Monday February 5: More facts about greatest common divisor and primes

Learning Objectives. By the end of class, students will be able to:

- Find the solutions to a specific Diophantine equation in three variables
- Prove that when a Diophantine equation in three variables has a solutions, it has infinitely many. .

Reading Strayer Section 1.5.

Turn in (a) The proof of Theorem 1.19 ends with "the cases $a = 1$ and $b > 1$, $a > 1$ and $b = 1$, and $a = b = 1$ are easily checked and are left as exercises. Do this.

(b) For Corollary 1.20, the book states "The (extremely easy) proof is left as an exercise for the reader." Complete this proof.

Solution: (a) When $a = 1$ and $b > 1$, then $(a, b) = 1$ and $[a, b] = b$. Then $(a, b)[a, b] = b = ab$. Similarly for $a > 1, b = 1$. When $a = b = 1$, then $(a, b) = [a, b] = 1$ and $(a, b)[a, b] = 1 = ab$.

(b) From Theorem 1.19, we know that $\gcd(a, b)\,\mathrm{lcm}[a, b] = ab$. Since $\gcd(a, b), \mathrm{lcm}[a, b]$, and ab are all positive, $\mathrm{lcm}[a, b] = \dfrac{ab}{\gcd(a, b)}$ if and only if $\gcd(a, b) = 1$.

Greatest common divisor and Diophantine equations (30 minutes)

Finish proof from Friday–end of notes from Week 3.

Proposition 1. *Let $a, b, c, d \in \mathbb{Z}$ and let $ax + by + cz = d$ be a linear Diophantine equation. If $(a, b, c) \nmid d$, then the equation has no solutions. If $(a, b, c) \mid d$, then there are infinitely many solutions.*

In-class Problem 1 *Find integral solutions to the Diophantine equation*

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

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

(b) *The linear Diophantine equation $8x_1 - 4x_2 = 4y$ has infinitely many solutions for all $y \in \mathbb{Z}$ by Theorem 6.2. Substituting into the original Diophantine equation gives $4y + 6x_3 = 6$, which has infinitely many solutions by Theorem 6.2, since $(4, 6) = 2 \mid 6$. Find them.*

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

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

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

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

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

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

Proof of Proposition 1 Let $a, b, c, d \in \mathbb{Z}$ and let $ax + by + cz = d$ be a linear Diophantine equation. If $(a, b, c) \mid d$, let $e = (a, b)$. Then

$$ax + by = ew \tag{1}$$

has a solution for all $w \in \mathbb{Z}$ by Theorem 6.2. Similarly, the linear Diophantine equation

$$ew + cz = d \tag{2}$$

has infinitely many solutions by Theorem 6.2, since $(e, c) = (a, b, c)$ by the Lemma 1 and $(a, b, c) \mid d$ by assumption. These solutions have the form

$$w = w_0 + \frac{cn}{(a, b, c)}, \quad z = z_0 - \frac{en}{(a, b, c)}, \qquad n \in \mathbb{Z},$$

where w_0, z_0 is a particular solution. Let x_0, y_0 be a particular solution to

$$ax + by = ew_0.$$

Then the general solution is

$$x = x_0 + \frac{bm}{e}, \quad y = y_0 - \frac{am}{e}, \qquad m \in \mathbb{Z}.$$

To verify that these formulas for x, y, and z give solutions to $ax + by + cz = d$, we substitute into equation 2 then 1

$$\begin{aligned} e\left(w_0 + \frac{cn}{(a, b, c)}\right) + c\left(z_0 - \frac{en}{(a, b, c)}\right) &= d \\ ew_0 + cz_0 &= d \\ a\left(x_0 + \frac{bm}{e}\right) + b\left(y_0 - \frac{am}{e}\right) + cz_0 &= d \\ ax_0 + by_0 + cz_0 &= d. \end{aligned}$$

When $(a, b, c) \nmid d$, $\dfrac{a}{(a, b, c)}, \dfrac{b}{(a, b, c)}, \dfrac{c}{(a, b, c)} \in \mathbb{Z}$ by definition, but $\dfrac{d}{(a, b, c)}$ is not an integer. Therefore, there are no integers such that

$$\frac{a}{(a, b, c)}x + \frac{b}{(a, b, c)}y + \frac{c}{(a, b, c)}z = \frac{d}{(a, b, c)}.$$

■

Wednesday February 7: Arithmetic progressions and introduction to Congruences

Learning Objectives. By the end of class, students will be able to:

- State and prove facts about prime factorizations using the Fundamental Theorem of Arithmetic
- Prove there are infinitely many primes of the form $4n+3$.
- Prove a given set is an equivalence relation .

