différente de 2. On se place dans le plan affine $\mathbf{A}^2(k) = \operatorname{Spec} k[x,y]$ et on considère un polynôme $f \in k[x]$ de degré 3 ayant des racines distinctes. On peut supposer que f est de la forme $f(x) = x^3 + ax + b$. Alors $\operatorname{Var}(y^2 - f(x))$ est une courbe lisse, on dit que c'est une courbe elliptique $\mathcal{C}$. La cloture de $\mathcal{C}$ dans $\mathbf{P}^2_k = \operatorname{Proj} k[x,y,z]$ (que l'on notera toujours $\mathcal{C}$) consiste à rajouter le point à l'infini $P_0 = (0,1,0)$.

2.1 Loi de groupe sur les points d'une courbe elliptique

L'intérêt des courbes elliptiques est que l'on peut définir une loi de groupes sur ses points rationnels.

Théorème 13 (Bézout): *Soit $\mathcal{C}_1$ et $\mathcal{C}_2$ deux courbes de degrés s et t dans $\mathbf{P}^2_k$, sans composantes irréductibles communes. Alors elles s'intersectent en st points, avec multiplicités.*

Maintenant une courbe elliptique est de degré 3, et deux points P_1 et P_2 sur la courbe donnent lieu à une droite L (qui n'est autre que la tangente à la courbe en P_1 si $P_1 = P_2$). L intersecte $\mathcal{C}$ en exactement un autre point P_3 par Bézout (car si $P_1 = P_2$ la multiplicité de l'intersection de $L \bigcap \mathcal{C}$ en P_1 est au moins 2), qui peut être égal à P_1 ou P_2. Si $P = (x : y : z)$ est un point de $\mathcal{C}$, on définit un point $-P$ sur la courbe par $-P := (x : -y : z) \in \mathcal{C}$. On définit alors la loi de groupe sur $\mathcal{C}(k)$ par $P_1 + P_2 := -P_3$.

On vérifie que si P est un point de la courbe, comme la ligne qui passe par P et P_0 est la ligne verticale passant par P, elle intersecte la courbe en $-P$, donc $P + P_0 = P$, P_0 est l'élément neutre (c'est vrai aussi si $P = P_0$ car P_0 est un point d'inflexion, et si $P = -P$ car alors la droite verticale est tangente à $\mathcal{C}$ en P). Comme la ligne qui passe par P et $-P$ est verticale, elle passe par P_0 d'où $P + -P = -P_0 = P_0$, donc $-P$ est bien l'inverse de P pour cette loi additive et on a bien un groupe.

Le point délicat que j'ai soigneusement omis de signaler est la vérification de l'associativité. On l'obtiendra plus tard lorsqu'on présentera une autre méthode pour construire le groupe associé à une courbe elliptique.

2.2 Loi de groupe induite sur les points rationnels de la courbe

Pour les besoins cryptographiques, $\mathcal{C}(k)$ étant un groupe infini ne peut convenir. On se ramène à un groupe fini de la manière suivante : on part d'un corps fini $\mathbf{F}_q$ et d'un polynôme f défini sur $\mathbf{F}_q$. Si on considère la courbe sur $\overline{\mathbf{F}}_q$ on peut regarder ses points rationnels $\mathcal{C}(\mathbf{F}_q)$[1].

Il faut vérifier que $\mathcal{C}(\mathbf{F}_q)$ est un sous-groupe fini de $\mathcal{C}(\overline{\mathbf{F}}_q)$. La finitude est claire puisque $\mathbf{P}^2_{\mathbf{F}_q}$ est de cardinal fini. Mais si $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ sont dans $\mathcal{C}(k)$, un calcul explicite (si P_1 et P_2 ne sont pas à l'infini et que $P_1 \neq -P_2$) montre que $P_1 + P_2 = P_3$ où $P_3 = (x_3, y_3)$ avec

