Homework #7 Rubrics

Proofs and writing

Section 2.4, Exercise 47 (See notes from February 21)

Section 4.2, Exercises 17,18

Finish the proof of Theorem 4.8

Section 4.3, Exercises 35, 36 (See notes from March 27)

Section 6.2, Exercise 12 (To disprove "there are no integral solutions," you need to find an integer solution)

Homework Problem 1 (Chapter 2, Exercise 47)**.** Let p be an odd prime number.

(a) Prove that $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

(b) If $p \equiv 1 \pmod{4}$, prove that $\left(\frac{p-1}{2}\right)!$ is a solution to $x^2 \equiv -1 \pmod{p}$.

(c) If $p \equiv 3 \pmod{4}$, prove that $\left(\frac{p-1}{2}\right)!$ is a solution to $x^2 \equiv 1 \pmod{p}$.

Solution: (a) Let p be an odd prime number. Then $(p-1)! \equiv 1 \pmod{p}$ by Wilson's Theorem. Note that $p - \frac{p-1}{2} = \frac{p+1}{2}$. Thus,

$$\begin{aligned} -1 \equiv (p-1)! &\equiv 1(2)\cdots\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\cdots(p-2)(p-1) \pmod{p} \\ &\equiv 1(2)\cdot\left(\frac{p-1}{2}\right)\left(-\frac{p-1}{2}\right)\cdots(-2)(-1) \pmod{p} \\ &\equiv \left(\frac{p-1}{2}\right)!(-1)^{(p-1)/2}\left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

Multiplying both sides of this congruence by $(-1)^{(p-1)/2}$ yields $(-1)^{(p+1)/2} \equiv \left(\frac{p-1}{2}\right)!\left(\frac{p-1}{2}\right)! \pmod{p}$.

(b) Assume $p \equiv 1 \pmod{4}$. Then there exists $k \in \mathbb{Z}$ such that $4p = 4k+1$. Thus, $\frac{p+1}{2} = 2k+1$ and $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{(p+1)/2} \equiv -1 \pmod{p}$.

(c) Assume $p \equiv 3 \pmod{4}$. Then there exists $k \in \mathbb{Z}$ such that $4p = 4k+3$. Thus, $\frac{p+1}{2} = 2k+2$ and $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{(p+1)/2} \equiv 1 \pmod{p}$.

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** Work shows partial understanding of the relationship between factorials and squares modulo p, but it has significant gaps or errors. Writing may be difficult to follow. It needs further review and significant revisions.

3 points **Demonstrates understanding** Mathematically correct proof for all parts with minor arithmetic, spelling, or grammatical errors. Or uses informal mathematical writing.

4 points **Exemplary** Mathematically correct and complete proof, likely using Wilson's Theorem and following the proof of Lemma 2.10 for Part (a). Or using Euler's Criterion. Part (b) and Part (c) likely use Part (a). Work is easy to follow with formal mathematical writing.

Homework Problem 2 (Chapter 4, Exercise 17)**.** Prove or disprove the following statements.

(a) Let p be an odd prime number and let a and b be quadratic nonresidues modulo p. Then the congruence $x^2 \equiv ab \pmod{p}$ is solvable.

(b) Let p and q be distinct odd prime numbers and let b be quadratic nonresidue of each p and q. Then the congruence $x^2 \equiv b \pmod{pq}$ is solvable.

Solution: (a) Let p be an odd prime number and let a and b be quadratic nonresidues modulo p. Then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$ and $\left(\frac{ab}{p}\right) = (-1)(-1) = 1$. Then the congruence $x^2 \equiv ab \pmod{p}$ is solvable.

(b) This is false; let $b = 2, p = 3$, and $q = 5$. By inspection, $x^2 \equiv a \pmod{15}$ is solvable if and only if $a \equiv 0, 1, 4, 6, 9, 10 \pmod{15}$. (0 and 10 are not quadratic residues since they are not relatively prime to 15)

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

Homework Problem 3 (Chapter 4, Exercise 18)**.** Let p be an odd prime number and let $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Prove that among the congruences $x^2 \equiv a \pmod{p}, x^2 \equiv b \pmod{p}$, and $x^2 \equiv ab \pmod{p}$, either all three are solvable or exactly one is solvable.

Solution: Let p be an odd prime number and let $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. If a and b are both quadratic residues modulo p, then so is ab, and thus all three congruences are solvable. If a and b are both quadratic nonresidues modulo p, then $x^2 \equiv ab \pmod{p}$ is solvable by Exercise 17a.

