4 HW 3

Deadline: Friday, 22nd of December at 9:00.

You can give it to me at the beginning of practicals, or you can send it in **pdf** format to "dominik.algebra.k@gmail.com". If you are scanning a hand-written solution, please make sure it is legible.

If you spot any mistakes, misprints or have a question concerning the homework, please write me an e-mail ("dominik.algebra.k@gmail.com")

General comment Each problem is worth 5 points. You should not only submit a solution, but you should also show that your solution is correct. Everything that is not immediately obvious needs to be proved or cited from lecture notes.

Problem 1

Let $f(x) = 2x^5 + 2x^3 - 4x^2 - 4$.

Write f as a product of irreducible polynomials in the following domains:

$$\mathbb{Z}[x],\ \mathbb{Q}[x],\ \mathbb{R}[x],\ \mathbb{Z}_3[x],\ and,\ \mathbb{Z}_7[x].$$

Prove that your polynomials are indeed irreducible.

Problem 2

Consider the following equation

$$x^2 + 1 = y^3.$$

Find all integer solutions and prove that there are no more solutions.

Recommended solution:

(0) Show that x is even.

Decompose the equation in $\mathbb{Z}[i][x]$ *as follows*

$$(x + i)(x - i) = y^3$$

and solve it in $\mathbb{Z}[i]$ *using the following steps:*

(1) Prove that for any even $x \in \mathbb{Z}$ we have $GCD_{\mathbb{Z}[i]}(x + i, x - i) = 1$.

(2)* Show that $x + i$ is associated with some third power of an element of $\mathbb{Z}[i]$, i.e., there is $\alpha \in \mathbb{Z}[i]$ such that $\alpha^3 \mid\mid x + i$. *Hint:* Recall that $\mathbb{Z}[i]$ U.F.D.

(3) Show that all invertible elements in $\mathbb{Z}[i]$ can be written as the third power of some element.

We can now assume that there exist $a,b \in \mathbb{Z}$ *such that*

$$x + i = (a + bi)^3$$

(4) Solve the original equation by solving it first for a real part and then for an imaginary part.

**Proof for* $x - i$ *is analogous and you can skip it.*

Problem 3 Consider field $T := \mathbb{F}_8 = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$ and a Reed-Solomon (2,4)-code over the alphabet T for $u_1 = 1$, $u_2 = \alpha$, $u_3 = \alpha^2$ and $u_4 = \alpha + 1$. Recall that this code can correct one mistake.

[1 point] Encode $(0,\alpha)$.

[2 points] We received a code $(\alpha,\alpha^2, \alpha+1,\alpha^2)$. What was the original word?

[2 points] We received a word $w = (0,0,1,1)$, but the channel was unreliable. Show that this word cannot be decoded. Explicitly, you are asked to:

-Show that there is no code c with a Hamming distance $\delta(c,w) \leq 1$.

-Find two codes c_1,c_2 such that $\delta(c_1,w) = \delta(c_2,w) = 2$.

Problem 4 Design a secret-sharing scheme for seven participants - two kings and five ephors such that the secret can be reconstructed either by both kings or one king and all five ephors.

a) The secret is a specific element of the field T. The choice of the field is up to you and the secret is up to you.

b) The probability of someone randomly guessing the secret is less than 2 %.

Formal requirements of your solution

1) Describe the field T and the secret.

2) Explicitly descibe the polynomial(s) you use in the protocol.

3) Describe how many keys each king gets and explicitly describe the keys that the ephors get (i.e., state the specific elements of the field T).

Problem 5 Consider an RSA system with a public key $(N,e) = (91,5)$.

a) [1 points] Encode the messege $x = 4$ using the key (91,5).

b) [2 points] Because we have chosen a small N, it is possible to decode a message without the private key. Decode messege $y = 61$ - what was the original messege?

c) [2 points] Now consider a different public key $(N,e) = (169,5)$. Find d and a number $0 < x < 169$ such that after decoding using the public key (169,5), RSA returns a different value than x.