

# Math 775 Homework 7

Austin Mohr

March 22, 2011

## Problem 1

**Proposition 1.** *Let  $R = (3, 4, 4, 4, 2)$  and  $S = (2, 4, 2, 4, 3, 2)$ . The class  $\mathcal{A}(R, S)$  is nonempty.*

*Proof.* We first construct the maximal  $5 \times 6$  matrix with row sum vector  $R$ , namely

$$\bar{A}_R = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The matrix above corresponds to the column sum vector  $S' = (5, 5, 4, 3, 0, 0)$ . By the Gale-Ryser Theorem,  $\mathcal{A}(R, S)$  is nonempty if and only if  $S'$  majorizes  $S$ . To establish this criterion, let  $s_i$  and  $s'_i$  denote the  $i^{\text{th}}$  partial sum of  $S$  and  $S'$  respectively. We have

$$s_1 = 4, s_2 = 8, s_3 = 11, s_4 = 13, s_5 = 15, s_6 = 17$$

and

$$s'_1 = 5, s'_2 = 10, s'_3 = 14, s'_4 = 17, s'_5 = 17, s'_6 = 17.$$

Thus,  $S'$  indeed majorizes  $S$ , and so  $\mathcal{A}(R, S)$  is nonempty. In particular, the canonical matrix  $\tilde{A}$  of  $\mathcal{A}(R, S)$  is given by

$$\tilde{A} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

□

## Problem 2

**Proposition 2.** *Let  $A$  be a Latin square of order  $4m + 2$  for  $m \in \mathbb{Z}^+$ . If  $A$  contains an order  $2m + 1$  subarray that is a Latin square, then there is no Latin square perpendicular to  $A$ .*

*Proof.* Given a matrix  $M$ , define the submatrices

$$\begin{aligned} M_1 &= M[[2m + 1], [2m + 1]] \\ M_2 &= M[[2m + 1], [4m + 2] \setminus [2m + 1]] \\ M_3 &= M[[4m + 2] \setminus [2m + 1], [2m + 1]]. \end{aligned}$$

(Loosely, if we split  $M$  in half vertically and horizontally,  $M_1$  is the upper left submatrix,  $M_2$  is the upper right submatrix, and  $M_3$  is the lower left submatrix.)

Without loss of generality, we may assume (by permuting labels of entries) that the Latin subsquare is on the set  $[2m + 1]$ . Moreover, we may assume (by permuting columns) that the entries of the first row of  $A$  are the elements  $1, \dots, 4m + 2$  in increasing order. With these assumptions, it follows that  $A_1$  is a Latin square on  $[2m + 1]$ . Since  $A$  in its entirety is Latin, it must be that  $A_2$  and  $A_3$  are Latin squares on  $[4m + 2] \setminus [2m + 1]$ .

Let now  $B$  be another latin square of order  $4m + 2$  and suppose, for the purpose of contradiction, that  $A$  and  $B$  are orthogonal. Denote by  $1(M)$  the number of 1-entries in a matrix. Observe that  $1(B_1) + 1(B_2) = 2m + 1$ , since  $B_1$  and  $B_2$  together comprise the first  $2m + 1$  rows of  $B$ , which is Latin. Similarly,  $1(B_1) + 1(B_3) = 2m + 1$ , as  $B_1$  and  $B_3$  comprise the first  $2m + 1$  columns of  $B$ . We have also that  $1(B_2) + 1(B_3) = 2m + 1$ . To see this, recall that  $A_2$  and  $A_3$  are Latin squares on  $[4m + 2] \setminus [2m + 1]$ . Moreover, all occurrences in  $A$  of the elements of  $[4m + 2] \setminus [2m + 1]$  take place in  $A_2$  and  $A_3$ . Since we supposed  $A$  and  $B$  to be orthogonal, it follows that there are precisely  $2m + 1$  1-entries in  $B$ .

We now derive our contradiction. From  $1(B_1) + 1(B_2) = 2m + 1$  and  $1(B_1) + 1(B_3) = 2m + 1$ , we see that  $1(B_2) = 1(B_3)$ . This is inconsistent with that fact that  $1(B_2) + 1(B_3) = 2m + 1$ , an odd number. Therefore, we conclude that there is no Latin square orthogonal to  $A$ . □

### Problem 3

Given below are four mutually orthogonal Latin squares of order 5. They are built using the construction based on  $GF(5)$ , and so are guaranteed to be mutually orthogonal.

$$A_1 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{bmatrix}$$

$$A_4 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}$$

This system of mutually orthogonal Latin squares gives rise to the following incidence matrix for a projective plane of order 5.

0	0	0	0	0	0
0	1	1	1	1	1
0	2	2	2	2	2
0	3	3	3	3	3
0	4	4	4	4	4
1	0	1	2	3	4
1	1	2	3	4	0
1	2	3	4	0	1
1	3	4	0	1	2
1	4	0	1	2	3
2	0	2	4	1	3
2	1	3	0	2	4
2	2	4	1	3	0
2	3	0	2	4	1
2	4	1	3	0	2
3	0	3	1	4	2
3	1	4	2	0	3
3	2	0	3	1	4
3	3	1	4	2	0
3	4	2	0	3	1
4	0	4	3	2	1
4	1	0	4	3	2
4	2	1	0	4	3
4	3	2	1	0	4
4	4	3	2	1	0

## Problem 4

**Proposition 3.** *Let  $\Pi$  denote a projective plane of order  $n$ . If  $\Pi' \neq \Pi$  is a subplane of order  $m$ , then  $n \geq m^2$ .*

*Proof.* Let  $p$  be a point in  $\Pi$  but not in  $\Pi'$ . We know that  $n + 1$  lines pass through this point. Moreover, we know that at most one of these lines belongs to  $\Pi'$  (otherwise,  $p \in \Pi'$ ). Let  $\mathcal{L}$  denote this collection of  $n$  lines belonging to  $\Pi$  but not  $\Pi'$ . Each  $L \in \mathcal{L}$  contains  $n$  points other than  $p$ . Now, since  $L$  is missing from  $\Pi'$ , at most one of these points can be present in  $\Pi'$  (otherwise,  $L \in \Pi'$ ).