Reading Strayer, Appendix B

Turn in Let R be the equivalence relation on $\mathbb{R}$ defined by

$$[a] = \{b \in \mathbb{R} : \sin(a) = \sin(b) \text{ and } \cos(a) = \cos(b)\}.$$

Prove that R is an equivalence relation on $\mathbb{R}$. Describe the equivalence classes on $\mathbb{R}$

Solution: Since $\sin(a) = \sin(a)$ and $\cos(a) = \cos(a)$, the relation R is reflexive.

If $\sin(a) = \sin(b)$ and $\cos(a) = \cos(b)$, the $\sin(b) = \sin(a)$ and $\cos(b) = \cos(a)$, so the relation is symmetric.

If $\sin(a) = \sin(b)$ and $\cos(a) = \cos(b)$, $\sin(b) = \sin(c)$ and $\cos(b) = \cos(c)$, then $\sin(a) = \sin(c)$ and $\cos(a) = \cos(c)$ is transitive.

Note that $\sin(a) = \sin(b)$ if $b = a + 2\pi k$ or $b = -a + \pi + 2\pi k$ for some $k \in \mathbb{Z}$, and $\cos(a) = \cos(b)$ if $b = a + 2\pi k$ or $b = -a + 2\pi k$ for some $k \in \mathbb{Z}$. These conditions are both true with $b = a + 2\pi k$. Thus, for $a \in [0, 2\pi)$,

$$[a] = \{\dots, a - 4\pi, a - 2\pi, a, a + 2\pi, a + 4\pi, \dots\}.$$

Practice with gcd proofs (20 minutes)

Finish proof from Monday.

In-class Problem 2 *(a) Do there exist integers x and y such that $x + y = 100$ and $(x, y) = 8$?*

Solution: *On Homework 3.*

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

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

Proof *Let $x \in \mathbb{Z}$ with $\boxed{\text{On Homework 3}}$. Let $y = \square$. Then $3 \mid y$ by $\boxed{\text{On Homework 3}}$. Then $(x, y) = 3$ since $\boxed{\text{On Homework 3}}$. Thus, there are infinitely many $x, y \in \mathbb{Z}$ $\boxed{\text{On Homework 3}}$.*

■

In-class Problem 3 *Let a and b be relatively prime integers. Prove that $(a+b, a-b)$ is either 1 or 2.*

Using the hint in the back of the book and Exercise 37, which states $(ca, cb) = |c|(a, b)$ for all $a, b \in \mathbb{Z}$, not both 0.

Proof *Let $(a+b, a-b) = d$ and note that $d \mid (a+b)+(a-b)$ and $d \mid (a+b)-(a-b)$ by* $\boxed{\text{linear combination}}$ $\boxed{\text{On Homework 3}}$ ■

Prime factorizations (20 minutes)

Note on $m^4 - n^4 = (m^2 - n^2)(m^2 + n^2)$: In order to sho w this is not prime, must prove that the factors cannot be 1 and the number itself. Hint: show that if one of the factors is 1 the other is 1 or 0 (or -1).

Corollary (Corollary 1.20)**.** *Let $a, b \in \mathbb{Z}$ with $a, b > 0$. Then $[a, b] = ab$ if and only if $(a, b) = 1$.*

A note on "if and only if" proofs:

- You can do two directions:
  - If $[a, b] = ab$, then $(a, b) = 1$.
  - If $(a, b) = 1$, then $[a, b] = ab$.
- Sometimes you can string together a series of "if and only if statements." Definitions are always "if and only if," even though rarely stated that way. For example, an integer n is even if and only if there exist an integer m such that $n = 2m$:
  - An integer n is even if and only if $2 \mid n$ (definition of even)
  - if and only if there exist an integer m such that $n = 2m$ (definition of $2 \mid n$).