[1]Schématiquement, si $\mathcal{C}$ est le schéma défini par $y^2 - f$, regarder la courbe sur $\overline{\mathbf{F}}_q$ revient à considérer le schéma $\overline{\mathcal{C}} := \mathcal{C} \otimes \overline{\mathbf{F}}_q$, et l'on a alors $\overline{\mathcal{C}}^{\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)} = \mathcal{C}$. Les points de $\mathcal{C}$ sont donc en bijection avec les orbites de points dans $\overline{\mathcal{C}}$.

$$x_3 = -x_1 - x_2 - \frac{b}{a} + \frac{1}{a}m^2 \tag{1}$$

$$y_3 = -y_1 + m(x_1 - x_3) \tag{2}$$

où

$$m = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{si } P_1 \neq P_2 \\ f'(x_1)/2y_1 & \text{si } P_1 = P_2 \end{cases} \tag{3}$$

Ce qui montre bien que la somme de deux points rationnels est rationnel (ce qui est d'ailleurs évident géométriquement, trouver l'intersection de la ligne (de degré 1) passant par P_1 et P_2 avec f (de degré 3) revient à calculer les racines d'un polynôme de degré 3. Si ce polynôme a deux racines rationnelles, il en va de même pour sa troisième racine).

3 Jacobienne d'une courbe

On aimerait pouvoir généraliser la construction à une courbe $\mathcal{C}$ lisse projective irréductible quelconque. Le problème c'est que si on prend deux points sur la courbe, la ligne qui les rejoint intersecte la courbe en $d-2$ autres points (avec multiplicités), où d est le degré de la courbe, par le Théorème 13.

Mais si l'on réfléchit à la construction qu'on a effectuée pour les courbes elliptiques, on dit que $P_1 + P_2 + P_3 = 0$ si et seulement si ils sont alignés. On va appliquer le même genre d'idées pour la courbe en disant qu'une somme de points est nulle si et seulement si il y a une ligne passant par ces points avec la bonne multiplicité, sauf qu'en fait pour obtenir des relations intéressantes on va remplacer les intersections de la courbe avec une ligne par n'importe quelle intersection de la courbe avec une de ses fonctions rationnelles.

3.1 Diviseurs de Weil sur une courbe

À partir de maintenant on emploie le mot courbe pour définir une variété projective irréductible lisse de dimension 1 sur un corps algébriquement clos k.

Définition 14: Un diviseur D sur $\mathcal{C}$ est une somme formelle de points de $\mathcal{C}$

$$D = \sum_{x \in \mathcal{C}} n_x x$$

où les $n_x \in \mathbf{Z}$ sont presque tous nuls. Le support de D est l'ensemble des $x \in \mathcal{C}$ tels que $n_x \neq 0$. On note $\mathrm{Div}(\mathcal{C})$ l'ensemble des diviseurs de $\mathcal{C}$, c'est le groupe abélien libre engendré par les points de $\mathcal{C}$. Un diviseur D est dit effectif si $n_x \geqslant 0$ pour tout $x \in \mathcal{C}$, on notera $D_1 \geqslant D_2$ lorsque $D_1 - D_2$ est effectif. Enfin on a un épimorphisme $\deg : \mathrm{Div}(\mathcal{C}) \to \mathbf{Z}$ en associant à un diviseur $D = \sum n_x x$, $\deg(D) = \sum n_x$.

À une fraction rationnelle $h \in K(X)$, on peut associer un diviseur de la manière suivante : si P est un point de la courbe, l'anneau $\mathcal{O}_P$ des germes en P est un anneau local régulier, donc factoriel, de dimension 1, c'est donc un anneau de valuation discrète, et l'on notera v_P la valuation associée sur $K(X)$. Si f est une fraction rationnelle, alors $v_P(f) \geqslant 0$, signifie que

f est définie au voisinage de P. Si $v_P(f) = 0$, f ne s'annule pas en P, sinon on dit que f a un zéro d'ordre $v_P(f)$ en P. Enfin si $v_P(f) < 0$ on dit que f a un pôle d'ordre $-v_P(f)$ en P. On définit alors le diviseur (f) associé à f par $(f) = \sum v_P(f).P$. On dit que (f) est un diviseur principal.

