MATH 4573 Elementary Number Theory–Spring 2021

Spring 2021

Contents

1 Monday, January 11: Introduction and Divisibility

1.1 Introduction (30 minutes)

What is number theory?

Elementary number theory is the study of integers, especially the positive integers. A lot of the course focuses on prime numbers, which are the multiplicative building blocks of the integers. Another big topic in number theory is integer solutions to equations such as the Pythagorean triples $x^2 + y^2 = z^2$ or the generalization $x^n + y^n = z^n$. Proving that there are no integer solutions when $n > 2$ was an open problem for close to 400 years.

The first part of this course reproves facts about divisibility and prime numbers that you are probably familiar with. There are two purposes to this: 1) formalizing definitions and 2) starting with the situation you understand before moving to the new material.

Go over syllabus

1.2 What is group work (10 minutes, breakout rooms)

Random breakout rooms to discuss good group work, using Google sheets to track conversations. `https://docs.google.com/spreadsheets/d/12eFSXAICNphMIVtMB4hgQb7h3jvkysvcFQ0mtikx980/edit?usp=sharing` Each group will have someone in charge of recording in the Google sheet, someone in charge summarizing the conversation, and someone in charge reporting back to the class. Groups of 4 will also have someone in charge of time keeping and facilitating conversation.

Have 1 minute to think before going to breakout rooms. 4 minutes of discussion in the breakout rooms (remind them to introduce themselves!) while watching the Google sheet to see if they are still discussing. 2-3 minutes of whole class discussion after the breakout rooms with instructor recording.

1.3 Divisibility (15 minutes)

The goal of this chapter is to review basic facts about divisibility, get comfortable with the new notation, and solve some basic linear equations.

Ask: what is a definition for "a divides b"?

Definition. *Let $a, b \in \mathbb{Z}$. If there is an integer x such that $b = ax$, and we write $a \mid b$. int he case b is not divisible by a, we write $a \nmid b$.*

If $a \mid b$ we say that a is a divisor of b.

Note that 0 is not a divisor of any integer other than itself. Also all integers are divisors of 0, as odd as that sounds at first.

Finish with a group sharing their proof, and reminding students about the reading for Wednesday.

2 Wednesday, January 13: Division algorithm, divisibility

Reading assignment: Section 1.1 of Jones & Jones

Reading assignment: Exercise 1.4, If a divides b, and c divides d, must $a + c$ divide $b + d$?

2.1 Review of reading assignment (5 minutes)

Section 1.1 introduces the division algorithm, which will come up repeatedly throughout the semester, as well as the definition of divisors from last class, and the greatest common multiple.

Poll question. *If a divides b, and c divides d, must $a + c$ divide $b + d$?*

Solution. Posted after class. No. For example, if $a = b = c = 1$ and $d = 2$, then $a \mid b, c \mid d$, but $a + c = 2$ does not divide $b + d = 3$. This can also be written $2 \nmid 3$. □

2.2 Division Algorithm (40 minutes)

Breakout Room Problem (5 minutes)**.** *Prove: $a \mid b$ and $b \mid c$ imply $a \mid c$, (that is, division is* transitive*).*

Solution. Homework problem 1a. □

Breakout Room Problem. *(5 minutes) Prove: If $x \in \mathbb{R}$, then $x - 1 < \lfloor x \rfloor \leq x$.*

Solution. Homework problem 7. □

Example from class: If $x = 7$, then $7 - 1 < \lfloor 7 \rfloor = 7$.

Now I will give a slightly different proof of the division algorithm than the one from the reading.

Theorem 1 (The Division Algorithm, Textbook Theorem 1.1)**.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that*

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

Proof. Let $q = \left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - b \left\lfloor \frac{a}{b} \right\rfloor$. Then $a = bq + r$ by rearranging the equation. Now we need to show $0 \leq r < b$. Since $x - 1 < \lfloor x \rfloor \leq x$, we have

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}.$$

Multiplying all terms by $-b$, we get

$$-a + b > -b\left\lfloor \frac{a}{b} \right\rfloor \geq -a.$$

Adding a to every term gives

$$b > a - b\left\lfloor \frac{a}{b} \right\rfloor \geq 0.$$

By the definition of r, we have shown $0 \leq r < b$.

Finally, we need to show that q and r are unique. Assume

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

$$a = bq_2 + r_2, \quad 0 \leq r_2 < b.$$

We need to show $q_1 = q_2$ and $r_1 = r_2$. We can subtract the two equations from each other.

$$\begin{aligned} a &= bq_1 + r_1, \\ \underline{-(a} &\underline{= bq_2 + r_2)}, \\ 0 &= bq_1 + r_1 - bq_2 - r_2 = b(q_1 - q_2) + (r_1 - r_2). \end{aligned}$$

Rearranging, we get $b(q_1 - q_2) = r_2 - r_1$. Thus, $b \mid r_2 - r_1$. From rearranging the inequalities:

$$\begin{aligned} 0 &\leq r_2 < b \\ -\underline{b} &\underline{< -r_1 \leq 0} \\ -b &< r_2 - r_1 < b. \end{aligned}$$

Thus, the only way $b \mid r_2 - r_1$ is that $r_2 - r_1 = 0$ and thus $r_1 = r_2$. Now, $0 = b(q_1 - q_2) + (r_1 - r_2)$ becomes $0 = b(q_1 - q_2)$. Since we assumed $b > 0$, we have that $q_1 - q_2 = 0$. □

Corollary 2 (Corollary 1.2)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that*

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

2.3 Divisibility (10 minutes)

Recall the definition of divisibility from last class and the reading. We will now do exercise 1.3 in breakout rooms.

Breakout Room Problem (Exercise 1.3, 15 minutes or end with 5 minutes left in class)**.** *Prove that for integers a, b, c, d and m*

(a) if $a \mid b$ and $b \mid d$, then $ac \mid bd$;

(b) if $m \neq 0$, then $a \mid b$ if and only if $ma \mid mb$;

(c) if $d \mid a$ and $a \neq 0$, then $|d| \leq |a|$.

Solution. Homework problem 1. □

Finish class with having different groups present the set up for different proofs. 10 minutes is not enough for full proofs.

Remind them about the course survey.

3 Friday, January 15: Greatest Common Divisor, Bezout's identity

Reading assignment: Section 1.2 of Jones & Jones

Turn in:

1. In the calculation before the statement of Theorem 1.6, the text says "since $b > r_1 > r_2 > \cdots \geq 0$, we must eventually get a remainder $r_n = 0$ (after at most b steps)." Why is this true?
2. Exercise 1.7, Express $\gcd(1485, 1745)$ in the form $1485u + 1745v$.

3.1 Finishing divisibility (15 minutes)

Breakout Room Problem (Part of Exercise 1.22, 10 minutes)**.** *Show that if a and b are integers with $b \neq 0$, then there is a unique pair of integers q and r such that $a = qb + r$ and $\frac{-|b|}{2} < r \leq \frac{|b|}{2}$.*

Solution. Homework problem 2. □

Theorem 3 (Theorem 1.3)**.** *(a) If c divides $a_1, \ldots, a_k$, then c divides $a_1u_1 + \cdots + a_ku_k$ for all integers $u_1, \ldots, u_k$.*

(b) $a \mid b$ and $b \mid a$ if and only if $a = \pm b$.

3.2 Reading review (5 minutes)

Very quick breakout room (2 minutes) how does the reading relate to your previous understanding of greatest common divisor?

Poll question. *Which of the following is a way to represent* $\gcd(1485, 1745)$ *in the form* $1485u + 1745v$*?*

Solution. Choices and solution posted after class

$u = -47, v = 40$

$u = 337, v = -396$

$u = -257, v = 302$

All are correct! □

3.3 Greatest common divisor (35 minutes)

Definition. *If $a \mid b$ and $a \mid c$ then a is a* common divisor *of b and c.*

If at least one of b and c is not 0, the greatest (positive) number among their common divisors is called the greatest common divisor of a and b *and is denoted $gcd(a, b)$ or just (a, b).*

If $gcd(a, b) = 1$, we say that a and b are relatively prime*.*

If we want the greatest common divisor of several integers at once we denote that by $(b_1, b_2, b_3, \ldots, b_n)$.

For example, $(4, 8)$ is 4 but $(4, 6, 8)$ is 2.

The GCD always exists. How to show this: 1 is always a divisor, and no divisor can be larger than the maximum of $|a|, |b|$. So there is a finite number of divisors, thus there is a maximum.

Breakout Room Problem (Exercise 1.8, 15 minutes)**.** *Show that $c|a$ and $c|b$ if and only if $c| \gcd(a, b)$.*

Instead of doing this problem for homework, go over the solution in class.

Solution. Posted after class.

In one direction, assume that $c|a$ and $c|b$. By definition, c is a common divisor of a and b. By Corollary 1.4, for any integers u and v, $c \mid (au+bv)$. By Theorem 1.7 (Bezout's identity), there exist $u, v \in \mathbb{Z}$ such that $\gcd(a,b) = au+bv$. Thus, $c \mid \gcd(a,b)$.

In the other direction, assume that $c \mid \gcd(a,b)$. Then $c \mid a$ and $c \mid b$ by the transitivity of division. □

Lemma 4 (Lemma 1.5)**.** *If $a, b \in \mathbb{Z}, a \geq b > 0$, and $a = bq + r$ with $q, r \in \mathbb{Z}$, then $\gcd(a,b) = \gcd(b,r)$.*

Proof. Let c be a common divisor of a and b. Then $c \mid a$ and $c \mid b$ implies $c \mid a - bq$ by Corollary 1.4. By definition, $a - bq = r$. That is, $c \mid r$.

Since c is any common divisor of a and b, we find that the greatest common divisor $\gcd(a,b)$ is also a common divisor of b and r. If we can show any common divisor of b and r is a common divisor of a and b, we are done.

Let d be a common divisor of b and r. Then we have that $d \mid bq + r$, so $d \mid a$.

Thus, every common divisor of a and b is a common divisor of b and r and vice versa. Since the common divisors are the same, the greatest common divisors are also the same. □

Contents

4 Wednesday, January 20: Least common multiple and the start of Linear Diophantine equations

Reading assignment: Section 1.3

Turn in: How does this section relate to your previous understanding of the least common multiple?

4.1 Announcements (5 minutes)

Office hours will be Wednesdays a 2pm Eastern and Thursdays at 1 pm Eastern. I am also available by appointment for those of you who cannot attend office hours. Office hours will use the same link as class. It may take a some time to get the corrects times into the Zoom menu on Carmen, as Zoom still does not allow bulk edit.

To address some of the concerns about learning from reading (as opposed to lecture), I will post videos working through the examples in the reading. This will take a bit of time to post. However, this course is set up for you to learn by doing. The breakout room problems are meant to help you break down and understand the material from both the reading and the lectures. The reading assignments help keep you on schedule and come to class prepared to start asking questions and working on the material. This is also why late assignments are not accepted except in the case of an excuse absence.

Since we have not covered the proof of the Euclidean algorithm in class yet, the problem modifying the Euclidean algorithm we moved from Homework 1 to Homework 2. This is also the first breakout room assignment of today.

4.2 The Euclidean algorithm (40 minutes)

Theorem 5 (Euclidean algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. By the division algorithm, there exist $q_1, r_1 \in \mathbb{Z}$ such that*

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

If $r_1 > 0$, (by the division algorithm) there exist $q_2, r_2 \in \mathbb{Z}$ such that

$$b = r_1 q_2 + r_2, \quad 0 \le r_2 < r_1.$$

If $r_2 > 0$, (by the division algorithm) there exist $q_3, r_3 \in \mathbb{Z}$ such that

$$r_1 = r_2 q_3 + r_3, \quad 0 \le r_3 < r_2.$$

Continuing this process, $r_n = 0$ for some n. If $n > 1$, then $(a, b) = r_{n-1}$. If $n = 1$, then $(a, b) = b$.

Proof. Note that $r_1 > r_2 > r_3 > \cdots \ge 0$ by construction. If the sequence did not stop, then we would have an infinite, decreasing sequence of positive integers, which is not possible. Thus, $r_n = 0$ for some n.

When $n = 1$, $a = bq + 0$ and $\gcd(a, b) = b$.

If $n > 1$, then by repeated application of the previous lemma, we have

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1})$$

Then $r_{n-2} = r_{n-1} q_n + 0$. Thus $\gcd(r_{n-2}, r_{n-1}) = r_{n-1}$. □

The Euclidean algorithm allows us to write the gcd (a, b) as a linear combination of a and b. That is $(a, b) = ma + by$ for some $m, n \in \mathbb{Z}$.

Breakout Room Problem (Exercise 1.22 and part of 1.23, 20 minutes)**.** *From last time, we have that if a and b are integers with $b \neq 0$, then there is a unique pair of integers q and r such that $a = qb + r$ and $\frac{-|b|}{2} < r \le \frac{|b|}{2}$.*

1. *Use this result instead of Corollary 1.2 to devise an alternative algorithm to Euclid's for calculating greatest common divisors (the least remainders algorithm). That is, define an algorithm from repeatedly applying the formula from last class.*
2. *Show that for this new algorithm, $r_n = 0$ for some n, and that if $n > 1$, then $\gcd(a, b) = |r_{n-1}|$.*
   Hint: *The interval $\left(\frac{-|b|}{2}, \frac{|b|}{2}\right]$ is length $|b|$, the interval $\left(\frac{-|r_1|}{2}, \frac{|r_1|}{2}\right]$ is length $|r_1|$, etc. Why does the length of the intervals decrease?*
3. *Use the least remainders algorithm to find $\gcd(1066, 1492)$, and compare to the Euclidean algorithm.*

Solution. Homework 2, problem 1. The Euclidean algorithm for $\gcd(1066, 1492)$ is example 1.3. □

Here is another example:

Example 1. $a = 35, b = 9$.

$$\begin{aligned} 35 &= 9(3) + 5, & r_1 &= 5 \\ 9 &= 5(1) + 4, & r_2 &= 4 \\ 5 &= 4(1) + 1 & r_3 &= 1 \\ 4 &= 1(4) + 0 & r_4 &= 0. \end{aligned} \qquad \begin{aligned} 35 &= 9(4) - 1, & r_1 &= -1 \\ 9 &= -1(-9) + 0, & r_2 &= 0 \quad (\textit{or } 9 = 1(9) + 0) \end{aligned}$$

Theorem 6 (Theorem 1.8)**.** *Let a and b be integers (not both 0) with greatest common divisor d. Then an integer c has the form $ax + by$ for some $x, y \in \mathbb{Z}$ if and only if c is a multiple of d. In particular, d is the least positive integer of the form $ax + by$ for $x, y \in \mathbb{Z}$.*

The proof of this theorem is one of the "modifying proofs" problems on the homework, so we will skip it.

Definition. *Two integers a and b are* coprime *or* relatively prime *if* $\gcd(a, b) = 1$.

Corollary 7 (Corollary 1.9)**.** *Two integers are coprime if and only if there exists integers x and y such that*

$$ax + by = 1.$$

Proof. Let $\gcd(a, d) = d$. If we put $c = 1$ in Theorem 1.8, we see that $ax + by = 1$ for some $x, y \in \mathbb{Z}$ if and only if $d \mid 1$. Thus, $d = 1$ (why?). □

4.3 Review of reading and least common multiple (5 minutes)

Start with questions from the reading.

This section formalizes the concept of the least common multiple. There is only one result.

Definition. *If a and b are integers, then a* common multiple of a and b *is an integer c such that $a \mid c$ and $b \mid c$.*

If both a and b are not 0, the least (positive) number among their common multiples is called the least common multiple of a and b *and is denoted $lcm(a, b)$ or $[a, b]$.*

If we want the least common multiple of several integers at once we denote that by $[b_1, b_2, b_3, \dots, b_n]$.

We have a theorem from the reading:

Theorem 8 (Theorem 1.12)**.** *Let a and b be positive integers, with $d = \gcd(a, b)$ and $\ell = \operatorname{lcm}(a, b)$. Then*

$$d\ell = ab.$$

This is a case where we will focus more on the result than the proof method. I will skip the proof here.

4.4 Introduction to Diophantine equations (5 minutes)

Here we will get ahead of the reading!

Definition. *A* Diophantine equation *is an equation in one or more variables where we want integer solutions.*

Some of the most famous Diophantine equations are integer solutions to the Pythagorean theorem $x^2 + y^2 = z^2$, Fermat's equation $x^n + y^n = z^n$ (we will cover both of these equations in Chapter 11), and Pell's equation $x^2 - ny^2 = 1$.

We will start with the more basic linear Diophantine equation $ax + by = c$.

Thought for next time: Why don't we start with $ax = c$?

5 Friday, January 22: Diophantine equations

Section 1.4

Turn in Does the equation $15m + 48n = -6$ have solutions? Why or why not? If it has solutions, how many solutions exist?

5.1 Linear Diophantine equations (40 minutes)

Theorem 9 (Theorem 1.13)**.** *Let a and b be integers, with a and b not both 0, and let $d = \gcd(a, b)$. Then the equation*

$$ax + by = c$$

has an integer solution if and only if c is a multiple of d, in which case there are infinitely many solutions. These are the pairs

$$x = x_0 + \frac{bn}{d}, \quad y = y_0 - \frac{an}{d} \quad n \in \mathbb{Z},$$

where x_0, y_0 is a particular solution.

The proof of Theorem 1.13 is one of the modifying proofs problems on the homework.

Example 2. *Let $a = 6, b = 8, c = 4$. Then the integer solutions to $6x + 8y = 4$ are the exact same as the integer solutions to $3x + 4y = 2$. Let (x_0, y_0) be a solution (we will find one in a second). Then Theorem 1.13 says that the solutions to $6x + 8y = 4$ are*

$$x = x_0 + \frac{8n}{2} = x_0 + 4n, \qquad\qquad y = y_0 - \frac{6n}{2} = y_0 - 3n$$

The reduced fraction form matches with the solutions to $3x + 4y = 2$ from the theorem! It's always good when things that should match do match!

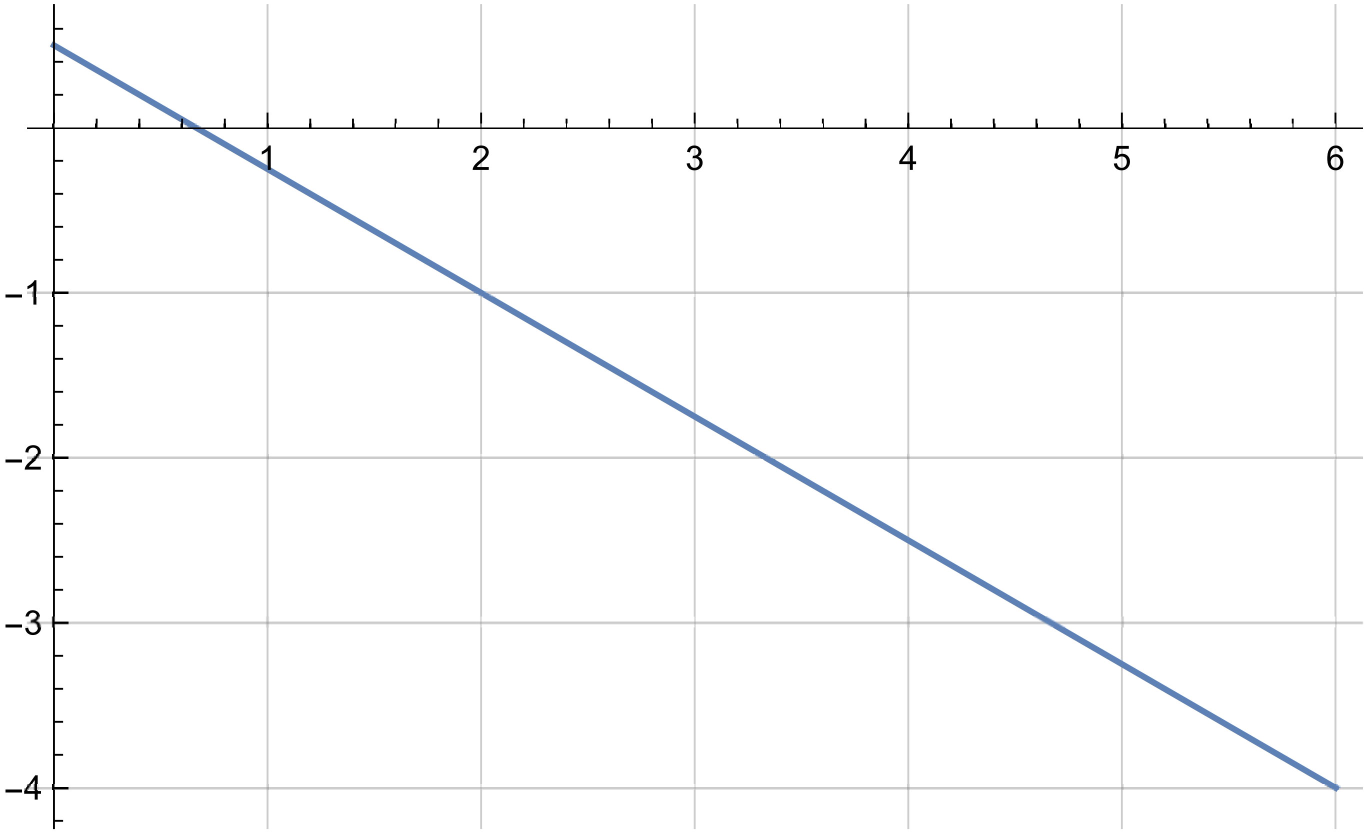
This is a good place for guess and check. $x_0 = 2, y_0 = -1$. Thus, $x = 2 + 4n, y = -1 - 3n$ for all $n \in \mathbb{Z}$.

Breakout Room Problem (Exercise 1.15, 5 minutes)**.** *Find the general solution of the Diophantine equation*

$$1485x + 1745y = 15.$$

We will go over this one in class

Discussion of lattice points, starting at at 25:24 in the Zoom recording. You can graph the equation as a line, then see where $x, y \in \mathbb{Z}$, which is where the gridlines meet if the gridlines are at every integer.



Breakout Room Problem (Exercise 1.16, 10 minutes)**.** *If $a_1, \dots, a_k$ and c are integers, when does the Diophantine equation*

$$a_1x_1 + \cdots + a_kx_k = c$$

have integer solutions $x_1, \dots, x_k$?

Provide a proof for your answer.

1. *You already know the answer for $k = 1$ and $k = 2$. What is it?*
2. *Try $k = 3$.*
3. *Try $k = 4$.*
4. *Can you generalize?*

5.2 Primes (10 minutes)

Definition. *An integer $p > 1$ is* prime *if the only positive divisors of p are* 1 *and itself. An integer n which is not prime is* composite.

Why is 1 not prime?

It has to do with units and invertibility. The number 1 holds a special place. It is the multiplicative identity, i.e., anything multiplied by 1 is just that thing again. Something is said to be invertible in a "group" (more on that later) if there exist something, which, when multiplied to it, gives you 1. How many invertible elements are there among the integers? Just two. 1 and −1. And that's the key. If we want to extend our results from positive integers to non-zero integers, we often just need to take into account ±1. That sounds obvious, but it turns out to be surprisingly critical and yet non-intuitive when we start moving from real integers to complex ones.

Contents

6 Monday, January 25: More primes

Reading: Section 2.1 Jones & Jones

Turn in: How does this section relate to your previous understanding of primes?

6.1 Primes (45 minutes)

Lemma 10 (Lemma 2.1 and Corollary 2.2)**.** *If p is prime and $a_1, \ldots, a_k$ are integers such that p divides $a_1 a_2 \cdots a_k$, then*

1. *either $p \mid a_i$ or $\gcd(a_i, p) = 1$ for each a_i,*
2. *p divides a_i for some i.*

Proof. 1. By definition $\gcd(a_i, p)$ is a positive divisor of p. Thus, it is either p or 1 since p is prime.

2. We use induction on k. If $k = 1$, then $p \mid a_i$ and we are done.

   If $k = 2$, then either $p \mid a_1$ and we are done, or $\gcd(a_1, p) = 1$ by part (a). Then by Bezout's identity, there exists integers u, v such that $1 = a_1 u + pv$. Thus, $a_2 = a_1 a_2 u + a_2 pv$. By assumption $p \mid a_1 a_2$, so p divides the linear combination $a_1 a_2 u + a_2 pv = a_2$.

   Now assume that $k > 2$ and that the result holds for all products of $k-1$ factors. Then we can write $a = a_1 \ldots a_{k-1}$ and $b = a_k$ and $p \mid ab$. By the $k = 2$ case, it follows that either $p \mid a$ or $p \mid b$. In the first case, $p \mid a = a_1 \cdots a_{k-1}$ means that $p \mid a_i$ for some i by the induction hypothesis. In the other case, $p \mid b$ means that $p \mid a_k$ by construction. □

For a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where $a_i \in \mathbb{Z}$, whether or not the a_i are divisible by some prime p helps determine if the polynomial can be factored.

Breakout Room Problem (Exercise 2.1, 5 minutes)**.** *Prove that if p is prime and $p \mid a^k$, then $p \mid a$, and thus $p^k \mid a^k$.*

Is this still valid if p is composite? Prove or provide a counterexample.

Theorem 11 (The Fundamental Theorem of Arithmetic, restatement of Textbook Theorem 2.3)**.** *Every integer $n \geq 2$ can be factored into a product of primes $n = p_1 p_2 p_3 \ldots p_n$ in a unique way (up to rearrangement).*

Proof. We work by induction. We can check that $2 = 2$, $3 = 3$ and $4 = 2^2$ all have prime factorizations. So assume now that all numbers n in the range $2 \leq n < N$ can be factored in the specified way, and we will show that N can be factored this way as well. If N is prime, then N is its own prime factorization. Otherwise N is composite and has some factor $2 \leq n_1 < N$. Thus we can write $N = n_1 n_2$. But n_2 must also be in the range $2 \leq n_2 < N$. Therefore n_1 and n_2 must be factorable into primes, say $n_1 = p_1 p_2 \ldots p_r$ and $n_2 = q_1 q_2 \ldots q_s$. Then $N = p_1 p_2 \ldots p_r q_1 q_2 \ldots q_s$. By induction, all integers $n \geq 2$ can be factored into a product of primes.

Now we must show this product is unique up to rearrangement. Suppose that n has two factorizations $p_1 p_2 \ldots p_r$ and $q_1 q_2 \ldots q_s$, and let us assume that $r \leq s$. By our previous theorem, since p_1 divides $q_1 q_2 \ldots q_s$, it must divide one of the q_i's, and, by rearranging, we can assume that $p_1 \mid q_1$. But q_1 is prime and only has 1 and q_1 as prime factors, so therefore, $p_1 = q_1$. Therefore we have $p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s$.

We can repeat this process (and repeatedly rearrange the q_i's as necessary) to show that $p_2 = q_2$, and then $p_3 = q_3$, and so on until we show that $1 = q_{r+1} q_{r+2} \ldots q_s$. If $s > r$, then the number on the right-hand side here is greater than 1, which is impossible, so we have that $r = s$ and $p_i = q_i$ for $1 \leq i \leq r$. This proves that the factorization is unique up to rearrangement. □

So let's suppose we want to factor an integer n. Let's start with $d = 2$.

We check to see if $d \mid n$. If it does, then we factor d out of n to get $n' = n/d$. We record the divisor d and henceforth work with n' in place of n, restarting at this step. Otherwise, we increment d by one and repeat this step.

Once $n = 1$, we have all the factors.

Now there are various ways we could try to speed this up. You might think we could only work with those trial divisors d that are prime, but it would take more time to check if d is a prime than it would to just see if it divides n. If it's composite, it won't, because we'll have already taken all its factors out of n beforehand.

