In Class Assignments MAT-255 Number Theory–Spring 2024

Claire Merriman

Spring 2024

Contents

MAT-255– Number Theory Spring 2024 In Class Work January 17

Your Name: _____ Group Members: _____ _____

In-class Problem 1 *Prove*

Theorem 1 (Ernst, Theorem 2.2)**.** *If n is an even integer, then n^2 is even.*

Solution: *If n is an even integer, then by definition, there is some $k \in \mathbb{Z}$ such that $n = 2k$. Then*

$$n^2 = (2k)^2 = 2(2k^2).$$

Since $2(k^2)$ is an integer, we have written n^2 in the desired form. Thus, n^2 is even.

In-class Problem 2 *Prove*

Theorem 2. *Let $a, b, c, m, n \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$ then $c \mid ma + nb$.*

MAT-255– Number Theory Spring 2024 In Class Work January 19

Your Name: _____ Group Members: _____ _____

Use the proofs of the following propositions as a guide.

Proposition 1. *Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof *Since $a \mid b$ and $b \mid c$, there exist $d, e \in \mathbb{Z}$ such that $b = ae$ and $c = bf$. Combining these, we see*

$$c = bf = (ae)f = a(ef),$$

so $a \mid c$. ■

Proposition 2. *Let $a, b, c, m, n \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$ then $c \mid ma + nb$.*

Proof *Let $a, b, c, m, n \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$. Then by definition of divisibility, there exists $j, k \in \mathbb{Z}$ such that $cj = a$ and $ck = b$. Thus,*

$$ma + nb = m(cj) + n(ck) = c(mj + nk).$$

Therefore, $c \mid ma + nb$ by definition. ■

In-class Problem 3 *Prove or disprove the following statements.*

(a) *If a, b, c, and d are integers such that if $a \mid b$ and $c \mid d$, then $a + c \mid b + d$.*

(b) *If a, b, c, and d are integers such that if $a \mid b$ and $c \mid d$, then $ac \mid bd$.*

(c) *If a, b, and c are integers such that if $a \nmid b$ and $b \nmid c$, then $a \nmid c$.*

In-class Problem 4 *Construct a truth table for $A \to B, \neg(A \to B)$ and $A \wedge \neg B$*

Solution:

A	B	$A \Rightarrow B$	$\neg(A \Rightarrow B)$	$A \wedge \neg B$
T	T	T	F	F
T	F	F	T	T
F	T	T	F	F
F	F	T	F	F

In-class Problem 5 *Prove that our two definitions of even are equivalent using the following outline:*

Proposition 3. *Let $n \in \mathbb{Z}$. Then there is some $k \in \mathbb{Z}$ such that $n = 2k$ if and only if $2 \mid n$.*

Proof ($\Rightarrow$) *Let $n \in \mathbb{Z}$. Assume that there is some $k \in \mathbb{Z}$ such that $n = 2k$. Thus, $2 \mid n$*

Free Response: *by definition of divides.*

($\Leftarrow$) *Let $n \in \mathbb{Z}$. Assume that $2 \mid n$. Then, there is some $k \in \mathbb{Z}$ such that $n = 2k$*

Free Response: *by definition of divides.*

■

In-class Problem 6 *Prove that our two definitions of odd are equivalent using the following outline:*

Proposition 4. *Let $n \in \mathbb{Z}$. Then there is some $k \in \mathbb{Z}$ such that $n = 2k + 1$ if and only if $2 \nmid k$.*

Proof ($\Rightarrow$) *Let $n \in \mathbb{Z}$. Assume that there is some $k \in \mathbb{Z}$ such that $n = 2k + 1$. Then*

Free Response: *by the division algorithm, there exists unique* $q, r \in \mathbb{Z}$ *such that* $n = 2q + r$ *and* $0 \leq r < 2$.

Thus, $2 \nmid k$.

($\Leftarrow$) *Let* $n \in \mathbb{Z}$. *Assume that* $2 \nmid k$. *Then*

Free Response: *by the division algorithm, there exists unique* $q, r \in \mathbb{Z}$ *such that* $n = 2q + r$ *and* $0 < r < 2$. *Thus,* $r = 1.1$

Thus, there is some $k \in \mathbb{Z}$ *such that* $n = 2k + 1$. ■

MAT-255– Number Theory Spring 2024 In Class Work January 22

Your Name: _____ Group Members: _____ _____

In-class Problem 7 *Use the division algorithm on $a = 47, b = 6$ and $a = 281, b = 13$.*

Solution: *When $a = 47, b = 6$, we have $q = 7$, and $r = 5$ since*

$$47 = 6(7) + 5 \quad \textit{and} \quad 0 \leq 5 < 6.$$

When $a = 281, b = 13$, we have $q = 21$, and $r = 8$ since

$$47 = 13(21) + 8 \quad \textit{and} \quad 0 \leq 8 < 13.$$

In-class Problem 8 *Let a and b be nonzero integers. Prove that there exists a unique $q, r \in \mathbb{Z}$ such that*

$$a = bq + r, \quad 0 \leq r < |b|.$$

(a) *Use the division algorithm to prove this statement as a corollary. That is, use the* conclusion *of the division algorithm as part of the proof. Use the following outline:*

(i) *Let a and b be nonzero integers. Since $|b| > 0$, the division algorithm says that there exist unique $p, s \in \mathbb{Z}$ such that* $\boxed{a = p|b| + s}$ *and* $\boxed{0 \leq s < |b|}$.

(ii) *There are two cases:*

i. When $\boxed{b > 0}$, *the conditions are already met, and* $r = \boxed{s}$ *and* $q = \boxed{b}$.

ii. Otherwise, $\boxed{b < 0}$, $r = \boxed{s}$ *and* $q = \boxed{-b}$.

(iii) *Since both cases used that the p, s are unique, then q, r are also unique*

(b) *Use the* proof *of the division algorithm as a template to prove this statement. That is, repeat the steps, adjusting as necessary, but do not use the conclusion.*

(i) *In the proof of the division algorithm, we let* $q = \left\lfloor \frac{a}{b} \right\rfloor$. *Here we have two cases:*

i. When $\boxed{b > 0}$, $q = \boxed{\left\lfloor \frac{a}{b} \right\rfloor}$ *and* $r = \boxed{a - bq}$.

Hint: *The TEXcode for the floor function is* `\lfloor ... \rfloor`

as in the proof of the division algorithm.

ii. When $\boxed{b < 0}$, $q = \boxed{-\left\lfloor \frac{a}{b} \right\rfloor}$ *and* $r = \boxed{a - bq}$.

(ii) *Summarizing these statements, rewrite q, r in terms of a and b, as in the original proof of the division algorithm.*

(iii) *Now use your scratch work and follow the outline of the proof of the division algorithm to provide a new proof* without referencing the division algorithm.

MAT-255– Number Theory Spring 2024 In Class Work January 24

Your Name: _____ Group Members: _____ _____

In-class Problem 9 *Let n be a positive integer with $n \neq 1$. Prove that if n^2+1 is prime, then n^2+1 can be written in the form $4k+1$ with $k \in \mathbb{Z}$.*

Hint: *Try showing the statement is true for all odd integers greater than 1.*

Solution: *Assume that n is a positive integer, $n \neq 1$, and n^2+1 is prime. If n is odd, then n^2 is odd, which would imply $n^2+1=2$, the only even prime. However, $n \neq 1$ by assumption. Thus, n is even.*

By definition of even, there exists $j \in \mathbb{Z}$ such that $n=2k$ and $n^2=4j^2$. Thus, $n^2+1=4k+1$ when $k=j^2$.

In-class Problem 10 *Prove or disprove the following conjecture, which is similar to the Twin Prime Conjecture:*

Conjecture 1. *There are infinitely many prime number p for which $p+2$ and $p+4$ are also prime numbers.*

Hint: *Show that the only prime where $p+2$ and $p+4$ are also prime is $p=3$.*

In-class Problem 11 *Without looking up the proof, prove Proposition 1.10: Let $a, b \in \mathbb{Z}$ with $(a,b)=d$. Then $\left(\frac{a}{d}, \frac{b}{d}\right)=1$.*

MAT-255– Number Theory Spring 2024 In Class Work January 26

Your Name: _____ Group Members: _____ _____

Use the first principle of mathematical induction to prove each statement.

In-class Problem 12 *For all $n \in \mathbb{N}$, 3 divides $4^n - 1$.*

Proof *We proceed by induction. The base case is $n = 1$. Since* $\boxed{3 \mid 4^1 - 1}$*, we are done.*

The induction hypothesis is that if $k \geq 1$ and $n = k$, then $\boxed{3 \mid 4^k - 1}$*. We want to show that* $\boxed{3 \mid 4^{k+1} - 1}$*.*

Free Response: *Then by the definition of divides, there exists m such that $3m = 4^k - 1$. Rewriting this equation, we get $3m + 1 = 4^k$. Multiplying both sides by 4 gives $4(3m) + 4 = 4^{k+1}$, or $3(4m + 1) = 4^{k+1} - 1$. Therefore, $3 \mid 4^{k+1} - 1$.*

■

In-class Problem 13 *Let $p_1, p_2, \ldots, p_n$ be n distinct points arranged on a circle. Then the number of line segments joining all pairs of points is $\dfrac{n^2 - n}{2}$.*

Proof *We proceed by induction. The base case is $n = 1$. Since*

Free Response: *There are $6\dfrac{1^2 - 1}{2} = 0$ line segments connecting the only point*

we are done.

