Université Bordeaux 1 | MAT913 – Master
Mathématiques | Année 2012–2013

Final Exam. 2007 December 11th, 14h – 18h.

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

Exercise (Square roots mod p)

Given p an odd prime and $a \in (\mathbb{F}_p^*)^2$, we wish to compute a square root of a. Let $t \in \mathbb{F}_p$ be given such that $t^2 - a$ is not a square in $\mathbb{F}_p$, and let $X \in \mathbb{F}_{p^2}$ a square root of $t^2 - a$.

1) Prove that such a t exists.

2) Prove that $(t+X)^{p+1} = (t-X)(t+X) = a$.

3) Noting that $p+1$ is even, write a formal algorithm computing a square root of a, given t, a and p.

4) Bound the complexity of your algorithm, neglecting the time needed to find t.

Note. The following argument, introducing the Jacobi sum $J(\chi,\chi)$, where χ is the Legendre symbol, shows that the number of suitable t in $\mathbb{F}_p$ is $(p-1)/2$:

$$\begin{aligned}\#\left\{t \in \mathbb{F}_p \colon t^2 - a \in (\mathbb{F}_p)^2\right\} &= \frac{1}{2}\#\left\{t \colon t^2 - a = 0\right\} + \frac{1}{2}\sum_t (1 + \chi(t^2 - a)) \\ &= 1 + p/2 + \chi(-1)J(\chi,\chi)/2 = (p+1)/2.\end{aligned}$$

5) Propose a randomized algorithm to find t and update your complexity estimate. [*You may use the Note above.*]

Problem (Dedekind's criterion)

Let $K = \mathbb{Q}[X]/(T)$ a number field, where $T \in \mathbb{Z}[X]$ is monic. We write α for the class of X modulo T and let $\mathcal{O} = \mathbb{Z}[\alpha] = \mathbb{Z}[X]/(T)$. Given a prime p, we want to study the p-maximality of $\mathcal{O}$. We write $\overline{f}$ for the canonical projection of $f \in \mathbb{Z}[X]$ to $\mathbb{F}_p[X]$. Conversely, given $\overline{f} \in \mathbb{F}_p[X]$, we let f denote any lift to $\mathbb{Z}[X]$ of $\overline{f}$.

Let I_p the ideal of those $x \in \mathcal{O}$ that become nilpotent in $\mathcal{O}/p\mathcal{O}$, and

$$\mathcal{O}' := (I_p : I_p) = \{x \in K : xI_p \subset I_p\}.$$

We proved during the lectures that $\mathcal{O} = \mathcal{O}'$ if and only if $\mathcal{O}$ is p-maximal. We factor T over $\mathbb{F}_p[X]$, $\overline{T} = \prod_i T_i^{e_i}$ where the T_i are distinct monic irreducible polynomials, and define

$$\overline{f} = \prod T_i, \qquad \overline{g} = \overline{T}/\overline{f}, \qquad h = \frac{T - fg}{p}.$$

1) Show that $I_p/p\mathcal{O}$ is generated by $\overline{f}$; hence $I_p = p\mathcal{O} + f(\alpha)\mathcal{O}$.

2) Let $x \in \mathcal{O}'$, which we write in the form $x = \beta/p$, $\beta \in K$. We have $\beta = B(\alpha)$ for some $B \in \mathbb{Q}[X]$.

a) Show that $xp \in I_p$ if and only if $B \in \mathbb{Z}[X]$ and $\overline{f} \mid \overline{B}$ in $\mathbb{F}_p[X]$.

b) Show that $xf(\alpha) \in I_p$ if and only if $\overline{gk} \mid \overline{B}$, where $\overline{k} := \overline{f}/(\overline{h}, \overline{f})$. [*We must have* $Bf \in p^2\mathbb{Z}[X] + pf\mathbb{Z}[X] + T\mathbb{Z}[X]$. *Reduce mod* p *to prove* $\overline{g} \mid \overline{B}$, *then write* $B = pU + gV$ *and refine.*]

3) Let $\delta = \gcd(\overline{f}, \overline{g}, \overline{h})$ in $\mathbb{F}_p[X]$.

a) Show that $\gcd(\overline{f}, \overline{kg}) = \overline{k}\delta$, then $\operatorname{lcm}(\overline{f}, \overline{gk}) = \overline{T}/\delta$.

b) Let $U \in \mathbb{Z}[X]$ a lift of $\overline{T}/\delta$; prove that $\mathcal{O}' = \mathcal{O} + \frac{U(\alpha)}{p}\mathcal{O}$.

c) Prove that $[\mathcal{O}' : \mathcal{O}] = p^{\deg \delta}$.

d) Given p and T, estimate the complexity of the computation of $\mathcal{O}'$ in terms of relevant parameters. Prove that the algorithm is polynomial-time in terms of the size of the input. What about the space complexity ?

4) A monic polynomial $T \in \mathbb{Z}[X]$ has *Eisenstein type at* p if

$$T = f^k + ph,$$

where $f, h \in \mathbb{Z}[X]$, f monic, such that $\overline{f}$ is irreducible and $\overline{f} \nmid \overline{h}$ in $\mathbb{F}_p[X]$. Show that T is irreducible and that $\mathbb{Z}[X]/(T)$ is p-maximal.

5) Let $\ell \neq \pm 1$ a squarefree integer and $T = X^3 - \ell$.

a) Show that $K = \mathbb{Q}[X]/(T)$ is a number field of degree 3.

★ b) Noting that $\operatorname{disc} T = 27\ell^2$, compute the ring of integers $\mathbb{Z}_K$ of K. You should use the result from **4)** for all troublesome primes, except possibly 3. [*We find* $\mathcal{O} := \mathbb{Z}[X]/(X^3 - \ell) = \mathbb{Z}_K$ *if and only if* $\ell \not\equiv \pm 1 \pmod 9$. *For the remaining case, compute* $\mathcal{O}'$ *(the final part uses* $\mathbb{Z}$*-linear algebra to reduce a system of* 6 *generators to the needed* 3*).*]

6) Let A, B two sub $\mathbb{Z}$-modules of rank $\dim_{\mathbb{Q}} K = n$, given by a $\mathbb{Z}$-basis.

a) Give a formal algorithm to compute $(A : B)$.

b) Estimate its complexity in terms of relevant parameters.

c) Compare to what we obtained above for the computation of $\mathcal{O}' = (I_p : I_p)$ using Dedekind's method.