Final Exam. 2006 December 19th, 14h – 18h.

Handwritten lecture notes are allowed as well as the course typescript. You may compose in either English or French.

Exercise I (Beyond Pocklington)

Let $N > 1$ be an integer, such that $N - 1 = FU$, where F and U are two integers such that the decomposition of F into primes is known. Assume that the local conditions of Pocklington's theorem are satisfied, *i.e.* any divisor d of N satisfies $d \equiv 1 \pmod F$. We assume further that

$$N^{1/3} \leqslant F < N^{1/2}.$$

We shall find an efficient test that still allows to certify that N is prime.

1) Prove that the base-F decomposition of N is of the form $c_2F^2 + c_1F + 1$.

2) In this question we assume that N is composite.

a) Show that N has exactly two prime divisors (possibly equal), of the form $p = aF + 1$, $q = bF + 1$, for positive integers a and b. We can assume that $a \leqslant b$.

b) Prove that $ab \leqslant F - 1$. Hence $a + b \leqslant F - 1$ *or* ($a = 1$ and $b = F - 1$).

c) Show that the latter case is in fact impossible; hence that $c_1 = a+b$, $c_2 = ab$.

3) Prove that N is prime *if and only if* $c_1^2 - 4c_2$ is not a square in $\mathbb{Z}$.

Exercise II (Primes as sums of squares)

Let p be a prime number congruent to 1 mod 4, which implies that p is a sum of two integer squares. Choose an integer r such that $r^2 + 1 \equiv 0 \pmod p$ and $0 < r < p$, then let $\Lambda \subset (\mathbb{R}^2, \|\cdot\|_2)$ the lattice generated by the two vectors $(p, 0)$ and $(r, 1)$.

1) Prove that for all $(a, b) \in \Lambda$, we have $a^2 + b^2 \equiv 0 \pmod p$.

2) Show that there exists a non-zero $(a, b) \in \Lambda$ such that $a^2 + b^2 \leqslant (4/\pi)p$. Prove that in fact $a^2 + b^2 = p$.

3) Prove that the first vector (a, b) in an LLL-reduced basis for Λ also satisfies $a^2 + b^2 = p$.

4) Given a prime p (as a string of digits in a fixed basis), show that it can be written as a sum of two squares $p = a^2 + b^2$ in randomized polynomial time. Compare with the naive algorithm, trying all values (a, b) in a suitable range.

★ **5)** p is now an arbitrary prime, possibly 2 or congruent to $3 \pmod 4$.

a) Show there exist r and s such that $r^2 + s^2 + 1 \equiv 0 \pmod p$.

b) Propose an algorithm to find such a pair (r, s). What is its complexity ? [*You may assume the GRH and use Bach's result.*]

c) Using the lattice generated by $(p, 0, 0, 0)$, $(0, p, 0, 0)$, $(r, s, 1, 0)$ and $(s, -r, 0, 1)$ in $\mathbb{R}^4$, prove that every prime is the sum of four squares. Do we obtain a polynomial time algorithm?

Problem (Point counting, the Shanks-Mestre algorithm)

Let $p > 2$ be a prime and $E : y^2z = x^3 + axz^2 + bz^3$ an elliptic curve over $\mathbb{F}_p$, with neutral element $O_E = (0 : 1 : 0)$. We write χ for the Legendre symbol, i.e. the quadratic character of $\mathbb{F}_p^*$, and choose g a quadratic non-residue. We define $E' : gy^2z = x^3 + axz^2 + bz^3$, the quadratic twist of E. For $P \in E(\mathbb{F}_p)$ and $n \in \mathbb{Z}_{\geqslant 0}$ we write $[n]P$ for the sum $P + \cdots + P$, with n summands. You may assume that adding two points in $E(\mathbb{F}_p)$ is done in time $O(\log p)^2$.

1)a) Noting that $1 + \chi(x) = \#\{y \in \mathbb{F}_p \colon y^2 = x\}$, prove that

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 + ax + b)$$

Show that this formula computes $\#E(\mathbb{F}_p)$ in time $\widetilde{O}(p)$.

b) Prove that $\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2p + 2$.

2) A theorem of Mestre [*taken for granted: do not try to prove this*] asserts that if $p > 457$, there exists a point of order $> 4\sqrt{p}$ on at least one of E, E'.

a) Suppose the largest order of an element in a finite abelian group G is m. Show that the proportion of elements of G with order m is at least $\varphi(m)/m$, where φ is Euler's totient function. [*Use elementary divisors.*]

b) Assuming $p > 457$, choose a pair of points (P, P') on $E(\mathbb{F}_p) \times E'(\mathbb{F}_p)$ uniformly at random. Prove that at least one of P or P' has order larger that $4\sqrt{p}$, with probability larger than $C/\log\log p$ for some absolute constant C.
[*You may assume that $\varphi(m)/m > c/\log\log(m)$ for some absolute constant c and all integers $m \geqslant 3$. You can try and prove this fact if you are familiar with analytic number theory: $\varphi(m)/m$ is smallest when $m = p_1 \dots p_r$, where p_i denotes the i-th prime.*]

3) Let S a totally ordered set, and two lists $A = (a_i)_{i<m}$ and $B = (b_j)_{j<n}$ of elements of S, with $m, n \leqslant N$. Explain how to find $A \cap B$ using $O(N \log N)$ comparisons.

4) Let $P \in E(\mathbb{F}_p)$.

a) Prove that there exists $w \in \mathbb{Z}$, $|w| < 2\sqrt{p}$ such that $[p + 1 - w]P = O_E$.

b) Let $B = \lceil (4\sqrt{p})^{1/2} \rceil$. Show that the two lists of points

$$\{[p + 1 - a]P \colon 0 \leqslant a < B\}, \quad \{[Bb]P \colon 0 \leqslant b \leqslant B\}$$

have non-empty intersection. [*Write w in base B.*]

c) Write an algorithm to find such a w given P, in time $\widetilde{O}(p^{1/4})$.

d) Assuming that the order of P is larger than $4\sqrt{p}$, show that

$$\#E(\mathbb{F}_p) = p + 1 - w.$$

5) Propose a randomized algorithm computing $\#E(\mathbb{F}_p)$ in time $\widetilde{O}(p^{1/4})$.