Theorem (Dirichlet's Theorem)**.** *Let $a, b \in \mathbb{Z}$ with $a, b > 0$ and $(a, b) = 1$. Then the arithmetic progression*

$$a, a+b, a+2b, \ldots, a+nb, \ldots$$

contains infinitely many primes.

Surprisingly, this proof involves complex analysis. The statement that there are infinitely many prime numbers is the case $a = b = 1$.

Warning 1. *You may not use this result to prove special cases, ie, specific values of a and b.*

Lemma (Lemma 1.23)**.** *If $a, b \in \mathbb{Z}$ such that $a = 4m + 1$ and $b = 4n + 1$ for some integers m and n, then ab can also be written in that form.*

We will not go over the proof in class.

Proof Let $a = 4m + 1$ and $b = 4n + 1$ for some integers m and n. Then

$$\begin{aligned} ab &= (4m+1)(4n+1) \\ &= 16mn + 4m + 4n + 1 \\ &= 4(4mn + m + n) + 1. \end{aligned}$$

■

Proposition (Proposition 1.22)**.** *There are infinitely may prime numbers expressible in the form $4n+3$ where n is a nonnegative integer.*

Proof (Similar to the proof that there are infinitely many prime numbers). Assume, by way of contradiction, that there are only finitely many prime numbers of the form $4n+3$, say $p_0 = 3, p_1, p_2, \ldots, p_r$, where the p_i are distinct. Let $N = 4p_1p_2 \cdots p_r + 3$. If every prime factor of N has the form $4n+1$, then so does N, by repeated applications of Lemma 1.23. Thus, one of the prime factors of N, say p, have the for $4n+3$. We consider two cases:

Case 1, $p = 3$: If $p = 3$, then $p \mid N - 3$ by linear combinations. Then $p \mid 4p_1p_2 \cdots p_r$. Then by Corollary 1.15, either $3 \mid 4$ or $3 \mid p_1p_2 \cdots p_r$. This implies that $p \mid p_i$ for some $i = 1, 2, \ldots, r$. However, $p_1, p_2, \ldots, p_r$ are distinct primes not equal to 3, so this is not possible. Therefore, $p \neq 3$.

Case 2, $p = p_i$ for some $i = 1, 2, \ldots, r$: If $p = p_i$, then $p \mid N - 4p_1p_2 \cdots p_r$ by linear combinations. Then $p \mid 3$. However, $p_1, p_2, \ldots, p_r$ are distinct primes not equal to 3, so this is not possible. Therefore, $p \neq p_i$ for $i = 1, 2, \ldots, r$.

Therefore, N has a prime divisor of the form $4n+3$ which is not on the list $p_0, p_1, \ldots, p_r$, which contradicts the assumption that $p_0, p_1, \ldots, p_r$ are all primes of this form. Thus, there are infinitely many primes of the form $4n+3$. ■

Equivalence Relation Practice (10 minutes)

In-class Problem 4 *Prove that*

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

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

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

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

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

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

and $y \in \{b \in \mathbb{Z} : 3 \mid (a{-}b)\}$. $\boxed{\text{Since the relation is reflexive, symmetric, and transitive, it is an equivalence relation.}}$

■

Friday, February 9: Modular arithmetic

Learning Objectives. By the end of class, students will be able to:

- Prove that congruence modulo m is an equivalence relation on $\mathbb{Z}$.
- Define a complete residue system.
- Practice using modular arithmetic. .

Reading Strayer, Section 2.1 through Example 1.

Turn in The book concludes the section with a caution about division. It states that $6a \equiv 6b \pmod 3$ for all integers a and b. Explain why this is true.

Solution: Since $3 \mid 6a - 6b = 3(2a - 2b)$, $6a \equiv 6b \pmod 3$ for all integers a and b.