The induction hypothesis is that if $k \geq 1$ and $n = k$, then

Free Response: *there are $\dfrac{k^2 - k}{2}$ line segments joining all pairs of distinct points $p_1, p_2, \ldots, p_k$ arranged on a circle.*

We want to show that

Free Response: *there are $\dfrac{(k+1)^2 - (k+1)}{2}$ line segments joining all pairs of distinct points $p_1, p_2, \ldots, p_k, p_{k+1}$ arranged on a circle.*

Free Response: *Adding a $k+1^{st}$ point adds an additional k pairs of points. Then there are $\dfrac{k^2 - k}{2} + k = \dfrac{k^2 + k}{2} = \dfrac{(k+1)^2 - (k+1)}{2}$ line segments joining all pairs of distinct points $p_1, p_2, \ldots, p_k, p_{k+1}$ arranged on a circle.*

■

In-class Problem 14 *If n is a positive integer, then*

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

Proof *We proceed by induction. The base case is $n = 1$. Since* $\boxed{1^3 = \dfrac{1^2(1+1)^2}{4}}$*, we are done.*

The induction hypothesis is that if $k \geq 1$ and $n = k$, then

$$\boxed{1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}}$$

We want to show that

$$\boxed{1^3 + 2^3 + 3^3 + \cdots + n^3 + (n+1)^3 = \frac{(n+1)^2(n+2)^2}{4}}$$

Free Response:

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

■

In-class Problem 15 *If n is an integer with $n \geq 5$, then*

$$2^n > n^2.$$

Proof *We proceed by induction. The base case is $n = 5$. Since $\boxed{2^5 > 5^2}$, we are done.*

The induction hypothesis is that if $k \geq 5$ and $n = k$, then $\boxed{2^k > k^2}$. We want to show that $\boxed{2^{k+1} > (k+1)^2}$.

Free Response: *Multiplying both sides by k gives $k2^k > 2^{k+1} > k^2$.*

■

Recall the notation $\gcd(a, b) = (a, b)$.

In-class Problem 16 *Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ with $a_1 \neq 0$. Prove that*

$$(a_1, \ldots, a_n) = ((a_1, a_2, a_3, \ldots, a_{n-1}), a_n).$$

Hint: *Try solving the $k = 3$ case as part of your scratch work.*

Proof *We proceed by induction. The base case is $n = 2$, since the statement we are trying to prove requires at least two inputs. Since*

$$\boxed{(a_1, a_2) = ((a_1, a_2))}$$

we are done.

The induction hypothesis is that if $k \geq 2$ and $n = k$, then

$$\boxed{(a_1, a_2, \ldots, a_k) = ((a_1, a_2, a_{k-1}), a_k)}$$

We want to prove that

$$\boxed{(a_1, a_2, \ldots, a_{k+1}) = ((a_1, a_2, a_k), a_{k+1})}$$

Free Response: *Let $d_k = (a_1, a_2, a_3, \ldots, a_k)$, $e = ((a_1, a_2, a_3, \ldots, a_k), a_{k+1}) = (d_k, a_{k+1})$, and $f = (a_1, a_2, a_3, \ldots, a_k, a_{k+1})$. We will show that $e \mid f$ and $f \mid e$. Since both e and f are positive, this will prove that $e = f$.*

Note that $e \mid (a_1, a_2, a_3, \ldots, a_k)$ and $e \mid a_{k+1}$ by definition. Since $(a_1, \ldots, a_k) = ((a_1, a_2, a_3, \ldots, a_{k-1}), a_k) = (d_{k-1}, a_k)$ by the induction hypothesis, $e \mid d_{k-1}$ and $e \mid a_k$ by defintion of (d_{k-1}, a_k). Again, by the induction hypothesis,

$d_{k-1} = (a_1, a_2, a_3, \ldots, a_{k-1}) = ((a_1, a_2, a_3, \ldots, a_{k-2}), a_{k-1}) = (d_{k-2}, a_{k-1})$, *so* $e \mid a_{k-1}$ *and* $e \mid d_{k-2}$ *by defintion of* (d_{k-2}, a_{k-1}). *Repeat this process until we get* $(a_1, a_2, a_3) = ((a_1, a_2), a_3)$, *so* $e \mid a_3$ *and* $e \mid (a_1, a_2)$ *by definition of* $((a_1, a_2), a_3)$. *Thus* $e \mid a_1, a_2, \ldots, a_{k+1}$ *by repeated applications of the induction hypothesis and the definition of greatest common divisor. By Problem 4 on Homework 3,* $e \mid f$.

To show that $f \mid e$, *we note that* $f \mid a_1, a_2, \ldots, a_k, a_{k+1}$ *by definition. Then* $f \mid d_k$ *by Problem 4 on Homework 3. Since* $e = (d_k, a_k)$, *we have that* $f \mid e$ *by Problem 4 on Homework 3.*

■

In-class Problem 17 *Redo the following proofs using induction:*

In-class Problem 17.1 *Let* $n \in \mathbb{Z}$. *Prove that* $3 \mid n^3 - n$.

Proof *We proceed by induction. The base case is* $n = 1$. *Since* $\boxed{3 \mid 1^3 - 1 = 3}$, *we are done.*

The induction hypothesis is that if $k \geq 1$ *and* $n = k$, *then* $\boxed{3 \mid k^3 - k}$. *We want to show that* $\boxed{3 \mid (k+1)^3 - (k+1)}$.

Free Response: *Since* $3 \mid 3(k^2 + k)$ *by the definition of divides, and* $3 \mid k^3 - k$ *by the induction hypothesis,* $k^3 - k + 3(k^2 + k)$ *by linear combination. Note that*

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

Thus, $3 \mid (k+1)^3 - (k+1)$.

■

In-class Problem 17.2 *Let* $n \in \mathbb{Z}$. *Prove that* $5 \mid n^5 - n$.

Proof *We proceed by induction. The base case is* $n = 1$. *Since* $\boxed{5 \mid 1^5 - 1 = 0}$, *we are done.*

The induction hypothesis is that if $k \geq 1$ *and* $n = k$, *then* $\boxed{5 \mid k^5 - k}$. *We want to show that* $\boxed{5 \mid (k+1)^5 - (k+1)}$.

Free Response: *Since* $5 \mid 5(k^4 + 2k^3 + 2k^2 + k)$ *by the definition of divides, and* $5 \mid k^5 - k$ *by the induction hypothesis,* $k^5 - k + 5(k^4 + 2k^3 + 2k^2 + k)$ *by linear combination. Note that*

$$\begin{aligned} k^5 - k + 5(k^4 + 2k^3 + 2k^2 + k) &= k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1 \\ &= (k+1)^5 - (k+1). \end{aligned}$$

Thus, $5 \mid (k+1)^5 - (k+1)$.

■

MAT-255– Number Theory Spring 2024 In Class Work January 26

Your Name: _____ Group Members: _____ _____

In-class Problem 18 *Find the greatest common divisors of the pairs of integers below and write the greatest common divisor as a linear combination of the integers.*

(a) $(21, 28)$

Solution: *By inspection:* $28 - 21 = 7$.

Using the Euclidean Algorithm: $a = 28, b = 21$

$$\begin{array}{lll} 28 = 21(1) + 7 & q_1 = 1, r_1 = 7 & 7 = 21(1) + 28(-1) \\ 21 = 7(3) + 0 & q_2 = 3, r_2 = 0 & \end{array}$$

so $28 + (-1)21 = 7 = (28, 21)$

(b) $(32, 56)$

Solution: *Using the Euclidean Algorithm:* $a = 56, b = 32$

$$\begin{array}{llll} 56 = 32(1) + 24 & q_1 = 1, r_1 = 24 & & 24 = 56(1) + 32(-1) \\ 32 = 24(1) + 8 & q_2 = 1, r_2 = 8 & 8 = 32(1) + 24(-1) = 32(1) + (56(1) + 32(-1))(-1) = 32(2) + 56(-1) & \\ 32 = 8(4) + 0 & q_3 = 4, r_3 = 0. & & \end{array}$$

so $56(-1) + 32(2) = 8 = (56, 32)$

(c) $(0, 113)$

Solution: *Since* $0 = 113(0)$, $(0, 113) = 113 = 0(0) = 113(1)$.