(f) est bien un diviseur, en effet f est régulière sur un ouvert U de X, or $X \setminus U$ est fini (car de dimension 0) donc ne fait intervenir qu'un nombre fini de points, et les zéros de f sont dans l'idéal définit par l'idéal de f, donc sont également en nombres finis, qui est fermé, donc fini.

Lemme 15: *(f) est de degré 0.*

Démonstration: Voir [Har] pour les détails. Si $f \in K(X)^\star$, l'inclusion $k(f) \subset k(X)$ induit un morphisme birationnel $\varphi : X \mapsto \mathbf{P}^1_k$, qui s'étend en un morphisme fini de $X \mapsto \mathbf{P}^1_k$ car X est projectif. (f) correspond au tiré en arrière du diviseur $(x) = (0) - (\infty)$ dans $\mathbf{P}^1_k$, et est donc de degré 0. ■

3.2 Groupe de Picard

En suivant les idées du début de la partie, on va dire qu'une somme de diviseur est (formellement) nulle s'il est le lieu des zéros (avec multiplicités et en comptant les pôles) d'une fonction rationnelle de $\mathcal{C}$.

Définition 16: On vérifie facilement que $f \mapsto (f)$ est un morphisme de $\mathrm{K}(X)^\star$ sur $\mathrm{Div}(\mathcal{C})$. On notera $\mathrm{PDiv}(\mathcal{C})$ l'image par ce morphisme. Le groupe de Picard de $\mathcal{C}$ est le groupe $\mathrm{Pic}(\mathcal{C})$ quotient de $\mathrm{Div}(\mathcal{C})$ par $\mathrm{PDiv}(\mathcal{C})$. Si D est D' ont la même image dans $\mathrm{Pic}(\mathcal{C})$, on dit qu'ils sont linéairement équivalents, et l'on note $D \sim D'$. Le Lemme 15 montre que l'application degré se factorise par $\mathrm{Pic}(\mathcal{C})$.

Remarque 17: Le groupe de Picard est infini, si D est un diviseur de degré non nul, les $nD, n \in \mathbf{Z}$ sont distincts car de degrés distincts.

Définition 18: La jacobienne d'une courbe $\mathcal{C}$ est le sous-groupe des éléments de degrés 0 dans le groupe de Picard de $\mathcal{C}$.

On a ainsi associé à toute courbe un groupe $\mathrm{Jac}(\mathcal{C})$. Il reste à vérifier que la jacobienne d'une courbe elliptique correspond aux points de la courbe elle même, et que la jacobienne d'une courbe sur un corps fini donne bien lieu à un groupe fini. Pour cela il faut d'abord définir ce qu'on appelle la jacobienne d'une courbe sur un corps non algébriquement clos, où plutôt comment définir les points k-rationnels d'une Jacobienne.

Définition 19: Soit k un corps parfait, et $\mathcal{C}$ une courbe définie sur k. On peut la regarder sur $\overline{k}$ et parler de sa jacobienne dans $\overline{k}$. Soit G le groupe de Galois de $\overline{k}/k$. Alors G agit sur $\mathcal{C}$ puisque $\mathcal{C}$ est définie sur k (et donc $G.\mathcal{C} = \mathcal{C}$ dans $\mathbf{A}^{\overline{k}}_2$). De plus l'image d'un diviseur principal (f) par $g \in G$ est le diviseur principal $(g.f)$. Donc le quotient induit une action naturelle de G sur $\mathrm{Pic}(\mathcal{C})$.

On dit alors qu'un élément du groupe de Picard de $\mathcal{C}$ est rationnel s'il est invariant par G, et on note $\mathrm{Jac}(\mathcal{C})(k)$ l'ensemble des éléments k-rationnels de la Jacobienne.

Remarque 20: Si l'on voit la variété $\mathcal{C}$ comme un schéma X, regarder $\mathcal{C}$ sur $\overline{k}$ revient à considérer $\overline{X} = \mathcal{C}(X) \otimes_k \overline{k}$. Les points de X correspondant à des orbites sour G de points de $\overline{X}$ on voit que $\mathrm{Div}(X) = \mathrm{Div}(\overline{X})^G$.

