MATH 558 Additional Homework Problems

Refer to Homework Assignment page for due dates of individual problems.

1. For what values of \( m \) will the equation \( x^2 - (2m + 2)x + (4m + 1) = 0 \) have equal roots? (You need to give values of \( m \) that work, and show no other values of \( m \) work.)

2. Suppose that 1, 2, and 3 are roots of the degree five polynomial equation,

\[
x^5 - 8x^4 + 15x^3 + 20x^2 - 76x + 48 = 0.
\]

The equation has two additional roots. What are they? (Hint: Avoid long division—and that means synthetic division, too.)

3. Find an integer \( k \in \mathbb{Z}_5 \) such that \( 1! + 2! + \cdots + 100! \equiv k \mod 5 \). (\( i! = i(i-1)\cdots2\cdot1 \)) Justify your answer.

4. Suppose \( a \) and \( b \) are integers, \( n \) and \( m \) are positive integers, and \( m|n \).

Prove: If \( a \equiv b \pmod{n} \), then \( a \equiv b \pmod{m} \).

5. Let \( a_0 = a_1 = 1 \) and \( a_{n+2} = a_{n+1} + 5a_n \) for \( n \geq 0 \). Prove (by induction) that \( a_n \leq 3^n \) for all \( n \geq 0 \).

6. Prove (by induction): For all positive integers \( n \), \( 5^n \equiv 1 + 4n \pmod{16} \).

7. (a) Find \( \gcd(350, 155) \).

(b) Find integers \( A \) and \( B \) such that \( 350A + 155B = \gcd(350, 155) \).

8. (a) Solve the equation \( x^4 \equiv 1 \) in \( \mathbb{Z}_5 \).

(b) Prove: If \( a \in \mathbb{Z}_5 \), \( a \neq 0 \), and \( q \) and \( r \) are nonnegative integers, then \( a^{4q+r} \equiv a^r \pmod{5} \).

(c) Do Exercise #18, p. 61. (Use part (b).)

9. Prove: If \( n \) is a positive integer and \( n \equiv 3 \pmod{4} \), then \( n \) has a prime divisor \( p \) such that \( p \equiv 3 \pmod{4} \).

10. Find an integer \( p \) such that \( p \) is prime in \( \mathbb{Z} \), but \( p = p + 0 \cdot \sqrt{-5} \) is not prime in \( \mathbb{Z}[\sqrt{-5}] \).

11. Prove: For any integer \( n \geq 2 \), the multiplicative inverse modulo \( n \) of \( n - 1 \) in \( \mathbb{Z}_n \) is \( n - 1 \).

12. (a) Prove: If \( p \) is prime and \( a \) is a nonzero element of \( \mathbb{Z}_p \), then \( a^{p-2} \) is a multiplicative inverse of \( a \) modulo \( p \).

(b) Use (a) to find a multiplicative inverse of 5 modulo 11 in \( \mathbb{Z}_{11} \).
13. Use the axioms defining fields to prove the following for any field $F$ and any element $a \in F$. Justify each step by referring to one of the defining axioms or to a previous result.

(a) $-(-a) = a$
(b) $a + (-1) \cdot a = 0$
(c) $(-1) \cdot a = -a$
(d) For $a \neq 0$, $(-a)^{-1} = -(a^{-1})$

14. Prove: If $F$ is any field and $a \in F$, $a \neq 0$, then the multiplicative inverse of $a$ is unique, i.e., only one element $a^{-1}$ satisfies $a \cdot a^{-1} = 1$.

15. Prove: If $P(x)$ and $Q(x)$ are nonzero polynomials in $F[x]$, then $P(x)Q(x)$ is not the zero polynomial.

16. Prove: If $P(x)$ is a polynomial in $F[x]$ of degree at least 1, then $P(x)$ does not have a multiplicative inverse, that is, there is no polynomial $Q(x)$ in $F[x]$ such that $P(x)Q(x) = 1$.

17. (a) For which $c \in \mathbb{Q}$ is $x - 1$ a factor of $x^{100} - 3x^{60} + 5x^{20} + 2x + c$ in $\mathbb{Q}[x]$? ($\mathbb{Q}$ is the field of rational numbers.)
   (b) For which $c \in \mathbb{Z}_3$ is $x - 1$ a factor of $x^{100} - 3x^{60} + 5x^{20} + 2x + c$ in $\mathbb{Z}_3[x]$?

18. Find all primes $p$ for which $x - 1$ is a factor of $x^{75} + 13x^{63} + 10x^{40} + 6x^5$ in $\mathbb{Z}_p[x]$.

19. Let $p$ be a prime.
   (a) Show that every degree 3 polynomial in $\mathbb{Z}_p[x]$ has either 0, 1, or 3 roots (counting multiplicities) in $\mathbb{Z}_p$.
   (b) For each $k$ in $\{0, 1, 3\}$, give a degree 3 polynomial in $\mathbb{Z}_3[x]$ that has $k$ roots in $\mathbb{Z}_3$.

20. Let $P(x) = \sum_{i=0}^{n} a_i x^i$ and $Q(x) = \sum_{j=0}^{m} b_j x^j$ be polynomials in $F[x]$, for any field. The product is a polynomial, so $P(x)Q(x) = \sum_{k=0}^{m+n} c_k x^k$ for some field elements $c_k$. Express $c_k$ in terms of the $a$’s and $b$’s. (Note: I have not followed the book’s convention, but instead matched the subscripts with the exponents; this makes the product formula easier.)

