NIE-MPI: Tutorial 7

created: October 26, 2022, 11:15

7.1 Discrete logarithm and Crytpography

Exercise 7.1. Solve

$$5^x \equiv 12 \pmod{23}.$$

Exercise 7.2. Alice wants to send a secrete message to Bob during a MPI lecture[1]. So she sends a small paper to Bob via her classmates saying this:

> Hi Bertíku, I'm gonna send you a secrete message using Diffie-Hellman protocol. My public key is $(29, 8)$ and the encrypted stuff is 24.

Bob's answer is:

> Cool Alenko! Mine is 15.

Alice:

> Super cool! Assuming that our shared secret number is n, let us meet on the $(n - 2 \mod 7)$-th day of next week at $(n - 7 \mod 24)$ o'clock in the pub in front of Building number $(2n + 42 \mod 10)$. See ya!

Where and when are they going to meet? Would it be easier to answer if you knew Alice's (or Bob's) private key?

7.2 Rings and fields

Exercise 7.3. Which of the following sets, together with the classical addition and multiplication, forms a ring or a field?

(a) The set of all even numbers.

(b) The set of all odd numbers.

(c) The set of non-negative even numbers.

(d) The set of rational numbers.

Exercise 7.4. Is $(\mathbb{R}^{n,n}, +, \cdot)$, i.e., the set of $n \times n$-matrices with matrix multiplication and addition, a ring? Is it a field? If not, how can we change it to get a field?

[1] Forgetting that the professor knows the trick too.

7.3 Finite fields of order p^n

Exercise 7.5. Find the Cayley table for both operations in the field $GF(2^2)$, where the multiplication is done modulo $x^2 + x - 1$. Find neutral elements and generators in the additive group and the multiplicative group of this field. Find also the inverses, for both sum and product, of $x + 1$ and x.

Exercise 7.6. Find the Cayley tables (both for addition and for multiplication) for $GF(3^2)$, where the multiplication is done mod $x^2 - x - 1$.

Exercise 7.7. Find all irreducible polynomials of degree less than 5 over the ring $\mathbb{Z}_2[x]$.

Exercise 7.8. Consider the field $GF(2^3)$, where the multiplication is done mod x^3+x+1.

(a) Decide whether $x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$.

(b) Find the inverse of 010.

(c) Calculate

$$100 \cdot (010)^{-1} + 010 \cdot 010.$$

Exercise 7.9. In the field $GF(3^3)$ with multiplication modulo $x^3 + 2x + 1$ find

(a) the inverse of 122,

(b) all y from this field satisfying

$$122 \cdot (100 + y) = 002\,.$$

Exercise 7.10. Let $v(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ be a polynomial from $\mathbb{Z}_p[x]$ with p prime and m positive integer. Show that

$$(v(x))^p = v(x^p).$$