TD Courbes Elliptiques 1

Damien Robert

5 janvier 2016

1 Prise en main Pari/GP

Exercice 1.1. Consulter l'aide de la fonction `isprime`. Le nombre $2^{2^{11}}+1$ est-il premier ?

Exercice 1.2. Le groupe $(\mathbb{Z}/42\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ est-il cyclique ?

Exercice 1.3. Consulter l'aide de la fonction `znstar`. Quelle est la structure de $(\mathbb{Z}/130\mathbb{Z})^\times$ en tant que groupe abélien ? Donner un système de générateurs pour ce groupe.

Exercice 1.4.

1. Quel est le degré de l'extension $\mathbb{F}_8/\mathbb{F}_2$?
2. Quelle est la structure de $\mathbb{F}_8$ en tant que groupe abélien ?

Exercice 1.5. L'objectif de cet exercice est de rappeler la méthode d'exponentiation binaire.

1. Étant donné un entier naturel n, rappelons que son écriture en base 2 est de la forme
$$n = \sum_{i=0}^{k} \epsilon_i 2^i$$
où $\epsilon_i \in \{0,1\}$ pour tout i. Écrire une procédure `base2`(n) qui renvoie la liste $(\epsilon_0, \epsilon_1, \dots, \epsilon_k)$ des chiffres de n dans son écriture en base 2.
2. En déduire un algorithme d'exponentiation efficace dans un ensemble E muni d'une loi de multiplication $*$.
3. Le programmer pour $E = \mathbb{R}$. On appellera `puissance`(x,n) la procédure obtenue, qui, étant donné un réel x et un entier n, renvoie x^n.
4. Expliquer comment, grâce à Pari/gp, le même programme peut être utilisé dans $E = \mathbb{Z}/m\mathbb{Z}$ muni de la multiplication modulo m. Tester quelques exemples.

2 Arithmétique

Exercice 2.1. Le petit théorème de Fermat affirme que, si p est un nombre premier, alors
$$\forall b \in \mathbb{Z}, \quad b^p \equiv b \pmod{p}.$$

1. Justifier brièvement ce théorème.
2. Montrer, en utilisant ce théorème, que $m = 10^5 + 7$ n'est pas un nombre premier.
3. Retrouver ce résultat en utilisant la commande `isprime` et la commande `ispseudoprime`. Comparer ces deux commandes à l'aide de la documentation.

4. Trouver la décomposition de m en facteurs premiers à l'aide de la commande `factor`.
5. Étudier expérimentalement la réciproque du petit théorème de Fermat, *i.e.* si
$$\forall b \in \mathbb{Z}, \quad b^n \equiv b \pmod{n}$$
alors n est un nombre premier.
6. Un **nombre de Carmichael** est un entier n qui n'est pas premier, mais qui satisfait quand même la conclusion du petit théorème de Fermat. Dresser la liste de tous les nombres de Carmichael inférieurs à 10000 à l'aide de gp.

Exercice 2.2. Donner la liste de tous les carrés dans $\mathbb{Z}/17\mathbb{Z}$.

Exercice 2.3. On considère le polynôme
$$P(X) = X^5 + X^4 + 2X^3 - 2X^2 - 4X - 3$$
1. En se servant de gp, factoriser P dans $\mathbb{C}[X]$ puis dans $\mathbb{Z}[X]$.
2. Qu'est-ce que le discriminant d'un polynôme ? Quelles sont ses propriétés ?
3. Calculer à l'aide de gp le discriminant de P.
4. Factoriser P dans $\mathbb{F}_2[X], \mathbb{F}_{11}[X], \mathbb{F}_{13}[X], \mathbb{F}_{23}[X], \mathbb{F}_{31}[X], \mathbb{F}_{37}[X]$. Que remarquez-vous ?

Exercice 2.4. L'objectif de cet exercice est de pouvoir manipuler de façon pratique les corps finis et les polynômes à coefficients dans les corps finis.