If exactly one of a and b is a quadratic residue modulo p, then either $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{b}{p}\right) = -1$ or $\left(\frac{a}{p}\right) = -1$ and $\left(\frac{b}{p}\right) = 1$. In either case $\left(\frac{ab}{p}\right) = -1$, so $x^2 \equiv ab \pmod{p}$ is not solvable. Thus, exactly one of $x^2 \equiv a \pmod{p}, x^2 \equiv b \pmod{p}$, and $x^2 \equiv ab \pmod{p}$ is solvable.

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

Homework Problem 4. Finish the proof of: Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & if\ p \equiv 1, 7 \pmod{8} \\ -1 & if\ p \equiv 3, 5 \pmod{8}. \end{cases}$$

for $p \equiv 3, 5, 7 \pmod{8}$.

Solution: From the proof in Strayer, $\left(\frac{2}{p}\right) = (-1)^{(p-1)/2 - \lfloor p/4 \rfloor}$ and it suffices to show that

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p-1}{2} \pmod{2}.$$

Following the proof of the $p \equiv 1 \pmod{8}$ case:

$p \equiv 3 \pmod 8$**:** Then there exists $k \in \mathbb{Z}$ such that $p = 8k + 3$. Then

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{8k+3-1}{2} - \left\lfloor \frac{8k+3}{4} \right\rfloor = 4k + 1 - 2k \equiv 1 \pmod 2$$

and

$$\frac{p^2-1}{8} = \frac{(8k+3)^2-1}{8} = \frac{64k^2+48k+9-1}{8} = 8k^2 + 6k + 1 \equiv 1 \pmod 2.$$

$p \equiv 5 \pmod 8$**:** Then there exists $k \in \mathbb{Z}$ such that $p = 8k + 5$. Then

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{8k+5-1}{2} - \left\lfloor \frac{8k+5}{4} \right\rfloor = 4k + 2 - 2k - 1 \equiv 1 \pmod 2$$

and

$$\frac{p^2-1}{8} = \frac{(8k+5)^2-1}{8} = \frac{64k^2+80k+25-1}{8} = 8k^2 + 10k + 3 \equiv 1 \pmod 2.$$

$p \equiv 7 \pmod 8$**:** Then there exists $k \in \mathbb{Z}$ such that $p = 8k + 7$. Then

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{8k+7-1}{2} - \left\lfloor \frac{8k+7}{4} \right\rfloor = 4k + 3 - 2k - 1 \equiv 0 \pmod 2$$

and

$$\frac{p^2-1}{8} = \frac{(8k+7)^2-1}{8} = \frac{64k^2+112k+49-1}{8} = 8k^2 + 14k + 6 \equiv 0 \pmod 2.$$

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** Mathematically correct proof for one case with attempts to prove the other two cases. Proof contains excess information, gaps, or errors that makes it difficult to determine understanding. Writing may be difficult to follow.

3 points **Demonstrates understanding** Mathematically correct proof for two case and minor errors in the third. May contain minor minor arithmetic, spelling, or grammatical errors while still demonstrating understanding. Or uses informal mathematical writing.

4 points **Exemplary** Mathematically correct for each of the cases, likely following the proof of the $p \equiv 1 \pmod 8$ case from class. Proof is easy to follow using formal mathematical writing.

Homework Problem 5 (Chapter 4, Exercise 35)**.** Let p be an odd prime. Prove the following statements:

(a) $\left(\dfrac{-2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \pmod 8$

(b) $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$

(c) $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{6}$

Solution: (a) Let p be an odd prime. Then $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$ if and only if $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right)$.

If $p \equiv 1 \pmod{8}$, then $p \equiv 1 \pmod{4}$ and $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$. If $p \equiv 3 \pmod{8}$, then $p \equiv 3 \pmod{4}$ and $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$.

If $p \equiv 5 \pmod{8}$, then $p \equiv 1 \pmod{4}$ and $\left(\frac{-1}{p}\right) = 1$ but $\left(\frac{2}{p}\right) = -1$. If $p \equiv 7 \pmod{8}$, then $p \equiv 3 \pmod{4}$ and $\left(\frac{-1}{p}\right) = -1$ but $\left(\frac{2}{p}\right) = 1$. Thus $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \pmod{8}$.