De plus si D est un diviseur dans X qui devient principal dans $\overline{X}$, alors D est principal dans X. En effet on note $D = (f)$ dans $\overline{X}$, D est invariant par G donc $(g.f) \sim (f)$. Donc la fonction rationnelle $g.f/f$ est dans $\Gamma(\overline{X}, \overline{k}[X]^\star)$ car le schéma étant intègre et lisse de dimension 1 est normal, or un anneau normal est égal à l'intersection de ses localisés en ses idéaux premiers de codimension 1. Mais $\Gamma(\overline{X}, \overline{k}[X]^\star) = \overline{k}^\star$ car $\overline{X}$ est propre. Donc quitte à remplacer f par un multiple, on peut supposer qu'elle est invariante par l'action du groupe de Galois, donc provient d'une fonction dans $X = \overline{X}^G$.

Cependant, on n'a pas $\mathrm{Pic}(\overline{X})^G = \mathrm{Pic}(X)$ en général. En effet on a la suite exacte $0 \mapsto \mathrm{PDiv}(\overline{X}) \mapsto \mathrm{Div}(\overline{X}) \mapsto \mathrm{Pic}(\overline{X}) \mapsto 0$ et si on lui applique le foncteur exact à gauche on a la début de la longue suite exacte de cohomologie correspondante : $0 \mapsto \mathrm{PDiv}(\overline{X}) = \mathrm{PDiv}(\overline{X})^G \mapsto \mathrm{Jac}(X) = \mathrm{Jac}(\overline{X})^G \mapsto \mathrm{Pic}(\overline{X})^G$ mais il peut y avoir des H^1 ensuite.

Il n'est pas clair que $\mathrm{Jac}(\mathcal{C})(k)$ soit un groupe fini si $k = \mathbf{F}_q$ est un corps fini. On verra plus tard que c'est effectivement le cas.

3.3 Fibrés en droite sur une courbe $\mathcal{C}$

On rappelle que se donner un fibré en droite sur $\mathcal{C}$ revient au même que se donner un faisceau de modules inversible.

Si $D = \sum n_P P$ est un diviseur effectif de $\mathcal{C}$ il définit un sous-schéma $\mathrm{Spec} \prod_{P \in \mathcal{C}} \mathcal{O}_{\mathcal{C},P}/P^{n_P}$ fermé fini de $\mathcal{C}$. Ce schéma fermé est défini par un faisceau quasi-cohérent d'idéaux de $\mathcal{O}$ que l'on note $\mathcal{O}(-D)$.

Par définition, les sections de $\mathcal{O}(-D)$ sur un ouvert U de $\mathcal{C}$ sont

$$\Gamma(U, \mathcal{O}(-D)) = \{f \in k[U], v_P(f) \geqslant n_P \text{ pout tout } P \in U\} \tag{4}$$
$$= \{f \in \mathrm{K}(\mathcal{C}), v_P(f) \geqslant n_P \text{ pout tout } P \in U\} \tag{5}$$

L'égalité à lieu puisque les v_P étant positifs, une fonction rationnelle dans la section est en fait définie sur U.

Ceci conduit à poser pour n'importe quel diviseur D.

$$\Gamma(U, \mathcal{O}(-D)) = \{f \in \mathrm{K}(\mathcal{C}), v_P(f) \geqslant -n_P \text{ pout tout } P \in U\} \tag{6}$$

$\mathcal{O}(-D)$ est un sous-faisceau quasi-cohérent de $\mathrm{K}(\mathcal{C})$. Son localisé en $P \in \mathbf{C}$ n'est autre que $\pi_P^{-n_P}\mathcal{O}_P$ où π_P est une uniformisante de l'anneau de valuation discrète $\mathcal{O}_P$, il est donc localement inversible.

Réciproquement, tout sous-faisceau de module M de $\mathrm{K}(\mathcal{C})$ est inversible et provient d'un diviseur, car si U est un ouvert affine, $A = \mathcal{O}_{\mathcal{C}}(U)$ est un anneau de Dedekind, donc $M(U)$ s'écrit comme un produit libre d'idéaux premiers dans A. Autrement dit $M(U)$ correspond sur U au faisceau associé à un diviseur restreint à U. On peut recoller les diviseurs sur un recouvrement ouvert de $\mathcal{C}$ car la décomposition d'un idéal fractionnaire en facteurs premiers sur un anneau de Dedekind est unique.