Quiz (10 min)

Definitions and examples of (mod m) (20 minutes)

Definition (divisibility definition of $a \equiv b \pmod m$)**.** Let $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a is *congruent to* b *modulo* m and write $a \equiv b \pmod m$ if $m \mid b - a$, and m is said to be the *modulus of the congruence.* The notation $a \not\equiv b \pmod m$ means a is not congruent to b modulo m, or a is *incongruent to* b *modulo* m.

Definition (remainder definition of $a \equiv b \pmod m$)**.** Let $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a is congruent to b modulo m if a and b have the same remainder when divided by m.

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

Proposition 2 (Definitions of congruence modulo m are equivalent)**.** *These two definitions are equivalent. That is, for $a, b, m \in \mathbb{Z}$ with $m > 0$, $m \mid b - a$ if and only if a and b have the same remainder when divided by m.*

Proof Let $a, b, m \in \mathbb{Z}$ with $m > 0$. By the Division Algorithm, there exists $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$aq_1m + r_1, 0 \leq r_1 < m, \text{ and}$$
$$bq_2m + r_2, 0 \leq r_2 < m.$$

If $m \mid b - a$, then by definition, there exists $k \in \mathbb{Z}$ such that $mk = b - a$. Thus, $mk = q_2m + r_2 - q_1m - r_1$. Rearranging, we get $m(k - q_2 + q_1) = r_2 - r_1$ and $m \mid r_2 - r_1$. Since $0 \leq r_1 < m, 0 \leq r_2 < m$, we have $-m < r_2 - r_1 < m$. Thus, $r_2 - r_1 = 0$, so a and b have the same remainder when divided by m.

In the other direction, if $r_1 = r_2$, then $a - b = q_1m - q_2m = m(q_1 - q_2)$. Thus, $m \mid a - b$. ■

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 3 or larger numbers. Instead of "divisible" or "not divisible" we have several gradations.

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.

Example 1. *We will eventually find a function that generates all integers solutions to the equation* $a^2+b^2=c^2$ *(this can be done with only divisibility, so feel free to try for yourself after class).*

Modular arithmetic allows us to say a few things about solutions.

First, let's look at $\pmod{2}$. *Note that* $0^2 \equiv 0 \pmod{2}$ *and* $1^2 \equiv 1 \pmod{2}$*.*

- **Case 1:** $c^2 \equiv 0 \pmod{2}$ *In this case,* $c \equiv 0 \pmod{2}$ *and either* $1^2+1^2 \equiv 0 \pmod{2}$ *or* $0^2+0^2 \equiv 0 \pmod{2}$*. So, we know* $a \equiv b \pmod{2}$. (Note: $\pmod{4}$ will eliminate the $a \equiv b \equiv 1 \pmod{2}$ case)

- **Case 2:** $c^2 \equiv 1 \pmod{2}$ *In this case,* $c \equiv 1 \pmod{2}$ *and either* $0^2+1^2 \equiv 1 \pmod{2}$*. So, we know* $a \not\equiv b \pmod{2}$.

Let's start with $\pmod{3}$. *Note that* $0^2 \equiv 0 \pmod{3}$*,* $1^2 \equiv 1 \pmod{3}$*, and* $2^2 \equiv 1 \pmod{3}$*.*

Case 1: $c^2 \equiv 0 \pmod{3}$**.** *In this case,* $c \equiv 0 \pmod{3}$ *and* $0^2+0^2 \equiv 0 \pmod{3}$*. So, we know* $a \equiv b \equiv c \equiv 0 \pmod{3}$.

Case 2: $c^2 \equiv 1 \pmod{3}$**.** *In this case,* c *could be* 1 *or* 2 *modulo* 3*. We also know* $0^2+1^2 \equiv 1 \pmod{3}$*, so* $a \not\equiv b \pmod{3}$.

Case 3: $c^2 \equiv 2 \pmod{3}$ *has no solutions.*

So at least one of a, b, c *is even, and at least one is divisible by* 3*.*

We can use the idea of congruences to simplify divisibility arguments