NUMBER THEORY THROUGH INQUIRY

LIAM KOUCH

Contents

Week 1

Definition. (Natural numbers and integers)

- The *natural numbers* are the numbers $\{1, 2, 3, 4, ...\}$.
- The *integers* are {...,-3,-2,-1,0,1,2,3,...}.

Definition. (Divides) Suppose a and d are integers. Then d divides a, denoted $d \mid a$ if and only if there is an integer k such that $a = kd$.

Definition. (Congruence) Suppose that a, b, and n are integers, with $n > 0$. We say that a and b are *congruent modulo* n if and only if $n \mid (a - b)$. We denote this relationship as

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

and read these symbols as "a is congruent to b modulo n."

Theorem (1.1)**.** *Let a, b, c be integers. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

Proof. Let a, b, c be integers. Let $a \mid b$ and $a \mid c$. By definition of divisibility there exist integers $n, m \in \mathbb{Z}$ such that $an = b$ and $am = c$. Then

$$b + c = an + am = a(n + m)$$

Since $n + m \in \mathbb{Z}$ it follows by definition of divisibility that $a \mid (b + c)$. □

Theorem (1.2)**.** *Let a, b, c be integers. If $a \mid b$ and $a \mid c$, then $a \mid (b - c)$.*

Proof. Let a, b, c be integers. Let $a \mid b$ and $a \mid c$. By definition of divisibility there exist integers $n, m \in \mathbb{Z}$ such that $an = b$ and $am = c$. Then

$$b - c = an - am = a(n - m)$$

Since $n - m \in \mathbb{Z}$ it follows by definition of divisibility that $a \mid (b - c)$. □

Theorem (1.3)**.** *Let a, b, and c be integers. If $a \mid b$ and $a \mid c$, then $a \mid bc$.*

Proof. Let a, b, c be integers. Let $a \mid b$ and $a \mid c$. By definition of divisibility there exist integers $n, m \in \mathbb{Z}$ such that $an = b$ and $am = c$. Then

$$bc = (an)(am) = a(amn)$$

Since $amn \in \mathbb{Z}$ it follows by definition of divisibility that $a \mid bc$ □

Question (1.4)**.** We can weaken the hypothesis of Theorem 1.3 from ($a \mid b$ *and* $a \mid c$) to ($a \mid b$ *or* $a \mid c$).

Proof. There are two new cases to consider. We have already proven the case for $a \mid b$ and $a \mid c$. Now we show it is true for $a \mid b$ and $a \nmid c$. Then $b = an$ and $c = am + p$ for some $n, m, p \in \mathbb{Z}$. Then

$$bc = (an)(am + p) = a(nam + np)$$

Since $(nam + np) \in \mathbb{Z}$ it follows by definition of divisibility that $a \mid bc$. Proving the case for when $a \nmid b$ and $a \mid c$ is proved similarly. □

We can prove a stronger conclusion. We prove if $a, b, c \in \mathbb{Z}$ and $a \mid b$ and $a \mid c$ then $a^2 \mid bc$.

Proof. By definition of divisibility there exist $n, m \in \mathbb{Z}$ such that $b = an$ and $c = am$. Then

$$bc = (an)(am) = a^2(mn)$$

Since $(mn) \in \mathbb{Z}$ it follows by definition of divisibility that $a^2 \mid bc$ □

Question (1.5)**.** I prove if $a, b, c \in \mathbb{Z}$ and if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. By definition of divisibility there exist $n, m \in \mathbb{Z}$ such that $b = an$ and $c = bm$. Then

$$c = bm = (an)m = a(nm)$$

Since $(nm) \in \mathbb{Z}$ it follows by definition of divisbility that $a \mid c$. □

Theorem (1.6)**.** *Let a, b, and c be integers. If $a \mid b$ then $a \mid bc$.*

Proof. Let a, b, c be integers. Let $a \mid b$ and $a \mid bc$. By definition of divisibility there exist $n \in \mathbb{Z}$ such that $b = an$. Then

$$bc = (an)c = a(nc)$$

Since $(nc) \in \mathbb{Z}$ it follows $a \mid bc$. □

Exercise (1.7)**.** Answer each of the following questions, and prove that your answer is correct.

(1) $45 - 9 = 36 = 4(9)$ so the answer is correct.
(2) $37 - 2 = 35 = 5(7)$ so the answer is correct.
(3) $37 - 3 = 34$. There is no integer $k \in \mathbb{Z}$ such that $5k = 34$ so this statement is not true.
(4) $37 - (-3) = 40 = 5(8)$ so this statement is true.

Exercise (1.8)**.** For each of the following congruences, characterize all the integers m that satisfy that congruence.

(1) All integers of the form $3k$ where $k \in \mathbb{Z}$.
(2) All integers of the form $3k + 1$ where $k \in \mathbb{Z}$.
(3) All integers of the form $3k + 2$ where $k \in \mathbb{Z}$.
(4) All integers of the form $3k$ where $k \in \mathbb{Z}$.
(5) All integers of the form $3k + 1$ where $k \in \mathbb{Z}$.

Theorem (1.9)**.** *Let a and n be integers with $n > 0$. Then $a \equiv a \pmod{n}$.*

Proof. Let a and n be integers with $n > 0$. Then $a - a = 0$ so then $0 = 0(n)$. It follows $n \mid 0$ or $n \mid (a - a)$. Then by definition of congruence this means $a \equiv a \pmod{n}$. □

Theorem (1.10)**.** *Let a, b, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.*

Proof. Let a, b, and n be integers with $n > 0$. Since $a \equiv b \pmod{n}$ it follows $n \mid (a - b)$ or there exists $k \in \mathbb{Z}$ such that $(a - b) = kn$. Then $(b - a) = (-k)n$ and since $(-k) \in \mathbb{Z}$ it follows $n \mid (b - a)$ and then by definition of congruence $b \equiv a \pmod{n}$ □

Theorem (1.11)**.** *Let a, b, c, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*

Proof. Let a, b, c, and n be integers with $n > 0$. By definition of congruence we have $n \mid (a - b)$ and $n \mid (b - c)$. Equivalently, we have $(a - b) = k_1 n$ and $(b - c) = k_2 n$ for some $k_1, k_2 \in \mathbb{Z}$. Then

$$(a - c) = (a - b) + (b - c) = k_1 n + k_2 n = (k_1 + k_2)n$$

$k_1, k_2 \in \mathbb{Z}$ and integers are closed under addition so $(k_1 + k_2) \in \mathbb{Z}$. It follows that $n \mid (a - c)$, hence by definition of congruence $a \equiv c \pmod{n}$. □

Week 2

Theorem (1.12)**.** *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.*

Proof. We assume the hypothesis of the theorem so let a, b, c, d and n be integers with $n > 0$. And suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then by definition of congruence we have $n \mid (a - b)$ and $n \mid (c - d)$. By definition of divisibility there is some $p, q \in \mathbb{Z}$ such that $a - b = np$ and $c - d = nq$. Adding these equations together gives $a - b + c - d = (a + c) - (b + d) = n(p + q)$. And integers are closed under addition so $(p + q) \in \mathbb{Z}$. Then by definition of congruence $a + c \equiv b + d \pmod{n}$ □

Theorem (1.13)**.** *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$.*

Proof. Assume a, b, c, d, and n are integers with $n > 0$. Let $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By definition of congruence we have $n \mid a - b$ and $n \mid c - d$. Equivalently, by definition of divisibility there exists integers $p, q \in \mathbb{Z}$ such that

$$a - b = np \tag{1}$$

$$c - d = nq \tag{2}$$

Now we subtract (2) from (1) which gives us $a-b-c+d = np-nq$ or $(a-c)-(b-d) = n(p-q)$. Due to closure of integers under addition and multiplication we have $(p-q) \in \mathbb{Z}$ and it follows by definition of congruence that $a - c \equiv b - d \pmod{n}$ □

Proof. Another proof is supplied. Assume the theorem's hypothesis. Then by definition of congruence we have $n \mid (a - b)$ and $n \mid (c - d)$. But due to closure of integers under addition and multiplication $(a - b)$ and $(c - d)$ are integers so by applying Theorem 1.2 we get

$$n \mid (a - b) - (c - d) \to n \mid (a - c) - (b - d)$$

It follows be definition of congruence that $a - c \equiv b - d \pmod{n}$. □

Theorem (1.14)**.** *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.*

Proof. Assume the hypothesis: let a, b, c, d and n be integers with $n > 0$. Then by definition of congruence we have $n \mid (a - b)$ and $n \mid (c - d)$. We then have $a - b = k_1 n$ and $c - d = k_2 n$ for some $k_1, k_2 \in \mathbb{Z}$.Rearranging terms gives $a = b + k_1 n$ and $c = d + k_2 n$. Multiplying these two equations gives

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1)n + k_1 k_2 n^2$$

$$ac - bd = n((bk_2 + dk_1) + k_1 k_2 n)$$

Integers are closed under addition and multiplication so $((bk_2 + dk_1) + k_1 k_2 n) \in \mathbb{Z}$. It follows $n \mid (ac - bd)$ and by definition of congruence we have $ac \equiv bd \pmod{n}$. □

Theorem (1.15)**.** *Let a, b, and n be integers $n > 0$. Show that if $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.*

Proof. Assume the hypothesis of the theorem: let a, b and n be integers with $n > 0$. Suppose $a \equiv b \pmod{n}$. Then by definition of congruence we have $n \mid (a - b)$. Then by definition of divisibility $a - b = kn$ where $k \in \mathbb{Z}$. This is the same as $a = b + kn$. Then squaring each

side we have $a^2 = b^2 + 2bkn + k^2n^2$. Then $a^2 - b^2 = n(2bk + k^2n)$. Integers are closed under addition and multiplication so $(2bk + k^2n) \in \mathbb{Z}$. So then $n \mid a^2 - b^2$. It follows by definition of congruence $a^2 \equiv b^2 \pmod{n}$. □

Theorem (1.16)**.** *Let a, b, and n be integers $n > 0$. Show that if $a \equiv b \pmod{n}$, then $a^3 \equiv b^3 \pmod{n}$.*

Proof. Assume the hypothesis of the theorem: let a, b, and n be integers with $n > 0$. Suppose $a \equiv b \pmod{n}$. Then by definition of congruence we have $n \mid (a - b)$. Then by definition of divisibility $a - b = kn$ for some $k \in \mathbb{Z}$. This is the same as $a = b + kn$. Then cubing both sides we get

$$a^3 = b^3 + 3b^2kn + 3bk^2n^2 + k^3n^3$$

So then $a^3 - b^3 = n(3b^2k + 3bk^2n + k^3n^2)$ and $(3b^2k + 3bk^2n + k^3n^2) \in \mathbb{Z}$ since integers are closed under addition and multiplication. It follows $n \mid (a^3 - b^3)$ and by definition of congruence we have $a^3 \equiv b^3 \pmod{n}$. □

Theorem (1.17)**.** *Let a, b, k, and n be integers with $n > 0$ and $k > 1$. Show that if $a \equiv b \pmod{n}$ and $a^{k-1} \equiv b^{k-1} \pmod{n}$, then*

$$a^k \equiv b^k \pmod{n}$$

Proof. Assume the hypothesis of the theorem: let a, b, k, and n be integers with $n > 0$ and $k > 1$. Suppose $a \equiv b \pmod{n}$ and $a^{k-1} \equiv b^{k-1} \pmod{n}$. By definition of congruence $n \mid (a - b)$ and $n \mid (a^{k-1} - b^{k-1})$. Then $a - b = pn$ and $a^{k-1} - b^{k-1} = qn$ for some $p, q \in \mathbb{Z}$. By algebra this is the same as $a = b + pn$ and $a^{k-1} = b^{k-1} + qn$. Then multiplying these two equations gives $a^k = b^k + bqn + b^{k-1}pn + pqn^2$. So then $a^k - b^k = n(bq + b^{k-1}p + pqn)$. Integers are closed under addition and multiplication so $(bq + b^{k-1}p + pqn) \in \mathbb{Z}$. It follows that $n \mid (a^k - b^k)$. Then by definition of congruence $a^k \equiv b^k \pmod{n}$. □

Theorem (1.18)**.** *Let a, b, k, and n be integers with $n > 0$ and $k > 0$. If $a \equiv b \pmod{n}$, then*

$$a^k \equiv b^k \pmod{n}$$

Proof. Assume the hypothesis: let a, b, k, and n be integers with $n > 0$ and $k > 0$ and $a \equiv b \pmod{n}$. We prove by induction. The basis step is done since we assume that $a^1 \equiv b^1 \pmod{n}$ from the hypothesis of the theorem. For the inductive step we use Theorem 1.17. Now assume in addition to $a \equiv b \pmod{n}$ we have $a^{k-1} \equiv b^{k-1} \pmod{n}$ for some $k > 1$. But we also know $a \equiv b \pmod{n}$ so by applying Theorem 1.17, it follows $a^k \equiv b^k \pmod{n}$. This concludes the induction. Hence, $a^k \equiv b^k \pmod{n}$ for all $k > 0$. □

Exercise (1.19)**.** Illustrate each of Theorems 1.12-1.18 with an example using actual numbers.

(12) Let $a = 4, b = 9, c = 12, d = 27, n = 5$. $4 \equiv 9 \pmod{5}$ and $12 \equiv 27 \pmod{5}$ and we have $16 \equiv 36 \pmod{5}$

(13) Let $a = 4, b = 9, c = 12, d = 27, n = 5$. $4 \equiv 9 \pmod{5}$ and $12 \equiv 27 \pmod{5}$ and we have $-8 \equiv -18 \pmod{5}$

(14) Let $a = 4, b = 9, c = 1, d = 6, n = 5$. $4 \equiv 9 \pmod{5}$ and $1 \equiv 6 \pmod{5}$ and we have $4 \equiv 54 \pmod{5}$

(15) Let $a = 4, b = 10, n = 3$. Then we have $4 \equiv 10 \pmod{3}$ and $16 \equiv 100 \pmod{3}$.

(16) Let $a = 1, b = 3, n = 2$. Then we have $1 \equiv 3 \pmod{2}$ and $1 \equiv 27 \pmod{2}$.

(17) Let $a = 1, b = 3, n = 2, k = 4$. Then $1 \equiv 3 \pmod 2$ and $1 \equiv 27 \pmod 2$. And we have $1 \equiv 81 \pmod 2$.
(18) Let $a = 1, b = 3, n = 2, k = 7$. Then $1 \equiv 3 \pmod 2$ and we have $1 \equiv 2187 \pmod 2$.

Question (1.20)**.** Let a, b, c, and n be integers for which $ac \equiv bc \pmod n$. Can we conclude that $a \equiv b \pmod n$?

No. By definition of congruence we have $n \mid c(a-b)$ and it is not necessary that $n \mid (a-b)$. For example, let $n = 4$, $c = 6$, $a = 20$, and $b = 10$. Then $120 \equiv 60 \pmod 4$ but $20 \not\equiv 10 \pmod 4$.

Week 3

Theorem (1.21)**.** *Let a natural number n be expressed in base 10 as*

$$n = a_k a_{k-1} \cdots a_1 a_0$$

If $m = a_k + a_{k-1} + \cdots + a_1 + a_0$, then $n \equiv m \pmod 3$.

Proof. Let n be a natural number which is expressed in base 10 as

$$n = a_k a_{k-1} \cdots a_1 a_0$$

with $m = a_k + a_{k+1} + \cdots a_1 + a_0$. Then the actual value of n is given as

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

We want to show $n \equiv m \pmod 3$ or by definition of congruence we have $3 \mid n-m$. Expanding this out we get

$$3 \mid a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + \cdots + a_1(10^1 - 1) + a_0(10^0 - 1)$$

By Lemma 1.21.1 we know $10^k \equiv 1 \pmod 3$ for all $k \geq 0$. By definition of congruence we have $3 \mid (10^k - 1)$ for all $k \geq 0$. By Theorem 1.6 it follows $3 \mid a_k(10^k - 1)$. By definition of divides, for each $i \in \mathbb{Z}$ where $0 \leq i \leq k$ there exists $q_i \in \mathbb{Z}$ such that $a_i(10^i - 1) = 3q_i$. Then we have

$$n - m = 3q_k + 3q_{k-1} + \cdots + 3q_1 + 3q_0 = 3(q_k + q_{k-1} + \cdots + q_1 + q_0)$$

And $(q_k + q_{k-1} + \cdots + q_1 + q_0) \in \mathbb{Z}$ since integers are closed under addition. Then it follows $3 \mid (n - m)$ and thus by definition of congruence we have $n \equiv m \pmod 3$. □

Lemma (1.21.1)**.** *We show that for any $k \in \mathbb{Z}$ and $k \geq 0$ that $10^k \equiv 1 \pmod 3$.*

Proof. We prove by induction. For $k = 0$ we have $10^k = 1$ and $1 \equiv 1 \pmod 3$ is true. Now suppose $10^k \equiv 1 \pmod 3$ it true. Then by definition of congruence we have $3 \mid (10^k - 1)$ which means there exists some $q \in \mathbb{Z}$ such that $10^k - 1 = 3q$. Multiplying by 10 on both sides gives $10^{k+1} - 10 = 30q$. Let $p = 10q$ then we have $10^{k+1} - 10 = 3p$ for some $p \in \mathbb{Z}$ since integers are closed under multiplication. Adding nine to both sides results in $10^{k+1} - 1 = 3p + 9$. Let $r = p + 3$. Then we have $10^{k+1} - 1 = 3r$ where $r \in \mathbb{Z}$ since integers are closed under addition. It follows by the definition of divisibility that $3 \mid (10^{k+1} - 1)$ and then by the definition of congruence that $10^{k+1} \equiv 1 \pmod 3$. This concludes the induction. The proof of Lemma 1.21.1 is finished. We now use this result to prove Theorem 1.21. □

Theorem. *A natural number that is expressed in base 10 is divisible by 3 if and only if the sum of its digits is divisible by 3.*

Theorem (1.22)**.** *If a natural number is divisible by 3, then, when expressed in base 10, the sum of its digits is divisible by 3.*

Proof. Suppose a natural number n is divisible by 3 or $3 \mid n$. Then by definition of congruence we have $n \equiv 0 \pmod 3$. Let n be expressed as the sum of digits in base 10. Then we have

$$n = a_k a_{k-1} \cdots a_1 a_0$$

for some $k \in \mathbb{Z}$ and $k \geq 0$. The actual value of n is given as

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots a_1 10^1 + a_0 10^0$$

Let m be defined as

$$m = a_k + a_{k-1} + \cdots a_1 + a_0$$

Then m is the sum of its digits expressed in base 10. By Theorem 1.21 it follows $n \equiv m \pmod 3$. We know $n \equiv 0 \pmod 3$ or $0 \equiv n \pmod 3$ by Theorem 1.10. Moreover, by Theorem 1.11 we know $\equiv$ is transitive. Since we know $0 \equiv n \pmod 3$ and $n \equiv m \pmod 3$ it follows by transitivity that $0 \equiv m \pmod 3$. By commutativity we have $m \equiv 0 \pmod 3$. By definition of congruence we have $3 \mid m$ and by definition of divisibility this implies the sum of digits m is divisible by 3. □

Theorem (1.23)**.** *If the sum of the digits of a natural number expressed in base 10 is divisible by 3, then the number is divisible by 3 as well.*

Proof. Suppose the sum of digits of a natural number expressed in base 10 is divisible by 3. Explicitly, we have n expressed as

$$n = a_k a_{k-1} \cdots a_1 a_0$$

where each a_i is a digit of a regular base 10 number. Let m be defined as

$$m = a_k + a_{k-1} + \cdots + a_1 + a_0$$

Since the sum of digits is divisible by 3 we have $3 \mid m$. Then by definition of congruence we have $m \equiv 0 \pmod 3$. But we know by Theorem 1.21 that $m \equiv n \pmod 3$. Moreover, we know that $\equiv$ is an equivalence relation and is therefore commutative and transitive. Or by Theorem 1.10 we know $m \equiv 0 \pmod 3$ means $0 \equiv m \pmod 3$. Putting $0 \equiv m \pmod 3$ and $m \equiv n \pmod 3$ we get $0 \equiv n \pmod 3$ because $\equiv$ is transitive by Theorem 1.11. Applying commutativity again we get $n \equiv 0 \pmod 3$ and by definition of congruence we have $3 \mid n$. Thus, n is divisible by 3. □

Exercise (1.24)**.** Devise and prove other divisibility criteria similar to the preceding one.

Theorem. *Let a natural number n be expressed in base 10 as*

$$n = a_k a_{k-1} \cdots a_1 a_0$$

If $m = a_k + a_{k-1} + \cdots + a_1 + a_0$, then $n \equiv m \pmod 9$.

