Number theory in cryptography

– Exercise set 11 –

The exercises T11.4, P11.1 have to be handed in on Tuesday, 14th May 2024, 8:30 at latest. (You can submit P11.1a) via Moodle).

Theoretical questions

T 11.1 Suppose that a cubic curve E over a field k of characteristic other than 2 or 3 is given by the reduced Weierstrass equation $y^2 = x^3 + Ax + B$.

a) Show that E is smooth if and only if the quantity $\Delta = -16(4A^3 + 27B^2)$ is non-zero. Note: of course the exercise would be true without the -16, but the particular quantity Δ we have written, called the *discriminant* of the Weierstrass equation, is an important invariant.

b) If $k = \mathbb{Q}$ and $p \neq 2, 3$ is a prime, we say that a reduced Weierstrass equation with coefficients in $\mathbb{Q}$ has good reduction at p if p does not divide the denominator of A or B and if the equation $y^2 = x^3 + Ax + B$ defines a smooth curve over $\mathbb{F}_p$. Assuming that E is smooth (i.e. is an elliptic curve), show that the set of primes where the Weierstrass equation does not have good reduction is finite.

T 11.2 The *zeta function* of an elliptic curve $E/\mathbb{F}_q$ is defined as the power series in $\mathbb{Q}[[T]]$ given by

$$Z(T, E/\mathbb{F}_q) := \exp\Big(\sum_{r \geqslant 1} N_r \frac{T^r}{r}\Big),$$

where $N_r := \#E(\mathbb{F}_{q^r})$. The French mathematician André Weil proved that in fact the zeta function is a rational function

$$Z(T, E/\mathbb{F}_q) = \frac{1 - a_q T + qT^2}{(1-T)(1-qT)},$$

where $a_q = N_1 - q - 1$ satisfies the Hasse bound.

a) Prove that the zeroes of the zeta function are complex conjugate of absolute value q^{-s} with $s = \frac{1}{2}$. Note: you should think of this as a Riemann Hypothesis in this setting!

b) The zeta function encodes data about all the cardinalities N_r. Writing the numerator of $Z(T, E/\mathbb{F}_q)$ as $(1 - \alpha T)(1 - \beta T)$, show that:

$$N_r = q^r + 1 - \alpha^r - \beta^r.$$

(Hint: take log derivatives of the two formulas for zeta).

c) Compute N_r for the so-called *Koblitz curves* defined over $\mathbb{F}_2$ by

$$y^2 + xy = x^3 + ax^2 + 1 \quad \text{for} \quad a \in \mathbb{F}_2.$$

T 11.3 Consider the lattice $L \subset \mathbb{R}^2$ generated by $a := (11, 9)$ and $b := (7, 6)$. Does $v := (1, 2)$ belong to L? Does $w := (-1, 0)$ belong to L?

T 11.4 We are going to use lattices to prove a special case of the following result.

Theorem 11.4.1 (Lagrange). *Every integer $n \geqslant 0$ is the sum of 4 squares of integers, that is: there exist $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ such that $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$.*

Namely, we will prove this result in the case where $n = p$ is an odd prime[2].

a) Prove that there exist integers $a, b \in \mathbb{Z}$ such that $a^2 + b^2 + 1 \equiv 0 \bmod p$. Hint: how many squares are there in $\mathbb{F}_p$? You may want to use T10.1.

b) Fix $a, b \in \mathbb{Z}$ as above. Let $L \subset \mathbb{Z}^4 \subset \mathbb{R}^4$ be the lattice generated by the vectors

$$v_1 = (p, 0, 0, 0), \quad v_2 = (0, p, 0, 0), \quad v_3 = (a, b, 1, 0), \quad v_4 = (b, -a, 0, 1).$$

Check that $\|v\|^2$ is a multiple of p for every $v \in L$.

c) Using Minkowski's theorem (theorem 9.2.3 in the lecture notes), prove that there exists a vector $u \in L \setminus \{0\}$ of norm $\|u\| < \sqrt{2p}$ and conclude that p is the sum of 4 squares of integers.

Programming exercises

P 11.1 This exercise treats the digital signature scheme ECDSA, which you probably use daily while browsing the internet and https websites! Here are the steps (just as in DSA):

- **Public parameter creation:** A trusted party chooses an elliptic curve E over $\mathbb{F}_p$ and a point P of large prime order q in $E(\mathbb{F}_p)$.
- **Key creation:** Sarah chooses a secret signing key $1 \leqslant a \leqslant q-1$ and computes and publishes the verification key $A = aP$.
- **Signature:** Sarah chooses a document $D \in \mathbb{Z}/q\mathbb{Z}$ (e.g., a hashed message) and a random integer k mod q. She computes $kP \in E(\mathbb{F}_p)$ and then publishes the signature $D^{\mathrm{sig}} = (S_1, S_2)$ given by:

$$S_1 \equiv x(kP) \bmod q, \qquad S_2 \equiv (D + aS_1)k^{-1} \bmod q.$$

- **Verification:** To verify the signature, Victor computes

$$V_1 = DS_2^{-1} \bmod q, \qquad V_2 = S_1 S_2^{-1} \bmod q$$

and checks that $x(V_1P + V_2A) \mod q = S_1$. (Here $x(Q)$ denotes the x-coordinate of a point $Q = (x(Q), y(Q))$ on E, and $x(Q) \bmod q$ means that we take the smallest positive representative of $x(Q) \in \mathbb{F}_p$ in $\{0, ..., p-1\} \subset \mathbb{Z}$ and then reduce it mod q).

a) Show that the verification step indeed succeeds if Sarah signed the document.

b) Consider the following data given below[3]. Using SAGE, check $qP = O_E$ and that q is indeed a prime number. Then verify that $D^{\mathrm{sig}} = (S_1, S_2)$ is a valid signature for the document D and the verification key A, knowing that $0 < \mathtt{int}(y(P)), \mathtt{int}(y(A)) < p/2$.

$$E : y^2 = x^3 - 3x + b \qquad \text{over } \mathbb{F}_p, \qquad p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1,$$

$$b = 27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575$$

$$x(P) = 9927569721545390815034713904622759727440640009568502331607218669906608389108530937089042810199441312117717067185412$$

$$q = 39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643$$

$$x(A) = 29400003852608672639867349879251432905099128866639045860503309429241268278901837643832541859075556345862458834761765$$

$$D = 1415574695691915124168896603027864661322838868352349273945839601722462604573059900203151158258340990168334336$$

$$S_1 = 13669797451316206272209337753571017954169997281397226685068093299839322753638412752144616602545722591906382790482469$$

$$S_2 = 22724282496840316001698707302101306704785167815942863432725566208290642414916361973166625614388772211458477112104622$$

[2]The general case can be deduced from there, using the fact that the set $\{ x_1^2 + x_2^2 + x_3^2 + x_4^2 \ : x_i \in \mathbb{Z} \} \subset \mathbb{Z}$ is closed under multiplication.

[3]The elliptic curve E is known as P-384, from the curves "recommended for U.S. Government Use" by the NIST. (See also `http://safecurves.cr.yp.to/rigid.html`).