Monday, January 22: Division algorithm and quantifiers

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

- Understand universal and existential quantifiers
- Negate statements using quantifiers
- Negate conditional statements using quantifiers
- Prove existence and uniqueness for the Division Algorithm .

Read Ernst Section 2.2 and Section 2.4

Turn in

- Ernst, Problem 2.59. Both of the following sentences are propositions. Decide whether each is true or false. What would it take to justify your answers?
  (a) For all $x \in \mathbb{R}$, $x^2 - 4 = 0$.

  Solution: False–find a counterexample.

  (b) There exists $x \in \mathbb{R}$ such that $x^2 - 4 = 0$.

  Solution: True–find a solution x.

- Ernst Problem 2.64. Suppose the universe of discourse is the set of real numbers and consider the predicate $F(x, y) :=$ "$x = y^2$". Interpret the meaning of each of the following statements.
  (a) There exists x such that there exists y such that $F(x, y)$.

  Solution: There exists x such that for some y, $x = y^2$.

  (b) There exists y such that there exists x such that $F(x, y)$.

  Solution: There exists $y \in \mathbb{R}$ such that for some $x \in \mathbb{R}$, $x = y^2$.

  (c) For all y, for all x, $F(x, y)$.

  Solution: For all real numbers x and y, $x = y^2$.

Go over reading assignment at the start of class.

Division Algorithm (45 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.

Theorem (Division Algorithm)**.** *(Theorem 1.4) Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that*

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

Before proving this theorem, let's think about division with remainders, ie long division. The quotient q should be the largest integer such that $bq \leq a$. If we divide both sides by b, we have $q \leq \frac{a}{b}$. We have a function to find the greatest integer less than or equal to $\frac{a}{b}$, namely $q = \left\lfloor \frac{a}{b} \right\rfloor$. If we rearrange the equation $a = bq + r$, we gave $r = a - bq$. This is our scratch work for existence.

Proof Let $a, b \in \mathbb{Z}$ with $b > 0$. Define $q = \left\lfloor \frac{a}{b} \right\rfloor$ 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 $x - 1 < \lfloor x \rfloor \leq x$ by Strayer, Lemma 1.3, 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 there exist $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with

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

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

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:

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

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 $q_1 - q_2 = 0$. ■

In-class Problem 1 *Use the Division Algorithm on $a = 47, b = 6$ and $a = 281, b = 13$.*

Solution: For $a = 47, b = 6$, we have that $a = (7)6 + 5, q = 7, r = 5$. For $a = 281, b = 13$, we have that $a = (21)13 + 8, q = 21, r = 8$.

Corollary 1. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that*

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

One proof method is using an existing proof as a guide.

In-class Problem 2 *Let a and b be nonzero integers. Prove that there exists a unique $q, r \in \mathbb{Z}$ such that*

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

(Outline updated from class)

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

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

  (ii) *There are two cases:*

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

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

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

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

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

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

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

  (ii) *Follow the steps of the* proof *of the Division Algorithm to finish the proof.*

Solution: *Problem on Homework 2. You only need to provide one proof on Homework 2.*

Wednesday, January 24: Primes

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

- Every integer greater than 1 has a prime divisor.
- Prove that there are infinitely many prime numbers.

Read Strayer, Section 1.2

Turn in
- The proof method for Euclid's infinitude of primes is an important method. Summarize this method in your own words.

  Solution: Summaries will vary

- Identify any other new proof methods in this section

Solution: Proof by construction may be new to some students. Students also identified:

– Introducing a variable to aid in proof

– Without loss of generality

- Exercise 22. Prove that 2 is the only even prime number.

  Solution: Assume that there exists another even prime number, call it p. Then there exists $2 \mid p$ by the definition of even, but that implies that $p = 2$ by the definition of prime. Thus, 2 is the only even prime number.

Primes (50 minutes)

Definition (prime and composite)**.** 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?

Corollary (Lemma 1.5)**.** *Every integer greater than 1 has a prime divisor.*

We will not go over this proof in class.