One thing we can do is only check d up to $\sqrt{n}$. This is because n cannot have two prime factors that are each $> \sqrt{n}$. So if we reach this point, whatever n remains must be prime. So that takes us down from a worst case scenario of $d = n$ to a worst case scenario of $d = \sqrt{n}$. That's a big improvement. It's still very slow.

We can write out a prime factorization (of a positive integer) by

$$a = \prod_p p^{e_p}$$

where e_p is the number of times p divides a evenly. Note that $\prod$ denote a product in the same way that $\sum$ denotes a sum, and that the subscript p means that the product ranges over all primes.

This is what we are doing when we write $12 = 2^2 \cdot 3$.

This gives us the textbook's formulation of the Fundamental Theorem of Arithmetic

6.2 An asside on unique factorization (10 minutes)

Let $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$.

Definition. *An element $a + b\sqrt{-6}$ is* irreducible in $\mathbb{Z}[\sqrt{-6}]$ *if it cannot be expressed as a product of two elements for $\mathbb{Z}[\sqrt{6}]$ except with the trivial factorizations*

$$a + b\sqrt{-6} = (1)(a + b\sqrt{6}) = (-1)(-a - b\sqrt{6}).$$

We also define the *norm* of a number in $\mathbb{Z}[\sqrt{-6}]$ to be $||a + b\sqrt{-6}|| = a^2 + 6b^2$. The product of the norm is the norm of the product. That is $||xy|| = ||x||||y||$ for $x, y \in \mathbb{Z}[\sqrt{-6}]$. Why?

Example 3. *Examples from Zoom poll questions:*

Question 1: $2 = 2 + 0\sqrt{-6}, ||2|| = 2^2 + 6(0^2) = 4,$ *Question 2:* $5 = 5 + 0\sqrt{-6}, ||5|| = 5^2 + 6(0^2) = 25,$ *and Question 3:* $2 + \sqrt{-6} = 2^2 + 6(1^2) = 10.$

Think about: How would the fundamental theorem of arithmetic (Theorem 1.16) change if we said 1 is a prime number?

7 Wednesday, January 27: More distribution of primes

Reading: Section 2.2, distribution of primes

Turn in: After Theorem 2.9, the book says "There are also infinitely many primes of the form $4q + 1$; however the proof is a little more subtle. . . Where does the method of the proof of Theorem 2.9 break down in this case?"

Answer this question.

7.1 Review of reading and announcements (5 minutes)

7.2 Finishing Unique factorizations (10 minutes)

Breakout Room Problem (10 minutes)**.** *Consider* $\mathbb{Z}[\sqrt{-6}]$.

1. *Prove that* 2 *and* 5 *are irreducible elements of* $\mathbb{Z}[\sqrt{-6}]$.
2. *Prove that* $2+\sqrt{-6}$ *and* $2-\sqrt{-6}$ *are irreducible elements of* $\mathbb{Z}[\sqrt{-6}]$.
3. *Prove that there are elements of* $\mathbb{Z}[\sqrt{-6}]$ *with two different factorizations into irreducible elements, and thus* $\mathbb{Z}[\sqrt{-6}]$ *does not have unique factorizations.*

7.3 Prime-power factorization (20 minutes)

Supposed that integers a and b have factorizations

$$a = p_1^{e_1}\dots p_k^{e_k} \quad \text{and} \quad b = p_1^{f_1}\dots p_k^{f_k}$$

for primes p_i and integers $e_i, f_i \geq 0$. Then we have the following formulas:

Breakout Room Problem (5 minutes)**.**

$$\begin{aligned}
ab &= p_1^{e_1+f_1}\cdots p_k^{e_k+f_k}\\
\frac{a}{b} &= p_1^{e_1-f_1}\cdots p_k^{e_k-f_k}\\
a^m &= p_1^{me_1}\cdots p_k^{me_k}\\
\gcd(a,b) &= p_1^{\min(e_1,f_1)}\cdots p_k^{\min(e_k,f_k)}\\
\operatorname{lcm}(a,b) &= p_1^{\max(e_1,f_1)}\cdots p_k^{\max(e_k,f_k)}
\end{aligned}$$

Prove each of these formulas.

For a prime p, we use the notation $p^e||n$ to indicate that e is the highest power of p that divides n.

Lemma 12 (Lemma 2.4)**.** *If* $a_1, \dots a_r$ *are mutually coprime integers and* $a_1\cdots a_r$ *is an* m^{th} *power (ie,* $a_1\cdots a-r = b^m$ *for some integer* b*) for some integer* $m \geq 2$*, then each* a_i *is an* m^{th} *power.*

Proof. It follows from the formula for a^m that a positive integer is an m^{th} power if and only if the exponent of each prime in its prime-power factorization is divisible by m (recall, equals signs are if and only if statements). If $a = a_1\cdots a_r$, where the factors a_i are mutually coprime (ie, pairwise relatively prime), then each prime that divides a divides exactly one of the a_i. Thus, p^{me} appears in the prime factorization of a, if and only it also appears in the prime factorization of exactly one of the a_i. Since is is true for all prime power divisors of a, each a_i is also an m^{th} power. □

The assumption that the a_i are pairwise relatively prime is important! The integers $4, 6, 9$ are relatively prime as a triple, but not in pairs since $\gcd(4,6) = 2, \gcd(6,9) = 3$. Both 4 and 9 are perfect squares, but 6 is not. However $4*6*9 = 216 = 6^3$.

7.4 Counting primes (25 minutes, some moved to Friday)

The reading serves as an introduction to counting the *distribution* or *density* of primes. Much of *analytic number* theory is dedicated to proving these types of results. We will only go over a few in detail.

Theorem 13 (Euclid's infinitude of primes, Theorem 2.6)**.** *There are infinitely many primes*

Proof. We proceed by contradiction. Assume that there are finitely many prime numbers, $p_1, p_2, \ldots, p_k$. Consider

$$m = p_1 p_2 \cdots p_k + 1.$$

Since m is an integer greater than 1, the Fundamental Theorem of Arithmetic (Theorem 2.3) implies that there exists some p prime such that $p \mid m$. By our assumption, p must be in the list $p_1, p_2, \ldots, p_k$. Then $p \mid p_1 p_2 \cdots p_k$ and $p \mid m$. Thus, $p \mid m - p_1 p_2 \cdots p_k = 1$. However, the only positive divisor of 1 is 1. Thus, we have reached a contradiction and there must be infinitely many primes. □

Theorem 14. *There are infinitely many primes of the form* $4q + 3$.

Reviewing this proof was part of the reading assignment. Questions on that proof?

8 Friday, January 29: Finishing up primes

Reading: Read the three attached introductions to modular arithmetic: Jones & Jones pages 37-40, Granville page 61-62, and Strayer pages 39-41.

In class, we will discuss editing and giving feedback on writing. In addition to analyzing the different writing styles, we will create rubrics for giving feedback. We will create "sentence stems" that can be used for giving feedback such as "This sentence helps me understand, because..."

Turn in: Give one potential sentence stem for giving feedback on mathematical writing.

Pick which reading you like the most and which you like the least and answer the following questions about each of them:

1. Why did you pick those two readings? What makes you like or dislike them?
2. For each reading, identify something that the author does that helps you understand the material.
3. For each reading, identify something that the author does that is confusing.

8.1 Announcements (5 minutes)

Hints to Homework 2, Problem 1b are linked from the *Divisibility* discussion board.

How to read Gradescope score: `https://help.gradescope.com/article/axm932lptr-student-view-submission`

8.2 Counting primes (20 minutes)

Breakout Room Problem (Exercise 2.6, 5 minutes)**.** *Prove that every prime* $p \neq 3$ *has the form* $3n + 1$ *or* $3n + 2$ *for some integer* n*. Prove that there are infinitely many primes of the form* $3n + 2$.

Hint. The □

Theorem 15 (Reformulation of Exercise 2.7)**.** *There are arbitrarily large gaps in the primes. In other words, for any positive integer* k*, there exist* k *consecutive composite integers.*

Breakout Room Problem (Exercise 2.7, 5 minutes)**.** *Find five consecutive composite integers. Show that for each integer* $k \geq 1$*, there is a sequence of* k *consecutive composite integers.*

Now, what about how many primes there are? We let $\pi(x)$ denote the number of primes up to x. So $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 2$ and so on.

Theorem 16 (Prime Number Theorem)**.**

$$\lim_{n\to\infty} \frac{\pi(x)}{x/\log x} = 1$$

Conjecture (Twin Prime Conjecture)**.** *There are infinitely many prime numbers p for which $p+2$ is also a prime number.*

8.3 Creating feedback rubrics (20 minutes)

Now we will look at the reading assignments and creating feedback rubrics.

In your breakout rooms, answer:

Breakout Room Problem. *What was one thing that you found helpful in one of the readings? What is one piece of advice you would like to give one of the authors?*

An example of a graded student homework is on the January 29 Participation assignment.

Contents

9 Monday, February 1: Modular arithmetic

Reading: Section 3.1 through the paragraph after Exercise 3.3 (page 43) of Jones and Jones, Modular arithmetic

Turn in: Exercise 3.2, Without using a calculator, find:

(a) the least non-negative residue of $34 * 17 \pmod{29}$;

(b) the least absolute residue of $19 * 14 \pmod{23}$;

(c) the remainder when 510 is divided by 19;

(d) the final decimal digit of $1! + 2! + 3! + ... + 10!$

9.1 Primality testing and factorization (10 minutes)

We will spend more time on divisibility testing when we talk about cryptography.

Lemma 17 (Lemma 2.14)**.** *An integer $n > 1$ is composite if and only if it is divisible by some prime $p \leq \sqrt{n}$.*

Proof. In one direction, assume that $p \mid n$ for some prime $p \leq \sqrt{n}$. Then since $1 < p \leq \sqrt{n} < n$, n must be composite by definition.

In the other direction, assume that n is composite. Then $n = ab$ for some positive integers $1 < a, b < n$. If both a and b are greater than $\sqrt{n}$, then $ab > n$. Thus, at least one of a or b is less than the $\sqrt{n}$. Without loss of generality, say that $a \leq \sqrt{n}$. By the Fundamental Theorem of Arithmetic, there exists a prime p that divides a. Thus, $p \leq \sqrt{n}$. □

9.2 Review of Reading (5 minutes)

Congruences generalize the concept of evenness and oddness. We typically think of even and odd as "divisible by 2" and "not divisible by 2", but a more useful interpretation is even means "there is no remainder when divided by 2" and "there is a remainder of 1 when divided by 2". This interpretation gives us more flexibility when replacing 2 by larger numbers. Instead of "divisible" or "not divisible" we have several gradations.

For example, we have the sets "remainder of 0 when divided by 3," "remainder of 1 when divided by 3," and "remainder of 2 when divided by 3."

9.3 Modular arithmetic (40 minutes)

Definition. *We say that a is congruent to b modulo m and write $a \equiv b \pmod{m}$ if a and b have the same remainder when divided by m. We generally apply this for $a, b \in \mathbb{Z}$ and an integer $m \geq 2$.*

If a and b are not equivalent $\pmod{m}$, we write $a \not\equiv b \pmod{m}$.

Poll question. *Select all numbers that are congruent to:*

Question 1: $5 \pmod{2}$

- *Answer 1: -1*
- *Answer 2: 3*
- *Answer 3: 6*
- *Answer 4: -10*

Question 2: $10 \pmod{4}$

- *Answer 1: -6*
- *Answer 2: -2*
- *Answer 3: 0*
- *Answer 4: 5*

Question 3: $100 \pmod{9}$

- *Answer 1: -8*
- *Answer 2: -17*
- *Answer 3: 1*
- *Answer 4: 10*

Solution. Options and answers posted after class.

Question 1: $-1 \equiv 3 \equiv 5 \pmod{2}$ Question 2: $-6 \equiv -2 \equiv 10 \pmod{4}$ Question 3: $-8 \equiv -17 \equiv 1 \equiv 10 \pmod{9}$ □

Be careful with this idea and negative values. Make sure you understand why $-2 \equiv 1 \pmod{3}$ or $-10 \equiv 4 \pmod{7}$.

Sometimes it will be helpful to think of congruences one way, sometimes the other. The latter is helpful for understanding why -2, 1, 4, and 7 are all equivalent modulo 3.

While this is a useful starting point for understanding congruences, it's only a starting point. Here's are two alternate definitions:

Lemma 18. *[Lemma 3.1 expanded]*

1. *a and b are equivalent modulo m if and only if m divides $a - b$.*
2. *a and b are equivalent modulo m if and only if they differ by a multiple of m.*

Breakout Room Problem (Lemma 3.1 expanded, 5 minutes)**.** *Prove that*

1. *a and b are equivalent modulo m if and only if m divides $a - b$.*
2. *a and b are equivalent modulo m if and only if they differ by a multiple of m.*

This is why it is helpful to know that every integer m divides 0.

We can use the idea of congruences to simplify some of the arguments from section 2.5. First, let's prove Lemma 3.3

Breakout Room Problem (Lemma 3.3 expanded, 5 minutes)**.** *Let a, b, c, d denote integers, then:*

(a) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ implies $a \equiv c \pmod{m}$

(b) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $a + c \equiv b + d \pmod{m}$

(c) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $ac \equiv bd \pmod{m}$.

(d) $a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$ implies $a \equiv b \pmod{d}$

(e) $a \equiv b \pmod{m}$ implies $ac \equiv bc \pmod{mc}$ for $c > 0$.

Parts (b), (c) *are proved in the book.*

Let's look at the various parts of this expanded Lemma 3.3 and see what they tell us about how congruences and moduli work.

The first two parts tell us that congruences behave a lot like equality.

The last two parts tell us how we can manipulate the modulus m. We can replace the modulus with a divisor of it at any time. We can replace the modulus with a multiple of it, provided we multiply a and b by the same multiple.

The remaining two parts are perhaps the most useful: they let us do arithmetic with congruences. In particular, they imply that whenever I'm adding or multiplying numbers, I can replace the numbers I have with any equivalent number that is more convenient to use. So for example, $37 * 210 \equiv 1 * 0 \pmod{2}$ or $651262 * 697016 \equiv 2 * 6 \pmod{10}$.

Note that this doesn't work for powers. It is not the case that $2^{20} \equiv 2^0 \pmod{2}$. Also, unlike for regular equality, we cannot cancel a common factor of both sides unless it is relatively prime to m. That is to say $ac \equiv bc \pmod{m}$ implies $a \equiv b \pmod{m}$ if $gcd(c, m) = 1$. (If $gcd(c, m) > 1$ we'll talk more on this later.)

10 Wednesday, February 3: Modular arithmetic

Reading: The rest of Section 3.1 of Jones and Jones, Modular arithmetic

Turn in: Part of Exercise 3.4, Prove that the following polynomials have no integer roots:

(a) $x^3 - x + 1$

10.1 Student questions (5 minutes)

Question of how to prove that 5 is irreducible in $\mathbb{Z}[\sqrt{-6}]$.

Notes from class linked from the Participation assignment.

10.2 Finish material from Monday (30 minutes)

Proposition 19. *A natural number is divisible by* 3 *if and only if the sum of its (base* 10*) digits is divisible by* 3.

Proof. Let a number $n \in \mathbb{N}$ have base 10 expansion $a_k a_{k-1} a_{k-2} \dots a_1 a_0$ so that $n = \sum_{i \leq k} a_i 10^i$. By the definition of congruences, we have that $3 \mid n$ if and only if $n \equiv 0 \pmod{3}$. Using the fact that $10 \equiv 1 \pmod{3}$, we know by Lemma 3.3 that any time we multiply by 10 (modulo 3) we could instead just multiply by 1 (modulo 3). So,

$$n \equiv \sum_{i \leq k} a_i 10^i \equiv \sum_{i \leq k} a_i 1^i \equiv \sum_{i \leq k} a_i \pmod{3}.$$

Therefore $n \equiv 0 \pmod{3}$ if and only if the sum of the digits of n is $0 \pmod{3}$. □

Breakout Room Problem (5 minutes)**.** *List all integers in the range 1 to 100 that are congruent to 7 mod 17.*

Go over this as a class.

Breakout Room Problem (5 minutes, with previous problem)**.** *Find all positive integers m for which the following statements are true:*

1. $13 \equiv 5 \pmod{m}$
2. $10 \equiv 9 \pmod{m}$
3. $-7 \equiv 6 \pmod{m}$.

Why study congruence relations? Why not stick to good old integers all the time?

There's two major reasons. As we've already seen, calculations get simplified for modular arithmetic. We'll see later that taking MASSIVE powers of MASSIVE numbers is a fairly doable feat in modular arithmetic. The second reason is that by reducing a question from all integers to modular arithmetic, we often have an easier time seeing what is not allowed.

Here's an example of this second phenomenon. Consider $a^2 + b^2 = c^2$, the Pythagorean relation. Suppose we have a solution to this. Since equality holds, then the weaker fact of congruence modulo 3 must also hold. So $a^2 + b^2 \equiv c^2 \pmod{3}$. Because of what we said before about multiplication, we can reduce all the values here to either 0, 1, or 2. But $0^2 \equiv 0 \pmod{3}$, $1^2 \equiv 1 \pmod{3}$, and $2^2 \equiv 4 \equiv 1 \pmod{3}$. Since it is impossible to have $c^2 \equiv 2 \pmod{3}$, we cannot have that $a^2 + b^2 \equiv 2 \pmod{3}$. Thus at least one of a or b must be $0 \pmod{3}$. We have learned something about what the possible solutions to $a^2 + b^2 = c^2$ look like by studying a congruence.

10.3 More on basics of modular arithmetic (20 minutes)

The point of the next theorem is to say that DIVISION is different and we must be careful with it. Here's the special rule.

Theorem 20. *1. $ax \equiv ay \pmod{m}$ if and only if $x \equiv y \pmod{\frac{m}{\gcd(a,m)}}$.*

2. If $ax \equiv ay \pmod{m}$ and $(a, m) = 1$ then $x \equiv y \pmod{m}$.

3. $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$ if and only if $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$.

This second part gives an idea of why prime values of m are so helpful!

The proof of the lemma is left for homework.

I will prove the first part for $a = 6, m = 8$, and the third part for $i = 2$. The general proof is left for homework.

Proof. 1. (Proof for $a = 6, m = 8$, and $\gcd(a, m) = 2$) If $6x \equiv 6y \pmod{8}$, then $6y - 6x = 8z$ for some integer z. Thus,

$$\frac{6}{2}(y - x) = \frac{8}{2}z,$$

and so $\frac{8}{2} = 4$ divides $3(y - x)$. Rewriting Corollary 10, we get $\gcd(6, 8) = 2 * \gcd(3, 4)$. Therefore, the only way 4 divides $3(y - x)$ is if it divides $y - x$. Then by definition $x \equiv y \pmod{4}$.

In the direction, suppose $x \equiv y \pmod{\frac{8}{2}}$. Then $4 \mid (x-y)$. Multiplying through by $\gcd(6, 8) = 2$ gives $8 \mid 2x-2y$. Since $\frac{6}{2} \in \mathbb{Z}$, we have $8 \mid 3(2x - 2y)$. Thus, $6x \equiv 6y \pmod{8}$.

2. Left for homework

3. (Proof for $i = 2$). If $x \equiv y \pmod{m_1}$ and $x \equiv y \pmod{m_2}$, then $m_i \mid (y-x)$ for $i = 1, 2$. That is, $y - x$ is a common multiple of m_1 and m_2. Therefore, by Exercise 1.14, $[m_1, m_2] \mid (y-x)$. This implies $x \equiv y \pmod{[m_1, m_2]}$

   In the other direction, if $x \equiv y \pmod{[m_1, m_2]}$, then $x \equiv y \pmod{m_i}$ by expanded Lemma 3.3 part 4, since $m_i \mid [m_1, m_2]$. □

11 Friday, February 5: Modular arithmetic with polynomials

Reading: No reading. Projects due.

11.1 Questions from students (5 minutes)

11.2 Modular arithmetic with polynomials (10 minutes)

We are going to look at polynomials, we will look at some very basic results now and then go into specific cases.

Lemma 21 (Lemma 3.5). *Let f denote a polynomial with integer coefficients. If $a \equiv b \pmod{m}$ then $f(a) = f(b) \pmod{m}$.*

Example 4. *Let $f(x) = x^2 + 1$. Then if $a \equiv b \pmod{5}$, then $f(a) \equiv f(b) \pmod{5}$. That is, $a^2 + 1 \equiv b^2 + 1 \pmod{5}$. If $a = 3, b = 8$, then this means $3^2 + 1 \equiv 10 \equiv 65 \equiv 8^2 + 1 \pmod{5}$.*

Proof. We can write $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ for some integers c_i. Then by Theorem 2.1 part 4, we have that $a \equiv b \pmod{m}$ implies $a^2 \equiv b^2 \pmod{m}, a^3 \equiv b^3 \pmod{m}, \ldots, a^n \equiv b^n \pmod{m}$. Also by Theorem 2.1 part 4, we have $c_i a^i \equiv c_i b^i \pmod{m}$. Finally, putting everything together with Theorem 2.1 part 3, we have that $c_n a^n + c_{n-1}a^{n-1} + \cdots + c_1 a + c_0 \equiv c_n b^n + c_{n-1}b^{n-1} + \cdots + c_1 b + c_0 \pmod{m}$. □

11.3 Residue classes, lots of definitions (40 minutes)

Definition. *If $x \equiv y \pmod{m}$ then y is called a residue of $x \pmod{m}$.*

A set $x_1, x_2, \ldots, x_m$ is called a complete residue system modulo m *if every integer y there exists exactly one x_j such that $y \equiv x_j \pmod{m}$.*

Implication: If you have a complete residue system $\pmod{m}$, then $x_i \not\equiv x_j \pmod{m}$ if $i \neq j$.

Definition. *Let $r_1, r_2, \ldots, r_m$ denote a complete residue system modulo m. The* number of solutions of $f(x) = 0 \pmod{m}$ *is the number of r_i such that $f(r_i) = 0 \pmod{m}$. That is, each solution r_1 is the representative of a congruence class of solutions, and we only count the number of congruence classes. This agrees with asking for the number of incongruent solutions (why?).*

Answer "why" as a class.

Definition. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. The* degree of the polynomial $\pmod{m}$ *is the largest integer j such that $a_j \not\equiv 0 \pmod{m}$. If all of the $a_i \equiv 0 \pmod{m}$, then the degree is 0.*

Definition. *The set of all numbers x satisfying $x \equiv a \pmod{m}$ is the* arithmetic progression $\ldots, a-m, a, a+m, a+2m, \ldots$ *and this is called a* residue class or congruence class modulo m.

Breakout Room Problem (2 minutes). *Find a complete residue system mod 17 where every number is a multiple of 3.*

Discussion as a class: The congruence classes of 17 are:

$$\begin{gathered}
\ldots, -34, -17, 0, 17, 34, \ldots \\
\ldots, -33, -16, 1, 18, 35, \ldots \\
\ldots, -32, -15, 2, 19, 36, \ldots \\
\ldots, -31, -14, 3, 20, 37, \ldots \\
\ldots, -30, -13, 4, 21, 38, \ldots \\
\ldots, -29, -12, 5, 22, 39, \ldots \\
\ldots, -28, -11, 6, 23, 40, \ldots \\
\ldots, -27, -10, 7, 24, 41, \ldots \\
\ldots, -26, -9, 8, 25, 42, \ldots \\
\ldots, -25, -8, 9, 26, 43, \ldots \\
\ldots, -24, -7, 10, 27, 44, \ldots \\
\ldots, -23, -6, 11, 28, 45, \ldots \\
\ldots, -22, -5, 12, 29, 46, \ldots \\
\ldots, -21, -4, 13, 30, 47, \ldots \\
\ldots, -20, -3, 14, 31, 48, \ldots \\
\ldots, -19, -2, 15, 32, 49, \ldots \\
\ldots, -18, -1, 16, 33, 50, \ldots
\end{gathered}$$

Each infinite list is one congruence class. To get a complete residue system, pick exactly one element from each list.

Definition. *A* reduced residue system modulo m *is a set of integers* r_i *such that* $\gcd(r_i, m) = 1$*, and for every* x *coprime to* m *is congruent modulo* m *to exactly one member* r_i *of the set.*

Now we need to know if this is well defined. How do we know if $\gcd(r, m) = 1$ is something that is preserved over a given residue class? By the following result:

Proposition 22. *If* $b \equiv c \pmod{m}$ *then* $\gcd(b, m) = \gcd(c, m)$.

Breakout Room Problem (5 minutes)**.** *Prove that if* $b \equiv c \pmod{m}$*, then* $\gcd(b, m) = \gcd(c, m)$*.*

Finally, we want to look out for some weird behavior in with modular arithmetic.

Breakout Room Problem (5 minutes)**.** *Find* $a, b, m \in \mathbb{Z}$ *such that* $ab \equiv 0 \pmod{m}$ *but* $a \not\equiv 0 \pmod{m}$ *and* $b \not\equiv 0 \pmod{n}$*.*

Go over as a class.

Contents

12 Monday, February 8: Linear Congruences

Reading assignment: Section 3.2 of Jones & Jones.

Turn in: The proof of Theorem 3.7 starts "Apart from a slight change of notation (n and b replacing b and c), the only part of this which is not a direct translation of Theorem 1.13 is...". Translate the statement of Theorem 3.7 to the statement of Theorem 1.13. In other words, provide the omitted steps of the proof of Theorem 3.7.

12.1 Questions about reading, announcements (5 minutes)

12.2 Zero Divisors (15 minutes)

Definition. *Let m be a positive integer. We denote the set of equivalence classes* $\pmod{m}$ *as* $\mathbb{Z}_m$*.*

Consider the $\pmod{8}$ multiplication chart:

x_8	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	0	2	4	6	0
3	3	6	1	4	7	2	5	0
4	4	0	4	0	4	0	4	0
5	5	2	7	4	1	6	3	0
6	6	4	2	0	6	4	2	0
7	7	6	5	4	3	2	1	0
8	0	0	0	0	0	0	0	0

Example 5. *Write every combination a, b in the chart where $ab \equiv 0 \pmod{8}$ and neither a or b is $8 \equiv 0 \pmod{8}$. Write every combination $ab \equiv 1 \pmod{8}$.*

Solution. $2(4) \equiv 4(2) \equiv 4(4) \equiv 4(6) \equiv 6(4) \equiv 0 \pmod{8}$. $1(1) \equiv 3(3) \equiv 5(5) \equiv 7(7) \equiv 1 \pmod{8}$. □

Right away, we can see things are weird. We have that $ab \equiv 0 \pmod{8}$ does not imply either a or b is 0. This means that our proof of the division algorithm (theorem 1.2) falls apart at the step where $0 = b(q_1 - q_2), b > 0$ implies $q_1 = q_2$ if we try to use the division algorithm mod m. That means that every proof that relies on the division algorithm, including the gcd results and the fundamental theorem of arithmetic, either fall apart or require new proofs. However, it is ok to use these as proven, we just can't say that they are true for modular arithmetic.

Another thing that is unusual is that $ab \equiv 1 \mod 8$ does not imply that $a = b = \pm 1$. This is a little less unusual, since this is true for rational numbers, just not integers.

Definition. *A number $a \in \mathbb{Z}$ is* invertible $\pmod{m}$ *if there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$. Another way to say this is a* has a multiplicative inverse in $\mathbb{Z}_m$*.*

In other words, $a \in \mathbb{Z}_m$ is invertible if there is a solution to $ax \equiv 1 \pmod{m}$. In this section, we will find to solutions to $ax \equiv b \pmod{m}$.

12.3 Linear Congruences (25 minutes)

Theorem 23 (Theorem 3.7)**.** *If $d = \gcd(a, n)$, then the linear congruence*

$$ax \equiv b \pmod{n}$$

has a solution if and only if d divides b. If d divides b, then there are exactly d incongruent solutions of the form

$$x = x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d},$$

where x_0 is a particular solution.