Donc on a obtenu une correspondance bijective entre diviseurs de $\mathcal{C}$ et sous-modules inversibles de $\mathrm{K}(\mathcal{C})$, cette correspondance envoie un diviseur principal (f) sur $f\mathcal{O}_{\mathcal{C}}$.

Or tout module inversible sur $\mathcal{C}$ est isomorphe à un sous-module inversible de $\mathrm{K}(\mathcal{C})$ et deux sous-modules inversibles de $\mathrm{K}(\mathcal{C})$ sont isomorphes si et seulement si ils différent par une fonction rationnelle. Autrement dit, l'identification canonique précédente donne lieu à une identification des modules inversibles à isomorphisme près au groupe $\mathrm{Pic}(\mathcal{C})$. Cet isomorphisme est compatible avec les lois de groupe sur $\mathrm{Pic}(\mathcal{C})$ et sur les modules inversibles (où la loi est donnée par le produit tensoriel). Autrement dit ce qu'on appelle usuellement le groupe de Picard correspond bien au groupe ici défini.

Si l'on revient à la définition, on voit que $\Gamma(\mathcal{C}, \mathcal{O}(D)$ est l'ensemble des fonctions rationnelles dont la multiplicité en P est plus grande que $-n_P$, autrement dit c'est l'ensemble des fonctions rationnelles telles que $(f) + D \geqslant 0$. Comme deux diviseurs principaux (f) et (g) sont égaux si et seulement si ils diffèrent d'un élément de $\Gamma(\mathcal{C}, \mathcal{O}_{\mathcal{C}}^{\star}) = k^{\star}$, on voit que le nombre de diviseurs effectifs linéairement équivalents à D a pour dimension $\dim_k \Gamma(\mathcal{C}, \mathcal{O}(D)) - 1 := l(D) - 1$. On notera $|D|$ l'ensemble des diviseurs effectifs linéairement équivalents à D.

En particulier si $l(D) \neq 0$ (i.e. le faisceau associé à D a des sections globales) alors D est équivalent à un diviseur effectif, donc $\deg D \geqslant 0$ (car deux diviseurs équivalents ont le même degré). Si de plus $\deg(D) = 0$, D est équivalent à (1) le seul diviseur de degré 0 effectif.

Connaître $l(D)$ nous aiderait donc pour trouver le nombre de manière que l'on a pour représenter un point de la Jacobienne. C'est l'objet du théorème de Riemann-Roch.

3.4 Riemann-Roch

Soit $\mathcal{C}$ une courbe. Le genre arithmétique de $\mathcal{C}$ est par définition $p_a(\mathcal{C}) = \dim_k H^1(\mathcal{C}, \mathcal{O}_{\mathcal{C}})$. Il coincide avec le genre géométrique[1] $p_g(\mathcal{C})$ car $\mathcal{C}$ est supposé lisse. On notera ce nombre g et on l'appellera genre de $\mathcal{C}$.

Exemple 21: Les courbes elliptiques sont les courbes de genre 1. En effet pour une courbe lisse définie par un polynôme homogène de degré d, le genre de la courbe est $g = (d-1)/2$

Si $k = \mathbf{C}$, le genre de $\mathcal{C}$ est simplement son genre vu comme surface différentielle réelle, c'est à dire son nombre de « trous ».

Théorème 22 (Riemann-Roch):

(i) Si D est un diviseur de $\mathcal{C}$, alors $\dim_k H^0(\mathcal{C}, \mathcal{O}_D) - \dim_k H^1(\mathcal{C}, \mathcal{O}_D) = \deg D + 1 - g$

(ii) Il existe un diviseur positif K sur $\mathcal{C}$ de degré $2g-2$ tel que pour tout diviseur D, $H^1(\mathcal{C}, \mathcal{O}_D)$ est isomorphe à $H^0(\mathcal{C}, \mathcal{O}(K-D))$.

