Université Bordeaux I – 2012/2013 — Courbes elliptiques
Master 1 Cryptologie et Sécurité Informatique — Yu. Bilu / J. Gillibert

Révisions de fin d'année

Exercice 1
Soit E la courbe elliptique définie sur $\mathbb{Q}$ par les coefficients

$$E = [1, 0, 1, 3857, 276806]$$

1. Quels sont les premiers de bonne réduction de E ?
2. Quel est le sous-groupe de torsion de $E(\mathbb{Q})$? Donner la liste explicite de ses éléments.
3. Engendrer aléatoirement des points sur $E(\mathbb{F}_{17^5})$. Calculer leur ordre en utilisant la méthode *baby-step giant-step*.
4. Soient $P = (221001, 233967)$ et $Q = (855901, 448685)$ deux points de E à coordonnées dans $\mathbb{F}_{1000003}$. Déterminer n tel que $nP = Q$ par la méthode *baby-step giant-step*, puis par la méthode rho de Pollard. Quelle méthode est la plus rapide ?
5. Expliquer pourquoi P et Q engendrent tous les deux le groupe $E(\mathbb{F}_{1000003})$.
6. Tester d'autres exemples de log discret.

Exercice 2
1. Montrer que le polynôme $X^4 + 1$ est réductible dans $\mathbb{F}_2[X]$.
2. Soit p un nombre premier impair. En remarquant que l'ordre de $\mathbb{F}_{p^2}^\times$ est un multiple de 8, montrer que le polynôme $X^4 + 1$ possède une racine dans $\mathbb{F}_{p^2}$. En déduire que $X^4 + 1$ est réductible dans $\mathbb{F}_p[X]$.
3. Montrer que le polynôme $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$.
4. Pari/gp peut-il nous aider à résoudre certaines de ces questions ?

Exercice 3
Soient p un nombre premier, et E une courbe elliptique définie sur $\mathbb{F}_p$. On rappelle que la trace du Frobenius de E sur $\mathbb{F}_p$, notée a_p, satisfait la propriété suivante :

$$\#E(\mathbb{F}_p) = p + 1 - a_p$$

Soient α et β les racines (complexes) du polynôme $T^2 - a_p T + p$. Le théorème de Weil affirme que

$$\#E(\mathbb{F}_{p^n}) = p^n + 1 - (\alpha^n + \beta^n).$$

1. En s'appuyant sur la fonction `ellap`, programmer une procédure `ellcard`(E, p, n) qui renvoie $\#E(\mathbb{F}_{p^n})$.
2. Soit la courbe elliptique sur $\mathbb{F}_2$ définie par l'équation

   $$y^2 + xy = x^3 + x^2 + 1$$

   déterminer le nombre de points de cette courbe sur $\mathbb{F}_{2^{42}}$.