math 228

SOLUTIONS TO FINAL EXAMINATION

Instructor: I. E. Leonard **Time: 2 Hours**

1. Let A be a commutative ring with identity $1 \in A$.

   (a) Define what is means for an element $a \in A$ to be a *unit*.

   Define what it means for an element $a \in A$ to be a *zero divisor*.

   (b) Let $\mathbb{Z}_{12}^*$ denote the set of all units in $\mathbb{Z}_{12}$. Construct a multiplication table for $\mathbb{Z}_{12}^*$ and answer the questions below.

   (i) How many units are there in $\mathbb{Z}_{12}$?

   (ii) How many zero divisors are there in Z_{12} ?

   (iii) How many elements in $\mathbb{Z}_{12}^*$ are their own inverse?

   Solution:

   (a) An element $a \in A$ is a **unit** if and only if a has a multiplicative inverse in A, that is, if and only if there exists an element $b \in A$ such that $a \cdot b = 1$.

   An element $a \in A$ is a **zero divisor** if and only if $a \neq 0$ and there exists an element $b \in A$, $b \neq 0$, such that $a \cdot b = 0$.

   (b) The multiplication table for $\mathbb{Z}_{12}^*$ is given below.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

   (i) There are 4 units in $\mathbb{Z}_{12}$: namely, 1, 5, 7, 11.

   (ii) There are 7 zero divisors in $\mathbb{Z}_{12}$: namely, 2, 3, 4, 6, 8, 9, 10, since

$$2 \cdot 6 = 0, \quad 3 \cdot 4 = 0, \quad 3 \cdot 8 = 0, \quad 4 \cdot 9 = 0, \quad 6 \cdot 10 = 0.$$

   (iii) From the table, we see immediately that every element of $\mathbb{Z}_{12}^*$ is its own inverse, that is $a^2 = a \cdot a = 1$ for all $a \in \mathbb{Z}_{12}^*$.

2. Use Gaussian elimination to solve the system of linear equations

$$\begin{aligned} 3x + 2y \quad\quad\; + \;\; w &= 2 \\ y + \;\, 4z + 2w &= 1 \\ x + 2y + \quad z + 3w &= 4 \end{aligned}$$

in $\mathbb{Z}_5$. How many solutions are there?

SOLUTION: We can use elementary row operations to reduce the augmented matrix for this system to an upper triangular matrix as follows.

$$\begin{pmatrix} 3 & 2 & 0 & 1 & 2 \\ 0 & 1 & 4 & 2 & 1 \\ 1 & 2 & 1 & 3 & 4 \end{pmatrix} \xrightarrow{R_1 \leftrightarrow R_3} \begin{pmatrix} 1 & 2 & 1 & 3 & 4 \\ 0 & 1 & 4 & 2 & 1 \\ 3 & 2 & 0 & 1 & 2 \end{pmatrix}$$

$$\xrightarrow{R_3 \to R_3 - 3R_1} \begin{pmatrix} 1 & 2 & 1 & 3 & 4 \\ 0 & 1 & 4 & 2 & 1 \\ 0 & 1 & 2 & 2 & 0 \end{pmatrix} \xrightarrow{R_3 \to R_3 - R_2} \begin{pmatrix} 1 & 2 & 1 & 3 & 4 \\ 0 & 1 & 4 & 2 & 1 \\ 0 & 0 & 3 & 0 & 4 \end{pmatrix}$$

We can read off the solution from the bottom up. The last row of the matrix is equivalent to the equation

$$3z = 4,$$

and multiplying this by 2, we have $z = 3$.

The second row of the matrix is equivalent to the equation

$$y + 4z + 2w = 1,$$

so that $y = 4 + 3w$.

Finally, the first row of the matrix is equivalent to

$$x + 2y + z + 3z = 4,$$

so that $x = 3 + w$.

Therefore, the solution to the system is given by

$$\begin{aligned} x &= 3 + w \\ y &= 4 + 3w \\ z &= 3, \end{aligned}$$

where $w \in \mathbb{Z}_5$ is arbitrary.

There are exactly 5 solutions to the system of equations, corresponding to $w = 0,\ 1,\ 2,\ 3,\ 4$.