En combinant ce qui précède, on obtient

$$l(D) - l(K - D) = \deg D + 1 - g$$

Ceci permet de monter que pour une courbe elliptique $\mathcal{C}$, il y a bijection entre la jacobienne de $\mathcal{C}$ et les points de la courbe. En effet si on choisit un point P_0 de $\mathcal{C}$ (typiquement on prend le point à l'infini), on a un morphisme de $\mathcal{C}(k) \to \mathrm{Jac}(\mathcal{C}(k))$ en envoyant P sur la classe de $P - P_0$. Pour monter qu'on a un isomorphisme, il suffit de montrer que si D est un diviseur de 0, il existe un unique point $P \in \mathcal{C}(k)$ tel que $D \sim P - P_0$ On applique Riemann-Roch à $D + P_0$ et on obtient

$$l(D + P_0) - l(K - D - P_0) = 1 + 1 - 1$$

[1] Que l'on peut définir comme le genre arithmétique d'une courbe lisse birationnelle à $\mathcal{C}$

Mais $degK = 2g-2 = 0$, donc $deg(K-D-P_0) = -1$ et $l(K-D-P_0) = 0$. Donc $l(D+P_0) = 1$, et $\dim_k |D + P_0| = 0$. Il y a donc un unique diviseur effectif P équivalent à $D + P_0$, il est de degré 1 donc c'est un point.

On va montrer sur un exemple comment fonctionne en pratique la correspondance (c'est à dire on va la montrer sans passer par Riemann-Roch), ce qui nous permettra au passage de vérifier que les deux lois de groupes coincident bien.

Soit donc $\mathcal{C}$ la courbe elliptique donnée par $y^2 = x^3 - x$ (ou $zy^2 = x^3 - xz^2$ en projectif). $\mathcal{C}$ est une sous-variété fermée de $\mathbf{P}^2_k$. Si $\mathcal{L}$ est un faisceau inversible sur $\mathbf{P}^2_k$, son tiré en arrière sur $\mathcal{C}$ est également inversible, et deux faisceaux inversibles isomorphes restent isomorphes quand on tire en arrière. En gardant à l'esprit la seconde caractérisation du groupe de Picard, on voit qu'on a définit un morphisme de $\mathrm{Pic}(\mathbf{P}^2_k) \mapsto \mathrm{Pic}(\mathcal{C})$.

Notons $P_0 = (0, 1, 0)$ le point infini. C'est un point d'inflexion, donc la ligne $z = 0$ rencontre la courbe en le diviseur $3P_0$. Si on prend une ligne quelconque qui rencontre la courbe en le diviseur $D = P + Q + R$ (avec multiplicités), comme deux lignes définissent le même diviseur dans $\mathrm{Pic}(\mathbf{P}^2_k)$, il en va de même de leur tiré en arrière qui n'est autre que le diviseur qu'elles définissent sur leur intersection avec $\mathcal{C}$. Ainsi $P+Q+R \sim 3P_0$, soit $P-P_0+Q-P_0+R-P_0 \sim 0$, on retrouve bien la loi de groupe issue des points de la courbe.

On peut vérifier élémentairement que $P \mapsto P - P_0$ donne bien une bijection de $\mathcal{C}(k)$ sur $\mathrm{Jac}(\mathcal{C})$. En effet, si $P - P_0 \sim Q - Q_0$, alors $P \sim Q$ mais il est connu que si deux points sur une courbe sont linéairement équivalents, la courbe est rationnelle (c'est à dire birationnelle à $\mathbf{P}^1_k$), donc de genre 0. Enfin pour la surjectivité, si D est un diviseur de degré 0, on peut l'écrire $D = \sum n_i(P_i - P_0)$, si l'un des n_i est négatif, en remplaçant P_i par son symétrique Q_i par rapport à l'axe des x, on peut se ramener à n_i positif (puisque $P_0 + P_i + Q_i \sim 3P_0$). Enfin, si les n_i sont positifs et qu'il y en a deux non nuls, correspondant à P et Q, alors la droite passant par P et Q intersecte $\mathcal{C}$ en un troisième point R et l'on a $P + Q + R \sim 3P_0$, soit $(P - P_0) + (Q - Q_0) \sim (T - T_0)$ et par un nombre fini d'étapes on se ramène à un diviseur de la forme $P - P_0$.