All told,  $\Pi'$  contains at most one point for each line of  $\mathcal{L}$  (thus at most  $n$  points contributed in this way) and  $m + 1$  points from the line through  $p$  (indeed, every line of  $\Pi'$  contains at most  $m + 1$  points). Since  $\Pi'$  contains  $m^2 + m + 1$  points in total, we have

$$m^2 + m + 1 \leq n + m + 1$$

and so  $n \geq m^2$ , as desired.  $\square$

## Problem 5

A *transversal* in an order  $n$  array is a collection of  $n$  entries with no two on a line. A transversal is *Latin* if its entries are distinct. Define the *circulant* Latin square  $\mathcal{C}_n = [a_{ij}]$  by  $a_{ij} = (j - i) \pmod{n}$  with  $i, j \in \{1, \dots, n\}$ .

**Proposition 4.** *If a transversal  $T$  in  $\mathcal{C}_n$  has  $\lambda_i$  occurrences of  $i$ , then  $\sum_{i=1}^n i\lambda_i \equiv 0 \pmod{n}$ .*

*Proof.* Any transversal can be represented as a sequence  $\{a_{i\sigma(i)} \mid i \in [n]\}$  for some permutation  $\sigma$  on  $[n]$ . Now, working modulo  $n$ , we have

$$\begin{aligned} \sum_{i=1}^n i\lambda_i &= \sum_{i=1}^n a_{i\sigma(i)} \\ &= \sum_{i=1}^n (\sigma(i) - i) \\ &= \sum_{i=1}^n \sigma(i) - \sum_{i=1}^n i \\ &= 0. \end{aligned}$$

$\square$

**Proposition 5.** *The circulant Latin square  $\mathcal{C}_n$  has a Latin transversal if and only if  $n$  is odd.*

*Proof.* For the forward implication, we have (working modulo  $n$ )

$$\begin{aligned} 0 &= \sum_{i=1}^n i \\ &= \frac{n(n+1)}{2}. \end{aligned}$$

Suppose, for the sake of contradiction, that  $n$  is even. Let  $n = 2^m q$  for some odd  $q$ . Now,  $\frac{n(n+1)}{2} = 2^{m-1} q(n+1)$ . Since  $n+1$  is odd, it possesses no factor of 2. Thus, we conclude that  $\frac{n(n+1)}{2}$  is not congruent to 0 modulo  $n$ . Therefore,  $n$  is odd.

For the reverse implication, consider the transversal  $\{a_{i,2i} \mid i \in [n]\}$  for odd  $n$ . To see that it is Latin, observe that 2 has an inverse modulo  $n$  whenever  $n$  is odd, and so  $2i = 2j$  if and only if  $i = j$ .  $\square$

## Problem 6

**Proposition 6.** *If  $F$  is a finite field, then  $|F| = p^\alpha$  for some prime  $p$  and some exponent  $\alpha \geq 1$ .*

*Proof.* Let  $p$  be a prime divisor of  $|F|$ . By Cauchy's Theorem, there is an element  $a$  of order  $p$  in the additive group  $(F, +)$ . That is,  $pa = 0$ , where  $pa$  denotes the sum  $\sum_{i=1}^p a$ .

Let now  $b$  be any nonzero element of  $F$ . Observe that

$$\begin{aligned} pb &= pb(aa^{-1}) && (a^{-1} \text{ exists since } (F, +, \times) \text{ is a field}) \\ &= b(pa)a^{-1} && (\text{associativity and commutativity of } \times) \\ &= 0. \end{aligned}$$

Hence, the order of any nonzero element of  $(F, +)$  must divide  $p$ , and so is equal to  $p$ .

Let now  $q$  be any prime divisor of  $|F|$ . Again by Cauchy's Theorem, there is an element  $c$  of order  $q$  in the additive group  $(F, +)$ . We have shown, however, that every element of  $(F, +)$  has order  $p$ , and so conclude that  $q = p$ . Therefore,  $|F| = p^\alpha$  for some exponent  $\alpha \geq 1$ .  $\square$

**Proposition 7.** *For any prime  $p$ , the set  $\mathbb{Z}_p$  of integers modulo  $p$  forms a field of order  $p$ .*

*Proof.* We verify the field axioms directly. In what follows, let  $a, b, c \in \mathbb{Z}_p$  and let  $r(x)$  denote the residue of  $x$  modulo  $p$ . We denote addition and multiplication in  $\mathbb{Z}_p$  by  $+_p$  and  $\times_p$ , respectively.

The underlying set of  $\mathbb{Z}_p$  is  $\{0, \dots, p-1\}$ , and so has order  $p$ .

