In Class Assignments MAT-255 Number Theory–Spring 2024

Claire Merriman

Spring 2024

Contents

January 17, 2024 3
January 19, 2024 5
January 22, 2024 7
January 24, 2024 8
January 26, 2024 10
January 26, 2024 14
February 5, 2024 15
February 7, 2024 16
February 9, 2024 17
February 14, 2024 18
February 21, 2024 19
February 28, 2024 20
February 28, 2024 21
March 13, 2024 22
March 18, 2024 24
March 27, 2024 26
April 1, 2024 28
April 3, 2024 31
April 5, 2024 32
April 17, 2024 35
April 19, 2024 37

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

Your Name: ____________ Group Members: ____________ ____________

In-class Problem 1 Prove

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

Wait for more lecture before proceeding to the back

In-class Problem 2 Prove

Theorem (Strayer, Proposition 1.2). *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 1 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 2 Construct a truth table for $A \to B, \neg(A \to B)$ and $A \wedge \neg B$

Pause for more lecture. If there is time, complete the following problem.

In-class Problem 3 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, $2 \mid n$* ______________________

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

In-class Problem 4 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 Thus, $2 \nmid k$.*

($\Leftarrow$) *Let $n \in \mathbb{Z}$. Assume that $2 \nmid k$. Then 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 1 Use the division algorithm on $a = 47, b = 6$ and $a = 281, b = 13$.

In-class Problem 2 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 ____________ and ____________.

  (ii) There are two cases:

    i. When ____________, the conditions are already met, and $r =$ ____________ and $q =$ ____________.

    ii. Otherwise, ____________, $r =$ ____________ and $q =$ ____________.

  (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 ____________, $q =$ ____________ and $r =$ ____________.

    as in the proof of the division algorithm.

    ii. When ____________, $q =$ ____________ and $r =$ ____________.

  (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 1 (Chapter 1, Exercise 29) 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 $k \in \mathbb{Z}$.

In-class Problem 2 (Chapter 1, Exercise 33) 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.*

Wait for more lecture before answering the problem on the back.

In-class Problem 3 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 1 (Ernst Theorem 4.5) For all $n \in \mathbb{N}$, 3 divides $4^n - 1$.

Proof We proceed by induction. The base case is $n = 1$. Since ________, we are done.

The induction hypothesis is that if $k \geq 1$ and $n = k$, then ________. We want to show that ________.

Complete the proof:

$\blacksquare$

In-class Problem 2 (Ernst Theorem 4.7) 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 ____________________ we are done.

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

We want to show that

Complete the proof:

$\blacksquare$

In-class Problem 3 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 ____________, we are done.
The induction hypothesis is that if $k \geq 1$ and $n = k$, then

We want to show that

Complete the proof:

$\blacksquare$

In-class Problem 4 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 ____________, we are done.
The induction hypothesis is that if $k \geq 5$ and $n = k$, then ____________. We want to show that ____________.
Complete the proof:

$\blacksquare$

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

In-class Problem 5 Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ with $a_1 \neq 0$. Prove that

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

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

we are done.

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

We want to prove that

Complete the proof:

$\blacksquare$

In-class Problem 6 Redo the following proofs using induction:

In-class Problem 7 Let $n \in \mathbb{Z}$. Prove that $3 \mid n^3 - n$.

Proof We proceed by induction. The base case is $n = 1$. Since ____________, we are done.
The induction hypothesis is that if $k \geq 1$ and $n = k$, then ____________. We want to show that ____________.

■

In-class Problem 8 Let $n \in \mathbb{Z}$. Prove that $5 \mid n^5 - n$.

Proof We proceed by induction. The base case is $n = 1$. Since ____________, we are done.
The induction hypothesis is that if $k \geq 1$ and $n = k$, then ____________. We want to show that ____________.

■

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

Your Name: ________________ Group Members: ________________ ________________

In-class Problem 1 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) $(21, 28)$

(b) $(32, 56)$

(c) $(0, 113)$

(d) $(78, 708)$

Pause for more lecture.

In-class Problem 2 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)?

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

MAT-255– NUMBER THEORY SPRING 2024 IN CLASS WORK FEBRUARY 5

Your Name: ____________ Group Members: ____________ ____________

In-class Problem 1 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 ____________ Substituting into the original Diophantine equation gives $4y + 6x_3 = 6$, which has infinitely many solutions by ____________ since $(4, 6) = 2 \mid 6$. Find them.

(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

$$x_1 = 1 + \underline{\hspace{3cm}}, \quad x_2 = 2 - \underline{\hspace{3cm}}, \quad \text{or}$$
$$x_1 = \underline{\hspace{3cm}}, \quad x_2 = \underline{\hspace{3cm}}, \quad m \in \mathbb{Z}.$$

(e) Then $x_1 =$ ____________, $x_2 =$ ____________, $x_3 =$ ____________ for $m \in \mathbb{Z}$.