3. (a) What does it mean for a positive integer p to be a *prime*?

   (b) What does it mean for two positive integers a and b to be *relatively prime*?

   (c) Is 409 a prime?

   (d) How many integers $k \in \mathbb{Z}$ with $1 \leq k \leq 409$ are there that are relatively prime to 409?

   (e) How many units are there in $\mathbb{Z}_{409}$?

   (f) Use the Euclidean algorithm to find the inverse of 135 in $\mathbb{Z}_{409}$.

SOLUTION:

(a) A positive integer p is a **prime** if and only if $p > 1$, and whenever $d \in \mathbb{N}$ and $d \,\big|\, p$, this implies that either $d = 1$ or $d = p$.

(b) Two positive integers a and b are **relatively prime** if and only if their greatest common divisor is 1, that is, whenever $d \in \mathbb{N}$ and $d \,\big|\, a$ and $d \,\big|\, b$ this implies that $d = 1$.

(c) It is easy to check that 409 has no prime divisors less than 21, so that 409 is a prime.

(d) The number of integers k with $1 \leq k \leq 409$ that are relatively prime to 409 is 408, namely, all the integers k with $1 \leq k \leq 408$.

(e) The number of units in $\mathbb{Z}_{409}$ is the number of integers $1 \leq k \leq 409$ that are relatively prime to 409, namely 408.

(f) We use the Euclidean algorithm to find the greatest common divisor of 135 and 409, which we know is 1, and then work from the bottom up to write 1 as a linear combination of 135 and 409.

$$\begin{aligned}409 &= 3 \cdot 135 + 4\\ 135 &= 33 \cdot 4 + 3\\ 4 &= 1 \cdot 3 + 1\\ 3 &= 3 \cdot 1 + 0\end{aligned}$$

and the last nonzero remainder is $(135, 409) = 1$. Working from the bottom up, we have

$$\begin{aligned}1 &= 4 - 3 = 4 - (135 - 33 \cdot 4) = 34 \cdot 4 - 135\\ &= 34 \cdot (409 - 3 \cdot 135) - 135 = 34 \cdot 409 - 103 \cdot 135\end{aligned}$$

and therefore $135^{-1} = -103 = 306$ in $\mathbb{Z}_{409}$.

4. (a) Given a polynomial $f(x)$ over a field $\mathbb{F}$, what does it mean to say that $f(x)$ is irreducible over $\mathbb{F}$?

   (b) Factor the polynomial $p(x) = x^5 + x^2 + x + 1$ into a product of irreducible factors in $\mathbb{Z}_2[x]$.

SOLUTION:

(a) A nonzero polynomial $f(x)$ is **irreducible over** $\mathbb{F}$ if and only if its only divisors are the nonzero constant polynomials and it associates, equivalently, if and only if

   (i) $\deg f(x) \geq 1$, and

   (ii) if $f(x) = p(x) \cdot q(x)$ in $\mathbb{F}[x]$, then either $\deg p(x) = 0$ or $\deg q(x) = 0$.

(b) If $p(x) = x^5 + x^2 + x + 1$, then $p(0) = 1$, and $p(1) = 0$, so that $p(x)$ has only the root $a = 1$ in $\mathbb{Z}_2$. From the Factor Theorem, $x - 1 = x + 1$ is a factor of $p(x)$, and from the Division Algorithm or long division, we have

$$p(x) = (x + 1)^2 (x^3 + x + 1),$$

and finally, since $x^3 + x + 1$ has no roots in $\mathbb{Z}_2$ and is of degree 3, then it is irreducible over $\mathbb{Z}_2$.

5. Let $p(x) = x^2 + x + 8$ in $\mathbb{Z}_{10}[x]$.

   (a) Find all the roots of $p(x)$ in $\mathbb{Z}_{10}$.

   (b) Give two different factorizations of $p(x)$ in $\mathbb{Z}_{10}[x]$.

