ETH Zürich, D-INFK
HS 2023, 1. December 2023

Prof. Ueli Maurer
Giovanni Deligios

Diskrete Mathematik

Solution 10

10.1 Warm-Up

a) A field is a nontrivial commutative ring F in which every nonzero element is a unit, i.e., $F^* = F \setminus \{0\}$ (see Definition 5.26).

b) A root of a polynomial $a(x) \in R[x]$ is an element $\alpha \in R$ such that $a(\alpha) = 0$. (see Definition 5.33).

c) $b(x)$ is not irreducible. Since $b(1) = 0$ and $b(2) = 0$, we obtain via Lemma 5.29 that $b(x) = (x+2)(x+1)$.

10.2 Integral Domains and Fields

a) For example, $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$.

b) We have to prove that every $a \in D \setminus \{0\}$ is a unit. Let $a \in D \setminus \{0\}$ be arbitrary. We define the function $f_a : D \to D$ by $f_a(x) = a \cdot x$. We show that f_a is bijective:

injective: Assume that there exist $x, y \in D$ such that $f_a(x) = f_a(y)$ and $x \neq y$.

$$0 = f_a(y) - f_a(x) = a \cdot y - (a \cdot x) = a \cdot y + a \cdot (-x) = a \cdot (y - x),$$

where the third step follows from Lemma 5.17, and the last step uses the distributive law. Since by assumption $a \neq 0$ and $y - x \neq 0$, it follows that a is a zero-divisor, which is a contradiction with D being an integral domain.

surjective: If f_a was not surjective, we would have $y \notin Im(f_a)$ for some $y \in D$, which for finite D implies $|Im(f_a)| < |D|$. But since f_a is injective, the function $f'_a : D \to Im(f_a)$ defined by $f'_a(x) = f_a(x)$ is bijective, so $|Im(f_a)| = |D|$, which is a contradiction.

The inverse of a is $f_a^{-1}(1)$, because $a \cdot f_a^{-1}(1) = f_a(f_a^{-1}(1)) = 1$, hence, a is a unit.

10.3 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:

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

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 5.29, 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 $(x^2+x+1)^2 = x^4+x^2+1$.

10.4 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 5.36,

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

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 $p(x) = x$.

10.5 Extension Fields

Let $F = \mathbb{Z}_5[x]_{x^2+4x+1}$.

a) The polynomial $b(x) = x^2 + 4x + 1 \in \mathbb{Z}_5[x]$ has no roots, because $b(0) = 1$, $b(1) = 1$, $b(2) = 3$, $b(3) = 2$, $b(4) = 3$. Since $b(x)$ has degree 2, this implies that it is irreducible (Corollary 5.30). Therefore, F is a field (Theorem 5.37).

b) By Lemma 5.34 we have $|F| = 5^2 = 25$, since $|\mathbb{Z}_5| = 5$ and $b(x)$ is of degree 2. As F is a field, we have $F^* = F \setminus \{0\}$. Thus, $|F^*| = |F| - 1 = 25 - 1 = 24$. By Corollary 5.9 the possible orders of an element in F^* are 1, 2, 3, 4, 6, 8, 12, and 24.

We prove that $\langle x+2 \rangle = F^*$. Due to the previous observation, it is sufficient to show that $(x+3)^k \not\equiv_{b(x)} 0$ for all $k \in \{1, 2, 3, 4, 6, 8, 12\}$. Clearly, $x + 3 \not\equiv_{b(x)} 1$. Moreover, we have