Proof. Let n be a natural number which is expressed in base 10 as

$$n = a_k a_{k-1} \cdots a_1 a_0$$

with $m = a_k + a_{k+1} + \cdots a_1 + a_0$. Then the actual value of n is given as

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

We want to show $n \equiv m \pmod 9$ or by definition of congruence we have $9 \mid n-m$. Expanding this out we get

$$9 \mid a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + \cdots + a_1(10^1 - 1) + a_0(10^0 - 1)$$

By Lemma 1.24.1 we know $10^k \equiv 1 \pmod 9$ for all $k \geq 0$. By definition of congruence we have $9 \mid (10^k - 1)$ for all $k \geq 0$. By Theorem 1.6 it follows $9 \mid a_k(10^k - 1)$. By definition of divides, for each $i \in \mathbb{Z}$ where $0 \leq i \leq k$ there exists $q_i \in \mathbb{Z}$ such that $a_i(10^i - 1) = 9q_i$. Then we have

$$n - m = 9q_k + 9q_{k-1} + \cdots + 9q_1 + 9q_0 = 9(q_k + q_{k-1} + \cdots + q_1 + q_0)$$

And $(q_k + q_{k-1} + \cdots + q_1 + q_0) \in \mathbb{Z}$ since integers are closed under addition. Then it follows $9 \mid (n - m)$ and thus by definition of congruence we have $n \equiv m \pmod 9$. $\square$

Lemma (1.24.1)**.** *We show that for any $k \in \mathbb{Z}$ and $k \geq 0$ that $10^k \equiv 1 \pmod 9$.*

Proof. We prove by induction. For $k = 0$ we have $10^k = 1$ and $1 \equiv 1 \pmod 9$ is true. Now suppose $10^k \equiv 1 \pmod 9$ it true. Then by definition of congruence we have $9 \mid (10^k - 1)$ which means there exists some $q \in \mathbb{Z}$ such that $10^k - 1 = 9q$. Multiplying by 10 on both sides gives $10^{k+1} - 10 = 90q$. Let $p = 10q$ then we have $10^{k+1} - 10 = 9p$ for some $p \in \mathbb{Z}$ since integers are closed under multiplication. Adding nine to both sides results in $10^{k+1} - 1 = 9p + 9$. Let $r = p + 1$. Then we have $10^{k+1} - 1 = 9r$ where $r \in \mathbb{Z}$ since integers are closed under addition. It follows by the definition of divisibility that $9 \mid (10^{k+1} - 1)$ and then by the definition of congruence that $10^{k+1} \equiv 1 \pmod 9$. This concludes the induction. The proof of Lemma 1.24.1 is finished. We now use this result to prove the theorem for Exercise 1.24. $\square$

Axiom. (The Well-Ordering Axiom for the Natural Numbers). Let S be any non-empty set of natural numbers. Then S has a smallest element.

Theorem. *For every natural number n there is a natural number k such that $7k$ differs from n by less than 7.*

Proof. We prove by induction. We induct on n. Let $n = 1$. Then let $k = 1$. Then $7k = 7$ and $7k - n = 7 - 1 = 6 < 7$. Now suppose for $n \in \mathbb{N}$ there exists $k_n \in \mathbb{N}$ such that $0 \leq 7k_n - n < 7$. Then there are two cases: either (1) $7k_n - n = 0$ or (2) $1 \leq 7k_n - n \leq 6$. Suppose we have case (1). Then $7k_n - (n + 1) = -1$. It follows $7(k_{n+1}) - (n + 1) = 6 < 7$. Then the for $(n + 1) \in \mathbb{N}$ let $k_{n+1} = k_n + 1$. And we have that $7k_{n+1} - (n + 1) = 6 < 7$. Now suppose we have case (2). Then we know $1 \leq 7k_n - n \leq 6$ so $0 \leq 7k_n - (n + 1) \leq 5$. Then let $k_{n+1} = k_n$. It follows for $(n + 1) \in \mathbb{N}$ that $7k_{n+1} - (n + 1) < 7$. Thus for both case (1) and (2) we have found an appropriate $k_{n+1} \in \mathbb{N}$ such that $1 \leq 7k_{k+1} - (n + 1) < 7$. This closes the induction. $\square$

Theorem. *(The Division Algorithm) Let n and m be natural numbers. Then (existence part) there exists integers q (for quotient) and r (for remainder) such that*

$$m = nq + r$$

and $0 \leq r \leq n - 1$. Moreover (uniqueness part), if q, q', r, and r' are any integers that satisfy

$$\begin{aligned} m &= nq + r \\ &= nq' + r' \end{aligned}$$

with $0 \leq r$, $r' \leq n - 1$, then $q = q'$ and $r = r'$.

Exercise (1.25)**.** Illustrate the Division Algorithm for:

(1) $m = 25, n = 7$. Then $q = 3$ and $r = 4$. $25 = (7)(3) + (4)$ and we have $0 \leq 4 \leq 6$.
(2) $m = 277, n = 4$. Then $q = 69$ and $r = 1$. $277 = (4)(69) + (1)$ and we have $0 \leq 1 \leq 3$.
(3) $m = 33, n = 11$. Then $q = 3$ and $r = 0$. $33 = (11)(3) + (0)$ and we have $0 \leq 0 \leq 10$.
(4) $m = 33, n = 45$. Then $q = 0$ and $r = 33$. $33 = (45)(0) + (33)$ and we have $0 \leq 33 \leq 44$.

Theorem (1.26)**.** *Prove the existence part of the Division Algorithm.*

Proof. We prove by induction. We induct on m. For the base case let $m = 1$. Then we want to show for any natural number n there exist integers q and r such that

$$1 = nq + r$$

and $0 \leq r \leq n - 1$. There are two cases: (1) $n = 1$ and (2) $n \geq 2$. For case (1) let $q = 1$ and $r = 0$. Then we have $q, r \in \mathbb{Z}$ and

$$1 = (1)(1) + (0)$$

Moreover, we have $0 \leq r \leq n - 1$. Since in this case $r = 0$ and $n - 1 = 0$. Now suppose we have case (2) where $n \geq 2$. A suitable choice of q and r is let $q = 0$ and $r = 1$. We have $q, r \in \mathbb{Z}$ and

$$1 = (n)(0) + 1$$

Moreover, $0 \leq r \leq n - 1$ since $r = 1$ and $n - 1 \geq 1$. This concludes the base case. Now for the inductive step assume that for any natural number n and for some particular natural number m that there exists integers q and r such that

$$m = nq + r$$

and $0 \leq r \leq n - 1$. Now we wish to show there exist integers q' and r' such that

$$m + 1 = nq' + r'$$

and $0 \leq r' \leq n$. We find q' and r' in two cases: (1) either $0 \leq r \leq n-2$ or (2) $r = n-1$. For case (1) we let $q' = q$ and $r' = r+1$. It follows q' is an integer since q is an integer. And r' is an integer due to closure of integers under addition. So $q', r' \in \mathbb{Z}$ and $nq'+r' = nq+r+1 = m+1$. Moreover, since $0 \leq r \leq n-2$ it follows $1 \leq r' = r+1 \leq n-1$ so then $0 \leq r' \leq n-1$. These q' and r' are appropriate integers. For case (2) we have $r = n - 1$. Then let $q' = q + 1$ and $r' = 0$. Then q' is an integer due to closure of integers under addition and r' is an integer since zero is an integer. And $0 \leq r' \leq n-1$ since $r' = 0$ and $n-1 \geq 0$ since $n \in \mathbb{N}$. Plugging in the values we have $nq'+r' = n(q+1)+0 = nq+n = nq+(n-1)+1 = nq+r+1 = m+1$ so q' and r' are appropriate integers that satisfy the conditions to be a quotient and remainder respectively. In both cases we have shown there exist $q', r' \in \mathbb{Z}$ such that $m + 1 = nq' + r'$ and $0 \leq r' \leq n - 1$. This concludes the induction. It follows for any $n, m \in \mathbb{Z}$ there exist integers $q, r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \leq r \leq n - 1$. □

Theorem (1.27)**.** *Prove the uniqueness part of the Division Algorithm.*

Proof. Let $n, m \in \mathbb{N}$. Let $q, r, q', r' \in \mathbb{Z}$ such that

$$m = nq + r = nq' + r'$$

where $0 \leq r, r' \leq n - 1$. For the sake of contradiction, suppose it is not the case that $q = q'$ and $r = r'$. Then we have three cases: (1) $q = q'$ but $r \neq r'$, (2) $q \neq q'$ but $r = r'$, and (3) $q \neq q'$ and $r \neq r'$. Suppose we have case (1). Then

$$nq + r = nq' + r$$
$$r = r'$$

But is a contradiction. Now suppose we have case (2). Then

$$nq + r = nq' + r'$$
$$nq = nq'$$
$$q = q'$$

But this is a contradiction. Now suppose we have case (3). Then

$$nq + r = nq' + r'$$
$$|n(q - q')| = |r' - r|$$

Since we have $0 \leq r, r' \leq n - 1$ it follows $|r - r'| \leq n - 1$. And since we assumed $q \neq q'$ and $q, q' \in \mathbb{Z}$ it follows $|q - q'| \geq 1$. So then $|n(q - q')| \geq n$ and $|r - r'| \leq n - 1$. But this is a contradiction because it is impossible to have an integer x satisfy both $x \geq n$ and $x \leq n - 1$ for some natural number $n \in \mathbb{N}$. Thus all three cases lead to a contradiction. It follows $q = q'$ and $r = r'$. $\square$

Theorem (1.28)**.** *Let a, b, and n be integers with $n > 0$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n. Equivalently, $a \equiv b \pmod{n}$ if and only if when $a = nq_1 + r_1$ $(0 \leq r_1 \leq n-1)$ and $b = nq_2 + r_2$ $(0 \leq r_2 \leq n-1)$, then $r_1 = r_2$.*

Proof. Let a, b, n be integers with $n > 0$. We prove the reverse direction first. Suppose we have $a = nq_1 + r_1$ and $b = nq_2 + r_2$ with $0 \leq r_1, r_2 \leq n-1$ and $r_1 = r_2$. Also, $r_1, r_2, q_1, q_2 \in \mathbb{Z}$. Then $b - a = n(q_2 - q_1) + (r_2 - r_1)$. But since $r_2 = r_1$ we have $r_2 - r_1 = 0$ so then $b - a = n(q_2 - q_1)$. Since $q_2, q_1 \in \mathbb{Z}$ it follows $(q_2 - q_1) \in \mathbb{Z}$ due to integers being closed under subtraction. By definition of congruence we have $b \equiv a \pmod{n}$. Moreover, we know $\equiv$ is commutative from Theorem 1.10. It follows $a \equiv b \pmod{n}$.

Now we prove the forward direction of the biconditional statement. Suppose $a \equiv b \pmod{n}$ and let $a = nq_1 + r_1$ and $b = nq_2 + r_2$ where $0 \leq r_1, r_2 \leq n-1$ and $q_1, r_1, q_2, r_2 \in \mathbb{Z}$. For the sake of contradiction suppose $r_1 \neq r_2$. By definition of congruence we have

$$\begin{aligned} n \mid (a - b) \\ n \mid (nq_1 + r_1 - nq_2 - r_2) \\ n \mid (n(q_1 - q_2) + (r_1 - r_2)) \end{aligned}$$

But then we require $n(q_1 - q_2) + (r_1 - r_2) = jn$ for some $j \in \mathbb{Z}$. Equivalently, we have

$$\begin{aligned} r_1 - r_2 &= jn - n(q_1 - q_2) \\ r_1 - r_2 &= n(j - (q_1 - q + 2)) \\ r_1 - r_2 &= n(j - q_1 + q_2) \\ r_1 - r_2 &= kn \\ |r_1 - r_2| &= |kn| \end{aligned}$$

for some integer $k \in \mathbb{Z}$ since $j, q_1, q_2 \in \mathbb{Z}$ and integers are closed under addition. We know $0 \leq r_1, r_2 \leq n-1$ so we have $0 \leq |r_1 - r_2| \leq n-1$. But since we assumed by contradiction that $r_1 \neq r_2$ it is not possible for $|r_1 - r_2| = 0$. Therefore, we have the following inequality.

$$0 < 1 \leq |r_1 - r_2| \leq n - 1 < n$$

It follows $|r_1 - r_2|$ cannot be an integer multiple of n since $|r_1 - r_2|$ is in between $0n$ and $1n$. But we required this for $a \equiv b \pmod{n}$. This is a contradiction. Therefore, we must have $r_1 = r_2$. □

Question (1.29)**.** Do every two integers have at least one common divisor?

Yes. Every integer is divisible by one.

Question (1.30)**.** Can two integers have infinitely many common divisors?

Yes, if you let $a = 0$ and $b = 0$.

Definition. (Greatest common divisor) The greatest common divisor of two integers a and b, not both 0, is the largest integer d such that $d \mid a$ and $d \mid b$. The greatest common divisor of two integers a and b is denoted $\gcd(a, b)$ or more briefly as just (a, b).

Definition. (Relatively prime) If $\gcd(a, b) = 1$, then a and b are said to be relatively prime.

Exercise (1.31)**.** Find the following greatest common divisors. Which are relatively prime?

(1) $(36, 22) = 2$
(2) $(45, -15) = 15$
(3) $(-296, -88) = 8$
(4) $(0, 256) = 256$
(5) $(15, 28) = 1$ so relatively prime
(6) $(1, -2436) = 1$ so relatively prime

Theorem (1.32)**.** *Let a, n, b, r, and k be integers. If $a = nb + r$ and $k \mid a$ and $k \mid b$, then $k \mid r$.*

Proof. Let a, n, b, r and k be integers. If $a = nb + r$ and $k \mid a$ and $k \mid b$, then $k \mid r$. By definition of divides we have $a = ik$ and $b = jk$ for some $i, j \in \mathbb{Z}$. By substitution we have

$$ik = njk + r$$
$$(i - nj)k = r$$

And $(i - nj) \in \mathbb{Z}$ since $i, n, j \in \mathbb{Z}$ and integers are closed under addition and multiplication. It follows by definition of divides that $k \mid r$. □

Theorem (1.33)**.** *Let a, b, n_1, and r_1 be integers with a and b not both 0. If $a = n_1 b + r_1$, then $(a, b) = (b, r_1)$.*

Proof. Let a, b, n_1 and r_1 be integers with a and b not both 0. Suppose $a = n_1 b + r_1$. We first show $(a, b) \leq (b, r_1)$. The greatest common divisor of a and b is defined as

$$(a, b) = \text{ maximum of } \{d \in \mathbb{Z} \mid a = k_1 d \text{ and } b = k_2 d \text{ and } k_1, k_2 \in \mathbb{Z}\}$$

Since (a, b) divides a and (a, b) divides b and we know $a, n_1, b, r_1, (a, b) \in \mathbb{Z}$ it follows from Theorem 1.32 that (a, b) divides r_1. Thus b and r_1 share a common divisor of (a, b) so then the greatest common divisor between b and r_1 must at least be equal (a, b). It follows $(a, b) \leq (b, r_1)$.

Now we show $(a, b) \geq (b, r_1)$. First we note that both b and r_1 cannot be zero. Otherwise we would have $a = n_1(0) + 0 = 0$ which would means $a = b = 0$ which contradicts the hypothesis of the theorem. Thus (b, r_1) exists. By definition of greatest common divisor it follows $(b, r_1) \mid b$ and $(b, r_1) \mid r_1$. So then we have $b = i(b, r_1)$ and $r_1 = j(b, r_1)$ for some $i, j \in \mathbb{Z}$. By substitution into

$$a = n_1 b + r$$
$$a = n_1 i(b, r_1) + j(b, r_1)$$
$$a = (n_1 i + j)(b, r_1)$$

We know $n_1, i, j \in \mathbb{Z}$ and integers are closed under addition and multiplication so $(n_1 i + j) \in \mathbb{Z}$. It follows by definition of divides that $(b, r_1) \mid a$. So we have both $(b, r_1) \mid b$ and $(b, r_1) \mid a$ which means (b, r_1) is a common divisor to both b and a. This means the greatest common divisor of a and b must be at least equal to (b, r_1). Thus we have $(a, b) \geq (b, r_1)$. But we know from before that $(a, b) \leq (b, r_1)$. In order for both of these inequalities to hold we must have $(a, b) = (b, r_1)$. □

Exercise (1.34)**.** As an illustration of the above theorem, note that

$$\begin{aligned} 51 &= 3 \cdot 15 + 6, \\ 15 &= 2 \cdot 6 + 3, \\ 6 &= 2 \cdot 4 + 0 \end{aligned}$$

Use the preceding theorem to show that if $a = 51$ and $b = 15$, then $(51, 15) = (6, 3) = 3$.

For the first equation we have $51 = 3(15) + 6$. By Theorem 1.33 it follows $(51, 15) = (15, 6)$. Then for the second equation we have $15 = 2(6) + 3$. By Theorem 1.33 it follows $(15, 6) = (6, 3)$. Then for the third equation we have $6 = 2(3) + 0$. By Theorem 1.33 it follows $(6, 3) = (3, 0)$. And we know the greatest common divisor of $(3, 0)$ is 3. Hence, we have $(51, 15) = (15, 6) = (6, 3) = (3, 0) = 3$.

Exercise (1.35)**.** (Euclidean Algorithm). Using the previous theorem and the Division Algorithm successively, devise a procedure for finding the greatest common divisor of two integers.

Suppose we have two integers. For each negative integer multiply it by negative one to make it positive. This is because $(x, y) = (|x|, |y|)$ for all $x, y \in \mathbb{Z}$ when x and y are not both zero. Also, if both integers are zero then we cannot perform the algorithm since there does not exist a greatest common divisor for zero. If we have one integer is nonzero and the other is zero, then the greatest common divisor is then the absolute value of the nonzero integer. Now we only have the case where both of our numbers are natural numbers. Since the Division Algorithm has been defined only for natural numbers we can use it now. Suppose we have natural numbers n_0 and m_0 where $m_0 \geq n_0$ and we want to find the greatest common divisor. Then we perform the division algorithm and we get some quotient q_0 and remainder $0 \leq r_0 \leq 1 - n_0$. Then in the next iteration of the division algorithm let $m_1 = q_0$ and $n_1 = r_0$

$$\begin{aligned} m_0 &= n_0 \cdot q_0 + r_0 \\ m_1 &= n_1 \cdot q_1 + r_1 \\ \vdots &= \vdots \end{aligned}$$

We keep going until we reach a remainder of 0. Suppose we reach a remainder of zero for r_i. Then q_i is the greatest common divisor of n_0 and m_0.

Exercise (1.36)**.** Use the Euclidean Algorithm to find

(1) $(96, 112) = (112, 96) = (96, 16) = (16, 0) = 16$.
(2) $(162, 31) = (31, 7) = (7, 3) = (3, 1) = (1, 0) = 1$.
(3) $(0, 256) = 256$.
(4) $(-288, -166) = (288, 166) = (166, 122) = (122, 44) = (44, 34) = (34, 10) = (10, 4) = (4, 2) = (2, 0) = 2$.
(5) $(1, -2436) = (1, 2436) = (2436, 1) = 1$.