Proof Assume by contradiction that there exists $n \in \mathbb{Z}$ greater than 1 with no prime divisor. By the Well Ordering Principle, we may assume n is the least such integer. By definition, $n \mid n$, so n is not prime. Thus, n is composite and there exists $a, b \in \mathbb{Z}$ such that $n = ab$ and $1 < a < n$, $1 < b < n$. Since $a < n$, then it has a prime divisor p. But since $p \mid a$ and $p \mid n$, $p \mid n$. This contradicts our assumption, so no such integer exists. ■

Theorem (Euclid's Infinitude of Primes)**.** *(Theorem 1.6) There are infinitely many prime numbers.*

Proof Assume by way of contradiction, that there are only finitely many prime numbers, so $p_1, p_2, \ldots, p_n$. Consider the number $N = p_1 p_2 \cdots p_n + 1$. Now N has a prime divisor, say, p, by Lemma 1.5. So $p = p_i$ for some i, $i = 1, 2, \ldots, n$. Then $p \mid N - p_1 p_2 \ldots p_n$, which implies that $p \mid 1$, a contradiction. Hence, there are infinitely many prime numbers. ■

Another important fact is there are arbitrarily large sequences of composite numbers. Put another way, there are arbitrarily large gaps in the primes. Another important proof method, which is a *constructive proof*:

Proposition (Proposition 1.8)**.** *For any positive integer n, there are at least n consecutive positive integers.*

Proof Given the positive integer n, consider the n consecutive positive integers

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n + 1.$$

Let i be a positive integer such that $2 \leq i \leq n+1$. Since $i \mid (n+1)!$ and $i \mid i$, we have

$$i \mid (n+1)! + i, \quad 2 \leq i \leq n+1$$

by linear combination (Proposition 1.2). So each of the n consecutive positive integers is composite. ■

In-class Problem 3 *Let n be a positive integer with $n \neq 1$. Prove that if n^2+1 is prime, then n^2+1 can be written in the form $4k+1$ with $k \in \mathbb{Z}$.*

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

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

In-class Problem 4 *Prove or disprove the following conjecture, which is similar to Conjecture 1:*
Conjecture: *There are infinitely many prime number p for which $p+2$ and $p+4$ are also prime numbers.*

Solution: *On Homework 2.*

Friday, January 26: Quiz 1, Induction, Greatest Common Divisors

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

- Understand induction
- Prove basic facts about the greatest common divisor .

Read Strayer Appendix A.1: The First Principle of Mathematical Induction or Ernst Section 4.1 and Section 4.2

Turn in Strayer Exercise Set A, Exercise 1a. If n is a positive integer, then

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof We proceed by induction. The base case is $n = 1$. Since $1^2 = \dfrac{1(1+1)(2*1+1)}{6}$, we are done.

Now assume that if $k \geq 1$ and for $n = k$,

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Adding $(k+1)^2$ to both sides gives,

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\ &= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} \\ &= \frac{(k+1)[2k^2 + k + 6k + 6]}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6}. \end{aligned}$$

So the desired statement is true for $n = k+1$. By the first principle of mathematical induction, the desired statement is true for all positive integers, and the proof is complete. ■

Quiz (10 minutes)

Greatest common divisor (20 min)

Definition (greatest common divisor)**.** 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 $\gcd(b_1, b_2, b_3, \ldots, b_n)$.

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

The GCD always exists when at least one of the integers is nonzero. 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.

Proposition (Proposition 1.11)**.** *Let $a, b \in \mathbb{Z}$ with a and b not both zero. Then*

$$\{(a, b) = \min\{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}.$$

This proof brings together definitions (of gcd), previous results (Division Algorithm, factors of linear combinations), the well-ordering principle, and some methods for minimum and maximum/greatest.

Proof Since $a, b \in \mathbb{Z}$ are not both zero, at least one of $1a + 0b, -1a + 0b, 0a + 1b, 0a + (-1)b$ is in $\{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$. Therefore, the set is nonempty and has a minimal element by the Well Ordering Principle. Call this element d, and $d = xa + yb$ for some $x, y \in \mathbb{Z}$.