(b) Let p be an odd prime. Since $3 \equiv 3 \pmod{4}$,[1] we need two cases for quadratic reciprocity.

If $p \equiv 1 \pmod{4}$, then $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ by quadratic reciprocity, and $\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$. Then $p \equiv 1 \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

If $p \equiv 3 \equiv -1 \pmod{4}$, then $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ by quadratic reciprocity, and $\left(\frac{p}{3}\right) = -1$ if and only if $p \equiv 2 \equiv -1 \pmod{3}$. Then $p \equiv -1 \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

Therefore, $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

(c) Let p be an odd prime. From Theorem 4.25(c), $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. Again, we have two cases.

If $p \equiv 1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = 1$ by Theorem 4.6 and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ by quadratic reciprocity. Thus, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$. Then $p \equiv 1 \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

If $p \equiv 3 \equiv -1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = -1$ by Theorem 4.6 and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ by quadratic reciprocity. Thus, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$. Then $p \equiv 7 \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

Therefore, $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1, 7 \pmod{12}$, which is equivalent to $p \equiv 1 \pmod{6}$.

[1] In this problem, this step is repetitive, but it is needed when $p \neq 3$.

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** Mathematically correct proof for one part but not the other two. Proof contains excess information, gaps, or errors that makes it difficult to determine understanding. Writing may be difficult to follow.

3 points **Demonstrates understanding** Mathematically correct proof for two parts and minor errors in the third. May contain minor minor arithmetic, spelling, or grammatical errors while still demonstrating understanding. Or uses informal mathematical writing.

4 points **Exemplary** Mathematically correct argument for both parts using facts about quadratic residues and systems of linear congruences. Probably uses outline from Class March 27, multiplicity of the Legendre symbol, and/or Quadratic Reciprocity. Proof is easy to follow using formal mathematical writing.

Homework Problem 6. Characterize all primes p where the following integers are quadratic residues modulo p. (For example: the statement of Problem (a) is all of the primes where -2 is a quadratic residue, and Problem (b) is all of the primes where 3 is a quadratic residue).

(a) 5

(b) -5

(c) 7

(d) -7

Solution: (a) Let p be an odd prime. Since $5 \equiv 1 \pmod 4$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 5$.

(b) Let p be an odd prime. Then $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = 1$ if and only if $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right)$. Since $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$ and $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 5$. If $p \equiv 1 \pmod 4$, $p \equiv 1 \pmod 5$ then $p \equiv 1 \pmod{20}$. If $p \equiv 1 \pmod 4$, $p \equiv -1 \pmod 5$ then $p \equiv 9 \pmod{20}$.

Since $\left(\frac{-1}{p}\right) = -1$ if and only if $p \equiv 3 \pmod 4$ and $\left(\frac{5}{p}\right) = -1$ if and only if $p \equiv \pm 2 \equiv \mp 3 \pmod 5$. If $p \equiv 3 \pmod 4$, $p \equiv 3 \pmod 5$ then $p \equiv 3 \pmod{20}$. If $p \equiv 3 \pmod 4$, $p \equiv -3 \pmod 5$ then $p \equiv 7 \pmod{20}$.

Thus $\left(\frac{-5}{p}\right) = 1$ if and only if $p \equiv 1, 3, 7, 9 \pmod{20}$.

(c) Let p be an odd prime. Since $7 \equiv 3 \pmod 4$, we need two cases for quadratic reciprocity.

If $p \equiv 1 \pmod 4$, then $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$ by quadratic reciprocity, and $\left(\frac{p}{7}\right) = 1$ if and only if $p \equiv 1, 2, 4 \pmod 7$. Then $p \equiv 1, 9, 25 \pmod{28}$, and these are the unique equivalence classes modulo 28 by the Chinese Remainder Theorem.

If $p \equiv 3 \pmod 4$, then $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$ by quadratic reciprocity, and $\left(\frac{p}{7}\right) = -1$ if and only if $p \equiv 3, 5, 6 \pmod 7$. Then $p \equiv 3, 19, 27 \pmod{28}$, and these are the unique equivalence classes modulo 28 by the Chinese Remainder Theorem.

Therefore, $\left(\frac{7}{p}\right) = 1$ if and only if $p \equiv 1, 3, 9, 19, 25, 27 \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$.

(d) Let p be an odd prime. From Theorem 4.25(c), $\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right)$. Thus, $\left(\frac{-7}{p}\right) = 1$ if and only if $\left(\frac{-1}{p}\right) = \left(\frac{7}{p}\right)$.

