Advanced cryptography: Pairing-based cryptography
winter term 2012/13

DANIEL LOEBENBERGER AND MICHAEL NÜSKEN

2. Exercise sheet
Hand in solutions until Monday, 05 November 2012, 23:59:59

Exercise 2.1 (Associativity). (0+7 points)

Show, using a computer algebra system of your choice, that the group law on elliptic curves in Weierstraß form as defined in the lecture is associative. That is given point P, Q, S on the curve, we have $(P+Q)+S = P+(Q+S)$. +7

Hint: Do not consider any special cases, i.e. assume that in all occuring additions we add affine points with $S \neq \pm T$.

Exercise 2.2 (Torsion). (5 points)

In class we considered the n-torsion of an elliptic curve E defined over $\mathbb{F}_q$ for $n = 2, 3$. In this exercise we will extend the results from the lecture: Prove by direct computations that in characteristic neither 2 nor 3 we have $E[4] \simeq \mathbb{Z}_4 \times \mathbb{Z}_4$. *Hint*: Consider points P with $2P = -2P$. 5

Exercise 2.3 (Torsion of arbitrary abelian groups). (7 points)

Let G be any (finite) additively written abelian group and denote by $G[n]$ the set of all points of order dividing m. Prove that if $n = a \cdot b$ with $\gcd(a, b) = 1$ then $G[n] \simeq G[a] \times G[b]$. *Hint*: Extended Euclidean Algorithm! 7

Exercise 2.4 (Endomorphisms). (6 points)

We now explore several constructions for morphisms from an elliptic curve $E\colon x^3 + ax + b$ over $\mathbb{F}_q$ to itself:

(i) Show that the map $-\colon E \to E,\ (x, y) \mapsto (x, -y)$ is a group homomorphism. Determine the size of its kernel. 1

(ii) Show that for each $k \in \mathbb{Z}$ the map $[k]\colon E \to E,\ P \mapsto [k]P$ is a group homomorphism. 1

(iii) Show that the Frobenius map $\varphi_q\colon E \to E,\ (x, y) \mapsto (x^q, y^q)$ is a group homomorphism. Determine the size of its kernel. Fact: The map $\varphi_q\colon \mathbb{F}_{q^k} \to \mathbb{F}_{q^k},\ x \mapsto x^q$ is a field automorphism. Its fixed points are exactly the elements of $\mathbb{F}_q$ and any automorphism of $\mathbb{F}_{q^k}$ fixing $\mathbb{F}_q$ is a power of φ_q (with exponent in $\mathbb{N}_{<k}$). 2

(iv) Show that for each $k \in \mathbb{Z}$ we have $\varphi_q \circ [k] = [k] \circ \varphi_q$. Hint: Do not try to find explicit formulae for kP! You may take as granted that for each k there are rational functions $r_1(x) \in k(x)$ and $r_2(x)y \in \mathbb{F}_q(x, y)$ such that for $P = (x_0, y_0)$ we have $[k]P = (r_1(x), r_2(x)y)$. 2

Exercise 2.5 (An alternate definition of the Weil pairing). (6+6 points)

Let E be an elliptic curve defined over a field k. In class we considered the Weil pairing $e\colon E[n] \times E[n] \to \mu_n,\ (Q, R) \mapsto e(Q, R)$. Goal of this exercise is to get a different insight in the properties of this pairing. We construct a pairing by first selecting an appropriate basis T_1, T_2 of $E[n]$ and a primitive nth root of unity ζ and require $e(T_1, T_2) := \zeta$. This leads to $e(a_1T_1 + a_2T_2, b_1T_1 + b_2T_2) =: \zeta^{a_1b_2 - a_2b_1} \in \mu_n$ by anticipating bilinearity and antisymmetry.

1 (i) Show that e is bilinear

1 (ii) and antisymmetric.

4 (iii) Show that e is nondegenerate.

+6 (iv) Prove that e is Galois compliant: $e(\sigma S, \sigma T) = \sigma(e(S, T))$.