Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Alain Kraus

Examen du 12 mai 2022

Durée 2h

Les documents du cours et des travaux dirigés, ainsi que les calculatrices portables, sont autorisés. Toutes les réponses doivent être soigneusement justifiées.

Les quatre exercices sont indépendants.

Exercice 1

Les quatre questions sont indépendantes.

1) Posons $n = 1513$.

   1.1) Factoriser n avec la méthode des divisions successives en un produit de deux nombres premiers.

   1.2) Afin de pouvoir se faire envoyer des messages secrets, un utilisateur du cryptosystème RSA utilise comme clé publique le couple $(37, n)$. Quelle est sa clé secrète ?

2) Posons $n = 7663$. Sachant que n est le produit de deux nombres premiers p et q, avec $p < q$, et que $\varphi(n) = 7488$ où $\varphi(n)$ est l'indicateur d'Euler de n, déterminer p et q.

3) Soit S l'ensemble des entiers a tels que $1 < a < 57$ et que 57 soit pseudo-premier en base a.

   3.1) Quel est le cardinal de S ?

   3.2) Déterminer S.

4) Montrer que 25 est pseudo-premier d'Euler en base 7.

Exercice 2

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

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

1) Justifier pourquoi E est une courbe elliptique définie sur $\mathbb{F}_5$.

2) Décrire le groupe $E(\mathbb{F}_5)$ des points de E rationnels sur $\mathbb{F}_5$. En déduire que $E(\mathbb{F}_5)$ est cyclique d'ordre 5.

3) Quel est le polynôme caractéristique du Frobenius de E ?

Notons $\mathbb{F}_{5^n}$ le corps de cardinal 5^n dans une clôture algébrique de $\mathbb{F}_5$.

4) Calculer l'ordre de $E(\mathbb{F}_{25})$.

5) Quelle est la classe d'isomorphisme du groupe $E(\mathbb{F}_{25})$?

6) Calculer l'ordre de $E(\mathbb{F}_{125})$.

7) Quel est le corps des points de 2-torsion de E ?

8) En déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_{125})$.

Exercice 3

Soit E la courbe elliptique définie sur $\mathbb{F}_5$ d'équation

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

1) Quel est l'ordre du groupe $E(\mathbb{F}_5)$ des points de E rationnels sur $\mathbb{F}_5$?

2) En déduire que E est une courbe elliptique ordinaire. Quel est l'ordre du groupe $E[5]$ des points de 5-torsion de E ?

3) Soit $\mathbb{F}_5(E[5])$ le corps des points de 5-torsion de E. En utilisant un exercice de la feuille de travaux dirigés du chapitre IV que l'on précisera, déterminer l'entier $r \geq 1$ tel que $\mathbb{F}_5(E[5]) = \mathbb{F}_{5^r}$.

4) Soit ϕ_5 l'endomorphisme de Frobenius de E. Soit P un point de 5-torsion non nul de E.

   4.1) Montrer que $\phi_5(P)$ est un multiple de P.

   4.2) Déterminer le plus petit entier $n \geq 1$ tel que $\phi_5(P) = nP$.

Exercice 4

Soit E une courbe elliptique définie sur $\mathbb{F}_{23}$. Soit $E(\mathbb{F}_{23})$ le groupe des points de E rationnels sur $\mathbb{F}_{23}$.

1) Quel est l'intervalle de Hasse pour le nombre premier 23 ? Rappeler pourquoi l'ordre de $E(\mathbb{F}_{23})$ appartient à cet intervalle.

On suppose que l'exposant du groupe $E(\mathbb{F}_{23})$ est égal à 8.

2) Quelles sont les deux valeurs possibles pour l'ordre de $E(\mathbb{F}_{23})$?

3) En déduire l'ordre et la classe d'isomorphisme du groupe $E(\mathbb{F}_{23})$.