21. How many different polynomials of degree $\leq d$ are there in $\mathbb{Z}_p[x]$? Of degree exactly $d$?

22. Let $P(x)$, $M(x)$, and $N(x)$ be polynomials over a field $F$ such that $P(x)$ is a divisor of the product $M(x)N(x)$. Prove: If $P(x)$ and $M(x)$ are relatively prime, then $P(x)$ is a divisor of $N(x)$.

23. Among the permutations of the set $A = \{1, 2, 3, 4, 5\}$, let $G$ be the set of those whose order is odd. Is $G$ a group of permutations? Justify your answer.
24. (a) Find two permutations $\sigma$ and $\rho$ of $\{1, 2, \ldots, n\}$ (for some $n$) that do not commute, that is, $\sigma \circ \rho \neq \rho \circ \sigma$.

(b) Consider the set $S_3$ of all permutations of $\{1, 2, 3\}$. (You listed them all in disjoint cycle form in \#6, p. 164.) For each $\sigma \in S_3$, $\sigma \neq \text{Id}$, find a permutation $\rho \in S_3$ such that $\sigma \circ \rho \neq \rho \circ \sigma$.

(c) Prove: If $n \geq 3$ then for each permutation $\sigma$ of $\{1, 2, \ldots, n\}$, $\sigma \neq \text{Id}$, there exists a permutation $\rho$ of $\{1, 2, \ldots, n\}$ such that $\sigma \circ \rho \neq \rho \circ \sigma$.

25. Let $G$ be a group, and $b$ an element of $G$. Consider the statement: If $b \neq 1_G$, then for all $a$ in $G$, $a \cdot b \neq a$. Write the contrapositive of this statement, and prove it.

26. Find an example of a group $(G, \ast)$ and elements $a$ and $b$ in $G$ such that $o(a)$ and $o(b)$ are relatively prime, but $o(ab) \neq o(a) \cdot o(b)$.

27. Prove: If $(G, \ast)$ and $(H, \oplus)$ are isomorphic groups with isomorphism $f : G \rightarrow H$, then for all $a$ in $G$, $f(a^{-1}) = (f(a))^{-1}$.

28. Let $G = \mathbb{R}^2$ (the set of ordered pairs of real numbers) with the following operation:

$$(a, b) \ast (c, d) = (ac + bd, ad + bc).$$

(a) Find an identity element $1_G = (i_1, i_2)$, that is, a pair that satisfies $(a, b) \ast (i_1, i_2) = (a, b)$ for all $(a, b)$.

(b) Show that the operation $\ast$ is commutative and associative.

(c) True/False? For every $(a, b) \in G$ there exists an $(r, s) \in G$ such that $(a, b) \ast (r, s) = (i_1, i_2)$ (the identity element you found in (a)).

(d) If the statement above is true, prove it by giving a formula for $r$ and $s$ in terms of $a$ and $b$. If it is false, prove it by giving a specific $(a, b)$ for which there is no $(r, s)$.

29. List all pairs of positive integers $a, b$ such that gcd($a, b$) = 18 and lcm($a, b$) = 540.

30. Prove: If $m$ and $n$ are relatively prime positive integers, $d$ is a positive integer and $d | (mn)$, then there exist unique positive integers $a$ and $b$ such that $d = ab$, $a | m$ and $b | n$.

31. Complete the statement of the theorem and prove it:

A permutation $\sigma$ of $\{1, 2, \ldots, n\}$ is of order 2 if and only if the disjoint cycle form of $\sigma$ is . . . .

32. The following is part of a group table. Fill in the rest of the table to make a full group table. (You do not have to check the result is associative.)

<table>
<thead>
<tr>
<th>$\ast_G$</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>B</td>
<td>D</td>
<td>E</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>F</td>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td>C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>E</td>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3
33. Find an isomorphism between the two groups, $G$ and $H$ whose operations are given in the tables below.

<table>
<thead>
<tr>
<th>$*_G$</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
</tr>
<tr>
<td>B</td>
<td>B</td>
<td>D</td>
<td>E</td>
<td>C</td>
<td>A</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
<td>E</td>
<td>B</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
<td>C</td>
<td>A</td>
<td>E</td>
<td>B</td>
</tr>
<tr>
<td>E</td>
<td>E</td>
<td>A</td>
<td>D</td>
<td>B</td>
<td>C</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$*_H$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

34. Prove: Let $f : G \to H$ be an isomorphism of groups and let $a \in G$. Then the order of $a$ in $G$ equals the order of $f(a)$ in $H$.

35. Prove: For every positive integer $n$, the $n$th derivative of $f(x) = \ln(x)$ is $f^{(n)}(x) = \frac{(-1)^{n+1} (n-1)!}{x^n}$.

36. Let $F_n$ be the Fibonacci sequence, defined by $F_n = F_{n-1} + F_{n-2}$, with $F_1 = F_2 = 1$.

Prove: For every positive integer $n$, $\sum_{j=1}^{n} F_j^2 = F_n F_{n+1}$.

37. Let $m$ and $n$ be positive integers, and for $1 \leq i \leq m$, let $a_i$ and $b_i$ be integers such that $a_i \equiv b_i \pmod{n}$. Then $\sum_{i=1}^{m} a_i \equiv \sum_{i=1}^{m} b_i \pmod{n}$. (Hint: We have already shown it for $m = 2$; you may use that without proving it again.)

38. Prove: For every positive integer $n$, $F_{n-1} F_{n+1} - F_n^2 = (-1)^n$

39. Complete the following to make a true theorem and prove it.

Theorem. Let $F$ be a field with binary operations $*$ and $+$, identity elements 0 and 1, and inverse operations $-a$ and $a^{-1}$. A subset $G \subseteq F$ is a field if and only if \ldots

(Your answer should not just repeat the definition of field, but should refer to $F$.)