Exercises for the Lecture on Computational Number Theory

Preda Mihăilescu

Exercise 1 (Primality).

In this exercise n is a large integer.

a) Suppose that there is an integer $F = \prod_{i=1}^{k} p_i^{e_i}$ with known primes p_i and $e_i > 0$ such that $F|(n-1)$ and $F > \sqrt{N}$. Let $R = (n-1)/F$ and assume that for each i there is an integer a_i such that the following conditions hold: $a_i^{RF} \equiv 1 \bmod n$ and $(a_i^{R(F/p_i)} - 1, n) = 1$. Show that $\mathbb{Z}/(n \cdot \mathbb{Z})^\times$ contains a primitive $F-$th root of unity and conclude that n is prime.

b) Let $\mathcal{N} = \mathbb{Z}/(n \cdot \mathbb{Z})$ and $s > \sqrt{n}$ be an integer with $t = \mathrm{ord}_s(n)$ the order of $n \bmod s$. Let $\Phi_s(X) \in \mathbb{Z}[X]$ be the $s-$th cyclotomic polynomial, i.e. the minimal polynomial of a primitive $s-$th root of units, e.g. $e^{2\pi\imath/s}$. Assume that there is a polynomial $\Psi \in \mathcal{N}[X]$ of degree t such that

(i) $\Psi(X)$ divides $\Phi_s(X)$ over $\mathcal{N}$.

(ii) Let $\zeta = X + (\Psi(X)) \in \mathcal{N}[X]/(\Psi(X))$. Then $\Psi(\zeta^{n^i}) = 0$ for $i = 1, 2, \ldots, t$.

Then $r|n$ iff $r \equiv n^i \bmod s$ for some $i \in \{1, 2, \ldots, t\}$.

Exercise 2 (Points on elliptic curves).

a) Consider the equation $cY^2 = dX^3 + aX + b$. Using multiplication by c^3d^2 on both sides of the equation, show that one obtains, after an adequate change of variables, the equation of an elliptic curve in Weierstrass normal form.

Use this fact in order to show that given a prime p, one can construct an elliptic curve $E(\mathbb{F}_p)$ together with a point $P = (X, y) \in E$ without taking square roots. **Hint**: Start with X and an arbitrary elliptic curve, such that $cY^2 = X^3 + aX + b$ and then use the previous construction.

b) Let n be a large integer and $E : Y^2 = X^3 + aX + b$ and let $P = (X, Y)$ satisfy the equation modulo n (note that n needs not be a prime). Assuming that $p|n$ is a prime factor such that $m = |E(\mathbb{F}_p)|$ is divisible only by primes $r \leq B$, for a given bound $B \in \mathbb{Z}_{>0}$ we construct the value $Q = [B!] \in \mathbb{Z}/(n \cdot \mathbb{Z})^2$ as follows: use the formal expression for repeated addition and doubling on the elliptic curve E and reduce the results at each step modulo n. The inversion will be performed by means of the Euclidean Algorithm.

Prove that in the process of computing Q one will in general encounter an expression of the type $[2]Q' = A/B$ or $Q' \oplus Q'' = A/B$, with $(B, n) = p$; here Q', Q'' are intermediate "points" in the given addition chain.

Show that this fact can be used for factoring integers and explain the case in which the GCD $(B, n) = n$. *This is the core idea of the Elliptic Curve Factoring Method - ECM*, descovered by H. Lenstra Jr. in 1984.