Exercise (1.37)**.** Find integers x and y such that $162x + 31y = 1$.

$$162 = 5(31) + 7$$
$$31 = 4(7) + 3$$
$$7 = 2(3) + 1$$
$$3 = 3(1) + 0$$

Multiply $31 = 4(7) + 3$ by two and we get $2(31) = 2(4)(7) + 2(3)$. But we know $7 = 2(3) + 1$ from the third line. So by substitution we get $2(31) = 2(4(7)) + 7 - 1$. Equivalently we have $2(31) = 9(7) - 1$. Multiply both sides of $162 = 5(31) + 7$ by nine and we get $9(162) = 45(31) + 9(7)$. But we know $9(7) = 2(31) + 1$ so by substitution we have $9(162) = 45(31) + 2(31) + 1 = 47(31) + 1$. So we have

$$9(162) - 47(31) = 1$$

Week 5

Theorem (1.38)**.** *Let a and b be integers. If $(a, b) = 1$, then there exist integers x and y such that $ax + by = 1$.*

Proof. Let a and b be natural numbers. Suppose $(a, b) = 1$. If $a = b$ then $a = b = 1$ and choose $x = 0$ and $y = 1$ and we are done. So let $a \neq b$. Without a loss of generality let $b > a$. First, suppose $x \in \mathbb{N}$. Then $x = qb + r$ where $0 \leq r \leq b - 1$ by the Division Algorithm. Then by Theorem 1.28 it follows for every natural number x we have $x \equiv r \pmod{b}$ where $0 \leq r \leq b - 1$. Now suppose we have the list

$$\begin{aligned} a(1) &\equiv r_1 \pmod{b} \\ &\equiv r_2 \pmod{b} \\ a(3) &\equiv r_3 \pmod{b} \\ &\vdots \\ a(b) &\equiv r_b \pmod{b} \end{aligned}$$

where for $r_i \colon \{1, 2, ..., b\} \to \{0, 1, ..., b - 1\}$. Here, we enumerate the remainders as we add keep adding a until we reach $a(b)$. Now we show r_i is surjective, that is, we reach every remainder from 1 to $b-1$ as we repeatedly add the quantity a. For the sake of contradiction suppose it were not. Then we must have some repeated remainder. That is, $r_i = r_j$ where $i \neq j$ and $i, j \in \{1, 2, ..., b\}$. Then we have $ai \equiv r_i \pmod{b}$ and $aj \equiv r_i \pmod{b}$ which implies $ai \equiv aj \pmod{b}$. Then by definition of congruence we have $b \mid a(i - j)$. Since a and b are relatively prime it follows $b \mid (i - j)$. However, $1 \leq i, j \leq b$ so $|i - j|$ cannot be divided by b. This is a contradiction. Therefore, there cannot be some repeated remainder. It follows r_i is surjective. Then for some $i \in \mathbb{N}$ we have $a(i) \equiv 1 \pmod{b}$. Then by definition of congruence we have $b \mid a(i) - 1$. Then by definition of divides we have $ai - 1 = kb$ for some integer k. Rearranging terms we have $ai + kb = 1$. We assumed that a and b are natural numbers. Suppose a and b are both negative integers. Then $-a$ and $-b$ are natural numbers. Then we find x and y such that $-ax - by = 1$. Then we have $a(-x) + b(-y) = 1$ so $-x$ and $-y$ are integers that work for negative integers. Suppose either are zero but not both. Without a loss of generality let $a \neq 0$ and $b = 0$. If $(a, b) = 1$ then we must have $a = -1$ or $a = 1$. If $a = -1$ then choose $x = -1$ and $y = 0$. If $a = 1$ then choose $x = 1$ and $y = 0$. This covers all cases. □

Proof. Let $P(n)$ be the statement that "if for any integers $a, b \in \mathbb{Z}$ and $a, b \geq 0$ where $(a, b) = 1$ and it takes the Euclidean Algorithm n steps to reach a remainder 1, then there exist integers x, y such that $ax + by = 1$." Now we prove the Theorem by inducting on n. Suppose $n = 1$. We show that $P(1)$ is true. Suppose we have integers $a, b \in \mathbb{Z}$ and $a, b \geq 0$ where $(a, b) = 1$ and it takes one step for the Euclidean Algorithm to reach a remainder of 1. Without a loss of generality let $a \geq b$. Since the algorithm takes one step we have $a = q_1 b + 1$ for some integer q_1. Then we have $(1)a - q_1 b = 1$. Then let $x = 1$ and $y = -q_1$ and we have $ax + by = 1$. It follows $P(1)$ is true. Now for the inductive step suppose it is true for $P(n)$. We show $P(n+1)$ must also be true. Suppose we have non-negative integers a, b such that $(a, b) = 1$ and it takes the Euclidean Algorithm $n + 1$ steps to reach a remainder of 1. Without a loss of generality let $a \geq b$. Then in the first step we have $a = q_1 b + r_1$ where

$q_1, r_1 \in \mathbb{Z}$ and $0 \leq r_1 \leq b-1$. Then to get to a remainder of 1 we perform n steps on (b, r_1). But since we assumed $P(n)$ is true by the inductive hypothesis it follows there exist integers w, z such that $bw + r_1 z = 1$. So then we have equations

$$a = q_1 b + r_1$$
$$bw + r_1 z = 1$$

which is the same as

$$az - q_1 bz - r_1 z = 0$$
$$bw + r_1 z = 1$$

Adding these equations together gives $az + b(w - q_1 z) = 1$. Let $x = z$ and $y = w - q_1 z$ and it follows $x, y \in \mathbb{Z}$ since integers are closed under addition and multiplication. Then we have $ax + by = 1$. It follows $P(n+1)$ is true. This concludes the inductive step. By induction, Theorem 1.38 holds. □

Theorem (1.39)**.** *Let a and b be integers. If there exist integers x and y with $ax + by = 1$, then $(a, b) = 1$.*

Proof. Suppose a, b, x, y are integers such that $ax + by = 1$. For the sake of contradiction suppose $(a, b) \neq 1$. Then we know let $d = (a, b)$. Without a loss of generality let $d > 1$ (for if d is negative then $-d$ is also a divisor and then $-d > d$. Since d is a common divisor we have $d \mid a$ and $d \mid b$. Then there exist integers k_1, k_2 such that $a = k_1 d$ and $b = k_2 d$. By substitution we have $k_1 dx + k_2 dy = d(k_1 x + k_2 y) = 1$. Then $d \mid 1$ but this is impossible since $d > 1$. This is a contradiction. It follows $(a, b) = 1$. □

Theorem (1.40)**.** *For any integers a and b not both 0, there are integers x and y such that*

$$ax + by = (a, b)$$

Proof. Let a and b be integers and not both be zero. Then there exists a greatest common divisor (a, b). By definition we have $(a, b) \mid a$ and $(a, b) \mid b$. Then there exist integers p, q such that $a = p(a, b)$ and $b = q(a, b)$. Then $p = a/(a, b)$ and $q = b/(a, b)$. Now we show p and q are relatively prime. For the sake of contradiction suppose they were not. Then there exists some integer $t > 1$ such that $p = k_1 t$ and $q = k_2 t$ for some integers $k_1, k_2 \in \mathbb{Z}$. Then by substitution we have $a = k_1 t(a, b)$ and $b = k_2 t(a, b)$. Then $t(a, b)$ divides both a and b and $t(a, b) > (a, b)$ since $t > 1$ thus $t(a, b)$ is a greater common divisor but this contradicts the definition of (a, b). Thus p and q are relatively prime. Then we can apply Theorem 1.38. Thus there exist integers x, y such that $px + qy = 1$. Multiplying both sides by (a, b) gives $ax + by = (a, b)$. □

Theorem (1.41)**.** *Let a, b, and c be integers. If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.*

Proof. Let a, b, and c be integers. Suppose $a \mid bc$ and $(a, b) = 1$. Then by the Theorem 1.38 it follows there exist integers x and y such that $ax + by = 1$. Since $a \mid bc$ we also have $bc = ka$ for some integer k. Together we have

$$c(ax + by = 1)$$
$$y(ak - bc = 0)$$

Add these two equations together gives $cax + yak = c$. This is the same as $a(cx + yk) = c$. Since c, x, y, k are all integers it follows (cx, yk) is an integer. Hence, by definition of divides we have $a \mid c$. □

Theorem (1.42)**.** *Let a, b, and n be integers. If* $a \mid n$*,* $b \mid n$*, and* $(a, b) = 1$*, and* $(ab, n) = 1$*, then* $ab \mid n$*.*

Proof. Let a, b, and n be integers. Suppose $a \mid n$, $b \mid n$, and $(a, b) = 1$. Then it follows $n = k_1 a$, $n = k_2 b$, and $ax + by = 1$ for where $k_1, k_2, x, y \in \mathbb{Z}$.

$$n = k_1 a$$
$$n = k_2 b$$

Multiplying the first equation by yb and the second by xa we get.

$$n(by) = yk_1 ab$$
$$n(ax) = xk_2 ba$$

Adding these two equations gives

$$n(ax + by) = ab(k_2 x + k_1 y)$$
$$n = ab(k_2 x + k_1 y)$$

Since k_1, k_2, x, y are all integers it follows that $(k_2 x + k_1 y)$ is an integer. Then by definition of divides we have $ab \mid n$. □

Week 6

Theorem (1.43)**.** *Let a, b, and n be integers. If* $(a, n) = 1$ *and* $(b, n) = 1$*, then* $(ab, n) = 1$*.*

Proof. Let a, b, and n be integers such that $(a, n) = 1$ and $(b, n) = 1$. By Theorem 1.38 it follows there exist integers x, y, w, z such that $ax + ny = 1$ and $bw + nz = 1$. This is the same as $ax = 1 - ny$ and $bw = 1 - nz$. Then we have $abwx = 1 - ny - nz + n^2yz$. This is the same as $(ab)(wx) + n(y + z - nyz) = 1$. Moreover, we know wx and $y + z - nyz$ are integers since integers are closed under addition and multiplication. It follows $(ab, n) = 1$ by Theorem 1.39. □

Question (1.44)**.** What hypotheses about a, b, c, and n could be added so that $ac \equiv bc \pmod{n}$ would imply $a \equiv b \pmod{n}$? State an appropriate theorem and prove it before reading on.

We can use Theorem 1.41. So we can add the statement $(c, n) = 1$.

Proof. Let a, b, c, and n be integers such that $ac \equiv bc \pmod{n}$ and $(n, c) = 1$. Then by definition of congruence we have $n \mid (ac - bc)$ which is equivalent to $n \mid c(a - b)$. And since $(n, c) = 1$ it follows by Theorem 1.41 that $n \mid (a - b)$. Then by definition of congruence we have $a \equiv b \pmod{n}$. □

Theorem (1.45)**.** *Let a, b, c, and n be integers with* $n > 0$*. If* $ac \equiv bc \pmod{n}$ *and* $(c, n) = 1$*, then* $a \equiv b \pmod{n}$*.*

Proof. This was proven in the proof above. □

Question (1.46)**.** Suppose a, b, and c are integers and that there is a solution to the linear Diophantine equation

$$ax + by = c$$

that is, suppose there are integers x and y that satisfy the equation $ax + by = c$. What condition must c satisfy in terms of a and b?

We know there exist integers for $ax + by = (a, b)$ so then c must be some multiple of (a, b). In other words $(a, b) \mid c$.

Question (1.47)**.** Can you make a conjecture by completing the following statement?

Conjecture. *Give integers a, b, and c, there exist integers x and y that satisfy the equation* $ax + by = c$ *if and only if* $(a, b) \mid c$*.*

Theorem (1.48)**.** *Given integers a, b, and c with a and b not both 0, there exist integers x and y that satisfy the equation* $ax + by = c$ *if and only if* $(a, b) \mid c$*.*

Proof. Let a, b, and c be integers with a and b not both 0. Then we prove the reverse direction first. We know there exist integers w, z such that $aw + bz = (a, b)$. Since $(a, b) \mid c$ by definition of divides there exists some integer k such that $c = k(a, b)$. Then we have $a(kw) + b(kz) = k(a, b)$. Then the integers kw and kz are integer solutions to the equation $ax + by = c$.

Now we prove the forward direction. Suppose there exist integers x and y that satisfy the equation $ax + by = c$. Since a and b are not both 0 then (a, b) exists. Then $(a, b) \mid a$ and $(a, b) \mid b$. Then by definition of divides there exist integers k_1, k_2 such that $a = k_1(a, b)$ and $b = k_2(a, b)$. Then by substitution we have $k_1(a, b)x + k_2(a, b)y = c$. Then we have

$c = (a, b)(k_1x + k_2y)$ and we know $k_1x + k_2y \in \mathbb{Z}$ since integers are closed under addition and multiplication. It follows $(a, b) \mid c$ by definition of divides. □

Question (1.49)**.** For integers a, b, and c, consider the linear Diophantine equation

$$ax + by = c$$

Suppose integers x_0 and y_0 satisfy the equation; that is $ax_0 + by_0 = c$. What other values

$$x = x_0 + h \text{ and } y = y_0 + k$$

also satisfy $ax + by = c$?

By substitution we get $a(x_0+h)+b(y_0+k) = c$ which results in $ah+bk = 0$. Then if a and b are not both 0 there exists $(a, b) \neq 0$. Then we can divide by (a, b) and get $n_1h + n_2k = 0$ where $a = n_1(a, b)$ and $b = n_2(a, b)$. Then n_1 and n_2 are relatively prime. Then the set of solutions are $h = n_2i$ and $k = -n_1i$ where $i \in \mathbb{Z}$. By substitution we have

$$h = \frac{b}{(a, b)}i \text{ and } k = -\frac{a}{(a, b)}i$$

Exercise (1.50)**.** A farmer lays out the sum of 1,770 crowns in purchasing horses and oxen. He pays 31 crowns for each horse and 21 crowns for each ox. What are the possible numbers of horses and oxen that the farmer bought?

We have to find integer solutions to the equations $ax + by = c$ where $a = 31$, $b = 21$, and $c = 1770$. After guessing different numbers, one solution is $x_0 = 51$ and $y_0 = 9$. Then the general form of solutions is $x = 51 + 21k$ and $y = 9 - 31k$ for some integer k. Since we are consider only non-negative solutions we possible solutions are 51 horses and 9 oxen, 30 horses and 40 oxen, and 9 horses and 71 oxen.

Theorem (1.51)**.** *Let a, b, c, x_0, and y_0 be integers with a and b not both 0 such that $ax_0 + by_0 = c$. Then the integers*

$$x = x_0 + \frac{b}{(a, b)} \text{ and } y = y_0 - \frac{a}{(a, b)}$$

also satisfy the linear Diophantine equation $ax + by = c$.

Proof. Let a, b, c, x_0, and y_0 be integers with a and b not both 0 such that $ax_0 + by_0 = c$. Then let $x = x_0 + \frac{b}{(a,b)}$ and $y = y_0 - \frac{a}{(a,b)}$. Then we get

$$\begin{aligned} ax_0 + \frac{ab}{(a, b)} + by_0 - \frac{ab}{(a, b)} &= c + \frac{ab}{(a, b)} - \frac{ab}{(a, b)} \\ &= c \end{aligned}$$

Thus x and y are solutions to the Diophantine equation. □

Week 7

Question (1.52)**.** HI

Theorem (1.53)**.** *Let a, b, and c be integers with a and b not both 0. If $x = x_0$ and $y = y_0$ is an integer solution to the equation $ax + by = c$ (that is, $ax_0 + by_0 = c$) then for every integer k, the numbers*

$$x = x_0 + \frac{kb}{(a,b)} \text{ and } y = y_0 - \frac{ka}{(a,b)}$$

are integers that also satisfy the linear Diophantine equation $ax + by = c$. Moreover; every solution to the linear Diophantine equation $ax + by = c$ is of this form.

Proof. Let a, b, and c be integers with a and b not both 0. Suppose x_0, y_0 are integer solutions to the equation $ax + by = c$. Then we show that $x = x_0 + kb/(a,b)$ and $y = y_0 - ka/(a,b)$ where $k \in \mathbb{Z}$ are also solutions the the Diophantine equation.

$$\begin{aligned} ax + by &= ax_0 + \frac{kab}{(a,b)} + by_0 - \frac{kab}{(a,b)} \\ &= c + \frac{kab}{(a,b)} - \frac{kab}{(a,b)} \\ &= c \end{aligned}$$

It follows x, y are solutions to the Diophantine equation. Now suppose x_1, y_1 are solutions to the Diophantine equation, that is $ax_1 + by_1 = c$. Then we show that

$$x_1 = x_0 + \frac{kb}{(a,b)} \text{ and } y_1 = y_0 + \frac{ka}{(a,b)}$$

where $k \in \mathbb{Z}$. So we have $ax_0 + by_0 = c$ and $ax_1 + by_1 = c$. Then $a(x_1 - x_0) + b(y_1 - y_0) = 0$. Then if we divide both sides by (a,b) we get $p(x_1 - x_0) + q(y_1 - y_0) = 0$ where p, q are relatively prime by Liam's Theorem. Let $\Delta x = x_1 - x_0$ and $\Delta y = y_1 - y_0$ where $\Delta x, \Delta y \in \mathbb{Z}$ since integers are closed under subtraction. Then we have $p\Delta x = -q\Delta y$. Since $q|(-q\Delta y)$ we must have $q|(p\Delta x)$ but $(q,p) = 1$ so by Theorem 1.41 it follows $q|\Delta x$. Similarly, since $p|(p\Delta x)$ we must have $p|(-q\Delta y)$ and because $(p,q) = 1$ it follows $p|-\Delta y$. Then by definition of divides we have $\Delta x = k_1 q$ and $\Delta y = -k_2 p$ for some integers k_1, k_2. Plugging these values into $p\Delta x = -q\Delta y$ results in

$$\begin{aligned} p(k_1 q) &= -q(-k_2 p) \\ k_1 &= k_2 \end{aligned}$$

So then let $k = k_1 = k_2$. Then $\Delta x = kq$ and $\Delta y = -kp$. Since $\Delta x = x_1 - x_0$ and $\Delta y = y_1 - y_0$ we have $x_1 = x_0 + \Delta x$ and $y_1 = y_0 + \Delta y$. So then $x_1 = x_0 + kq$ and $y_1 = y_0 - kp$. Moreover, $p = a/(a,b)$ and $q = b(a,b)$ so then we have

$$x_1 = x_0 + \frac{kb}{(a,b)} \text{ and } y_1 = y_0 + \frac{ka}{(a,b)}$$

where $k \in \mathbb{Z}$. □

Exercise (1.54)**.** Find all integer solutions to the equation $24x + 9y = 33$.

One solution is $x = 1$ and $y = 1$. And $(24, 9) = 3$ so then in general solutions to this Diophantine equation are of the form $x = 1 + 3k$ and $y = 1 - 8k$ for some $k \in \mathbb{Z}$.

Theorem (1.55)**.** *If a and b are integers, not both 0, and k is a natural number, then*

$$gcd(ka, kb) = k \cdot gcd(a, b)$$

Proof. By definition of gcd we have $a = q_1(a, b)$ and $b = q_2(a, b)$ for some integers q_1, q_2. Then $ka = kq_1(a, b)$ and $kb = kq_2(a, b)$. Thus it follows $k(a, b)|ka$ and $k(a, b)|kb$ so then $(ka, kb) \geq k(a, b)$. I was not able to figure out how to show $(ka, kb) \leq k(a, b)$. But showing this would be sufficient to show $(ka, kb) = k(a, b)$. □

Theorem (A)**.** *Let a and b be integers, and c be a natural number. If $a \equiv b \pmod{c}$, then $(a, c) = (b, c)$.*

Proof. Let a and b be integers and c be a natural number. Suppose $a \equiv b \pmod{c}$. By definition of congruence we have $c|(a - b)$ and by definition of divides we have $a - b = kc$ for some integer k. Then $a = kc + b$. Moreover, a and c cannot both be zero since c is a natural number. Then by Theorem 1.33 it follows $(a, c) = (c, b)$. Hence, $(a, c) = (b, c)$. □

Theorem (B)**.** *Show that if a and b are integers with $(a, b) = 1$, then $(a + b, a - b) = 1$ or 2.*

Proof. Since $(a + b, a - b)|a + b$ and $(a + b, a - b)|a - b$ it follows $(a + b, a - b)|a + b + a - b$ so $(a + b, a - b)|2a$ and similarly divides $2b$. So then $(a + b, a - b)$ is a common divisor of $2a$ and $2b$. And since $(a, b) = 1$ then gcd of 2a and 2b is 2. it follows $(a + b, a - b) = 1$ or 2. □

roof

Week 8

Exercise (1.56)**.** For natural numbers a and b, give a suitable definition for "least common multiple of a and b", denoted lcm(a,b). Construct and compute some examples.

Consider the sets

$$A = \{ka \mid k \in \mathbb{N}\}$$
$$B = \{kb \mid k \in \mathbb{N}\}$$

Then let lcm(a,b) = minimum of $A \cap B$.

Theorem (1.57)**.** *If a and b are natural numbers, then $gcd(a,b) \cdot lcm(a,b) = ab$*

Proof. Let a and b be natural numbers. Let $g = \gcd(a,b)$ and $\ell = \text{lcm}(a,b)$. We show $g\ell = ab$. By definition of g we have $a = k_1 g$ and $b = k_2 g$. Then together we have $ab = k_1 k_2 g^2$. So then $ab = g(k_1 k_2 g)$. We show $k_1 k_2 g$ is the least common multiple of a and b. Since $k_1 k_2 g = a k_2$ it follows $a | k_1 k_2 g$. And since $k_1 k_2 g = b k_1$ it follows $b | k_1 k_2 g$. It follows $k_1 k_2 g$ is a common multiple. For the sake of contradiction, suppose there were a smaller common multiple m. By definition of a multiple we have $b|m$ so then $m = q_1 b$ for some integer q_1. Moreover $b = k_2 g$ so then $m = q_1 k_2 g$. And since we assumed $m < k_1 k_2 g$ it follows

$$m = q_1 k_2 g < k_1 k_2 g$$

It follows $q_1 < k_1$. Moreover, we must have $a|m$ so then $k_1 g | q_1 k_2 g$. Then $q_1 k_2 g = h k_1 g$ for some integer h. Then $q_1 k_2 = h k_1$ so the by definition of divides we have $k_1 | q_1 k_2$. $k_1 = a/g$ and $k_2 = b/g$ so by Liam's theorem $(k_1, k_2) = 1$. Since k_1 and k_2 are relatively prime and k_1 divides $q_1 k_2$, by Theorem 1.41 it follows $k_1 | q_1$. So then $q_1 = h k_1$ where h is a natural number since q_1 and k_1 are natural numbers. Then $q_1 > k_1$ which is a contradiction. It follows there is no common multiple less than $k_1 k_2 g$. Hence $\text{lcm}(a,b) = \ell = k_1 k_2 g$. It follows $g\ell = ab$. □

The proof below was my first attempt.