We show next the closure of addition in  $\mathbb{Z}_p$ . We know that  $a + b = mp + r(a + b)$  for some integer  $m \geq 0$ . Now,

$$\begin{aligned} a +_p b &= r(a + b) \\ &\in \mathbb{Z}_p. \end{aligned}$$

We show next the closure of multiplication in  $\mathbb{Z}_p$ . We know that  $ab = kp + r(ab)$  for some integer  $k \geq 0$ . Now,

$$\begin{aligned} a \times_p b &= r(ab) \\ &\in \mathbb{Z}_p. \end{aligned}$$

We show next the associativity of addition in  $\mathbb{Z}_p$ . We know that  $a + b = mp + r(a + b)$  and  $b + c = np + r(b + c)$  for some integers  $m, n \geq 0$ . Now,

$$\begin{aligned} (a +_p b) +_p c &= r(r(a + b) + c) \\ &= r(a + b - mp + c) \\ &= r(a + b + c). \end{aligned}$$

Similarly,

$$\begin{aligned} a +_p (b +_p c) &= r(a + r(b + c)) \\ &= r(a + b + c - np) \\ &= r(a + b + c). \end{aligned}$$

Hence, addition is associative in  $\mathbb{Z}_p$ .

The associativity of multiplication in  $\mathbb{Z}_p$  is similar. As before, we know  $ab = kp + r(ab)$  and  $bc = \ell p + r(bc)$  for some integers  $m, n \geq 0$ . Now,

$$\begin{aligned} (a \times_p b) \times_p c &= r(r(ab)c) \\ &= r((ab - kp)c) \\ &= r(abc - ckp) \\ &= r(abc). \end{aligned}$$

Similarly,

$$\begin{aligned} a \times_p (b \times_p c) &= r(ar(bc)) \\ &= r(a(bc - \ell p)) \\ &= r(abc - a\ell p) \\ &= r(abc). \end{aligned}$$

Hence, multiplication is associative in  $\mathbb{Z}_p$ .

We show next that addition and multiplication are commutative in  $\mathbb{Z}_p$ . It follows immediately from the commutativity of addition in  $\mathbb{Z}$  that

$$\begin{aligned}a +_p b &= r(a + b) \\ &= r(b + a) \\ &= b +_p a.\end{aligned}$$

Similarly, because of the commutativity of multiplication in  $\mathbb{Z}$ ,

$$\begin{aligned}a \times_p b &= r(ab) \\ &= r(ba) \\ &= b \times_p a.\end{aligned}$$

We show next that 0 is the additive identity and 1 the multiplicative identity in  $\mathbb{Z}_p$ . It follows immediately from the fact that 0 is the additive identity in  $\mathbb{Z}$  that

$$\begin{aligned}a +_p 0 &= r(a + 0) \\ &= r(a) \\ &= a.\end{aligned}$$

Similarly, since 1 is the multiplicative identity in  $\mathbb{Z}$ ,

$$\begin{aligned}a \times_p 1 &= r(a \times 1) \\ &= r(a) \\ &= a.\end{aligned}$$

We show next that, for all  $a \in \mathbb{Z}_p$ , there exists an additive inverse  $-a \in \mathbb{Z}_p$ . Observe that  $0 \leq a < p$ , and so  $0 < p - a \leq p$  (here,  $p - a$  denotes subtraction in  $\mathbb{Z}$ ). Define  $-a$  to be  $p - a$ , which is an element of  $\mathbb{Z}_p$ . It follows that

$$\begin{aligned}a +_p -a &= a +_p (p - a) \\ &= r(a + p - a) \\ &= r(a - a) \\ &= 0.\end{aligned}$$

Hence, every element of  $\mathbb{Z}_p$  has an additive inverse.

We show next that, for all  $a \in \mathbb{Z}_p$ , there exists a multiplicative inverse  $a^{-1} \in \mathbb{Z}_p$ . To establish this fact, we show that the set

$$S = \{1 \times_p a, \dots, (p-1) \times_p a\}$$

contains  $p-1$  distinct nonzero elements, and so one of the products equals 1.

Observe first that no element of  $S$  is zero. Suppose, to the contrary, that  $k \times_p a = 0$  for some  $k \times_p a \in S$ . Since  $p$  is prime and  $p$  divides 0,  $p$  divides one of  $k$  or  $a$ , which is impossible.

Next, we show that all elements of  $S$  are distinct. Let  $j \times_p a = k \times_p a$  for  $j \times_p a, k \times_p a \in S$ . Since  $ja = mp + r(ja)$  and  $ka = np + r(ka)$  for some integers  $m$  and  $n$ , we have

$$\begin{aligned} (j-k)a &= ja - ka \\ &= mp + r(ja) - (np + r(ka)) \\ &= mp - np \\ &= (m-n)p. \end{aligned}$$

Thus,  $p$  divides  $(j-k)a$ , and so  $p$  divides  $j-k$  (since it cannot divide  $a$ ). Since  $j-k < p$ , it follows that  $j-k = 0$ . In other words,  $j = k$ , and so the chosen elements of  $S$  are identical. Therefore,  $S$  contains  $p-1$  distinct nonzero elements, and so a multiplicative inverse exists for  $a$ .