Soit p un nombre premier. On note $\mathbb{F}_p$ le corps fini à p éléments. Pour tout entier $n \geq 1$, on note $\mathbb{F}_{p^n}$ le corps fini à p^n éléments, qui est une extension de degré n de $\mathbb{F}_p$. Tous ces corps sont **uniques à isomorphisme près**.

1. Montrer que $\mathbb{F}_4$ est isomorphe en tant que corps à
$$\mathbb{F}_2[X]/(X^2 + X + 1).$$
Écrire les tables d'addition et de multiplication de ce corps en s'aidant de gp.
2. On cherche à décrire explicitement $\mathbb{F}_8$.
   a) Soit x dans $\mathbb{F}_8 \setminus \mathbb{F}_2$. Montrer que $\mathbb{F}_8 = \mathbb{F}_2[x]$.
   b) En déduire que $\mathbb{F}_8$ est isomorphe en tant que corps à $\mathbb{F}_2[X]/(Q(X))$ où $Q(X)$ est le polynôme minimal de x sur $\mathbb{F}_2$. Rappelez les propriétés d'un tel polynôme.
   c) Combien existe-t-il de polynômes de degré 3 à coefficients dans $\mathbb{F}_2$? Dressez la liste des polynômes de degré 3 à coefficients dans $\mathbb{F}_2$ et $\mathbb{F}_2$-irréductibles en s'aidant de gp.
   d) En déduire que $\mathbb{F}_8$ est isomorphe en tant que corps à
$$\mathbb{F}_2[X]/(X^3 + X + 1) = \mathbb{F}_{8,1}$$
et à
$$\mathbb{F}_2[X]/(X^3 + X^2 + 1) = \mathbb{F}_{8,2}.$$
   e) Écrire les tables d'addition et de multiplication de $\mathbb{F}_{8,1}$ et $\mathbb{F}_{8,2}$ en s'aidant de gp.
   f) Soit α une racine de $X^3 + X + 1$. Montrer à l'aide de gp que α^2 et α^4 sont les autres racines de $X^3 + X + 1$. Montrer également à l'aide de gp que α^3, α^5 et α^6 sont les racines de $X^3 + X^2 + 1$.
   g) Écrire un isomorphisme explicite entre $\mathbb{F}_{8,1}$ et $\mathbb{F}_{8,2}$.
3. On fixe à présent un polynôme $Q(X) \in \mathbb{F}_p[X]$, irréductible de degré n.
   a) Montrer que $\mathbb{F}_p[X]/(Q(X))$ est le corps fini de cardinal $q = p^n$, noté $\mathbb{F}_q$.

b) Montrer que pour tous x et y dans $\mathbb{F}_q$ et pour tout entier naturel t,

$$(x+y)^{p^t} = x^{p^t} + y^{p^t}.$$

c) En déduire que l'application

$$\begin{array}{rccc} \text{Frob}_p : & \mathbb{F}_q & \to & \mathbb{F}_q \\ & x & \mapsto & x^p \end{array}$$

est un automorphisme[1] de $\mathbb{F}_q$, dont l'ensemble des points fixes est exactement $\mathbb{F}_p$.

d) En déduire que pour tout élément x de $\mathbb{F}_q$ et tout entier naturel t,

$$(Q(x))^{p^t} = Q\left(x^{p^t}\right).$$

e) En déduire également que si α est une racine de $Q(X)$ alors les autres racines de $Q(X)$ sont $\alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{n-1}}$.

4. Comment trouver un polynôme irréductible de degré n, à coefficients dans $\mathbb{F}_p$?
   a) Écrire une procédure permettant de tirer aléatoirement un polynôme de degré n à coeffcients dans $\mathbb{F}_p$.
   b) Tester l'irréductibilité d'un tel polynôme de plusieurs façons.
   c) Donner une estimation du nombre d'essais à faire par rapport à n pour que le polynôme aléatoire fourni par la procédure précédente soit $\mathbb{F}_p$-irréductible.
5. Tester sur des gros exemples tout ce qui a été vu dans cet exercice *i.e.* $n > 10^3$ et/ou $p > 10^{10}, 10^{100}$. Qu'en pensez-vous ?

[1] Frob_p est le **morphisme de Frobenius** de $\mathbb{F}_q$