Exercise 3 (Polynomial reduction). Let D be an integral ring and $f \in D[X]$ with $f(0) = 1$ have degree m.

a) Use the Newton algorithm for finding a polynomial $g \in D[X]$ with $f \cdot g \equiv 1 \bmod x^l$. **Hint**: Construct recursively a sequence $g_i \in D[X]$ with $fg_i \equiv 1 \bmod x^{2^i}$.

b) Let $a, b \in D[X]$ be two polynomials. We give here an algorithm for computing the euclidean division $a = qb+r$ using only multiplications and truncations. We denote by $\mathrm{rev}_m(b) = X^m b(1/X)$; if $m = \deg(b)$, we simply write $\mathrm{rev}(b) = X^{\deg(b)} b(1/X)$. Show that the following algorithm computes the euclidean quotient and remainder for a, b:

1. If $\deg(a) < \deg(b)$ then $q = 0$ and $r = a$, return.
2. Let $m = \deg(a) - \deg(b)$ and compute $h = \mathrm{rev}(b)^{-1}$ using the algorithm in the previous point.
3. Let $q^* = \mathrm{rev}(a) \cdot h \mathrm{rem} x^{m+1}$.
4. Let $q = \mathrm{rev}_m(q*), r = a - qb$ and return.

Comment upon the computational advantages of this algorithm.

Exercise 4 (Multiplication on elliptic curves).

Let $E : Y^2 = X^3 + aX + B$ be an elliptic curve. We define the *division polynomials* $\psi_m \in \mathbb{Z}[X, Y, a, b]$ by the following recursion:

$$\begin{aligned}
\psi_0 &= 0, \quad \psi_1 = 1, \quad \psi_2 = y, \\
\psi_3 &= 3X^4 + 6aX^2 + 12bX - a^2 \quad \psi_4 = 4Y(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4abX - 8b^2 - a^3), \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{for } m \geq 2, \\
\psi_{2m} &= \frac{\psi_m}{2Y} \cdot \left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right) \quad \text{for } m \geq 2.
\end{aligned}$$

Furthermore, we define $\phi_m = X\psi_m^2 - \psi_{m+1}\psi_{m-1}$ and $\omega_m = \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4Y}$.

a) Assuming that $Y^2 = X^3 + aX + b$, show that $\psi_n, \phi_n, \omega_n \in \mathbb{Z}[X, a, b] \cup Y\mathbb{Z}[X, a, b]$ and distinguish when the polynomials are divisible by Y and when not.

b) Prove that if $P = (X, Y) \in E$, then

$$[n]P = \left(\frac{\phi_n(X)}{\psi_n(X)^2}, \frac{\omega_n(X, Y)}{\psi_n(X, Y)^3}\right).$$

Comment upon the appearance of Y. (The proof is involved and uses knowledge of the Weierstraß $\wp$-function.)

c) Deduce that $P \in E[n]$ is an n-torsion point iff $\psi_n(P_x) = 0$.

Exercise 5 (Deriving the torsion polynomials).

Let $\wp(nz) = R_n(\wp(z))$ for $R_n \in \mathbb{C}(X)$. We have seen that

$$(\wp(nz), \wp'(nz)) = (R_n(\wp(z)), \frac{1}{n}\wp'(z)R_n'(\wp(z)).$$

We aim to compute recursively $R_n(x)$ and then identify terms in the above equation.

a) Show that there is an elliptic function verifying

$$f_n^2(z) = n^2 \cdot \prod_{0 \neq u \in (\mathbb{C}/L)[n]} (\wp(z) - \wp(u)).$$

For odd n, we have $f_n = P_n(\wp)$ with $\deg(P_n) = \frac{n^2-1}{2}$ and leading coefficient being n.

For even n, we have $f_n = \wp' P_n(\wp)$ with $\deg(P_n) = \frac{n^2-4}{2}$ and leading coefficient being $n/2$.

The zeroes of f_n are simple zeroes at the points $0 \neq u \in (\mathbb{C}/L)[n]$ and the expantion at 0 is

$$f_n(z) = \frac{(-1)^{n+1}n}{z^{n^2-1}} + O(z^{-n^2+2}).$$

b) For $n \geq 2$ we have

$$\wp(nz) = \wp(z) - \frac{f_{n-1}(z)f_{n+1}(z)}{f_n^2(z)}.$$

Hint: Use expansions at 0.

