ETH Zürich, D-INFK
HS 2020, 2. December 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Solution 11

11.1 Polynomials over a Field

a) In $\mathbb{Z}_7$, the multiplicative inverse of 5 is 3, because $3 \cdot 5 \equiv_7 1$. Therefore, the first coefficient of the result is 3. The rest of the computation proceeds analogously:

$$
\begin{array}{rrrrrl}
(x^5 & & & +\,6x^2 & & +5) \;:\; (5x^2+2x+1) \;=\; 3x^3+3x^2+x+3 \\
-(x^5+ & 6x^4+ & 3x^3 & & &) \\
\hline
 & x^4+ & 4x^3+ & 6x^2+ & & +5 \\
 & -(\,x^4+ & 6x^3+ & 3x^2 & &) \\
\cline{2-6}
 & & 5x^3+ & 3x^2+ & & +5 \\
 & & -(5x^3+ & 2x^2+ & x &) \\
\cline{3-6}
 & & & + & x^2+6x+5 & \\
 & & & -(& x^2+6x+3) & \\
\cline{4-6}
 & & \text{Remainder:} & & & 2
\end{array}
$$

b) The irreducible polynomials of degree 4 over $\mathrm{GF}(2)$ are x^4+x^3+1, x^4+x+1 and $x^4+x^3+x^2+x+1$.

We show this by eliminating all *reducible* polynomials of degree four. A polynomial $p(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ is reducible if it is divisible by a polynomial of degree one or two (if it is divisible by a polynomial of degree three, then it must also be divisible by one of degree one).

By Lemma 5.28, the polynomials $p(x)$ divisible by a polynomial of degree one are exactly those for which $p(0) = 0$ or $p(1) = 0$. Hence, we have to eliminate the polynomials for which $a_0 = 0$ or $a_3 + a_2 + a_1 + a_0 = 1$. Remaining are the polynomials: x^4+x^3+1, x^4+x+1, x^4+x^2+1 and $x^4+x^3+x^2+x+1$.

Furthermore, over $\mathrm{GF}(2)$ there is only one irreducible polynomial of degree two, namely x^2+x+1 (the other polynomials: x^2, x^2+1 and x^2+x can be eliminated in the same way we did above). Hence, we have to also eliminate $(x^2+x+1)^2 = x^4+x^2+1$.

c) Since 2 is a double root, it follows that $a(x) = (x-2)^2 b(x)$, where $b(x)$ is a polynomial of degree 2. We know that $2 = a(3) = (3-2)^2\, b(3)$, $3 = a(4) = (4-2)^2\, b(4)$ and $5 = a(6) = (6-2)^2\, b(6)$. Hence, we have $b(3) = 2$, $b(4) = 3 \cdot 4^{-1} = 6$ and $b(6) = 5 \cdot 2^{-1} = 6$. In order to determine $b(x)$, we apply Lagrange's interpolation:

$$
\begin{aligned}
b(x) &= 2\frac{(x-4)(x-6)}{(3-4)(3-6)} + 6\frac{(x-3)(x-6)}{(4-3)(4-6)} + 6\frac{(x-3)(x-4)}{(6-3)(6-4)} \\
&= 3(x+3)(x+1) + 4(x+4)(x+1) + (x+4)(x+3) \\
&= x^2 + 4x + 2
\end{aligned}
$$

Therefore, $a(x) = (x-2)^2(x^2+4x+2) = x^4+4x^2+x+1$ and $a(0) = 1$.

11.2 The Ring $F[x]_{m(x)}$

a) The zero-divisors are those elements of $\mathrm{GF}(3)[x]_{x^2+2x} \setminus \{0\}$ (that is, the non-zero polynomials of degree at most 1 with coefficients in $\mathbb{Z}_3$) which share a common factor (a polynomial of degree at least 1) with the modulus x^2+2x. The factors of x^2+2x are x and $x+2$, so the zero-divisors are the multiples of x and $x+2$ of degree at most 1. These are ax and $b(x+2)$ for $a, b \in \mathbb{Z}_3$. Hence, the zero-divisors are:

$$x, 2x, x+2, 2x+1.$$

b) We have

$$\mathrm{GF}(3)[x]_{x^2+2} = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.$$

By Lemma 5.35,

$$\mathrm{GF}(3)[x]^*_{x^2+2} = \{a(x) \in \mathrm{GF}(3)[x]_{x^2+2} \mid \gcd(a(x), x^2+2) = 1\}.$$

The task is to find all polynomials $a(x) \in \mathrm{GF}(3)[x]$ of degree at most one, such that $\gcd(a(x), x^2+2) = 1$. Note first that over $\mathrm{GF}(3)$, we have $x^2+2 = x^2-1 = (x+1)(x-1) = (x+1)(x+2)$. Hence, all polynomials $b(x)$ of degree at most one, for which $\gcd(b(x), (x+1)(x+2)) \neq 1$ are $u(x+1)$ and $v(x+2)$ for some $u, v \in \mathrm{GF}(3)$. These polynomials are: $x+1, x+2, 2x+2, 2x+1$ and 0.

