Elliptic curve cryptography, winter 2009

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

6. Exercise sheet
Hand in solutions until Monday, 07 December 2009, 23^{59}

Exercise 6.1 (Differentiation revised). (5 points)

Let $g\colon \mathbb{R} \to \mathbb{R},\ x \mapsto g(x)$, $h\colon \mathbb{R} \to \mathbb{R},\ x \mapsto h(x)$ and $f\colon \mathbb{R}^2 \to \mathbb{R},\ (g,h) \mapsto f(g,h)$ smooth functions. In the lecture we used the fact that

$$\frac{\mathrm{d}f}{\mathrm{d}x} = \frac{\mathrm{d}f}{\mathrm{d}g}\frac{\mathrm{d}g}{\mathrm{d}x} + \frac{\mathrm{d}f}{\mathrm{d}h}\frac{\mathrm{d}h}{\mathrm{d}x}.$$

(i) Deduce the above fact from the chain-rule $\frac{\mathrm{d}(\varphi\circ\psi)}{\mathrm{d}x} = \left(\frac{\mathrm{d}\varphi}{\mathrm{d}\psi}\circ\psi\right)\cdot\frac{\mathrm{d}\psi}{\mathrm{d}x}$. 3

(ii) Use the above fact for proving the product-rule $\frac{\mathrm{d}(g\cdot h)}{\mathrm{d}x} = g\frac{\mathrm{d}h}{\mathrm{d}x} + \frac{\mathrm{d}g}{\mathrm{d}x}h$. 2

Exercise 6.2 (An important endomorphism). (11 points)

Consider an elliptic curve E defined over the field $\mathbb{F}_q$. Let φ_{q^e} be the Frobenius endomorphism that maps a point (x,y) on E to (x^{q^e}, y^{q^e}) and consider the endomorphism $\alpha = \varphi_{q^e} - 1 \in \mathrm{End}(E)$.

(i) Describe the kernel of α. 3

(ii) Prove that α is separable. 2

(iii) Conclude the degree of α. 1

(iv) We can write $\alpha(x,y) = (r_1(x), r_2(x)y)$. Assume you know r_1. Express r_2 in terms of r_1. Hint: You need almost no further calculation to answer this! 2

Now consider the endomorphism $[n]$.

(v) Asssume $\gcd(n,q) = 1$ and you know polynomials ϕ_n, ψ_n such that $nP = (\frac{\phi_n}{\psi_n^2}, r_2(x)y)$. Show that you can now express $r_2 = \frac{n^{-1}q}{\psi^3}$ for some polynomial q. 3

Exercise 6.3 (An omitted calculation). (5 points)

During the proof in the lecture we considered an elliptic curve $E\colon y^2 = x^3 + ax + b$ with a point $P = (x, y)$ and a constant point $Q = (u, v)$ on it. Write $P + Q = (f(x, y), g(x, y))$ where f, g are rational functions in x and y with coefficients depending on u, v. Verify, using a computer algebra system of your choice, that considering y as a function of x defined by E we have 5

$$y\frac{\mathrm{d}}{\mathrm{d}x}f(x, y) - g(x, y) = 0.$$

Hint: Use the fact that $2yy' = 3x^2 + a$ and the curve equation.

Exercise 6.4 (Addon: the group stucture of singular cubics). (0+5 points)

+5 Consider the curve $E\colon y^2 = x^2(x - a)$ with $0 \neq a \in k$. Let $E_{ns}(k)$ be the nonsingular points on E with coordinates in k. Assume there is $\alpha \in k$ such that $\alpha^2 = a$. Show that the map

$$\tau\colon \begin{array}{ccc} E_{ns} & \longrightarrow & k^\times, \\ (x, y) & \longmapsto & \frac{y+\alpha x}{y-\alpha x} \end{array}$$

is an isomorphism from E_{ns} to $k^\times$ considered as a multiplicative group. Use a computer algebra system for side calculation.