Université Pierre et Marie Curie — 2009-2010
Certificat MM067 — Cryptologie, cryptographie algébrique

Examen du 16 avril 2010

Durée 3 heures

Les documents, calculatrices et téléphones portables sont interdits.

Les trois exercices sont indépendants.

Exercice 1

Les cinq questions sont indépendantes.

1) Soit K un corps de cardinal 4. Soit α un élément de K distinct de 0 et 1.

   1.1) Que vaut $\alpha^2 + \alpha$?

   1.2) Montrer que le polynôme $X^3 + X + \alpha \in K[X]$ est irréductible sur K.

   Errata : il y a dans cette question une erreur d'énoncé. Ce polynôme est réductible sur K (voir la correction).

   1.3) Quel est le nombre de polynômes irréductibles unitaires de degré 3 dans $K[X]$?

2) Soit p un nombre premier ≥ 5. Posons

$$n = \frac{10^p - 1}{9}.$$

   2.1) Montrer que n n'est pas divisible par 3.

   2.2) Soit ℓ un diviseur premier de n. Montrer que ℓ est congru à 1 modulo $2p$.

   2.3) En déduire que l'entier 11111 est composé, ainsi que sa décomposition en facteurs premiers.

3) Montrer que 65 est pseudo-premier fort en base 8.

4) Factoriser 2001 avec la méthode de Fermat.

5) Posons $n = 203$.

   5.1) Factoriser n avec la méthode rho de Pollard, en utilisant le couple (f, x_0) où

$$f = X^2 + 1 \in \mathbb{Z}[X] \quad \text{et} \quad x_0 = 2.$$

   5.2) Résoudre l'équation $x^2 = 2$ dans $\mathbb{Z}/n\mathbb{Z}$.

   5.3) Quel est le nombre d'entiers a tels que $1 < a < n$ et que n soit pseudo-premier en base a ?

Exercice 2

Soient K un corps fini de cardinal q et E une courbe elliptique définie sur K. Notons $E(K)$ le groupe des points de E rationnels sur K.

Hypothèse. On suppose qu'il existe un entier $n \geq 1$ tel que les groupes

$$E(K) \quad \text{et} \quad \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

soient isomorphes.

Posons

$$t = q + 1 - n^2.$$

1) Montrer que l'on a $t \equiv 2$ mod. n.

   Posons

$$t = 2 + rn \quad \text{avec } r \in \mathbb{Z}.$$

2) Montrer que l'on a $|r| \leq 2$.

3) En déduire que q est l'un des entiers

$$n^2 + 1, \quad n^2 + n + 1, \quad n^2 - n + 1, \quad (n+1)^2, \quad (n-1)^2.$$

4) Supposons que l'on ait $q \equiv 11$ mod. 12. Montrer que l'hypothèse faite n'est jamais réalisée.

Exercice 3

Soit E la courbe projective plane sur $\mathbb{F}_5$ d'équation

$$y^2 z = x^3 - xz^2 + z^3.$$

1) Montrer que E est une courbe elliptique définie sur $\mathbb{F}_5$.
2) Décrire l'ensemble $E(\mathbb{F}_5)$ des points de E rationnels sur $\mathbb{F}_5$.
3) Déterminer la classe d'isomorphisme du groupe abélien $E(\mathbb{F}_5)$.
4) Quel est le polynôme caractéristique du Frobenius de E ?

   Soit $\mathbb{F}_{25}$ le corps de cardinal 25 dans une clôture algébrique de $\mathbb{F}_5$.

5) Quel est l'ordre du groupe $E(\mathbb{F}_{25})$ des points de E rationnels sur $\mathbb{F}_{25}$?
6) Montrer que le groupe des points de 2-torsion de E est contenu dans $E(\mathbb{F}_{25})$.
7) En déduire que $E(\mathbb{F}_{25})$ n'est pas un groupe cyclique.
8) Admettons qu'il existe un point d'ordre 4 de E qui n'est pas rationnel sur $\mathbb{F}_{25}$. En déduire la classe d'isomorphisme du groupe abélien $E(\mathbb{F}_{25})$.