(d) $(78, 708)$

Solution: *Using the Euclidean Algorithm:* $a = 708, b = 78$

$$\begin{array}{lll} 708 = 78(9) + 6 & q_1 = 9, r_1 = 6 & 6 = 708(1) + 78(-9) \\ 78 = 6(13) + 0 & q_2 = 13, r_2 = 0. & \end{array}$$

so $708(1) + 78(-6) = 6 = (78, 708)$

In-class Problem 19 *Let p be prime.*

(a) *If $(a, b) = p$, what are the possible values of (a^2, b)? Of (a^3, b)? Of (a^2, b^3)?*

Solution: *If $(a, b) = p$, then there exist $j, k \in \mathbb{Z}$ such that $a = pj, b = pk$, and $p \nmid j$ or $p \nmid k$ (otherwise $(a, b) = p^2$).*

$$a^2 = p^2 j^2, \quad a^3 = p^3 j^3, \quad b^3 = p^3 k^3$$

Then (a^2, b) is p if $p \nmid k$ or p^2 if $p \mid k$; and (a^3, b) is p if $p \nmid k$, p^2 if $p \mid k$ and $p^2 \nmid k$, or p^3 if $p^2 \mid k$.

If $p \mid j$, then $p \nmid k$ and $(a^2, b^3) = p^3$. If $p \nmid j$, then $(a^2, b^3) = p^2$.

(b) *If* $(a, b) = p$ *and* $(b, p^3) = p^2$*, find* (ab, p^4) *and* $(a + b, p^4)$*.*

Solution: *There exists* $j, k \in \mathbb{Z}$ *such that* $a = pj, b = p^2k$*, and* $p \nmid k, p \nmid k$*. Then* $ab = p^3jk$ *and* $a + b = pj + p^2k = p(j + pk)$*. Thus,* $(ab, p^4) = p^3$ *and* $(a + b, p^4) = p$*.*

MAT-255– Number Theory Spring 2024 In Class Work February 5

Your Name: _____ Group Members: _____ _____

In-class Problem 20 *Find integral solutions to the Diophantine equation*

$$8x_1 - 4x_2 + 6x_3 = 6.$$

(a) *Since* $(8, -4, 6) = 2$, *solutions exist*

(b) *The linear Diophantine equation* $8x_1 - 4x_2 = 4y$ *has infinitely many solutions for all* $y \in \mathbb{Z}$ *by*

Free Response: *Theorem 6.2.*

Substituting into the original Diophantine equation gives $4y + 6x_3 = 6$, *which has infinitely many solutions by*

Free Response: *Theorem 6.2,*

since $(4, 6) = 2 \mid 6$. *Find them.*

Solution: *By inspection,* $y = 0, x_3 = 1$ *is a particular solution. Then by Theorem 6.2, the solutions have the form*

$$\begin{aligned} y &= 0 + \frac{6n}{2}, \quad x_3 = 1 - \frac{4n}{2}, \quad \text{or} \\ y &= 0 + 3n, \quad x_3 = 1 - 2n, \qquad n \in \mathbb{Z}. \end{aligned}$$

(c) *For a particular value of* y, *the Diophantine equation* $8x_1 - 4x_2 = 0$ *has solutions, find them.*

(d) *By inspection,* $x_1 = 1, x_2 = 2$ *is a particular solution. Then by Theorem 6.2, the solutions have the form*

$$\begin{aligned} x_1 &= 1 + \boxed{\frac{-4m}{4}}, \quad x_2 = 2 - \boxed{\frac{8m}{4}}, \quad \text{or} \\ x_1 &= \boxed{1 - m}, \quad x_2 = \boxed{2 - 2m}, \qquad m \in \mathbb{Z}. \end{aligned}$$

The first row should not have reduced fractions. Then simplify your answer for the second row.

(e) *Then* $x_1 = \boxed{1 - m}, x_2 = \boxed{2 - 2m}, x_3 = \boxed{1}$ *for* $m \in \mathbb{Z}$.

MAT-255– Number Theory Spring 2024 In Class Work February 7

Your Name: _____ Group Members: _____ _____

In-class Problem 21 (a) *Do there exist integers x and y such that $x + y = 100$ and $(x, y) = 8$?*

Solution: *No. By linear combination, $(x, y) \mid x + y$. Since $8 \nmid 100$, there does not exist integers x and y such that $x + y = 100$ and $(x, y) = 8$*

(b) *Prove that there exist infinitely many pairs of integers x and y such that $x + y = 87$ and $(x, y) = 3$.*

Scratch Work. Note that $87 = \boxed{3(29)}$. To ensure that $(x, y) = 3$, not just $3 \mid x$ and $3 \mid y$, let $x = 3n$ where $\boxed{29} \nmid n$.

Proof *Let $x \in \mathbb{Z}$ with*

Free Response: *$x = 3n$ for some $n \in \mathbb{Z}$ where $29 \nmid n$.*

Let $y = \boxed{87 - 3n}$. Then $3 \mid y$ by $\boxed{\text{linear combination}}$. Then $(x, y) = 3$ since $\boxed{29 \nmid n}$. Thus, there are infinitely many $x, y \in \mathbb{Z}$

Free Response: *where $x + y = 87$ and $(x, y) = 3$.*

■

In-class Problem 22 *Let a and b be relatively prime integers. Prove that $(a + b, a - b)$ is either 1 or 2.*

Hint: *From the back of Strayer: Let $(a + b, a - b) = d$ and note that $d \mid (a + b) + (a - b)$ and $d \mid (a + b) - (a - b)$.*

Hint: *Use Homework 3, Problem 2 which states $(ca, cb) = |c|(a, b)$ for all $a, b \in \mathbb{Z}$, not both 0.*

Solution: *Let $(a + b, a - b) = d$ and note that $d \mid (a + b) + (a - b)$ and $d \mid (a + b) - (a - b)$ by linear combination. Since $d \mid 2a$ and $d \mid 2b$, $d \mid (2a, 2b) = 2(a, b)$. Since $(a, b) = 1$ by assumption, $d \mid 2$. Thus, $d = 1, 2$.*

MAT-255– Number Theory Spring 2024 In Class Work February 9

Your Name: _____ Group Members: _____ _____

In-class Problem 23 *Prove that*

$$[a] = \{b \in \mathbb{Z} : 3 \mid (a - b)\}$$

is an equivalence relation on $\mathbb{Z}$.

Solution: *Let* $a, b \in \mathbb{Z}$. *We must show that the relation is reflexive, symmetric, and transitive.*

To show the relation is reflexive, we must show $a \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$. *Since* $3 \mid a - a = 0$, $a \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$.

To show the relation is symmetric, we must show that if $x \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$, *then* $a \in \{b \in \mathbb{Z} : 3 \mid (x - b)\}$. *If* $x \in \{b \in \mathbb{Z} : 3 \mid (a-b)\}$, *then there exists* $k \in \mathbb{Z}$ *such that* $3k = a-x$. *Therefore,* $-3k = b-a$ *and* $a \in \{b \in \mathbb{Z} : 3 \mid (x-b)\}$.

To show the relation is transitive, we must show that if $x \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$ *and* $y \in \{b \in \mathbb{Z} : 3 \mid (x - b)\}$, *then* $x \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$. *If* $x \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$, *then there exists* $k \in \mathbb{Z}$ *such that* $3k = a - x$. *Similarly, if* $y \in \{b \in \mathbb{Z} : 3 \mid (x - b)\}$, *then there exists* $m \in \mathbb{Z}$ *such that* $3m = x - y$. *Therefore,* $3(m + k) = a - k$ *and* $y \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$.

Since the relation is reflexive, symmetric, and transitive, it is an equivalence relation.

MAT-255– Number Theory Spring 2024 In Class Work February 14

Your Name: _____ Group Members: _____ _____

In-class Problem 24 *Find the addition and multiplication tables modulo* $3, 4, 5, 6, 7, 8$ *and* 9.

Solution: **Modulo** 3

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

*	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Modulo 4

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

*	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Modulo 5

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[0]
[4]	[4]	[0]	[1]	[2]	[3]

*	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Modulo 6

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

*	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Modulo 7

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

*	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

Modulo 8

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[0]	[1]	[2]	[3]	[4]	[5]	[6]

∗	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Modulo 9

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]

∗	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[2]	[0]	[2]	[4]	[6]	[0]	[1]	[3]	[5]	[7]
[3]	[0]	[3]	[6]	[0]	[3]	[6]	[0]	[3]	[6]
[4]	[0]	[4]	[8]	[3]	[7]	[2]	[6]	[1]	[5]
[5]	[0]	[5]	[1]	[6]	[2]	[7]	[3]	[8]	[4]
[6]	[0]	[6]	[3]	[0]	[6]	[3]	[0]	[6]	[3]
[7]	[0]	[7]	[5]	[3]	[1]	[8]	[6]	[4]	[2]
[8]	[0]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

MAT-255– Number Theory Spring 2024 In Class Work February 21

Your Name: _____ Group Members:_____ _____

In-class Problem 25 *Let p be an odd prime. Use that* $\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \pmod{p}$ *to show*

(a) *If* $p \equiv 1 \pmod 4$, *then* $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}$

(b) *If* $p \equiv 3 \pmod 4$, *then* $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod{p}$

Solution: (a) *Let p be a prime with* $p \equiv 1 \pmod 4$. *Then* $p = 4k+1$ *for some* $k \in \mathbb{Z}$. *From part (a),*

$$\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \equiv (-1)^{(4k+1+1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}.$$

(b) *Let p be a prime with* $p \equiv 3 \pmod 4$. *Then* $p = 4k+3$ *for some* $k \in \mathbb{Z}$. *From part (a),*

$$\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \equiv (-1)^{(4k+3+1)/2} \equiv (-1)^{2k+2} \equiv 1 \pmod{p}.$$

MAT-255– Number Theory Spring 2024 In Class Work February 28

Your Name: _____ Group Members:_____ _____

In-class Problem 26 *Let p, q be distinct primes. Prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.*

Proof *Let p, q be distinct primes. Then* $\boxed{q^{p-1} \equiv 1} \pmod{p}$ *and* $\boxed{p^{q-1} \equiv 1} \pmod{q}$ *by Fermat's Little Theorem, and* $\boxed{p^{q-1}} \equiv 0 \pmod{p}$ *and* $\boxed{p^{q-1}} \equiv 0 \pmod{q}$ *by* $\boxed{definition}$.