We show finally that multiplication distributes over addition in  $\mathbb{Z}_p$ . We know that

$$\begin{aligned} b + c &= np + r(b+c), \\ ab &= kp + r(ab), \text{ and} \\ ac &= jp + r(ac). \end{aligned}$$

It follows that

$$\begin{aligned} a \times_p (b +_p c) &= r(ar(b+c)) \\ &= r(a(b+c - np)) \\ &= r(ab + ac - anp) \\ &= r(ab + ac). \end{aligned}$$

Similarly,

$$\begin{aligned}
(a \times_p b) +_p (a \times_p c) &= r(r(ab) + r(ac)) \\
&= r(ab - kp + ac - jp) \\
&= r(ab + ac - (k + j)p) \\
&= r(ab + ac).
\end{aligned}$$

Hence, multiplication distributes over addition in  $\mathbb{Z}_p$ .

Having verified the field axioms, we conclude that the integers modulo  $p$  indeed form a field of order  $p$ .  $\square$

**Proposition 8.** *For all integers  $\alpha > 1$ , the collection  $\mathbb{Z}_{p^\alpha}$  does not form a field.*

*Proof.* Let  $q = p^\alpha$ . Consider  $p^\beta, p^\gamma \in \mathbb{Z}_q$  with  $\beta + \gamma = \alpha$ . We see that

$$\begin{aligned}
p^\beta p^\gamma &= p^{\beta+\gamma} \\
&= q,
\end{aligned}$$

and so  $p^\beta \times_q p^\gamma = 0$ .

We show now that  $p^\beta$  cannot have a multiplicative inverse. Assume first that  $\times_q$  is commutative and associative and that 0 is the multiplicative identity in  $\mathbb{Z}_q$  (if not, then  $\mathbb{Z}_q$  is certainly not a field). Now, for any element  $a \in \mathbb{Z}_q$ ,

$$\begin{aligned}
(p^\beta \times_q a) \times_q p^\gamma &= (p^\beta \times_q p^\gamma) \times_q a \\
&= 0 \times_q a \\
&= 0.
\end{aligned}$$

Were  $a$  the multiplicative inverse of  $p^\beta$ , the computation above would have yielded  $p^\gamma$ . Hence,  $a$  is not the multiplicative inverse of  $p^\beta$ . As  $a$  was arbitrary, we conclude that  $p^\beta$  has no multiplicative inverse, and so  $\mathbb{Z}_q$  is not a field.  $\square$

**Proposition 9.** *Let  $P(\omega)$  be a monic irreducible polynomial of degree  $\alpha$ . Define  $Q(\omega) \equiv R(\omega) \pmod{P(\omega)}$  for  $Q(\omega), R(\omega) \in \mathbb{Z}_p[\omega]$  provided there exists  $P_1(\omega) \in \mathbb{Z}_p[\omega]$  such that*

$$Q(\omega) = R(\omega) + P_1(\omega)P(\omega).$$

*The relation  $\equiv$  defined above is an equivalence relation on  $p^\alpha$  classes.*

*Proof.* We verify directly the axioms of equivalence relations. In what follows, let  $Q(\omega), R(\omega), S(\omega) \in \mathbb{Z}_p[\omega]$ .

We see that  $\equiv$  is reflexive, as

$$Q(\omega) = Q(\omega) + 0 \cdot P(\omega).$$

We show next that  $\equiv$  is symmetric. To that end, suppose  $Q(\omega) \equiv R(\omega)$ . That is, there exists  $P_1(\omega) \in \mathbb{Z}_p[\omega]$  such that

$$Q(\omega) = R(\omega) + P_1(\omega) \cdot P(\omega).$$

Rearranging terms, we have

$$R(\omega) = Q(\omega) + (-P_1(\omega)) \cdot P(\omega),$$

and so  $R(\omega) \equiv Q(\omega)$ .

We show finally that  $\equiv$  is transitive. To that end, suppose  $Q(\omega) \equiv R(\omega)$  and  $R(\omega) \equiv S(\omega)$ . That is, there exists  $P_1(\omega), P_2(\omega) \in \mathbb{Z}_p[\omega]$  such that

$$Q(\omega) = R(\omega) + P_1(\omega) \cdot P(\omega)$$

and

$$R(\omega) = S(\omega) + P_2(\omega) \cdot P(\omega).$$

Substituting the second equation into the first yields

$$\begin{aligned} Q(\omega) &= (S(\omega) + P_2(\omega) \cdot P(\omega)) + P_1(\omega) \cdot P(\omega) \\ &= S(\omega) + (P_1(\omega) + P_2(\omega)) \cdot P(\omega), \end{aligned}$$

and so  $Q(\omega) \equiv S(\omega)$ .

Having verified the axioms, we conclude that  $\equiv$  is indeed an equivalence relation.

Consider now a typical polynomial in  $\mathbb{Z}_p[\omega]$ . Since the maximum degree is  $\alpha - 1$ , there are  $\alpha$  coefficients if we regard missing coefficients as being 0. Since  $|\mathbb{Z}_p| = p$ , there are  $p$  choices for each coefficient, and so  $p^\alpha$  distinct polynomials in  $\mathbb{Z}_p[\omega]$ . Hence, there are at least  $p^\alpha$  equivalence classes. To see that there are no more, let

$$Q(\omega) = R(\omega) + P_1(\omega) \cdot P(\omega).$$

Recall that an appropriate choice of  $P_1(\omega)$  ensures  $\deg(R(\omega)) < \alpha$ . That is,  $Q(\omega)$  is always equivalent to one of the aforementioned  $p^\alpha$  polynomials. Therefore, there are exactly  $p^\alpha$  equivalence classes.  $\square$

**Proposition 10.** *The collection  $S$  of equivalence classes of  $\mathbb{Z}_p[\omega]$  together with  $+$  and  $\times$  defined via*

$$[Q_1(\omega)] + [Q_2(\omega)] = [Q_1(\omega) + Q_2(\omega)]$$

and

$$[Q_1(\omega)] \times [Q_2(\omega)] = [Q_1(\omega) \times Q_2(\omega)]$$

is a field.