Proof. (Solution to the reading assignment question posted after class) A solution to $ax \equiv b \pmod{n}$ exists if and only if there exists y such that $ax - b = ny$. That is, if and only if $ax - ny = b$ has solutions. From Theorem 1.13, this equation has a solution if and only if $d \mid b$.

Note that

$$x_0 + \frac{nt}{d} \equiv x_0 + \frac{nu}{d} \pmod{n}$$

if and only if

$$\frac{nt}{d} \equiv \frac{nu}{d} \pmod{n}.$$

This congruence is true if and only if n divides $\frac{n(t-u)}{d}$, which in turn is true if and only if $\frac{t-u}{d}$ is an integer. Thus the d solutions of the form

$$x = x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$$

represent different congruence classes. □

Corollary 24 (Corollary 3.8)**.** *If* $\gcd(a, n) = 1$*, then the solutions to* $ax \equiv b \pmod{n}$ *form a single congruence class* $\pmod{n}$*. In other words, there is a unique solution to* $[a][x] = [b]$ *in* $\mathbb{Z}_n$*.*

Breakout Room Problem (Exercise 3.7, 15 minutes)**.** *Using the algorithm given in Section 3.2, on page 51 and 52, for each of the following congruences, decide whether a solution exists and if it does exist, find the general solution:*

(a) $3x \equiv 5 \pmod{7}$*,*

(b) $12x \equiv 15 \pmod{22}$*,*

(c) $19x \equiv 42 \pmod{50}$*,*

(d) $18x \equiv 42 \pmod{50}$*.*

For two of these equivalences can also do this slightly differently, using multiplicative inverses. By a quick check, we see that $3(5) \equiv 1 \pmod{7}$ and $19(29) \equiv 1 \pmod{50}$. Thus,

$$x \equiv 5(3x) \equiv 5(5) \equiv 4 \pmod{7},$$

and

$$x \equiv 29(19x) \equiv 29(42) \equiv 18 \pmod{50}.$$

13 Wednesday, February 10: Chinese remainder theorem

Reading: Scanned notes on the Chinese Remainder Theorem. NOTE: The scanned notes only prove the $k = 2$ case of the Chinese Remainder Theorem, with the "multiple congruences extension of the Chinese Remainder Theorem" left as an exercise. The Chinese Remainder Theorem is typically stated for k congruences, as in Theorem 3.10 in Jones and Jones.

Turn in: In the proof of the Chinese Remainder Theorem in the scanned notes, it says "In Exercise 23, you will complete the proof of the theorem by showing that this solution is unique modulo ab." Complete the proof.

Revisiting infinitude of primes (15 minutes)

Revisiting the proof that there are infinitely many primes of the form $4n + 3$**.**

From the division algorithm, we know that all integers can be written as $4n, 4n + 1, 4n + 2$, or $4n + 3$.
All integers of the form $4n$ are composite, since they are divisible by 4.
All integers of the form $4n + 2$ are even, since they can be written $2(2n + 1)$. When $n \neq 0$, integers of this form are composite.

When seeking a contradiction, the book says "Suppose that there are only finitely many primes of this $[4n + 3]$ form, say $p_1, \ldots, p_k$. Let $m = 4p_1 \cdots p_k - 1$...Since m is odd..." The fact that m is odd comes from the fact that $4n$ is always even, so $4n-1$ is always odd. It also means that there are no factors of the form $4n+2$ or $4n$. Thus, the only options are $4n+1$ and $4n+3$. From there, the proof shows that one of the factors must have the form $4n+3$ and not be on the list $p_1, \ldots, p_k$.

Proof that there are infinitely many primes of the form $3n+2$.

From the division algorithm, we know that all integers can be written as $3n, 3n+1$, or $3n+2$.
For $n \neq 1$, all integers of the form $3n$ are composite.

When seeking a contradiction, Suppose that there are only finitely many primes of the form $3n+2$, say $q_1, \ldots, q_j$. Let $k = 3q_1 \cdots q_k - 1$. By construction, k is not of the form $3n$, so none of the prime factors are, either.

In the $4n+3$ case, we had to eliminate factors of the form $4n+2$, but there is no analogous step here. The options are already only $3n+1$ and $3n+2$.

Chinese Remainder Theorem

Breakout Room Problem (Exercise 3.15, 5 minutes)**.** *As a party trick, you ask a friend to choose an integer from 1 to 100, and to tell you its remainders on division by 3,5 and 7. How can you instantly identify the chosen number?*

Breakout room: First person alphabetically by Zoom display name picks a number from 1 to 100 and tells the group the remainders when divisible by 3,5, and 7. The rest of the group then determines the number.

We are going to go through the proof of the Chinese remainder theorem.

Theorem 25 (Chinese remainder theorem, Theorem 3.10)**.** *Let $m_1, m_2, \ldots m_r$ be pairwise relatively prime positive integers (that is, any pair* $\gcd(m_i, m_j) = 1$ *when $i \neq j$). Let $a_1, a_2, \ldots, a_r$ be integers. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \cdots_r$. This solution has the form

$$x_0 = \sum_{i=1}^{r} \frac{M}{m_i} b_i a_i,$$

where $b_i(\frac{M}{m_i}) \equiv 1 \pmod{m_i}$.

Proof. We start by constructing a solution mod $M = m_1 m_2 \cdots_r$. By construction, $\frac{M}{m_i}$ is an integer. Since each the m_i are pairwise relatively prime, $\gcd(\frac{M}{m_i}, m_i) = 1$. Thus, by Corollary 3.8, for each i there is an integer b_i where $\frac{M}{m_i} b_i \equiv 1 \pmod{m_i}$. We also have that $(\frac{M}{m_i}, m_j) = m_j$ when $i \neq j$, so $\frac{M}{m_i} b_i \equiv 0 \pmod{m_j}$ when $i \neq j$. Let

$$x_0 = \sum_{i=1}^{r} \frac{M}{m_i} b_i a_i.$$

Then $x_0 \equiv \frac{M}{m_i} b_i a_i \equiv a_i \pmod{m_i}$ for each $i = 1, 2, \ldots, r$. We have found a solution to the system of equivalences.

If we have some other solution x_1, we have that $x_0 \equiv x_1 \pmod{m_i}$ for all $i = 1, 2, \ldots, r$. Then $m_i \mid x_0 - x_1$ for all $i = 1, 2, \ldots, r$ and $M \mid x_0 - x_1$. Thus, $x_0 \equiv x_1 \pmod{M}$. □

However, we don't have to work with relatively prime moduli.

Example 6. *Solve the system of equivalences*

$$\begin{aligned} x &\equiv 2 \pmod 6 \\ x &\equiv 8 \pmod 9 \end{aligned}$$

and find a (possible) modulus m where solutions are congruent $\pmod m$*.*

Solution. One thing we can do is list possible solutions.

$$\begin{aligned} x &\equiv 2 \pmod 6, \quad x = 2, 8, 14, 20, 26, \ldots, 2+6j, \ldots \\ x &\equiv 8 \pmod 9, \quad x = 8, 17, 26, \ldots, \ldots 8+9k, \ldots \end{aligned}$$

We see that 8 and 26 are solutions. We have $26 - 8 = 18$, so $m = 18$.

There are no smaller moduli that work, since that would introduce options that do not work. For example $x \equiv 2 \pmod 3$ includes 2 and 5 which are not solutions $\pmod 9$. □

Theorem 26 (Generalized Chinese Remainder Theorem)**.** *Let $m_1, m_2, \ldots m_r$ be positive integers, and let $a_1, a_2, \ldots, a_r$ be integers. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a solution if and only if $\gcd(m_i, m_j) \mid a_i - a_j$ *for all $i \neq j$. In this case, the solution is unique modulo* $M = \operatorname{lcm}[m_1, m_2, \ldots, m_r]$.

Proof. Homework 5, also textbook Theorem 3.12. □

14 Friday, February 12: Fermat's Little Theorem and Euler's generalization

Reading: Scanned notes on Wilson's theorem and Fermat's Little Theorem.

Turn in: Prove that $9^{10} = 1 \pmod{11}$ by following the steps in the proof of Fermat's Little Theorem (Theorem 2.13 in the reading, Theorem 4.3 in Jones & Jones).

14.1 Fermat's Little Theorem and Euler's generalization (25 minutes)

Breakout Room Problem (10 minutes)**.** *Prove the Generalized Chinese Remainder Theorem for $r = 2$. Let m_1, m_2 be positive integers, and let a_1, a_2 be integers. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

has a solution if and only if $\gcd(m_i, m_j) \mid a_i - a_j$ *for all $i \neq j$. In this case, the solution is unique modulo* $\operatorname{lcm}[m_1, m_2]$.

Theorem 27. *Let p be a prime number and a be an integer not divisible by p. Then the numbers $a, 2a, 3a, \ldots, (p-1)a$* $\pmod p$ *are the same as the numbers $1, 2, 3, \ldots, (p-1)$, but may be in a different order.*

Proof. The list $a, 2a, \ldots, (p-1)a$ contains $p-1$ numbers. Each takes the form ka for some $1 \leq k \leq p-1$, and thus, since neither k nor a is divisible by p, we have that nothing in this list is divisible by p either. Now we want to show the elements of this list are distinct. Let $1 \leq j < k \leq p-1$ and suppose $ja \equiv ka \pmod{p}$. Then $p \mid (k-j)a$, or, since $p \nmid a$, we have $p \mid (k-j)$. So $k-j = px$ for some integer x. But we divide by p and see that $(k-j)/p$ is an integer between 0 and 1 again, thus a contradiction.

So $a, 2a, 3a, \ldots, (p-1)a$ is a list of $p-1$ distinct elements from the set $1, 2, 3, \ldots, (p-1)$, thus it must be the list $1, 2, 3, \ldots, (p-1)$, just possibly rearranged. □

Breakout Room Problem (5 minutes)**.** *For $p = 7$, pick an a and show that this theorem really does work. That is, show that $a, 2a, \ldots, (p-1)a$*

Breakout Room Problem (5 minutes)**.** *Fill in the table with the values of $a^m \pmod{m}$. The values of a are in the first column, the values of m are in the first row. Use a value between 0 and $m-1$ (inclusive).*

a\m	*1*	*2*	*3*	*4*	*5*	*6*
2	$2^1 \pmod{1}$	$2^2 \pmod{2}$				
3	$3^1 \pmod{1}$					
4						
5						
6						

Theorem 28 (Theorem 4.3, Fermat's Little Theorem)**.** *Let p be a prime and let a be any number with $a \not\equiv 0 \pmod{p}$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

In other words, this equivalence has LOTS of solutions, it has as many as it possibly could. This is also a somewhat peculiar result. This says, for instance that if you take ANY number that is not a multiple of 5, raise it to the fourth power and subtract one, you get a multiple of 5, every single time.

Note This allows us to simplify calculations another way. If $b_1 \equiv b_2 \pmod{p-1}$ then $a^{b_1} \equiv a^{k(p-1)+b_2} \equiv (a^{p-1})^k \cdot a^{b_2} \equiv a^{b_2} \pmod{p}$. This works even if $a \equiv 0 \pmod{p}$. This also means that it doesn't make sense to look at polynomials modulo p with degree greater than $p-1$, as you can always reduce to a polynomial of at most degree $p-1$.

Proof of Fermat's Little Theorem. Since a is not divisible by p by assumption, we have that the lists

$$a, 2a, \ldots, (p-1)a \pmod{p} \text{ and } 1, 2, \ldots, (p-1) \pmod{p}$$

are the same, and thus

$$a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p},$$

or, after rearranging both sides

$$a^{p-1}((p-1)!) \equiv (p-1)! \pmod{p}$$

Now p does not divide $(p-1)!$, so it can be canceled from both sides, leaving the modulus alone. Thus we have the desired relation $a^{p-1} \equiv 1 \pmod{p}$. □

Fermat's little theorem can be greatly extended to cases where things aren't prime moduli.

Definition. *Given $m \geq 1$, let $\phi(m)$ denote the number of positive integers less than or equal to m that are relatively prime to m.*

Theorem 29 (Theorem 5.3)**.** *Euler's generalized of Fermat's Theorem. If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

The proof of this follows almost identically to the proof of Fermat's little theorem, just that one has to care about only counting things that are reduced residue classes.

Now here is one fact about the phi-function: The question is about what values can $\phi(m)$ take? Well let V be the set of all values $\phi(m)$ can take for some m. Note that $2 \in V$ because $\phi(3) = 2$, but you cannot find an m so that $\phi(m) = 3$, so $3 \notin V$.

Contents

15 Monday, February 15: Applications of the Chinese Remainder Theorem

Section 3.5 of Jones and Jones, An extension of the Chinese Remainder Theorem

Turn in: Exercise 3.14

15.1 Applications of the Chinese Remainder Theorem (55 minutes)

Theorem 30 (Corollary to the Chinese Remainder Theorem)**.** *Let $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e^k}$ be the prime factorization of m. For each element y of the complete residue system $\{0, 1, \ldots, m-1\}$, there exists a system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{p_1^{e_1}} \\ x &\equiv a_2 \pmod{p_2^{e_2}} \\ &\vdots \\ x &\equiv a_k \pmod{p_r^{e_k}} \end{aligned}$$

where y is a solution modulo m. The same is true for any pairwise relatively prime m_i where $m = \prod m_i$.

Solution. There are $p_1^{e_1}$ choices for a_1, $p_2^{e_2}$ choices for a_2, etc, thus there are $p_1^{e_1} p_2^{e_2} \cdots p_k^{e^k}$ such systems of congruences. From the Chinese remainder theorem, there exists a unique solution modulo m. Since the solution to two distinct systems of congruences are incongruent for some mod $p_i^{\alpha_i}$, they are distinct mod m by the contrapositive of Theorem 2.1 part 5. The same proof holds for any pairwise relatively prime m_i where $m = \prod m_i$. □

Theorem 31. *If p is prime, then $ax \equiv 0 \pmod{p}$ implies either $a \equiv 0 \pmod{p}$ or $x \equiv 0 \pmod{p}$. If m is a positive composite integer, then there is a solution to $ax \equiv 0 \pmod{m}$ where both $a \not\equiv 0 \pmod{m}$ and $x \not\equiv 0 \pmod{m}$.*

Proof. Theorem 3.7 says that $ay \equiv 1 \pmod{p}$ has a solution if and only if $\gcd(a, p)$ divides 1. That is, if and only if $\gcd(a, p) = 1$. In this case the solution is unique. This allow us to cancel terms by using $ay \equiv 1 \pmod{p}$.

For p prime, $\{0, 1, \ldots, p-1\}$ is a complete residue class mod p, so either $a \equiv 0 \pmod{p}$ or $\gcd(a, p) = 1$. If $a \equiv 0 \pmod{p}$, then $ax \equiv 0 \pmod{p}$.

If $a \not\equiv 0 \pmod{p}, a$ has a multiplicative inverse $\overline{a}$ mod p for all $1 \leq a \leq p-1$. Returning to our congruence $ax \equiv 0 \pmod{p}$, either $a \equiv 0 \pmod{p}$ or $\overline{a}ax \equiv x \equiv 0 \pmod{p}$.

For the case where m is composite, then there exist integers $1 < a, x < m$ where $m = ax$. Then $ax \equiv 0 \pmod{m}$ but $a \not\equiv 0 \pmod{m}$ and $x \not\equiv 0 \pmod{m}$. □

Example 7. *Let's look at two examples:*

$$\begin{aligned} x^3 + 2x - 3 &\equiv 0 \pmod{5} \\ x^3 + 2x - 3 &\equiv 0 \pmod{4} \end{aligned}$$

One has 0 divisors and the other does not. Both of these are small enough to guess-and-check

Breakout Room Problem (10 minutes)**.** *Find all solutions*

Let's try a technique that is going to generalize a bit better. Although cubics are hard to factor, we can quickly guess-and-check that $x = 1$ *is solution over the integers, so* $x^3 + 2x - 3 = (x - 1)(x^2 + x + 3)$.

(mod 5) *Let's start modulo* 5. *Then* $(x - 1)(x^2 + x + 3) \equiv 0 \pmod 5$ *when either*

$$x - 1 \equiv 0 \pmod 5 \quad \textit{or} \quad x^2 + x + 3 \equiv 0 \pmod 5,$$

since 5 is prime. Then one solution is $x \equiv 1 \pmod 5$, *which is good since* $x = 1 \equiv 1 \pmod m$ *for any integer* m.
We are going to do something a bit funny for the other equivalence. We rewrite

$$\begin{aligned} x^2 + x + 3 &\equiv 0 \pmod 5 \\ x^2 + x + 3 + 2 &\equiv 2 \pmod 5 && \textit{so that we will be able to factor out an } x \\ x^2 + x &\equiv 2 \pmod 5 \\ x(x + 1) &\equiv 2 \pmod 5. \end{aligned}$$

Then we have a slightly faster time checking $1(1 + 1), 2(2 + 1), 3(3 + 1), 4(4 + 1)$. *The only solutions are* $x \equiv 1 \pmod 5$ *(which we already found) and* $x \equiv 3 \pmod 5$.

This allows us to factor (and double check that):

$$\begin{aligned} (x - 1)(x - 1)(x - 3) &\equiv x^3 - 5x^2 + 7x - 3 \\ &\equiv x^3 + 2x - 3 \pmod 5. \end{aligned}$$

(mod 4) *Now we do modulo* 4. *Then* $(x - 1)(x^2 + x + 3) \equiv 0 \pmod 4$ *when*

$$\begin{aligned} &x - 1 \equiv 0 \pmod 4, \quad \textit{or} \quad x^2 + x + 3 \equiv 0 \pmod 4, \\ \textit{or} \quad &x - 1 \equiv x^2 + x + 3 \equiv 2 \pmod 4. \end{aligned}$$

We start with $x - 1 \equiv 0$ (mod *), so* $x \equiv 1 \pmod 4$ *as expected.*
We rewrite

$$\begin{aligned} x^2 + x + 3 &\equiv 0 \pmod 4 \\ x^2 + x + 3 + 1 &\equiv 1 \pmod 4 && \textit{so that we will be able to factor out an } x \\ x^2 + x &\equiv 1 \pmod 5 \\ x(x + 1) &\equiv 1 \pmod 5. \end{aligned}$$

This means that both x *and* $x + 1$ *are odd, so there are no solutions* (mod 4).
Finally, we check $x - 1 \equiv x^2 + x + 3 \equiv 2 \pmod 4$. *The only possible solution to* $x - 1 \equiv 2 \pmod 4$ *is* $x \equiv 3 \pmod 4$, *but* $3^2 + 3 + 3 \equiv 3 \pmod 4$, *so it is not a solution.*

Thus, $x \equiv 1 \pmod 4$ *is the only solution* mod 4.

Example 8. *Solve* $x^3 + 2x - 3 \equiv 0 \pmod{20}$. *It would be tempting to try to factor this, although cubics are hard to factor, but*

$$\begin{aligned} 5 * 4 \equiv 5 * 8 \equiv 5 * 10 \equiv 5 * 16 \equiv 10 * 2 \equiv 10 * 4 \equiv 10 * 6 \equiv 10 * 8 \\ \equiv 10 * 10 \equiv 10 * 12 \equiv 10 * 14 \equiv 10 * 16 \equiv 10 * 18 \equiv 0 \pmod{20}. \end{aligned}$$

($5 * 4k \equiv 10 * 2 \equiv 0 \pmod{25}, k = 1, 2, 3, 4, j = 1, 2, 3, \ldots, 9$ *for 13 total options). Checking each option is going to be really time consuming.*

16 Wednesday: Order of elements $\mathbb{Z}_p$, quadratic polynomials mod n, polynomials mod p.

Reading: None.

Turn in: Look at the chart of $a^n \pmod{11}$. The first column is 1^n, the second column is 2^n, etc. That is, the top of the column is the base, the left gives the exponent, all are reduced mod 11.

1. For each $a \in \mathbb{Z}_{11}$, what is the smallest n such that $a^n = 1$ (ie, what is the smallest n such that $a^n \equiv 1 \pmod{11}$?
2. What patterns do you notice?

a^1	1	2	3	4	5	6	7	8	9	10
a^2	1	4	9	5	3	3	5	9	4	1
a^3	1	8	5	9	4	7	2	6	3	10
a^4	1	5	4	3	9	9	3	4	5	1
a^5	1	10	1	1	1	10	10	10	1	10
a^6	1	9	3	4	5	5	4	3	9	1
a^7	1	7	9	5	3	8	6	2	4	10
a^8	1	3	5	9	4	4	9	5	3	1
a^9	1	6	4	3	9	2	7	7	5	10
a^{10}	1	1	1	1	1	1	1	1	1	1
a^{11}	1	2	3	4	5	6	7	8	9	10

Solution. Posted after class □

16.1 Announcements (5 minutes)

Project 2 description is up. This one is to be turned in on Carmen. If you are doing something that involves video or audio editing, keep in mind it will probably take longer than you expect! Carmen has very low storage limits, so you will probably need to link to BuckeyeBox, OneDrive, or Google Drive (or YouTube).

There are a few videos on the Chinese remainder theorem linked on the class playlist. You can access this playlist from the main course page or Modules. The link says "Video examples from the book," although these are not from the book.

Reminder that your homework feedback is on Gradescope. I also added the Gradescope guide for students to the playlist. Revising and resubmitting is an opportunity for you to learn from the feedback and improve your grade. You only need to submit the problems which you would like regraded.

16.2 Roots of a cubic (20 minutes)

Example 9. *Solve* $x^3 + 2x - 3 \equiv 0 \pmod{20}$. *It would be tempting to try to factor this, although cubics are hard to factor, but*

$$\begin{aligned} 5*4 &\equiv 5*8 \equiv 5*10 \equiv 5*16 \equiv 10*2 \equiv 10*4 \equiv 10*6 \equiv 10*8 \\ &\equiv 10*10 \equiv 10*12 \equiv 10*14 \equiv 10*16 \equiv 10*18 \equiv 0 \pmod{20}. \end{aligned}$$

($5*4k \equiv 10*2 \equiv 0 \pmod{25}, k = 1,2,3,4, j = 1,2,3,\ldots,9$ *for 13 total options). Checking each option is going to be really time consuming. Let's reduce the modulus to reduce this list.*

Breakout Room Problem (5 minutes)**.** *If* $d \mid m, d > 0$*, and* u *is a solution to* $f(x) \equiv 0 \pmod{m}$*, then* u *is a solution to* $f(x) \equiv 0 \pmod{d}$*.*

Solution. From the definition of a solution $f(x) \equiv 0 \pmod{m}$, $f(u) \equiv 0 \pmod{m}$. Then from Lemma 3.3, we have that $f(u) \equiv 0 \pmod{d}$, meaning u is a solution to $f(x) \equiv 0 \pmod{d}$. □

One way to try to find solutions to congruences is to reduce the modulus. However, we do have a powerful tool from the contrapositive. If $d \mid m, d > 0$ and u is not a solution to $f(x) \equiv 0 \pmod{d}$, then u is not a solution to $f(x) \equiv 0 \pmod{m}$. This means that we can make a list of possible solutions to $f(x) \equiv 0 \pmod{m}$.

Returning to $x^3+2x-3 \equiv 0 \pmod{20}$, we already found that the possible solutions are $x \equiv 1 \pmod{5}, x \equiv 3 \pmod{5}$, and $x \equiv 1 \pmod{4}$. In fact, we need a solution that works both modulo 5 and modulo 4. Then we are looking for a solution to the system of congruences $x \equiv 1 \pmod{5}$ and $x \equiv 1 \pmod{4}$ and a solution to the congruence $x \equiv 3 \pmod{5}$, and $x \equiv 1 \pmod{4}$.

Case $x \equiv 1 \pmod{5}$: *By the Chinese remainder theorem, there is a unique solution modulo 20. We have that $a_1 = 1, M_1 = 4$, and $x_1 * 4 \equiv 1 \pmod{5}$, so $x_1 \equiv 4 \pmod{5}$. Notice that we can find this using the Euclidean algorithm:*

$$5 = 4 + 1, \quad 5 - 4 = 1,$$

so -1 is the multiplicative inverse of $4 \mod 5$. It is easier to do arithmetic with -1 that 4, so we will use that representative of the congruence class.

We also have that $a_2 = 1, M_2 = 5$, and $x_2 * 5 \equiv x_2 \equiv 1 \pmod{4}$, so $x_2 \equiv 1 \pmod{4}$.

This solution is $1 * 4 * (-1) + 1 * 5 * 1 \equiv 1 \pmod{20}$.

Case $x \equiv 3 \pmod{5}$: *By the Chinese remainder theorem, there is a unique solution modulo 20. $a_1 = 3, M_1 = 4$, and $x_1 * 4 \equiv 1 \pmod{5}$, so $x_1 \equiv -1 \pmod{5}$, and $a_2 = 1, M_2 = 5, x_2 = 1$ as before. This solution is $3 * 4 * (-1) + 1 * 5 * 1 \equiv 13 \pmod{20}$.*

Now we check: $1^2+2*1-3 \equiv 0 \pmod{20}$ (again, we expect this since $x = 1$ is a solution to the equation $x^2+2x-3 = 0$), and $13^2 + 2 * 13 - 3 \equiv 0 \pmod{20}$.

16.3 Order of elements $\mathbb{Z}_p$ (30 minutes)

Poll question. *For each $a \in \mathbb{Z}_{11}$, what are all of the values of n where $a^n \equiv 1 \pmod{11}$?*

Solution. 1,2,5 or 10. □

Breakout Room Problem (5 minutes)**.** *Make a similar chart for $\mathbb{Z}_3$ and $\mathbb{Z}_4$. What patterns do you notice?*

Solution.

a^1	1	2
a^2	1	1
a^3	1	2

a^1	1	2	3
a^2	1	0	1
a^3	1	0	3
a^4	1	0	1

□

Definition. *Let $a \in \mathbb{Z}_n$ be a reduced residue (ie, $\gcd(a, n) = 1$). The* order *of a in $\mathbb{Z}_n$ is the smallest positive integer r such that $a^r \equiv 1 \pmod{n}$. Our textbook just gives the order a name (often k) when it is notationally useful, but the standard notation is $\text{ord}_n(a)$.*

From the previous exercise, what can you guess about $\text{ord}_n(a)$?

17 Friday: Polynomials mod p.

Reading: Scanned notes, Section 10.2 of *Number Theory: A Lively Introduction with Proofs, Applications, and Stories* by Pommershiem, Marks, and Flapan.

Turn in: How many incongruent solutions are there to $x^2 \equiv 1 \pmod 8$? Why does this not violate Theorem 10.2.1 in the reading? What part of the proof of Theorem 10.2.1 no longer holds?

17.1 Finishing order of elements (20 minutes)

Breakout Room Problem (5 minutes). *Let $n \in \mathbb{Z}, n > 0, a \in \mathbb{Z}_n$ where $\gcd(a, n) = 1$, and $r = \operatorname{ord}_n(a)$. For an integer e, $a^e \equiv 1 \pmod n$ (or $a^e = 1$ in $\mathbb{Z}_n$) if and only if $r \mid e$.*

Proof. ($\Leftarrow$) Assume $r \mid e$. Then there exists an integer k where $e = rk$. By exponent rules,

$$a^e \equiv a^{rk} \equiv (a^r)^k \equiv 1^k \equiv 1 \pmod n.$$

($\Rightarrow$) (*Proof by contradiction*) Assume $a^e \equiv 1 \pmod n$. To get a contradiction, assume that $r \nmid e$. By the division algorithm, there exist q, b where $e = rq + b$ and $0 < b < r$. By assumption, we have $1 \equiv a^e \equiv a^{rq+b} \equiv a^{rq}a^b \equiv a^b \pmod n$. By assumption, r is the smallest positive integer where $a^r \equiv 1 \pmod n$, we have a contradiction. Thus, $r \mid e$.