Free Response: *Thus, $p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$ and $p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$ by modular addition. Thus, $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ and this is the unique congruence class modulo pq by the Chinese Remainder Theorem.*

■

In-class Problem 27 *Let us prove that $\phi(20) = \phi(4)\phi(5)$. First, note that $\phi(4) =$* $\boxed{2}$ *and $\phi(5) =$* $\boxed{4}$, *so we will prove $\phi(20) =$* $\boxed{8}$.

(a) *A number a is relatively prime to 20 if and only if a is relatively prime to* $\boxed{4}$ *and* $\boxed{5}$. *The first blank should be smaller than second blank for the automatic grading to work.*

Hint: *The number in each blank should be relevant to what we are trying to show.*

(b) *We can partition the positive integers less that or equal to 20 into*

$$1 \equiv \boxed{5} \equiv \boxed{9} \equiv \boxed{13} \equiv \boxed{17} \pmod{4}$$
$$2 \equiv \boxed{6} \equiv \boxed{10} \equiv \boxed{14} \equiv \boxed{18} \pmod{4}$$
$$3 \equiv \boxed{7} \equiv \boxed{11} \equiv \boxed{15} \equiv \boxed{19} \pmod{4}$$
$$4 \equiv \boxed{8} \equiv \boxed{12} \equiv \boxed{16} \equiv \boxed{20} \pmod{4}$$

For any b in the range $1, 2, 3, 4$, define s_b to be the number of integers a in the range $1, 2, \ldots, 20$ such that $a \equiv b \pmod{4}$ and $\gcd(a, 20) = 1$. Thus, $s_1 =$ $\boxed{4}$, *$s_2 =$* $\boxed{0}$, *$s_3 =$* $\boxed{4}$, *and $s_4 =$* $\boxed{0}$.

We can see that when $(b, 4) = 1$, $s_b = \phi($ $\boxed{4}$ *) and when $(b, 4) > 1$, $s_b =$* $\boxed{0}$.

(c) *$\phi(20) = s_1 + s_2 + s_3 + s_4$. Why?*

Free Response: *Every positive integers less that or equal to 20 is counted by exactly one s_b.*

(d) *We have seen that $\phi(20) = s_1 + s_2 + s_3 + s_4$, that when $(b, 4) = 1$, $s_b =$* $\boxed{\phi(5)}$, *This blank is asking for a function, not a number. and that when $(b, 4) > 1$, $s_b =$* $\boxed{0}$. *To finish the "proof" we show that there are $\phi($* $\boxed{4}$ *) integers b where $(b, 4) = 1$. Thus, we can say that $\phi(20) =$* $\boxed{\phi(4)\phi(5)}$.

In-class Problem 28 *Repeat the same proof for m and n where $(m, n) = 1$.*

Solution: *Let m and m be relatively prime positive integers. A number a is relatively prime to mn if and only if a is relatively prime to* $\boxed{m}$ *and* $\boxed{n}$.

We can partition the positive integers less that or equal to mn into

$$\begin{aligned}
1 &\equiv \boxed{m+1} \equiv \boxed{2m+1} \equiv \cdots \equiv \boxed{(n-1)m+1} \pmod{m} \\
2 &\equiv \boxed{m+2} \equiv \boxed{2m+2} \equiv \cdots \equiv \boxed{(n-1)m+2} \pmod{m} \\
&\vdots \\
m &\equiv \boxed{2m} \equiv \boxed{3m} \equiv \cdots \equiv \boxed{nm} \pmod{m}
\end{aligned}$$

For any b in the range $1, 2, 3, \ldots, m$, define s_b to be the number of integers a in the range $1, 2, \ldots, mn$ such that $a \equiv b \pmod{m}$ and $\gcd(a, mn) = 1$. Thus, when $(b, m) = 1$, $s_b = \phi(\boxed{m})$ and when $(b, m) > 1$, $s_b = \boxed{0}$.

Free Response: *Since every positive integers less that or equal to mn is counted by exactly one s_b, $\phi(mn) = s_1 + s_2 + \cdots + s_m$.*

We have seen that $\phi(mn) = s_1 + s_2 + \cdots + s_m$, that when $(b, m) = 1$, $s_b = \boxed{\phi(n)}$, This blank is asking for a function, not a value. and that when $(b, m) > 1$, $s_b = \boxed{0}$. Since there are $\phi(\boxed{m})$ integers b where $(b, m) = 1$. Thus, we can say that $\phi(mn) = \boxed{\phi(m)\phi(n)}$.

MAT-255– Number Theory Spring 2024 In Class Work February 28

Your Name: _____ Group Members: _____ _____

In-class Problem 29 *Repeat the proof from last class to prove*

Theorem (Theorem 3.2)**.** *Let m and n be positive integers where $(m,n)=1$. Then $\phi(mn)=\phi(m)\phi(n)$.*

Proof *Let m and m be relatively prime positive integers. A number a is relatively prime to mn if and only if a is relatively prime to $\boxed{m}$ and $\boxed{n}$.*

We can partition the positive integers less that or equal to mn into

$$\begin{aligned}
1 &\equiv \boxed{m+1} \equiv \boxed{2m+1} \equiv \cdots \equiv \boxed{(n-1)m+1} \pmod{m}\\
2 &\equiv \boxed{m+2} \equiv \boxed{2m+2} \equiv \cdots \equiv \boxed{(n-1)m+2} \pmod{m}\\
&\vdots\\
m &\equiv \boxed{2m} \equiv \boxed{3m} \equiv \cdots \equiv \boxed{nm} \pmod{m}
\end{aligned}$$

For any b in the range $1,2,3,\ldots,m$, define s_b to be the number of integers a in the range $1,2,\ldots,mn$ such that $a\equiv b \pmod{m}$ and $\gcd(a,mn)=1$. Thus, when $(b,m)=1$, $s_b=\phi(\boxed{m})$ and when $(b,m)>1$, $s_b=\boxed{0}$.

Free Response: *Since every positive integers less that or equal to mn is counted by exactly one s_b, $\phi(mn)=s_1+s_2+\cdots+s_m$.*

We have seen that $\phi(mn)=s_1+s_2+\cdots+s_m$, that when $(b,m)=1$, $s_b=\boxed{\phi(n)}$, This blank is asking for a function, not a value. and that when $(b,m)>1$, $s_b=\boxed{0}$. Since there are $\phi(\boxed{m})$ integers b where $(b,m)=1$. Thus, we can say that $\phi(mn)=\boxed{\phi(m)\phi(n)}$. ■

In-class Problem 30 *Complete the proof of Theorem 3.2 by proving*

Proposition 5. *If m,n, and i are positive integers with $(m,n)=(m,i)=1$, then the integers*

$$i, m+i, 2m+i, \ldots, (n-1)m+i$$

form a complete system of residues modulo n.

MAT-255– Number Theory Spring 2024 In Class Work March 13

Your Name: _____ Group Members: _____ _____

Proposition (Proposition 5.4)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If i is a positive integer, then*

$$\operatorname{ord}_m(a^i) = \frac{\operatorname{ord}_m a}{\gcd(\operatorname{ord}_m a, i)}.$$

In-class Problem 31 *Use only the results through Proposition 5.3/Reading Lemma 10.3.5 (ie, not Proposition 5.4) to prove the primitive root version:*

Proposition. *Let $r, m \in \mathbb{Z}$ with $m > 0$ and r a primitive root modulo m. If i is a positive integer, then*

$$\operatorname{ord}_m(r^i) = \frac{\phi(m)}{\gcd(\phi(m), i)}.$$

Solution: *Let r be a primitive root modulo m. Then by Proposition 5.3, $\{r, r^2, \ldots, r^{\phi(m)}\}$ is a complete residue system modulo m. By Proposition 5.1, $\operatorname{ord}_m(r^i) \mid \phi(m)$ and by Proposition 5.3, $r, r^2, \ldots, r^{\phi(m)}$ is a complete residue system modulo m*

In-class Problem 32 *Prove*

Proposition (Proposition 10.2.2)**.** *Let p be prime, and let m be a positive integer. Consider*

$$x^m \equiv 1 \pmod{p}.$$

(a) *If $m \mid p - 1$, then there are exactly m incongruent solutions modulo p.*

(b) *For any positive integer m, there are $\gcd(m, p - 1)$ incongruent solutions modulo p.*

Solution: *Let p be prime, and let m be a positive integer. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$.*

(a) *If $m \mid p - 1$, then there exists $k \in \mathbb{Z}$ such that $mk = p - 1$. If $a^m \equiv 1 \pmod{p}$*

In-class Problem 33 *Prove the following statement, which is the converse of Reading Proposition 10.3.2:*

Let p be prime, and let $a \in \mathbb{Z}$. If every $b \in \mathbb{Z}$ such that $p \nmid b$ is congruent to a power of a modulo p, then a is a primitive root modulo p.