Proof. Let a and b be natural numbers. Let $\gcd(a,b) = d$ and $\text{lcm}(a,b) = \ell$ We show $d\ell = ab$. For the sake of contradiction, suppose $d\ell > ab$. Then $\ell > ab/d$. Now we show ab/d is a a common multiple of a and b. By definition of greatest common divisor we have $d|a$ and $d|a$. By definition of divides, there exist integers k_1 and k_2 such that $a = k_1 d$ and $b = k_2 d$. Then

$$b = k_2 d$$
$$ab = k_2 da$$
$$ab/d = k_2 a$$

By definition of divides it follows $a|(ab/d)$. In addition we have

$$a = k_1 d$$
$$ab = k_1 db$$
$$ab/d = k_1 b$$

By definition of divides, it follows $b|(ab/d)$. It follows ab/d is a common multiple of a and b. Moreover, assumed $\ell > ab/d$. So then ab/d is a common multiple less than the least common multiple which is a contradiction. Thus, $d\ell \not> ab$

For the sake of contradiction, suppose $d\ell < ab$. Equivalently, we have $d < ab/\ell$. We show ab/ℓ is a common divisor of a and b. By definition of least common multiple we have $\ell = j_1 a$ and $\ell = j_2 b$ for some integers j_1, j_2. Then we have

$$\begin{aligned} \ell &= j_1 a \\ \ell b &= j_1 ab \\ b &= j_1(ab/\ell) \end{aligned}$$

It follows by definition of divides, that $(ab/\ell)|b$. Similarly, we have

$$\begin{aligned} \ell &= j_2 b \\ \ell a &= j_2 ab \\ a &= j_2(ab/\ell) \end{aligned}$$

By definition of divides, we have $(ab/\ell)|a$. Hence, (ab/ℓ) is a common divisor of a and b. But we assumed that $ab/\ell > d$. It follows ab/ℓ is a common divisor greater than the greatest common divisor which is a contradiction. It follows $d\ell \not< ab$. Therefore, we must have $d\ell = ab$. □

Corollary (1.58)**.** *If a and b are natural numbers, then $lcm(a, b) = ab$ if and only if a and b are relatively prime.*

Proof. Suppose a and b are natural numbers. We prove the forward direction first. Let us denoted lcm of a and b as ℓ and the gcd of a and b as d. Suppose $\ell = ab$. We know by Theorem 1.57 that $d\ell = ab$ for all natural numbers a and b. Then $d = 1$. Then by definition a and b are relatively prime.

Now we prove the reverse direction. If a and b are relatively prime, then by definition we have $d = 1$. Since $d\ell = ab$ it follows $\ell = ab$. This concludes the proof. □

Definition. A natural number $p > 1$ is prime if and only if p is not the product of natural numbers less than p.

Definition. A natural number n is composite if and only if n is a product of natural numbers less than n.

Theorem (2.1)**.** *If n is a natural number greater than* 1*, then there exists a prime p such that $p|n$.*

Proof. We prove this theorem by strong induction. Let $P(n)$ be the statement that "there exists a prime p such that $p|n$." We show $P(n)$ is true for all natural numbers greater than 1, that is, $n \geq 2$. For the base case consider the natural number 2. The only possible product of two natural numbers is $2 \times 1 = 2$. Then by definition, 2 is prime. It follows $P(2)$ is true since a prime number divides itself.

Now we move on to the inductive step. Let the inductive hypothesis be $P(k)$ is true for all natural numbers k where $2 \leq k \leq m$ for some natural number $m \geq 2$. Now we show $P(m + 1)$ must be true. There are two cases: either m+1 is prime or composite. If $m + 1$ is prime then we are done since any prime number divides itself. Now suppose $m + 1$ is composite. Then $m + 1 = k_1 \times k_2$ for some natural numbers k_1 and k_2 where $2 \leq k_1, k_2 \leq m$. By the inductive hypothesis, we know $P(k_1)$ is true. It follows there exists some prime p

such that $p|k_1$. Then we have $k_1 = qp$ for some integer q. Then we have

$$\begin{aligned} m+1 &= k_1 \times k_2 \\ &= q \times p \times k_2 \\ &= (q \times k_2) \times p \end{aligned}$$

Since q and k_2 are integers it follows $q \times k_2$ is an integer since integers are closed under multiplication. By definition of divides we have $p|(m+1)$. Hence, $P(m+1)$ is true. This concludes the induction. It follows $P(n)$ is true for all natural numbers $n \geq 2$. □

Exercise (2.2)**.** Write down the primes less than 100 without the aid of a calculator or a table of primes and think about how you decide whether each number you select is prime or not.

2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97. I check if the numbers are divisible by 2,3,5, or 7.

Theorem (2.3)**.** *A natural number $n > 1$ is prime if and only if for all primes $p \leq \sqrt{n}$, p does not divide n.*

Proof. Suppose we have a natural number n. We prove the forward direction first. Suppose n is prime. By definition of a prime we know n is not a product of natural numbers less than n. For the sake of contradiction, suppose there exists some natural number k_1 such that $1 < k_1 < n$ and $k_1|n$. Then $n = k_1k_2$ where k_2 is some natural number. Then we have

$$1 < \frac{k_1}{k_1} < \frac{n}{k_1} = k_2 < n$$

It follows $1 < k_2 < n$. Then n is a product of two natural numbers less than n, k_1 and k_2. This is a contradiction. It follows there does not exist any natural number k where $1 < k < n$ such that $k|n$. If we have some prime p such that $1 < p \leq \sqrt{n}$, it follows $1 < p < n$ so then $p \nmid n$.

Now we prove the reverse direction by proving the contrapositive. Suppose the natural number $n > 1$ is not prime. Then there exists some natural numbers $1 < k_1, k_2 < n$ such that $n = k_1k_2$. There are two cases: either $k_1 = k_2$ or $k_1 \neq k_2$. If $k_1 = k_2$, then we have $1 < k_1^2 = n$. Then $1 < k_1 \leq \sqrt{n}$. By Theorem 2.1, we know there exists a prime p such that $p|k_1$. Then by definition of divides we have $k_1 = ap$ for some integer a. Moreover, a must be positive since k_1 and p are both natural numbers. Since $k_1^2 = n$ we have $a^2p^2 = n$. Then $n = (a^2p)p$. Moreover, a^2p is an integer since a and p are integers and integers are closed under multiplication. Then by definition of divides, we have $p|n$. Moreover, since $k_1 = ap$ and $1 < k_1 < \sqrt{n}$ and a is positive, we have

$$1 < p < k_1 < \sqrt{n}$$

It follows $1 < p < \sqrt{n}$ and $p|n$

Now suppose $k_1 \neq k_2$. Without a loss of generality let $k_1 < k_2$. Since $k_1k_2 = n$ and $k_1 < k_2$ it follows $k_1^2 < n$ so then $1 < k_1 < \sqrt{n}$. Since $k_1 > 1$ it follows by Theorem 2.1 there exists a prime p such that $p|k_1$. Then by definition of divides there exists integer b such that $k_1 = bp$. Since $k_1k_2 = n$ we have $bpk_2 = (bk_2)p = n$. Note bk_2 is an integer is since b and k_2 are integers and integers are closed under multiplication. Then by definition of divides, we have $p|n$. It follows there exists a prime p such that $1 < p < \sqrt{n}$ and $p|n$.

In both cases where $k_1 = k_2$ and $k_1 \neq k_2$ we have shown there exists a prime number p such that $1 < p < \sqrt{n}$ and $p|n$. It follows, we have proven the contrapositive of the reverse direction of Theorem 2.3 $\square$

Exercise (2.4)**.** Use the preceding theorem to verify that 101 is prime.

By Theorem 2.3 we only check if primes $p|101$ such that $p < \sqrt{101}$. Since $100 < 101 < 121$ it follows $10 < \sqrt{101} < 11$ we only check primes that are less than or equal to 10. Those primes are $2, 3, 5, 7$.

$$101 = 50(2) + 1$$
$$101 = 33(3) + 2$$
$$101 = 20(5) + 1$$
$$101 = 14(7) + 3$$

It follows 101 is prime.

Exercise (Sieve of Eratosthenes(2.5))**.** Write down all the natural numbers from 1 to 100, perhaps on a 10×10 array. Circle the number 2, the smallest prime. Cross off all numbers divisible by 2. Circle 3, the next number that is not crossed out. Cross off all larger numbers that are divisible by 3. Continue to circle the smallest number that is not crossed out and cross out its multiples. Repeat. Why are the circled numbers all the primes less than 100?

Because we cancelled out all multiples of primes. What is left are numbers that are not divisible by primes smaller then themselves which by Theorem 2.3 implies they are prime.

Exercise (2.6)**.** For each natural number n, define $\pi(n)$ to be the number of primes less than or equal to n.

(1) Graph $\pi(n)$ for $n = 1, 2, ..., 100$.
(2) Make a guess about approximately how large $\pi(n)$ is relative to n.

Week 9

Problem (Liam's). Let a and b be natural numbers, and let $\ell = \text{lcm}(a, b)$. Then $\ell | ab$.

Proof. By the lemma below we know that $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$. Then by definition of divides, it follows $\ell | ab$. □

Lemma. *If a and b are natural numbers, then gcd$(a, b) \cdot$ lcm$(a, b) = ab$.*

Proof. Let a and b be natural numbers. Let $g = \gcd(a, b)$ and $\ell = \text{lcm}(a, b)$. We show $g\ell = ab$. By definition of g we have $a = k_1 g$ and $b = k_2 g$. Then together we have $ab = k_1 k_2 g^2$. So then $ab = g(k_1 k_2 g)$. We show $k_1 k_2 g$ is the least common multiple of a and b. Since $k_1 k_2 g = a k_2$ it follows $a | k_1 k_2 g$. And since $k_1 k_2 g = b k_1$ it follows $b | k_1 k_2 g$. It follows $k_1 k_2 g$ is a common multiple. For the sake of contradiction, suppose there were a smaller common multiple m. By definition of a multiple we have $b | m$ so then $m = q_1 b$ for some integer q_1. Moreover $b = k_2 g$ so then $m = q_1 k_2 g$. And since we assumed $m < k_1 k_2 g$ it follows

$$m = q_1 k_2 g < k_1 k_2 g$$

It follows $q_1 < k_1$. Moreover, we must have $a | m$ so then $k_1 g | q_1 k_2 g$. Then $q_1 k_2 g = h k_1 g$ for some integer h. Then $q_1 k_2 = h k_1$ so the by definition of divides we have $k_1 | q_1 k_2$. $k_1 = a/g$ and $k_2 = b/g$ so by Liam's theorem $(k_1, k_2) = 1$. Since k_1 and k_2 are relatively prime and k_1 divides $q_1 k_2$, by Theorem 1.41 it follows $k_1 | q_1$. So then $q_1 = h k_1$ where h is a natural number since q_1 and k_1 are natural numbers. Then $q_1 > k_1$ which is a contradiction. It follows there is no common multiple less than $k_1 k_2 g$. Hence $\text{lcm}(a, b) = \ell = k_1 k_2 g$. It follows $g\ell = ab$. □

Theorem (2.3)**.** *A natural number $n > 1$ is prime if and only if for all primes $p \leq \sqrt{n}$, p does not divide n.*

Proof. Suppose we have a natural number n. We prove the forward direction first. Suppose n is prime. By definition of a prime we know n is not a product of natural numbers less than n. For the sake of contradiction, suppose there exists some natural number k_1 such that $1 < k_1 < n$ and $k_1 | n$. Then $n = k_1 k_2$ where k_2 is some natural number. Then we have

$$1 < \frac{k_1}{k_1} < \frac{n}{k_1} = k_2 < n$$

It follows $1 < k_2 < n$. Then n is a product of two natural numbers less than n, k_1 and k_2. This is a contradiction. It follows there does not exist any natural number k where $1 < k < n$ such that $k | n$. If we have some prime p such that $1 < p \leq \sqrt{n}$, it follows $1 < p < n$ so then $p \nmid n$.

Now we prove the reverse direction by proving the contrapositive. Suppose the natural number $n > 1$ is not prime. Then there exists some natural numbers $1 < k_1, k_2 < n$ such that $n = k_1 k_2$. There are two cases: either $k_1 = k_2$ or $k_1 \neq k_2$. If $k_1 = k_2$, then we have $1 < k_1^2 = n$. Then $1 < k_1 \leq \sqrt{n}$. By Theorem 2.1, we know there exists a prime p such that $p | k_1$. Then by definition of divides we have $k_1 = ap$ for some integer a. Moreover, a must be positive since k_1 and p are both natural numbers. Since $k_1^2 = n$ we have $a^2 p^2 = n$. Then $n = (a^2 p)p$. Moreover, $a^2 p$ is an integer since a and p are integers and integers are closed under multiplication. Then by definition of divides, we have $p | n$. Moreover, since $k_1 = ap$ and $1 < k_1 < \sqrt{n}$ and a is positive, we have

$$1 < p < k_1 < \sqrt{n}$$

It follows $1 < p < \sqrt{n}$ and $p | n$

Now suppose $k_1 \neq k_2$. Without a loss of generality let $k_1 < k_2$. Since $k_1 k_2 = n$ and $k_1 < k_2$ it follows $k_1^2 < n$ so then $1 < k_1 < \sqrt{n}$. Since $k_1 > 1$ it follows by Theorem 2.1 there exists a prime p such that $p|k_1$. Then by definition of divides there exists integer b such that $k_1 = bp$. Since $k_1 k_2 = n$ we have $bpk_2 = (bk_2)p = n$. Note bk_2 is an integer is since b and k_2 are integers and integers are closed under multiplication. Then by definition of divides, we have $p|n$. It follows there exists a prime p such that $1 < p < \sqrt{n}$ and $p|n$.

In both cases where $k_1 = k_2$ and $k_1 \neq k_2$ we have shown there exists a prime number p such that $1 < p < \sqrt{n}$ and $p|n$. It follows, we have proven the contrapositive of the reverse direction of Theorem 2.3 □

Theorem (2.7–**Fundamental Theorem of Arithmetic-Existence Part**)**.** *Every natural number greater than* 1 *is either a prime number or it can be expressed as a finite product of prime numbers. That is, for every natural number n greater than 1, there exist distinct primes* $p_1, p_2, ..., p_m$ *and natural numbers* $r_1, r_2, ..., r_m$ *such that*

$$n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$

Proof. We prove by strong induction. Let $P(i)$ be the statement that natural number i is either prime or can be expressed as a finite product of prime numbers.

For the base case consider the natural number 2. Since 2 is prime we are done. It follows $P(2)$ holds. Now we move on to the inductive step. Assume $P(i)$ is true for all $1 \leq i \leq k$ where $k \in \mathbb{N}$. We show that $P(k+1)$ is true. If $k+1$ is prime we are done. If $k+1$ is not prime, then it is the product of two natural numbers j_1, j_2 such that $1 < j_1, j_2 < k+1$. By the inductive hypothesis we have $P(j_1)$ and $P(j_2)$ are both true. Then

$$j_1 = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$
$$j_2 = q_1^{s_1} q_2^{s_2} \cdots q_n^{s_n}$$

Then $k+1 = j_1 j_2$ which is a finite product of primes. They are not necessarily distinct since they may share primes. Then for every pair of primes shared between j_1 and j_2 we combine them by add their exponents together. We express this more formally as follows.

Let $J_1 = \{p_1, p_2, \ldots, p_m\}$ and $J_2 = \{q_1, q_2, \ldots, q_n\}$. For convenience define $T_\ell = \{1, 2, \ldots, \ell\}$ for all $\ell \in \mathbb{N}$. Take $J = J_1 \cup J_2$. Moreover, we can express J as $J = \{u_1, u_2, \ldots, u_w\}$ where $w \in \mathbb{N}$ and $w \leq m + n$. Then for all $i \in T_w$ we define v_i in three separate cases. First, if there exists $j \in T_m$ and $k \in T_n$ such that $p_j = u_i$ and $q_k = u_i$ then let $v_i = r_j + s_k$. Second, if there only exists $j \in T_m$ such that $p_j = u_i$ but there does not exist $k \in T_n$ such that $q_k = u_i$ then let $v_i = r_j$. Third, if there does not exist $j \in T_m$ such that $p_j = u_i$ but there exists $k \in T_n$ such that $q_k = u_i$ then let $v_i = s_k$. Then we have

$$k + 1 = j_1 j_2 = u_1^{v_1} u_2^{v_2} \cdots u_w^{v_w}$$

It follows $k+1$ can be expressed as a product of distinct primes. □

Lemma (2.8)**.** *Let* p *and* $q_1, q_2, ..., q_n$ *all be primes and let* k *be a natural number such that* $pk = q_1 q_2 \cdots q_n$*. Then* $p = q_i$ *for some* i*.*

Proof. Let $P(n)$ be the statement that "let p and $q_1, q_2, ..., q_n$ all be primes and let k be a natural number such that $pk = q_1 q_2 \cdots q_n$. Then $p = q_i$ for some i." We show $P(n)$ is true for all $n \in \mathbb{N}$. Consider the base case where $n = 1$. Then we have two primes p and q and a natural number k such that $pk = q$. If $p = q$ then we are done. Suppose $p \neq q$. Then by Theorem AA it follows $(p, q) = 1$. Since $q|q$ it follows $q|pk$ and because $(p, q) = 1$ by

Theorem 1.41 it follows $q|k$. Then we have $k = dq$ for some integer d. Then by substitution we have $pdq = q$ which implies $pd = 1$. But this is a contradiction since $p > 1$. It follows $p = q$. Hence, $P(1)$ is true.

Now we move on to the inductive step. Suppose we know $P(i)$ is true. We show that $P(i+1)$ must also be true. Let p and $q_1, q_2, ..., q_{i+1}$ all be primes and let k be a natural number such that $pk = q_1 q_2 \cdots q_{i+1}$. If $p = q_1$ we are done. Suppose $p \neq q_1$. Then by Theorem AA it follows $(p, q_1) = 1$. We know $q_1 | q_1 q_2 \cdots q_{i+1}$ so then $q_1 | pk$. Since $(p, q_1) = 1$ it follows from Theorem 1.41 that $q_1 | k$. Then we have $k = dq_1$ where d is some integer. Moreover, we know $k, q_1 > 1$ so then d is a natural number. Then we have

$$pdq_1 = q_1 q_2 \cdots q_{i+1}$$

which implies

$$pd = q_2 q_3 \cdots q_{i+1}$$

The right hand side is a product of i primes. By the inductive hypothesis we know $P(i)$ to be true so then $p = q_j$ for some $j = \{2, 3, ..., i+1\}$. Hence, $P(i+1)$ is true. This concludes the induction. It follows $P(n)$ is true for all $n \in \mathbb{N}$. □

Theorem (**AA**). *Suppose p and q are two primes. Then $(p, q) = 1$.*

Proof. Let p and q be two distinct primes. Suppose $(p, q) > 1$. Then $(p, q)|p$ and $(p, q)|q$ so then $p = m_1(p, q)$ and $q = m_2(p, q)$ for some integers m_1 and m_2. Without a loss of generality let $p > q$. Suppose $(p, q) = p$ Then

$$q = m_2(p, q) = m_2 p$$

which implies

$$q \geq p$$

which is a contradiction. So we have $1 < (p, q) < p$. Since $(p, q) > 1$ and $p = m_1(p, q)$ it follows $m_1 < p$ and since $(p, q) < p$ it follows $m_1 > 1$. So then we have $1 < m_1, (p, q) < p$. It follows p is composite which is a contradiction. Therefore, $(p, q) = 1$. □

Theorem (2.9–**Fundamental Theorem of Arithmetic-Uniqueness part**). *Let n be a natural number. Let $\{p_1, p_2, ..., p_m\}$ and $\{q_1, q_2, ..., q_s\}$ be sets of primes with $p_i \neq p_j$ if $i \neq j$ and $q_i \neq q_j$ if $i \neq j$. Let $\{r_1, r_2, ..., r_m\}$ and $\{t_1, t_2, ..., t_s\}$ be sets of natural numbers such that*

$$\begin{aligned} n &= p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \\ &= q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s} \end{aligned}$$

Then $m = s$ and $\{p_1, p_2, ..., p_m\} = \{q_1, q_2, ..., q_s\}$.

Proof. We prove by inducting on m. Let $P(m)$ be the statement "Let n be a natural number. Let $\{p_1, p_2, ..., p_m\}$ and $\{q_1, q_2, ..., q_s\}$ be sets of primes with $p_i \neq p_j$ if $i \neq j$ and $q_i \neq q_j$ if $i \neq j$. Let $\{r_1, r_2, ..., r_m\}$ and $\{t_1, t_2, ..., t_s\}$ be sets of natural numbers such that

$$\begin{aligned} n &= p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \\ &= q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s} \end{aligned}$$

Then $m = s$ and $\{p_1, p_2, ..., p_m\} = \{q_1, q_2, ..., q_s\}$." We show $P(m)$ is true for all natural numbers m. Consider the base case $m = 1$. Then we have a sets of primes $\{p\}$ and $\{q_1, ..., q_s\}$ and sets of natural numbers $\{r\}$ and $\{t_1, ..., t_s\}$ such that

$$\begin{aligned} n &= p^r \\ &= q_1^{t_1} \cdots q_s^{t_s} \end{aligned}$$

Then we have $p^r = q_1^{t_1} \cdots q_s^{t_s}$. Then we have $p(p^{r-1}) = q_1^{t_1} \cdots q_s^{t_s}$. Then by Theorem 2.8 we know that $p = q_i$ for some $i \in \{1, ..., s\}$. Now we show $r = t_i$. For the sake of contradiction and without a loss of generality, suppose $r > t_i$. Then we divide both sides by t_i and we are left with

$$p^{r-t_i} = q_1^{t_1} \cdots q_i^{t_i} \cdots q_s^{t_s}$$

Then

$$p(p^{r-t_i-1}) = q_1^{t_1} \cdots q_i^{t_i} \cdots q_s^{t_s}$$

which implies $p = q_k$ for some $k \neq i$ which is a contradiction since each prime q is distinct. A similar case holds for when $r < t_i$. It follows $r = t_i$. Then $p = q_i$ and $r = t_i$. Then if we divide both sides by p_r we get

$$1 = q_1^{t_1} \cdots q_{i-1}^{t_{i-1}} \cdots q_{i+1}^{t_{i+1}} \cdots q_s^{t_s}$$

This is a contradiction. It follows we only have a unique factorization $n = p^r$.

