Crypto, $2^{ème}$ Semestre 2012/2012

INTRODUCTION AUX COURBES ELLIPTIQUES

Les courbes elliptiques

1. Introduction

Les courbes elliptiques sont à la base de cryptosystèmes, reposant sur la difficultés que problème du logarithme discret sur les groupes elliptiques.

2. Les courbes elliptiques sur les réels

La courbe elliptique réelle $C_{a,b}$ de paramètres a,b est l'ensemble des points $(x, y) \in \mathbb{R}^2$ qui satisfont l'équation :
$y^2 = x^3 + ax + b$, où a et b sont des nombres réels.
Par exemple, la figure ci-dessous représente la courbe elliptique $C_{-4,1}$ d'équation $y^2 = x^3 - 4x + 1$
Si $4a^3 + 27b^2 \neq 0$, alors la courbe elliptique $y^2 = x^3 + ax + b$ peut être utilisée pour former un groupe. Le groupe $(G, +)$ associé à la courbe elliptique réelle $C_{a,b}$ est constitué des points de la courbe elliptique $C_{a,b}$ complété d'un point spécial Ω appelé *point à l'infini*. Ce groupe est muni d'une addition que l'on va décrire maintenant.

2.1. **Description géométrique de l'addition.** L'addition de deux points comme l'opposé d'un point dans une courbe elliptique sont défini géométriquement. Commençons par l'opposé : l'opposé d'un point $P = (x_P, y_P)$ est son symétrique suivant l'axe des x, c'est à dire le point $-P$ de coordonnées $(x_P, -y_P)$. Notez que pour chaque point P sur une courbe elliptique, le point $-P$ est également sur la courbe.
Pour l'addition de P avec Q, on va commencer par supposer que P et Q sont deux points distincts sur la courbe elliptique, et que P est différent de $-Q$. Alors, on trace une ligne passant par les deux points P et Q. Cette ligne coupe la courbe elliptique en exactement un point de plus, R. On définit alors $P + Q = -R$.
Pour l'addition de P avec $-P$, si l'on garde la même stratégie, la droite passant par P et $-P$ ne coupe pas la courbe elliptique en un autre point, elle coupe la courbe au point à l'infini, on définit alors que $P + (-P) = \Omega$.

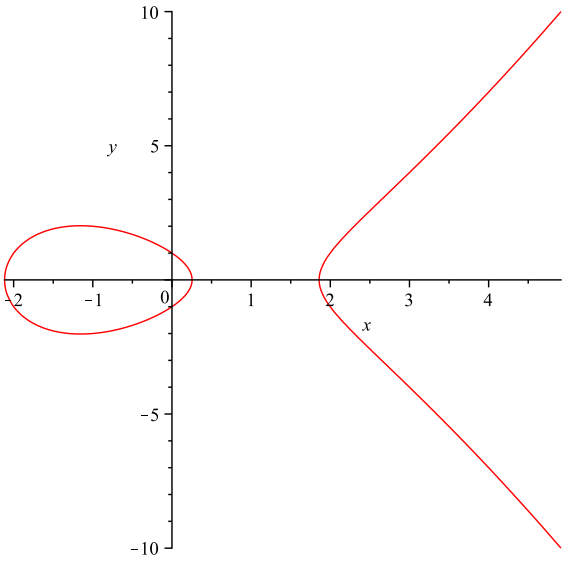

Figure 1. $y^2 = x^3 - 4x + 1$

Pour ajouter un point P à lui-même, on trace la tangente à la courbe au point P. Si y_P n'est pas nul, alors la tangente coupe la courbe elliptique en exactement un autre point R. On définit alors $P + P = -R$. Si $y_P = 0$, la tangent au point P est verticale et on pose $P + P = \Omega$

2.2. **Description arithmétique de l'addition.** Quand $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ ne sont symétriques l'un de l'autre par rapport à l'axe des x.
Alors $P + Q = S$ où
On calcul la pente de la droite passant par P et Q :

$$s = (y_P - y_Q)/(x_P - x_Q)$$

puis,

$$x_S = s^2 - x_P - x_Q \text{ et } y_S = -y_P + s(x_P - x_S).$$

Quand $y_P \neq 0$, alors $2P = S$ avec

$$s = (3x_P^2 + a)/(2y_P)$$

et

$$x_S = s^2 - 2x_P \text{ et } y_S = -y_P + s(x_P - x_S)$$