TD Elliptic Curves 1

Damien Robert

02 September 2022

1 First Sage commands

Exercice 1.1. Consult the help of the function `is_prime`. Is the number $2^{2^{11}}+1$ prime?

Exercice 1.2. Is the group $(\mathbb{Z}/42\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ cyclic? If yes, find a generator.

Exercice 1.3. Look at functions available on a `Zmod` object. What is the structure of the multiplicative group $(\mathbb{Z}/130\mathbb{Z})^\times$? Give a system of generators of this group.

Exercice 1.4. Compute all squares in $\mathbb{Z}/17\mathbb{Z}$.

Exercice 1.5. Fermat's little theorem says that if p is a prime number, then

$$\forall b \in \mathbb{Z}, \quad b^p \equiv b \pmod{p}.$$

1. Give a proof of this theorem.
2. Show that $m = 10^5 + 7$ is not a prime number.
3. What is the difference between the functions `is_prime` and `is_pseudoprime`?
4. Find a factorisation of m.
5. A **Carmichael number** number is an integer n which is not prime but satisfy Fermat condition. Compute all Carmichael numbers less than 10000.

2 Polynomials and finite fields

Exercice 2.1. Consider the polynomial $P(X) = X^5 + X^4 + 2X^3 - 2X^2 - 4X - 3$.

1. Factorize P in $\mathbb{C}[X]$ and in $\mathbb{Z}[X]$.
2. Recall what is the discriminant of a polynomial and what are its properties? Compute the discriminant of P.
3. Factorize P in $\mathbb{F}_2[X]$, $\mathbb{F}_{11}[X]$, $\mathbb{F}_{13}[X]$, $\mathbb{F}_{23}[X]$, $\mathbb{F}_{31}[X]$, $\mathbb{F}_{37}[X]$. What do you remark? (Hint: factorize the discriminant.)

Exercice 2.2. The finite field with four elements.

1. Show that $\mathbb{F}_4$ is isomorphic as a field to
$$\mathbb{F}_2[X]/(X^2+X+1).$$
2. Write the addition and multiplication table of $\mathbb{F}_4$.

Exercice 2.3. Let's try to understand $\mathbb{F}_8$.

1. Let $x \in \mathbb{F}_8 \ \ \mathbb{F}_2$. Show that $\mathbb{F}_8 = \mathbb{F}_2[x]$.
2. Deduce that $\mathbb{F}_8$ is isomorphic as a field to $\mathbb{F}_2[X]/(Q(X))$ where $Q(X)$ is the minimal polynomial of x over $\mathbb{F}_2$.
3. Give the list of all irreducible degree 3 polynomials over $\mathbb{F}_2$.
4. Show that $\mathbb{F}_8$ is isomorphic as a field to
$$\mathbb{F}_2[X]/(X^3+X+1) = \mathbb{F}_{8,1}$$
and to
$$\mathbb{F}_2[X]/(X^3+X^2+1) = \mathbb{F}_{8,2}.$$
5. Write the addition and multiplicative table of $\mathbb{F}_{8,1}$ and $\mathbb{F}_{8,2}$.
6. Let α a root of X^3+X+1. Show that α^2 and α^4 are the other roots of X^3+X+1. Show that α^3, α^5 and α^6 are the roots of X^3+X^2+1.
7. Write an isomorphism between $\mathbb{F}_{8,1}$ and $\mathbb{F}_{8,2}$.

Exercice 2.4.

1. Construct the finite field $\mathbb{F}_{3^4}$.
2. What is the degree of the extension $\mathbb{F}_{3^4}/\mathbb{F}_3$?
3. What is the structure of $\mathbb{F}_{3^4}$ as an abelian group?
4. What is the multiplicative structure of $(\mathbb{F}_{3^4}^*, \times)$ as an abelian group?

Exercice 2.5 (Frobenius morphism)**.** Let $Q(X) \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree n.

1. Show that $\mathbb{F}_p[X]/(Q(X))$ is the finite field of cardinal $q = p^n$, denoted $\mathbb{F}_q$.
2. Show that for all x, y in $\mathbb{F}_q$ and all integer t,
$$(x+y)^{p^t} = x^{p^t} + y^{p^t}.$$

3. Deduce that the application

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

is an automorphism[1] of $\mathbb{F}_q$, and that its set of fixed points is exactly $\mathbb{F}_p$.

4. Deduce that for any polynomial P over $\mathbb{F}_p$, all x in $\mathbb{F}_q$ and all integer t,

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

5. Show that if α is a root of $Q(X)$, the other roots of $Q(X)$ are $\alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{n-1}}$.

Exercice 2.6. Irreducible polynomials.

1. Write a function that compute a random polynomial of degree n over $\mathbb{F}_p$.
2. Compute the irreductibility of this polynomial.
3. Give an estimate on the number of tries needed to find an irreducible polynomial.
4. Test your code on large p or n *i.e.* $n > 10^3$ and/or $p > 10^{10}, 10^{100}$.

Exercice 2.7. Discriminants.

1. Compute the discriminant of $aX^2 + bX + c$.
2. Compute the discriminant of $X^3 + aX + b$.

3 Fast exponentiation

Exercice 3.1. Given a number n, its base 2 decomposition is

$$n = \sum_{i=0}^{k} \varepsilon_i 2^i$$

where $\varepsilon_i \in \{0, 1\}$ for all i.

1. Write a function `base2(n)` which give the list $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_k)$ of the digits of n in base 2 from right to left.
2. Write an efficient exponentiation algorithm `power`.
3. Try this to compute x^n for $x \in \mathbb{R}$ or x in a finite field, and compare with the built-in method.
4. Write a function `base2bis(n)` which give the list $(\varepsilon_k, \varepsilon_1, \dots, \varepsilon_0)$ of the digits of n in base 2 from left to right.

---

[1] Frob_p is the **Frobenius morphism** of $\mathbb{F}_q$

5. Rewrite `power` using this left to right binary decomposition of n.

Exercice 3.2. Windowing and sliding windows.

1. Implement a windowing method of length m to compute `power` (the windowing method is essentially the same as using the base 2^m decomposition);
2. Improve this method by doing a sliding window.