Now we move on to the inductive step. Suppose we know $P(m)$ to be true. We show $P(m+1)$ to also be true. Suppose we have

$$\begin{aligned} n &= p_1^{r_1} \cdots p_{m+1}^{r_{m+1}} \\ &= q_1^{t_1} \cdots q_s^{t_s} \end{aligned}$$

Then we have $p_1(p_1^{r_1-1} p_2^{r_2} \cdots p_{m+1}^{r_{m+1}}) = q_1^{t_1} \cdots q_s^{t_s}$. Again, by Lemma 2.8 we know $p_1 = q_i$ for some $i \in \{1, 2, ..., s\}$. And by the same argument as we did in the base case, it follows $p_1 = q_i$ and $r_1 = t_i$. Then dividing both sides by $p_1^{r_1}$ gives

$$p_2^{r_2} \cdots p_{m+1}^{r_{m+1}} = q_1^{t_1} \cdots q_{i-1}^{t_{i-1}} \cdot q_{i+1}^{t_{i+1}} \cdots q_s^{t_s}$$

Then by the inductive hypothesis, we know $|\{p_2, ..., p_{m+1}\}| = |\{q_1, ..., q_{i-1}, q_{i+1}, q_s\}|$ and that $\{p_2, ..., p_{m+1}\} = \{q_1, ..., q_{i-1}, q_{i+1}, q_s\}$. It follows $P(m+1)$ is true. □

Dr. Miner said we should at least get to 2.9. So the other problems can be done later.

Theorem (2.12)**.** *Let a and b be natural numbers greater than 1 and let $p_1^{r_1}p_2^{r_2}\cdots p_m^{r_m}$ be the unique prime factorization of a and let $q_1^{t_1}q_2^{t_2}\cdots q_s^{t_s}$ be the unique prime factorization of b. Then $a|b$ if and only if for all $i \leq m$ there exists a $j \leq s$ such that $p_i = q_j$ and $r_i \leq t_j$.*

Proof. We prove the reverse direction first. Let $P = \{p_1, p_2, ..., p_m\}$ and $Q = \{q_1, q_2, ..., q_s\}$. Since for all $i \leq m$ there exists $j \leq s$ such that $p_i = q_j$, it follows $P \subset Q$. Then let $H = Q - P = \{h_1, h_2, ..., h_k\}$ where H contains all the primes that are not in P. And the associated powers of the primes in H are $u_1, ..., u_k$. Construct the sequence $\{x_i\}$ where $i \in \{1, 2, ..., m\}$ such that $x_i = j$ where $p_i = q_j$. Then

$$\begin{aligned} b &= (q_{x_1}^{t_{x_1}} q_{x_2}^{t_{x_2}} \cdots q_{x_m}^{t_{x_m}})(h_1^{u_1} h_2^{u_2} \cdots h_k^{u_k}) \\ &= (q_{x_1}^{r_1} q_{x_2}^{r_2} \cdots q_{x_m}^{r_m})(q_{x_1}^{t_{x_1}-r_1} q_{x_2}^{t_{x_2}-r_2} \cdots q_{x_m}^{t_{x_m}-r_m})(h_1^{u_1} h_2^{u_2} \cdots h_k^{u_k}) \\ &= a(q_{x_1}^{t_{x_1}-r_1} q_{x_2}^{t_{x_2}-r_2} \cdots q_{x_m}^{t_{x_m}-r_m})(h_1^{u_1} h_2^{u_2} \cdots h_k^{u_k}) \end{aligned}$$

Since $t_{x_i} \geq r_i$ for all $i \in \{1, 2, ..., m\}$ it follows $(q_{x_1}^{t_{x_1}-r_1} q_{x_2}^{t_{x_2}-r_2} \cdots q_{x_m}^{t_{x_m}-r_m})(h_1^{u_1} h_2^{u_2} \cdots h_k^{u_k})$ is an integer. Then $a \mid b$ by definition of divides.

Now we prove the forward direction. We prove the contrapositive. Suppose there exists some $i \leq m$ such that for all $j \leq s$ we have $p_i \neq q_j$. Since all q_j are prime and $p_i > 1$ it follows $p_i \nmid q_j$ for all $j \leq s$. Then $p_i \nmid b$ since it did then $kp_i = b$. Then b divides kp_i but $(p_i, b) = 1$ so $b|k$ but $k < b$ which is a contradiction. Since $p_i \nmid b$ it follows $a \nmid b$. This proves the contrapositive. □

Theorem (2.13)**.** *If a and b are natural numbers and $a^2 \mid b^2$, then $a \mid b$.*

Proof. Suppose $a^2 \mid b^2$. Let $a = p_1^{r_1}p_2^{r_2}\cdots p_m^{r_m}$ and $b = q_1^{t_1}q_2^{t_2}\cdots q_s^{t_s}$. If $a^2 \mid b^2$, then by Theorem 2.12 it follows for all $i \leq m$ there exists a $j \leq s$ such that $p_i = q_j$ and $2r_i \leq 2t_j$. But this implies that $r_i \leq t_i$ for all $i \leq m$ so then $a \mid b$. □

Exercise (2.14)**.** Find $(3^{14} \cdot 7^{22} \cdot 11^5 \cdot 17^3, 5^2 \cdot 11^4 \cdot 13^8 \cdot 17)$

$\gcd = 11^4 \cdot 17$

Exercise (2.15)**.** Find $\text{lcm}(3^{14} \cdot 7^{22} \cdot 11^5 \cdot 17^3, 5^2 \cdot 11^4 \cdot 13^8 \cdot 17)$

$\text{lcm} = 3^{14} \cdot 5^2 \cdot 7^{22} \cdot 11^5 \cdot 13^8 \cdot 17^3$.

Theorem (2.16)**.**

Proof. Let $g = \gcd(a, b) = \prod_{i=1}^{u} g_i^{\min(r_i, t_i)}$. Suppose there exists some common divisor $g' > g$. By Theorem 2.12, it follows that the primes in the unique prime factorization of g' consists of primes in $P \cap Q$. Then if $g' > g$, we must have $g' = dg$ where d is a product of primes in $P \cap Q$. Then we have

$$g' = \prod_{i=1}^{u} g_i^{\min(r_i, t_i)+k_i}$$

where $k_i \geq 0$ is some integer. Since $g' > g$ we must have $k_i \geq 1$ for some $i \in \{1, 2, ..., u\}$. Then suppose we try to divide a and b by g'. Then let j be the natural number such that $k_j > 0$. Then without a loss of generality, let $r_j < \min(r_j, t_j) + k_j$. Then by Theorem 2.12 it follows g' does not divide a. Hence g is the greatest common divisor.

Similarly, let $\ell = \prod_{i=1}^{v} \ell_i^{\max(r_i,t_i)}$. Suppose there exists some $\ell' < \ell$ such that $a \mid \ell'$ and $b \mid \ell'$. By the same argument as above we must have $\ell' = \prod_{i=1}^{v} \ell_i^{\max(r_i,t_i)-z_i}$ where $z_i \leq 0$ and $z_j < 0$ for some $j \in \{1, 2, ..., v\}$. But then by Theorem 2.12, this would be a contradiction to $a \mid \ell'$ and $b \mid \ell'$. Hence, ℓ is the least common multiple. □

Question (2.17)**.** Do you think this method is always better, always worse, or sometimes better and sometimes worse than using the Euclidean Algorithm to find (a, b)? Why?

I feel like for at least very large numbers, computationally using Theorem 2.16 is better since the computation doesn't get harder when the powers are very large. It is hard to do the Euclidean Algorithm for extremely large numbers.

Theorem (2.19)**.** *There do not exist natural numbers m and n such that $7m^2 = n^2$.*

Proof. For the sake of contradiction, suppose there did. Then by definition of divides we have $7 \mid n^2$. Then by Theorem 2.13 it follows $\sqrt{7} \mid n$ which is a contradiction since 7 is prime and hence $\sqrt{7}$ is not an integer. □

Theorem (2.20)**.** *There do not exist natural numbers m and n such that $24m^3 = n^3$.*

Proof. For the sake of contradiction, suppose there did. Then by definition of divides we have $24m^3 = n^3$. Then $24 \mid n^3$. By the lemma below it follows $24^{1/3} \mid n$. However, $24^{1/3}$ is not an integer. $8 < 24 < 27$ so then $2 < 24^{1/3} < 3$. This is a contradiction. □

Lemma (A)**.** *If a, b, and k are natural numbers and $a^k \mid b^k$ then $a \mid b$.*

Proof. Suppose $a^k \mid b^k$. Let $a = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ and $b = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$. If $a^2 \mid b^2$, then by Theorem 2.12 it follows for all $i \leq m$ there exists a $j \leq s$ such that $p_i = q_j$ and $kr_i \leq kt_j$. But this implies that $r_i \leq t_i$ for all $i \leq m$ so then $a \mid b$. □

Exercise (2.21)**.** Show that $\sqrt{7}$ is irrational. That is, there do not exist natural numbers n and m such that $\sqrt{7} = n/m$.

By application of Theorem 2.24.

Exercise (2.22)**.** Show that $\sqrt{12}$ is irrational.

By application of Theorem 2.24.

Exercise (2.23)**.** Show that $7^{1/3}$ is irrational.

By application of Theorem 2.24.

Theorem (2.24)**.**

Proof. Let $n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$. Suppose $d \nmid r_i$ for some i. Then for $n^{1/d}$ we have $p_i^{r_i/d}$ and $r_i/d \notin \mathbb{N}$. Now we show that $p_i^{r_i/d}$ is irrational. For the sake of contradiction, suppose it were rational. Then $p_i^{r_i/d} = n/m$ where n and m are relatively prime. Note $n/m \neq 1$ since 1 to any power is one and one is not prime. Then $m^d p_r^{r_i} = n^d$. By Lemma A proved above this would imply $m|n$ and since we assumed $m/n \neq 1$, this implies m and n are not relatively prime. This is a contradiction. It follows $p_i^{r_i/d}$ is irrational. Hence $n^{1/d}$ is irrational. □

Week 11

Theorem (2.25)**.** *Let a, b, and n be integers. If $a \mid n$, $b \mid n$, and $(a, b) = 1$, then $ab \mid n$.*

Proof. Since $(a, b) = 1$ there exist integers x and y such that $ax + by = 1$. Since $a \mid n$ and $b \mid n$ we have $n = ja$ and $n = kb$ for some integers j and k. Then we have $nax + nby = n$. By substitution, we have $kabx + jaby = n$. Then we have $ab(kx + jy) = n$ where $(kx + jy) \in \mathbb{Z}$ since integers are closed under addition and multiplication. Then we have $ab \mid n$ by definition of divides. □

Theorem (2.26)**.** *Let p be a prime and let a be an integer. Then p does not divide a if and only if $(a, p) = 1$.*

Proof. We prove the forward direction first. Since p is prime there are only two possible common divisors of p and a, which are 1 and p. However, if p does not divide a, then the only common divisor is 1. Hence, $(a, p) = 1$.

Now we prove the reverse direction. Suppose $(a, p) = 1$. For the sake of contradiction, suppose $p \mid a$. Well $p \mid p$ as well so then p would be a common divisor which is greater than (a, p). This is a contradiction. Hence $p \nmid a$. □

Theorem (2.27)**.** *Let p be a prime and let a and b be integers. If $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. Let p be prime and let a and b be integers. Suppose $p \mid ab$. If $(a, p) = 1$, then by Theorem 1.41 it follows $p \mid b$. If $(a, p) > 1$, then the greater common divisor must be p since p has only two divisors, one and itself. Then $p \mid a$. □

Theorem (2.28)**.** *Let a, b, and c be integers. If $(b, c) = 1$, then $(a, bc) = (a, b) \cdot (a, c)$.*

Proof. Let a, b, and c be integers such that $(b, c) = 1$. First we show that $(a, bc) \mid (a, b) \cdot (a, c)$. By Theorem 1.38 there exists integers such that

$$ax_1 + by_1 = (a, b)$$
$$ax_2 + cy_2 = (a, c)$$

The multiplying these gives

$$a(ax_1x_2 + cx_1y_2 + bx_2y_1) + bc(y_1y_2) = (a, b)(a, c)$$

Hence, Theorem 1.48 we have $(a, bc) \mid (a, b)(a, c)$. Now we show $(a, b)(a, c) \mid (a, bc)$.

First we show $(a, b)(a, c)$ is a common divisor of a and bc. We show that (a, b) and (a, c) are relatively prime. For the sake of contradiction suppose they are not relatively prime. Then there exists divisor $d > 1$ such that $d \mid (a, b)$ and $d \mid (a, c)$. Then we have $(a, b) = k_1d$ and $(a, c) = k_2d$ for some integers k_1, k_2. Since $(a, b) \mid b$ and $(a, c) \mid c$, we have $b = j_1k_1d$ and $c = j_2k_2d$ where $j_1, j_2 \in \mathbb{Z}$. Then $d \mid b$ and $d \mid c$. This is a contradiction since $(b, c) = 1$.

Hence $\gcd((a, b), (a, c)) = 1$. Since $(a, b) \mid a$ and $(a, c) \mid a$ and $\gcd((a, b), (a, c)) = 1$ it follows $(a, b)(a, c) \mid a$ by Theorem 1.42. Now we show $(a, b)(a, c) \mid bc$. Since $(a, b) \mid b$ we have $b = t_1(a, b)$ and since $(a, c) \mid c$ we have $c = t_2(a, c)$. Then $bc = t_1t_2(a, b)(a, c)$. Hence, by definition of divides we have $(a, b)(a, c) \mid bc$.

Since $(a, b)(a, c) \mid a$ and $(a, b)(a, c) \mid bc$. It follows $(a, b)(a, c)$ is a common divisor. By Lemma A we know that any common divisor divides the greatest common divisor. Hence $(a, b)(a, c) \mid (a, bc)$.

Since $(a, b)(a, c) \mid (a, bc)$ and $(a, bc) \mid (a, b)(a, c)$ it follows $(a, b)(a, c) = (a, bc)$

□

Lemma (A)**.** *Let a and b be integers and let a and b not both be zero. If d is a common divisor, then $d \mid (a, b)$.*

Proof. Suppose d is a common divisor. Then we have $a = q_1 d$ and $b = q_2 d$ for some integers q_1 and q_2. Then $\gcd(a, b) = \gcd(q_1 d, q_2 d) = d \gcd(q_1, q_2)$. Hence, by definition of divides, $d \mid \gcd(a, b)$. □

Theorem (2.29)**.** *Let a, b, and c be integers. If $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$*

Proof. Since $(a, b) = 1$ and $(a, c) = 1$, by Theorem 1.38, there exist integers x, y, z, and w such that $ax + by = 1$ and $az + cw = 1$. Then $by = 1 - ax$ and $cw = 1 - az$. Then $bcyw = 1 - ax - az + a^2xz$. Then we have

$$a(x + z + axz) + bc(yw) = 1$$

And we know $(x + z + axz)$ and (yw) are integers since integers are closed under addition and multiplication. It follows by Theorem 1.39 that $(a, bc) = 1$. □

Theorem (2.30)**.** *Let a and b be integers. If $(a, b) = d$, then $(\frac{a}{d}, \frac{b}{d}) = 1$.*

Proof. Let a and b be integers. Let $d = (a, b)$. Let $p = a/d$ and $q = b/d$. Now we show $(p, q) = 1$. For the sake of contradiction, suppose $(p, q) > 1$. Then there exists some e such that $e \mid p$ and $e \mid q$. Then by definition of divides, we have $p = k_1 e$ and $q = k_2 e$. for some integers k_1 and k_2. Then we have $a = pd = k_1 ed$ and $b = qd = k_2 ed$ so then $ed \mid a$ and $ed \mid b$ and $ed > (a, b)$ which is a contradiction. Hence, $(a/d, b/d) = 1$. □

Theorem (2.31)**.** *Let a, b, u, and v be integers. If $(a, b) = 1$ and $u \mid a$ and $v \mid b$ then $(u, v) = 1$.*

Proof. Let a, b, u, and v be integers such that $(a, b) = 1$, $u \mid a$, and $v \mid b$. For the sake of contradiction, suppose $(u, v) > 1$. Let $d = (u, v)$. Then $u = k_1 d$ and $v = k_2 d$ for some integers k_1 and k_2. Since $u \mid a$ and $v \mid b$ we have $a = j_1 u$ and $b = j_2 v$ for some integers j_1 and j_2. Then by substitution we have $a = j_1 k_1 d$ and $b = j_2 k_2 d$. Then $d \mid a$ and $d \mid b$ and $d > 1 = (a, b)$. This is a contradiction. Hence, $(u, v) = 1$. □

Week 12

Theorem (2.32)**.** *For all natural numbers, n, $(n, n+1) = 1$.*

Proof. $n+1 = (1)(n)+1$. Then by Theorem 1.33 we have $(n+1, n) = (n, 1)$. Since the only positive divisor in common with n and 1 is 1, we have $(n, 1) = 1$. Hence, $(n+1, n) = 1$. □

Theorem (2.33)**.** *Let k be a natural number. Then there exists a natural number n such that no natural number less than k and greater than 1 divides n.*

Proof. Take $n = (1 \cdot 2 \cdot 3 \cdot \cdots \cdot (k-1)) + 1$. Then we have $n = mq + 1$ where $m = 1, 2, ..., (k-1)$ and $q \in \mathbb{Z}$. It follows $(n, m) = (m, 1) = 1$. Hence, no natural number m where $1 < m < k$ divides n. □

Theorem (2.34)**.** *Let k be a natural number. Then there exists a prime larger than k.*

Proof. By Theorem 2.35, it follows there are infinitely many primes. For the sake of contradiction suppose there exists some natural number k such that there is no prime number larger than k. Then there is at most k primes. Hence, there is a finite number of primes. However, this contradicts Theorem 2.35. It follows for all natural numbers, there exists a prime larger than it. □

Theorem (2.35)**.** *There are infinitely many prime numbers*

Proof. For the sake of contradiction, suppose there are a finite number, say n, of primes $p_1, p_2, ..., p_n$. Then consider $p = p_1 p_2 \cdots p_n + 1$. Then we have $p = (k)(p_i) + 1$ where $k \in \mathbb{N}$. Hence by Theorem 1.33 we have $(p, p_i) = (p_i, 1) = 1$. Hence p cannot be divided by any prime less than p. Hence, p must be prime. Then there are at least $n+1$ primes which is a contradiction. Hence, there is not a finite number of primes. □

Question (2.36)**.** What were the most clever or most difficult parts in your proof of the Infinitude of Primes Theorem

The clever part was using a proof by contradiction.

Theorem (2.37)**.** *If $r_1, r_2, ..., r_m$ are natural numbers and each one is congruent to 1 modulo 4, then the product $r_1 r_2 \cdots r_m$ is also congruent to 1 modulo 4.*

Proof. Let $P(i)$ the the statement of the theorem for when $m = i$. We prove $P(i)$ is true for all $i \in \mathbb{N}$. It is trivially true for $P(1)$. Now suppose $P(k)$ is true and we have $r_i \equiv 1 \pmod 4$ for all $1 \leq i \leq k+1$. Then by the inductive hypothesis, we know $r_1 r_2 \cdots r_k \equiv 1 \pmod 4$. And since $r_{k+1} \equiv 1 \pmod 4$, by Theorem 1.14 it follows $r_1 r_2 \cdots r_{k+1} \equiv 1 \pmod 4$. Hence, $P(k+1)$ holds. This concludes the induction. □

Theorem (2.38)**.** *There are infinitely many prime numbers that are congruent to 3 modulo 4.*

Proof. Suppose there are a finite number of primes that are congruent to 3 modulo 4, say $p_1, p_2, ..., p_n$. Then consider the first m primes $q_1, q_2, ..., q_m$ such that $p_n = q_m$. Note that for all q_i we have $q_i \equiv 1 \pmod 4$ or $q_i \equiv 3 \pmod 4$ except for $q_1 = 2$. It follows by Theorem 1.14 that $q_2 \cdots q_m \equiv 1 \pmod 4$ or $q_2 \cdots q_m \equiv 3 \pmod 4$. In either case we have $q_1 \cdots q_m \equiv 2 \pmod 4$. Hence $q_1 \cdots q_m + 1 \equiv 3 \pmod 4$. Hence $q_1 \cdots q_m + 1 = 4j + 3$ for some $j \in \mathbb{N}$. Moreover, $q_1 \cdots q_m + 1$ is prime. Let $p' = q_1 \cdots q_m + 1$. □

Week 13

Theorem (C)**.** *There are infinitely many prime numbers that are congruent to 5 modulo 6.*

Theorem (2.38)**.** *There are infinitely many prime numbers that are congruent to 3 modulo 4.*

Proof. Suppose there are a finite number of $4k+3$ primes, say n of them. Let us call them $p_1, p_2, \ldots, p_n$. Then take q as

$$q = 4p_0p_1 \cdots p_n + 3$$

Note that q is odd so 2 is not a prime factor of q. Moreover, 2 is the only even prime factor. Then all other prime factors are of the form $4k+1$ or $4k+3$. Then q must contain a prime factor of the form $4k+3$. Otherwise, if all prime factors of q are of the form $4k+1$, then by Theorem 2.37 we would have q is of the form $4k+1$ which is a contradiction. Hence, q contains a prime factor of the form $p' = 4k+3$.