   SOLUTION:

   (a) For $p(x) = x^2 + x + 8$ in $\mathbb{Z}_{10}[x]$, we have

$$\begin{array}{llll} p(0) = 8, & p(1) = 0, & p(2) = 4, & p(3) = 0, \\ p(4) = 8, & p(5) = 8, & p(6) = 0, & p(7) = 4, \\ p(8) = 0, & p(9) = 8, & p(10) = 8, & \end{array}$$

   Therefore, $p(x)$ has 4 roots in $\mathbb{Z}_{10}$, namely, $1,\ 3,\ 6,\ 8$.

   (b) From the Division Algorithm or long division, we have the following factorizations of $p(x)$,

$$p(x) = (x-1)\cdot(x-8) \qquad \text{and} \qquad p(x) = (x-3)\cdot(x-6)$$

   in $\mathbb{Z}_{10}[x]$.

6. Let $f(x) = x^4 + 4$ in $\mathbb{C}[x]$.

   (a) Show that $f(x)$ has no roots in $\mathbb{Q}$.

   (b) Show that $f(x)$ is not irreducible over $\mathbb{Z}$.

   (c) Factor $f(x)$ into a product of irreducible factors over $\mathbb{C}$.

   SOLUTION:

   (a) If $r = \dfrac{c}{d} \in \mathbb{Q}$ is a root of $f(x)$, then from the Rational Roots Theorem, we have $d \mid 1$ and $c \mid 4$, and the only possibilities are $d = \pm 1$ and $c = \pm 1, \pm 2, \pm 4$. Therefore, the only possible roots in $\mathbb{Q}$ are $\pm 1, \pm 2, \pm 4$, none of which is a root, so $f(x)$ has no roots in $\mathbb{Q}$.

   (b) If $f(x)$ factors over $\mathbb{Z}$, then it also factors over $\mathbb{Q}$, and since it has no linear factors, it must factor into the product of two quadratics. By symmetry, we may assume that

$$f(x) = \big(x^2 + ax + 2\big)\cdot\big(x^2 - ax + 2\big)$$

   for some $a \in \mathbb{Z}$. After simplifying this product, we have

$$f(x) = x^4 + (4 - a^2)x^2 + 4,$$

   so that $a^2 = 4$ and $a = \pm 2$. Thus, $f(x) = x^4 + 4$ factors over $\mathbb{Z}$ as

$$x^4 + 4 = (x^2 + 2x + 2)\cdot(x^2 - 2x + 2)$$

   so that $f(x)$ is not irreducible over $\mathbb{Z}$.

   (c) Note that

$$x^2 + 2x + 2 = x^2 + 2x + 1 + 1 = (x+1)^2 + 1 = (x+1)^2 - i^2 = (x+1+i)\cdot(x+1-i)$$

   and that

$$x^2 - 2x + 2 = x^2 - 2x + 1 + 1 = (x-1)^2 + 1 = (x-1)^2 - i^2 = (x-1+i)\cdot(x-1-i)$$

   so that we can write

$$f(x) = (x+1+i)\cdot(x+1-i)\cdot(x-1+i)\cdot(x-1-i)$$

   as a product of irreducibles over $\mathbb{C}$.

7. (a) Given a prime p and a polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x],$$

we define the **reduction of** $f(x)$ **modulo** p to be the polynomial

$$\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_n x^n \in \mathbb{Z}_p[x].$$

Show that the mapping $T : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ given by $T(f(x)) = \overline{f}(x)$ for $f(x) \in \mathbb{Z}[x]$, is a ring homomorphism onto $\mathbb{Z}_p[x]$.

(b) Prove *Gauss's Lemma*: If $f(x) = g(x) \cdot h(x)$ in $\mathbb{Z}[x]$ and if a prime p divides every coefficient of $f(x)$, then either p divides every coefficient of $g(x)$ or p divides every coefficient of $h(x)$.

Solution:

(a) Suppose that $f(x) = \sum_i a_i x^i$ and $g(x) = \sum_i b_i x^i$ in $\mathbb{Z}[x]$, then $f(x) + g(x) = \sum_i (a_i + b_i) x^i$ in $\mathbb{Z}[x]$. Therefore,

$$T\left(f(x) + g(x)\right) = \sum_i \left(\overline{a_i + b_i}\right) x^i = \sum_i \left(\overline{a}_i + \overline{b}_i\right) x^i = \sum_i \overline{a}_i x^i + \sum_i \overline{b} x^i = T\left(f(x)\right) + T\left(g(x)\right)$$

in $\mathbb{Z}_p[x]$.

