MPRI – cours 2.12.2

F. Morain, B. Smith

Final exam, 2014/03/10

The following exercises are independent and can be treated in any order.

Exercise 1 Arithmetic

Let N be an odd composite number, $a \in (\mathbb{Z}/N\mathbb{Z})^*$. Suppose we can find the order of a modulo N, say r. In which case(s) can one factor N given r ?

Exercise 2 Decomposing an integer into primes

Decomposing an integer means finding primes p_i's such that

$$N = \prod_{i=1}^{k} p_i^{\alpha_i}$$

with $p_i \neq p_j$ and $\alpha_i > 0$. Give an algorithm that accomplishes this task using the different methods seen during the course. Make sure it works on the following numbers : 128, 15, 101, 143, 75.

Exercise 3 2-torsion points

Let p be an odd prime > 3.

3.1 How many points of order 2 can an elliptic curve $E/\mathbb{F}_p$ have ? Relate each case to the equation of $E : Y^2 = X^3 + AX + B$.

3.2 Same question for the Jacobian of a hyperelliptic curve $Y^2 = f(X)$ of genus g over $\mathbb{F}_p$.

Exercise 4 Playing with the $L(1/4)$ complexity

At the beginning of 2013, Joux proposed a new algorithm for the discrete logarithm problem in finite fields of small characteristic with a complexity in $L_N(1/4)$, where N is the cardinality of the finite field. In the following, we do not study this algorithm, but we play with this unusual complexity.

4.1 Assume that a black-box outputs uniformly distributed random integers between 0 and N. Let $c > 0$ be constant. After $L_N(1/4, c)$ integers have been output, what is the expected smoothness of the smoothest integer among those ?
Answer.

4.2 Taking the Number Field Sieve algorithm (NFS) as a tool for testing the smoothness of an integer, what is the expected cost of finding this smoothest integer ?
Answer.

4.3 Assume that there is an algorithm that can find all factors less than B of an integer bounded by N in time $(\log N)^{O(1)} L_N(1/2, 1)$. What is the expected cost of finding the smoothest integer using this tool instead of NFS ?
Answer.

4.4 Same questions with polynomials over $\mathbb{F}_q$: among $L_N(1/4, c)$ polynomials of degree at most $\log_q(N)$, how smooth is expected to be the smoothest polynomial and what is the expected cost of finding it ?

Answer.

Exercise 5 Elliptic Curves 1

Consider the elliptic curve

$$\mathcal{E} : y^2 = x^3 + x - 2 \quad \text{over} \quad \mathbb{F}_p \ ,$$

where $p \notin \{2, 7\}$ is a prime.

1. Why have we excluded $p = 2$ and $p = 7$?
2. What is the order of the automorphism group of $\mathcal{E}$?
3. Give upper and lower bounds on the order of $\mathcal{E}(\mathbb{F}_p)$.
4. What is the best strategy for determining $N = \#\mathcal{E}(\mathbb{F}_p)$ if $\log_2 p \sim 384$?
5. Suppose we know $N = \#\mathcal{E}(\mathbb{F}_p)$. What is the exact value of $\#\mathcal{E}(\mathbb{F}_{p^2})$? What about $\#\mathcal{E}(\mathbb{F}_{p^n})$ for $n > 2$?
6. Give upper bounds on the largest prime factors of $\#\mathcal{E}(\mathbb{F}_p)$ and $\#\mathcal{E}(\mathbb{F}_{p^2})$.
7. What is the asymptotic complexity for solving an instance of the DLP in $\mathcal{E}(\mathbb{F}_p)$ as $p \to \infty$?
8. What is the asymptotic complexity for solving an instance of the DLP in $\mathcal{E}(\mathbb{F}_{p^2})$ as $p \to \infty$?
9. Consider the curve
$$\mathcal{E}' : y^2 = x^3 + x + 2 \ ,$$
defined over the same $\mathbb{F}_p$ as $\mathcal{E}$. How are the values of $\#\mathcal{E}(\mathbb{F}_p)$ and $\#\mathcal{E}'(\mathbb{F}_p)$ related ?

Answer.

Exercise 6 Elliptic Curves 2

Consider the elliptic curve

$$\mathcal{E} : y^2 = x^3 + 1 \quad \text{over } \mathbb{F}_p \ , \quad \text{where } p := 2^{255} - 3015$$

(ie, p is a 254-bit prime). We have

$$\#\mathcal{E}(\mathbb{F}_p) = p + 1 = 2 \cdot 9 \cdot r \ ,$$

where r is a 251-bit prime. Let ζ be the automorphism of $\mathcal{E}$ defined by

$$\zeta : (x, y) \longmapsto (\rho_3 x, y) \ ,$$

where ρ_3 is a primitive cube root of unity in $\overline{\mathbb{F}}_p$.

1. What is the smallest e such that ζ is defined over $\mathbb{F}_{p^e}$?
2. What is the characteristic polynomial of ζ ?
3. Let $\pi : (x, y) \mapsto (x^p, y^p)$ be the Frobenius endomorphism of $\mathcal{E}$. Show that $\pi\zeta \neq \zeta\pi$.

4. Is $\mathcal{E}$ pairing-friendly ? Explain why or why not.
5. Let $\mathcal{G}$ be the order-r subgroup of $\mathcal{E}$. What impact does the Menezes–Okamoto–Vanstone reduction have on the difficulty of discrete logarithms in $\mathcal{G}$?
6. Is $\mathcal{E}$ a good choice of curve for use in the Boneh–Lynn–Schacham short signature scheme ? Explain why or why not.

Answer.