Notes: This exam consists of 5 exercises. You have from 14:00 – 17:00 to solve them. You can reach 50 points.
Make sure to justify your answers in detail and to give clear arguments. Document all steps, in particular of algorithms; it is not sufficient to state the correct result without the explanation. If the problem requires usage of a particular algorithm other solutions will not be accepted even if they give the correct result.
All answers must be submitted on TU/e letterhead; should you require more sheets ask the proctor. State your name on every sheet.
Do not write in red or with a pencil.
You are allowed to use any books and notes, e.g. your homework. You are not allowed to use the textbooks of your colleagues.
You are allowed to use a simple, non-graphical pocket calculator. Usage of laptops and cell phones is forbidden.
1. This exercise is about groups. Let \( S := \{(a, b) \in \mathbb{Z}^2 \mid 2a + 3b \in 7\mathbb{Z}\} \).

(a) We define an operation \( \circ \) on elements of \( S \) as follows:
\[
(a_1, b_1) \circ (a_2, b_2) = (a_1 + a_2, b_1 + b_2).
\]
Show that \( (S, \circ) \) is a commutative group.  

(b) We define a different operation \( \diamond \) on \( S \) as follows:
\[
(a_1, b_1) \diamond (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).
\]
Investigate whether \( (S, \Diamond) \) forms a group.

2. This exercise is about polynomials over \( \mathbb{F}_2 \).

(a) Compute the number \( N_2(4) \) of irreducible polynomials of degree 4 over \( \mathbb{F}_2 \).  

(b) Let \( f(x) = x^4 + x^3 + 1 \) be a polynomial in \( \mathbb{F}_2[x] \). Compute \( \gcd(x^2 + x, f(x)) \) and \( \gcd(x^2 + x, f(x)) \).

(c) Use the Miller-Rabin test to show that \( f \) is irreducible over \( \mathbb{F}_2 \); you can use part b).

(d) State the product of the other irreducible polynomials of degree 4 over \( \mathbb{F}_2 \) using the results from the previous parts.

3. The integer \( p = 41 \) is prime and \( \mathbb{F}^*_41 = \langle 6 \rangle \). Alice uses the multiplicative group \( \mathbb{F}^*_41 \) with generator \( g = 6 \) as basis of a discrete-logarithm based system and has published her public key \( g_A = 30 \). Use the Pohlig-Hellman algorithm to compute an integer \( a \) so that \( g_a = g_A \) in \( \mathbb{F}^*_41 \). You can use that \( 6^{-1} = 7 \) and \( 6^{-2} = 8 \) in this group.

4. (a) Find all affine points on the twisted Edwards curve 
\[-x^2 + y^2 = 1 + 5x^2y^2 \text{ over } \mathbb{F}_{11}.\]

(b) Verify that \( P = (9, 3) \) and \( Q = (9, 8) \) are on the curve. Compute \( [2]P + Q \) in affine coordinates.
5. The Elliptic Curve Digital Signature Algorithm works as follows: The system parameters are an elliptic curve \( E \) over a finite field \( \mathbb{F}_p \), a point \( P \in E(\mathbb{F}_p) \) on the curve, the number of points \( n = |E(\mathbb{F}_p)| \), and the order \( \ell \) of \( P \). Furthermore a hash function \( h \) is given along with a way to interpret \( h(m) \) as an integer.

Alice creates a public key by selecting an integer \( 1 < a < \ell \) and computing \( P_A = [\ell]P \); \( a \) is Alice’s long-term secret and \( P_A \) is her public key.

To sign a message \( m \), Alice first computes \( h(m) \), then picks a random integer \( 1 < k < \ell \) and computes \( R = [k]P \). Let \( r \) be the \( x \) coordinate of \( R \) considered as an integer and then reduced modulo \( \ell \); for primes \( p \) you can assume that each field element of \( \mathbb{F}_p \) is represented by an integer in \([0, p-1]\) and that this integer is then reduced modulo \( \ell \). If \( r = 0 \) Alice repeats the process with a different choice of \( k \). Finally, she calculates

\[
s = k^{-1}(h(m) + r \cdot a) \mod \ell.
\]

If \( s = 0 \) she starts over with a different choice of \( k \).

The signature is the pair \((r, s)\).

To verify a signature \((r, s)\) on a message \( m \) by user Alice with public key \( P_A \), Bob first computes \( h(m) \), then computes \( w \equiv s^{-1} \mod \ell \), then computes \( u_1 \equiv h(m) \cdot w \mod \ell \) and \( u_2 \equiv r \cdot w \mod \ell \) and finally computes

\[
S = [u_1]P + [u_2]P_A.
\]

Bob accepts the signature as valid if the \( x \) coordinate of \( S \) matches \( r \) when computed modulo \( \ell \).

(a) Show that a signature generated by Alice will pass as a valid signature by showing that \( S = R \). [3 points]

(b) Show how to obtain Alice’s long-term secret \( a \) when given the random value \( k \) for one signature \((r, s)\) on some message \( m \). [3 points]

(c) You find two signatures made by Alice. You know that she is using an elliptic curve over \( \mathbb{F}_{1009} \) and that the order of the base point is \( \ell = 1013 \). The signatures are for \( h(m_1) = 345 \) and \( h(m_2) = 567 \) and are given by \((r_1, s_1) = (365, 448)\) and \((r_2, s_2) = (365, 969)\). Compute (a candidate for) Alice’s long-term secret \( a \) based on these signatures, i.e. break the system. [6 points]