MAT-255– NUMBER THEORY SPRING 2024 IN CLASS WORK FEBRUARY 7

Your Name: ____________ Group Members: ____________ ____________

In-class Problem 1 (a) Do there 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 $87 =$ ____________. To ensure that $(x, y) = 3$, not just $3 \mid x$ and $3 \mid y$, let $x = 3n$ where ______ $\nmid n$.

Proof Let $x \in \mathbb{Z}$ with ____.
Let $y =$ ____________. Then $3 \mid y$ by ______________. Then $(x, y) = 3$ since ____________. Thus, there are infinitely many $x, y \in \mathbb{Z}$

■

In-class Problem 2 (Strayer Chapter 1, Exercise 38) Let a and b be relatively prime integers. Prove that $(a + b, a - b)$ is either 1 or 2.

MAT-255– NUMBER THEORY SPRING 2024 IN CLASS WORK FEBRUARY 9

Your Name: ______________ Group Members: ______________ ______________

In-class Problem 1 Prove that

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

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

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

Your Name: ____________________ Group Members: ____________________ ____________________

In-class Problem 1 Find the addition and multiplication tables modulo $3, 4, 5, 6, 7, 8$ and 9.

MAT-255– NUMBER THEORY SPRING 2024 IN CLASS WORK FEBRUARY 21

Your Name: __________________ Group Members: __________________ __________________

In-class Problem 1 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 $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod{p}$

MAT-255– NUMBER THEORY SPRING 2024 IN CLASS WORK FEBRUARY 28

Your Name: ____________ Group Members: ____________ ____________

In-class Problem 1 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 ____________ $\pmod p$ and ____________ $\pmod q$ by Fermat's Little Theorem, and ____________ $\equiv 0 \pmod p$ and ____________ $\equiv 0 \pmod q$ by ____________.

∎

In-class Problem 2 Let us prove that $\phi(20) = \phi(4)\phi(5)$. First, note that $\phi(4) =$ ______ and $\phi(5) =$ ______, so we will prove $\phi(20) =$ ______.

(a) A number a is relatively prime to 20 if and only if a is relatively prime to ______ and ______.

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

$$\begin{aligned}
1 &\equiv ___ \equiv ___ \equiv ___ \equiv ___ \pmod 4\\
2 &\equiv ___ \equiv ___ \equiv ___ \equiv ___ \pmod 4\\
3 &\equiv ___ \equiv ___ \equiv ___ \equiv ___ \pmod 4\\
4 &\equiv ___ \equiv ___ \equiv ___ \equiv ___ \pmod 4
\end{aligned}$$

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, $s_1 =$ ______, $s_2 =$ ______, $s_3 =$ ______, and $s_4 =$ ______.

We can see that when $(b, 4) = 1$, $s_b = \phi($______$)$ and when $(b, 4) > 1$, $s_b =$ ______.

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

(d) We have seen that $\phi(20) = s_1 + s_2 + s_3 + s_4$, that when $(b, 4) = 1$, $s_b =$ ______, [1] and that when $(b, 4) > 1$, $s_b =$ ______. To finish the "proof" we show that there are $\phi($______$)$ integers b where $(b, 4) = 1$. Thus, we can say that $\phi(20) =$ ____________.

In-class Problem 3 Repeat the same proof for m and n where $(m, n) = 1$.

[1] This blank is asking for a function, not a numbers.

MAT-255– NUMBER THEORY SPRING 2024 IN CLASS WORK FEBRUARY 28

Your Name: ____________ Group Members: ____________ ____________

In-class Problem 1 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 ______ and ______.

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

$$\begin{aligned} 1 &\equiv \underline{\qquad} \equiv \underline{\qquad} \equiv \cdots \equiv \underline{\qquad} \pmod{m} \\ 2 &\equiv \underline{\qquad} \equiv \underline{\qquad} \equiv \cdots \equiv \underline{\qquad} \pmod{m} \\ &\vdots \\ m &\equiv \underline{\qquad} \equiv \underline{\qquad} \equiv \cdots \equiv \underline{\qquad} \pmod{m} \end{aligned}$$

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 $(b,m)=1$, $s_b=\phi($______$)$ and when $(b,m)>1$, $s_b=$ ______.

We have seen that $\phi(mn)=s_1+s_2+\cdots+s_m$, that when $(b,m)=1$, $s_b=$ ______, [3] and that when $(b,m)>1$, $s_b=$ ______. Since there are $\phi($______$)$ integers b where $(b,m)=1$. Thus, we can say that $\phi(mn)=$ __________. ■

In-class Problem 2 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.