Solution: *Let p be prime, and let $a \in \mathbb{Z}$ such that every integer $b \in \mathbb{Z}$ where $p \nmid b$ is congruent to a^i modulo p for some positive integer i. Thus, $(a, p) = 1$, otherwise 1 would not be congruent to a power of a. ByProposition 5.2, $a^i \equiv a^j \pmod{p}$ if and only if $i \equiv j \pmod{p - 1}$. Thus, $a^1, a^2, \ldots, a^{p-1}$ are distinct congruence classes and only one of $a^1, a^2, \ldots, a^{p-1}$ is congruent to 1 modulo p. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, so $\operatorname{ord}_p a = p - 1$.*

In-class Problem 34 *Prove the following generalization of Reading Lemma 10.3.5*

Lemma. *Let $n \in \mathbb{Z}$ and let $x_1, x_2, \ldots, x_m$ be reduced residues modulo n. Suppose that for all $i \neq j$, $\operatorname{ord}_n(x_i)$ and $\operatorname{ord}_n(x_j)$ are relatively prime. Then*

$$\operatorname{ord}_n(x_1 x_2 \cdots x_m) = (\operatorname{ord}_n x_1)(\operatorname{ord}_n x_2) \cdots (\operatorname{ord}_n x_m).$$

MAT-255– Number Theory Spring 2024 In Class Work March 18

Your Name: _____ Group Members: _____ _____

Previous Results

Lemma 1. *Let $a, b \in \mathbb{Z}$, not both zero. Then any common divisor of a and b divides the greatest common divisor.*

Lemma 2. *Let $a, b \in \mathbb{Z}$, not both zero. Then any divisor of (a, b) is a common divisor of a and b.*

Proposition (Proposition 5.1)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then $a^n \equiv 1 \pmod{m}$ for some positive integer n if and only if $\operatorname{ord}_m a \mid n$. In particular, $\operatorname{ord}_m a \mid \phi(m)$.*

Problems

In-class Problem 35 *Let p be prime, m a positive integer, and $d = (m, p-1)$. Prove that $a^m \equiv 1 \pmod{p}$ if and only if $a^d \equiv 1 \pmod{p}$.*

Proof *Let p be prime, m a positive integer, and $d = (m, p-1)$. Let $a \in \mathbb{Z}$. If $p \mid a$, then $a^i \equiv \boxed{0 \pmod{p}}$ for all positive integers. Otherwise, $a^{p-1} \equiv 1 \pmod{p}$ by $\boxed{\textit{Fermat's Little Theorem}}$.*

By Proposition 5.1, $a^m \equiv 1 \pmod{p}$ if and only if $\boxed{\operatorname{ord}_p a \mid m}$. Similarly, $\boxed{a^{p-1} \equiv 1 \pmod{p}}$ if and only if $\boxed{\operatorname{ord}_p a \mid p-1}$. Thus, $\boxed{\operatorname{ord}_p a}$ is a common divisor of $\boxed{m}$ and $\boxed{p-1}$. Combining Lemmas 1 and 2 gives $\operatorname{ord}_p a$ is a common divisor of $\boxed{m}$ and $\boxed{p-1}$ if and only if $\operatorname{ord}_p a \mid d$. One final application of Proposition 5.1 gives $\boxed{\operatorname{ord}_p a \mid d}$ if and only if $\boxed{a^d \equiv 1 \pmod{p}}$. ■

In-class Problem 36 *Let p be prime and m a positive integer. Prove that*

$$x^m \equiv 1 \pmod{p}$$

has exactly $(m, p-1)$ incongruent solutions modulo p.

Proof *Let p be prime, m a positive integer, and $d = (m, p-1)$. From Problem 1,*

Free Response: *$x^m \equiv 1 \pmod{p}$ if and only if $x^d \equiv 1 \pmod{p}$.*

Now find a result that allows you to finish the proof in 1-2 sentences.

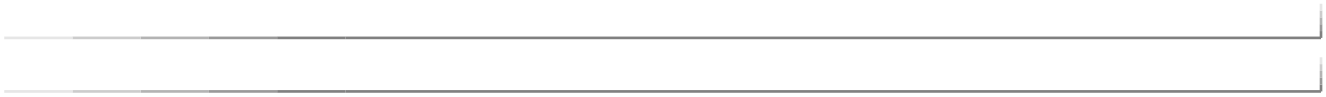
Free Response: *By Proposition 5.8 there are exactly d solutions to $x^d \equiv 1 \pmod{p}$. Thus, there are exactly d solutions to $x^m \equiv 1 \pmod{p}$.*

■

In-class Problem 37 *Prove the following statement, which is the converse of Proposition 5.4 (for a prime):*

Let p be prime, and let $a \in \mathbb{Z}$. If every $b \in \mathbb{Z}$ such that $p \nmid b$ is congruent to a power of a modulo p, then a is a primitive root modulo p.

Solution: *Let p be prime, and let $a \in \mathbb{Z}$ such that every integer $b \in \mathbb{Z}$ where $p \nmid b$ is congruent to a^i modulo p for some positive integer i. Thus, $(a, p) = 1$, otherwise 1 would not be congruent to a power of a. By Proposition 5.2, $a^i \equiv a^j \pmod{p}$ if and only if $i \equiv j \pmod{p-1}$. Thus, $a^1, a^2, \ldots, a^{p-1}$ are distinct congruence classes and only one of $a^1, a^2, \ldots, a^{p-1}$ is congruent to 1 modulo p. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, so $\operatorname{ord}_p a = p-1$.*



MAT-255– Number Theory Spring 2024 In Class Work March 27

Your Name: _____ Group Members: _____ _____

From class March 20:

Modulus	Quadratic residues	Quadratic nonresidues
2	1	None
3	1	2
5	1, 4	2, 3
7	1, 2, 4	3, 5, 6

Proposition (Proposition 4.5)**.** *Let p be an odd prime number and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Then*

(a) $\left(\frac{a^2}{p}\right) = 1$

(b) If $a \equiv b \pmod{p}$ *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Theorem (Theorem 4.6)**.** *Let p be an odd prime number. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}.$$

Theorem (Quadratic reciprocity)**.** *Let p and q be distinct primes.*

(a) If $p \equiv 1 \pmod 4$ *or* $q \equiv 1 \pmod 4$, *then* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

(b) If $p \equiv q \equiv 3 \pmod 4$, *then* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

In-class Problem 38 *Let p be an odd prime number. Prove the following statements the following provided outlines, which will help solve the next problem, as well.*

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

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

Proof (a) Since $3 \equiv \boxed{3} \pmod 4$,[1] we need two cases for Quadratic reciprocity.

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

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

(ii) If $p \equiv 3 \equiv -1 \pmod 4$, then $\left(\frac{3}{p}\right) = \boxed{-\left(\frac{p}{3}\right)}$ by Quadratic reciprocity, and $\left(\frac{p}{3}\right) = -1$ if and only if $p \equiv \boxed{2 \equiv -1 \pmod 3}$. Then $p \equiv \boxed{-1} \pmod{12}$, 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 $p \equiv \pm 1 \pmod{12}$.

(b) From Theorem 4.25(c), $\left(\frac{-3}{p}\right) = \boxed{\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)}$. Again, we have two cases.

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

(ii) If $p \equiv 3 \equiv -1 \pmod 4$, then $\left(\frac{-1}{p}\right) = \boxed{-1}$ by Theorem 4.6 and $\left(\frac{3}{p}\right) = \boxed{-\left(\frac{p}{3}\right)}$ by Quadratic reciprocity. Thus, $\left(\frac{-3}{p}\right) = \boxed{\left(\frac{p}{3}\right)} = 1$ if and only if $p \equiv \boxed{1 \pmod 3}$. Then $p \equiv \boxed{7} \pmod{12}$, 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 $p \equiv \boxed{1, 7} \pmod{12}$, which is equivalent to $p \equiv 1 \pmod 6$.

■

In-class Problem 39 *Find congruences characterizing all prime numbers p for which the following integers are quadratic residues modulo p, as done in the previous exercise.*

Outline is provided for the first part.

