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

Travail préparatoire au DS

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

$$E = [1, -1, 0, -167, 616]$$

1. Quel est le discriminant Δ de E ?

— Rappellons que l'on obtient, en réduisant l'équation de E modulo un premier p ne divisant pas Δ, une courbe elliptique sur $\mathbb{F}_p$, que l'on notera E_p dans tout le texte.

2. Soient $P = (-12, 34)$ et $Q = (24, 88)$. Vérifiez que P et Q sont sur la courbe E. Montrez que ce sont des points d'ordre infini dans le groupe $E(\mathbb{Q})$.

— Si p est un nombre premier ne divisant pas Δ, on note $\tilde{P}$ et $\tilde{Q}$ les points obtenus en réduisant modulo p les points P et Q. On note $\langle \tilde{P}, \tilde{Q} \rangle$ le sous-groupe de $E_p(\mathbb{F}_p)$ engendré par ces deux points.

3. Donner un exemple de nombre premier p pour lequel $\langle \tilde{P}, \tilde{Q} \rangle = E_p(\mathbb{F}_p)$.
4. Donner un exemple de nombre premier p pour lequel $\langle \tilde{P}, \tilde{Q} \rangle \neq E_p(\mathbb{F}_p)$.

Exercice 2
Soit G la courbe elliptique définie sur $\mathbb{F}_{211}$ par les coefficients

$$G = [0, -1, 0, 56, 108]$$

Soit $R(X)$ le polynôme donné par la commande `ffinit`$(211, 3)$, et soit t la classe de X modulo $R(X)$. On considère les points ci-dessous, à coordonnées dans $\mathbb{F}_{211^3}$

$$P = (83 * t^2 + 123 * t + 69, 165 * t^2 + 157 * t + 150)$$

$$Q = (25 * t^2 + 11 * t + 58, 122 * t^2 + 111 * t + 27)$$

1. Déterminer l'ordre de P.
2. On admet que Q appartient au groupe cyclique engendré par P. En utilisant l'algorithme de Shanks, trouver un entier n tel que $[n]P = Q$.

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 $T^2 - a_pT + p$. 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 $\mathbb{F}_{2^{42}}$.

Exercice 1 – Soit $p \geqslant 5$ un nombre premier et soit q une puissance de p. Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Soit m un entier strictement positif. On note $E[m]$ l'ensemble des points P de la courbe E qui vérifient $[m]P = 0$.

1) Donner un exemple de courbe sur $\mathbb{F}_7$ telle que $E[2]$ contient au moins deux points.

2) On s'intéresse à présent au cas particulier $m = p$. Regardons la courbe E définie sur $\mathbb{F}_{19}$ par l'équation affine $y^2 = x^3 + x$. Calculer $\mathrm{Card}(E(\mathbb{F}_{19}))$. Calculer $\mathrm{Card}(E[19])$.

Lorsqu'une courbe E définie sur $\mathbb{F}_p$ vérifie $\mathrm{Card}(E(\mathbb{F}_p)) = p+1$, on dit que c'est une courbe **supersingulière** en p.

Exercice 2 – On étudie dans cet exercice la notion de **courbe anormale**. Soit p un nombre premier. Une courbe elliptique E définie sur $\mathbb{F}_p$ est dite **anormale en** p si elle vérifie $\mathrm{Card}(E(\mathbb{F}_p)) = p$.

1) Quelle est la structure d'un groupe de cardinal p ? Que peut-on en déduire pour $E(\mathbb{F}_p)$?

2) Donner un exemple de courbe anormale pour $p = 23$.

Exercice 3 – On se propose dans cet exercice de calculer quelques logarithmes discrets.

1) Réviser les fonctions znlog, fflog. Terminer l'implémentation d'un calcul de log-discret sur une courbe elliptique (méthode de Pollard par exemple) et le tester sur des exemples sur $E(\mathbb{F}_{11^5})$.