From part (c), $\left(\frac{7}{p}\right) = 1$ if and only if $p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$. If $p \equiv 1, 9, 25 \pmod{28}$, then $p \equiv 1 \pmod 4$ and $\left(\frac{-1}{p}\right) = 1$.

Again from part (c), $\left(\frac{7}{p}\right) = -1$ if and only if $p \equiv 5, 11, 13, 15, 17, 23 \pmod{28}$ (removing the cases where p is not relatively prime to 28). If $p \equiv 11, 15, 23 \pmod{28}$, then $p \equiv 3 \pmod 4$ and $\left(\frac{-1}{p}\right) = -1$.

Therefore, $\left(\frac{-7}{p}\right) = 1$ if and only if $p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}$.

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** Mathematically correct proof for two parts but not the others. Or lists a case where p is composite. Proof contains excess information, gaps, or errors that makes it difficult to determine understanding. Writing may be difficult to follow.

3 points **Demonstrates understanding** Minor minor arithmetic, spelling, or grammatical errors. This could include losing a negative sign, if the proofs otherwise demonstrate understanding, ie, incorrectly copying a previous step. Or uses informal mathematical writing.

4 points **Exemplary** Mathematically correct argument for all parts using facts about quadratic residues and systems of linear congruences. Probably uses part (a) to solve part (b) and part (c) to solve part (d), multiplicity of the Legendre symbol, and/or Quadratic Reciprocity. Proof is easy to follow using formal mathematical writing.

Homework Problem 7 (Chapter 6, Exercise 12)**.** Prove or disprove the following statements.

(a) The Diophantine equation $x^2 + y^2 + 1 = 4z$ has no integer solutions.

(b) The Diophantine equation $x^2 + y^2 + 3 = 4z$ has no integral solutions.

(c) The Diophantine equation $x^2 + 2y^2 + 1 = 8z$ has no integral solutions.

(d) The Diophantine equation $x^2 + 2y^2 + 3 = 8z$ has no integral solutions.

Solution: (a) Consider $x^2 + y^2 + 1 = 4z$ modulo 4. Then we are looking for solutions to $x^2 + y^2 + 1 \equiv 0 \pmod 4$. Since $x^2, y^2 \equiv 0, 1 \pmod 4$, $x^2 + y^2 + 1 \equiv 1, 2, 3 \pmod 4$, and thus no solutions exist.

Alternately, $x^2 + y^2 + 1 \equiv 0 \pmod 4$ has solutions if and only if $x^2 + y^2 \equiv -1 \pmod 4$ has solutions. Then no solutions exist.

(b) This is false. Let $x = 0, y = 1, z = 1$. Then $x^2 + y^2 + 3 = 4z$.

(c) Consider $x^2 + 2y^2 + 1 = 8z$ modulo 2. Then $x^2 + 1 \equiv 0 \pmod 2$. Thus, x is odd and $x^2 \equiv 1 \pmod 8$. Also $x^2+2y^2+1 \equiv 0 \pmod 8$, so $1+2y^2+1 \equiv 0 \pmod 8$. That is, $2y^2 \equiv -2 \pmod 8$. Since $y^2 \equiv 0, 1, 4 \pmod 8$, no solutions exist.

(d) Conside $x^2 + 2y^2 + 3 = 8z$ modulo 2. Then $x^2 + 1 \equiv 0 \pmod 2$. Thus, x is odd and $x^2 \equiv 1 \pmod 8$. Also $x^2+2y^2+3 \equiv 0 \pmod 8$, so $1+2y^2+3 \equiv 0 \pmod 8$. That is, $2y^2 \equiv 4 \pmod 8$. Since $y^2 \equiv 0, 1, 4 \pmod 8$, no solutions exist.

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** Mathematically correct proof or counterexample for at least one part. Work shows partial understanding of the material, but it has significant gaps or errors. Writing may be difficult to follow. It needs further review and significant revisions.

3 points **Demonstrates understanding** Mathematically correct proof or counterexample for at least two parts, with minor errors in the other parts, but still able to demonstrate understanding. May contain minor arithmetic, spelling, or grammatical errors. Or uses informal mathematical writing.

4 points **Exemplary** For all four parts, mathematically correct proofs that no integer solutions exist or examples of integer solutions. Proofs may use congruences, quadratic residues, divisibility, or other results. Work is easy to follow with formal mathematical writing.