Also, $f(x) \cdot g(x) = \sum_k c_k x^k$ in $\mathbb{Z}[x]$, where $c_k = \sum_i a_i \cdot b_{k-i}$. Therefore,

$$T\left(f(x) \cdot g(x)\right) = \sum_k \overline{c}_k x^k$$

where

$$\overline{c}_k = \overline{\sum_i a_i \cdot b_{k-i}} = \sum_i \overline{a_i \cdot b_{k-i}} = \sum_i \overline{a}_i \cdot \overline{b}_{k-i},$$

so that $T\left(f(x) \cdot g(x)\right) = T\left(f(x)\right) \cdot T\left(g(x)\right)$ in $\mathbb{Z}_p[x]$.

Therefore,

$$T\left(f(x) + g(x)\right) = T\left(f(x)\right) + T\left(g(x)\right) \qquad \text{and} \qquad T\left(f(x) \cdot g(x)\right) = T\left(f(x)\right) \cdot T\left(g(x)\right)$$

for all $f(x)$, $g(x) \in \mathbb{Z}[x]$, and $T : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ is a ring homomorphism.

To see that T is onto, given any $g(x) = \sum_i \overline{a}_i x^i \in \mathbb{Z}_p[x]$, we have

$$g(x) = T\left(f(x)\right)$$

where $f(x) = \sum_i a_i x^i \in \mathbb{Z}[x]$.

(b) If $f(x) = g(x) \cdot h(x)$ in $\mathbb{Z}[x]$ and p is a prime that divides every coefficient of $f(x)$, then

$$\overline{f}(x) = \overline{g}(x) \cdot \overline{h}(x) = \overline{0}$$

in $\mathbb{Z}_p[x]$, and since $\mathbb{Z}_p[x]$ is an integral domain, then either $\overline{g}(x) = \overline{0}$ or $\overline{h}(x) = \overline{0}$, that is, either all coefficients of $g(x)$ are divisible by p, or all coefficients of $h(x)$ are divisible by p.

8. (a) State the Chinese Remainder Theorem.

(b) When the marchers in the annual Mathematics Department Parade lined up 4 abreast, there was 1 odd person; when they tried 5 abreast, there were 2 left over; and when they tried 7 abreast, there were 3 left over. How large is the department?

SOLUTION:

(a) The **Chinese Remainder Theorem** states that if the positive integers $m_1, m_2, \ldots, m_k$ are pairwise relatively prime, then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo $M = m_1 \cdot m_2 \cdots m_k$.

(b) We have to solve the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{4} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

where $m_1 = 4$, $m_2 = 5$, and $m_3 = 7$. As in class, we let

$$M_1 = m_2 \cdot m_3 = 5 \cdot 7 = 35, \qquad M_2 = m_1 \cdot m_3 = 4 \cdot 7 = 28, \qquad M_3 = m_1 \cdot m_2 = 4 \cdot 5 = 20,$$

and let

$$\begin{aligned} y_1 &\equiv M_1^{-1} (\mathrm{mod}\ m_1) \equiv 3 \pmod{4} \\ y_2 &\equiv M_2^{-1} (\mathrm{mod}\ m_2) \equiv 2 \pmod{5} \\ y_3 &\equiv M_3^{-1} (\mathrm{mod}\ m_3) \equiv 6 \pmod{7} \end{aligned}$$

then the solution is

$$x \equiv a_1 \cdot y_1 \cdot M_1 + a_2 \cdot y_2 \cdot M_2 + a_3 \cdot y_3 \cdot M_3 \pmod{m_1 \cdot m_2 \cdot m_3},$$

and we have

$$x \equiv 1 \cdot 3 \cdot 35 + 2 \cdot 2 \cdot 28 + 3 \cdot 6 \cdot 20 \equiv 17 \pmod{140}.$$

However, in light of the fact that they have an annual parade, a more reasonable size for the Department of Mathematics might be $x = 17 + 140 = 157$.