*Proof.* We verify the field axioms directly. In what follows, let  $Q(\omega), R(\omega), S(\omega) \in \mathbb{Z}_p[\omega]$  and let  $r(X(\omega))$  denote the residue of  $X(\omega)$  modulo  $P(\omega)$ .

We show first the closure of addition in  $\mathbb{Z}_p[\omega]$ . We know that  $Q(\omega) + R(\omega) = P_1(\omega)P(\omega) + r(Q(\omega) + R(\omega))$  for some polynomial  $P_1(\omega) \in \mathbb{Z}_p[\omega]$ . Now,

$$\begin{aligned} [Q(\omega)] + [R(\omega)] &= [Q(\omega) + R(\omega)] \\ &= r(Q(\omega) + R(\omega)) \\ &\in \mathbb{Z}_p[\omega]. \end{aligned}$$

We show next the closure of multiplication in  $\mathbb{Z}_p[\omega]$ . We know that  $P(\omega)Q(\omega) = P_1(\omega)P(\omega) + r(P(\omega)Q(\omega))$  for some polynomial  $P_1(\omega) \in \mathbb{Z}_p[\omega]$ . Now,

$$\begin{aligned} [Q(\omega)] \times [R(\omega)] &= [Q(\omega)R(\omega)] \\ &= r(Q(\omega)R(\omega)) \\ &\in \mathbb{Z}_p[\omega]. \end{aligned}$$

We show next the associativity of addition in  $\mathbb{Z}_p[\omega]$ . We know that  $Q(\omega) + R(\omega) = P_1(\omega)P(\omega) + r(Q(\omega) + R(\omega))$  and  $R(\omega) + S(\omega) = P_2(\omega)P(\omega) + r(R(\omega) + S(\omega))$  for some polynomials  $P_1(\omega), P_2(\omega) \in \mathbb{Z}_p[\omega]$ . Now,

$$\begin{aligned} ([Q(\omega)] + [R(\omega)]) + [S(\omega)] &= r(r(Q(\omega) + R(\omega)) + S(\omega)) \\ &= r(Q(\omega) + R(\omega) - P_1(\omega)P(\omega) + S(\omega)) \\ &= r(Q(\omega) + R(\omega) + S(\omega)). \end{aligned}$$

Similarly,

$$\begin{aligned} [Q(\omega)] + ([R(\omega)] + [S(\omega)]) &= r(Q(\omega) + r(R(\omega) + S(\omega))) \\ &= r(Q(\omega) + R(\omega) + S(\omega) - P_2(\omega)P(\omega)) \\ &= r(Q(\omega) + R(\omega) + S(\omega)). \end{aligned}$$

Hence, addition is associative in  $\mathbb{Z}_p[\omega]$ .

The associativity of multiplication in  $\mathbb{Z}_p[\omega]$  is similar. As before, we know  $Q(\omega)R(\omega) = P_3(\omega)P(\omega) + r(Q(\omega)R(\omega))$  and  $R(\omega)S(\omega) = P_4(\omega)P(\omega) + r(R(\omega)S(\omega))$  for some polynomials  $P_3(\omega), P_4(\omega) \in \mathbb{Z}_p[\omega]$ . Now,

$$\begin{aligned} ([Q(\omega)] \times [R(\omega)]) \times [S(\omega)] &= r(r(Q(\omega)R(\omega))S(\omega)) \\ &= r((Q(\omega)R(\omega) - P_3(\omega)P(\omega))S(\omega)) \\ &= r(Q(\omega)R(\omega)S(\omega) - S(\omega)P_3(\omega)P(\omega)) \\ &= r(Q(\omega)R(\omega)S(\omega)). \end{aligned}$$

Similarly,

$$\begin{aligned} [Q(\omega)] \times ([R(\omega)] \times [S(\omega)]) &= r(Q(\omega)r(R(\omega)S(\omega))) \\ &= r(Q(\omega)(R(\omega)S(\omega) - P_4(\omega)P(\omega))) \\ &= r(Q(\omega)R(\omega)S(\omega) - Q(\omega)P_4(\omega)P(\omega)) \\ &= r(Q(\omega)R(\omega)S(\omega)). \end{aligned}$$

Hence, multiplication is associative in  $\mathbb{Z}_p[\omega]$ .

We show next that addition and multiplication are commutative in  $\mathbb{Z}_p[\omega]$ . It follows immediately from the commutativity of addition in  $\mathbb{Z}$  that

$$\begin{aligned} [Q(\omega)] + [R(\omega)] &= [Q(\omega) + R(\omega)] \\ &= [R(\omega) + Q(\omega)] \\ &= [R(\omega)] + [Q(\omega)]. \end{aligned}$$

Similarly, because of the commutativity of multiplication in  $\mathbb{Z}$ ,

$$\begin{aligned} [Q(\omega)] \times [R(\omega)] &= [Q(\omega)R(\omega)] \\ &= [R(\omega)Q(\omega)] \\ &= [R(\omega)] \times [Q(\omega)]. \end{aligned}$$