First we will show that $d \mid a$. By the Division Algorithm, there exist unique $q, r \in \mathbb{Z}$ such that $a = qd + r$ with $0 \leq r < d$. Then,

$$r = a - qd = a - q(xa + yb) = (1 - qx)a - qyb,$$

so r is an integral linear combination of a and b. Since d is the least positive such integer, $r = 0$ and $d \mid a$. Similarly, $d \mid b$.

It remains to show that d is the *greatest* common divisor of a and$b$. Let $c$be any common divisor of a and b. Then $c \mid ax + by = d$, so $c \mid d$. ■

Since we assume a and b are not both zero, we could also simplify the first sentence using *without loss of generality*. Since there is no difference between a and b, we can assume $a \neq 0$.

More induction (15 minutes)

In-class Problem 5 *Theorems in Ernst Section 4.1*

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

Solution: *We proceed by induction. When $n = 1$, $3 \mid 4^n - 1 = 3$. Thus, the statement is true for $n = 1$.*

Now assume $k \geq 1$ and the desired statement is true for $n = k$. Then the induction hypothesis is

$$3 \mid 4^k - 1.$$

By the definition of a divides b, there exists $m \in \mathbb{Z}$ such that $3m = 4^k - 1$. In other words, $3m + 1 = 4^k$. Multiplying both sides by 4 gives $12m + 4 = 4^{k+1}$. Rewriting this equation gives $3(4m + 1) = 4^{k+1} - 1$. Thus, $3 \mid 4^{k+1} - 1$, and the desired statement is true for $n = k + 1$. By the (first) principle of mathematical induction, the statement is true for all positive integers, and the proof is complete.

Theorem (Ernst Theorem 4.7)**.** *Let $p_1, p_2, \ldots, p_n$ be n distinct points arranged on a circle. Then the number of line segments joining all pairs of points is $\dfrac{n^2 - n}{2}$.*

Solution: *We proceed by induction. When $n = 1$, there is only one point, so there are no lines connecting pairs of points. Additionally,* $\frac{1^2 - 1}{2} = 0$.[1]

Now assume $k \geq 1$ and the desired statement is true for $n = k$. Then the induction hypothesis is for k distinct points arranged in a circle, the number of line segments joining all pairs of points is $\frac{k^2 - k}{2}$. Adding a $(k+1)^{st}$ point on the circle will add an additional k line segments joining pairs of points, one for each existing point. Note that

$$\frac{k^2 - k}{2} + k = \frac{k^2 + k}{2} = \frac{k^2 + k + k + 1 - (k+1)}{2} = \frac{(k+1)^2 - (k+1)}{2}$$

In-class Problem 6 . *Use the first principle of mathematical induction to prove each statement.*

(b) *If n is a positive integer, then*

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

Solution: *We proceed by induction. When $n = 1$, $1^3 = \frac{1^2(1+1)^2}{4}$. Thus, the statement is true for $n = 1$.*

Now assume $k \geq 1$ and the desired statement is true for $n = k$. Then the induction hypothesis is

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

Adding $(k+1)^3$ to both sides gives

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

Thus, the desired statement is true for $n = k + 1$. By the (first) principle of mathematical induction, the statement is true for all positive integers, and the proof is complete.

(c) *If n is an integer with $n \geq 5$, then*

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

Solution: *We proceed by induction with base case $n = 5$. When $n = 5, 32 = 2^5 > 5^2 = 25$. Thus, the statement is true for $n = 1$.*

Now assume $k \geq 1$ and

$$2^k > k^2$$

[1] Alternately, you could use $n = 2$ for the base case. Then there is one line connecting the only pair of points and $\frac{2^2 - 2}{2} = 1$

is true for $n = k$*. Multiplying both sides of the inequality by 2 gives* $2^{k+1} > 2k^2$*. Notice that* $2k^2 > k^2 + 2k + 1$ *when* $(k-1)^2 > 0$*, which is true for all* $k \geq 5$*. Thus*

$$2^{k+1} > 2k^2 > (k+1)^2.$$

Thus, the desired statement is true for $n = k + 1$*. By the (first) principle of mathematical induction, the statement is true for all positive integers, and the proof is complete.*