CS-E4500 Problem Set 7

Jaan Tollander de Balsch - 452056

March 13, 2019

Material used in this report: (Gathen and Gerhard 2013, Sections 14.1–2, 25.3–4).

Problem 1

(a)

Find a monic irreducible polynomial of degree 2 in $\mathbb{Z}_3[x]$.

Let f be a monic polynomial of degree 2 in $\mathbb{Z}_3[x]$. It can be written in the form

$$f = \varphi_0 + \varphi_1 x + x^2.$$

Then the set of all possible coefficient pairs (φ_0, φ_1) is

$$S = \mathbb{Z}_3 \times \mathbb{Z}_3.$$

Let $\tilde{f}$ be a reducible monic polynomial of degree 2 in $\mathbb{Z}_3[x]$

$$\begin{aligned}\tilde{f} &= gh \\ &= (a+x) \cdot (b+x) \\ &= a \cdot b + (a+b)x + x^2\end{aligned}$$

where $a, b \in \mathbb{Z}_3$ and $g, h \in \mathbb{Z}_3[x]$ and $g, h \notin \mathbb{Z}_3$. Then the set of all coefficient pairs which form a reducible monic polynomial of degree 2 is

$$S' = \{(a \cdot b, a+b) \mid a, b \in \mathbb{Z}_3\}.$$

Therefore all coefficients pairs which form monic irreducible polynomials of degree 2 are given by the set difference

$$S \setminus S' = \{(1, \quad 0), (2, \quad 1), (2, \quad 2)\}.$$

For example, $f = 1 + x^2$ is a monic irreducible polynomial of degree 2 in $\mathbb{Z}_3[x]$.

(b)

Using your solution to part (a), present addition and multiplication tables for $\mathbb{F}_9$. For each nonzero element of $\mathbb{F}_9$, present its multiplicative inverse in $\mathbb{F}_9$.

Problem 2

Using your solution to Problem 1, find for each nonzero element of $\mathbb{F}_9$ its multiplicative order.

Problem 3

Problem 4

References

Gathen, Joachim von zur, and Jurgen Gerhard. 2013. *Modern Computer Algebra*. 3rd ed. New York, NY, USA: Cambridge University Press.