CS-E4500 Problem Set 7

Jaan Tollander de Balsch - 452056

March 17, 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 $d=2$ in $\mathbb{Z}_p[x]$ where $p=3$ is a prime. 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

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

We can choose

$$f = 1 + x^2$$

as our 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 $\mathbb{F}_9$.

The set of elements of the finite field $F = \mathbb{F}_{p^d} = \mathbb{Z}_p[x]/\langle f\rangle = \mathbb{F}_{3^2} = \mathbb{Z}_3[x]/\langle f\rangle$ are the set of all polynomials of degree at most $d - 1 = 1$ in $\mathbb{Z}_3[x]$

$$S = \{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\}$$

Addition table

$$\begin{bmatrix}
0 & 1 & 2 & x & x+1 & x+2 & 2x & 2x+1 & 2x+2 \\
1 & 2 & 0 & x+1 & x+2 & x & 2x+1 & 2x+2 & 2x \\
2 & 0 & 1 & x+2 & x & x+1 & 2x+2 & 2x & 2x+1 \\
x & x+1 & x+2 & 2x & 2x+1 & 2x+2 & 0 & 1 & 2 \\
x+1 & x+2 & x & 2x+1 & 2x+2 & 2x & 1 & 2 & 0 \\
x+2 & x & x+1 & 2x+2 & 2x & 2x+1 & 2 & 0 & 1 \\
2x & 2x+1 & 2x+2 & 0 & 1 & 2 & x & x+1 & x+2 \\
2x+1 & 2x+2 & 2x & 1 & 2 & 0 & x+1 & x+2 & x \\
2x+2 & 2x & 2x+1 & 2 & 0 & 1 & x+2 & x & x+1
\end{bmatrix}$$

Multiplication table

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & x & x+1 & x+2 & 2x & 2x+1 & 2x+2 \\
0 & 2 & 1 & 2x & 2x+2 & 2x+1 & x & x+2 & x+1 \\
0 & x & 2x & 2 & x+2 & 2x+2 & 1 & x+1 & 2x+1 \\
0 & x+1 & 2x+2 & x+2 & 2x & 1 & 2x+1 & 2 & x \\
0 & x+2 & 2x+1 & 2x+2 & 1 & x & x+1 & 2x & 2 \\
0 & 2x & x & 1 & 2x+1 & x+1 & 2 & 2x+2 & x+2 \\
0 & 2x+1 & x+2 & x+1 & 2 & 2x & 2x+2 & x & 1 \\
0 & 2x+2 & x+1 & 2x+1 & x & 2 & x+2 & 1 & 2x
\end{bmatrix}$$

Multiplicative inverses can be read from the multiplication table

$$1 \cdot 1 = 1$$
$$2 \cdot 2 = 1$$
$$x \cdot 2x = 1$$
$$(x+1) \cdot (x+2) = 1$$
$$(2x+1) \cdot (2x+2) = 1.$$

Problem 2

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

The order of a nonzero element $a \in \mathbb{F}_q \setminus \{0\}$ is the least positive integer k such that $a^k = 1$.

For the elements $\mathbb{F}_9$ we have

$$
\begin{aligned}
1^1 &= 1 \\
2^2 &= 1 \\
x^4 &= (2x)^4 = 1 \\
(x+1)^8 &= (x+2)^8 = (2x+1)^8 = (2x+2)^8 = 1.
\end{aligned}
$$

Element 1 has order of 1, element 2 has order of 2, elements $x, 2x$ have order of 4 and elements $x+1, x+2, 2x+1, 2x+2$ have order of 8.

Problem 3

Let R be a commutative ring with $0_R \neq 1_R$. for a polynomial $f = \sum_{i=0}^{d} \varphi_i x^i \in R[x]$, define the *formal derivative* $f' \in R[x]$ of f by

$$
f' = \sum_{i=0}^{d} i_R \varphi_i x^{i-1},
$$

where $i_R = 1_R + 1_R + ... + 1_R$ obtained by taking the sum of i copies of the multiplicative identity 1_R of R.

Show that the formal derivative satisfies each of the following properties:

(a) $'$ is R-linear,
(b) $'$ satisfies the Leibniz (product) rule $(fg)' = f'g + fg'$, and
(c) $'$ satisfies the chain rule $f(g)' = f'(g)g'$.

Let f and g be polynomials in $R[x]$. Let $\deg f = d_1$ and $\deg g = d_2$ be their degrees.

(a)

Let the linear combination of polynomials f and g be

$$\begin{aligned}\alpha f + \beta g &= \alpha \sum_{i=0}^{d} \varphi_i x^i + \beta \sum_{i=0}^{d} \rho_i x^i \\ &= \sum_{i=0}^{d} (\alpha\varphi_i + \beta\rho_i) x^i\end{aligned}$$

where $\alpha, \beta \in R$ and $d = \deg(\alpha f + \beta g) = \max\{\deg f, \deg g\}$.

Then the formal derivative is R-linear

$$\begin{aligned}(\alpha f + \beta g)' &= \sum_{i=0}^{d} i_R(\alpha\varphi_i + \beta\rho_i) x^{i-1} \\ &= \alpha \sum_{i=0}^{d} i_R \varphi_i x^{i-1} + \beta \sum_{i=0}^{d} i_R \rho_i x^{i-1} \\ &= \alpha f' + \beta g'.\end{aligned}$$

(b)

The multiplication of the polynomials f and g can be written

$$fg = \sum_{n=0}^{d_1} \sum_{m=0}^{d_2} \varphi_n \rho_m x^n x^m$$

Using linear we have

$$\begin{aligned}(fg)' &= \Big(\sum_{n=0}^{d_1} \sum_{m=0}^{d_2} \varphi_n \rho_m x^n x^m \Big)' \\ &= \sum_{n=0}^{d_1} \sum_{m=0}^{d_2} \varphi_n \rho_m (x^n x^m)'.\end{aligned}$$

where

$$\begin{aligned}(x^n x^m)' &= (x^{n+m})' \\ &= (n+m)x^{n+m-1} \\ &= (nx^{n-1}x^m) + (x^n m x^{m-1}) \\ &= (x^n)' x^m + x^n (x^m)'.\end{aligned}$$

Now we can form the product rule

$$(fg)' = f'g + fg'.$$

(c)

Using linearity we need to only prove the case where $f = x^n$ and $g = x^m$

$$\begin{aligned}
(f(g))' &= ((x^m)^n)' \\
&= (x^{mn})' \\
&= mnx^{mn-1} \\
&= mnx^{m(n-1)+(m-1)} \\
&= (n(x^m)^{n-1})(mx^{m-1}) \\
&= f'(g)g'.
\end{aligned}$$

Problem 4

References

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