(a) 5

(b) -5

(c) 7

(d) -7

Proof (a) *Since* $5 \equiv \boxed{1} \pmod 4$, $\boxed{\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)}$ *by Quadratic reciprocity. Then* $\left(\frac{5}{p}\right) = \boxed{\left(\frac{p}{5}\right)} = 1$ *if and only if* $\boxed{p \equiv 1, 4 \pmod 5}$.

■

MAT-255– Number Theory Spring 2024 In Class Work April 1

Your Name: _____ Group Members: _____ _____

Results

Theorem 3 (Euler's Criterion)**.** *Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

Theorem (Theorem 4.6)**.** *Let p be an odd prime number. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}.$$

Theorem (Quadratic reciprocity)**.** *Let p and q be distinct primes.*

(a) If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

(b) If $p \equiv q \equiv 3 \pmod 4$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Lemma 3 (Gauss's Lemma)**.** *Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least positive residues of the integers $a, 2a, 3a, \ldots, \frac{p-1}{a}$ modulo p that are greater than $\frac{p}{2}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Problems

We can combine these results to find the Legendre symbol many different ways.

In-class Problem 40 *Use the following methods to find $\left(\frac{-6}{11}\right)$:*

(a) *Euler's Criterion, from March 22:*

$\left(\frac{-6}{11}\right) \equiv (-6)^{(11-1)/2} \equiv (-6)^5 \pmod{11}$ *By Euler's Criterion. Then*

$$(-6)^5 \equiv ((6)^2)^2(-6) \equiv 3^2(-6) \equiv -54 \equiv 1 \pmod{11}$$

(b) *Factor into $\left(\frac{-6}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (\boxed{-1})\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$. From here, we will explore the various was to find $\left(\frac{2}{11}\right)$ and $\left(\frac{3}{11}\right)$.*

(i) *Find $\left(\frac{2}{11}\right)$ using the specified method:*

- *Using Euler's Criterion.*

Solution: *From Euler's Criterion,*

$$\left(\frac{2}{11}\right) \equiv 2^{(11-1)/2} \equiv 32 \equiv -1 \pmod{11}.$$

- *Using Gauss's Lemma.*

  Solution: *First, find the least nonnegative residues of* $2, 2(2), 3(2), 4(2), 5(2)$ *modulo* 11. *These are*

  $$2, 4, 6, 8, 10,$$

  and $n = \boxed{3}$ *are greater than* $\frac{11}{2}$. *Thus, by Gauss's Lemma,*

  $$\left(\frac{2}{11}\right) = (-1)^{\boxed{3}} = \boxed{3}.$$

(ii) *Find* $\left(\frac{3}{11}\right)$ *using the specified method:*

- *Using Euler's Criterion.*

  Solution: *From Euler's Criterion,*

  $$\left(\frac{3}{11}\right) \equiv 3^{(11-1)/2} \equiv (-2)^2(3) \equiv 1 \pmod{11}.$$

- *Using Quadratic reciprocity*

  Solution: *Since* $11 \equiv 3 \pmod 4$, $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1.$

- *Using Gauss's Lemma.*

  Solution: *First, find the least nonnegative residues of* $3, 2(3), 3(3), 4(3), 5(3)$ *modulo* 11. *These are*

  $$\boxed{3, 6, 9, 1, 4}$$

  and $n = \boxed{2}$ *are greater than* $\frac{11}{2}$. *Thus, by Gauss's Lemma,*

  $$\left(\frac{3}{11}\right) = (-1)^{\boxed{2}} = \boxed{1}.$$

Thus, $\left(\frac{-6}{11}\right) = \boxed{1}$

(c) *Use that* $-6 \equiv 5 \pmod{11}$, *so* $\left(\frac{-6}{11}\right) = \left(\frac{5}{11}\right)$. *Then find* $\left(\frac{5}{11}\right)$ *the specified method:*

(i) *Using Euler's Criterion.*

Solution: *From Euler's Criterion,*

$$\left(\frac{5}{11}\right) \equiv 5^{(11-1)/2} \equiv (3)^2(5) \equiv 1 \pmod{11}.$$

(ii) *Using Quadratic reciprocity*

Solution: *Since* $5 \equiv 1 \pmod 4$, $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$.

(iii) *Using Gauss's Lemma.*

Solution: *First, find the least nonnegative residues of* $5, 2(5), 3(5), 4(5), 5(5)$ *modulo* 11. *These are*

$$\boxed{5, 10, 4, 9, 2},$$

and $n = \boxed{2}$ *are greater than* $\frac{11}{2}$. *Thus, by Gauss's Lemma,*

$$\left(\frac{5}{11}\right) = (-1)^{\boxed{2}} = \boxed{1}.$$

In-class Problem 41 *Now we will examine the Legendre symbol of 2 using Gauss's Lemma. First, note that* $2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$ *are already least nonnegative residues modulo p. It will be slightly easier to count how many are* less than $\frac{p}{2}$, *then subtract from the total number,* $\frac{p-1}{2}$.

Let $k \in \mathbb{Z}$ *with* $1 \le k \le \frac{p-1}{2}$. *Then* $2k < \frac{p}{2}$ *if and only if* $k < \boxed{\left\lfloor \frac{p}{4} \right\rfloor}$. *Thus,* $\frac{p-1}{2} - \left\lfloor \boxed{\frac{p}{4}} \right\rfloor$ *of* $2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$ *are greater than* $\frac{p}{2}$.

Hint: *The two blanks should be the same, and also go in the blanks below*

Now complete this table

p	$\left\lfloor \boxed{\frac{p}{4}} \right\rfloor$	$\frac{p-1}{2} - \left\lfloor \boxed{\frac{p}{4}} \right\rfloor$	$2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$	$\left(\frac{2}{p}\right)$
3	$\boxed{0}$	$\boxed{1}$	*Less than* $\frac{3}{2}$: $\boxed{N/A}$ *Greater than* $\frac{3}{2}$: $\boxed{2}$	$(-1)^{\boxed{1}} = \boxed{-1}$
5	$\boxed{1}$	$\boxed{1}$	*Less than* $\frac{5}{2}$: $\boxed{2}$ *Greater than* $\frac{5}{2}$: $\boxed{4}$	$(-1)^{\boxed{1}} = \boxed{-1}$
7	$\boxed{1}$	$\boxed{2}$	*Less than* $\frac{7}{2}$: $\boxed{2}$ *Greater than* $\frac{7}{2}$: $\boxed{4, 6}$	$(-1)^{\boxed{2}} = \boxed{1}$
11	$\boxed{2}$	$\boxed{3}$	*Less than* $\frac{11}{2}$: $\boxed{2, 4}$ *Greater than* $\frac{11}{2}$: $\boxed{6, 8, 10}$	$(-1)^{\boxed{3}} = \boxed{-1}$
13	$\boxed{3}$	$\boxed{3}$	*Less than* $\frac{13}{2}$: $\boxed{2, 4, 6}$ *Greater than* $\frac{13}{2}$: $\boxed{8, 10, 12}$	$(-1)^{\boxed{3}} = \boxed{-1}$
17	$\boxed{4}$	$\boxed{4}$	*Less than* $\frac{17}{2}$: $\boxed{2, 4, 6, 8}$ *Greater than* $\frac{17}{2}$: $\boxed{10, 12, 14, 16}$	$(-1)^{\boxed{4}} = \boxed{1}$
19	$\boxed{4}$	$\boxed{5}$	*Less than* $\frac{19}{2}$: $\boxed{2, 4, 6, 8}$ *Greater than* $\frac{17}{2}$: $\boxed{10, 12, 14, 16, 18}$	$(-1)^{\boxed{5}} = \boxed{-1}$
p	$\boxed{5}$	$\boxed{6}$	*Less than* $\frac{17}{2}$: $\boxed{2, 4, 6, 8, 10}$ *Greater than* $\frac{17}{2}$: $\boxed{12, 14, 16, 18, 20, 22}$	$(-1)^{\boxed{6}} = \boxed{1}$

MAT-255– Number Theory Spring 2024 In Class Work April 3

Your Name: _____ Group Members: _____ _____

Lemma 4. *Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Consider*

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a, \frac{p+1}{2}a, \ldots, (p-1)a.$$

The least absolute residues of ak and $a(p-k)$ differ by a negative sign. In other words,

$$ak \equiv -a(p-k) \pmod{p}.$$

Furthermore, for each $k = 1, 2, \ldots, \frac{p-1}{2}$, the exactly one of k and $-k$ is a least absolute residue of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$.