(*Direct proof*) Assume $a^e \equiv 1 \pmod n$. Then by the division algorithm, there exist q, b where $e = rq+b$ and $0 \leq b < r$. By assumption, we have $1 \equiv a^e \equiv a^{rq+b} \equiv a^{rq}a^b \equiv a^b \pmod n$. By assumption, r is the smallest positive integer where $a^r \equiv 1 \pmod n$, we have that $b = 0$. Thus, $r \mid e$. □

Theorem 32. *Let p be prime and $a \in \mathbb{Z}_p, a \neq 0$. Then $\operatorname{ord}_p(a) \mid p - 1$.*

Proof. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod p$. Then from the previous theorem, $\operatorname{ord}_p(a) \mid p - 1$. □

Let's return to the pattern in the exponent table: that the even exponent rows are symmetric mod 11. It turns out that this is true for all mods, not just prime. We need to translate this into a math statement that we can prove:

Theorem 33. *For positive integers m and k and any integer a, $a^{2k} \equiv (m - a)^{2k} \pmod m$.*

Proof. First we note that $-a \equiv m - a \pmod m$ for any integer a and positive integer n. By repeated applications of modular multiplication (or induction), we have seen that $(-a)^n \equiv (m - a)^n \pmod m$ for any nonnegative integer n. Then $(m - a)^{2k} \equiv (-a)^{2k} \equiv (-1)^{2k}a^{2k} \equiv a^{2k} \pmod m$. □

We will finish the discussion of order of an element (for now).

Theorem 34. *Let $a, m \in \mathbb{Z}, m > 0$, and $(a, m) = 1$. Then for any positive integer k, $\operatorname{ord}_m(a^k) = \dfrac{\operatorname{ord}_m(a)}{(k, \operatorname{ord}_m(a))}$.*

Proof. From the breakout room problem, $(a^k)^{\operatorname{ord}_m(a^k)} \equiv 1 \pmod m$ if and only if $\operatorname{ord}_m(a) \mid k \operatorname{ord}_m(a^k)$. We also have that this is true if and only if $\frac{\operatorname{ord}(a)}{(k,\operatorname{ord}(a))} \mid \frac{k}{(k,\operatorname{ord}(a))} \operatorname{ord}(a^k)$. Now we have that $\left(\frac{\operatorname{ord}(a)}{(k,\operatorname{ord}(a))}, \frac{k}{(k,\operatorname{ord}(a))}\right) = 1$, so $\frac{\operatorname{ord}(a)}{(k,\operatorname{ord}(a))} \mid \operatorname{ord}(a^k)$. Thus, the smallest integer where this is true is $\frac{\operatorname{ord}(a)}{(k,\operatorname{ord}(a))}$. □

Alternate proof with names for $\operatorname{ord}_m(a)$ and $\operatorname{ord}_m(a^k)$:

Proof. Let $\operatorname{ord}_m(a) = h$ and $\operatorname{ord}_m(a^k) = j$. From the breakout room problem, $(a^k)^j \equiv 1 \pmod{m}$ if and only if $h \mid kj$. We also have that this is true if and only if $\frac{h}{(k,h)} \mid \frac{k}{(k,h)} j$. Now we have that $\left(\frac{h}{(k,h)}, \frac{k}{(k,h)}\right) = 1$, so $\frac{h}{(k,h)} \mid j$). Thus, the smallest integer j where $(a^k)^j \equiv 1 \pmod{m}$ is $\frac{h}{(k,h)}$. □

17.2 Quadratic polynomials mod n (30 minutes)

Let's take a minute go back to the integers. For integers a, b and c, we have a formula for when $ax^2 + bx + c = 0$. We are going to start with this familiar case.

Theorem 35. *Let $a, b, c \in \mathbb{Z}$ where $a \neq 0$. Consider the polynomial equation*

$$ax^2 + bx + c = 0. \tag{★}$$

Let $d = b^2 - 4ac$.

1. *If there exists $s \in \mathbb{Z}$ such that $s^2 = d$, then the rational solutions to ★ are*

$$x = (-b + s)(2a)^{-1} \quad \text{and} \quad x = (-b - s)(2a)^{-1}.$$

   If $2a \mid -b - s$ or $2a \mid -b + s$, there are integer solutions.

2. *If no such s exists, there is no rational solution. If $d < 0$, no real solution exists.*

Proof. We are going to derive the quadratic formula. Since we have an idea of where we are going, we start with multiplying through by $4a$.

$$\begin{aligned} 4a^2x^2 + 4abc + 4ac &= 0 && (1)\\ 4a^2x^x + 4abx &= -4ac && (2)\\ 4a^2x + 4abx + b^2 &= b^2 - 4ac && (3)\\ (2ax + b)^2 &= d && (4)\\ 2ax + b &= \pm\sqrt{d} && (5)\\ x &= \frac{-b \pm \sqrt{d}}{2a}. && (6) \end{aligned}$$

Thus, if there exists an integer s where $s^2 = d$, x is rational. Otherwise, there are no rational solutions, and if $d < 0$ there are no real solutions. □

Poll question. *Which steps might not work for modular arithmetic. Think to yourself, this is a quick gut-check.*

Solution. Step 5 does not always exist in the integers (or real numbers), and this is also true mod p. Step 6 also might not work. □

For modular arithmetic, we do not have square roots and may not have multiplicative inverses. We may also have zero divisors. We can avoid some of these problems by working modulo a prime.

Theorem 36. *Let $p > 2$ be prime, and $a, b, c \in \mathbb{Z}_p$ where $a \not\equiv 0$. Consider the polynomial congruence*

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{★★}$$

Let $d \in \mathbb{Z}_p$ where $d \equiv b^2 - 4ac \pmod{p}$.

1. *If there exists $s \in \mathbb{Z}_p$ such that $s^2 = d$ (ie, $s^2 \equiv d \pmod{p}$), then the rational solutions to ★★ are*

$$x \equiv (-b+s)(2a)^{-1} \pmod{p} \quad \text{and} \quad x \equiv (-b-s)(2a)^{-1} \pmod{p},$$

where $(2a)^{-1}$ denotes the multiplicative inverse of $2a \pmod{p}$.

2. *If no such s exists, there is no solution in $\mathbb{Z}_p$.*

Proof. Homework 6, Problem 7 □

Breakout Room Problem (3 minute, group of 3)**.** *Why do we need $p > 2$? How many different quadratic polynomials are there mod 2? What are their roots?*

Solution. $2a \equiv 0 \pmod{2}$ for every integer a.

There are four polynomials: x^2+x+1 with no roots, x^2+x with roots $0, 1$, x^2+1 with root 1, and x^2 with root 0. □

Contents

18 Monday, February 22: Congruences with a Prime-power Modulus

Reading: Section 4.1 of Jones and Jones. Note that we have now covered a lot of this material in the readings from Pommersheim, Marks, and Flapan.

Turn in: Exercise 4.2.

18.1 Quadratic polynomials mod n (15 minutes)

Breakout Room Problem (10 minutes, check in, potentially additional 5 minutes)**.** *Prove the $\mathbb{Z}_p$ version of the quadratic formula.*

Let $p > 2$ be prime, and $a, b, c \in \mathbb{Z}_p$ where $a \not\equiv 0$. Consider the polynomial congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}. \qquad (★★)$$

Let $d \in \mathbb{Z}_p$ where $d \equiv b^2 - 4ac \pmod{p}$.

1. *If there exists $s \in \mathbb{Z}_p$ such that $s^2 = d$ (ie, $s^2 \equiv d \pmod{p}$), then the rational solutions to ★★ are*

$$x \equiv (-b+s)(2a)^{-1} \pmod{p} \quad \text{and} \quad x \equiv (-b-s)(2a)^{-1} \pmod{p},$$

where $(2a)^{-1}$ denotes the multiplicative inverse of $2a \pmod{p}$.

2. *If no such s exists, there is no solution in $\mathbb{Z}_p$.*

What happens for composite modulus?

Chat blast. *Which steps might not work for composite modulus?*

Solution. Multiplicative inverses may not exist. □

There may not be a multiplicative inverse. On the reading, we saw that $x^2 \equiv 1 \pmod{8}$ has four incongruent solutions. From the very end of Section 2.3, we have that we can break composite cases into prime power moduli (like mod 8).

18.2 The arithmetic of $\mathbb{Z}_p$ (30 minutes)

Definition. *Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdot + a_1x + a_0$. The degree of the polynomial mod m is the largest integer j such that $a_j \not\equiv 0 \pmod{m}$. If all of the $a_i \equiv 0 \pmod{m}$., then the degree is 0.*

The degree of the polynomial mod m is not the same as the degree of the polynomial over $\mathbb{Z}$. For example, $f(x) = 6x^3 + 3x^2 + 1$ has degree 3 over the integers and mod 5, but degree 2 mod 6 and mod 2.

Theorem 37 (Theorem 4.1, Lagrange)**.** *Let p be a prime number and let*

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

be a polynomial of degree $n \geq 0$ with integral coefficients where $p \nmid a_n$. Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n incongruent solutions mod p (in other words, at most n solutions in $\mathbb{Z}_p$).

Proof. We are going to use induction on the degree n. If $n = 0$, then $f(x) \equiv a_0 \equiv 0 \pmod{p}$ has no (ie, 0) solutions since we assumed $p \nmid a_0$. For $n = 1$, we have that $f(x) = a_1x + a_0$ where $p \nmid a_1$. Since p is prime, this guarantees $(a_1, p) = 1$ and $a_1x \equiv -a_0 \pmod{p}$ has exactly one incongruent solution by Theorem 3.7, so the theorem holds for $n = 1$.

Next, we induct. Assume that the theorem is true for all $n = k \geq 1$. Then we need to show that the theorem is true for $n = k+1$. Let $f(x) = a_{k+1}x^{k+1} + a_kx^k + \cdots a_1x + a_0$ where $p \nmid a_{k+1}$. If there are no solutions to $f(x) \equiv 0 \pmod{n}$, then the theorem is true and we are done.

If $f(x) \equiv 0 \pmod{p}$ has at least one solution a_1, then we can factor out $x - a_1$. However, proving this is difficult, and we need to show that modulo a prime is enough to say we have reduced the degree. We are going to use a different method.

Let's relate this to the proof we have already seen: assume there are $k + 2$ distinct roots mod p, and call them $d_1, d_2, \ldots, d_{k+2}$. Then we define $h(x) = f(x) - a^{k+1}(x - d_1)(x - d_2) \cdots (x - d_{k+1})$. Then $h(x)$ has at least $k+1$ distinct roots mod p.

Case1: If every coefficient of $h(x)$ is $0 \pmod{p}$, then $h(x) \equiv 0 \pmod{p}$ for all integers x. Then $f(d_{k+2}) \equiv 0 \pmod{p}$ and $h(d_{k+2}) \equiv 0 \pmod{p}$ implies d_{k+2} is a root of $a^{k+1}(x - d_1)(x - d_2) \cdots (x - d_{k+1})$ mod p. But this is a contradiction, since none of the factors are 0 and p is prime.

Case 2: $h(x)$ is not identically 0. Then $h(x)$ has degree less $n = k + 1$ mod p. By induction hypothesis, $h(x)$ has at more k roots, so $f(x)$ has at more k roots. □

Breakout Room Problem (Exercise 4.1, 5 minutes)**.** *Find the roots of the polynomial $f(x) = x^2 + 1$ in $\mathbb{Z}_p$ for each prime $p \leq 17$. Make a conjecture about how many roots $f(x)$ has in $\mathbb{Z}_p$ for each prime p.*

Example 10 (Example 4.1)**.** *Let us find the least nonnegative residue of $2^{68} \pmod{19}$.*

Sice $p = 19$ is prime and $19 \nmid 2$, Fermat's Little Theorem $2^{18} \equiv 1 \pmod{19}$, and $68 = 18 * 3 + 14$, so

$$2^{68} \equiv (2^{18})^3 2^{14} \equiv 2^{14} \pmod{19}$$

Here we can use a method called repeated squaring. Since $2^4 \equiv 16 \equiv -3 \pmod{19}$,

$$2^{12} \equiv (-3)^3 \equiv -27 \equiv -8 \pmod{19}.$$

We get that

$$2^{68} \equiv 2^{14} \equiv -8 * 2^2 \equiv 6 \pmod{19}$$

Breakout Room Problem (5 minutes)**.** *Let us find the least nonnegative residue of* $6^{4162} \pmod{41}$.

$$64162 \equiv 6^{4000+160+2} \equiv 6^{4000}6^{160}6^2 \equiv (6^{40})^{10}(6^{40})^4 6^2 \equiv 1^{10}1^4 36 \equiv 36 \pmod{41}$$

Theorem 38 (Theorem 4.6)**.** *Let p be an odd prime. Then the quadratic congruence $x^2+1 \equiv 0 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*

Proof. Suppose p is an odd prime, and let $k = \frac{p-1}{2}$. Consider the product

$$(p-1)! = 1 * 2 * \cdots * k * (k+1) * \cdots * (p-2)(p-1).$$

Note that $p-1 \equiv -1 \pmod{p}, p-2 \equiv -2 \pmod{p}, \ldots, k+1 = p-k \equiv -k \pmod{p}$. Then

$$(p-1)! \equiv k!(-1)^k(k!) \pmod{p}.$$

□

19 Friday, February 26: Primality testing

Turn in:

1. Reflect on how the article on classroom mindset relates to this course. This could be the course content, the course structure, mathematics classes in general, college in general...However you see the article relating to our course.
2. What is the most confusing thing we have learned so far?
3. Is there anything we have learned so far that surprised you?
4. What was a problem or concept that you really struggled with, but now understand?
5. What is something that you have done this semester that makes you feel like a mathematician? It does not have to be limited to this course.

19.1 Updates and reminders (15 minutes)

A few things that I've talked about in office hours but want to make sure the whole class hears. Sometimes it can be better to use share the framing or phrasing your classmates use, as it's probably a bit closer to how you think about things.

On Gradescope, if there is not anything in the "score" section, then the problem was not assigned a score. Normally, I catch this on the first submission, and I will work to be better on the resubmits. If you do not have a score, you can use the regrade request or email me.

For the resubmissions, I grade it as an entirely new assignment. The only difference is at the end, I open the excel file and update scores. If a problem is graded as one problem the first time, it will be graded as one problem the second time. Sometimes, if you have a difficult to read submission or confusing wording, it can be challenging to see where feedback is necessary. The proofs and justifications in this course are more complicated and nuanced that in non-proofs courses, and it can be hard to see exactly where the confusion is. When I submit papers, sometimes I get back referee reports that says I didn't explain something, or completely misunderstands what I was trying to say. I try to take a bit, and then see how the phrasing what unclear.

Someone also suggested thinking about explaining your reasoning as the grader has not read the section. This could be a useful framing for some of you. I had been avoiding similar phrasing since it was resulting in 2-3 page answers last semester, but if that helps, use it.

There was also a good office hours question about how to go about solving problems and proofs. Even if the problem is not in the "modifying proofs" section, the proofs of theorems from class or the book can be very useful outlines or have useful tricks. There are also answers in the back of the book for the exercises that come from the book. Now, you should not be copying the solutions word for word, but in the process of trying to rephrase things, you are going to need to understand what is happening.

19.2 Finishing polynomial roots (30 minutes)

Breakout Room Problem (Exercise 4.1, 5 minutes)**.** *Find the roots of the polynomial $f(x) = x^2 + 1$ in $\mathbb{Z}_p$ for each prime $p \leq 17$. Make a conjecture about how many roots $f(x)$ has in $\mathbb{Z}_p$ for each prime p.*

Solution. From Theorem 4.1, we know that there are at most 2 roots for each modulus. Since we have not yet proven Homework 6 problem 5, then best approach is guess-and-check brute force.

For $p = 2, x \equiv 1 \pmod 2$.

For $p = 5, x \equiv 2 \pmod 5$ and $x \equiv -2 \equiv 3 \pmod 5$.

For $p = 13, x \equiv 5 \pmod{13}$ and $x \equiv -5 \equiv 8 \pmod{13}$.

For $p = 17, x \equiv 4 \pmod{17}$ and $x \equiv -4 \equiv 13 \pmod{17}$.

For $p = 3, 7, 11$, there are no solutions. This can be seen through a guess and check brute force. □

This brings us to the next theorem:

Theorem 39 (Theorem 4.6)**.** *Let p be an odd prime. Then the quadratic congruence $x^2+1 \equiv 0 \pmod p$ has a solution if and only if $p \equiv 1 \pmod 4$.*

Proof. Suppose p is an odd prime, and let $k = \frac{p-1}{2}$. Consider the product

$$(p-1)! = 1 * 2 * \cdots * k * (k+1) * \cdots * (p-2)(p-1).$$

Note that $p - 1 \equiv -1 \pmod p, p - 2 \equiv -2 \pmod p, \ldots, p - k \equiv -k \pmod p$, and $p - k = \frac{2p-p+1}{2} = \frac{p-1+2}{2} = k + 1$. Then

$$-1 \equiv (p-1)! \equiv k!(-1)^k(k!) \pmod p.$$

If $x = k!$, then $(-1)^k x^2 + 1 \equiv 0 \pmod p$, by rewriting the convergence. When k is even, this is the congruence $x^2 + 1 \equiv 0 \pmod p$. We also know that when k is even, there exists some m such that $2m = k = \frac{p-1}{2}$. Thus, $p = 4m + 1$. Therefore, we have found a solution to $x^2 + 1 \equiv 0 \pmod p$ when $p \equiv 1 \pmod 4$.

Now we must check that there is not some other solution with $p \equiv 3 \pmod 4$. Now, in both cases, we know that Fermat's Little Theorem (Theorem 4.3) says that $x^{p-1} \equiv x^{2k} \equiv 1 \pmod p$. In the case that $p \equiv 3 \pmod 4$, we know that $k = \frac{p-1}{2}$ is odd. By rewriting $(-1)^k x^2 + 1 \equiv 0 \pmod p$, we see that $1 \equiv x^2 \mod p$. Thus, $x^{2k} \equiv 1^k \pmod p$, which contradicts Fermat's Little Theorem. Thus, so solutions exist. □

19.3 Primality Testing (10 minutes)

We have seen a lot of places where it is useful to have prime numbers. We need to be able to determine if a number is prime or composite. Factoring is slow, so we would like a better algorithm.

Definition. *If $a^{n-1} \not\equiv 1 \pmod n$, we know that n is composite. In this case, we say that a is a* Fermat witness to the compositeness of n.

Breakout Room Problem (3 minutes)**.** *Is there a Fermat witness to the compositeness of 4?*

Solution. $2^3 \equiv 0 \pmod 4$ is a witness. $3^3 \equiv 3 \pmod 4$. □

Contents

20 Monday, March 1: Primality testing and Carmichael Numbers

20.1 Primality Testing (10 minutes)

We have seen a lot of places where it is useful to have prime numbers. We need to be able to determine if a number is prime or composite. Factoring is slow, so we would like a better algorithm.

Definition. *If* $a^{n-1} \not\equiv 1 \pmod{n}$*, we know that* n *is composite. In this case, we say that* a *is a* Fermat witness to the compositeness of n.

Chat blast. *Using this test,* $2^{340} \equiv 1 \pmod{341}$*. What can we conclude?*

Solution. That 2 is not a Fermat witness for 341. However, $341 = 11 * 31$, so it is composite. □

Breakout Room Problem (5 minutes)**.** *A* nontrivial *factor of a number* n *is a factor that is not equal to* ± 1 *or* $\pm n$*. It is nontrivial because all numbers* n *have* ± 1 *and* $\pm n$ *as factors. Are all* nontrivial *factors of positive composite integers* n *Fermat witnesses to the compositeness of* n*? Prove or provide counterexample.*

Solution. □

20.2 Carmichael Numbers (25 minutes)

Definition. *A* Carmichael number *is a composite integer where for every integer* a *where* $\gcd(a, n) = 1$ *implies* $a^{n-1} \equiv 1 \pmod{n}$.

The smallest Carmichael number is $561 = 3 * 11 * 17$. There are only 43 Carmichael numbers less than 1 million, but Alford, Granville, and Pomerance proved that there are infinitely many in 1994.

Theorem 40. *Let* n *be a positive composite integer. Then* n *is a Carmichael number if and only if*

1. *For every prime* p *such that* $p \mid n$*, we have* $p - 1 \mid n - 1$.
2. n *is the product of distinct primes (ie,* n *is* square free *meaning no prime is raised to a power higher than 1).*

Proof. ($\Leftarrow$) Let n be composite and assume (1) and (2) are true. Then $n = p_1 p_2 \dots p_s$ where the p_j are distinct and $p_j - 1 \mid n - 1$.

In order to show that n is a Carmichael number, we need to show that $a^{n-1} \equiv 1 \pmod{n}$ for every integer a where $(a, n) = 1$. If $\gcd(a, n) = 1$, then $a^{p_j - 1} \equiv 1 \pmod{p_j}$ by Fermat's Little Theorem. Since $p_j - 1 \mid n - 1$, there exists a positive integer k_j such that $(p_j - 1)k_j = n - 1$. Thus, $a^{n-1} \equiv a^{(p_j-1)k_j} \equiv 1 \equiv 1^{k_j} \equiv 1 \equiv \pmod{p_j}$. Thus, we have a system of congruences

$$\begin{aligned} x = a^{n-1} &\equiv 1 \pmod{p_1} \\ x = a^{n-1} &\equiv 1 \pmod{p_2} \\ &\vdots \\ x = a^{n-1} &\equiv 1 \pmod{p_s}. \end{aligned}$$

By the Chinese remainder theorem, there exists a unique solution to this system of congruences modulo n, we want to show that the solution is $1 \pmod{n}$. There is a one-to-one correspondence between systems of congruences modulo $p_1, p_2, \dots, p_s$ and possible solutions modulo n. By the corollary to the Chinese remainder theorem, there is a unique system of congruences modulo $p_1, p_2, \ldots, p_s$ with solution $x \equiv 1 \pmod{n}$. By Theorem 2.1 part 4, since each $p_j \mid n$, if $x \equiv 1 \pmod{n}$, then $x \equiv 1 \pmod{p_j}$. Thus, $x = a^{n-1} \equiv 1 \pmod{n}$.

($\Rightarrow$) This is much harder. More primality testing and proving this theorem is a possible optional topic. □

We have a related test:

Theorem 41. *Let n be a positive integer. If an integer a exists such that $a^{n-1} \equiv 1 \pmod{n}$ and $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all prime divisors q of $n-1$, then n is prime.*

Proof. Since $a^{n-1} \equiv 1 \pmod{n}$, we have that $\operatorname{ord}_n(a) \mid n-1$, so there exists positive integer k such that $n - 1 = k \operatorname{ord}_n(1)$. We want to show that $k = 1$. In order to get a contradiction, assume that $\operatorname{ord}_n(1) \neq n-1$, so $k > 1$. Let q be a prime divisor of k, and thus $n-1$. Thus,

$$a^{(n-1)/q} = a^{k(\operatorname{ord}_n(a))/q} = (a^{\operatorname{ord}_n(a)})^{k/q} \equiv 1 \pmod{n}.$$

This is a contradiction. Now, $\operatorname{ord}_n(a) \leq \phi(n) \leq n-1$. Since $\operatorname{ord}_n(a) = n-1$, we have that $\phi(n) = n-1$ and thus n is prime. □

21 Wednesday, March 3: Primality testing

A code is a system that substitutes prescribed sets of characters for other sets of characters. To encode a message is to replace its elements by a different combination of characters or figures. A cipher is a system where individual letters are replaced by other letters, either individually or in blocks. One famous example is the cipher Julius Caesar used to send letters to his army. He would take each letter and replace it with the one three places later in the alphabet. Here we say that the original message is the plaintext, the message that gets passed to the troops is the "ciphertext," and the key is $k = 3$, since you shift forward 3 letters in the alphabet. We can translate this to modular arithmetic with the following chart:

a	b	c	d	e	f	g	h	i	j	k	l	m
1	2	3	4	5	6	7	8	9	10	11	12	13

n	o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25	26

Then the Caesar shift translates to adding 3 mod 26. We call this an *additive cipher* when we use $x + k$ to encrypt x with key k. You can also use multiplication to define a *multiplicative cipher* when we use xk to encrypt to encrypt x with key k.

Turn in: Keep in mind that a cipher must be able to be encrypted and decrypted. It is not useful to use a cipher were a and b both get encrypted as c, since we would not know how to decrypt c.

1. How many additive ciphers are there mod 26?
2. How many multiplicative ciphers are there mod 26? (*Hint:* this is not the same as your previous answer)
3. What equivalence classes do not work as multiplicative ciphers mod 26? Why?

21.1 Computational Complexity of Factoring (50 minutes)

The day was spent on the following problems from Homework 8. More details on their solutions on the Zoom recording

`https://osu.zoom.us/rec/share/E1e9ROE9n7qqX6i3YsQPLrmo9CJ9i9UUMM8aOOlZ-8GMbFrms7bdCjY8R4oTGQZV.8JbC7d4O9bTi`

Breakout Room Problem (Rest of class). 1. *Let n be a positive integer, and suppose x and y are integers such that $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$. Prove that $d = \gcd(x-y, n)$ and $e = \gcd(x+y, n)$ are factors of n that are not equal to ± 1 or $\pm n$.*

2. *We are going to use problem 1 to explore how finding the order of an integer modulo n is at least as computationally complex as factoring.*
   (a) *Suppose you wish to factor* 713*. Use that* 3 *has order* 330 *modulo* 713*,* $330 = 2(165)$*, and* $3^{165} \equiv 185 \pmod{713}$*. Let* $x = 185$*. How do you know that* $x^2 \equiv 1 \pmod{713}$*? Use the previous problem to find a factor of n using the Euclidean algorithm to find the greatest common divisor.*

   (b) *Suppose a is an integer where* $(a, n) = 1$ *and* $\operatorname{ord}_n(a) = r$*. Assume that r is even, and let* $x = a^{r/2}$*. Show that* $x^2 \equiv 1 \pmod{n}$*, but* $x \not\equiv 1 \pmod{n}$*.*

   (c) *Now assume that x in the previous problem is not equivalent to* -1 *modulo n. How does this help find a factor of n?*

22 Friday, March 5: Practice with additive ciphers, Diffie-Hellman, and RSA

No reading, Projects due.

22.1 Creating algorithms with something other than numbers (25 minutes)

Definition. *The* Euler ϕ function $\phi(n)$ *gives the number of relatively prime positive integers less that n.*

Breakout Room Problem (1 minute)**.** *Why can we conclude n is prime when* $\phi(n) = n - 1$*?*

Solution. For all integers n, there are $n - 1$ positive integers less than n. Thus, $\phi(n) \leq n - 1$. If the exists some other factor of n, then it is not relatively prime to n, and thus $\phi(n) \leq n - 2$. □

In the reading for Wednesdays assignment, we saw some basics of encrypting secret messages: translate the alphabet into the integers 1-26, pick an encryption scheme and an encryption key. With the Caesar shift, we add 3. We can actually avoid the modular arithmetic by using this decoder wheel.

The word DOG becomes GRJ, and we can undo this by applying -3. There are many problems with this encryption scheme, including that it's not hard for a computer to check all 25 additive schemes, or really even all 26! possible schemes that send one letter of the English alphabet to another. However, for any encryption scheme, there is an issue of communicating sharing both the encryption rules and the key. If you know how to encrypt a message, then in theory you know how to decrypt it. We need to come up with a way to share keys and rules that does not give away how to decrypt the message.

We are going to do a thought experiment.

