Lecture #3 Exercises

Distributed Lab

August 1, 2024

Exercise 1. Oleksandr decided to build $\mathbb{F}_{49}$ as $\mathbb{F}_7[i]/(i^2+1)$. Compute $(3+i)(4+i)$.

As a result, you would get $a+bi$. Write down $a+b$ as an answer.

Exercise 2. Suppose we build an extension $\mathbb{F}_{p^3} := \mathbb{F}_p[v]/(v^3+1)$. For which of the following values p such construction would not be valid? (you can assume that listed numbers are primes)

a) 8431.

b) 9173.

c) 9419.

d) 6947.

Exercise 3. This question demonstrates the concept of so-called *tower of extensions*. Suppose we want to build an extension field $\mathbb{F}_{p^4}$. Of course, we can find some irreducible polynomial $\mu(X)$ of degree 4 over $\mathbb{F}_p$ and build $\mathbb{F}_p[w]/(\mu(X))$. However, we can also build it as $\mathbb{F}_{p^2}[u]/(\nu(u))$ where $\nu(u)$ is an irreducible polynomial of degree 2 over $\mathbb{F}_{p^2}$.

Exercise 3. Suppose that elliptic curve is defined as $E/\mathbb{F}_7 : y^2 = x^3 + b$. Suppose $(2, 3)$ lies on the curve. What is the value of b?

Exercise 4. Consider an elliptic curve E over $\mathbb{F}_{167^2}$. Denote by r the order of the group of points on E (that is, $r = |E|$). Which of the following **can** be the value of r?

a) $167^2 - 5$

b) $167^2 - 1000$

c) $167^2 + 5 \cdot 167$

d) 170^2

e) 160^2

Exercise 5. Suppose that for some elliptic curve E the order is $|E| = qr$ where both q and r are prime numbers. Among listed, what is the most optimal complexity of algorithm to solve the discrete logarithm problem on E?

a) $O(qr)$

b) $O(\sqrt{qr})$

c) $O(\sqrt{\max\{q, r\}})$
d) $O(\sqrt{\min\{q, r\}})$
e) $O(\max\{q, r\})$

Exercise 6. Sum of which of the following pairs of points on the elliptic curve $E/\mathbb{F}_{11}$ is equal to the point at infinity $\mathcal{O}$?

a)