Advanced Cryptography: Algorithmic Cryptanalysis

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

12. Exercise sheet
Hand in solutions until Saturday, 09 July 2011, 23:59h.

To estimate the average effort you put into solving the following exercises, please add after each exercise the amount of time you spent for it.

Exercise 12.1 (smooth numbers and index calculus). (14 points)

In the first part of this exercise, consider the factor base $\mathcal{B} = \{2, 3, 5, 7, 11\}$ consisting of the first five prime numbers.

We want to get a feeling for the probability that a randomly chosen number in the range from 1 to 1000 factors over $\mathcal{B}$, i.e. is B-*smooth*.

(i) In a loop, draw random integers between 1 and 1000. Test whether they factor over $\mathcal{B}$ (note that no complete factorization is required for this). Repeat until you have found 20 B-smooth numbers. The fraction $20/i$, where i is the total number of performed iterations, is an estimate for the fraction of B-smooth numbers among the integers between 1 and 1000. What is yours? 3

In the second part, we want to see the index calculus in action. We are interested in the multiplicative group $G = \mathbb{Z}_p^\times$ with $p = 227$ and generator $g = 2$. We choose as factor base $\mathcal{B} = \{2, 3, 5, 7, 11\}$ with all primes up to the bound $B = 11$.

In the preprocessing step we compute the discrete logarithms of all elements in the factor base $\mathcal{B}$.

(ii) Instead of randomly choosing exponents e and testing, whether $g^e \mod p$ factors over $\mathcal{B}$, we have already prepared a list with suitable exponents for you. Let e take values from $\{40, 59, 66\}$, give the factorization of $g^e \mod p$ over $\mathcal{B}$ and the corresponding linear congruence modulo $(p-1)$ involving the discrete logarithms of the elements in $\mathcal{B}$. 3

(iii) The discrete logarithm of the generator $g = 2$ is obviously 1, but even with this information, the three linear relations from (ii) are not enough to determine the remaining four unknown discrete logarithms. Find one additional linear congruence from an exponent $e > 10$ yourself. 2

(iv) Assuming that your additional congruence is linearly independent from the three previous ones, solve the system of congruences for the discrete logarithms of the base elements. (If you do this by hand, note that division by 2 is impossible modulo $(p-1)$. If you use a computer algebra system, note that those are aware of this problem and have special commands to solve systems of congruences with a given module, e.g. `msolve` in MAPLE, `solve_mod` in SAGE and `LinearSolve[A, b, Modulus -> m]` in MATHEMATICA.) 3

Once we have found the discrete logarithms for the elements in the factor base, we can finally compute the discrete logarithm of any element x in the group with the following method:

- Choose random exponents e until $xg^e \mod p$ factors over $\mathcal{B}$, say $xg^e \equiv p_1^{\beta_1} p_2^{\beta_2} \cdots p_h^{\beta_h}$.
- The corresponding linear relation reads

$$\mathrm{d}\ell\mathrm{og}_g\, x + e = \beta_1\, \mathrm{d}\ell\mathrm{og}_g\, p_1 + \beta_2\, \mathrm{d}\ell\mathrm{og}_g\, p_2 + \cdots + \beta_h\, \mathrm{d}\ell\mathrm{og}_g\, p_h \mod (p-1)$$

- Since all the $\mathrm{d}\ell\mathrm{og}_g\, p_i$ have already been determined in the preprocessing step, you can solve this equation modulo $(p-1)$ for $\mathrm{d}\ell\mathrm{og}_g\, x$.

3 (v) Apply this procedure to compute $\mathrm{d}\ell\mathrm{og}_2\, 224$ in $\mathbb{Z}_{227}^\times$.

