Lab Week 05 solutions

Finite field exercises

Here are the solutions to the three questions from the lab.

1. The product of the polynomials is initially expressed by expanding out the brackets and using ordinary integer arithmetic. Then the coefficients are reduced modulo 11, due to the coefficients coming from $\mathbb{Z}_{11}$, as stated in the question.

$$\begin{aligned}(x^2 + 2x + 9) \cdot (x^3 + 10x^2 + x + 7) &= x^5 + 12\,x^4 + 30\,x^3 + 99\,x^2 + 23\,x + 63 \\ &= x^5 + \ x^4 + 8\,x^3 + \ x + 8\end{aligned}$$

The second example, done in the same way, is

$$\begin{aligned}(8x^2 + 3x + 2) \cdot (5x^2 + 6) &= 40\,x^4 + 15\,x^3 + 58\,x^2 + 18\,x + 12 \\ &= 7\,x^4 + 4\,x^3 + 3\,x^2 + 7\,x + 1\end{aligned}$$

2. Remember in this question we are dealing with polynomials with coefficients from $\mathrm{GF}(2)$, i.e. polynomials with binary coefficients. So arithmetic on coefficients is done with modulo 2 addition without carry. This is the same as the XOR operation on coefficients.

   - The first polynomial $x^2 + 1$ is not irreducible as it can be factorized as

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

   - The second polynomial $x^2 + x + 1$ is irreducible as it cannot be factorised into the product of two polynomials of degree 1. The only polynomials of degree 1 are x and $x + 1$. There's no way to make $x^2 + x + 1$ as a product of these.

   - The third polynomial $x^4 + x + 1$ is irreducible. It cannot be factored into a product of two polynomials of degree 2 or into a product of a two polynomials, one of degree 1 and the other of degree 3. There are a few possibilities to check, but they are soon exhausted.

3. For the first pair $(x^3 + 1)$ and $(x^2 + x + 1)$, with binary coefficients, the Euclidean algorithm runs as

$$\begin{aligned}x^3 + 1 &= x(x^2 + x + 1) + x^2 + x + 1 \\ &= (x + 1)(x^2 + x + 1) + 0.\end{aligned}$$

   So in fact we see that $x^2 + x + 1$ divides $x^3 + 1$, leaving remainder 0. So we can say that

$$\gcd(x^3 + 1,\ x^2 + x + 1) = x^2 + x + 1.$$

For the second pair $(x^4 + 8x^3 + 7x + 8)$ and $(2x^3 + 9x^2 + 10x + 1)$, with coefficients from $\mathbb{Z}_{11}$, the Euclidean algorithm runs as

$$\begin{aligned} x^4 + 8x^3 + 7x + 8 &= (6x + 10)(2x^3 + 9x^2 + 10x + 1) + 4x^2 + 9 \\ (2x^3 + 9x^2 + 10x + 1) &= (6x + 5)(4x^2 + 9) + 0 \end{aligned}$$

In the second polynomial division we see a remainder of 0. So the Euclidean algorithm has ended and the gcd will be the last non-zero remainder, i.e. the polynomial $4x^2 + 9$. So

$$\gcd(x^4 + 8x^3 + 7x + 8,\, 2x^3 + 9x^2 + 10x + 1) = 4x^2 + 9,$$

when interpreted as polynomials with coefficients from the field $\mathbb{Z}_{11}$.