3.5 La variété jacobienne

On a vu que la Jacobienne d'une courbe est un groupe. En fait on peut montrer qu'elle est représentée par un schéma en groupe, i.e. il existe une variété projective sur k dont les points correspondent aux éléments de la Jacobienne et telle que la loi de groupe sur les points induite par la structure de groupe sur la Jacobienne est algébrique.

Plus précisément, soit X une courbe. Si T est un schéma sur k, on définit $\mathrm{Pic}^0(X \times T)$ comme étant le sous-groupe de $\mathrm{Pic}(X \times T)$ des faisceaux inversibles dont la restriction à chaque fibre X_t est de degré 0. On note $\mathrm{Pic}^0(X/T)$ le quotient de $\mathrm{Pic}^0(X \times T)$ par les faisceaux inversibles sur T tirés en arrière sur $X \times T$. On peut voir $\mathrm{Pic}^0(X/T)$ comme des familles de faisceaux inversibles de degrés 0 sur X paramétrées par T.

Alors le foncteur $Pic^0(X/T)$ est représentable par un schéma J de type fini sur k. C'est à dire qu'on a un élément $\mathcal{L} \in \mathrm{Pic}^0(X/J)$ tel que pour tout schéma T de type fini sur k et $\mathcal{M} \in \mathrm{Pic}^0(X/T)$ il existe un unique morphisme $f : T \mapsto J$ tel que $\mathcal{M} = f^\star\mathcal{L}$.

La propriété universelle de J montre que ses points fermés sont en bijections avec $\mathrm{Pic}^0(X)$, que J est un schéma en groupe, qu'elle est propre sur k (donc projective), lisse et de dimension g (son espace tangent en 0 étant $H^1(X, \mathcal{O}_X)$).

En particulier, si $k = \overline{\mathbf{F}}_q$, on voit que les points $\mathbf{F}_q$ rationnels de la jacobienne sont en

nombre fini.

4 Algorithmes de comptage de points

Pour toute courbe $\mathcal{C}$ définie sur un corps $\mathbf{F}_q$ (lisse, projective, ...) on sait construire un groupe associé $\mathrm{Jac}(\mathcal{C})$, qui est fini si on regarde ses points sur $\mathbf{F}_q$ (ou une extension finie de $\mathbf{F}_q$).

On espère que ce groupe a de bonnes propriétés cryptographiques en terme de logarithme discret. Une condition indispensable pour cela est que le groupe soit divisible par un grand nombre premier (voir l'algorithme de Pohlig-Hellmann). Pour le vérifier il nous faut donc calculer son cardinal. On va voir que cela revient au même que de calculer le nombre de points sur la courbe directement, au moins en genre $g \leqslant 2$.

4.1 Fonction zêta

On note N_k le nombre de points $\mathbf{F}_q^k$ rationnels de $\mathcal{C}$. La fonction zêta de $\mathcal{C}$ est alors

$$Z(t) = \exp\left(\sum_{k \geqslant 1} N_k \frac{t^k}{k}\right)$$

Les conjectures de Weil nous disent que

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)}$$

où $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$ est un polynôme de degré $2g$ vérifiant $a_0 = 1$, $a_{2g} = q^g$ et $a_{2g-i} = q^{g-i} a_i$ pour $0 \leqslant i \leqslant g$ et tel que les inverses de ses racines sont de module $\sqrt{(}q)$. En particulier $|a_i| \leqslant \binom{2g}{i} q^{i/2}$.

$\mathrm{Jac}(\mathcal{C})$ étant définie sur $\mathbf{F}_q$, le morphisme de Frobenius $x \mapsto x^q$ laisse stable $\mathrm{Jac}(\mathcal{C})$. Il se trouve que son polynôme caractéristique χ_π est le polynôme réciproque de L. On en déduit que le nombre de $\mathbf{F}_q$ points dans la jacobienne (égal à $\chi_\pi(1)$ se déduit de $Z(t)$. Réciproquement, si l'on connaît $\chi_\pi(1)$ et que le genre est $\leqslant 2$, la forme des coefficients de L permet de retrouver Z.