$$\begin{aligned}
(x+3)^2 &\equiv_{b(x)} x^2+6x+9\\
&\equiv_{b(x)} b(x)+(2x+3)\\
&\equiv_{b(x)} 2x+3\\
&\not\equiv_{b(x)} 1,\\
(x+3)^4 &\equiv_{b(x)} (2x+3)^2\\
&\equiv_{b(x)} 4x^2+2x+4\\
&\equiv_{b(x)} 4b(x)+x\\
&\equiv_{b(x)} x\\
&\not\equiv_{b(x)} 1,\\
(x+3)^8 &\equiv_{b(x)} (x)^2\\
&\equiv_{b(x)} b(x)+(x+4)\\
&\equiv_{b(x)} x+4\\
&\not\equiv_{b(x)} 1,\\
(x+3)^3 &\equiv_{b(x)} (2x+3)(x+3)\\
&\equiv_{b(x)} 2x^2+4x+4\\
&\equiv_{b(x)} 2b(x)+(x+2)\\
&\equiv_{b(x)} x+2\\
&\not\equiv_{b(x)} 1,\\
(x+3)^6 &\equiv_{b(x)} (x+2)^2\\
&\equiv_{b(x)} x^2+4x+4\\
&\equiv_{b(x)} 4b(x)+3\\
&\equiv_{b(x)} 3\\
&\not\equiv_{b(x)} 1,\\
(x+3)^{12} &\equiv_{b(x)} (3)^2\\
&\equiv_{b(x)} 4\\
&\not\equiv_{b(x)} 1.
\end{aligned}$$

This concludes the proof.

c) Observe that $2x+3 \equiv_{b(x)} (x+3)^2$ and $2x+1 \equiv_{b(x)} 2(x+3)$. Therefore we can write

$$a(y) = (x+3)^2y^2 + 2(x+3)y + 1 = ((x+3)y+1)^2.$$

10.6 Secret Sharing

a) By Lemma 5.32, the polynomial $a(x)$ is uniquely determined by the t values $s_i =$

$a(\alpha_i)$, known to the t generals. Hence, the generals can use the Lagrange's interpolation formula to reconstruct $a(x)$ and the secret code s.

b) There are q possibilities for the secret s. Without loss of generality, consider the shares $s_1, \ldots, s_{t-1}$ of the generals $G_1, \ldots, G_{t-1}$. By Lemma 5.32, for every $s \in \mathrm{GF}(q)$, 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 $a(0) = s$, which could be the key.

Note. This polynomial is unique, so there is a bijection between the secrets s and the possible polynomials $a(x)$. Since the polynomial was chosen at random, the secret s is random given the $t-1$ shares.

10.7 Structure of Multiplicative Groups of Finite Fields

a) ($\Rightarrow$) Assume that $d = \gcd(a, b)$. By Definition 4.2 we have both $d \mid a$ and $d \mid b$. Furthermore, by Corollary 4.5 we can write $d = ax + by$ for some $x, y \in \mathbb{Z}$. Dividing both sides of this last equation by d we obtain $\frac{a}{d}x + \frac{b}{d}y = 1$ which implies (recall Exercise 7.1) that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

($\Leftarrow$) Assume that both $d \mid a$ and $d \mid b$, and also $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. By Corollary 4.5 we can write $\frac{a}{d}x + \frac{b}{d}y = 1$. Multiplying by d on both sides we obtain $ax + by = d$. Suppose that for some $d' \in \mathbb{Z}$ we have both $d' \mid a$ and $d' \mid b$. Then $d'k_1 = a$ and $d'k_2 = b$ for some $k_1, k_2 \in \mathbb{Z}$. Therefore, we can write $d'k_1x + d'k_2y = d'(k_1x + k_2y) = d$ which shows $d' \mid d$. We conclude $d = \gcd(a, b)$ (Definition 4.2).

b) We have

$$\begin{aligned} A(d) &= \{k \in \{1, \ldots, n\} \mid \gcd(k, n) = d\} \\ &= \left\{ k \in \{1, \ldots, n\} \;\middle|\; (d \mid k) \wedge (d \mid n) \wedge \gcd\left(\frac{k}{d}, \frac{n}{d}\right) = 1 \right\} && \text{(Subtask a))} \\ &= \left\{ \ell d \in \{1, \ldots, n\} \;\middle|\; (d \mid n) \wedge \gcd\left(\ell, \frac{n}{d}\right) = 1 \right\} && \left(\text{Set } \frac{k}{d} = \ell \in \mathbb{Z}\right) \end{aligned}$$