We show next that  $[0]$  is the additive identity and  $[1]$  the multiplicative identity in  $\mathbb{Z}_p[\omega]$ . It follows immediately from the fact that  $0$  is the additive identity in  $\mathbb{Z}$  that

$$\begin{aligned} [Q(\omega)] + [0] &= [Q(\omega) + 0] \\ &= [Q(\omega)]. \end{aligned}$$

Similarly, since 1 is the multiplicative identity in  $\mathbb{Z}$ ,

$$\begin{aligned} [Q(\omega)] \times [1] &= [Q(\omega) \cdot 1] \\ &= [Q(\omega)]. \end{aligned}$$

We show next that, for all  $Q(\omega) \in \mathbb{Z}_p[\omega]$ , there exists an additive inverse  $-Q(\omega) \in \mathbb{Z}_p[\omega]$ . Let  $Q(\omega) = a_0 + a_1\omega + \cdots + a_{\alpha-1}\omega^{\alpha-1}$  and  $-Q(\omega) = (-a_0) + (-a_1)\omega + \cdots + (-a_{\alpha-1})\omega^{\alpha-1}$ . It follows that

$$\begin{aligned} [Q(\omega)] + [-Q(\omega)] &= [Q(\omega) + (-Q(\omega))] \\ &= [(a_0 - a_0) + (a_1 - a_1)\omega + \cdots + (a_{\alpha-1} - a_{\alpha-1})\omega^{\alpha-1}] \\ &= [0]. \end{aligned}$$

Hence, every element of  $\mathbb{Z}_p[\omega]$  has an additive inverse.

We show next that, for all  $Q(\omega) \in \mathbb{Z}_p[(\omega)]$ , there exists a multiplicative inverse  $Q^{-1}[(\omega)] \in \mathbb{Z}_p[(\omega)]$ . To establish this fact, we show that the set

$$S = \{S(\omega) \times Q(\omega) \mid S(\omega) \in \mathbb{Z}_p[(\omega)]\}$$

contains  $|\mathbb{Z}_p[(\omega)]|$  distinct elements, and so one of the products equals 1.

Observe first that the only zero element of  $S$  is  $0 \times_p Q(\omega)$ . Suppose, to the contrary, that  $R(\omega) \times_p Q(\omega) = 0$  for some  $R(\omega) \in \mathbb{Z}_p[\omega]$ . Since  $P(\omega)$  is irreducible and  $P(\omega)$  divides 0,  $P(\omega)$  divides  $R(\omega)$  (since it cannot divide  $Q(\omega)$ ). Thus,  $R(\omega) = 0$ .

Next, we show that all elements of  $S$  are distinct. Let  $R(\omega) \times Q(\omega) = S(\omega) \times Q(\omega)$  for  $R(\omega), S(\omega) \in \mathbb{Z}_p[\omega]$ . Since  $R(\omega)Q(\omega) = R'(\omega)P(\omega) + r(R(\omega)Q(\omega))$  and  $S(\omega)Q(\omega) = S'(\omega)P(\omega) + r(S(\omega)Q(\omega))$  for some  $R'(\omega), S'(\omega) \in \mathbb{Z}_p[\omega]$ , we have

$$\begin{aligned} (R(\omega) - S(\omega))Q(\omega) &= R(\omega)Q(\omega) - S(\omega)Q(\omega) \\ &= R'(\omega)P(\omega) + r(R(\omega)Q(\omega)) - (S'(\omega)P(\omega) + r(S(\omega)Q(\omega))) \\ &= R'(\omega)P(\omega) - S'(\omega)P(\omega) \\ &= (R'(\omega) - S'(\omega))P(\omega). \end{aligned}$$

Thus,  $P(\omega)$  divides  $(R(\omega) - S(\omega))Q(\omega)$ , and so  $P(\omega)$  divides  $R(\omega) - S(\omega)$  (since it cannot divide  $Q(\omega)$ ). Since  $R(\omega) - S(\omega) \in \mathbb{Z}_p[\omega]$ , it follows that  $R(\omega) - S(\omega) = 0$ . In other words,  $R(\omega) = S(\omega)$ , and so the chosen elements of  $S$  are identical. Therefore,  $S$  contains  $|\mathbb{Z}_p[\omega]|$  distinct elements, and so a multiplicative inverse exists for  $Q(\omega)$ .

We show finally that multiplication distributes over addition in  $\mathbb{Z}_p[\omega]$ . We know that

$$\begin{aligned} R(\omega) + S(\omega) &= P_2(\omega)P(\omega) + r(Q(\omega) + R(\omega)), \\ Q(\omega)R(\omega) &= P_3(\omega)P(\omega) + r(Q(\omega)R(\omega)), \text{ and} \\ Q(\omega)S(\omega) &= P_5(\omega)P(\omega) + r(Q(\omega)S(\omega)). \end{aligned}$$

It follows that

$$\begin{aligned} [Q(\omega)] \times ([R(\omega)] + [S(\omega)]) &= r(Q(\omega)r(R(\omega) + S(\omega))) \\ &= r(Q(\omega)(R(\omega) + S(\omega) - P_2(\omega)P(\omega))) \\ &= r(Q(\omega)R(\omega) + Q(\omega)S(\omega) - Q(\omega)P_2(\omega)P(\omega)) \\ &= r(Q(\omega)R(\omega) + Q(\omega)S(\omega)). \end{aligned}$$

Similarly,

$$\begin{aligned} ([Q(\omega)] \times [R(\omega)]) + ([Q(\omega)] \times [S(\omega)]) &= r(r(Q(\omega)R(\omega)) + r(Q(\omega)S(\omega))) \\ &= r(Q(\omega)R(\omega) - P_3(\omega)P(\omega) + Q(\omega)S(\omega) - P_5(\omega)P(\omega)) \\ &= r(Q(\omega)R(\omega) + Q(\omega)S(\omega) - (P_3(\omega) + P_5(\omega))P(\omega)) \\ &= r(Q(\omega)R(\omega) + Q(\omega)S(\omega)). \end{aligned}$$

Hence, multiplication distributes over addition in  $\mathbb{Z}_p[\omega]$ .