c) Prove the identities

$$\begin{aligned} f_{2n+1} &= f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1}, \\ \wp' f_{2n+1} &= f_n \cdot (f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2). \end{aligned}$$

d) For all $n \geq 1$, we have

$$f_n(z) = \psi_n \cdot \left(\wp(z), \frac{1}{2}\wp'(z)\right).$$

Hint: Use the induction for the definition of ψ_n and the identities for f_n derived above.

e) Prove

$$\wp'(nz) = f_{2n}(z)/f_n^4(z).$$

f) Use the above identities for proving that for all $n \geq 1$ we have indeed

$$n(X, Y) = \left(\frac{\phi_n(X, Y)}{\psi_n^2(X, Y)}, \frac{\omega_n(X, Y)}{\psi_n^3(X, Y)}\right).$$

Exercise 6 (Complex multiplication).

Let L be a lattice which has complex multiplication by $\alpha \in \mathbb{C}$, i.e. $\alpha L \subset L$.

a) Prove that $\alpha \in \mathbb{K} := \mathbb{Q}[\sqrt{-n}]$ for some $n \in \mathbb{N}$.

b) Show that there is an order $\mathcal{O} \subset \mathcal{O}(\mathbb{K})$ containing α and such that L has complex multiplication by all $\beta \in \mathcal{O}$.

c) Show that there are two polynomials $A, B \in \mathbb{C}[X]$ with $\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z)}$ and $\deg(A) = \deg(B) + 1 = [L : \alpha L] = N(\alpha)$.

Exercise 7 (Schoof's algorithm)**.**

Let $E : Y^2 = f(X) = X^3 + aX + b$ be an ordinary elliptic curve over the prime finite field $\mathbb{F}_p$ with $p \neq 2, 3$. Let $\ell \neq p$ be an odd prime and $g(X) = \psi_\ell(X, Y)$; show that f does indeed only depend upon X, using the fact that ℓ is odd.

a) Show that $\mathbb{T} := \mathbb{F}_p[X, Y]/(g(X), Y^2 - f(X))$ is a galois algebra. What is the degree of its maximal subfield? Let $P = (\hat{X}, \hat{Y}) = (X + g(X), Y + (Y^2 - f(X))) \in \mathbb{T}$ be the *generic* ℓ-torsion point.

b) Let $\Phi : \mathbb{T} \to \mathbb{T}$ be the map $\hat{X} \mapsto \hat{X}^p, \hat{Y} \mapsto \hat{Y}^p$. Show that there is a representation $\rho : \langle \Phi \rangle \to \ \mathrm{GL}(2, \mathbb{F}_\ell)$.

c) Let $\Phi^2 + t\Phi + p = 0$ be the characteristic equation of the Frobenius in $\mathrm{End}(E)$. Show that $\mathbf{Tr}(\rho(\Phi)) \equiv t \bmod \ell$.

d) The polynomial $g(X)$ factors over $\mathbb{F}_p$ and its irreducible factors will be orbits of $\hat{X}$ under the action of Frobenius. Recall that $E[\ell] \cong \mathbb{F}_\ell^2$ and use the diagonalization of $\rho(\Phi)$ over $\mathbb{F}_\ell$ or $\mathbb{F}_{\ell^2}$ in order to determine the factorzation pattern of $g(X)$ in dependence on its eigenvalues.

d) Show that if the Legendre symbol $\left(\frac{t^2-4p}{\ell}\right) = 1$, then $g(X)$ allows at least two factors $g_1(X), g_2(X) \in \mathbb{F}_p[X]$ of degree $\frac{\ell-1}{2}$. These factors need not be irreducible.

e) Show that if the Legendre symbol $\left(\frac{t^2-4p}{\ell}\right) = -1$, then $g(X)$, all the irreducible factors of $g(X)$ have the same degree and deduce this degree in function of the roots of the characteristic polynomial of the Frobenius over $\mathbb{F}_\ell$.

f) Show that if the Legendre symbol $\left(\frac{t^2-4p}{\ell}\right) = 0$, then either $g(X)$ factors in polynomials of equal degree dividing $\frac{\ell-1}{2}$, or it has a factor of degree ℓ.