This means $|A(d)| = \left|\left\{\ell \in \left\{1, \ldots, \frac{n}{d}\right\} \mid (d \mid n) \wedge \gcd\left(\ell, \frac{n}{d}\right) = 1\right\}\right| = \varphi\left(\frac{n}{d}\right)$ (Definitions 5.16 and 5.17).

c) Observe that $\bigcup_{d|n} A(d) = \{1, \ldots, n\}$ and $A(d) \cap A(d') = \varnothing$ for all $d \neq d'$, that is, the sets $A(d)$ as d ranges over the divisors of n form a partition of $[1, n]$. This means that $n = |\{1, \ldots, n\}| = \left|\bigcup_{d|n} A(d)\right| = \sum_{d|n} |A(d)| = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$, where the last equality follows from subtask b) and the second to last from the fact that the sets are disjoint.

d) This is simply because as d ranges over the divisors of n so does $\frac{n}{d}$. Let's prove this formally. Let $D(n)$ denote the set of divisors of n. Consider the map $f : D(n) \to D(n)$ that maps $d \mapsto \frac{n}{d}$. First of all, notice that the map is well-defined, because if $d \mid n$, then $dk = n$ for some $k \in \mathbb{Z}$, which means that $\frac{n}{d} \in \mathbb{Z}$. Therefore, we can write $n = \frac{n}{d}d$ which shows that $\frac{n}{d} \mid n$. Furthermore, this map is bijective, because for any divisor d of n we can write $d = \frac{n}{k} = f(k)$. This shows that f is surjective (and therefore automatically injective). Therefore, we get

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{\{f(d) \ | \ d|n\}} \varphi\left(\frac{n}{f(d)}\right) = \sum_{d|n} \varphi(d).$$

By the previous subtask, we conclude that $\sum_{d|n} \varphi(d) = n$.

e) The polynomial $x^d - 1$ is a polynomial of degree d over the finite field F. By Theorem 5.31 it has at most d roots. Now, observe that if $k \in B(d)$ then $k^d = 1$ so that k is a root of $x^d - 1$. Therefore $|B(d)| \leq d$. Suppose that $B(d) \neq \varnothing$. Let $k \in B(d)$ and consider the cyclic subgroup $\langle k \rangle$ of F^* generated by k. By Theorem 5.7 the number of elements of $\langle k \rangle$ that has order d is exactly $\varphi(d)$ (all the elements of the form k^i with $\gcd(d, i) = 1$). This shows that if $B(d)$ is not empty then $|B(d)| \geq \varphi(d)$. Now, suppose by contradiction that $|B(d)| > \varphi(d)$. This means that there is $y \in B(d)$ such that $y \notin \langle k \rangle$. But then the polynomial $x^d + 1$ would have $d + 1$ roots (namely all elements of $\langle k \rangle$ in addition to y), a contradiction. This shows that $|B(d)| = \varphi(d)$ whenever $B(d) \neq \varnothing$.

f) Again, observe that the union $\bigcup_{d \in [1,n]} B(d) = \bigcup_{d|n} B(d) = F^*$, where the first equality follows from Corollary 5.9. Furthermore, if $d \neq d'$ then $B(d) \cap B(d') = \varnothing$ (the order of an element of F^* is uniquely defined).

We have $\sum_{d|n} \varphi(d) = n = |F^*| = |\bigcup_{d|n} B(d)| = \sum_{d|n} |B(d)|$, where the first equality follows from subtask d), and the lasts from the facts that the sets $B(d)$ for distinct d are disjoint. By subtask e) we know that the number of elements of $B(d)$ is either $\varphi(d)$ or 0. Suppose that for some d' such that $d' \mid n$ we have $|B(d')| = 0$. Then clearly $n = \sum_{d|n, d \neq d} |B(d)| < \sum_{d|n} \varphi(d) = n$, a contradiction.

g) Subtask f) in particular implies that $|B(n)| = \varphi(n) > 0$ which in turn implies $B(n) \neq \varnothing$, so that there is an element a of order n in F^*. This shows that F^* is cyclic.