Having verified the field axioms, we conclude that the set  $S$  of equivalence classes of polynomials in  $\mathbb{Z}_p[\omega]$  together with addition and multiplication as defined is indeed a field.  $\square$

We give below the addition and multiplication tables for  $GF(8)$ .

+	0	1	$\omega$	$\omega + 1$	$\omega^2$	$\omega^2 + 1$	$\omega^2 + \omega$	$\omega^2 + \omega + 1$
0	0	1	$\omega$	$\omega + 1$	$\omega^2$	$\omega^2 + 1$	$\omega^2 + \omega$	$\omega^2 + \omega + 1$
1	1	0	$\omega + 1$	$\omega$	$\omega^2 + 1$	$\omega^2$	$\omega^2 + \omega + 1$	$\omega^2 + \omega$
$\omega$	$\omega$	$\omega + 1$	0	1	$\omega^2 + \omega$	$\omega^2 + \omega + 1$	$\omega^2$	$\omega^2 + 1$
$\omega + 1$	$\omega + 1$	$\omega$	1	0	$\omega^2 + \omega + 1$	$\omega^2 + \omega$	$\omega^2 + 1$	$\omega + 1$
$\omega^2$	$\omega^2$	$\omega^2 + 1$	$\omega^2 + \omega$	$\omega^2 + \omega + 1$	0	1	$\omega$	$\omega + 1$
$\omega^2 + 1$	$\omega^2 + 1$	$\omega^2$	$\omega^2 + \omega + 1$	$\omega^2 + \omega$	1	0	$\omega + 1$	$\omega$
$\omega^2 + \omega$	$\omega^2 + \omega$	$\omega^2 + \omega + 1$	$\omega^2$	$\omega^2 + 1$	$\omega$	$\omega + 1$	0	1
$\omega^2 + \omega + 1$	$\omega^2 + \omega + 1$	$\omega^2 + \omega$	$\omega^2 + 1$	$\omega^2$	$\omega + 1$	$\omega$	1	0

16

$\times$	0	1	$\omega$	$\omega + 1$	$\omega^2$	$\omega^2 + 1$	$\omega^2 + \omega$	$\omega^2 + \omega + 1$
0	0	0	0	0	0	0	0	0
1	0	1	$\omega$	$\omega + 1$	$\omega^2$	$\omega^2 + 1$	$\omega^2 + \omega$	$\omega^2 + \omega + 1$
$\omega$	0	$\omega$	$\omega^2$	$\omega^2 + \omega$	$\omega + 1$	1	$\omega^2 + \omega + 1$	$\omega^2 + 1$
$\omega + 1$	0	$\omega + 1$	$\omega^2 + \omega$	$\omega^2 + 1$	$\omega^2 + \omega + 1$	$\omega^2$	1	$\omega$
$\omega^2$	0	$\omega^2$	$\omega + 1$	$\omega^2 + \omega + 1$	$\omega^2 + \omega$	$\omega$	$\omega^2 + 1$	1
$\omega^2 + 1$	0	$\omega^2 + 1$	1	$\omega^2$	$\omega$	$\omega^2 + \omega + 1$	$\omega + 1$	$\omega^2 + \omega$
$\omega^2 + \omega$	0	$\omega^2 + \omega$	$\omega^2 + \omega + 1$	1	$\omega^2 + 1$	$\omega + 1$	$\omega$	$\omega^2$
$\omega^2 + \omega + 1$	0	$\omega^2 + \omega + 1$	$\omega^2 + 1$	$\omega$	1	$\omega^2 + \omega$	$\omega^2$	$\omega + 1$

We give below all reducible polynomials of degree 3 along with their factorizations.

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

The remaining polynomials

$$\begin{aligned}
&\omega^3 + \omega + 1, \text{ and} \\
&\omega^3 + \omega^2 + 1
\end{aligned}$$

must therefore be irreducible.

We give below all reducible polynomials of degree 4 along with their factorizations.

$$\begin{aligned}
\omega^4 &= \omega\omega\omega\omega \\
\omega^4 + \omega^3 &= \omega\omega\omega(\omega + 1) \\
\omega^4 + \omega^2 &= \omega\omega(\omega + 1)(\omega + 1) \\
\omega^4 + \omega^3 + \omega^2 + \omega &= \omega(\omega + 1)(\omega + 1)(\omega + 1) \\
\omega^4 + 1 &= (\omega + 1)(\omega + 1)(\omega + 1)(\omega + 1) \\
\omega^4 + \omega^3 + \omega^2 &= \omega\omega(\omega^2 + \omega + 1) \\
\omega^4 + \omega &= \omega(\omega + 1)(\omega^2 + \omega + 1) \\
\omega^4 + \omega^3 + \omega + 1 &= (\omega + 1)(\omega + 1)(\omega^2 + \omega + 1) \\
\omega^4 + \omega^2 + \omega &= \omega(\omega^3 + \omega + 1) \\
\omega^4 + \omega^3 + \omega^2 + 1 &= (\omega + 1)(\omega^3 + \omega + 1) \\
\omega^4 + \omega^3 + \omega &= \omega(\omega^3 + \omega^2 + 1) \\
\omega^4 + \omega^2 + \omega + 1 &= (\omega + 1)(\omega^3 + \omega^2 + 1) \\
\omega^4 + \omega^2 + 1 &= (\omega^2 + \omega + 1)(\omega^2 + \omega + 1)
\end{aligned}$$

The remaining polynomials

$$\begin{aligned}
&\omega^4 + \omega + 1 \\
&\omega^4 + \omega^3 + 1 \\
&\omega^4 + \omega^3 + \omega^2 + \omega + 1
\end{aligned}$$

must therefore be irreducible.