Exercise 12.2. (3 points)

3 The polynomial

$$f(x, y) = y^2 - x^3 - ax - b$$

defines a curve in the x-y-plane via the equation $f(x, y) = 0$. Show that the curve has a well-defined tangent vector in every point on the curve, i.e. the curve is *smooth*, if and only if

$$4a^3 + 27b^2 \neq 0.$$

Hint: Consider the inequality $\left(\frac{\partial f(x,y)}{\partial x}, \frac{\partial f(x,y)}{\partial y}\right)\Big|_P \neq (0, 0)$ for the tangent vector in the point $P = (u, v)$.

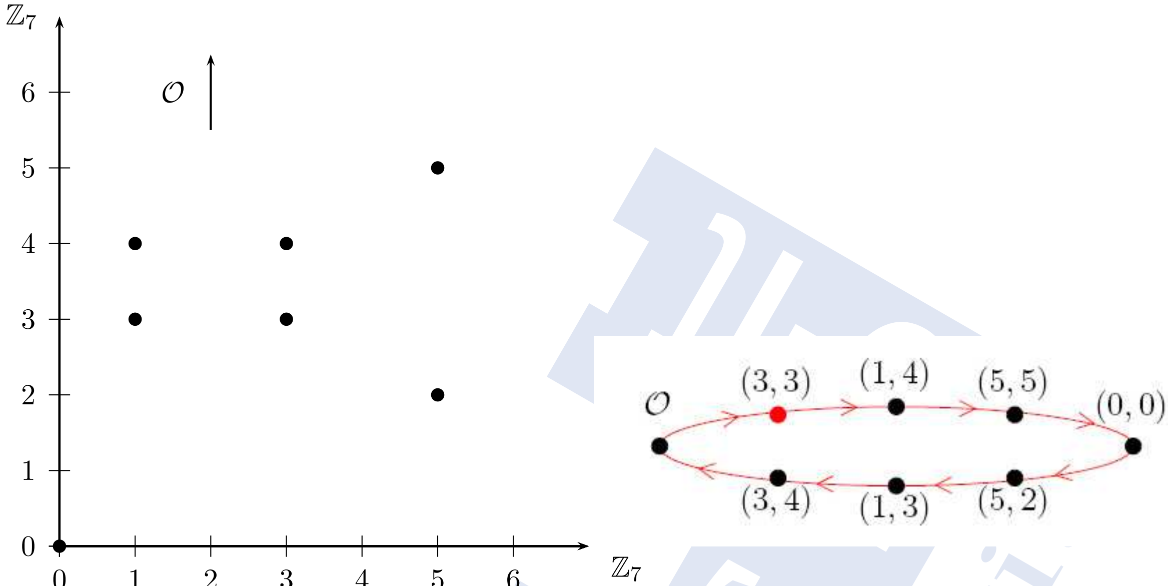

Figure 12.1: Graph and diagram for the group structure of E

Exercise 12.3. (9 points)

Consider the example $E = \{(u, v) \in \mathbb{Z}_7^2 : v^2 = u^3 + u\} \cup \{\mathcal{O}\}$ for an elliptic curve over $\mathbb{Z}_7$ (see Figure 12.1).

2 (i) Let $P = (5, 5)$. Determine $S = 2 \cdot P$ and $T = 5 \cdot P$ from the diagram on the right of Figure 12.1.

The addition of two distinct points corresponds to a secant of the graph. The doubling of a point corresponds to a tangent to the graph.

(ii) Draw the tangent corresponding to $S = 2 \cdot P$ into the graph on the left of Figure 12.1. 2

(iii) Determine $S + T$ from the graph on the left and check your result by doing the same computation in the diagram on the right. 1

Alice and Bob heard about the cryptographic applications of elliptic curves. They want to perform a Diffie-Hellman key exchange using the elliptic curve E from above.

(iv) List all possible generators for the cyclic group E. 1

Alice and Bob publicly agree on the generator P from above. The secret key of Alice is 3 and the secret key of Bob is 4.

(v) Which messages are exchanged over the insecure channel and what is Alice's and Bob's common secret key? 3