Breakout Room Problem (15 minutes)**.** *Alice wants to buy something from Bob. She has to put her credit card into his website, so she wants to make sure it is encrypted. They have some sort of magical encryption device where they can use the content of these envelopes to encrypt and decrypt her credit card number, but only if the content of both envelopes is identical. The eavesdroppers (Eve) cannot see the content of the envelopes when they are closed, or when Alice or Bob are putting pieces in, but she can see inside if either Alice or Bob looks. Also, anyone holding the envelope can magically duplicate the contents and use it for encryption and decryption...*

The tricky part is for Alice and Bob to obtain identical envelopes to begin with, without anyone else obtaining copies of those envelopes or guessing their contents (knowledge of the contents would allow someone else to create an identical envelope thus defeating the purpose of encrypting the message.)

Now, we are going to try an online version of this, but instead of the colorful squares I used last year, we will use shapes on the slide. (Go over how to draw on Jamboard) `https://jamboard.google.com/d/1HOkyHuasytbRryUBVbnD8E8qW8jV-InmCo` `edit?usp=sharing`

Alice wants to buy something from Bob and wants to make sure her credit card information is encrypted. They have a magic encryption device that uses the number of circles, triangles squares, diamonds, etc on the ”Alice” slide to encrypt this information, and the same information on the ”Bob” slide to decrypt.

In order to work correctly, the information on both slides must match. Alice and Bob cannot see what the other person input (although you can, you need to pretend you cannot). Alice puts information on her slide, sends it to Bob and waits for him to send back his slide. Bob puts information on his slide, and sends it to Alice. At this point, anyone else in the group can duplicate the slides (again, pretend that you cannot see the contents, but could copy/paste without reading it).

How can Alice and Bob guarantee the slides have the same information without communicating or letting the other people in the other group know what is on the slides?

The first person alphabetically is Alice, second is Bob. If someone is having technical difficulties accessing the slides, go to the next person alphabetically.

Find your breakout room number, probably at the top of your Zoom Window.

Alice puts some number of circles, triangles, etc on the slide labeled ”Alice Breakout Room [your room number]” and Bob puts some number on ”Bob Breakout Room [your room number]” .

Before exchanging slides, determine the next step as a group:

BEFORE looking at the other person’s slides and without telling anyone what you put on the slides, make a plan for how to make the two slides match. (Remember, we are simulating hiding the encryption method without knowing what the other person contributed).

Solution. Alice and Bob both put pieces in their envelope, remember what they did, then switch envelopes and put the same pieces in. □

22.2 Diffie-Hellman Key Exchange (25 minutes)

How does this relate to real world encryption algorithms? Diffie-Hellman key exchange works by exchanging encryption keys modulo a prime p. One difficult step of this is finding a primitive root modulo p.

a	b	c	d	e	f	g	h	i	j	k	l	m
01	02	03	04	05	06	07	08	09	10	11	12	13
n	o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25	26
space	.	,										
27	28	00										

In order to send encrypted messages, we must convert to numbers. To get a feel for how these encryption rules work, we are going to work with small numbers.

To convert the word CAT to numbers, we use this chart: 03 01 20. First, we are going to work modulo 29. Using additive key 3, the encrypted message is 06 04 23.

If we know that the message 07 18 10 was encrypted with additive key 3 modulo 29, we can decrypt by subtracting 3 to get 04 15 07, then convert to letters to get DOG.

We are going to start with Diffie-Hellman key exchange to get an additive key modulo 29. $29 = 2 * 14 + 1$ and 14 is not prime, so it is not quite as easy to find a primitive root.

Theorem 42. *If* $\gcd(a, n) = 1$*, then* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Example 11.

- *Public knowledge: working modulo* $p = 29$ *with primitive root* $a = 2$.

- *Private knowledge: Alice randomly generates $m = 3$ and Bob randomly generates $n = 8$.*

1. *Calculate the publicly published $a^m \pmod{p}$ and $a^n \pmod{p}$.*
2. *Calculate the privately known $(a^m)^n \equiv (a^n)^m \pmod{p}$.*

Solution. 1. $2^3 \equiv 8 \pmod{2}9$ and $2^8 \equiv 24 \pmod{2}9$

2. $24^3 \equiv (-5)^3 \equiv -25 * 5 \equiv 4 * 5 \equiv 20 \pmod{2}9$.

□

Contents

23 Monday, March 8: Practice Diffie-Hellman, RSA

If you have not taken an abstract algebra course or need a refresher, read Appendix B in Jones and Jones.

Turn in: Look at Chapter 5 in Jones and Jones. What parts have we already covered?

23.1 Diffie-Hellamn (10 minutes)

Breakout Room Problem (10 minutes). • *Public knowledge: working modulo $p = 29$ with primitive root $a = 2$.*

- *Private knowledge: Alice randomly generates $m = 3$ and Bob randomly generates $n = 4$.*

1. *Calculate the publicly published $a^m \pmod{p}$ and $a^n \pmod{p}$.*
2. *Calculate the privately known $(a^m)^n \equiv (a^n)^m \pmod{p}$.*
3. *Use the table and additive key a^{mn} to encrypt the message "DOG AND CAT".*

This means anyone can know $p, a, a^m \pmod{p}$, and $a^n \pmod{p}$. This could include publishing the information on the internet (assuming you are using very large numbers and something more secure than an additive cipher).

Only Alice knows her exponent m, and only Bob knows his exponent n. Only Alice and Bob know $a^{mn} \pmod{p}$. This method guarantees they end up with the same result without knowing each other's exponent (secret key).

Solution. 1. $2^3 \equiv 8 \pmod{2}9$ and $2^4 \equiv 16 \pmod{2}9$

2. $16^3 \equiv 8^4 \equiv 64^2 \equiv 6^2 \equiv 36 \equiv 7 \pmod{2}9$.

3. Translate to numbers: 04 15 07 27 01 14 04 27 03 01 20. Add 7 modulo 29: 11 22 14 05 08 21 11 05 10 08 27 □

Homework 9 problem 3: $n = 8$, see class from Friday, March 8. Message is "CAT AND DOG"

23.2 RSA (20 minutes)

We can also look at messages for RSA. The person decrypting the message:

- Calculates $n = pq$ for distinct primes p, q. The smallest such n greater than 26 is $n = 7 * 5 = 35$.
- Calculates $\phi(n)$.
- Choses e such that $\gcd(e, \phi(n)) = 1$.
- Use the Euclidean algorithm (or some other method) to find d such that $ed \equiv 1 \pmod{\phi(n)}$.
- Publishes n and e so that anyone can encrypt a message m modulo n.

The person encrypting the message:

- Converts the message to numbers.
- Calculates $m^e \pmod{n}$.
- Publishes/sends the message.

The person decrypting now calculates $(m^e)^d \equiv m^{k\phi(n)+1} \equiv m \pmod{n}$.

Theorem 43 (Theorem 5.3)**.** *If* $\gcd(a, n) = 1$*, then* $a^{\phi(n)} \equiv 1 \pmod{n}$*.*

Proof. We follow closely the proof of Fermat's Little Theorem. Recall that $a, 2a, 3a, \dots, (n-1)a$ is a set of incongruent integers $\pmod{n}$, none of which are 0. Thus, this is a complete set of integers $\pmod{n}$.

Let $R = \{r_1, r_2, \dots, r_{\phi(n)}\}$ be the set of positive integers less than n that are relatively prime to n. Then $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ is a set of integers that are relatively prime to n and distinct $\pmod{n}$. Now

$$ar_1ar_2\cdots ar_{\phi(n)} \equiv a^{\phi(n)}r_1r_2\cdots r_{\phi(n)} \equiv r_1r_2\cdots r_{\phi(n)} \pmod{n}.$$

Since each r_i has a multiplicative inverse $\pmod{n}$, we can cancel out terms on both sides of the congruence.

Thus $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Lemma 44. *Let n be a positive integer. If* $\gcd(e, \phi(n)) = 1$ *for some integer e, then there exists an integer d such that $ed \equiv 1 \pmod{\phi(n)}$ by Theorem 3.7/Corollary 3.8. For any positive integer m, $m^{ed} \equiv m \pmod{n}$.*

Proof. If $m \equiv 0 \pmod{n}$, we are done, since $0^a \equiv 0 \pmod{n}$ for any nonzero integer a. Otherwise, we use the fact that $ed \equiv 1 \pmod{\phi(n)}$ means there exists an integer k such that $k\phi(n) = ed - 1$. Thus, $m^{ed} \equiv m^{k\phi(n)+1} \equiv m \pmod{n}$. □

Theorem 45 (Theorem 5.6)**.** *If $n = pq$ for distinct primes p and q, $\phi(n) = (p-1)(q-1)$.*

Proof. There are $n - 1 = pq - 1$ positive integers less that n. Now, we need to determine how many are relatively prime to n. We do this by subtracting off those that are not relatively prime. Here, we have $p, 2p, \dots, (q-1)p$ are $q-1$ distinct positive integers less that n that are not relatively prime to n. Now we can say $\phi(n) \leq n-1-(q-1) = pq-q$. We repeat this process for q: $q, 2q, \dots, (p-1)q$. This list is disjoint from the other since p and q are relatively prime. Thus $\phi(n) \leq pq - q - p + 1$. Since p and q are the only prime factors of n, these two lists give all possible numbers less that n that are not relatively prime to n. Thus, $\phi(n) = pq - q - p + 1 = (p-1)(q-1)$. □

24 Wednesday, March 10: Logarithms, groups, rings, and fields

Turn in: Show that addition on the integers modulo m is closed, commutative, has an identity, and every element a has an additive inverse.

If we use $n = 12$, this theorem breaks down for factors $2, 6$, since they are not relatively prime. We would get the lists $2, 2(2), 3(2), 4(2), 5(2)$ and 6. Notice that 6 is on both lists, but 3 and 9 are not on either list. We will prove that $\phi(12) = \phi(3)\phi(4)$, although this counting method does not work (2 and 10 will not be on either list).

24.1 Logarithms (40 minutes)

Definition. *Let p be a prime, and let $a \in \mathbb{Z}_p$ with $a \neq 0$ (ie, $0 < a \leq p-1 \pmod{p}$). Then a is a* primitive root *in $\mathbb{Z}_p$ if $\text{ord}_p(a) = p-1$. We can also say that a* is a primitive root mod p.

Now, we have been doing a lot of exponentiation. Let's look at a logarithms

Definition. *For real numbers a and x, the logarithm (base a) of x is a real number y such that $a^y = x$. We also have that for real numbers, $\log(xy) = \log(x) + \log(y)$. Let p be a prime and a, x positive integers such that a is a primitive root modulo p and x is nonzero modulo p. The* discrete logarithm (base a) of x modulo p *is a positive integer y such that $a^y \equiv x \pmod{p}$.*

Breakout Room Problem (10 min, a lemma)**.** *Show that for a prime p, $a^m \equiv a^n \pmod{p}$ if and only if $m \equiv n \pmod{p-1}$.)*

Breakout Room Problem (5 minutes)**.** *Let $x, y \in \mathbb{Z}_p$ and let a be a primitive root modulo a. Let l_x be the discrete logarithm base a of x, l_y be the discrete logarithm base a of y, and l_{xy} be the discrete logarithm base a of xy. Prove that $l_{xy} \equiv l_x + l_y \pmod{p-1}$.*

Solution. Homework 9, problem 1 □

24.2 Groups, rings, and fields (15 minutes)

Definition. *An* equivalence relation *on a set A is denoted $a \sim b$ where:*

1. *$a \sim a$ is defined for all $a \in A$. Then we say that $\sim$ is* reflexive.
2. *$a \sim b$ implies $b \sim a$ for all $a, b \in A$. Then we say that $\sim$ is* symmetric.
3. *If $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in A$. Then we say that $\sim$ is* transitive.

Since congruence is an equivalence relation, we can talk about the congruence classes $\{a + mn : a, n \in \mathbb{Z}\}$ modulo m as one element mod m. We will formalize this statement in a bit.

Definition. *A* group *is a set A along with a binary operation $*$ where:*

1. *$a * b \in A$ for all $a, b \in A$. We say A is* closed *under the operation.*
2. *there exists an element $e \in A$ such that $e * a = a * e = a$ for all $a \in A$. We call e the* identity element*.*
3. *for each $a \in A$, there exists $\overline{a} \in A$ where $a\overline{a} = \overline{a}a = e$. We call $\overline{a}$ the* inverse*. Another way to phrase this requirement is to say that every element $a \in A$ is* invertible under the binary operation*.*
4. *$a * (b * c) = (a * b) * c$ for all $a, b, c \in A$ (we say the binary operation is* associative*)*

If $a * b = b * a$, we say a and *b* commute*. If $a * b = b * a$ for all $a, b \in A$, then we say the group is* commutative*.*

On the reading assignment we saw that the integers under addition is a group. Show that the even integers under addition is a group, but the odd integers under addition are not.

Definition. *A* ring *is a nonempty set, R, together with a two binary operations on R(which we will denote by the symbols, $+$ and $*$), where:*

- *If $a, b \in R$, then $a + b \in R$ and $a * b \in R$ (we say R is* closed under addition and multiplication*).*
- *If $a, b, c \in R$, then $(a + b) + c = a + (b + c)$ and $a * (b * c) = (a * b) * c$ (we say addition and multiplication are* associative*).*
- *There is some $e \in R$ where $a + e = e + a = a$ for all $a \in R$ (we say e is the* additive identity*).*
- *For every $a \in R$, there is some $b \in R$ where $a + b = e$ (we say b is the* additive inverse of *a).*

- *For every $a, b \in R$, $a + b = b + a$ (we say addition is* commutative*).*
- *For ever $a, b, c \in R$, $a * (b + c) = a * b + a * c$ (we say* multiplication distributes*).*
- **There is a multiplicative identity. Some sources leave off this requirement and say a ring with a multiplicative identity is a* ring with unity*. We are going to include it.*

25 Friday, March 12: Primitive roots

Read: LivelyIntroductionPrimitiveRoots.pdf

Note that this book uses slightly different notation. It states $\mathbb{Z}_p$ at the beginning of a problem or theorem, then works mod p without writing the congruence. It also uses the bar over a number to indicate that it is the representative of the congruence class.

Turn in: The check for understanding questions on page 3.

25.1 Homework related announcements (5 minutes)

On Homework 8, Problem 5, the summation should be to $m-1$, not $mn-1$. It is fine if i starts at 1 or 0, since $s_0 = 0$.

A note about the problems with exponents. We know that $(a^2)^{\frac{k}{2}} = a^k$ by exponent rules, but it is not always the case that $k/2$ is an integer.

Prove that $\mathbb{Z}_p$ is a field if and only if p is prime. Look at proofs that $\mathbb{Z}_n$ is a ring as a guide.

Moved to HW 10

25.2 Groups, rings, and fields (30 minutes)

The reading uses $\bar{a} \in \mathbb{Z}_p$ to denote the congruence class of $a \pmod p$. Our textbook uses $[a]$. I will continue to use $a \pmod p$, but you should know the book's notation.

Definition. *A multiplicative inverse for a class $[a] \in \mathbb{Z}_n$ is a class $[b] \in \mathbb{Z}_n$ such that $[a][b] = [1]$. A class $[a] \in \mathbb{Z}_n$ is a unit if it has a multiplicative inverse in Z_n. (In this case, we sometimes say that the integer a is a* unit $\pmod n$*, meaning that $ab \equiv 1 \pmod n$ for some integer b.)*

Lemma 46 (Lemma 5.1)**.** *$[a]$ is a unit in $\mathbb{Z}_n$ if and only if* $\gcd(a, b) = 1$.

Proof. This is equivalent to saying that $a \pmod n$ has a multiplicative inverse if and only if $\gcd(a, n) = 1$. That is, there exists some $b \in \mathbb{Z}_n$ such that $ab \equiv 1 \pmod n$ if and only if $\gcd(a, n) = 1$, by Theorem 3.7/Corollary 3.8. □

The addition on the integers modulo m is also commutative, which we say the "inherit" from the regular integers, so we have a commutative group.

Since an integer a has a multiplicative inverse modulo m if and only if $\gcd(a, m) = 1$ by Theorem 3.7/Corollary 3.8, multiplication on the nonzero integers modulo m is a group precisely when m is prime. Associativity also comes from the integers and the multiplicative identity is 1. Multiplication is also commutative.

Breakout Room Problem (5 minutes)**.** *The number of units in $\mathbb{Z}_n$ is $\phi(n)$.*

Therefore, our definition of $\phi(n)$ matches with the one in the book.

Solution. Our definition of $\phi(n)$ is the number of positive integers less than n that are coprime to n. By the previous lemma, this is the number of units in $\mathbb{Z}_n$. □

25.3 Primitive roots (15 minutes)

Today we are going to follow the notation and definitions from the reading. On Monday and probably Wednesday we will spend some time proving that the definitions from the reading are equivalent to the more group theoretic (or ring theoretic) definitions in our book. That is, we will do a lot of "if and only if" proofs like the one where we proved the number of units in $\mathbb{Z}_n$ is $\phi(n)$.

We looked at powers modulo 11 a while ago. As a review, we have

$$\begin{aligned}
&\operatorname{ord}_{11}(1) = 1,\\
&\operatorname{ord}_{11}(10) = 2,\\
&\operatorname{ord}_{11}(3) = \operatorname{ord}_{11}(4) = \operatorname{ord}_{11}(5) = \operatorname{ord}_{11}(9) = 5,\\
&\operatorname{ord}_{11}(2) = \operatorname{ord}_{11}(6) = \operatorname{ord}_{11}(7) = \operatorname{ord}_{11}(8) = 10.
\end{aligned}$$

Thus, the primitive roots modulo 11 are 2,6,7, and 8.

Theorem 47 (Reading Proposition 10.3.2, Textbook definition of a primitive root when p is prime)**.** *Let p be prime and let $a \in \mathbb{Z}_p$ be a primitive root. Then every nonzero element of $\mathbb{Z}_p$ (that is, every congruence class that is not congruent to $0 \pmod{p}$) appears exactly once on the list*

$$a^0, a^1, \dots a^{p-2}.$$

Instead of following the proof from the reading, here is how we can use the Lemma from last class: Homework 9, Problem 1a.

Proof. Let p be prime and let $a \in \mathbb{Z}_p$ be a primitive root. Then $a^m \equiv a^n \pmod{n}$ if and only if $m \equiv n \pmod{p-1}$.

Since the exponents of the list

$$a^0, a^1, \dots a^{p-2}$$

are not equivalent $\pmod{p-1}$, the elements fo the list are distinct.

There are $p-1$ distinct elements on the list, and none of them are $0 \pmod{p}$. There are also $p-1$ distinct nonzero elements of $\mathbb{Z}_p$. Thus, each element appears exactly once on the list. □

For help proving the Lemma from last class, see the note or recording from class or the proof of this statement in the reading.

Theorem 48 (Primitive root theorem)**.** *Let p be prime. Then there exists a primitive root modulo p.*

Lemma 49 (Lemma 10.3.4)**.** *Let p be a prime, and let q^s be a prime power divisor of $p-1$. That is, q is prime and $q^s \mid p-1$. Then there exists an element of order q^s in $\mathbb{Z}_p$.*

Example when $p = 101$ in the reading. We will not go over this proof in class.

Lemma 50 (Lemma 10.3.5)**.** *Let $n \in \mathbb{Z}^+$ and let $a, b \in \mathbb{Z}$ be reduced residues $\pmod{n}$ (that is, relatively prime to n). If $\operatorname{ord}_n(a)$ and $\operatorname{ord}_n(b)$ are relatively prime, then*

$$\operatorname{ord}_n(ab) = \operatorname{ord}_n(a) \operatorname{ord}_n(b).$$

Contents

26 Monday, March 15: Primitive roots, rings, fields

26.1 Primitive roots (50 minutes)

Theorem 51 (Primitive root theorem, rephrased Corollary 6.6)**.** *Let p be prime. Then there exists a primitive root modulo p.*

Proof. Let p be prime. If $p = 2$, then $1 \pmod 2$ is a primitive root.

Assume that $p > 2$. First, we are going to factor $p - 1 = q_1^{a_1} q_2^{a_2} \cdots q_m^{a_m}$. By Lemma 10.3.4 in the reading, for each $k = 1, 2, \dots, m$ there exists an element $x_k \in \mathbb{Z}_p$ where the $\operatorname{ord}_p(x_k) = q_k^{a_k}$. Let

$$x \equiv x_1 x_2 \cdots x_m \pmod p.$$

By repeatedly applying Lemma 10.3.5 from last class, we find that

$$\begin{aligned}\operatorname{ord}_p(x) &= \operatorname{ord}_p(x_1) \operatorname{ord}_p(x_2) \cdots \operatorname{ord}_p(x_m)\\ &= q_1^{a_1} q_2^{a_2} \cdots q_m^{a_m}\\ &= p - 1.\end{aligned}$$

Therefore, x is a primitive room $\pmod p$. □

Lemma 52 (Lemma 10.3.6 from reading)**.** *Let p be prime, and let $a \in \mathbb{Z}_p$ be a primitive root. Then for any $j \in \mathbb{Z}$, a^j is a primitive root if and only if* $\gcd(j, p-1) = 1$.

See corrected statement re: Lemma 6.4 at the beginning of class Wednesday.

Breakout Room Problem (10 minutes)**.** *Let $a \in \mathbb{Z}_n$ for a nonnegative integer n and* $\gcd(a, n) = 1$. *Let* $s = \operatorname{ord}_n(a)$. *For any $j \in \mathbb{Z}^+$,*

$$\operatorname{ord}_n(a^j) = \frac{s}{\gcd(j, s)}.$$

Solution. Homework 10, Problem 1. See class recording. Note that $\frac{s}{\gcd(j,s)}$ and $\frac{j}{\gcd(j,s)}$ are relatively prime. □

Proof of Lemma 10.3.6 from reading. Let p be prime, and let $a \in \mathbb{Z}_p$ be a primitive root modulo p. By the breakout room problem,

$$\operatorname{ord}_p(a^j) = \frac{p-1}{\gcd(j, p-1)}.$$

Thus, $\operatorname{ord}_p(a^j) = p - 1$ if and only if $\gcd(j, p-1) = 1$. □

27 Wednesday, March 17: Primitive roots, rings, fields

27.1 Corrections (10 minutes)

I have fixed the grading on Quiz 9. The person decrypting the message:

- Calculates $n = pq$ for distinct primes $p = 5, q = 11$. So $n = 55$.
- Calculates $\phi(n) = \phi(p)\phi(q) = 40$.
- Choses e such that $\gcd(e, \phi(n)) = 1$.
- Use the Euclidean algorithm (or some other method) to find d such that $ed \equiv 1 \pmod{\phi(n)}$.
- Publishes n and e so that anyone can encrypt a message m modulo n.

Fixing a statement from Monday: Lemma 6.4 in the textbook is a consequence of Lemma 10.3.6 from the reading, but it is not equivalent. Lemma 10.3.6 is finding all

27.2 Group Isomorphisms, Cyclic Groups, equivalences with the textbook (40 minutes)

Definition. *Two groups $(G, +)$ and $(H, *)$ are* isomorphic *if there exists a bijective map $F : G \to H$ such that $f(a + b) = f(a) * f(b)$ for all $a, b \in G$.*

Proposition 53. *Any two complete residue systems mod m are isomorphic as additive groups.*

Proof. Let $\{a_1, a_2, \dots, a_m\}$ and $\{b_1, b_2, \dots, b_m\}$ be complete residue systems mod m. Then for each a_i, there exists a unique b_j where $a_i \equiv b_j \pmod{m}$. Define f to be that map $f(a_i) = b_j$ where $a_i \equiv b_j$. By the definition of complete residue system, this map is injective and surjective. By Lemma 3.3, $f(a_i + a_k) = f(a_i) + f(a_k)$ since $a_i \equiv f(a_i) \pmod{m}$ and $a_k \equiv f(a_k) \pmod{m}$. □

Breakout Room Problem (2 min)**.** *The complete residue systems $\{1, 2, 3, 4, 5\}$ and $\{2, 4, 6, 8, 10\}$ are isomorphic as representations of $\mathbb{Z}_5$.*

Define the map f to be that map $f(a_i) = b_j$ where $a_i \equiv b_j \pmod{5}$. You can define it element by element, not looking for some arithmetic/algebraic function.

Solution. One option is $f(a) = 2a$. Another option is $f(1) = 6, f(2) = 2, f(3) = 8, f(4) = 4, f(5) = 10$. □

Now, we see that $f(1 + 3) = f(4) = 4$ and $f(1) + f(3) = 6 + 8 \equiv 4 \pmod{5}$.

Definition. *A group $(G, *)$ is* cyclic *if there exists some element $a \in G$ such that every element of G can be written as a^n for some integer n. The element a is called a* generator *for $(G, *)$.*

Example 12. *Let's consider U_5, the group of units modulo 5.* $1 \equiv 2^4 \pmod{5}, 2 \equiv 2^1 \pmod{5}, 3 \equiv 2^3 \pmod{5}$ *and* $4 \equiv 2^2 \pmod{5}$. *So U_5 is cyclic with generator* 2.

Homework: Show that 3 *is also generators for U_5.*

Corollary 54 (Corollary 6.6)**.** *If p is prime, then the group U_p is cyclic.*

Proof. Reading Proposition 10.3.2, says:

Let p be prime and let $a \in \mathbb{Z}_p$ be a primitive root. Then every nonzero element of $\mathbb{Z}_p$ (that is, every congruence class that is not congruent to $0 \pmod{p}$) appears exactly once on the list

$$a^0, a^1, \dots a^{p-2}.$$

Thus, any primitive root is a generator for U_p. □

Our textbook uses the following definition:

Definition. *If U_n is cyclic then any generator g for U_n is called a* primitive root mod (n). *This means that g has order equal to the order $\phi(n)$ of U_n, so that the powers of g yield all the elements of U_n.*

Breakout Room Problem (1 min)**.** *We saw last week that the number of units in $\mathbb{Z}_n$ is $\phi(n)$. That is, there are $\phi(n)$ elements in U_n. If every element in U_n can be represented by g^r for some $r \in \mathbb{Z}$, then it must be that* $\text{ord}_n(g) = \phi(n)$.

Why?

28 Friday, March 19: Other common number theory functions, start of quadratic residues

Read Sections 7.1 and 7.2

Turn in: Exercise 7.1. Find all the solutions in $\mathbb{Z}_{15}$ of the congruence $x^2 - 3x + 2 \equiv 0 \pmod{15}$.

Why does this not contradict our earlier results?

28.1 Announcements (5 minutes)

Proving that $\mathbb{Z}_p$ is a field if and only if p is prime is moved to Homework 10.

Another reminder, since it came up in office hours, that you are not expected to have seen the group theory material before. Some students have seen it in other classes, but that is not the expectation.

28.2 Group Isomorphisms, Cyclic Groups, equivalences with the textbook (20 minutes)

Now we are going to finish translating back to the book's definitions. From the reading assignment Wednesday, it looks like people were a fuzzy on the translations. Hopefully class Wednesday helped, but here is my list:

No equivalents to Section 6.1. This is because we are not going to use that framing, so I did not want to focus on it.

In class Wednesday, we finished connecting the Jones and Jones definition of primitive roots and $\phi(n)$ to the one we'd been using in class.

Lemma 6.4 is related to Lemma 10.3.4 and 10.3.5 in the reading, but for prime and composite moduli.

We are about to state Theorem 6.5, but the "modifying proofs" version is on Homework 10.

We did Corollary 6.6 on Wednesday.

Theorem 55 (Theorem 6.5)**.** *If p is prime, then the group U_p has $\phi(d)$ element of order d for each d dividing $p-1$.*

Proof. The $p = 7$ case is on Homework 10. □

Theorem 56 (Theorem 6.11)**.** *The group U_n is cyclic if and only if*

$$n = 1, 2, 4, p^e, \text{ or } 2p^e,$$

where p is an odd prime.