[3] This blank is asking for a function, not a value.

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 1 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*

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

In-class Problem 2 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.*

In-class Problem 3 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.

In-class Problem 4 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 1 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 $a^i \equiv$ ____________ for all positive integers. Otherwise, $a^{p-1} \equiv 1 \pmod{p}$ by ____________.

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

Problem 2 on back page

In-class Problem 2 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,

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

■

If you have time, start working on this problem from the homework.

In-class Problem 3 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.

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 1 (Strayer Chapter 4, Exercise 35) 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 $3 \equiv$ __________ $\pmod{4}$,[4] we need two cases for Quadratic reciprocity.

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

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

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

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

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

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

■

In-class Problem 2 (Strayer Chapter 4, Exercise 36) 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 $5 \equiv$ __________ (mod 4), ________________ by Quadratic reciprocity. Then $\left(\frac{5}{p}\right) =$ _____ $=$ 1 if and only if ________________.

■

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

Your Name: ________________ Group Members: ________________ ________________

Results

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

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

- Using Euler's Criterion.

- Using Gauss's Lemma.

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

- Using Euler's Criterion.

- Using Quadratic reciprocity

- Using Gauss's Lemma.

Thus, $\left(\dfrac{-6}{11}\right) = $ ______

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

(i) Using Euler's Criterion.

(ii) Using Quadratic reciprocity

(iii) Using Gauss's Lemma.

In-class Problem 2 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 $1 \leq k \leq \frac{p-1}{2}$. Then $2k < \frac{p}{2}$ if and only if $k <$ ______. Thus, $\frac{p-1}{2} - \lfloor \_\_\_\_\_\_ \rfloor$ of $2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$ are greater than $\frac{p}{2}$.

Now complete this table

p	$\lfloor \_\_\_\_\_\_ \rfloor$	$\frac{p-1}{2} - \lfloor \_\_\_\_\_\_ \rfloor$	$2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$	$\left(\frac{2}{p}\right)$
3			Less than $\frac{3}{2}$: Greater than $\frac{3}{2}$:	
5			Less than $\frac{5}{2}$: Greater than $\frac{5}{2}$:	
7			Less than $\frac{7}{2}$: Greater than $\frac{7}{2}$:	
11			Less than $\frac{11}{2}$: Greater than $\frac{11}{2}$:	
13			Less than $\frac{13}{2}$: Greater than $\frac{13}{2}$:	
17			Less than $\frac{17}{2}$: Greater than $\frac{17}{2}$:	
19			Less than $\frac{19}{2}$: Greater than $\frac{17}{2}$:	
p			Less than $\frac{17}{2}$: Greater than $\frac{17}{2}$:	

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

Your Name: ____________ Group Members: ____________ ____________

Lemma 3. *Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Consider*

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

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

In-class Problem 1 Check Lemma 1 for

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

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

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

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

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

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

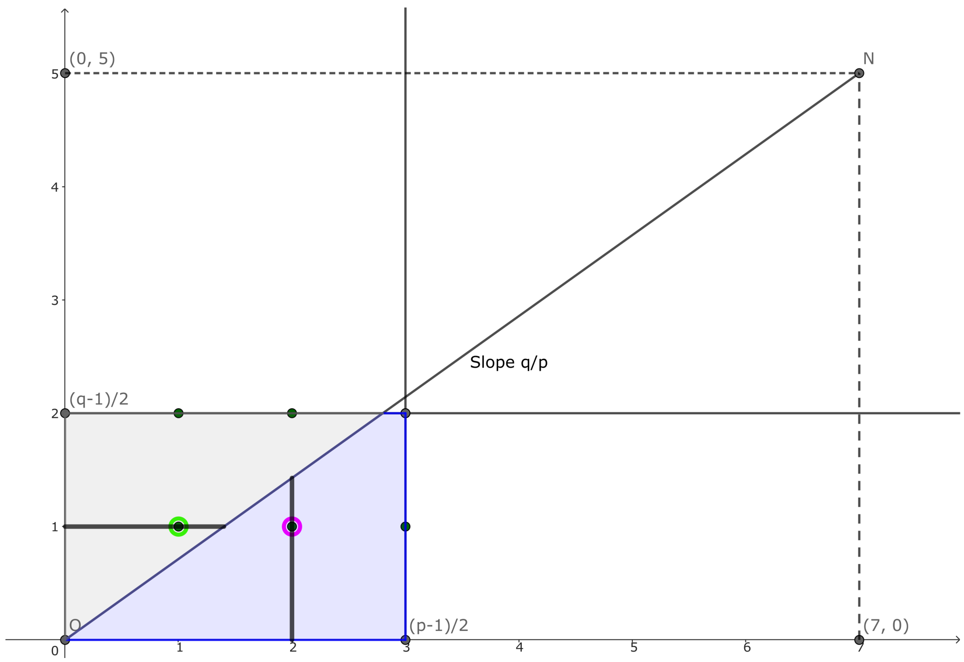

Figure 1: The lattice for the $p = 7, q = 5$ problem, with the $j = 1$ and $k = 2$ cases highlighted

(a) The line segment between the origin and $(7, 5)$ has slope ______. 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 ______ lattice points.
- When $j = 2$, there are ______ lattice points.

