Université Joseph Fourier – Grenoble INP
UFR IM^{2}AG

Master SCCI – SAC

Homework – Due before November 4, 2013, 8:00 am

You will send your answers (in a pdf file generated with LaTeX) and programs (firstname_name.gp file format) to vanessa.vitse@ujf-grenoble.fr. You must use the same notations as in the subject.

Exercise 1

Let q be a prime power.

1. Prove that for any $k \in \mathbb{N}^*$, the following equality holds in $\mathbb{F}_q[X]$:
$$X^{q^k} - X = \prod_{\substack{P \in \mathbb{F}_q[X] \text{ irred. of deg } l \\ \text{with } l|k}} P$$

Let $P \in \mathbb{F}_q[X]$ be a polynomial of degree d.

2. Show that if P does not divide $X^{q^d} - X$, then P is reducible over $\mathbb{F}_q$.
3. Let $d = \prod_{i=1}^n p_i^{\alpha_i}$ be the prime decomposition of the degree d of P. Show that if the gcd $P \wedge (X^{q^{d/p_i}} - X)$ is different from 1 for a given $1 \leq i \leq n$, then P is reducible over $\mathbb{F}_q$.
4. Conversely, show that if $P|(X^{q^d} - X)$ and $P \wedge (X^{q^{d/p_i}} - X) = 1$ for all $1 \leq i \leq n$, then P is irreducible over $\mathbb{F}_q$.
5. Write an efficient algorithm that tests if P is an irreducible polynomial over $\mathbb{F}_q$ (hint: how to compute efficiently $X^{q^k} \bmod P$ for a given k?). Give its complexity.
6. Implement your algorithm in pari-gp at least when q is a prime and test on random polynomials of composite degree over $\mathbb{F}_{65537}[X]$. Is the polynomial $P(X) = X^{30} + X + 35$ irreducible over $\mathbb{F}_{65537}$?

Exercise 2

The goal of this exercise is to study and implement some factorization algorithms. Let $B \in \mathbb{N}^*$. An integer n is called B-smooth if $p_i \leq B$ for all primes p_i in the prime decomposition of n.

1. Let N be an integer and $C(B,N) = \prod_{p \text{ prime}, p \leq B} p^{\lfloor \log_p(N) \rfloor}$. Show that any B-smooth integer n smaller than N divides $C(B,N)$.

2. Assume that N has a prime factor p such that $\#(\mathbb{F}_p)^* = p - 1$ is B-smooth (for some not-too-large integer B). Show that any integer a not divisible by p satisfies $a^{C(B,N)} = 1 \bmod p$. In particular, the element $g = a^{C(B,N)} - 1 \in \mathbb{Z}/N\mathbb{Z}$ is not invertible and it is likely that $\gcd(g, N)$ is a non-trivial factor of N.

3. What do we learn if $\gcd(g, N) = 1$? And if $\gcd(g, N) = 0$?

4. Write an algorithm that, given N and B, tries to compute a factor of N; give its complexity. What can be done if the algorithm fails to find a factor?

5. Write a modified algorithm that takes only N as input and implement it in pari-gp. Try it on $N = 770977$ and $N = 4131833089164730750 1$.

This algorithm (called "$p - 1$") is clearly inefficient if N has no prime factor that is B-smooth for a not-too-large integer B. We will now study a similar algorithm, based on elliptic curves, which is currently the most efficient for finding "small" factors of large integers.

Let $a, b \in \mathbb{Z}/N\mathbb{Z}$. We define the "elliptic curve" of equation $Y^2 = X^3 + aX + b$ over $\mathbb{Z}/N\mathbb{Z}$ as the set of points

$$E(\mathbb{Z}/N\mathbb{Z}) = \{(x, y) \in (\mathbb{Z}/N\mathbb{Z})^2 : y^2 = x^3 + ax + b \bmod N\} \cup \{\mathcal{O}\}.$$

6. Explain why it is not always possible to compute the sum of two points $P, Q \in E(\mathbb{Z}/N\mathbb{Z})$ using the "chord and tangent" law (hint: not all integers are invertible modulo N). If P and Q cannot be summed, show that it is possible to deduce a non-trivial factor of N.

For any prime divisor p of N, we consider the elliptic curve $E(\mathbb{F}_p)$ obtained by reducing the equation $Y^2 = X^3 + aX + b$ modulo p. We can also reduce modulo p the coordinates of any point $P \in E(\mathbb{Z}/N\mathbb{Z})$ and obtain a point P_p in $E(\mathbb{F}_p)$.

7. Let $P, Q \in E(\mathbb{Z}/N\mathbb{Z})$. If their sum can be computed, show that $(P + Q)_p = P_p + Q_p$. If $P_p + Q_p = \mathcal{O}_p$, show that either $P + Q = \mathcal{O}$ or their sum cannot be computed.

8. Assume that N has a prime factor p such that $\#E(\mathbb{F}_p)$ is B-smooth and let $P \in E(\mathbb{Z}/N\mathbb{Z})$. Explain why the computation of $[C(B, N)]P$ (with the double-and-add algorithm) is very likely to fail and thus yields a non-trivial factor of N.

By contrast with the $p-1$ method, if this method fails to find a factor we can always start again with a new curve. Since $\#E(\mathbb{F}_p)$ can take all values in $[p+1-2\sqrt{p}; p+1+2\sqrt{p}]$, we are almost sure to hit a B-smooth cardinality after enough attempts.

9. Write and implement in pari-gp an algorithm that takes N and B as inputs and uses this method to find a factor of N (hint: in order to find an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ with a point on it, start by choosing randomly a, x, y and then set $b = y^2 - x^3 - ax \bmod N$).

10. Test your program on the first Fermat numbers $2^{2^n} + 1$ for $n \geq 5$. Experiment with the parameter B, to determine when the computation is optimal.