That is, a primitive root exists modulo n if and only if

$$n = 1, 2, 4, p^e, \text{ or } 2p^e,$$

where p is an odd prime.

Proving the "only if" direction is one of the Project 3 options.

28.3 Rings and fields (15 minutes)

Definition. *A* ring *is a nonempty set, R, together with a two binary operations on R(which we will denote by the symbols, $+$ and $*$), where:*

- *R is a commutative group under $+$.*
- *If $a, b \in R$, then $a * b \in R$ (we say R is* closed under multiplication*).*

- *If $a, b, c \in R$, then $a * (b * c) = (a * b) * c$ (we say multiplication are* associative*).*
- *There is some $e \in R$ where $a * e = e * a = a$ for all $a \in R$ (we say e is the* multiplicative identity*). *Some sources leave off this requirement and say a ring with a multiplicative identity is a* ring with unity*. We are going to include it.*
- *For ever $a, b, c \in R$, $a * (b + c) = a * b + a * c$ (we say* multiplication distributes*).*

Breakout Room Problem (5 minutes)**.** *Let $\mathbb{Z}_m$ be the set of integers $\{0, 1, \ldots, m-1\}$ along with addition and multiplication modulo m. That is, $\mathbb{Z}_m$ is the least nonnegative complete residue system modulo m. Prove that $\mathbb{Z}_m$ is a ring.*

Two elements $a, b \in \mathbb{Z}_m$ where $a \equiv b \pmod{m}$ are said to be representatives of the same congruence class $\pmod{m}$*.*

Any two complete residue systems mod m are also isomorphic as rings.

Definition. *A* field *is a nonempty set, F, together with two binary operations $+$ and $*$ where:*

1. *F is a ring.*
2. *$a * b = b * a$ for all $a, b, \in F$.*
3. *For all $a \in F, a \neq 0$, there exists $a^{-1} \in F$ where $a * a^{-1} = a^{-1}a = 1$. Here 0 is the additive identity and 1 is the multiplicative identity.*

Proving that $\mathbb{Z}_p$ is a field if and only if p is prime is on Homework 10.

28.4 Other common number theory functions (10 minutes)

We are going to look at some other functions that show up in analytic number theory. Some of these also show up in the proofs in section 6.2

- $d(n)$ is the number of positive divisors of n. For example, $d(12) =$. We introduce the notation $\sum_{d|n}$ as "the sum over the divisors of n," called the *divisor sum*. For the normal sum: $\sum_{i=1}^{n} 1 = n$. Then, $\sum_{d|n} 1 = d(n)$.
- In the proof of Theorem 6.5, textbook defines $\Omega_d = \{a \in U_p : a \text{ has order } d\}, \omega(d) = !\Omega_d|$, and $\sum_{d|n} \omega(d)$. For $p = 7$, this would be $\omega(1) + \omega(2) + \omega(3) + \omega(6)$.

Contents

29 Monday, March 22: Quadratic residues

Definition. *An element $a \in U_n$ is a quadratic residue $\pmod{n}$ if $a = s^2$ for some $s \in U_n$.*

That is, $a \in \mathbb{Z}$ such that $\gcd(a, n)$ is a quadratic residue if there exists $s \in \mathbb{Z}$ such that $a \equiv s^2 \pmod{n}$.

The set of such quadratic residues is denoted by Q_n. For small n, one can determine Q_n simply by squaring all the elements $s \in U_n$.

If there exists no such x then we say that a is a quadratic non-residue.

This is the modular arithmetic of perfect squares.

Example 13 (Example 7.1)**.** *$Q_7 = \{1, 2, 4\} \subset U_7 \subset \mathbb{Z}_7$, while $Q_8 = \{1\} \subset U_8 \subset \mathbb{Z}_8$.*

Breakout Room Problem (5 min, Exercise 7.3)**.** *Find Q_n for each $n \leq 12$*

Hint: write out $1^2 = (-1)^2, 2^2 = (-2)^2, 3^2 = (-3)^2, 4^2 = (-4)^2, 5^2 = (-5)^2, 6^2 = (-6)^2$ first.

Lemma 57 (Lemma 7.2)**.** *Q_n is a subgroup of U_n. That is, $Q_n \subset U_n$ is a group under multiplication $\pmod n$.*

Breakout Room Problem (5 min)**.** *Prove Lemma 7.2*

What could go wrong: Closed: The odd integers are a subset of the integers, but not closed under addition

Identity: The odd integers are a subset of the integers, but do not contain the additive identity (0)

Inverses: $\mathbb{Q}\backslash\{0\} = \{\text{rationals that are not } 0\}$ are a group under multiplication. $\mathbb{Z}\backslash\{0\} = \{\text{integer that are not } 0\}$, $\mathbb{Z} \subset \mathbb{Q}$ but does not have multiplicative inverses.

Proof. $a = s^2, b = t^2, ab = (st)^2$

We need to show that Q_n contains the identity element of U_n, and is closed under taking products and inverses.

Firstly, $1 \in Q_n$ since $1 = 1^2$ with $1 \in U_n$.

If $a, b \in Q_n$ then $a = s^2$ and $b = t^2$ for some, $t \in U_n$, so $ab = (st)^2$ with $s, t \in U_n$, giving $ab \in Q_n$.

Finally, if $a \in Q_n$ then $a = s^2$ for some $s \in U_n$; since a and s are are units mod (n) they have inverses a^{-1} and s^{-1} in U_n, and $a^{-1} = (s^{-1})^2$ so that $a^{-1} \in Q_n$. □

Theorem 58 (Theorem 3.11)**.** *Let $n = n_1 \dots n_k$ where the integers n_i are mutually coprime, and let $f(x)$ be a polynomial with integer coefficients. Suppose that for each $i = 1, \dots, k$ there are N_i congruence classes $x \in \mathbb{Z}_{n_i}$ such that $f(x) \equiv 0 \pmod{n_i}$. Then there are $N = N_1 \dots N_k$ classes $x \in \mathbb{Z}_n$ such that $f(x) \equiv 0 \pmod n$.*

Example 14. *Let's find solutions to $x^2 + 5x + 6 \equiv 0 \pmod{60}$. Now, $60 = 2^2(3)(5)$, so we can find solutions modulo 3, 4, and 5.*

On Wednesday, we will see that there are 2 solutions mod 3, 2 solutions mod 4, and 2 solutions mod 5 for $2(2)(2) = 8$ total solutions.

30 Wednesday, March 24: Quadratic reciprocity

Read section 7.3 on the Legendre symbol.

Turn in: Exercise 7.8

Determine whether 3 and 5 are quadratic residues mod (29).

Example 15. *Let's find solutions to $x^2 + 5x + 6 \equiv 0 \pmod{60}$. Now, $60 = 2^2(3)(5)$, so we can find solutions modulo 3, 4, and 5.*

$$\begin{aligned} x^2 + 5x + 6 &\equiv 0 \pmod 3 \\ x^2 + 2x &\equiv 0 \pmod 3 \\ x(x+2) &\equiv 0 \pmod 3 \end{aligned}$$

Thus, $x \equiv 0 \pmod 3$ or $x \equiv -2 \equiv 1 \pmod 3$.

$$
\begin{aligned}
x^2+5x+6 &\equiv 0 \pmod 4\\
x^2+x+2 &\equiv 0 \pmod 3
\end{aligned}
$$

Thus, $x \equiv 1 \pmod 4$ *or* $x \equiv 2 \pmod 4$.

$$
\begin{aligned}
x^2+5x+6 &\equiv 0 \pmod 5\\
x^2+1 &\equiv 0 \pmod 5\\
x^2 &\equiv -1 \equiv 4 \pmod 5
\end{aligned}
$$

Thus, $x \equiv 2 \pmod 5$ *or* $x \equiv -2 \equiv 3 \pmod 5$.

Breakout Room Problem (10 min)**.** *Set up the systems of congruences necessary to find the roots using the Chinese remainder thm. Then start to solve these congruences.*

Solution.

$$
\begin{aligned}
x \equiv 0 &\pmod 3, x \equiv 1 \pmod 4, x \equiv 3 \pmod 5, \text{ thus } x \equiv 33 \pmod{60}\\
x \equiv 0 &\pmod 3, x \equiv 1 \pmod 4, x \equiv 2 \pmod 5, \text{ thus } x \equiv 57 \pmod{60}\\
x \equiv 1 &\pmod 3, x \equiv 1 \pmod 4, x \equiv 3 \pmod 5, \text{ thus } x \equiv 13 \pmod{60}\\
x \equiv 1 &\pmod 3, x \equiv 1 \pmod 4, x \equiv 2 \pmod 5, \text{ thus } x \equiv 37 \pmod{60}\\
x \equiv 0 &\pmod 3, x \equiv 2 \pmod 4, x \equiv 3 \pmod 5, \text{ thus } x \equiv 18 \pmod{60}\\
x \equiv 0 &\pmod 3, x \equiv 2 \pmod 4, x \equiv 2 \pmod 5, \text{ thus } x \equiv 42 \pmod{60}\\
x \equiv 1 &\pmod 3, x \equiv 2 \pmod 4, x \equiv 3 \pmod 5, \text{ thus } x \equiv 58 \pmod{60}\\
x \equiv 1 &\pmod 3, x \equiv 2 \pmod 4, x \equiv 2 \pmod 5, \text{ thus } x \equiv 22 \pmod{60}
\end{aligned}
$$

□

See recording for more details, or notes uploaded to participation assignment. For a reminder about the Chinese Remainder Theorem, see Chapter 3, Week 5 notes, or `https://youtu.be/zIFehsBHB8o`

Example 16 (Example 3.18)**.** *Wish to find solutions to* $f(x) = x^2 - 1$ *modulo* n. *Now, we know that when* n *is prime, there are at most* 2 *solutions. We also know that* $x \equiv \pm 1 \pmod n$ *is always a solution.*

If we factor n *into its prime power factorization, we can then use the Chinese remainder theorem to find the number of solutions modulo* N. *We count solutions to* $x^2 \equiv 1 \pmod{p^e}$ *where* p *is prime and* e *is a positive integer.*

If p *is odd, then there are just two classes of solutions:* $x \equiv \pm 1 \pmod{p^e}$ *are always solutions, since* $(\pm 1)^2 = 1$. *To show there are no other solutions, consider that* $0 \equiv x^2 - 1 \equiv (x+1)(x-1) \pmod{p^e}$. *Thus,* $p^e \mid (x+1)(x-1)$. *Thus,* $p^e \mid x+1$ *or* $p^e \mid x-1$. *If* $p \mid (x+1)$ *and* $p \mid (x-1)$, *then by linear combinations,* $p \mid x+1+x-1 = 2x$. *Since* p *is odd, this would mean* $x \equiv 0 \pmod p$.

Now we need to consider $p = 2$. *If* $p^e = 2$, *then by inspection the solution is* $x \equiv 1 \pmod 2$. *Similarly, for* $p^e = 4$, *the solutions are* $x \equiv \pm 1 \pmod 4$. *For* $2^e \geq 8$, *we see that* $x \equiv \pm 1 \pmod{2^e}$, *but also that* $x \equiv 2^{e-1} \pm 1 \pmod{2^e}$. *This comes from the fact that* $2^e \mid (x+1)(x-1)$. *Thus,* $2^e \mid x+1$ *or* $2^e \mid x-1$. *Since* $2 \mid 2x$, *we do not get the contradiction from the previous case.*

31 Friday, March 26: Quadratic reciprocity

Turn in Compare and contrast the proofs of Corollary 7.8 (infinitely many primes of the form 1 mod 4), Theorem 2.9 (infinitely many primes of the form 4q + 3), and Exercise 2.6 (infinitely many primes of the form 3q+2).

31.1 Announcements/reminders (10 minutes)

Next week has a very weird schedule. We do not have class next Wednesday, but we are to treat Friday as a Wednesday. For this class, this means:

- Office hours will be on Friday at 2 pm or by appointment. The department is using the instructional break to schedule a bunch of meetings, so I will not have normal office hours Wednesday and Thursday.
- Homework 11 is actually due on April 9, along with Homework 12. This is correct in Carmen, but in Gradescope it means the "late" deadline is April 10 instead on April 3.
- **Added during class** I will do the same thing for Project 2.
- No quiz next week.
- For the sake of simplicity, the revise and resubmit deadlines will still be the same.

Homework 11 is short since we are going pretty slowly this week, with 1) review of the Chinese remainder theorem, 2) problems and proofs in class that are long. Homework 12 will also be shorter, since it only covers two days of class. However, the material is a bit more conducive to short calculation problems.

31.2 Finishing review of Chapter 3 (30 minutes)

Theorem 59 (Theorem 3.11)**.** *Let $n = n_1 \dots n_k$ where the integers n_i are mutually coprime, and let $f(x)$ be a polynomial with integer coefficients. Suppose that for each $i = 1, \dots, k$ there are N_i congruence classes $x \in \mathbb{Z}_{n_i}$ such that $f(x) \equiv 0 \pmod{n_i}$. Then there are $N = N_1 \dots N_k$ classes $x \in \mathbb{Z}_n$ such that $f(x) \equiv 0 \pmod{n}$.*

Proof. We will start with $n = p^\alpha q^\beta$ for primes p, q, then apply the same technique to generalize. Let $a_1, a_2, \dots, a_{N_{p^\alpha}}$ be the solutions to $f(x) \equiv 0 \pmod{p^\alpha}$, and $b_1, b_2, \dots, b_{N_{q^\beta}}$ be the solutions to $f(x) \equiv 0 \pmod{b^\beta}$. From the fact that $n \mid f(x)$ and $n = p^\alpha q^\beta$, we know that a solution to $f(x) \equiv 0 \pmod{m}$ is also a solution to $f(x) \equiv 0 \pmod{p^\alpha}$ and $f(x) \equiv 0 \pmod{q^\beta}$. So we are looking for solutions that work modulo p^α and q^β. Then for each pair $x \equiv a_i \pmod{p^\alpha}, x \equiv b_j \pmod{q^\beta}$, the Chinese remainder theorem tells us that there exists a unique solution modulo n. There are $N(p^\alpha)N(q^\beta)$ such pairs, so there are at most $N_{p^\alpha} N_{q^\beta}$ solutions to $f(x) \equiv 0 \pmod{m}$.

We can also say that for each a_i, b_j, there is a $0 \leq x_{ij} \leq m$ where $f(x_{ij}) \equiv 0 \pmod{p^\alpha}$ and $f(x_{ij}) \equiv 0 \pmod{q^\beta}$. The Theorem 2.3 part 3 gives us $f(x_{ij}) \equiv 0 \pmod{m}$. Thus, all possible $N_{p^\alpha} N_{q^\beta}$ solutions to $f(x) \equiv 0 \pmod{m}$ are solutions.

Since the Chinese remainder thm and Theorem 2.3 part 3 apply to arbitrarily many factors, this proof holds with more prime power factors. □

Thus, Example 3.18 from last class shows that for $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $x^2 - 1 \equiv 0 \pmod{n}$ has N incongruent solutions, where

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \pmod{8} \\ 2^{k-1} & \text{if } n \equiv 2 \pmod{4} \\ 2^k & \text{otherwise,} \end{cases}$$

where k is the number of distinct primes dividing n. For instance, if $n = 60 = 2^2(3)(5)$ then $k = 3$ and there are $2^k = 8$ classes of solutions, namely $x \equiv \pm 1, \pm 11, \pm 19, \pm 29 \pmod{60}$.

31.3 Connecting results from Chapter 3 and Homework 6 to Quadratic residues (15 minutes)

Lemma 60 (Lemma 7.1)**.** *Let k denote the number of distinct primes dividing n. If $a \in Q_n$, then the number N of elements $t \in U_n$ such that $t^2 = a$ (that is, the number of incongruent solutions to $t^2 \equiv a \pmod{n}$) is given by*

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \pmod 8 \\ 2^{k-1} & \text{if } n \equiv 2 \pmod 4 \\ 2^k & \text{otherwise.} \end{cases}$$

Proof. If $a \in Q_n$ then $s^2 = a$ for some $s \in U_n$. Any element $t \in U_n$ has the form $t \equiv sx \pmod{n}$ for some unique $x \in U_n$. To see this, note that by the definition of U_n, there exists a unique $s^{-1} \in U_n$ where $ss^{-1} \equiv 1 \pmod{n}$. Thus, $x \equiv s^{-1}t \pmod{n}$.

Thus, $t^2 \equiv a \pmod{n}$ if and only if $x^2 \equiv 1 \pmod{n}$. By Example 3.18, this means that N has the desired form. □

On Homework 6, we saw that for an odd prime p:

- If $p \equiv 1$ mod 4, $\left(\frac{p-1}{2}\right)!$ is a solution of the quadratic congruence $x^2 \equiv -1$ mod p.
- If $p \equiv 3$ mod 4, $\left(\frac{p-1}{2}\right)!$ is a solution of the quadratic congruence $x^2 \equiv 1$ mod p.

Now, $1^2 \equiv (-1)^2 \equiv 1 \pmod{n}$ means that 1 is always a quadratic residue, so the second statement is not particularly helpful.

But if p is prime such that $p \equiv 1 \pmod 4$, then -1 is a quadratic residue $\pmod{p}$. One goal is to show that for an odd prime p, if -1 is a quadratic residue $\pmod{p}$, then $p \equiv 1 \pmod 4$. (Corollary 7.7).

Contents

32 Monday, March 29: Quadratic reciprocity

If you did not submit March 24 Participation or March 26 Participation, you can do that here.

32.1 Quadratic residues and the Legendre symbol (10 minutes)

Let $p > 2$ be a prime, and let a be an integer between 0 and $p - 1$. We have three options:

- If a is a unit, and a "perfect square", then a is a quadratic residue
- If a is a unit but not a square, then a is a quadratic nonresidue
- if a is not a unit, then $\gcd(a, p) \neq 1$. Since p is prime, this means $p \mid a$.

Breakout Room Problem (1 min)**.** *What happens with $a^{\frac{p-1}{2}} \pmod{p}$ in each case?*

- If a is a quadratic residue modulo p, then $a^{(p-1)/2} = 1$.
- If a is a quadratic nonresidue modulo p, then $a^{(p-1)/2} = -1$.
- Otherwise, $a^{(p-1)/2} = 0$.

Proof at the end of class.

Definition. *We define the* Legendre symbol *for a prime p and integer a to be*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \\ 0 & \text{if } p \mid a \end{cases}$$

Euler's identity: Let $p > 2$ be a prime, and let a be an integer. Then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Proof at the end of class.

Theorem 61. *Let $p > 2$ be prime.*

- *If $p \equiv 1 \pmod 4$, then -1 is a quadratic residue modulo p.*
- *If $p \equiv 3 \pmod 4$, then -1 is a quadratic nonresidue modulo p.*

Proof. We know that $(-1)^{(p-1)/2} \equiv (-1)^{(4k+1-1)/2} \equiv 1 \pmod{p}$ if $p \equiv 1 \pmod 4$, and $(-1)^{(p-1)/2} \equiv (-1)^{(4k+3-1)/2} \equiv 1 \pmod{p}$ if $p \equiv 3 \pmod 4$. Since $p > 1$, -1 is a unit modulo p.

Euler's identity tells us that $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$. Thus, we get

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

Let $p > 2$ be prime, and let a and b be integers that are not congruent to $0 \pmod{p}$.

- If ab is a quadratic residue, then what do we know about a and b?
- If ab is a quadratic nonresidue, then what do we know about a and b?

One approach is to consider the three options:

- both a and b are quadratic residues
- both a and b are quadratic nonresidues
- one is a quadratic residue and one is a quadratic nonresidue

Let's go through case by case:

- If $s, t \in \mathbb{Z}$ exist such that $a \equiv s^2 \mod p$ and $b \equiv t^2 \pmod{p}$, then $ab \equiv (st)^2 \pmod{p}$.
- If $a^{(p-1)/2} \equiv b^{(p-1)/2} \equiv -1 \pmod{p}$, then $(ab)^{(p-1)/2} \equiv (-1)^2 \equiv 1 \pmod{p}$. So ab is a quadratic residue.

  This may seem surprising, but think about $36 = 6^2 = 6(6) = 4(9) - = 3(12)$.
- If $a^{(p-1)/2} \equiv 1 \pmod{p}$ and $b^{(p-1)/2} \equiv -1 \pmod{p}$, then $(ab)^{(p-1)/2} \equiv 1(-1) \equiv -1 \pmod{p}$. So ab is a quadratic nonresidue.

Proof of Euler's Criterion. Let $p > 2$ be a prime, and let a be an integer between 0 and $p - 1$.

If $\gcd(a, p) = 1$, the $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. Thus, $(a^{(p-1)/2})^2 \equiv 1 \pmod{p}$. Since p is an odd prime, we know that $\frac{p-1}{2}$ is an integer and the solutions to $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1 \pmod{p}$. We need to determine when we have 1 and when we have -1.

If a is a quadratic residue, then there exists s where $a \equiv s^2 \pmod{p}$. Thus, we also know $s^{-1} \equiv 1 \pmod{p}$ by the Fermat's Little Theorem. Thus, $a^{(p-1)/2} \equiv (s^2)^{(p-1)/2} \equiv 1 \pmod{p}$.

If a is a quadratic nonresidue, for each $i = 1, 2, \ldots, p-1$ there exists a unique j such that $ij \equiv a \pmod{p}$ by Corollary 3.8. We know that $i \neq j$, since that would mean $i^2 \equiv a \pmod{p}$.

Thus, we can write $(p-1)! = 1(2)(3)\cdots(p-1) \pmod{p}$ by pairing these integers i and j. There are $\frac{p-1}{2}$ pairings. Thus,

$$\begin{aligned} (p-1)! &\equiv -1 \pmod{p} && \text{by Wilson's Theorem} \\ a^{(p-1)/2} &\equiv (p-1)! && textrmbytheprecedingargument \end{aligned}$$

so $a^{(p-1)/2} \equiv -1 \pmod{p}$.

If $a \equiv 0 \pmod{p}$, then $a^{(p-1)/2} \equiv 0 \pmod{p}$. □

33 Friday, April 2: Quadratic reciprocity

33.1 Quadratic reciprocity

We are going to explore the relationship between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$. Let's look at an example: We want to know if 3 is a quadratic residue modulo 107. It would be a lot easier to check if 107 is a quadratic residue modulo 3. We know that $107 \equiv 2 \pmod{3}$, so $\left(\frac{107}{3}\right) = -1$. It would be nice if this also gave us $\left(\frac{3}{107}\right)$.

Breakout Room Problem (5 minutes)**.** *Another example: Find* $\left(\frac{p}{5}\right)$ *and* $\left(\frac{5}{p}\right)$.

p	*3*	*5*	*7*	*11*	*13*
$\left(\frac{p}{5}\right)$	-1	0	-1	1	-1
$\left(\frac{5}{p}\right)$	*-1*	*0*	*-1*	*1*	*-1*

Another example: Find $\left(\frac{p}{7}\right)$ *and* $\left(\frac{7}{p}\right)$.

p	*3*	*5*	*7*	*11*	*13*
$\left(\frac{p}{7}\right)$	-1	-1	*0*	1	-1
$\left(\frac{7}{p}\right)$	1	-1	*0*	*-1*	*-1*

This gives some evidence for our thm:

Theorem 62. *Let p and q be odd primes with $p \neq q$.*

- *if* $p \equiv 1 \pmod{4}$ *or* $q \equiv 1 \pmod{4}$*, then* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
- *if* $p \equiv q \equiv 3 \pmod{4}$*, then* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Our goal for this week is to prove this.

Let's try some examples:

Poll question. $\left(\frac{11}{47}\right) = -1 * \left(\frac{47}{11}\right)$. *We can reduce* $47 \equiv 3 \pmod{11}$*, which*

- *is*
- *is not*

a quadratic residue modulo 11.

Poll question. $\left(\frac{3}{107}\right) = -1 * \left(\frac{107}{3}\right)$. *We can reduce* $107 \equiv 2 \pmod{3}$*, which*

- *is*
- *is not*

a quadratic residue modulo 3.

We are going to restate quadratic reciprocity as

Theorem 63 (Restatement of quadratic reciprocity)**.** *Let p and a be odd primes with $p \neq q$. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proposition 64. *The restatement of quadratic reciprocity implies quadratic reciprocity.*

Proof. Let p and q be odd primes with $p \neq q$. We assume that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ is true. Then we have two cases:

- $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$ [To show $\left(\frac{p}{q}\right) = 1 * \left(\frac{q}{p}\right)$.]

  Without loss of generality, we assume $p \equiv 1 \pmod 4$. Then there exists a $k \in \mathbb{Z}$ such that $p = 4k + 1$. This implies that $\frac{p-1}{2} = 2k$. Thus,

  $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1^{\frac{q-1}{2}} = 1.$$

  Thus, we have that $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ must either both be $+1$ or both be -1.

- $p \equiv q \equiv 3 \pmod 4$[To show $\left(\frac{p}{q}\right) = -1 * \left(\frac{q}{p}\right)$.] There exists $k, m \in \mathbb{Z}$ such that $p = 4k + 3$ and $q = 4m + 3$. This implies that $\frac{p-1}{2} = 2k + 1$ and $\frac{q-1}{2} = 2k + 1$. Thus,

  $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}} = -1.$$

  Thus, we have that exactly one of $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ is $+1$ and the other is -1. □

In order to prove this, we first need to prove two rather technical lemmas. Then we will use a geometric proof to finish.

Lemma 65 (Gauss's lemma)**.** *Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least positive residues of the integers $a, 2a, \ldots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$. Then*

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

Use Gauss's lemma to find $\left(\frac{6}{11}\right)$. We need to find n, the number of least nonnegative positive residues of the integers $6, 2 * 6, 3 * 6, 4 * 6, 5 * 6$ greater that 5.5 We have

$$\begin{aligned} 6 &\equiv 6 \pmod{11} \\ 2 * 6 &\equiv 1 \pmod{11} \\ 3 * 6 &\equiv 7 \pmod{11} \\ 4 * 6 &\equiv 2 \pmod{11} \\ 5 * 6 &\equiv 8 \pmod{11} \end{aligned}$$

Thus, $n = 3$ and $(-1)^n = -1$.

Contents

34 Monday, April 5: Lemmas to prove quadratic reciprocity

Reading: Section 7.4

Turn in: Let p be an odd prime. Let $r_1, r_2, \ldots, r_n$ least representatives of $a, 2a, 3a, ..., \frac{(p-1)a}{2}$ modulo p which are greater than p/2 and s1,s2,...,sm be the least nonnegative representatives of a,2a,3a,...,(p-1)a/2 modulo p which are less than p/2. That is, some of the (p-1)/2 elements of the list a,2a,...,(p-1)a/2 are on the list r1,r2,...,rn and the rest are on the list s1,s2,...,sm.

We write the greatest integer (or floor) function of x as [x].

Then for each j=1,2, ...,(p-1)/2 we have that ja=p[ja/p]+(remainder depending on j)

where each of r1,r2,...,rn,s1,s2,...,sm appears exactly once as a remainder. Why?

34.1 Reminders (5 min)

34.2 Proof of quadratic reciprocity lemmas (50 minutes)

In order to prove

Theorem 66 (Quadratic reciprocity, Theorem 7.11)**.** *Let p and q be odd primes with $p \neq q$.*

- *if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$*
- *if $p \equiv q \equiv 3 \pmod 4$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$*

We are going to prove

Theorem 67 (Restatement of quadratic reciprocity, listed as a Comment on page 131)**.** *Let p and q be odd primes with $p \neq q$. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

In order to do that, we have to prove two technical lemmas. Today and Wednesday going to be long and technical arguments. We are going to try some fill-in-the-blank to help with following along.