Now we show $p' \neq p_i$ for all $i = 1, 2, \ldots, n$. It is sufficient to show $p_i \nmid q$ for all i. for the sake of contradiction, suppose $p_i \mid q$. Since $p_i \mid q$ and $p_i \mid 4p_0p_1 \cdots p_n$ it follows $p_i \mid 3$. Then $p_i = 3$; however, 3 cannot be a factor of q since $3 \nmid 4p_0p_1 \cdots p_n$. This is a contradiction. Then p' is a factor of q and p_i is not a factor of q for all i. Hence, $p' \neq p_i$ for all p_i. This contradicts there being n primes of the form $4k+3$. Therefore, there are infinitely many $4k+3$ primes.

□

Question (2.39)**.** Are there other theorems like the previous one that you can prove?

There are infinitely many prime numbers that are congruent 5 modulo 6.

Exercise (2.40)**.** Find the current record for the longest arithmetic progression of primes.

24.

Exercise (2.41)**.** Use the polynomial long division to compute $(x^m - 1)/(x - 1)$.

$(x^m - 1)/(x - 1) = (x^{m-1} + x^{m-2} + \cdots + x + 1)$.

Theorem (2.42)**.** *If n is a natural number and $2^n - 1$ is prime, then n must be prime.*

Proof. The contrapositive is proven. Suppose n is composite. Then there exist natural numbers k and j such that $j, k > 1$ and $n = jk$. Then $2^n - 1 = 2^{jk} - 1 = (2^j)^k - 1$. Let $x = 2^j$. Then we have $x^k - 1$. Then by Exercise 2.41 we have

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

Since $j > 1$ it follows $2^j > 2$. Hence $x - 1 = 2^j - 1 > 1$. Moreover,

$$x^{k-1} + x^{k-2} + \cdots + x + 1 > x - 1$$

It follows $x^k - 1 = 2^n - 1$ is composite. □

Theorem (2.43)**.** *If n is a natural number and $2^n + 1$ is prime, then n must be a power of 2.*

Proof. The contrapositive is proven. Suppose n is a natural number and is not a power of 2. Either n is odd or even. First consider if n is odd. Then we have

$$x^n + 1 = (x + 1)(x^{n-1} - x^{n-2} + x^{n-3} - \cdots + 1)$$

for all natural numbers n that are odd. Then

$$2^n + 1 = (2+1)(2^{n-1} - 2^{n-2} + 2^{n-3} - \cdots + 1)$$

We can rewrite the right hand factor as

$$2^{n-1} - 2^{n-2} + 2^{n-3} - \cdots + 1 = 1 + \sum_{i=1}^{(n-1)/2} 2^{2i} - 2^{2i-1}$$

Moreover, $2^{2i} - 2^{2i-1} > 0$ for all $i = 1, 2, \ldots, (n-1)/2$. Hence,

$$2^{n-1} - 2^{n-2} + 2^{n-3} - \cdots + 1 > 1$$

Moreover, $3 \mid 2^n + 1$ so $2^n + 1$ is composite.

Now suppose n is even but not a power of 2. Then the prime factorization of n is

$$\begin{aligned} n &= 2^{r_1} p_2^{r_2} \cdots p_m^{r_m} \\ &= 2^{r_1} d \end{aligned}$$

where $m \geq 2$ since n is not a power of 2. Then we have

$$\begin{aligned} 2^n + 1 &= 2^{2^{r_1} d} + 1 \\ &= \left(2^{2^{r_1}}\right)^d + 1 \end{aligned}$$

where d is odd. Then we apply the previous result which gives us the following factorization

$$2^n + 1 = \left(2^{2^{r_1}} - 1\right)\left(2^{d-1} - 2^{d-2} + 2^{d-3} - \cdots + 1\right)$$

Note $r_1 \geq 1$ so $2^{2^{r_1}} - 1 > 2$ and $2^{2^{r_1}} - 1 \mid 2^n + 1$. Hence, $2^n + 1$ is composite. □

Exercise (2.44)**.** Find the first few Mersenne primes and Fermat primes.

Exercise (2.45)**.** For an A in the class and a Ph.D. in mathematics, prove that there are infinitely many Mersenne primes (or Fermat primes) or prove that there aren't (your choice).

Theorem (2.46)**.** *There exist arbitrarily long strings of consecutive composite numbers. That is, for any natural number n there is a string of more than n consecutive composite numbers.*

Proof. Suppose we want a string of $k-1$ consecutive composite numbers where k is some natural number such that $k > 2$. Note that $k! \equiv 0 \pmod{k!}$. Consider the following congruences

$$\begin{aligned} k! + 2 &\equiv 0 \pmod 2 \\ k! + 2 &\equiv 0 \pmod 3 \\ &\vdots \\ k! + k &\equiv 0 \pmod k \end{aligned}$$

So $n \mid k! + n$ for all $n = 2, 3, \ldots, k$. Then $k! + n$ is composite for all $n = 2, 3, \ldots, k$. Hence, the string

$$k! + 2, k! + 3, \ldots, k! + k$$

is a string of $k-1$ consecutive composite numbers. This holds for all $k > 2$. □

Theorem (D)**.** *If a and b are natural numbers, then the sequence $a, a+b, a+2b, \ldots$ contains an arbitrary number of consecutive composite terms. (Prove this without using Theorem 2.46)*

Question (2.47)**.** Are there infinitely many pairs of prime numbers that differ from one another by two.

Exercise (2.48)**.** Express each of the first 20 even numbers greater than 2 as a sum of two primes.

(1) $4 = 2 + 2$
(2) $6 = 3 + 3$
(3) $8 = 3 + 5$
(4) $10 = 5 + 5$
(5) $12 = 5 + 7$
(6) $14 = 7 + 7$
(7) $16 = 5 + 11$
(8) $18 = 7 + 11$
(9) $20 = 3 + 17$
(10) $22 = 5 + 17$
(11) $24 = 7 + 17$
(12) $26 = 23 + 3$
(13) $28 = 23 + 5$
(14) $30 = 23 + 7$
(15) $32 = 29 + 3$
(16) $34 = 29 + 5$
(17) $36 = 29 + 7$
(18) $38 = 31 + 7$
(19) $40 = 37 + 3$
(20) $42 = 37 + 5$

2.49 Blank Paper Exercise

Exercise (2.50)**.** Find the current record for the largest known Mersenne prime.

It is $2^{82,589,933} - 1$.

Week 14

Exercise (3.1)**.** Show that 41 divides $2^{20} - 1$.

$2^5 = 32$. And $32 - (-9) = 41$, hence, $2^5 \equiv -9 \pmod{41}$. Moreover, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$ holds. Hence, with repeated application of this property, step 2 is true. Step 3 is true by algebra and since $81 \equiv -1 \pmod{41}$ it follows $81^2 \equiv (-1)^2 \pmod{41}$. Step 4 is true since $2^{20} \equiv 1 \pmod{41}$ and by algebra we have $2^{20} - 1 \equiv 0 \pmod{41}$.

Question (3.2)**.** In your head, can you find the natural number $k, 0 \leq k \leq 11$, such that $k \equiv 37^{453} \pmod{12}$.

Note that $37 \equiv 1 \pmod{12}$ hence $37^{453} \equiv 1 \pmod{12}$. Hence $k = 1$.

Question (3.3)**.** Find natural number $k, 0 \leq k \leq 6$ such that $2^{50} \equiv k \pmod{7}$.

Note that $2^3 \equiv 1 \pmod{7}$. Hence, $(2^3)^{16} \equiv 1 \pmod{7}$. Thus, $2^{50} \equiv 4 \pmod{7}$.

Question (3.4)**.** Find natural number $k, 0 \leq k \leq 11$, such that $39^{453} \equiv k \pmod{12}$.

$39 \equiv 3 \pmod{12}$. Then $39^2 \equiv -3 \pmod{12}$. Then $39^3 \equiv 3 \pmod{12}$. Then $39^{453} \equiv 3 \pmod{12}$. Then $k = 3$.

Exercise (3.5)**.** Show that 39 divides $17^{48} - 5^{24}$.

Note that $5^4 \equiv 1 \pmod{39}$ and $17^6 \equiv 1 \pmod{39}$. Hence, $(17^6)^8 \equiv 1 \pmod{39}$ and $(5^4)^6 \equiv 1 \pmod{39}$. Then we have $39 \mid 17^{48} - 1$ and $39 \mid 5^{24} - 1$. Then we have $39 \mid 17^{48} - 1 - 5^{24} + 1$.

Question (3.6)**.** Let a, n, and r be natural numbers. Describe how to find the number k where $0 \leq k \leq n - 1$ such that $k \equiv a^r \pmod{n}$ subject to the restraint that you never multiply numbers larger than n and that you only have to do about $\log_2 r$ such multiplications.

Suppose we have a^r where a and r are natural numbers. Then

$$r = 2^j x_j + 2^{j-1} x_{j-1} + \cdots + 2^1 x_1 + 2^0 x_0$$

where $x_i = 0$ or $x_i = 1$ for all $0 \leq i \leq j$. Then we perform the following algorithm to find $2^i \equiv k \pmod{n}$ for some natural numbers n and k where $0 \leq k \leq n - 1$. Start with $2^0 \equiv R_0 \pmod{n}$. We also have $2^1 \equiv 2(R_0) \pmod{n}$ so then $2(R_0) \equiv R_1 \pmod{n}$ where $0 \leq R_0, R_1 \leq n - 1$. Now suppose we have $2^i \equiv R_i \pmod{n}$ where $0 \leq R_i \leq n - 1$. Then $2^{i+1} \equiv 2R_i \pmod{n}$ so then $2R_i \equiv R_{i+1} \pmod{n}$. We repeat this proves until we find R_j. Then we have

$$a^r = a^{2^j x_j + \cdots + 2^0 x_0} = (a^{2^j x_j}) \cdots (a^{2^0 x_0})$$

Then we have

$$a^r \equiv R_j^{x_j} \cdots R_0^{x_0} \pmod{n}$$

And note that $0 \leq R_i \leq n - 1$ for all $0 \leq i \leq j$. Then multiplying these numbers gives k. Note there are about $\log_2 r$ such multiplications.

Question (3.7)**.** Let $f(x) = 13x^{49} - 27x^{27} + x^{14} - 6$. Is it true that

$$f(98) \equiv f(-100) \pmod{99}$$

Since $98 \equiv -100 \pmod{99}$ by Theorem 3.8 it follows $f(98) \equiv f(-100) \pmod{99}$.

Theorem (3.8)**.** *Suppose* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *is a polynomial of degree* $n > 0$ *with integer coefficients. Let* a*,* b*, and* m *be integers with* $m > 0$*. If* $a \equiv b \pmod{m}$*, then* $f(a) \equiv f(b) \pmod{m}$*.*

Proof. Since $a \equiv b \pmod{m}$ then $a^i \equiv b^i \pmod{m}$ for all $0 \leq i \leq n$. Moreover, since $a_i \equiv a_i \pmod{m}$ and $a^i \equiv b^i \pmod{m}$ for all i we have $a_i a^i \equiv a_i b^i \pmod{m}$ for all $0 \leq i \leq n$. Then we have

$$\sum_{i=0}^{n} a_i a^i \equiv \sum_{i=0}^{n} a_i b^i \pmod{n}$$

Hence, $f(a) \equiv f(b) \pmod{n}$. □

Corollary (3.9)**.** *Let the natural number* n *be expressed in base 10 as*

$$n = a_k a_{k-1} ... a_1 a_0$$

Let $m = a_k + a_{k-1} + \cdots + a_1 + a_0$*. Then* $9 \mid n$ *if and only if* $9 \mid m$*.*

Proof. Since $10 \equiv 1 \pmod{9}$ we have $f(10) \equiv f(1) \pmod{9}$. Hence, $n \equiv m \pmod{9}$. Then $9 \mid n - m$. Then $n - m = 9k$. So then if $9 \mid n$ then $9 \mid m$ and if $9 \mid m$ then $9 \mid n$. □

Corollary (3.10)**.** *Let the natural number* n *be expressed in base 10 as*

$$n = a_k a_{k-1} ... a_1 a_0$$

Let $m = a_k + a_{k-1} + \cdots + a_1 + a_0$*. Then* $3 \mid n$ *if and only if* $3 \mid m$*.*

Proof. Since $10 \equiv 1 \pmod{3}$ we have $f(10) \equiv f(1) \pmod{3}$. Hence, $n \equiv m \pmod{3}$. Then $3 \mid n - m$. Then $n - m = 3k$. So then if $3 \mid n$ then $3 \mid m$ and if $3 \mid m$ then $3 \mid n$. □

Theorem (3.11). *Suppose $f(x) = a_n x^n + \cdots + a_0$ is a polynomial of degree $n > 0$ and suppose $a_n > 0$. Then there is an integer k such that if $x > k$, then $f(x) > 0$.*

Proof. Suppose we have the polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_n > 0$. By Lemma B, for all $0 \leq i \leq n-1$, there exists a natural number k_i such that

$$\frac{a_n}{n}x^n > -a_i x^i$$

for all $x > k_i$, since $a_n/n > 0$ and $n > i$. Then define the function $s_i \colon \mathbb{R} \to \mathbb{R}$ as

$$s_i(x) = \frac{a_n}{n}x^n + a_i x^i$$

and note that $s_i(x) > 0$ for all $x > k_i$. Take $k = \max\{k_0, k_1, \ldots, k_{n-1}\}$. Then for all $i = 0, 1, \ldots, n-1$ we have $s_i(x) > 0$ for all $x > k$. Notice the sum $\sum_{i=0}^{n-1} s_i(x) = f(x)$. Moreover, since $s_i(x) > 0$ for all i for all $x > k$ it follows $f(x) > 0$ for all $x > k$. □

Lemma (A). *If $x, y \in \mathbb{R}$ and $x > 0$ there exists a natural number n such that $nx > y$.*

I take this lemma for granted.

Lemma (B). *Let $a, b \in \mathbb{R}$ and $n, m \in \mathbb{N} \cup \{0\}$ such that $a > 0$ and $n > m$. Then there exists a natural number k such that $ax^n > bx^m$ for all x where $x \in \mathbb{R}$ and $x > k$.*

Proof. Since $a > 0$, by Lemma A, there exists a natural number k such that $ak > b$. Since $k \geq 1$ it follows $ax \geq ak$ for all $x > k$. Hence, $ax > b$ for all $x > k$. Since $ax > b$, $x \geq 1$, and $n - m \in \mathbb{N}$ it follows $ax^{n-m} > b$ for all $x > k$. Then we have $ax^{n-m}x^m > bx^m$ for all $x > k$. Hence, $ax^n > bx^m$ for all $x > k$. □

Theorem (3.12). *Suppose $f(x) = a_n x^n + \cdots + a_0$ is a polynomial of degree $n > 0$ and suppose $a_n > 0$. Then for any number M there is an integer k (which depends on M) such that if $x > k$, then $f(x) > M$.*

Proof. Consider the polynomial $g(x) = f(x) - M$ where $M \in \mathbb{R}$. Then we have $g(x) = a_n x^n + \cdots + (a_0 - M)$. Since $a_n > 0$ there exists an integer k such that $g(x) > 0$. Hence, $f(x) > M$ for all $x > k$. □

Theorem (3.13). *Suppose $f(x) = a_n x^n + \cdots + a_0$ is a polynomial of degree $n > 0$ with integer coefficients. Then $f(x)$ is a composite number for infinitely many integers x.*

Proof. First consider the case where $a_0 = 0$. Let j be a natural number that is composite. Then $f(mj) = \sum_{i=1}^{n} a_i (mj)^i$. It follows $j \mid f(mj)$ where for all natural numbers m. By Theorem 3.12 there is some natural number k such that $f(x) > 1$ for all $x > k$. Moreover, there exists some $m_0 \in \mathbb{N}$ such that $m_0 > k$. Then we have $f(mj) > 1$ for all $m \geq m_0$. Since $j \mid f(mj)$ we have $f(mj) = d_m j$ where $d_m \in \mathbb{Z}$ for all $m \geq m_0 > 1$. And since $f(mj) > 1$ for all m we have $f(mj) \neq 0$ for all m. Hence, $d_m \neq 0$. Then since j is composite it follows $f(mj)$ is composite for all $m > m_0$.

Now consider the case where $|a_0| > 1$. Then $a_0 \mid f(|a_0|)$. Without a loss of generality, let $a_n > 0$. Then there exists natural number k such that $f(x) > |a_0|$ for all $x > k$. Moreover, there exists $m_0 \in \mathbb{N}$ such that $m_0|a_0| > k$. Then $f(m|a_0|) > |a_0|$ for all $m \geq m_0$. Since $f(m|a_0|) > |a_0|$ and $|a_0| \mid f(m|a_0|)$ it follows $f(m|a_0|) = d|a_0|$ where $d, |a_0| > 1$. Hence, $f(m|a_0|)$ is composite. An analogous argument proves the case for $a_n < 0$.

Now consider the case where $|a_0| = 1$. Now let $f\colon \mathbb{R} \to \mathbb{R}$ be defined as

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

as defined in the theorem statement. Moreover, without a loss of generality, let $a_n > 0$. Then

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

Then define b_i for $i = 0, 1, \ldots, n$ such that

$$f(x+h) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$$

We desire an h such that $|b_0| > 1$. By Theorem 3.12 there exists a natural number k such that $f(x) > 1$ for all $x > k_1$. Note $f(0+h) = f(h) = b_0$. If $h > k_1$, then $f(h) = b_0 > 1$. Hence, we desire h such that $h > k_1$. Let $h = r|b_0| > k_1$ for some $r \in \mathbb{N}$. Now define the function $g\colon \mathbb{R} \to \mathbb{R}$ as

$$g(x) = f(x+h) = b_n x^n + \cdots b_0$$

Since $a_n > 0$, by Theorem 3.12 there exists $k_2 \in \mathbb{N}$ such that $g(x) > b_0$ for all $x > k_2$. Moreover, there exists $m_0 \in \mathbb{N}$ such that $m_0 b_0 > k_2$. Then $g(mb_0) > b_0$ for all $m \geq m_0$ and $b \mid g(mb_0)$ for all $m \geq m_0$. It follows $g(mb_0)$ is composite for all $m \geq m_0$. Then $g(mb_0 - rb_0)$ is composite for all $m \geq m_0 + r$. And $g(mb_0 - rb_0) = f(mb_0)$. Hence, $f(mb_0)$ is composite for all $m \geq m_0 + r$. Then $f(x)$ is composite for infinitely many x. A similar argument proves the case when $a_n < 0$. This concludes the proof for when $|a_0| = 1$. □

Theorem (3.14)**.** *Given any integer a and any natural number n, there exists a unique integer t in the set $\{0, 1, 2, ..., n-1\}$ such that $a \equiv t \pmod{n}$.*

Proof. There are three cases: $a < 0, a = 0, a > 0$. If $a > 0$ then by the division algorithm there exists integers q and r such that $a = nq + r$ where $0 \leq r \leq n-1$. Then $nq = a - r$ so $a \equiv r \pmod{n}$. Take $t = r$. Moreover, t is unique by the uniqueness of the division algorithm.

Now suppose $a = 0$. Then we have $0 \equiv t \pmod{n}$. Then $t = dn$ for some integer d. Since $t \in \{0, 1, 2, ..., n-1\}$ it follows $t = 0$. Since there is only one possible value, t is unique.

Now suppose $a < 0$. Then $-a > 0$. Then by the division algorithm, there exists integers q_0 and r_0 such that $-a = nq_0 + r_0$ where $0 \leq r_0 \leq n-1$. Then we have $a = n(-q_0) - r_0$ where $-n+1 \leq r_0 \leq 0$. If $-r_0 = 0$ then let $r = r_0$ and $q = q_0$. Then let $t = r$ and $t = 0$ and t is unique by the uniqueness of the division algorithm. If $-r_0 = -1, -2, ..., -n+1$ then let $q = -q_0 - 1$ and $r = -r_0 + n$. Then $0 \leq r \leq n-1$. Let $t = r$ and then $t \in \{1, 2, ..., n-1\}$ and t is unique by the uniqueness of the division algorithm. In all cases we have $a = qn + t$ where $0 \leq t \leq n-1$. And by definition of congruence we have $a \equiv t \pmod{n}$. □

Exercise (3.15)**.** Find three complete residue systems modulo 4: the canonical complete residue system, one containing negative numbers, and one containing no two consecutive numbers.

The canonical complete residue system is $\{0, 1, 2, 3\}$. A complete residue system containing negative numbers is $\{-1, 0, 1, 2\}$. A complete residue system containing no two consecutive numbers is $\{-1, 1, 4, 6\}$.

Theorem (3.16)**.** *Let n be a natural number. Every complete residue system modulo n contains n elements.*

Proof. Suppose we have a complete residue system modulo n, denoted by the set $A = \{a_1, ..., a_m\}$. We also have the canonical complete residue system modulo n given as $B = \{0, 1, 2, ..., n-1\}$.