The polynomials of degree at most one that are left are in $\mathrm{GF}(3)[x]^*_{x^2+2}$. Therefore, $\mathrm{GF}(3)[x]^*_{x^2+2} = \{1, 2, x, 2x\}$.

c) The inverse of $x \in \mathrm{GF}(3)[x]^*_{x^2+2}$ is a polynomial $p(x) \in \mathrm{GF}(3)[x]^*_{x^2+2}$, such that $x \cdot p(x) \equiv_{x^2+2} 1$ (where 1 is the constant polynomial). Since all the polynomials in $\mathrm{GF}(3)[x]^*_{x^2+2}$ have degree at most 1 (Definition 5.34), we have $p(x) = ax+b$ for some $a, b \in \mathrm{GF}(3)$. Therefore, we only need to find a and b such that $x \cdot (ax+b) \equiv_{x^2+2} 1$. Note that

$$x \cdot (ax+b) \equiv_{x^2+2} ax^2 + bx \equiv_{x^2+2} -2a + bx \equiv_{x^2+2} a + bx.$$

It is now easy to see that $a + bx \equiv_{x^2+2} 1$ when $b = 0$ and $a = 1$. Hence, the inverse of the polynomial x is $p(x) = x$.

11.3 Extension Fields

Let $F = \mathbb{Z}_5[x]_{x^2+3}$.

a) The polynomial $a(x) = x^2+3 \in \mathbb{Z}_5[x]$ has no roots, because $a(0) = 3$, $a(1) = 4$, $a(2) = 2$, $a(3) = 2$, and $a(4) = 4$. Since $a(x)$ has degree two, this implies that it is irreducible (Corollary 5.29). Therefore, F is a field (Theorem 5.36).

b) By Lemma 5.33 we have $|F| = 5^2 = 25$, since $|\mathbb{Z}_5| = 5$ and x^2+3 is of degree 2. As F is a field, we have $F^* = F \setminus \{0\}$. Thus, $|F^*| = |F| - 1 = 25 - 1 = 24$.

c) We have $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for $a = 3x+2$, $b = 4x$, $c = 3x$, and $d = x+1$. Thus,

$$\begin{aligned} ad - bc &= (3x+2)(x+1) - (4x)(3x) \\ &= (3x^2 + 3x + 2x + 2) - 12x^2 \\ &= -9x^2 + 5x + 2 \\ &= x^2 + 2 \\ &\equiv_{x^2+3} 2 - 3 \\ &= 4. \end{aligned}$$

We have $4^{-1} \equiv_5 4$. Therefore, we obtain

$$\begin{aligned} M^{-1} &= (ad-bc)^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= 4 \cdot \begin{pmatrix} x+1 & -4x \\ -3x & 3x+2 \end{pmatrix} \\ &= \begin{pmatrix} 4x+4 & 4x \\ 3x & 2x+3 \end{pmatrix}. \end{aligned}$$

11.4 Polynomials over Extension Fields (⋆ ⋆)

The elements of $\mathrm{GF}(2)[x]_{x^2+x+1}$ are $0, 1, x$ and $x+1$. We first check whether any of these elements is a root of $a(y)$:

$a(0) = x$
$a(1) = x + x + (x+1) + x = 1$
$a(x) = x \cdot x^3 + x \cdot x^2 + (x+1) \cdot x + x = x^4 + x^3 + x^2 = x^2(x^2 + x + 1) = 0$

Since x is a root, $a(y)$ is divisible by $y - x \equiv_2 y + x$.

$$\begin{array}{rrrrrl} xy^3+ & xy^2+ & (x+1)y+ & x & : \; y+x & = xy^2 + y + 1 \\ -(xy^3+ & (x+1)y^2 & &) & & \\ \hline & y^2+ & (x+1)y+ & x & & \\ - & (y^2+ & xy &) & & \\ \hline & & y+ & x & & \\ & - & (y+ & x) & & \\ \hline & & & 0 & & \end{array}$$

In the first step of the division we used the fact that in $\mathrm{GF}(2)[x]_{x^2+x+1}$ we have $x^2 = x + 1$. We have $xy^3 + xy^2 + (x+1)y + x = (y+x)(xy^2 + y + 1)$. Let $b(y) = xy^2 + y + 1$. The only possible roots of $b(y)$ are x and $x+1$, because if 1 or 0 were roots of $b(y)$, they would also be roots of $a(y)$, which we already excluded.

$b(x) = x \cdot x^2 + x + 1 = x^3 + x + 1 = (x^2 + x + 1)(x+1) + x = x$
$b(x+1) = x \cdot (x+1)^2 + (x+1) + 1 = x^3 = (x^2 + x + 1) \cdot (x+1) + 1 = 1$

Since $\deg(b(y)) = 2$ and $b(y)$ has no roots, $b(y)$ is irreducible. Hence, the factorization of $a(y)$ is $a(y) = (y+x)(xy^2 + y + 1)$.

11.5 Secret Sharing

a) By Lemma 5.31, the polynomial $a(x)$ is uniquely determined by the t values $s_i = a(\alpha_i)$, known to the t monkeys. Hence, the monkeys can use the Lagrange's interpolation formula to reconstruct $a(x)$ and the secret code a_0.

b) There are q possibilities for the secret a_0. Without loss of generality, consider the clan consisting of monkeys $M_1, \ldots, M_{t-1}$ with shares $s_1, \ldots, s_{t-1}$. By Lemma 5.31, for every $a_0 \in \mathrm{GF}(q)$, there exists a polynomial $a(x)$ of degree at most $t-1$, such that $a(\alpha_1) = s_1, \ \ldots, \ a(\alpha_{t-1}) = s_{t-1}$ and $a_0 = a(0) = s$, which could have been the one chosen by the zookeeper.

Note. This polynomial is unique, so there is a bijection between the secrets a_0 and the possible polynomials $a(x)$. Since the polynomial was chosen at random, the secret a_0 is random given the information of the greedy monkeys.