The first Lemma we stated Friday.

Lemma 68 (Gauss's lemma, Theorem 7.9)**.** *Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least positive residues of the integers $a, 2a, \ldots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$. Then*

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

Now, we are going to go to breakout rooms and to look at 2, which we keep ignoring.

Breakout Room Problem. *Use Gauss's lemma to find $\left(\frac{2}{11}\right)$.*

We now prove Gauss's lemma.

Proof. Let $r_1, r_2, \ldots r_n$ be the least nonnegative residues of the integers $a, 2a, \ldots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$ and $s_1, s_2, \ldots, s_m$ be the least nonnegative residues that are less that $\frac{p}{2}$. Note that no r_i or s_j is 0, since p does not divide any of $a, 2a, \dots \frac{p-1}{2}$. Consider the $\frac{p-1}{2}$ integers given by

$$p - r_1, p - r_2, \dots, p - r_n, s_1, s_2, \dots, s_m.$$

We want to show that these integers are the integers from 1 to $\frac{p-1}{2}$ inclusive in some order. Since each integer is less than or equal to $\frac{p-1}{2}$, it suffices to show that no two of these integers are congruent modulo p.

If $p - r_i \equiv p - r_j \pmod p$ for some $i \neq j$, then $r_i \equiv r_j \pmod p$, but this implies that there exists some $k_i, k_j \in \mathbb{Z}$ such that $r_i = k_i a \equiv k_j a = r_j \pmod p$ with $k_i \neq k_j$ and $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Since $p \nmid a$ we know that the multiplicative inverse of a modulo p exists, and thus $k_i \equiv k_j \pmod p$, a contradiction. Thus, no two of the first n integers are congruent modulo p.

Similarly, no two of the second m integers are congruent. Now, if $p - r_i \equiv s_j \pmod p$, for some i and j, then $-r_i \equiv s_j \pmod p$. Thus, there exists $k_i, k_j \in \mathbb{Z}$ such that $-r_i = -k_i a \equiv k_j a = s_j \pmod p$ with $k_i \neq k_j$ and $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Since $p \nmid a$, we know that the multiplicative inverse of a modulo p exists, and thus $-k_i \equiv k_j \pmod p$, a contradiction. Thus, the $\frac{p-1}{2}$ integers $p - r_1, p - r_2, \dots, p - r_n, s_1, s_2, \dots, s_m$ are the integers $1, 2, \dots, \frac{p-1}{2}$ in some order.

Then,

$$(p - r_1)(p - r_2) \cdots (p - r_n) s_1 s_2 \cdots s_m \equiv \frac{p-1}{2}! \pmod p$$

implies that

$$(-1)^n r_1 r_2 \cdots r_n s - 1 s_2 \cdots s_m \equiv \frac{p-1}{2}! \pmod p.$$

By the definition of r_i and s_j, we have

$$(-1)^n a(2a)(3a) \cdots (\frac{p-1}{2} a) \equiv \frac{p-1}{2}! \pmod p.$$

By reordering, we have

$$(-1)^n a^{(p-1)/2} \frac{p-1}{2}! \equiv \frac{p-1}{2}! \pmod p.$$

Thus, $(-1)^n a^{(p-1)/2} \equiv 1 \pmod p$, and $a^{(p-1)/2} \equiv (-1)^n \pmod p$. By Euler's criterion, we get that $\left(\frac{a}{p}\right) \equiv (-1)^n \pmod p$. Since both sides of the congruence must be ± 1, we have $\left(\frac{a}{p}\right) = (-1)^n$. □

We are going to prove a result about $\left(\frac{2}{p}\right)$ before our next technical lemma.

Theorem 69 (Corollary 7.10)**.** *Let p be an odd prime. Then*

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

Proof. By Gauss's Lemma, we have that $\left(\frac{2}{p}\right) = (-1)^n$, where n is the number of least positive residues of the integers $2, 2 * 2, 2 * 3, \dots, 2 * \frac{p-1}{2}$ that are greater than $\frac{p}{2}$. Let $k \in \mathbb{Z}$ with $1 \leq k \leq \frac{p-1}{2}$. Then $2k < \frac{p}{2}$ if and only if $k < \frac{p}{4}$; so

Chat blast. *$\lfloor \frac{p}{4} \rfloor$ of the integers $2, 2 * 2, 2 * 3, \dots, 2 * \frac{p-1}{2}$ that are less than $\frac{p}{2}$, where $\lfloor \cdot \rfloor$ is the greatest integer (or floor) function.*

So, $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$ of these integers are greater than $\frac{p}{2}$, from which

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor}$$

by Gauss's Lemma. For the first equality, it suffices to show that

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod{2}.$$

To be finished Wednesday and on Homework 13. □

35 Wednesday, April 7: Proving quadratic reciprocity

Turn in: A lattice point is a point (x, y) in $\mathbb{R}^2$ where x and y are both integers. We can write this as (x, y) in $\mathbb{Z}^2$. Let p and q be odd primes with $p > q$. Consider the rectangle with vertices

- $O = (0, 0)$,
- $A = (\frac{(p-1)}{2}, 0)$,
- $B = (\frac{(p-1)}{2}, \frac{(q-1)}{2})$,
- $C = (0, \frac{(q-1)}{2})$.

How many lattice points are in this rectangle, including those on the edges AB and BC, but not OA or OC? Why?

35.1 Finishing proof of technical Lemmas (50 minutes)

Theorem 70 (Corollary 7.10)**.** *Let p be an odd prime. Then*

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

Proof. Monday, we got to where we needed to show:

If $p \equiv 1 \pmod{8}$, the $p = 8k + 1$ for some $k \in \mathbb{Z}$. That gives us

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

and

$$\frac{p^2-1}{8} = \frac{8k+1)^2-1}{8} = 8k^2 + 2k \equiv 0 \pmod{2}.$$

Thus, holds when $p \equiv 1 \pmod{8}$. The rest of the cases are part of Homework 13. □

Lemma 71. *Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$ and a odd. If*

$$N = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor,$$

then

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

Where $\lfloor \cdot \rfloor$ is the greatest integer (or floor) function. This gives us another way of computing Legendre symbols. Let's look at an example before diving into the technical proof.

Breakout Room Problem (5 minutes)**.** *Use this lemma to find* $\left(\frac{7}{11}\right)$. *We have*

$$\begin{aligned} N = \sum_{j=1}^{5} \left\lfloor \frac{j7}{11} \right\rfloor &= \left\lfloor \frac{7}{11} \right\rfloor + \left\lfloor \frac{14}{11} \right\rfloor + \left\lfloor \frac{21}{11} \right\rfloor + \left\lfloor \frac{28}{11} \right\rfloor + \left\lfloor \frac{35}{11} \right\rfloor \\ &= 0 + 1 + 1 + 2 + 3 \\ &= 7 \end{aligned}$$

So $\left(\frac{7}{11}\right) = (-1)^7 = -1$.

Proof. Let $r_1, r_2, \dots, r_n$ are the least nonnegative representatives of $a, 2a, 3a, \dots, \frac{p-1}{2}a$ modulo p which are greater than $\frac{p}{2}$ and $s_1, s_2, \dots, s_m$ be the least nonnegative representatives of $a, 2a, 3a, \dots, \frac{p-1}{2}a$ modulo p which are less than $\frac{p}{2}$. Then for each $j = 1, 2, \dots, \frac{p-1}{2}$ we have that

$$ja = p\left\lfloor \frac{ja}{p} \right\rfloor + (\text{remainder depending on } j)$$

where each of $r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_m$ appears exactly once as a remainder.

By adding the $\frac{p-1}{2}$ equations above, we get

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{(p-1)/2} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j \tag{7}$$

The integers $p - r_1, p - r_2, \dots, p - r_n, s_1, s_2, \dots, s_m$ are precisely the integers from 1 to $\frac{p-1}{2}$ in some order, so we have

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{n}(p - r_j) + \sum_{j=1}^{m} s_j = pn - \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j \tag{8}$$

We subtract (8) from (7) to get

$$\begin{aligned} \sum_{j=1}^{\frac{p-1}{2}} ja - \sum_{j=1}^{(p-1)/2} j &= \sum_{j=1}^{(p-1)/2} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j - \left(pn - \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j\right) \\ &= \sum_{j=1}^{(p-1)/2} p\left\lfloor \frac{ja}{p} \right\rfloor - pn + 2\sum_{j=1}^{n} r_j. \end{aligned}$$

Now, we can factor the left hand side to get

$$(\underline{\qquad\quad}) \sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{(p-1)/2} p\left\lfloor \frac{ja}{p} \right\rfloor - pn + 2\sum_{j=1}^{n} r_j.$$

Reducing both sides of the equation modulo 2 gives

$$0 \equiv \sum_{j=1}^{(p-1)/2} p\left\lfloor \frac{ja}{p} \right\rfloor - n \pmod 2$$

since $p \equiv 1 \pmod 2$. Equivalently $n \equiv \sum_{j=1}^{(p-1)/2} p\left\lfloor \frac{ja}{p} \right\rfloor \pmod 2$.

Thus, $n \equiv N \pmod 2$, thus $\left(\frac{a}{p}\right) = (-1)^n = (-1)^N$.

□

36 Friday, April 7: A return to Diophantine equations

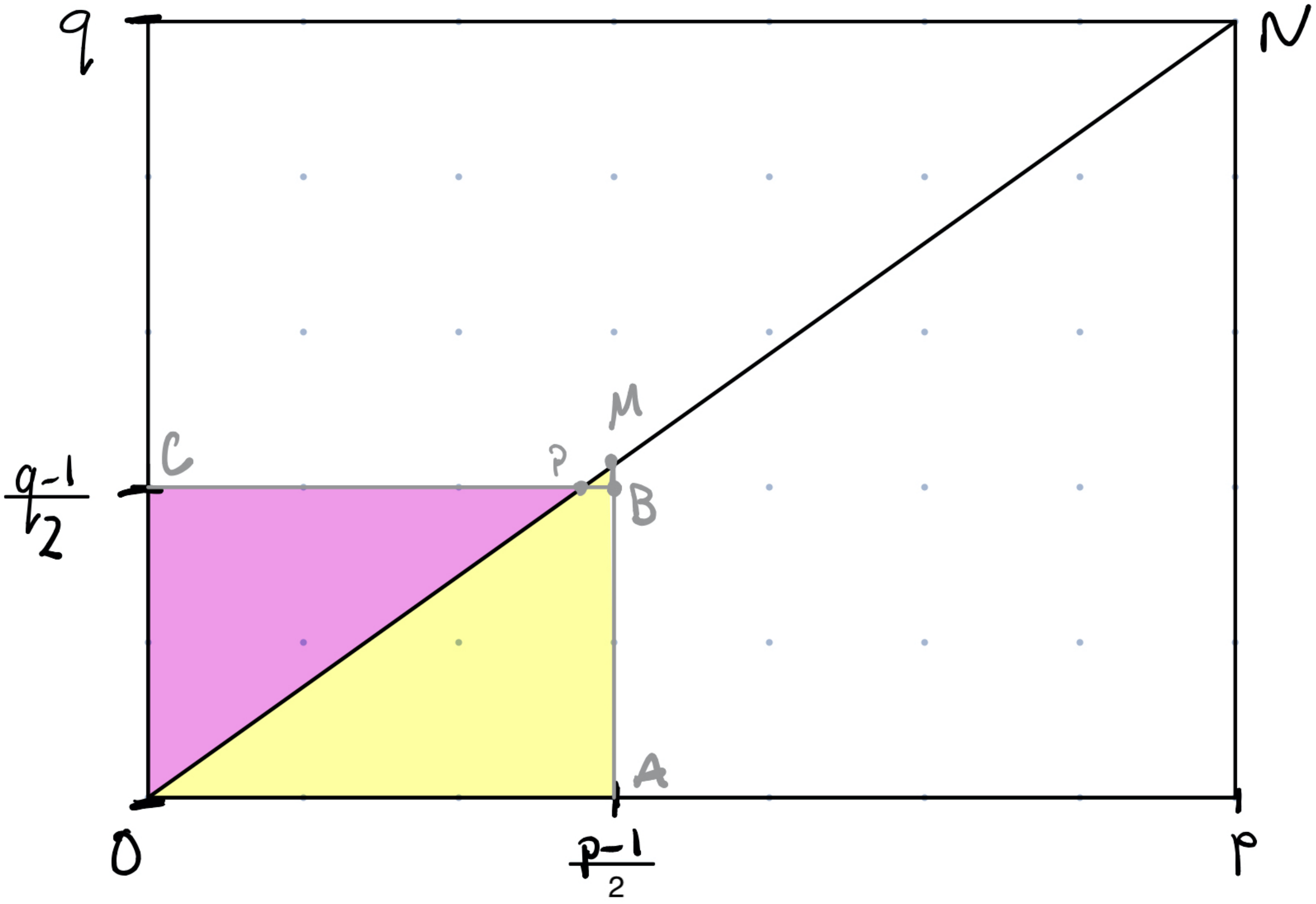
36.1 Proof of quadratic reciprocity (40 minutes)

Theorem 72 (Restatement of quadratic reciprocity)**.** *Let p and a be odd primes with $p \neq q$. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Definition. *A* lattice point *is a point $(x, y) \in \mathbb{R}^2$ where $x, y \in \mathbb{Z}$. We can write this as $(x, y) \in \mathbb{Z}^2$.*

Proof. Without loss of generality, assume that $p > q$. We draw the rectangle $O = (0, 0), A = \left(\frac{p-1}{2}, 0\right), B = \left(\frac{p-1}{2}, \frac{q-1}{2}\right)$, and $C = \left(0, \frac{q-1}{2}\right)$, like in the graphic below:



The reading assignment was to count the lattice points in the rectangle $OABC$ outlined in grey, including those on the lines AB and BC, but not those on OA or OC.

In order to count these lattice points another way, we are going to show that there are N_1 lattice points in the triangle OPC not including OC(pink) and N_2 lattice points in in OAM not including OA (yellow), thus the total number of lattice points is $N_1 + N_2$. We will find that $N_1 = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$ and $N_2 = \sum_{j=1}^{\frac{-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$. Thus, by the previous lemma, $\left\lfloor \frac{p}{q} \right\rfloor = (-1)^{N_1}$ and $\left\lfloor \frac{q}{p} \right\rfloor = (-1)^{N_2}$, which will let us finish the proof.

We will do an examples first:

Example 17. *We look at the example above with $p = 7$ and $q = 5$.*

a) The line ON has slope ______. Since p and q are distinct primes, there are no lattice points on ON except the endpoints.

b) The x-coordinate of M is ______, y-coordinate of M is______.

c) The y-coordinate of M lies between two consecutive integers ______ and ______.

Thus, the triangle PMB has no lattice points except possibly those on PB. We can then count the number of lattice points in $OABC$ by adding the number of lattice points in OCP to those in OAM.

To find N_1, the number of lattice points in OPC, not including those on OC, we count how many lattice points on the line $y = j$ are to the left of ON for $j = 1, 2, \ldots, \frac{q-1}{2}$ (in our case, this is only $j = 1, 2$.) Another was of saying this is for each j, we want the number of nonnegative integers less than

Poll question.

- $\frac{7j}{5}$
- $\frac{5j}{7}$

Thus, we have for each j, there are

Poll question.

- $\left\lfloor \frac{7j}{5} \right\rfloor$
- $\left\lfloor \frac{5j}{7} \right\rfloor$

lattice points in OPC. Then $N_1 =$

Poll question.

- $\sum_{j=1}^{2} \left\lfloor \frac{7j}{5} \right\rfloor$
- $\sum_{j=1}^{2} \left\lfloor \frac{5j}{7} \right\rfloor$

To find N_2, we use a similar counting method on OAM. Now, we count the lattice points on $x = j$ for $j = 1, 2, \ldots, \frac{p-1}{2}$. Thus, for each j, we want the number of nonnegative integers less than

Poll question.

- $\frac{7j}{5}$
- $\frac{5j}{7}$

Thus, we have for each j, there are

Poll question.

- $\left\lfloor \frac{7j}{5} \right\rfloor$
- $\left\lfloor \frac{5j}{7} \right\rfloor$

lattice points in OPC. Then $N_2 =$

Poll question.

- $\sum_{j=1}^{3} \left\lfloor \frac{7j}{5} \right\rfloor$
- $\sum_{j=1}^{3} \left\lfloor \frac{5j}{7} \right\rfloor$

Now we generalize this idea to any odd primes p and q with $p > q$.

(a) The line ON has slope $\frac{q}{p}$. Since p and q are distinct primes, there are no lattice points on ON except the endpoints.

(b) The x-coordinate of M is $\frac{p-1}{2}$, y-coordinate of M is $\frac{(p-1)}{2}\frac{q}{p} = \frac{q}{2} - \frac{q}{2p}$.

(c) The y-coordinate of M lies between two consecutive integers $\frac{q-1}{2}$ and $\frac{q+1}{2}$, since

$$\frac{q-1}{2} = \frac{q}{2} - \frac{1}{2} < \frac{q}{2} - \frac{q}{2p} < \frac{q}{2} < \frac{q+1}{2}$$

Thus, the triangle PMB has no lattice points except possibly those on PB. We can then count the number of lattice points in $OABC$ by adding the number of lattice points in OCP to those in OAM.

We will finish the proof Monday.

Contents

37 Monday, April 12: Finishing the proof of Quadratic Reciprocity and Pythagorean Triples

37.1 Finishing the proof of Quadratic Reciprocity (15 minutes)

Let's review what where we left off:

We are trying to show that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$.

From the lemma from last Wednesday, we know that for

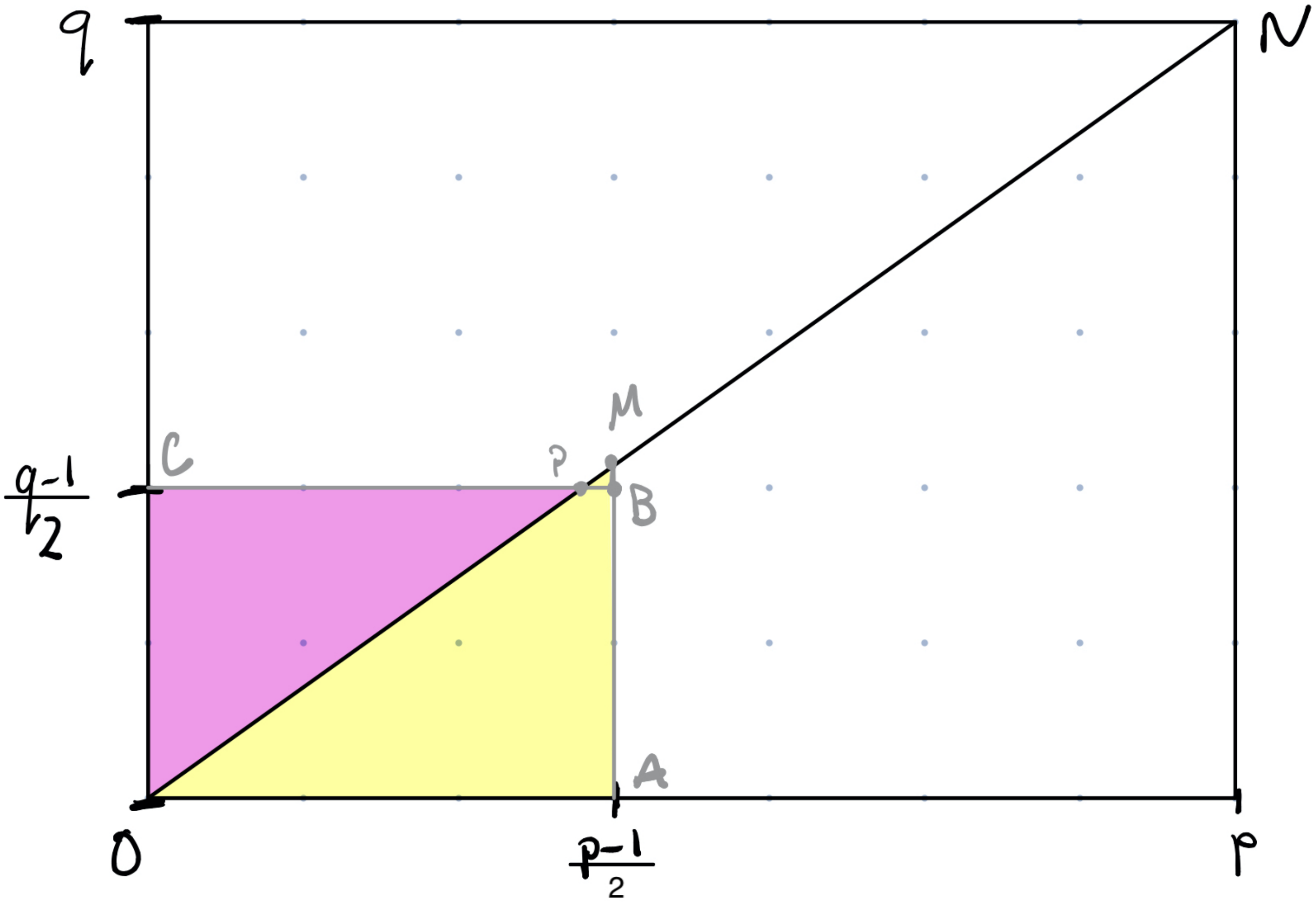
$$N_1 = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor, N_2 = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jp}{q} \right\rfloor$$

then

$$\left(\frac{q}{p}\right) = (-1)^{N_1}, \left(\frac{p}{q}\right) = (-1)^{N_2}.$$

We are trying to then show that $N_1 + N_2 = \frac{(p-1)}{2}\frac{(q-1)}{2}$.

We assumed that $p > q$ and drew the rectangle $O = (0,0), A = \left(\frac{p-1}{2}, 0\right), B = \left(\frac{p-1}{2}, \frac{q-1}{2}\right)$, and $C = \left(0, \frac{q-1}{2}\right)$, like in the graphic below:



We showed that here are $\frac{(p-1)}{2}\frac{(q-1)}{2}$. Our goal is to show that there are N_1 lattice points in the pink area and N_2 lattice points in the yellow. Last class, we showed that the triangle OMA and the quadrilateral $OPBA$ have the same number of lattice points. It is slightly easier to count points for the triangle, so we do that.

Proof. To find N_1, the number of lattice points in OPC, not including those on OC, we count how many lattice points on the line $y = j$ are to the left of ON for $j = 1, 2, \dots, \frac{q-1}{2}$. Another was of saying this is for each j, we want the number of nonnegative integers less than $\frac{jp}{q}$

Thus, we have for each j, there are $\left\lfloor \frac{jp}{q} \right\rfloor$ lattice points in OPC. Thus, in total there are $N_1 = \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{jp}{q} \right\rfloor$ lattice points in OPC.

To find N_2, we use a similar counting method on OAM. Now, we count the lattice points on $x = j$ for $j = 1, 2, \dots, \frac{p-1}{2}$. Thus, for each j, we want the number of nonnegative integers less than $\frac{jq}{p}$. Thus, we have for each j, there are $\left\lfloor \frac{jq}{p} \right\rfloor$ lattice points in OPC. Thus, in total there are $N_2 = \sum_{j=1}^{2} \left\lfloor \frac{jq}{p} \right\rfloor$ lattice points in OMA. From the previous Lemma,

$\left(\frac{p}{q}\right) = (-1)^{N_1}$ and $\left(\frac{q}{p}\right) = (-1)^{N_2}$. Thus,

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{p}{q}\right) &= (-1)^{N_1}(-1)^{N_2}\\ &= (-1)^{N_1+N_2}\\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\end{aligned}$$

with the result from the April 7 reading assignment. □

Quadratic reciprocity means that determining all quadratic residues (perfect squares) modulo an odd prime is a finite problem. In terms of Legendre symbol, this is finding all a where $\left(\frac{a}{p}\right) = 1$ for a given p. For example, when $p = 11$, we can check all positive integers a. However, what about the reverse? Quadratic reciprocity allows us to find all odd primes p where $\left(\frac{11}{p}\right) = 1$, even though there are infinitely many odd primes. This idea is also on Homework 12, Short Proofs.

37.2 Announcements (5 min)

We are going to leave quadratic reciprocity for nonprimes for independent study. Hopefully, if you need this information in the future, you have gained some of the skill of reading and working through mathematics.

In the interest of moving away from super technical topics, we are going to skip arithmetic functions and the Möbius inversion formula. This will make the last week a bit of a grab bag of number theory topics, but I want to move into Diophantine equations, which are more concrete. This will also keep us looking at things that are vaguely geometric.

We also are going to take a slightly different approach than the book, and use Pythagorean triples as our motivating example. This means we will do parts of Chapter 11 before Chapter 10.

37.3 Linear Diophantine equation review (10 minutes)

Definition. *A* Diophantine equation *is any equation in one or more variables to be solved in the integers.*

Definition. *Let $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$ with $a_1, a_2, \ldots, a_n$ not zero. A Diophantine equation of the form*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

is a linear Diophantine equation *in the n variable $x_1, \ldots, x_n$.*

The participation assignment classifies linear Diophantine equations in one variable.

The question of whether there are solutions to Diophantine equations becomes harder when there is more than one variable. Then next step is to classify Diophantine equations in two variables.

Theorem 73 (Theorem 1.13)**.** *Let $ax + by = c$ be a linear Diophantine equation in the variables x and y. Let $d = \gcd(a, b)$. If $d \nmid c$, then the equation has no solutions; if $d \mid c$, then the equation has infinitely many solutions. Furthermore, if x_0, y_0 is a particular solution of the equation, then all solution are given by $x = x_0 + \frac{b}{d}n$ and $y = y_0 - \frac{a}{d}n$ where $n \in \mathbb{Z}$.*

Breakout Room Problem (7 minutes)**.** *Find all solutions to $803x + 154y = 11$.*

37.4 Nonlinear Diophantine equations (5 minutes)

Definition. *A Diophantine equation is* nonlinear *if it is not linear.*

Example 18. *1. The Diophantine equation $x^2 + y^2 = z^2$ is our next section. Solutions are called Pythagorean triples.*

2. Let $n \in \mathbb{Z}$ with $n \geq 3$. The Diophantine equation $x^n + y^n = z^n$ is the subject of the famous Fermat's Last Theorem. We will also prove one case of this.

3. Let $n \in \mathbb{Z}$. The Diophantine equation $x^2 + y^2 = n$ tells us which integers can be represented as the sum of two squares.

4. Let $d, n \in \mathbb{Z}$. The Diophantine equation $x^2 - dy^2 = n$ is known as Pell's equation.

Sometimes we can use congruences to show that a particular nonlinear Diophantine equation has no solutions.

Example 19. *Prove that $3x^2 + 2 = y^2$ is not solvable.*

Assume that there is a solution. Then any solution to the Diophantine equation is also a solution to the congruence $3x^2 + 2 \equiv y^2 \mod 3$, which implies $2 \equiv y^2 \mod 3$, which we know is false. Thus there are no integer solutions to $3x^2 + 2 = y^2$.

Note: viewing the same equation modulo 2 says $x^2 \equiv y^2 \mod 2$, which does not give us enough information to prove a solution does not exist.

38 Wednesday, April 14: Pythagorean triples and Fermat's Last Theorem

Read Sections 6.1 The Pythagorean equation and 6.2 No solutions to a Diophantine equation through descent in Number Theory Revealed: A Master Class (Links to an external site.) (the link should take you to the start of Section 6.1)

In your own words, explain how the method of decent works.

38.1 Pythagorean triples (40 minutes)

One of the most famous math equations is $x^2 + y^2 = z^2$, probably because we learn it in high school. We are going to classify all integer solutions to the equation.

Definition. *A triple (x, y, z) of positive integers satisfying the Diophantine equation $x^2+y^2 = z^2$ is called* Pythagorean triple.