For the sake of contradiction and without a loss of generality suppose $m < n$. Then there exists integers i, j, k such that $0 \leq i, j \leq n-1$ and $1 \leq k \leq m$ such that $i \neq j$. Moreover, $i \equiv a_k \pmod{n}$ and $a_k \equiv j \pmod{n}$. By transitivity of congruence we have $i \equiv j \pmod{n}$ which is a contradiction. An analogous contradiction occurs when we consider $m > n$. Hence, $m = n$. □

Theorem (3.17)**.** *Let n be a natural number. Any set, $\{a_1, a_2, ..., a_n\}$, of n integers for which no two are congruent modulo n is a complete residue system modulo n.*

Proof. Let $A = \{a_1, a_2, ..., a_n\}$. Let k be an integer. First we show there is at most one $i \in \{1, ..., n\}$ such that $k \equiv a_i \pmod{n}$. Otherwise, if there exists i, j such that $i \neq j$ and $a_i \equiv k \pmod{n}$ and $k \equiv a_j \pmod{n}$, then we have $a_i \equiv a_j \pmod{n}$ which is a contradiction to our set. Now we show there is at least one $i \in \{1, 2, ..., n\}$ such that $k \equiv a_i \pmod{n}$. Let $B = \{0, 1, ..., n-1\}$. Note that for all $i, j \in \{1, 2, ..., n\}$ we have $a_i \not\equiv a_j \pmod{n}$ implies if $a_i = nq_i + r_i$ and $a_j = nq_j + r_j$ where $0 \leq r_i, r_j \leq n-1$ then $r_i \neq r_j$. It follows the mapping $f \colon A \to B$ where $f(a_i) = r$ where $r = r_i$ from the division algorithm is an injection. Then $|A| \leq |B|$. Moreover, we know A has n distinct integers so $|A| = |B| = n$. It follows f is a bijection. By the existence part of the division algorithm there exists $r \in B$ such that $k \equiv r \pmod{n}$ and since f is a bijection there exists $i \in \{1, 2, ..., n\}$ such that $a_i \equiv k \pmod{n}$. Hence, A is a complete residue system modulo n. □

Theorem (3.11). *Suppose $f(x) = a_n x^n + \cdots + a_0$ is a polynomial of degree $n > 0$ and suppose $a_n > 0$. Then there is an integer k such that if $x > k$, then $f(x) > 0$.*

Proof. Suppose we have the polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_n > 0$. By Lemma B, for all $0 \leq i \leq n-1$, there exists a natural number k_i such that

$$\frac{a_n}{n}x^n > -a_i x^i$$

for all $x > k_i$, since $a_n/n > 0$ and $n > i$. Then define the function $s_i \colon \mathbb{R} \to \mathbb{R}$ as

$$s_i(x) = \frac{a_n}{n}x^n + a_i x^i$$

and note that $s_i(x) > 0$ for all $x > k_i$. Take $k = \max\{k_0, k_1, \ldots, k_{n-1}\}$. Then for all $i = 0, 1, \ldots, n-1$ we have $s_i(x) > 0$ for all $x > k$. Notice the sum $\sum_{i=0}^{n-1} s_i(x) = f(x)$. Moreover, since $s_i(x) > 0$ for all i for all $x > k$ it follows $f(x) > 0$ for all $x > k$. □

Lemma (A). *If $x, y \in \mathbb{R}$ and $x > 0$ there exists a natural number n such that $nx > y$.*

I take this lemma for granted.

Lemma (B). *Let $a, b \in \mathbb{R}$ and $n, m \in \mathbb{N} \cup \{0\}$ such that $a > 0$ and $n > m$. Then there exists a natural number k such that $ax^n > bx^m$ for all x where $x \in \mathbb{R}$ and $x > k$.*

Proof. Since $a > 0$, by Lemma A, there exists a natural number k such that $ak > b$. Since $k \geq 1$ it follows $ax \geq ak$ for all $x > k$. Hence, $ax > b$ for all $x > k$. Since $ax > b$, $x \geq 1$, and $n - m \in \mathbb{N}$ it follows $ax^{n-m} > b$ for all $x > k$. Then we have $ax^{n-m}x^m > bx^m$ for all $x > k$. Hence, $ax^n > bx^m$ for all $x > k$. □

Theorem (3.13). *Suppose $f(x) = a_n x^n + \cdots + a_0$ is a polynomial of degree $n > 0$ with integer coefficients. Then $f(x)$ is a composite number for infinitely many integers x.*

Proof. First consider the case where $a_0 = 0$. Let j be a natural number that is composite. Then $f(mj) = \sum_{i=1}^{n} a_i (mj)^i$. It follows $j \mid f(mj)$ where for all natural numbers m. By Theorem 3.12 there is some natural number k such that $f(x) > 1$ for all $x > k$. Moreover, there exists some $m_0 \in \mathbb{N}$ such that $m_0 > k$. Then we have $f(mj) > 1$ for all $m \geq m_0$. Since $j \mid f(mj)$ we have $f(mj) = d_m j$ where $d_m \in \mathbb{Z}$ for all $m \geq m_0 > 1$. And since $f(mj) > 1$ for all m we have $f(mj) \neq 0$ for all m. Hence, $d_m \neq 0$. Then since j is composite it follows $f(mj)$ is composite for all $m > m_0$.

Now consider the case where $|a_0| > 1$. Then $a_0 \mid f(|a_0|)$. Without a loss of generality, let $a_n > 0$. Then there exists natural number k such that $f(x) > |a_0|$ for all $x > k$. Moreover, there exists $m_0 \in \mathbb{N}$ such that $m_0|a_0| > k$. Then $f(m|a_0|) > |a_0|$ for all $m \geq m_0$. Since $f(m|a_0|) > |a_0|$ and $|a_0| \mid f(m|a_0|)$ it follows $f(m|a_0|) = d|a_0|$ where $d, |a_0| > 1$. Hence, $f(m|a_0|)$ is composite. An analogous argument proves the case for $a_n < 0$.

Now consider the case where $|a_0| = 1$. Now let $f \colon \mathbb{R} \to \mathbb{R}$ be defined as

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

as defined in the theorem statement. Moreover, without a loss of generality, let $a_n > 0$. Then

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

Then define b_i for $i = 0, 1, \ldots, n$ such that

$$f(x+h) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$$

We desire an h such that $|b_0| > 1$. By Theorem 3.12 there exists a natural number k such that $f(x) > 1$ for all $x > k_1$. Note $f(0+h) = f(h) = b_0$. If $h > k_1$, then $f(h) = b_0 > 1$. Hence, we desire h such that $h > k_1$. Let $h = r|b_0| > k_1$ for some $r \in \mathbb{N}$. Now define the function $g\colon \mathbb{R} \to \mathbb{R}$ as

$$g(x) = f(x+h) = b_n x^n + \cdots b_0$$

Since $a_n > 0$, by Theorem 3.12 there exists $k_2 \in \mathbb{N}$ such that $g(x) > b_0$ for all $x > k_2$. Moreover, there exists $m_0 \in \mathbb{N}$ such that $m_0 b_0 > k_2$. Then $g(mb_0) > b_0$ for all $m \geq m_0$ and $b \mid g(mb_0)$ for all $m \geq m_0$. It follows $g(mb_0)$ is composite for all $m \geq m_0$. Then $g(mb_0 - rb_0)$ is composite for all $m \geq m_0 + r$. And $g(mb_0 - rb_0) = f(mb_0)$. Hence, $f(mb_0)$ is composite for all $m \geq m_0 + r$. Then $f(x)$ is composite for infinitely many x. A similar argument proves the case when $a_n < 0$. This concludes the proof for when $|a_0| = 1$. □

Theorem (3.16)**.** *Let n be a natural number. Every complete residue system modulo n contains n elements.*

Proof. Suppose we have a complete residue system modulo n, denoted by the set $A = \{a_1, ..., a_m\}$. We also have the canonical complete residue system modulo n given as $B = \{0, 1, 2, ..., n-1\}$.

For the sake of contradiction and without a loss of generality suppose $m < n$. Then there exists integers i, j, k such that $0 \leq i, j \leq n-1$ and $1 \leq k \leq m$ such that $i \neq j$. Moreover, $i \equiv a_k \pmod{n}$ and $a_k \equiv j \pmod{n}$. By transitivity of congruence we have $i \equiv j \pmod{n}$ which is a contradiction. An analogous contradiction occurs when we consider $m > n$. Hence, $m = n$. □

Theorem (3.17)**.** *Let n be a natural number. Any set, $\{a_1, a_2, ..., a_n\}$, of n integers for which no two are congruent modulo n is a complete residue system modulo n.*

Proof. Let $A = \{a_1, a_2, ..., a_n\}$. Let k be an integer. First we show there is at most one $i \in \{1, ..., n\}$ such that $k \equiv a_i \pmod{n}$. Otherwise, if there exists i, j such that $i \neq j$ and $a_i \equiv k \pmod{n}$ and $k \equiv a_j \pmod{n}$, then we have $a_i \equiv a_j \pmod{n}$ which is a contradiction to our set. Now we show there is at least one $i \in \{1, 2, ..., n\}$ such that $k \equiv a_i \pmod{n}$. Let $B = \{0, 1, ..., n-1\}$. Note that for all $i, j \in \{1, 2, ..., n\}$ we have $a_i \not\equiv a_j \pmod{n}$ implies if $a_i = nq_i + r_i$ and $a_j = nq_j + r_j$ where $0 \leq r_i, r_j \leq n-1$ then $r_i \neq r_j$. It follows the mapping $f\colon A \to B$ where $f(a_i) = r$ where $r = r_i$ from the division algorithm is an injection. Then $|A| \leq |B|$. Moreover, we know A has n distinct integers so $|A| = |B| = n$. It follows f is a bijection. By the existence part of the division algorithm there exists $r \in B$ such that $k \equiv r \pmod{n}$ and since f is a bijection there exists $i \in \{1, 2, ..., n\}$ such that $a_i \equiv k \pmod{n}$. Hence, A is a complete residue system modulo n. □

Exercise (3.18)**.** Find all solutions in the appropriate canonical complete residue system modulo n that satisfy the following linear congruences:

(1) $26x \equiv 14 \pmod{3}$
(2) $2x \equiv 3 \pmod{5}$
(3) $4x \equiv 7 \pmod{8}$
(4) $24x \equiv 123 \pmod{213}$

The solutions for (1) are $x = 1$. The solutions for (2) are $x = 4$. There are no solutions for (3). There exist solutions for (4). Solutions are found in Exercise 3.22.

Theorem (3.19)**.** *Let a, b, and n be integers with $n > 0$. Show that $ax \equiv b \pmod{n}$ has a solution if and only if there exist integers x and y such that $ax + by = b$.*

Proof. We prove the forward direction first. By definition of congruence we have $n \mid ax - b$. Then by definition of divides we have $ax - b = kn$ where $k \in \mathbb{Z}$. Note that $(a, n) \mid ax$ and $(a, n) \mid kn$. Then by Theorem 1.32 we have $(a, n) \mid b$. Then by Theorem 1.48 we have there exists integers x and y such that $ax + ny = b$.

Now we prove the reverse direction. Suppose there exist integers x and y such that $ax + ny = b$. By algebra we have $ax - b = -ny$. Note $-y \in \mathbb{Z}$ so then by definition of congruence and divides we have $ax \equiv b \pmod{n}$ □

Theorem (3.20)**.** *Let a, b, and n be integers with $n > 0$. The equation $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n) \mid b$.*

Proof. We prove the forward direction. If there is a solution to $ax \equiv b \pmod{n}$ has a solution then by Theorem 3.19 there exist integers x and y such that $ax + ny = b$. Then by Theorem 1.48 we have $(a, n) \mid b$.

Now we prove the reverse direction. If we have $(a, n) \mid b$ then by Theorem 1.48 there exist integers x and y such that $ax + ny = b$. Then we have $ax - b = -ny$ so then by definition of congruence we have $ax \equiv b \pmod{n}$. □

Question (3.21)**.** What does the preceding theorem tell us about congruence (4) in Exercise 3.18 above?

Since $(24, 213) = 3$ and $3 \mid 123$ it follows there exist solutions to $24x \equiv 123 \pmod{213}$.

Exercise (3.22)**.** Use the Euclidean Algorithm to find a member x of the canonical complete residue system modulo 213 that satisfies $24x \equiv 123 \pmod{213}$. Find all members x of the canonical complete residue system modulo 213 that satisfy $24x \equiv 123 \pmod{213}$.

We need to find integer solutions to $24x \equiv 123 \pmod{213}$. Then by definition of congruence we need to find integers x and y such that $24x - 213y = 123$. This is a diophantine equation. Equivalently, we have $8x - 71y = 41$. Note that if $x = 9$ and $y = 1$ then we have $72 - 71 = 1$. It follows one solution is $x = 9 \times 41 = 369$ and $y = 1 \times 41$. We know that the general form of all solutions to the diophantine equation is

$$x = x_0 + \frac{kb}{(a, b)} \text{ and } y = y_0 + \frac{ka}{(a, b)}$$

for some $k \in \mathbb{Z}$. Then we have

$$x = 369 + 71k \text{ and } y = 41 - 8k$$

Plugging in appropriate values of k we get solutions $x = 14, 85, 156$ which are in the canonical complete residue system modulo 213.

Theorem (3.13)**.** *Suppose $f(x) = a_n x^n + \cdots + a_0$ is a polynomial of degree $n > 0$ with integer coefficients. Then $f(x)$ is a composite number for infinitely many integers x.*

Proof. First consider the case where $a_0 = 0$. Let j be a natural number that is composite. Then $f(mj) = \sum_{i=1}^{n} a_i (mj)^i$. It follows $j \mid f(mj)$ where for all natural numbers m. By Theorem 3.12 there is some natural number k such that $f(x) > 1$ for all $x > k$. Moreover, there exists some $m_0 \in \mathbb{N}$ such that $m_0 > k$. Then we have $f(mj) > 1$ for all $m \geq m_0$. Since $j \mid f(mj)$ we have $f(mj) = d_m j$ where $d_m \in \mathbb{Z}$ for all $m \geq m_0 > 1$. And since $f(mj) > 1$ for all m we have $f(mj) \neq 0$ for all m. Hence, $d_m \neq 0$. Then since j is composite it follows $f(mj)$ is composite for all $m > m_0$.

Now consider the case where $|a_0| > 1$. Then $a_0 \mid f(|a_0|)$. Without a loss of generality, let $a_n > 0$. Then there exists natural number k such that $f(x) > |a_0|$ for all $x > k$. Moreover, there exists $m_0 \in \mathbb{N}$ such that $m_0 |a_0| > k$. Then $f(m|a_0|) > |a_0|$ for all $m \geq m_0$. Since $f(m|a_0|) > |a_0|$ and $|a_0| \mid f(m|a_0|)$ it follows $f(m|a_0|) = d|a_0|$ where $d, |a_0| > 1$. Hence, $f(m|a_0|)$ is composite. An analogous argument proves the case for $a_n < 0$.

Now consider the case where $|a_0| = 1$. Now let $f \colon \mathbb{R} \to \mathbb{R}$ be defined as

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

as defined in the theorem statement. Moreover, without a loss of generality, let $a_n > 0$. Then

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

Then define b_i for $i = 0, 1, \ldots, n$ such that

$$f(x + h) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$$

We desire an h such that $|b_0| > 1$. By Theorem 3.12 there exists a natural number k such that $f(x) > 1$ for all $x > k_1$. Note $f(0 + h) = f(h) = b_0$. If $h > k_1$, then $f(h) = b_0 > 1$. Hence, we desire h such that $h > k_1$. Let $h = r|b_0| > k_1$ for some $r \in \mathbb{N}$. Now define the function $g \colon \mathbb{R} \to \mathbb{R}$ as

$$g(x) = f(x + h) = b_n x^n + \cdots b_0$$

Since $a_n > 0$, by Theorem 3.12 there exists $k_2 \in \mathbb{N}$ such that $g(x) > b_0$ for all $x > k_2$. Moreover, there exists $m_0 \in \mathbb{N}$ such that $m_0 b_0 > k_2$. Then $g(mb_0) > b_0$ for all $m \geq m_0$ and $b \mid g(mb_0)$ for all $m \geq m_0$. It follows $g(mb_0)$ is composite for all $m \geq m_0$. Then $g(mb_0 - rb_0)$ is composite for all $m \geq m_0 + r$. And $g(mb_0 - rb_0) = f(mb_0)$. Hence, $f(mb_0)$ is composite for all $m \geq m_0 + r$. Then $f(x)$ is composite for infinitely many x. A similar argument proves the case when $a_n < 0$. This concludes the proof for when $|a_0| = 1$. □

Exercise (3.22)**.** Use the Euclidean Algorithm to find a member x of the canonical complete residue system modulo 213 that satisfies $24x \equiv 123 \pmod{213}$. Find all members x of the canonical complete residue system modulo 213 that satisfy $24x \equiv 123 \pmod{213}$.

We find solutions to the congruence $8x \equiv 41 \pmod{71}$. This means we have $71 \mid 8x - 41$. Then by definition of divides we want to find integer solutions x and y to the diophantine equation

$$8x - 71y = 41$$

Note that $(8)(9) \equiv 1 \pmod{71}$ so then $(8)(9)(41) \equiv 41 \pmod{71}$. Then the general form of the solutions to the diophantine equations is

$$x = 369 - 71k \text{ and } y = 41 - 8k$$

for all $k \in \mathbb{Z}$. Then the x-part of the solutions within the interval $[0, 213]$ are $x = 156, 85, 14$.

Question (3.23)**.** Let a, b, and n be integers with $n > 0$. How many solutions are there to the linear congruence $ax \equiv b \pmod{n}$ in the canonical complete residue system modulo n? Can you describe a technique to find them?

Check if $(a, b) \mid b$. If not then there are no solutions. If it holds, then find a solution. Then all other solutions are of the form

$$x = x_0 + \frac{kb}{(a, b)}$$

for some $k \in \mathbb{Z}$. Then take the solutions that are within the interval $[0, n - 1]$.

Theorem (3.24)**.** *Let a, b, and n be integers with $n > 0$. Then*

(1) *The congruence $ax \equiv b \pmod{n}$ is solvable in integers if and only if $(a, n) \mid b$.*
(2) *If x_0 is a solution to the congruence $ax \equiv b \pmod{n}$, then all solutions are given by*

$$x_0 + \left(\frac{n}{(a, n)} \cdot m\right) \pmod{n}$$

for $m = 0, 1, 2, \ldots, (a, n) - 1$
(3) *If $ax \equiv b \pmod{n}$ has a solution, then there are exactly (a, n) solutions in the canonical complete residue system modulo n.*

Proof. Part (1) holds from Theorem 3.20. First we show solutions of the form in part (2) are in fact solutions. Suppose there exist integers x and y such that $ax - ny = b$. Then by definition of divides we have $n \mid ax - b$. It follows by definition of congruence we have $ax \equiv b \pmod{n}$. Note the general form for solutions to the Diophantine equation $ax - ny = b$ is

$$x = x_0 + \frac{mn}{(a, n)} \text{ and } y = y_0 + \frac{ma}{(a, n)}$$

for some $m \in \mathbb{Z}$. So we know the general form of solutions to the congruence $ax \equiv b \pmod{n}$ is $x = x_0 + mn/(a, n)$. By the Division Algorithm there exist integers q and r such that $x_0 + mn/(a, n) = nq + r$ where $0 \leq r \leq n - 1$. Since $x_0 + mn/(a, n)$ is a solution we have

$$a(x_0 + \frac{nm}{(a, n)}) \equiv b \pmod{n}$$

So by substitution we have

$$nq + r \equiv b \pmod{n}$$

Then by definition of divides we have $n \mid nq + r - b$. Then we have $nq + r - b = nd$ for some $d \in \mathbb{Z}$. Then we have $r - b = n(d - q)$. Then by definition of congruence we have $r \equiv b \pmod{n}$. Hence

$$x_0 + \left(\frac{n}{(a, n)} \cdot m\right) \pmod{n}$$

is a solution to the congruence $ax \equiv b \pmod{n}$.

Now we show all solutions must be of the form given in the Theorem. We know that by Theorem 1.53 all solutions of the Diophantine equation $ax - ny = b$ must be of the form

$$x = x_0 + \frac{mn}{(a,n)} \text{ and } y = y_0 + \frac{ma}{(a,n)}$$

Hence, all solutions to the congruence must be of the form

$$x_0 + \left(\frac{n}{(a,n)} \cdot m\right)$$

By the division algorithm we have $m = (a,n)q + r$ for some integers q and r where $0 \leq r \leq (a,n) - 1$. Then by substitution we have

$$x_0 + \frac{nm}{(a,n)} = x_0 + \frac{n((a,n)q + r)}{(a,n)} = x_0 + nq + \frac{nr}{(a,n)}$$

Hence, we have

$$x_0 + nq + \frac{nr}{(a,n)} \equiv x_0 + \frac{nr}{(a,n)} \pmod{n}$$

It follows every solution is congruent to one of the solutions given in the Theorem statement of part 2.

Now we prove part (3). In the proof of the previous part, we showed that if there is a solution, then there all solutions are congruent to $x_0 + nm/(a,n) \pmod{n}$ for some $m = 0, 1, \ldots, (a,n) - 1$. Moreover, the solutions given in part 2 are in fact solutions to the linear congruence. Now we show no two solutions are the same. That is if $i \neq j$ and $i, j = 0, 1, \ldots, (a,n) - 1$ then $x_0 + ni/(a,n) \not\equiv x_0 + nj/(a,n) \pmod{n}$. For the sake of contradiction, suppose it were true. Then by definition of congruence and divides we get $i/(a,n) - j/(a,n) = k$ so then $i - j = k(a,n)$. But $i, j = 0, 1, 2, \ldots, (a,n) - 1$. This is a contradiction since $|i - j| \leq (a,n) - 1$. This concludes the proof. □

Exercise (3.25)**.** A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The coins were redistributed, but this time an equal division left 10 coins. Again they fought about who should get the remaining coins and another pirate was killed. Now, fortunately, the coins could be divided evenly among the surviving 15 pirates. What was the fewest number of coins that could have been in the sack?