In-class Problem 42 *Check Lemma 1 for*

(a) $a = 3, p = 7$

(b) $a = 5, p = 11$

(c) $a = 6, p = 11$

Solution: (a) $a = 3, p = 7$

$$\begin{aligned} 3 \pmod 7,\ 3(2) \equiv -1 \pmod 7,\ 3(3) \equiv 2 \pmod 7,\\ 3(4) \equiv -2 \pmod 7,\ 3(5) \equiv 1 \pmod 7,\ 3(6) \equiv -3 \pmod 7, \end{aligned}$$

(b) $a = 5, p = 11$

$$\begin{aligned} 5 \pmod{11},\ 5(2) \equiv -1 \pmod{11},\ 5(3) \equiv 4 \pmod{11},\\ 5(4) \equiv -2 \pmod{11},\ 5(5) \equiv 3 \pmod{11},\\ 5(6) \equiv -3 \pmod{11},\ 5(7) \equiv -2 \pmod{11},\ 5(8) \equiv -4 \pmod{11},\\ 5(9) \equiv 1 \pmod{11},\ 5(10) \equiv -5 \pmod{11}, \end{aligned}$$

(c) $a = 11, p = 23$

$$\begin{aligned} 11 \pmod{23},\ 11(2) \equiv -1 \pmod{23},\ 11(3) \equiv 10 \pmod{23},\\ 11(4) \equiv -2 \pmod{23},\ 11(5) \equiv 9 \pmod{23},\ 11(6) \equiv -3 \pmod{23},\\ 11(7) \equiv 8 \pmod{23},\ 11(8) \equiv -4 \pmod{23},\ 11(9) \equiv 7 \pmod{23},\\ 11(10) \equiv -5 \pmod{23},\ 11(11) \equiv 6 \pmod{23},\\ 11(12) \equiv -6 \pmod{23},\ 11(13) \equiv 5 \pmod{23},\\ 11(14) \equiv -7 \pmod{23},\ 11(15) \equiv 4 \pmod{23},\ 11(16) \equiv -8 \pmod{23},\\ 11(17) \equiv 3 \pmod{23},\ 11(18) \equiv -9 \pmod{23},\ 11(19) \equiv 2 \pmod{23},\\ 11(20) \equiv -10 \pmod{23},\ 11(21) \equiv 1 \pmod{23},\ 11(22) \equiv -11 \pmod{23}, \end{aligned}$$

Access GeoGebra at https://www.geogebra.org/m/tuf7y6sh.

Two stills from the GeoGebra interactive are in Figure 1 and Figure 2.

Geogebra link: `https://tube.geogebra.org/m/tuf7y6sh`

In-class Problem 43 *The steps below outline the proof in the general case, when $p = 7$ and $q = 5$. This case is in Figure 1. Move the sliders to $p = 7$ and $q = 5$.*

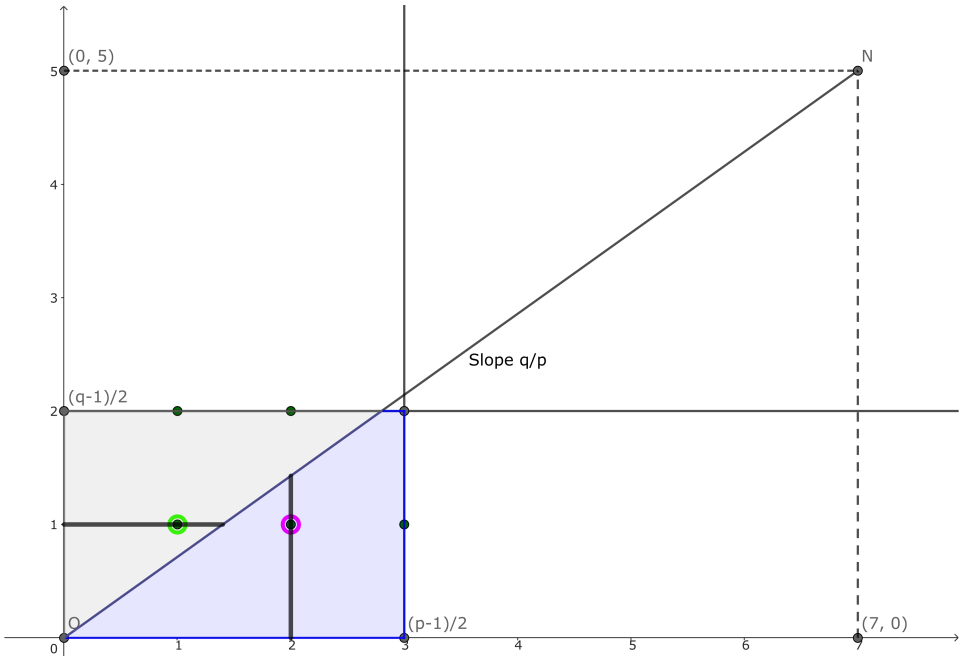


Figure 1: The lattice for the $p = 7, q = 5$ problem, with the $j = 1$ and $k = 2$ cases highlighted

(a) *The line segment between the origin and $(7, 5)$ has slope $\boxed{\frac{5}{7}}$. Since $p = 7$ and $q = 5$ are distinct primes, there are no lattice points on line segment except the endpoints.*

(b) *First, we will count the number of points N_1 where $\frac{5-1}{2} \geq y > \frac{5}{7}x > 0$. This triangle is grey in the GeoGebra. We will count how many lattice points on each horizontal lines $j = 1, 2$. Let's just check the numbers we should get:*

- *When $j = 1$, there are $\boxed{1}$ lattice points.*
- *When $j = 2$, there are $\boxed{2}$ lattice points.*

For each j, we are counting positive integers $x < \boxed{\frac{7}{5}}j$. Which is,

Multiple Choice:

(i) $\left\lfloor \frac{7j}{5} \right\rfloor$ ✓ .

(ii) $\left\lfloor \frac{5j}{7} \right\rfloor$.

Thus, the total number of lattice points in this triangle, N_1, is

Multiple Choice:

(i) $N_1 = \sum_{j=1}^{2} \left\lfloor \frac{7j}{5} \right\rfloor$ ✓

(ii) $N_1 = \sum_{j=1}^{2} \left\lfloor \frac{5j}{7} \right\rfloor$

(iii) $N_1 = \sum_{j=1}^{3} \left\lfloor \frac{7j}{5} \right\rfloor$

(iv) $N_1 = \sum_{j=1}^{3} \left\lfloor \frac{5j}{7} \right\rfloor$

(c) *Next we will count the rest of the lattice points in the rectangle, the blue region in the GeoGebra. We willl call this number* N_2.

The region is bounded by $0 < x \leq \frac{7-1}{2}$, $0 < y < \frac{5}{7}x$, *and* $y \leq \frac{5-1}{2}$. *Now, the point A where* $y = \frac{5}{7}x$ *intersects* $y = \frac{5-1}{2}$ *is between two consecutive lattice points, with coordinates* $x = \boxed{2}, y = \boxed{2}$ *and* $x = \boxed{3}, y = \boxed{2}$. *Similarly, the point B where* $y = \frac{5}{7}x$ *intersects* $x = \frac{7-1}{2}$ *is between two consecutive lattice points, with coordinates* $x = \boxed{3}, y = \boxed{2}$ *and* $x = \boxed{3}, y = \boxed{3}$. *Thus, the only lattice point in the triangle* A, B *and* $\left(\frac{7-1}{2}, \frac{5-1}{2}\right)$ *is* $\left(\frac{7-1}{2}, \frac{5-1}{2}\right)$. *Therefore, there are also* N_2 *lattice points in the triangle with vertices* $(0,0), \left(\frac{7-1}{2}, 0\right), \left(\frac{7-1}{2}, \frac{5-1}{2}\right)$.

(d) *We use the same method as* N_1 *to find* N_2. *We will count how many lattice points on each vertical lines* $k = 1, 2, 3$. *Let's just check the numbers we should get:*

- *When* $k = 1$, *there are* $\boxed{0}$ *lattice points.*
- *When* $k = 2$, *there are* $\boxed{1}$ *lattice points.*
- *When* $k = 3$, *there are* $\boxed{2}$ *lattice points.*

For each k, we are counting positive integers $y < \boxed{\frac{5}{7}}k$. *Which is,*

Multiple Choice:

(i) $\left\lfloor \frac{7j}{5} \right\rfloor$.

(ii) $\left\lfloor \frac{5j}{7} \right\rfloor$ ✓ .

Thus, the total number of lattice points in this triangle is

Multiple Choice:

(i) $N_2 = \sum_{k=1}^{2} \left\lfloor \frac{7k}{5} \right\rfloor$

(ii) $N_2 = \sum_{k=1}^{2} \left\lfloor \frac{5k}{7} \right\rfloor$

(iii) $N_2 = \sum_{k=1}^{3} \left\lfloor \frac{7k}{5} \right\rfloor$

(iv) $N_2 = \sum_{k=1}^{3} \left\lfloor \frac{5k}{7} \right\rfloor$ ✓

Thus, the total number of lattice points is $N_1 + N_2 = \boxed{(3)(2)}$.