Select the Pythagorean triples:

Poll question.

- *3,4,5*
- *5,12,13*
- *-3,4,5*
- *6,8,10*
- *0,1,1*

It is actually possible to classify all Pythagorean triples, just like we did for linear Diophantine equations in two variables. To simplify this process, we will work with $x, y, z > 0$, and $(x, y, z) = 1$. For any given solution of this form, we have that $(-x, y, z), (x, -y, z), (x, y, -z), (-x, -y, z), (x, -y, -z), (-x, y, -z)$, and $(-x, -y, -z)$ are also solutions to the Diophantine equation, as is (nx, ny, nz) for any integer n. Thus, we call such a solution a *primitive Pythagorean triple.* We call $(0, n, \pm n)$ and $(n, 0, \pm n)$ the *trival solutions.*

Theorem 74. *For a primitive Pythagorean triple (x, y, z), exactly one of x and y is even.*

Proof. If x and y are both even, then z must also be even, contradicting that $(x, y, z) = 1$.

If x and y are both odd, then z is even. Now we can work modulo 4 to get a contradiction. Since x and y are odd, we have that $x^2 \equiv y^2 \equiv 1 \pmod 4$. Since z is even, we have that $z^2 \equiv 0 \pmod 4$, but $x^2 + y^2 \equiv 2 \pmod 4$.

Thus, the only remaining option is exactly one of x and y is even. □

Theorem 75. *There are infinitely many primitive Pythagorean triples x, y, z with y even. Furthermore, they are given precisely by the equations*

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

where $m, n \in \mathbb{Z}, m > n > 0, (m, n) = 1$ and exactly one of m and n is even.

Before proving this theorem, we illustrate it with some examples:

Breakout Room Problem. *(5 min)*

1. *$m = 2$ and $n = 1$ satisfy the conditions of m and n in the theorem. This gives* $(3, 4, 5)$.
2. *$m = 3$ and $n = 2$ gives* $(5, 12, 13)$.
3. *Try with your own values of m and n.*

Now we are going to prove

Theorem 76. *There are infinitely many primitive Pythagorean triples x, y, z with y even. Furthermore, they are given precisely by the equations*

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

where $m, n \in \mathbb{Z}, m > n > 0, (m, n) = 1$ and exactly one of m and n is even.

Proof. We first show that given a primitive Pythagorean triple with y even, there exist m and n as described. Since y is even, y and z are both odd. Moreover, $(x, y) = 1, (y, z) = 1$, and $(x, z) = 1$. Now,

$$y^2 = z^2 - x^2 = (x + z)(z - x)$$

implies that

$$\left(\frac{y}{2}\right)^2 = \frac{(x + z)}{2} \frac{(z - x)}{2}.$$

To show, $\left(\frac{(x+z)}{2}, \frac{(z-x)}{2}\right) = 1$, let $\left(\frac{(x+z)}{2}, \frac{(z-x)}{2}\right) = d$. Then $d \mid \frac{z+x}{2}$ and $d \mid \frac{z-x}{2}$. Thus, $d \mid \frac{z+x}{2} + \frac{z-x}{2} = z$ and $d \mid \frac{z+x}{2} - \frac{z-x}{2} = x$. Since $(x, z) = 1$, we have that $d = 1$. Thus, $\frac{(x+z)}{2}$ and $\frac{(z-x)}{2}$ are perfect squares.

Let

$$m^2 = \frac{(x + z)}{2}, \quad n^2 = \frac{(z - x)}{2}.$$

Then $m > n > 0, (m, n) = 1, m^2 - n^2 = x, 2mn = y$, and $m^2 + n^2 = z$. Also, $(m, n) = 1$ implies that not both m and n are both even. If both m and n are odd, we have that z and x are both even, but $(x, z) = 1$. This proves that every primitive Pythagorean triple has this form.

Now we prove that given any such m and n, we have a primitive Pythagorean triple. First, $(m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = (m^2 + n^2)^2$. We need to show that $(x, y, z) = 1$. Let $(x, y, z) = d$. Since exactly one of m and n is even, we have that x and z are both odd. Then d is odd, and thus $d = 1$ or d is divisible by some odd prime p. Assume that $p \mid d$. Thus, $p \mid x$ and $p \mid z$. Thus, $p \mid z + x$ and $p \mid z - x$. Thus, $p \mid (m^2 + n^2) + (m^2 - n^2) = 2m^2$ and $p \mid (m^2 + n^2) - (m^2 - n^2) = 2n^2$. Since p is odd, we have that $p \mid m^2$ and $p \mid n^2$, but $(m, n) = 1$, so $d = 1$. □

While this proof is not obvious, it does not use any concepts beyond chapter 1. Thus, this proof is considered *elementary.* Such elementary proofs often involve deep insights and intricate calculations, but no concepts beyond what we are learning in this course (and often not including things like divisor sums).

39 Friday, April 16: Fermat's Last Theorem and Sums of Squares

Read Section 9.1 in Number Theory Revealed: A Masterclass (Links to an external site.)

Turn in: Exercise 9.1.3. Find four distinct representations of 1105 = 5 (13)(17) as a sum of two squares.

39.1 Fermat's Last Theorem (35 minutes)

After the Diophantine equation $x^2 + y^2 = z^2$, one generalization is $x^n + y^n = z^n$ for $n \geq 3$. Fermat's Last Theorem was first conjectured in 1637 and proven in 1995 by Andrew Wiles. Attempts to solve this problem through the centuries have created new branches of mathematics.

Theorem 77 (Fermat's Last Theorem)**.** *The Diophantine equation $x^n + y^n = z^n$ has no nonzero integer solutions for $n \geq 3$.*

We will show that it suffices to prove Fermat's Last Theorem for the cases of n and odd prime and $n = 4$.

Theorem 78. *The Diophantine equation $x^n + y^n = z^n$ has a solution no solutions for $n \geq 3$ if and only if there are no solutions for n and odd prime or $n = 4$.*

Proof. Let $n \in \mathbb{Z}$ and $n \geq 3$. Let $n = ab$ where $a, b \in \mathbb{Z}$ and b is either an odd prime or 4. If x, y, z is a solution to $x^n + y^n = z^n$, then x^a, y^a, z^a is a solution to $x^b + y^b = z^b$. By contraposition, if $x^b + y^b = z^b$ has no solutions, then $x^n + y^n = z^n$ has no solutions. □

We will prove the case where $n = 4$ using the *method of decent.* This is the only case that Fermat proved. The next 400+ years were spent proving the theorem for odd primes.

The idea of the method of decent for proving no solution exists for a Diophantine equation is to assume a solution exists. Then use this solution to construct one that has one component that is strictly smaller than the original solution. This process could be repeated indefinitely, but it is not possible to construct an infinitely decreasing list of positive integers. Thus, no solution exists.

Theorem 79. *The Diophantine equation $x^4 + y^4 = z^2$ has not solutions in nonzero integers x, y, z.*

Chat blast. *Now why does this tell us there are no solutions to $x^4 + y^4 = z^4$?*

Proof. Assume by way of contradiction, that $x^4 + y^4 = z^2$ has a solution x_1, y_1, z_1 nonzero integers. Without loss of generality, we may assume $x_1, y_1, z_1 > 0$ and $\gcd(x_1, y_1) = 1$. We will show that there is another solution x_2, y_2, z_2 positive integers such that $\gcd(x_2, y_2) = 1$ and $0 < z_2 < z_1$. Now, $(x_1)^2, (y_1)^2, z_1$ is a Pythagorean triple with $\gcd(x_1^2, y_1^2, z_1) = 1$, and without loss of generality, y_1^2 is even. Thus, by the first theorem of the day says that there exists $m, n \in \mathbb{Z}$ such that $\gcd(m, n) = 1, m > n > 0$, and exactly one of m and n is even such that $x_1^2 = m^2 - n^2, y_1^2 = 2mn, z_1 = m^2 + n^2$. Now, $x_1^2 = m^2 - n^2$ implies $x_1^2 + n^2 = m^2$ and x_1, m, n is a Pythagorean triple with $\gcd(x_1, m, n) = 1$ and n is even. Applying the same theorem again, we get that there exists $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1, a > b > 0$, exactly one of a and b is even, with $x_1 = a^2 - b^2, n = 2ab, m = a^2 + b^2$.

We want to show that m, a and b are perfect squares. Once we have done that, we can conclude that we have constructed another solution.

Breakout Room Problem (15 minutes). *Show that m, a and b are perfect squares.*

See also: `https://ximera.osu.edu/math4573/April6/April6/April6`

Contents

40 Monday, April 19: Sums of Two Squares

40.1 Finishing Fermat's Last Theorem (10 minutes)

Theorem 80. *The Diophantine equation $x^4 + y^4 = z^2$ has not solutions in nonzero integers x, y, z.*

Chat blast. *Now why does this tell us there are no solutions to $x^4 + y^4 = z^4$?*

Note: If x, y, z is a solution to $x^4+y^4 = z^4$, then x, y, z^2 is a solution to $x^4+y^4 = z^4$. By contraposition, if $x^4+y^4 = z^2$ has no solutions, then $x^4 + y^4 = z^4$ has no solutions.

Proof. We assumed that there exists $x_1, y_1, z_1 > 0$ with $\gcd(x_1, y_1, z_1) = 1$ and $x_1^4 + y_1^4 = z_1^2$. We found $m, n \in \mathbb{Z}$ with $m > n > 0$, n even, and $x_1^2 = m^2 - n^2, y_1^2 = 2mn, z_1 = m^2 + n^2$. Now, $x_1^2 = m^2 - n^2$ implies $x_1^2 + n^2 = m^2$ and x_1, m, n is a Pythagorean triple with $\gcd(x_1, m, n) = 1$.

We then found that there exists $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1, a > b > 0$, exactly one of a and b is even, with $x_1 = a^2 - b^2, n = 2ab, m = a^2 + b^2$.

We proved that m, a, and b are perfect squares.

Thus, we have constructed another solution as desired. That is, we assumed the existence of a solution to $x^4+y^4 = z^2$ in the positive integers, we can construct another solution with a strictly smaller value of z. This is a contradiction sine there are only finitely many positive integers between a given positive integer and zero. So $x^4 + y^4 = z^2$ has no solutions on nonzero x, y, z. □

40.2 Sums of Two Squares (45 minutes)

Theorem 81 (Lemma 10.1). *Let $n_1, n_2 \in \mathbb{Z}$ with $n_1, n_2 > 0$. If n_1 and n_2 are expressible as the sum of two squares of integers, then $n_1 n_2$ is expressible as the sum of two squares of integers.*

Example 20. *Since $13 = 3^2 + 2^2$ and $17 = 4^2 + 1^2$ are each expressible as the sum of two squares, $13 * 17 = 221 = 14^2 + -5^2$.*

Breakout Room Problem (5 minutes). *Prove this theorem Let $a, b, c, d \in \mathbb{Z}$ such that $n_1 = a^2 + b^2$ and $n_2 = c^2 + d^2$. Then $n_1 n_2 = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$.*

We will prove that every prime that congruent to 1 (mod 4) is expressible as the sum of two squares.

Theorem 82 (Primes as sums of squares). *If p is a prime such that $p \equiv 1 \pmod 4$, then there exists $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}$ and $0 < k < p$.*

Proof. Since $p \equiv 1 \pmod 4$, we have that $\left(\frac{-1}{p}\right) = 1$. Thus, there exists $x \in \mathbb{Z}$ with $0 < x \le \frac{p-1}{2}$ such that $x^2 \equiv -1 \pmod p$. Then, $p \mid x^2 + 1$, and we have that $x^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Thus, we found x and $y = 1$. Since $x^2 + 1$

and p are positive, so is k. Also,

$$kp = x^2 + y^2 < \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$. □

Breakout Room Problem (5 minutes)**.** *If $n \equiv 3 \pmod 4$, then n cannot be written as the sum of two squares.*

Solution. The options for squares mod 4 are $1^2 \equiv 3^2 \equiv 1 \pmod 4$ and $0^2 \equiv 2^2 \equiv 0 \pmod 4$. Then the options for $x^2 + y^2$ are $0, 1, 2 \pmod 4$. □

The next theorem will prove that primes $p \equiv 1 \pmod 4$ and $p = 2$ can be written as the sum of two square integers.

Theorem 83 (Theorem 10.2)**.** *If p is a prime number such that $p \not\equiv 3 \pmod 4$, then p is expressible as the sum of two squares of integers.*

Proof. When $p = 2 = 1^2 + 1^2$, we are done.

Assume that $p \equiv 1 \pmod 4$. Let m be the least integer such that there exists $x, y \in \mathbb{Z}$ with $x^2 + y^2 = mp$ and $0 < m < p$ as in the previous theorem. We show that $m = 1$. Assume, by way of contradiction, that $m > 1$. Let $a, b \in \mathbb{Z}$ such that

$$a \equiv x \pmod m, \qquad \frac{-m}{2} < a \leq \frac{m}{2}$$

and

$$b \equiv y \pmod m, \qquad \frac{-m}{2} < b \leq \frac{m}{2}.$$

Then

$$a^2 + b^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod m,$$

and so there exists $k \in \mathbb{Z}$ with $k > 0$ such that $a^2 + b^2 = km$. (Why?)

Now,

$$(a^2 + b^2)(x^2 + y^2) = (km)(mp) = km^2p.$$

By Lemma 10.1, $(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$, so $(ax + by)^2 + (ay - bx)^2 = km^2p$.

41 Wednesday, April 21: Sums of Two or Three Squares

Turn in

Why can $x^2 + y^2 + z^2$ never be 7 mod 8?

Let $4^m(8n + 7) = x^2 + y^2 + z^2$ for $m > 0$. Why are x, y, and z all even?

41.1 Finishing Sum of Two Squares (20 minutes)

Since $a \equiv x \pmod m$ and $b \equiv y \pmod m$,

$$ax + by \equiv x^2 + y^2 \equiv 0 \pmod m$$

and

$$ay - bx \equiv xy - yx \equiv 0 \pmod m$$

so $\frac{ax+by}{m}, \frac{ay-bx}{m} \in \mathbb{Z}$ and

$$\left(\frac{ax + by}{m}\right)^2 + \left(\frac{ay - bx}{m}\right)^2 = \frac{km^2p}{m^2} = kp.$$

Now, $\frac{-m}{2} < a \leq \frac{m}{2}$ and $\frac{-m}{2} < b \leq \frac{m}{2}$ imply that $a^2 \leq \frac{m^2}{4}$ and $b^2 \leq \frac{m^2}{4}$. Thus, $km = a^2 + b^2 \leq \frac{m^2}{2}$. Thus, $k \leq \frac{m}{2} < m$, but this contradicts that m is the smallest such integer.

Thus, $m = 1$. □

We finish with a characterization of which integers are expressible as the sum of two square integers and some examples.

Theorem 84 (Theorem 10.3)**.** *Let $n \in \mathbb{Z}$ with $n > 0$. Then n is expressible as the sum of two squares if and only if every prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n.*

Proof. ($\Rightarrow$) Assume that p is an odd prime number and that $p^{2i+1}, i \in \mathbb{Z}$ occurs in the prime factorization of n. We will show that $p \equiv 1 \pmod 4$. Since n is expressible as the sum of two squares of integers, there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + y^2$. Let $(x, y) = d, a = \frac{x}{d}, b = \frac{y}{d}$ and $m = \frac{n}{d^2}$. Then $(a, b) = 1$ and $a^2 + b^2 = m$. Let $p^j, j \in \mathbb{Z}$ be the largest power of p dividing d. Then $p^{(2i-1)-2j} \mid m$; since $(2i + 1) - 2j) \geq 1$, we have $p \mid m$. Now, $p \nmid a$ since $(a, b) = 1$. Thus, there exists $z \in \mathbb{Z}$ such that $az \equiv b \pmod p$. Then $m = a^2 + b^2 \equiv a^2 + (az)^2 \equiv a^2(1 + z^2) \pmod p$.

Since $p \mid m$, we have

$$a^2(1 + z^2) \equiv 0 \pmod p$$

or $p \mid a^2(1 + z^2)$ or $z \equiv -1 \pmod p$. Thus, -1 is a quadratic residue modulo p, so $p \equiv 1 \pmod 4$. By contrapositive, any prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n as desired.

($\Leftarrow$) Assume that every prime factor of n congruent to 3 modulo 4 occurs to an even power in the prime factorization of n. Then n can be written as $n = m^2 p_1 p_2 \ldots p_r$ where $m \in \mathbb{Z}$ and $p_1, p_2, \ldots, p_r$ are distinct prime numbers equal to 2 or equivalent to 1 modulo 4. Now, $m^2 = m^2 + 0^2$, so is expressible as the sum of two squares, and each p_1 is also expressible as the sum of two squares by the theorem labeled Primes as Sums of Squares. Thus, by the first theorem of the day, n is expressible as the sum of two squares. □

Example 21. *Determine whether 374^{695} is expressible as the sum of two squares. The prime factorization of 374 is $2 * 11 * 17$. So $374^{695} = 2^{695}11^{695}17^{695}$*

Poll question. *Is 374^{695} expressible as the sum of two squares?*

Example 22. *Express 4410 as the sum of two squares by splitting into factors that can be written as the sum of two squares.*

The prime factorization of 4410 is $2 * 3^2 * 5 * 7^2$. We group this into $4410 = (2 * 7^2)(3^2 * 5) = 98 * 45$. By inspection, the larger of these factors is $98 = 7^2 + 7^2$ and the smaller is $45 = 6^2 + 3^2$.

The method from the participation assignment gives $4410 = 63^2 + 21^2$.

We finish out the sums of squares section by classifying which integers can be written as the sum of three squares and sum of four squares. These cases are more difficult than the sum of two squares since there is no formula analogous to the April 8 participation assignment.

42 Friday, April 21: Sums of Four Squares

42.1 Sums of Three Squares (20 minutes)

Theorem 85 (Sum of three squares necessary condition)**.** *Let $m, n \in \mathbb{Z}$ with $m, n \geq 0$. If $N = 4^m(8n + 7)$, then N can not be written as the sum of 3 squares.*

Proof. We start by proving the $m = 0$ case. In order to get a contradiction, assume that $N = 8n + 7$ can be written as the sum of three squares. Thus, there exists $x, y, z \in \mathbb{Z}$ such that

$$8n + 7 = x^2 + y^2 + z^2.$$

Now, $8n+7 \equiv 7 \pmod 8$ and $x^2+y^2+z^2 \not\equiv 7 \pmod 8$ (by participation assignment), which gives the contradiction we are looking for.

Now we assume $m > 0$. and again assume $N = 4^m(8n+7)$ can be written as the sum of three squares. As before, there exist $x, y, z \in \mathbb{Z}$ such that

$$4^m(8n+7) = x^2+y^2+z^2$$

and x, y, z are even (by participation assignment). So there exists x', y' and z' such that $x = 2x', y = 2y'$, and $z = 2z'$. Substituting into our definition of N, we get

$$4^{m-1}(8n+7) = (x')^2+(y')^2+(z')^2.$$

Repeating this process $m-1$ times, we find $8n+7$ is expressible as a sum of three squares, a contradiction. Thus, $N = 4^m(8n+7)$ cannot be written as the sum of three squares. □

Now, the converse is true. Legendre proved this in 1798, but is much harder to prove, due to the lack of formula like the one from Lemma 10.1. Note that any integer that cannot be written as the sum of three squares cannot be written as the sum of two squares.

Example 23. *Determine whether* 1584 *is expressible as the sum of three squares.*

The highest power of 4 *that divides* 1584 *evenly is* 16*, leaving* $99 \equiv 3 \pmod 8$. *Thus,* 1584 *can be written as the sum of three squares:*

Poll question. - *True*

- *False*
- *Not enough information*

Since this also allows us to factor 1584*, we also know* 1584 *can be written as the sum of two squares:*

Poll question. - *True*

- *False*
- *Not enough information*

42.2 Sums of Four Squares (15 minutes)

We now prove that all positive integers can be written as the sum of four squares. The new few results are similar to the proof of the sum of two squares. Some of these calculations are even more involved, but still use multiplication and factoring. I will upload a scan of the sums of squares section from *Elementary Number Theory* by James K. Strayer. All of the missing calculations are expanding and refactoring polynomial expression.

Theorem 86 (Euler, Lemma 10.5)**.** *Let $n_1, n_2 \in \mathbb{Z}$ with $n_1, n_2 > 0$. If n_1 and n_2 are expressible as the sum of four squares, then so is $n_1 n_2$.*

Proof. Let $a, b, c, d, w, x, y, u \in \mathbb{Z}$ such that

$$n_1 = a^2+b^2+c^2+d^2$$

and

$$n_1 = w^2+x^2+y^2+z^2.$$

Then

$$n_1 n_2 = (aw+bx+cy+dz)^2+(-ax+bw-cz+dy)^2+(-ay+bz+cw-dx)^2+(-az-by+cx+dw)^2$$

as desired. □

Theorem 87 (Also Euler)**.** *If p is an odd prime number, then there exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 + 1 = kp$ for some $k \in \mathbb{Z}$ with $0 < k < p$.*

Proof. We consider two cases.

Case 1: $p \equiv 1 \pmod 4$.

Breakout Room Problem (10 minutes)**.** *Prove this case.*

Then $\left(\frac{-1}{p}\right) = 1$, so there exists $x \in \mathbb{Z}$ with $0 < x \leq \frac{p-1}{2}$ such that $x^2 \equiv -1 \pmod p$. Then, $p \mid x^2 + 1$, and we have that $x^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Thus, we found x and $y = 0$. Since $x^2 + 1$ and p are positive, so is k. Also,

$$kp = x^2 + 1 < \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$.

Case 2: $p \equiv 3 \pmod 4$. Let a be the least positive quadratic nonresidue modulo p. Note that $a \geq 2$. Then

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

and so there exists $x \in \mathbb{Z}$ with $0 < x \leq \frac{p-1}{2}$ such that $x^2 \equiv -a \pmod p$. Now, $a - 1$ is positive and less than a, then $a - 1$ is a quadratic residue modulo p. Thus, there exists $y \in \mathbb{Z}$ with $0 < y \leq \frac{p-1}{2}$ such that $y^2 \equiv a - 1 \pmod p$. Thus,

$$x^2 + y^2 + 1 \equiv (-a) + (a - 1) + 1 \equiv 0 \pmod p$$

or, equivalently, $x^2 + y^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Again, $k > 0$. Furthermore,

$$kp = x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$. □

We will prove that every prime number can be written as the sum of four squares.

Theorem 88 (Lagrange, 1770)**.** *All prime numbers can be written as the sum of four squares.*

Proof. When $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$, we are done. In fact, we can also writes a prime p where $p \equiv 1 \pmod 4$ as $p = x^2 + y^2 + 0^2 + 0^2$, but the following method works for all odd primes.

Let m be the least positive integer where $x^2 + y^2 + z^2 + w^2 = mp$ and $0 < m < p$. We want to show that $m = 1$. To get a contradiction, assume $m > 1$. We consider two cases.

Case 1: m even. There are three posibilities: w, x, y, z are all even; w, x, y, z are all odd; two of w, x, y, z are odd and the other two are even. In all three cases, we can assume $w \equiv x \pmod 2$ and $y \equiv z \pmod 2$. Then $\frac{w+x}{2}$, $\frac{w-x}{2}$, $\frac{y+z}{2}$, $\frac{y-z}{2}$ are integers and

$$\left(\frac{w+x}{2}\right)^2 + \left(\frac{w-x}{2}\right)^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 = \frac{mp}{2}$$

which contradicts the fact that m is minimal.

Case 2: m is odd. Skip! Repeat argument that $p \equiv 1 \pmod 4$ can be written as the sum of two squares.

Then $m \geq 3$. Let $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{aligned} a &\equiv w \pmod{m}, \frac{-m}{2} < a < \frac{m}{2} \\ b &\equiv x \pmod{m}, \frac{-m}{2} < b < \frac{m}{2} \\ c &\equiv y \pmod{m}, \frac{-m}{2} < c < \frac{m}{2} \\ d &\equiv z \pmod{m}, \frac{-m}{2} < d < \frac{m}{2}. \end{aligned}$$

Then $a^2 + b^2 + c^2 + d^2 \equiv w^2 + x^2 + y^2 + z^2 \equiv mp \equiv 0 \pmod{m}$ and so there exists $k \in \mathbb{Z}$ with $k > 0$ such that $a^2 + b^2 + c^2 + d^2 = km$. Now

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = (km)(mp) = km^2 p.$$

By theorem 2 from today, we can rewrite $a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2)$ as the sum of four squares $(aw + bx + cy + dz)^2 + (-ax + bw - cz + dy)^2 + (-ay + bz + cw - dx)^2 + (-az - by + cx + dw)^2 = km^2 p$. Since $a \equiv w \pmod{m}, b \equiv x \pmod{m}, c \equiv y \pmod{m}, \frac{-m}{2} < c < \frac{m}{2}, d \equiv z \pmod{m}, \frac{-m}{2} < d < \frac{m}{2}$, we have

$$\begin{aligned} aw + bx + cy + dz &\equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{m} \\ -ax + bw - cz + dy &\equiv -wx + xw - yz + zy \equiv 0 \pmod{m} \\ -ay + bz + cw - dx &\equiv -wy + yw + xz - zx \equiv 0 \pmod{m} \\ -az - by + cx + dw &\equiv -wx + zw - xy + yx \equiv 0 \pmod{m} \end{aligned}$$

Let $W = \frac{w^2+x^2+y^2+z^2}{m}, X = \frac{-wx+xw-yz+zy}{m}, Y = \frac{-wy+yw+xz-zx}{m}, Z = \frac{-wx+zw-xy+yx}{m}$. Then $W^2 + X^2 + Y^2 + Z^2 = \frac{km^2p}{m^2} = kp$. Since $\frac{-m}{2} < a, b, c, d < \frac{m}{2}$, then $a^2, b^2, c^2, d^2 < \frac{m^2}{4}$. Thus,

$$km = a^2 + b^2 + c^2 + d^2 < \frac{4m^2}{4}$$

and $k < m$. This contradicts that m is the smallest such integers.

Thus, $m = 1, w^2 + x^2 + y^2 + z^2 = p$. □

Theorem 89 (Lagrange, Theorem 10.6)**.** *All positive integers can be written as the sum of four squares.*

Proof. Let $n \in \mathbb{Z}$ with $n > 1$. If $n = 1 = 1^2 + 0^2 + 0^2 + 0^2$. If $n > 1$, then n is the product of primes by the Fundamental Theorem of Arithmetic. By the previous theorem, every prime number can be written as the sum of four squares. By theorem 2 from today, n is can be written by the sum of four squares. □

We finish this section with a few famous problems.

Example 24 (Waring's Problem, 1770)**.** *Let $k \in \mathbb{Z}$ with $k > 0$. Does there exist a minimum integer $g(k)$ such that every positive integer can be written as the sum of at most $g(k)$ nonnegative integers to the k^{th} power?*

For example, $g(1) = 1$. Today we showed that $g(2) = 4$. The next step would be to find if $g(3)$ exists and what it equals.

Theorem 90 (Hilbert, 1906)**.** *Let $k \in \mathbb{Z}$ with $k > 0$. There exists a minimal integer $g(k)$ such that every positive integer can be written as the sum of at most $g(k)$ nonnegative integers to the k^{th} power.*

The proof of Hilbert's theorem does not provide a formula for $g(k)$, merely proves it exists. Numerical evidence suggests $g(k) = \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + 2^k - 2$. It's been proven that there are only finitely many (or 0) k where the formula does not hold, and the formula holds when $k \leq 471{,}600{,}000$. Thus, $g(3) = 9, g(4) = 19$, and $g(5) = 37$. Proofs of these facts come from analytic number theory.