Exercise 8 (Elkies' variant of Schoof's algorithm)**.**

Let E, ℓ, p be like in the previous exercise and let $G(X)|g(X)$ be any polynomial dividing $g(X)$ over $\mathbb{F}_p$. Define $\mathbb{T} := \mathbb{F}_p[X, Y]/(G(X), Y^2 - f(X))$ and show that it is a galois algebra too.

a) Define $\mathbb{T} := \mathbb{F}_p[X, Y]/(G(X), Y^2 - f(X))$ and show that it is a galois algebra too.

b) Show that $(\Phi^2(P) + p\Phi(P))_x = t_\ell \Phi(P)$ for some $t_\ell \in \{0, 1, \ldots, \frac{\ell-1}{2}\}$ with $t_\ell \equiv \pm t \bmod \ell$.

c) Use the above to prove the existence of an improved variant of Schoof's algorithm, provided the knowledge of a polynomial $G|g$.

Projects for the Lecture on Computational Number Theory

Preda Mihăilescu

Exercise 1 (Schoof-Elkies).

Implement the Schoof-Elkies algorithm on a computer, using some Symbolic Computation package of your choice (Magma, PARI, Mathematica, MAPLE, etc.). For determining the polynomial $G(X)$ in exercise 8, you need not use automorphic functions (but those who do are welcome!). You can instead construct the division polynomials ψ_ℓ recursively, let $\hat{X} = X + (\psi_\ell)$ and $h(X) \equiv X^p \bmod \psi_\ell(X)$. Then retrieve the gcd $(h(X), \psi_\ell(X))$. Explain why this approach works and provide a description of the implementation. The algorithm should be first tested on some small primes p, and then compute $E(\mathbb{F}_p)$ for some curves over fields with characteristic of, say, 1000 binary digits.

Exercise 2 (Division Polynomials). Give a complete solution of exercises 4 and 5.

Exercise 3 (Complex multiplication). It was mentioned that if the lattice L has CM by α, then there are polynomials $A(X), B(X)$ with $\deg(A) = \deg(B) + 1 = N(\alpha)$ such that $\wp(\alpha z) = \frac{A(\wp(z))}{B(z)}$.

1. Choose three CM curves and complex multiplyers and determine the respective polynomial A, B (the α-division polynomials.
2. Attempt to find a general solution using induction, like for the case of integer multiplication. **Hint**: Do some literature research before attempting to solve this part of the problem.

Exercise 4 (Kronecker's Jugendtraum).

For this Project you are advised to use Cox's book given in the reference. The solutions should reflect your understanding of the subject, so it should contain more than a list of references to results proved in a book. Think of it as a small essay (Cambridge style, not literature!).

Let $L = [1, \tau] \subset \mathbb{C}$ be a CM - lattice with $\alpha L \subset L, \alpha \in C \setminus \mathbb{Z}$

1. Show that there is an imaginary quadratic extension $\mathbb{K} = \mathbb{Q}[\sqrt{-d}]$ such that $\tau, \alpha \in \mathbb{K}$.
2. Let $\mathcal{O} \subset \mathcal{O}(\mathbb{K})$ be the smallest subring with $\alpha \in \mathcal{O}$. Show that $\beta L \subset L$ for all $\beta \in \mathcal{O}$.
3. Show that there is a proper fractional ideal $\mathfrak{a} \subset \mathcal{O}$ such that the $\mathbb{Z}$-module $[1, \tau] \subset \mathcal{O}$ is equal to $\mathfrak{a}$. Conclude that the j-function parametrizes the group of classes of proper ideals in $\mathcal{O}$.
4. Prove that $j(\mathfrak{a}) = j(\tau)$ is an algebraic number. **Hint**: Use the modular equation.
5. Prove that $\mathbb{H} = \mathbb{K}[j(\mathfrak{a})]$ is the class field of the group of classes of proper ideals (ring class group) of $\mathcal{O}$. This is the first step in the proof of Kronecker's Jugendtraum.