Homework #5 Rubrics

Proofs and writing

Exercise Set 2.4, Exercises 43, 44, 45

Exercise Set 2.5, Exercises 57 (using Fermat's Little Theorem), 60.

Exercise Set 2.6, Exercises 67 (must parallel the proof of Theorem 2.17), 71 using Theorem 2.17, 74

Exercise Set 3.2, Exercise 11, Exercise 12 (you may use any result in Section 3.2)

Homework Problem 1 (Exercise 43)**.** (a) Prove that is p is an odd prime number, then $2(p-3)! \equiv -1 \pmod{p}$.

(b) Find the least nonnegative residue of 2(100!) modulo 103

Rubric:

0 points Work does not contain enough of the relevant concepts to provide feedback.

1 points **Does not demonstrate understanding** Contains a reasonable attempt to prove each part, but does not meet the criteria for two points.

2 points **Needs revisions**

3 points **Demonstrates understanding**

4 points **Exemplary**

Solution: (a)

(b)

Homework Problem 2 (Exercise 44)**.** Let $n \in \mathbb{Z}$ with $n > 1$. Prove that n is a prime number if and only if $n-2)! \equiv 1 \pmod{n}$.

Rubric:

0 points Work does not contain enough of the relevant concepts to provide feedback.

1 points **Does not demonstrate understanding** Contains a reasonable attempt to prove each part, but does not meet the criteria for two points.

2 points **Needs revisions**

3 points **Demonstrates understanding**

4 points **Exemplary**

Proof ■

Homework Problem 3 (Exercise 45)**.** Let n be a composite integer greater than 4. Prove that $(n-1)! \equiv 0 \pmod{n}$.

Rubric:

0 points Work does not contain enough of the relevant concepts to provide feedback.

1 points **Does not demonstrate understanding** Contains a reasonable attempt to prove each part, but does not meet the criteria for two points.

2 points **Needs revisions**

3 points **Demonstrates understanding**

4 points **Exemplary**

Proof ■

Homework Problem 4 (Exercise 57, using Fermat's Little Theorem)**.** Let n be an integer. Prove each congruence below.

(a) $n^{21} \equiv n \pmod{30}$

(b) $n^{7} \equiv n \pmod{42}$

(c) $n^{13} \equiv n \pmod{2730}$.

Rubric:

0 points Work does not contain enough of the relevant concepts to provide feedback.

1 points **Does not demonstrate understanding** Contains a reasonable attempt to prove each part, but does not meet the criteria for two points.

2 points **Needs revisions**

3 points **Demonstrates understanding**

4 points **Exemplary**

Proof (a)

(b)

(c)

■

Homework Problem 5 (Exercise 60)**.** Let p and q be distinct prime numbers with $p-1 \mid q-1$. If $a \in \mathbb{Z}$ with $(a, pq) = 1$, prove that $a^{q-1} \equiv 1 \pmod{pq}$.

Rubric:

0 points Work does not contain enough of the relevant concepts to provide feedback.

1 points **Does not demonstrate understanding** Contains a reasonable attempt to prove each part, but does not meet the criteria for two points.

2 points **Needs revisions**

3 points **Demonstrates understanding**

4 points **Exemplary**

Proof ■

Homework Problem 6 (Exercise 67)**.** Prove that $9^8 \equiv 1 \pmod{16}$ following the steps in the proof of Euler's Theorem (Theorem 2.17)

Rubric:

0 points Work does not contain enough of the relevant concepts to provide feedback.

1 points **Does not demonstrate understanding** Contains a reasonable attempt to prove each part, but does not meet the criteria for two points.

2 points **Needs revisions**

3 points **Demonstrates understanding**

4 points **Exemplary**

Proof ■

Homework Problem 7 (Exercise 71, using Theorem 2.17 and the Chinese Remainder Theorem)**.** (a) Let n be an integer not divisible by 3. Prove that $n^7 \equiv n \pmod{63}$.

(b) Let n be an integer divisible by 9. Prove that $n^7 \equiv n \pmod{63}$.

Rubric:

0 points Work does not contain enough of the relevant concepts to provide feedback.

1 points **Does not demonstrate understanding** Contains a reasonable attempt to prove each part, but does not meet the criteria for two points.

2 points **Needs revisions**

3 points **Demonstrates understanding**

4 points **Exemplary**

Proof (a)

(b)

■

Homework Problem 8 (Exercise 74)**.** Let p be an odd prime number. Prove that

$$\left\{\frac{-(p-1)}{2}, \frac{-(p-3)}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-2}{2}, \frac{p-1}{2}\right\}$$

is a reduced residue system modulo p.

Rubric:

0 points Work does not contain enough of the relevant concepts to provide feedback.

1 points **Does not demonstrate understanding** Contains a reasonable attempt to prove each part, but does not meet the criteria for two points.

2 points **Needs revisions**

3 points **Demonstrates understanding**

4 points **Exemplary**

Proof ■

Homework Problem 9 (Chapter 3, Exercise 11)**.** Complete the proof of Theorem 3.2 by proving that if m, n and i are positive integers with $(m, n) = (m, i) = 1$, then teh integers $i, m+i, 2m+i, \ldots, (n-1)m+i$ form a complete system of residues modulo n.

Rubric:

0 points Work does not contain enough of the relevant concepts to provide feedback.

1 points **Does not demonstrate understanding** Contains a reasonable attempt to prove each part, but does not meet the criteria for two points.

2 points **Needs revisions**

3 points **Demonstrates understanding**

4 points **Exemplary**

Proof ■

Homework Problem 10 (Chapter 3, Exercise 12)**.** Let $n \in \mathbb{Z}$ with $n > 1$. If $p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ is the prime factorization of n, prove that

$$\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_m^{a_m-1} \prod_{i=1}^{m} (p_i - 1).$$

Rubric:

0 points Work does not contain enough of the relevant concepts to provide feedback.

1 points **Does not demonstrate understanding** Contains a reasonable attempt to prove each part, but does not meet the criteria for two points.

2 points **Needs revisions**

3 points **Demonstrates understanding**

4 points **Exemplary**