Problems

▪ On the discrete logarithm system

Problem 1.1^M
Users A and B want to use the Diffie-Helleman to fix a common key over a public channel. They use GF(p), with $p = 541$ and primitive element α=2.
User B makes $c_B = 123$ public. If $m_A = 432$, what will be the common key $k_{A,B}$ that A and B use for their communication?

Problem 1.2^M
Demonstrate the special caase version of the Pohlig-Helmann algorithm, that computes logarithms in finite fields of size $q = 2^n + 1$, by evaluating $\log_3(142)$ in GF(257).

Problem 1.3^M
Find a solution of $\log_{44} 55$ in GF(197) by means of the Baby-Step Giant Step method, when only 15 field elements can be stored.

Problem 1.4^M
Check that $\alpha = 662$ is a primitive 2003-th root of unity in GF(4007) (note that 4007 is a prime number). Let G be the multiplicative subgroup G of order 2003 in GF(4007) generated by α.
Check that 2124 is an element of G.
Determine $\log_{662} 2124$ by the Pollard-ρ method.

Problem 1.5^M
Check that $g = 996$ is a generator of the multiplicative group $\mathbb{Z}_{4007}^*$. Set up the index-calculus method with a factor base of size 6 and determine $\log_{996} 1111$.

▪ On elliptic curve cryptosystems

Problem 2.1 ^{M}
How many points lie on the elliptic curve defined by the equation $y^2 = x^3 + \alpha x + 1$ over $GF(2^4) = GF(2)[\alpha] / (1 + \alpha^3 + \alpha^4)$?

Problem 2.1
Find the intersection points over $\mathbb{Z}_{31}$ of the lines $y = 4x + 20$ and $y = 4x + 21$ with the elliptic curve $y^2 = x^3 + 25x + 10$.

Problem 2.3 ^{M}
Consider the elliptic curve $\mathcal{E}$ defined by $y^2 = x^3 + 11x^2 + 17x + 25$ over $\mathbb{Z}_{31}$.
Check that the points $P = \{12, 10\}$ and $Q = \{25, 14\}$ lie on $\mathcal{E}$. What is $-P$? Compute the sum of P and Q without using the *Mathematica* procedure presented before.

Problem 2.4 ^{M}
Consider (again) the elliptic curve $\mathcal{E}$ defined by $y^2 = x^3 + 11x^2 + 17x + 25$ over $\mathbb{Z}_{31}$.
Determine the orders of $P = \{27, 10\}$ and $Q = \{24, 28\}$. What can you conclude about the cardinality of $\mathcal{E}$?

What is the cardinality of $\mathcal{E}$?
Construct a point of maximal order from P and Q.