## Problem 7

**Proposition 11.** *Let  $p$  be a fixed prime. The number  $m_\alpha$  of monic irreducible polynomials of degree  $\alpha$  over  $\mathbb{Z}_p$  satisfies the inequality*

$$m_\alpha \geq \frac{1}{\alpha} \left( p^\alpha - \sum_{d=1}^{\lfloor \frac{\alpha}{2} \rfloor} p^d \right),$$

which is greater than zero for all primes  $p$  and all  $\alpha \geq 1$ .

*Proof.* (I see that  $p^d$  is the total number of monic polynomials of degree  $d$  over  $\mathbb{Z}_p$ , so the righthand side of

$$\sum_{d=0}^{\infty} p^d x^d = \prod_{\alpha=1}^{\infty} (1 + x^\alpha + x^{2\alpha} + \dots)^{m_\alpha}$$

should admit some enumeration of factorizations of the polynomials. I am unable to work out the details of this count, however.)

Using the geometric series, we obtain

$$\begin{aligned} \sum_{d=0}^{\infty} p^d x^d &= \sum_{d=0}^{\infty} (px)^d \\ &= \frac{1}{1 - px} \end{aligned}$$

and

$$\begin{aligned} 1 + x^\alpha + x^{2\alpha} + \dots &= \sum_{j=0}^{\infty} (x^\alpha)^j \\ &= \frac{1}{1 - x^\alpha}. \end{aligned}$$

Thus,

$$\frac{1}{1 - px} = \prod_{\alpha=1}^{\infty} \left( \frac{1}{1 - x^\alpha} \right)^{m_\alpha}.$$

Taking the formal logarithm of both sides yields

$$-\ln(1 - px) = \sum_{\alpha=1}^{\infty} -m_\alpha \ln(1 - x^\alpha).$$

Now, using the Taylor series for the natural logarithm,

$$\begin{aligned} -\ln(1 - px) &= -\sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j} (-px)^j \\ &= \sum_{j=1}^{\infty} \frac{p^j}{j} x^j \end{aligned}$$

and

$$\begin{aligned} -\ln(1 - x^\alpha) &= -\sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j} (-x^\alpha)^j \\ &= \sum_{j=1}^{\infty} \frac{x^{j\alpha}}{j}. \end{aligned}$$

Thus,

$$\begin{aligned} \sum_{j=1}^{\infty} \frac{p^j}{j} x^j &= \sum_{\alpha=1}^{\infty} m_\alpha \sum_{j=1}^{\infty} \frac{x^{j\alpha}}{j} \\ &= \sum_{k=1}^{\infty} \sum_{\alpha|k} m_\alpha \frac{\alpha}{k} x^k, \end{aligned}$$

where  $k = j\alpha$ . Matching coefficients, we see that

$$\frac{p^k}{k} = \sum_{\alpha|k} m_\alpha \frac{\alpha}{k},$$

for each  $k$ , and so

$$p^k = \sum_{\alpha|k} m_\alpha \alpha.$$

Applying Möbius inversion, we obtain

$$\begin{aligned}
m_\alpha &= \frac{1}{\alpha} \sum_{d|\alpha} \mu\left(\frac{\alpha}{d}\right) p^d \\
&= \frac{1}{\alpha} \left( p^\alpha + \sum_{\substack{d=1 \\ d|\alpha}}^{\lfloor \frac{\alpha}{2} \rfloor} \mu\left(\frac{\alpha}{d}\right) p^d \right) \\
&\geq \frac{1}{\alpha} \left( p^\alpha - \sum_{d=1}^{\lfloor \frac{\alpha}{2} \rfloor} p^d \right).
\end{aligned}$$

We show by induction on  $\alpha$  that the expression above is greater than zero for all primes  $p$  by showing, equivalently,

$$p^\alpha > \sum_{d=1}^{\lfloor \frac{\alpha}{2} \rfloor} p^d.$$

For the base case  $\alpha = 1$ , we have  $p > 1$ . Assume now the inequality holds for a given  $\alpha$ . It follows that

$$\begin{aligned}
p^{\alpha+1} &= pp^\alpha \\
&> p \sum_{d=1}^{\lfloor \frac{\alpha}{2} \rfloor} p^d \\
&= \sum_{d=1}^{\lfloor \frac{\alpha}{2} \rfloor} p^{d+1} \\
&= \sum_{d=2}^{\lfloor \frac{\alpha+1}{2} \rfloor} p^d \\
&> \sum_{d=1}^{\lfloor \frac{\alpha+1}{2} \rfloor} p^d.
\end{aligned}$$

Therefore, there are monic irreducible polynomials in  $GF(p^\alpha)$  for all primes  $p$  and  $\alpha \geq 1$ .  $\square$