For each j, we are counting positive integers $x <$ ______j. Which is,

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

(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 Similarly, the point B where $y = \frac{5}{7}x$ intersects $x = \frac{7-1}{2}$ is between two consecutive lattice points, with coordinates 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 ______ lattice points.
- When $k = 2$, there are ______ lattice points.
- When $k = 3$, there are ______ lattice points.

For each k, we are counting positive integers $y <$ ______k. Which is,

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

Thus, the total number of lattice points is $N_1 + N_2 =$ ____________.

In-class Problem 2 The steps below outline the proof in the general case, when $p = 23$ and $q = 13$.

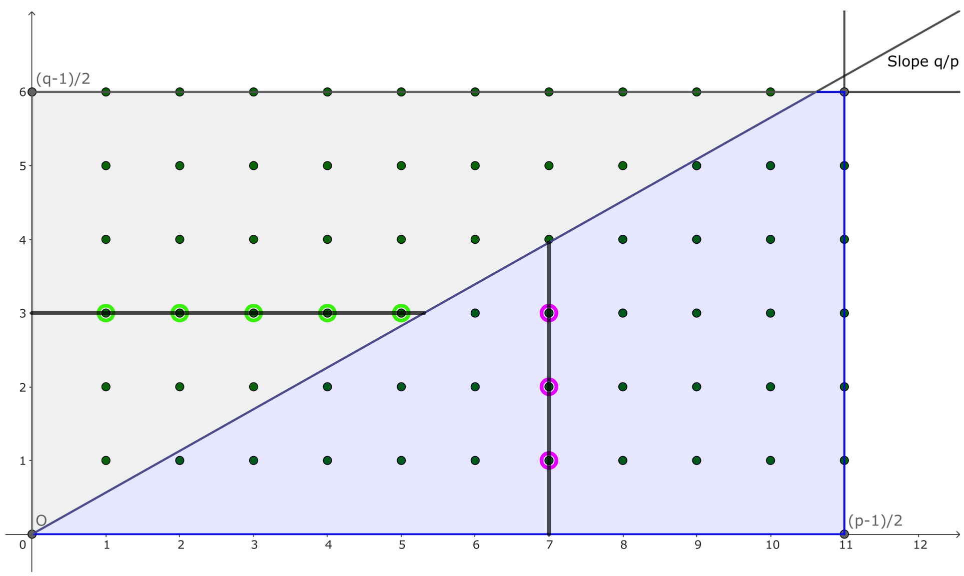

Figure 2: The lattice for the $p = 23, q = 13$, with the $j = 3$ and $k = 7$ cases highlighted

(a) The line segment between the origin and $(23, 13)$ has slope ______. 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 $j = 1, 2, \ldots,$ ______. Let's just check one case, we should get:

- When $j = 3$, as in Figure 2, there are ______ lattice points.

For each j, we are counting positive integers $x <$ ______j. Which is,

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

(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 Similarly, the point B where $y = \frac{13}{23}x$ intersects $x = \frac{23-1}{2}$ is between two consecutive lattice points, with coordinates 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 $k = 1, 2, \ldots,$ ______. Let's just check the numbers we should get:

- When $k = 7$, as in Figure 2, there are ______ lattice points.

For each k, we are counting positive integers $y <$ ______k. Which is,

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

Thus, the total number of lattice points is $N_1 + N_2 =$ ____________.

MAT-255– NUMBER THEORY SPRING 2024 IN CLASS WORK APRIL 17

Your Name: __________________ Group Members:__________________ __________________

In-class Problem 1 (Chapter 6, Exercise 34) 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 $n \in \mathbb{Z}$.

($\Leftarrow$) 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.

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 $x =$ __________ and $y =$ __________. Therefore every odd number can be written as the difference of two squares since

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?

Similar to the odd prime case, $4n = x^2 - y^2 = (x - y)(x + y)$ when $x =$ ____________ and $y =$ ____________.

■

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

Your Name: ____________________ Group Members: ____________________ ____________________

In-class Problem 1 (Chapter 6, Exercise 20) 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 $p \mid (x + y - z)$.