In-class Problem 44 *The steps below outline the proof in the general case, when* $p = 23$ *and* $q = 13$. *Move the*

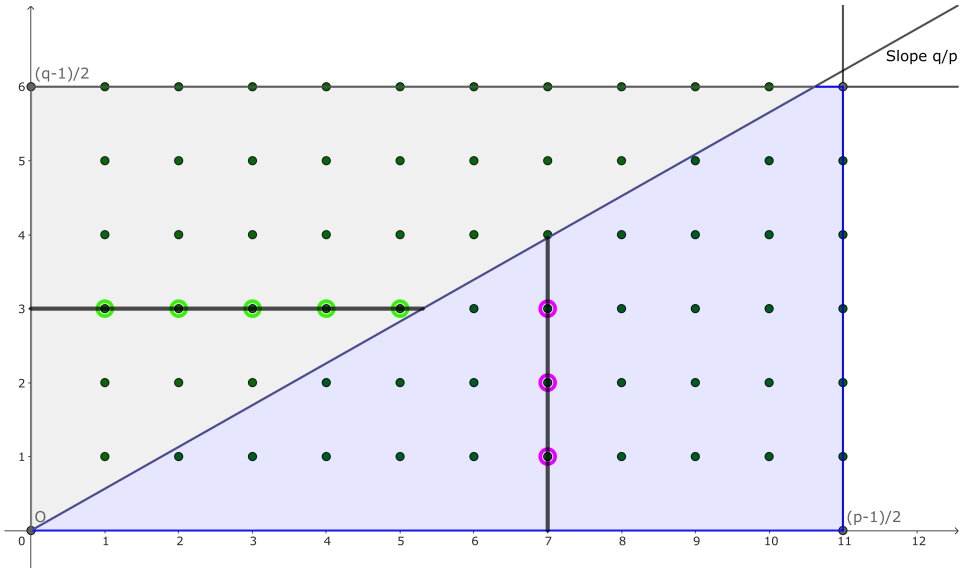


Figure 2: The lattice for the $p = 23, q = 13$, with the $j = 3$ and $k = 7$ cases highlighted

sliders to $p = 23$ *and* $q = 13$.

(a) *The line segment between the origin and* $(23, 13)$ *has slope* $\boxed{\frac{13}{23}}$. *Since* $p = 23$ *and* $q = 13$ *are distinct primes, there are no lattice points on line segment except the endpoints.*

(b) *First, we will count the number of points* N_1 *where* $\frac{13-1}{2} \geq y > \frac{13}{23}x > 0$. *This triangle is grey in the GeoGebra. We will count how many lattice points on each horizontal lines* $j = 1, 2, \ldots, \boxed{6}$. *Let's just check one case, we should get:*

- *When* $j = 3$, *as in Figure 2, there are* $\boxed{5}$ *lattice points.*

For each j, *we are counting positive integers* $x < \boxed{\frac{23}{13}} j$. *Which is,*

Multiple Choice:

(i) $\left\lfloor \frac{23j}{13} \right\rfloor$ ✓ .

(ii) $\left\lfloor \frac{13j}{23} \right\rfloor$.

Thus, the total number of lattice points in this triangle is

Multiple Choice:

(i) $N_1 = \sum_{j=1}^{6} \left\lfloor \frac{23j}{13} \right\rfloor$ ✓

(ii) $N_1 = \sum_{j=1}^{6} \left\lfloor \frac{13j}{23} \right\rfloor$

(iii) $N_1 = \sum_{j=1}^{11} \left\lfloor \frac{23j}{13} \right\rfloor$

(iv) $N_1 = \sum_{j=1}^{11} \left\lfloor \frac{13j}{23} \right\rfloor$

(c) *Next we will count the rest of the lattice points in the rectangle, the blue region in the GeoGebra. We willl call this number* N_2.

The region is bounded by $0 < x \leq \frac{23-1}{2}$, $0 < y < \frac{13}{23}x$, *and* $y \leq \frac{13-1}{2}$. *Now, the point A where* $y = \frac{13}{23}x$ *intersects* $y = \frac{13-1}{2}$ *is between two consecutive lattice points, with coordinates* $x = \boxed{10}, y = \boxed{6}$ *and* $x = \boxed{11}, y = \boxed{6}$. *Similarly, the point B where* $y = \frac{13}{23}x$ *intersects* $x = \frac{23-1}{2}$ *is between two consecutive lattice points, with coordinates* $x = \boxed{11}, y = \boxed{6}$ *and* $x = \boxed{11}, y = \boxed{7}$. *Thus, the only lattice point in the triangle* A, B *and* $\left(\frac{23-1}{2}, \frac{13-1}{2}\right)$ *is* $\left(\frac{23-1}{2}, \frac{13-1}{2}\right)$. *Therefore, there are also* N_2 *lattice points in the triangle with vertices* $(0,0), \left(\frac{23-1}{2}, 0\right), \left(\frac{23-1}{2}, \frac{13-1}{2}\right)$.

(d) *We use the same method as* N_1 *to find* N_2. *We will count how many lattice points on each vertical lines* $k = 1, 2, \ldots, \boxed{11}$. *Let's just check the numbers we should get:*

- *When* $k = 7$, *as in Figure 2, there are* $\boxed{3}$ *lattice points.*

For each k, *we are counting positive integers* $y < \boxed{\frac{13}{23}}k$. *Which is,*

Multiple Choice:

(i) $\left\lfloor \frac{23j}{13} \right\rfloor$.

(ii) $\left\lfloor \frac{13j}{23} \right\rfloor$ ✓ .

Thus, the total number of lattice points in this triangle is

Multiple Choice:

(i) $N_2 = \sum_{k=1}^{6} \left\lfloor \frac{23k}{13} \right\rfloor$

(ii) $N_2 = \sum_{k=1}^{6} \left\lfloor \frac{13k}{23} \right\rfloor$

(iii) $N_2 = \sum_{k=1}^{11} \left\lfloor \frac{23k}{13} \right\rfloor$

(iv) $N_2 = \sum_{k=1}^{11} \left\lfloor \frac{13k}{23} \right\rfloor$ ✓

Thus, the total number of lattice points is $N_1 + N_2 = \boxed{(11)(6)}$.

MAT-255– Number Theory Spring 2024 In Class Work April 17

Your Name: _____ Group Members: _____ _____

In-class Problem 45 *Prove that a positive integer can be written as the difference of two squares of integers if and only if it is not of the form $4n + 2$ for some $n \in \mathbb{Z}$.*

Proof ($\Rightarrow$) *We will show that if a positive integer can be written as the difference of two squares of integers, then it is not of the form $4n + 2$ for some $n \in \mathbb{Z}$.*

Free Response:

($\Leftarrow$) *We will show that any positive integer not of the form $4n + 2$ for some $n \in \mathbb{Z}$ can be written as the difference of two squares of integers.*

First, we will show that if a and b are positive integers that can be written as the difference of two squares of integers, then so can ab.

Free Response:

Now we will show that every odd prime can be written as the difference of two squares of integers. Let p be an odd prime. Then $p = x^2 - y^2 = (x - y)(x + y)$ when $x = \boxed{\frac{p+1}{2}}$ and $y = \boxed{\frac{p-1}{2}}$. Therefore every odd number can be written as the difference of two squares since

Free Response: *every odd number is a product of odd primes, and we proved that the product of integers that can be written as the difference of two squares can also be written as the difference of two squares.*

It remains to show that every positive integer of the form $4n$ for some $n \in \mathbb{Z}$ can be written as the difference of two squares of integers. Why is this the only remaining case?

Free Response: *Every even integer has the form $4n$ or $4n+2$.*

Similar to the odd prime case, $4n = x^2 - y^2 = (x-y)(x+y)$ when $x = \boxed{n+1}$ and $y = \boxed{n-1}$.

■

MAT-255– Number Theory Spring 2024 In Class Work April 19

Your Name: _____ Group Members: _____ _____

In-class Problem 46 *Let $x, y, z \in \mathbb{Z}$ and let p be a prime number.*

(a) *Prove that if $x^{p-1} + y^{p-1} = z^{p-1}$, then $p \mid xyz$.*

(b) *Prove that if $x^p + y^p = z^p$, then $p \mid (x + y - z)$.*

Hint: *Recall Fermat's Little Theorem and its corrollaries.*

Solution: *Let p be a prime number.*

(a) *Let $x, y, z \in \mathbb{Z}$ such that $x^{p-1} + y^{p-1} = z^{p-1}$.*

By Fermat's Little Theorem, if $p \nmid x$, then $x^{p-1} \equiv 1 \pmod{p}$. If $p \mid x$, then $x^{p-1} \equiv 0 \pmod{p}$. Similarly for y and z. Thus,

$$x^{p-1} + y^{p-1} \equiv \begin{cases} 0+0 \pmod{p} \\ 0+1 \pmod{p} \\ 1+1 \pmod{p} \end{cases}$$

has a solution if andd only if p divides at least one of x, y. Thus, $p \mid xyz$.

(b) *Let $x, y, z \in \mathbb{Z}$ such that $x^p + y^p = z^p$.*

By Corollary 5.8, $x^p \equiv x \pmod{p}, y^p \equiv y \pmod{p}$, and $z^p \equiv z \pmod{p}$. Thus,

$$\begin{aligned} x^p + y^p &\equiv z^p \pmod{p} \\ x + y &\equiv z \pmod{p}. \end{aligned}$$

In otherwords, $p \mid (x + y - z)$.