4.2 L'algorithme de Schoof

Soit A une variété abélienne de dimension g définie sur $\mathbf{F}_q$ pour laquelle on cherche à calculer le polynôme caractéristique χ_π du Frobenius.

Soit l un nombre premier différent de la caractéristique p de k. Alors le groupe des points de l-torsion de A, que l'on note $A[l]$ a une structure de $\mathbf{Z}/l\mathbf{Z}$-espace vectoriel de dimension $2g$, sur lequel le Frobenius agit de manières $\mathbf{Z}/l\mathbf{Z}$ linéaire. Le polynôme caractéristique de cette restriction de l'endomorphisme de Frobenius est alors $\chi_\pi(t) \mod l$.

L'algorithme de Schoof consiste à étudier l'action du Frobenius sur les points de l-torsion pour suffisamment de l de manière à déduire χ_π par restes chinois. Le plus grand coefficient de χ_π a un nombre de chiffres de l'ordre de $O(g \log q)$, il nous faut donc considérer environ $O(g \log q)$ nombres premiers l de taille $O(g \log q)$.

Le problème principal vient du fait que l'on ne sait pas a priori exhiber la structure de $\mathbf{Z}/l\mathbf{Z}$-espace vectoriel de $A[l]$, ce qui oblige à travailler sur tous les points de $A[l]$ (soit l^{2g} points) au lieu d'une base.

Décrire ces l^{2g} points nécessite un polynôme $f(X)$ de degré au moins l^{2g}, donc de taille environ $l^{2g}\log q$. Pour trouver le polynôme caractéristique de l'action de π, il nous faut calculer l'action de π sur les points de $A[l]$ ce qui se traduit par un calcul de type $X^q \mod f(X)$. Ceci nous coûte $O(\log q\,\mathrm{M}(l^{2g}\log q)$ où $\mathrm{M}(n)$ représente le temps de calcul nécessaire pour calculer le produit de deux polynômes de degré n, $\mathrm{M}(n) = O(n\log n\log\log n)$ si l'on utilise une transformée de Fourrier rapide. Il reste aussi à faire un peu d'algèbre linéaire pour trouver le polynôme caractéristique, mais on peut la négliger par rapport aux autres opérations.

Au final on s'attend à faire cette étape en $O(l^{2g}\log^2 q)$ opérations au mieux (en négligeant certains termes en $\log\log$), avec l de taille $O(g\log q)$, et on doit répéter cette étape envirion $O(g\log q)$ fois. D'où un coût au mieux en $O(g^{1+2g}(\log q)^{2g+3})$.

Dans le cas des courbes elliptiques, l'algorithme de Schoof donne bien un algorithme en $O((\log q)^5)$, mais pour les courbes de genre 2, le meilleur algorithme que l'on connaît est en $O((\log q)^8)$ alors que l'on espérait du $O((\log q)^7)$. Cela vient de la difficulté à décrire efficacement $A[l]$.

Comme le coût exponentiel de l'algorithme vient de la grande taille de $A[l]$, on peut chercher à travailler dans un sous-espace de $A[l]$ de dimension inférieure qui permet quand même d'extraire de bonnes informations sur χ_π. C'est ce genre d'améliorations qu'ont apportées Atkin et Elkies à l'algorithme de Schoof dans le cas elliptique pour former l'algorithme SEA, qui est de complexité heuristique $O\left((\log q)^4\right)$.

Références

[CF] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* Lecture Note Series 230.

[Eis] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.*

[Gau] Pierrick Gaudry. Algorithmes de comptage de points d'une courbe définie sur un corps fini. Prépublication.

[Har] Robin Hartshorne. *Algebraic Geometry.*

[Kob] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms.* Second edition.

[Las] Yves Laszlo. Introduction à la géométrie algébrique. Polycopié de cours de M2.

[Ler97] Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis.* PhD thesis, École Polytechnique, 1997.

[Per] Daniel Perrin. *Géométrie Algébrique, une introduction.*