We have the following congruences

$$\begin{aligned} x &\equiv 3 \pmod{17} \\ x &\equiv 10 \pmod{16} \\ x &\equiv 0 \pmod{15} \end{aligned}$$

By the first congruence we know $x = 17k + 3$ for some $k \in \mathbb{Z}$. Then substituting this into the second congruence, we get $k \equiv 7 \pmod{16}$ so then $k = 16j + 7$ for some integer j. Then we have $x = 272j + 122$. Then substituting this into the third congruence, we get $j \equiv -1 \pmod{15}$. Then we have $x = 4080i - 150$ for some integer i. The value of x of this form that is positive is 3930.

Exercise (3.26)**.** When eggs in a basket are removed two, three, four, five or six at a time, there remain, respectively, one, two, three, four, or five eggs. When they are taken out seven at a time, none are left over. Find the smallest number of eggs that could have been contained in the basket.

We have the following congruences

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 5 \pmod 6 \end{aligned}$$

From $x \equiv 5 \pmod 6$ we get $x = 6a + 5$. Then with $x \equiv 4 \pmod 5$ we get $a \equiv 4 \pmod 5$. Then we have $x = 30b + 29$. Then with $x \equiv 3 \pmod 4$ we get $x = 60c + 59$. Now this form already satisfies the other two remaining congruences. The smallest positive value is $x = 59$.

Theorem (3.27)**.** *Let a, b, m, and n be integers with $m > 0$ and $n > 0$. Then the system*

$$\begin{aligned} x &\equiv a \pmod n \\ x &\equiv b \pmod m \end{aligned}$$

has a solution if and only if $(n, m) \mid a - b$.

Proof. We prove the forward direction first. Suppose there exists a solution x such that both congruences hold. Then there exist integers i and j such that $-x + a = in$ and $x - b = jm$. Then adding these together we get $a - b = in + jm$. This is a Diophantine equation. Since i and j are solutions to the equation, by Theorem 1.48 we must have $(n, m) \mid a - b$.

Now we prove the reverse direction. We prove the contrapositive. Suppose there does not exist x that satisfies the system of linear congruences. Then there does not exist x, k_1, k_2 such that $x - a = k_1 n$ and $x - b = k_2 m$. Adding these, we get $a - b = k_2 m - k_1 n$. Then there does not exist integer solutions to this Diophantine equation. Then by Theorem 1.48 it follows $(n, m) \nmid (a - b)$. □

Theorem (3.28)**.** *Let a, b, m, and n be integers with $m > 0$, $n > 0$, and $(m, n) = 1$. Then the system*

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

has a unique solution modulo mn.

Proof. If $(n, m) = 1$ then $(n, m) \mid k$ for all integers k by definition of divides. Hence, for any a, b we have $(n, m) \mid a - b$. Then by Theorem 3.27 there exists a solution to the system. Suppose there exists two solutions x and y to the system. Then we have $x \equiv a \pmod{n}$ and $y \equiv a \pmod{n}$. Then we have $x \equiv y \pmod{n}$. Then by definition of congruence we have $n \mid x - y$. Similarly, since $x \equiv b \pmod{m}$ and $y \equiv b \pmod{m}$ we have $m \mid x - y$. Since $n \mid x-y$, $m \mid x-y$, and $(n, m) = 1$, by Theorem 1.42 we have $nm \mid x-y$. Then by definition of congruence $x \equiv y \pmod{nm}$. Hence, x is a unique solution modulo mn. □

Theorem (3.29)**.** *Suppose $n_1, n_2, \ldots, n_L$ are positive integers that are pairwise relatively prime, that is, $(n_i, n_j) = 1$ for $i \neq j$, $i \leq i, j \leq L$. Then the system of L congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_L \pmod{n_L} \end{aligned}$$

has a unique solution modulo the product $n_1 n_2 \ldots n_L$.

Proof. We prove by induction. Let $P(m)$ be the statement of the theorem for when $L = m$. For the base case, consider when $m = 2$. Then $P(2)$ holds by Theorem 3.28.

For the inductive step, assume $P(L-1)$ is true. Consider the first system of L congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_L \pmod{n_L} \end{aligned}$$

Then for the first $L - 1$ congruences, there exists a unique solution x_0 modulo $n_1 \ldots n_{L-1}$. Then consider the second system of two congruences

$$\begin{aligned} x &\equiv x_0 \pmod{n_1 \cdots n_{L-1}} \\ x &\equiv a_L \pmod{n_L} \end{aligned}$$

Note $(n_L, n_1 \cdots n_{L-1}) = 1$. Otherwise if $(n_L, n_1 \ldots n_{L-1}) = d > 1$, then $d \mid n_L$ and $d \mid n_i$ for some $i = 1, 2, \ldots, L - 1$. Then $(n_L, n_i) \geq d$ which is a contradiction them being relatively prime. Since $(n_L, n_1 \cdots n_{L-1}) = 1$ by Theorem 3.28 there is a unique solution to this second system of two congruences modulo the product $n_1 \cdots n_L$. Let us denote this solution as z. So we have $z \equiv a_L \pmod{n_L}$. Moreover, $z \equiv x_0 \pmod{n_1 \cdots n_{L-1}}$. Then $n_1 \cdots n_{L-1} \mid z - x_0$ so then $n_i \mid z - x_0$ and then $z \equiv x_0 \pmod{n_i}$ for all $i = 1, 2, \ldots, L - 1$. It follows z is a solution to the first system of L congruences.

Now we show z is a unique solution modulo $n_1 \cdots n_L$. Suppose there exist two solutions z_1 and z_2 to the system of L congruences. Then z_1 and z_2 are solutions to the system of the first $L-1$ congruences; and z_1 and z_2 are solutions to the last congruence. Then we have

$$\begin{aligned} z_1 &\equiv x_0 \pmod{n_1 \cdots n_{L-1}} \\ z_1 &\equiv a_L \pmod{n_L} \\ z_2 &\equiv x_0 \pmod{n_1 \cdots n_{L-1}} \\ z_2 &\equiv a_L \pmod{n_L} \end{aligned}$$

Since z_1 and z_2 are solutions to the second system of two congruences and by Theorem 3.28 we know the solution to this system is unique modulo $n_1 \cdots n_L$, it follows $z_1 \equiv z_2 \pmod{n_1 \cdots n_L}$. □

Exercise (4.1)**.** For $i = 0, 1, 2, 3, 4, 5$, and 6, find the number in the canonical complete residue system to which 2^i is congruence modulo 7. In other words compute $2^0 \pmod 7$, $2^1 \pmod 7$, $2^2 \pmod 7$, …, $2^6 \pmod 7$.

$$\begin{aligned} 2^0 &\equiv 1 \pmod 7 \\ 2^1 &\equiv 2 \pmod 7 \\ 2^2 &\equiv 4 \pmod 7 \\ 2^3 &\equiv 1 \pmod 7 \\ 2^4 &\equiv 2 \pmod 7 \\ 2^5 &\equiv 4 \pmod 7 \\ 2^6 &\equiv 1 \pmod 7 \end{aligned}$$

Theorem (4.2)**.** *Let a and n be natural numbers with $(a, n) = 1$. Then $(a^j, n) = 1$ for any natural number j.*

Proof. We prove by induction. Let $P(m)$ be the statement of the theorem for when $j = m$. Consider when $m = 1$. Then $P(1)$ is trivially true. For the inductive step, suppose $P(m-1)$ is true. Consider a^m. Then $a^m = a(a^{m-1})$. Since $(a, n) = 1$, by the inductive hypothesis we have $(a^{m-1}, n) = 1$. Since $(a, n) = 1$ and $(a^{m-1}, n) = 1$, by Theorem 1.43 we have $(a(a^{m-1}), n) = 1$. Hence, $P(m)$ holds. This concludes the induction. □

Theorem (4.3)**.** *Let a, b, and n be integers with $n > 0$ and $(a, n) = 1$. If $a \equiv b \pmod n$, then $(b, n) = 1$.*

Proof. Since $a \equiv b \pmod n$ by definition of congruence we have $n \mid a - b$ and by definition of divides we have $a - b = kn$ for some integer k. Then $a = kn + b$. Note that $n > 0$ so then we can apply Theorem 1.33. Then we have $(a, n) = (n, b)$. Since $(a, n) = 1$ we then have $(b, n) = 1$. □

Theorem (4.4)**.** *Let a and n be natural numbers. Then there exist natural numbers i and j, with $i \neq j$, such that $a^i \equiv a^j \pmod n$.*

Proof. Consider the canonical complete residue system modulo n. We then have the set $A = \{0, 1, 2, \ldots, n-1\}$. Since there are infinitely many natural numbers and A is only finite, then by the pigeonhole principle, there exist natural numbers i and j such that $i \neq j$ and $a^i \equiv a^j \pmod{n}$. □

Theorem (4.5)**.** *Let a, b, c, and n be integers with $n > 0$. If $ac \equiv bc \pmod{n}$ and $c \equiv n \pmod{1}$, then $a \equiv b \pmod{n}$.*

Proof. Since $ac \equiv bc \pmod{n}$ by definition of congruence we have $n \mid ac - bc$ so then $n \mid c(a-b)$. If $n \mid c(a-b)$ and $(c, n) = 1$, then by Theorem 1.41 we have $n \mid (a-b)$. Then by definition of congruence we have $a \equiv b \pmod{n}$. □

Theorem (4.6)**.** *Let a and n be natural numbers with $(a, n) = 1$. Then there exists a natural number k such that $a^k \equiv 1 \pmod{n}$.*

Proof. By Theorem 4.4 there exists $i \neq j$ such that $a^i \equiv a^j \pmod{n}$. Without a loss of generality let $i > j$. Then by definition of congruence we have $n \mid a^i - a^j$ so then $n \mid a^j(a^{i-j} - 1)$. Since $(a, n) = 1$ it follows by Theorem 4.2 that $(a^j, n) = 1$. Then by Theorem 1.41 we have $n \mid a^{i-j} - 1$. Then by definition of congruence we have $a^{i-j} \equiv 1 \pmod{n}$. Moreover, $i - j > 0$ and $i, j \in \mathbb{Z}$ so $i - j \in \mathbb{N}$. □

Question (4.7)**.** Choose some relatively prime natural numbers a and n and compute the order of a modulo n. Frame a conjecture concerning how large the order of a modulo n can be, depending on n.

Let $a = 2$ and $n = 5$.

$$2^1 \equiv 2 \pmod 5$$
$$2^2 \equiv 4 \pmod 5$$
$$2^3 \equiv 3 \pmod 5$$
$$2^4 \equiv 1 \pmod 5$$

The order of a modulo n is 4.

Theorem (4.8)**.** *Let a and n be natural numbers with $(a, n) = 1$ and let $k = ord_n(a)$. Then the numbers $a^1, a^2, \ldots, a^k$ are pairwise incongruent modulo n.*

Proof. For the sake of contradiction, suppose there exists two natural numbers i and j such that $1 \leq i, j \leq k$ with $i \neq j$ and $a^i \equiv a^j \pmod n$. Without a loss of generality, let $i > j$. By definition of congruence $n \mid a^i - a^j$ or equivalently $n \mid a^j(a^{i-j} - 1)$. Note that $(a, n) = 1$ so by Theorem 4.2 $(a^j, n) = 1$. Then by Theorem 1.41 $n \mid a^{i-j} - 1$ and by definition of congruence $a^{i-j} \equiv 1 \pmod n$. Since $i > j$ and $1 \leq i, j \leq k$ it follows $1 \leq i - j < k$. This contradicts the definition of k which is $k = \text{ord}_n(a)$. Hence, $a^1, a^2, \ldots, a^k$ are pairwise incongruent modulo n. □

Theorem (4.9)**.** *Let a and n be natural numbers with $(a, n) = 1$ and let $k = ord_n(a)$. For any natural number m, a^m is congruent modulo n to one of the numbers $a^1, a^2, \ldots, a^k$.*

Proof. By the division algorithm there exist integers q and r such that $m = kq + r$ where $0 \leq r \leq k - 1$. Then $a^m = a^{kq+r} \equiv a^{kq}a^r \equiv (a^k)^q a^r \equiv a^r \pmod n$. If $1 \leq r \leq k - 1$ let $i = r$. Otherwise if $r = 0$ let $i = k$. Then $a^m \equiv a^i \pmod n$ for some $i \in \{1, 2, \ldots, k\}$. □

Theorem (4.10)**.** *Let a and n be natural numbers with $(a, n) = 1$, let $k = ord_n(a)$, and let m be a natural number. Then $a^m \equiv 1 \pmod n$ if and only if $k \mid m$.*

Proof. We prove the forward direction first. By the division algorithm there exist integers q and r such that $m = kq + r$ where $0 \leq r \leq k - 1$. Suppose $a^m \equiv 1 \pmod n$. Then $a^m \equiv a^r \equiv 1 \pmod n$. Note $0 \leq r \leq k-1$ and k is the order of a modulo n. If $1 \leq r \leq k-1$ this would contradict the definition of k. Hence, $r = 0$. Then $m = kq$. By definition of divides we have $k \mid m$.

Now we prove the reverse direction. If $k \mid m$ then there exists a natural number d such that $m = kd$. Then $a^m = (a^k)^d \equiv 1^d \equiv 1 \pmod n$. □

Theorem (4.11)**.** *Let a and n be natural numbers with $(a, n) = 1$. Then $ord_n(a) < n$.*

Proof. If $n = 1$. Then 1 is the smallest natural number such that $a^1 \equiv 1 \pmod 1$. So $\text{ord}_n(a) = 1$. But $n = 1$ and $1 < 1$ is false. So the theorem is not true for $n = 1$. Thus assume $n \geq 2$.

Suppose $\text{ord}_n(a) = n$. Then the numbers $a^1, a^2, \ldots, a^n$ are pairwise incongruent modulo n. Then By Theorem 3.17 it follows the set $\{a^1, a^2, \ldots, a^n\}$ for a complete residue system

modulo n. Then for some $i \in \{1, 2, \ldots, n\}$ we have $0 \equiv a^i \pmod{n}$. Then $n \mid a^i$. However, $(a, n) = 1$ so $(a^i, n) = 1$ which contradicts $n \mid a^i$ since $n \geq 2$.

Now suppose $\text{ord}_n(a) > n$. By Theorem 4.8, the numbers $a^1, a^2, \ldots, a^n, a^{n+1}, \ldots, a^{\text{ord}_n(a)}$ are pairwise incongruent modulo n. Then $\{a^1, a^2, \ldots, a^n\}$ for a complete residue system modulo n by Theorem 3.17. Since $\text{ord}_n(a) > n$ it follows $a^{\text{ord}_n(a)} \equiv a^i \pmod{n}$ for some $i \in \{1, 2, \ldots, n\}$. This is a contradiction.

Since assuming $\text{ord}_n(a) = n$ or $\text{ord}_n(a) > n$ lead to contadictions, it follows $\text{ord}_n(a) < n$. □

Exercise (4.12)**.** Compute $a^{p-1} \pmod{p}$ for various numbers a and primes p, and make a conjecture.

If natural number a and prime p are relatively prime then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem (4.13)**.** *Let p be a prime and let a be an integer not divisible by p; that is, $(a, p) = 1$. Then $\{a, 2a, 3a, \ldots, pa\}$ is a complete residue system modulo p.*

Proof. Suppose $ia \equiv ja \pmod{p}$ where $1 \leq i, j \leq p$. Then $p \mid a(i - j)$. Since $(a, p) = 1$, by Theorem 1.41 $p \mid (i - j)$. Since $1 \leq i, j \leq p$ we have $0 \leq |i - j| \leq p - 1$. Then the only possible value of $|i - j|$ is $|i - j| = 0$. Hence, $i = j$. Thus, the numbers $1a, 2a, \ldots, pa$ are pairwise incongruent modulo p. Moreover, $\{1a, 2a, \ldots, pa\}$ has a cardinality of p. Then by Theorem 3.17, it follows $\{1a, 2a, \ldots, pa\}$ form a complete residue system modulo p. □

Theorem (4.14)**.** *Let p be a prime and let a be an integer not divisible by p. Then*

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

Proof. Let $B = \{0, 1, 2, \ldots, p - 1\}$ and $A^* = \{a, 2a, \ldots, pa\}$. It follows both A^* and B are complete residue systems modulo p. Note that $0 \equiv pa \pmod{p}$ so $A = \{0, a, \ldots, (p-1)a\}$ is also a complete residue system modulo p. Let $A' = A - \{0\}$ and $B' = B - \{0\}$. Then there is a bijection $f \colon A' \to B'$ defined as $f(m) = r$ where $m = pq + r$ where $0 \leq r \leq p - 1$ and $q \in \mathbb{Z}$ from the division algorithm for all $m \in A'$. Then $m \equiv f(m) \pmod{p}$ for all $m \in A'$. It follows

$$\prod_{i \in A'} i \equiv \prod_{i \in A'} f(i) \pmod{p}$$

□

Theorem (4.15)**.** *If p is a prime and a is an integer relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. If p is a prime and a is an integer relatively prime to p. Then $p \nmid a$. Then by Theorem 4.14 we have

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

Then by definition of congruence we have $p \mid (p-1)!(a^{p-1}-1)$. Since p is prime $(p,(p-1)!) = 1$. By Theorem 1.41 $p \mid a^{p-1}-1$ so then by definition of congruence we have $a^{p-1} \equiv 1 \pmod{p}$. □

Theorem (4.16)**.** *If p is a prime and a is any integer, then $a^p \equiv a \pmod{p}$.*

Proof. First suppose $(a,p) = 1$. By Theorem 4.15 it follows $a^{p-1} \equiv 1 \pmod{p}$. Note $a \equiv a \pmod{p}$ so then $a^{p-1}(a) \equiv 1(a) \pmod{p}$. Then $a^p \equiv a \pmod{p}$.

Now suppose a and p are not relatively prime. Then $p \mid a$ by Theorem 2.46. Then $p \mid a(a^{p-1}-1)$ so then $a^p \equiv a \pmod{p}$. □

Theorem (4.17)**.** *The two versions of Fermat's Little Theorem stated above are equivalent to one another, that is, each one can be deduced from the other.*

Proof. We first show Theorem 4.15 implies 4.16. First suppose $(a,p) = 1$. By Theorem 4.15 it follows $a^{p-1} \equiv 1 \pmod{p}$. Note $a \equiv a \pmod{p}$ so then $a^{p-1}(a) \equiv 1(a) \pmod{p}$. Then $a^p \equiv a \pmod{p}$.

Now suppose a and p are not relatively prime. Then $p \mid a$ by Theorem 2.46. Then $p \mid a(a^{p-1}-1)$ so then $a^p \equiv a \pmod{p}$.

Now we prove the reverse direction; show Theorem 4.16 implies Theorem 4.15. Suppose p is prime and a is relatively prime to p. Then by Theorem 4.16 we have $a^p \equiv a \pmod{p}$. By definition of congruence we have $p \mid a^p - a$ or $p \mid a(a^{p-1}-1)$. Since a and p are relatively prime we have $(a,p) = 1$. Then by Theorem 1.41 it follows $p \mid a^{p-1}-1$. Then by definition of congruence, we have $a^{p-1} \equiv 1 \pmod{p}$. □

Theorem (4.18)**.** *Let p be a prime and a be an integer. If $(a,p) = 1$, then $ord_p(a)$ divides $p-1$, that is, $ord_p(a) \mid p-1$.*

Proof. For the sake of contradiction suppose $\mathrm{ord}_p(a) \nmid p-1$. Then we have

$$p - 1 = \mathrm{ord}_p(a)q + r$$

where $1 \leq r \leq \mathrm{ord}_p(a) - 1$. Then we have $1 \equiv a^{p-1} \equiv a^{\mathrm{ord}_p(a)q}a^r \equiv a^r \pmod{p}$. Note $r < \mathrm{ord}_p(a)$ which is a contradiction. Hence, $\mathrm{ord}_p(a) \mid p-1$. □

Exercise (4.19)**.** Compute each of the following without the aid of a calculate or computer.

(1) $512^{372} \pmod{13}$
(2) $3444^{3233} \pmod{17}$
(3) $123^{456} \pmod{23}$

For (1) note that $512 \equiv 5 \pmod{13}$. Also $5^4 \equiv 1 \pmod{13}$ and $4 \mid 372$. Then $512^{372} \equiv 1 \pmod{13}$. For (2) note that $3444 \equiv 10 \pmod{17}$. And then $10^8 \equiv -1 \pmod{17}$ so $10^16 \equiv 1 \pmod{17}$. Then $3444 = 202(16)+1$. Hence $3444^{3233} \equiv 10 \pmod{17}$. For (3) we find $123 \equiv 8 \pmod{23}$ and $8^{11} \equiv 1 \pmod{23}$. Also $456 = 41(11)+5$. Then $123^{456} \equiv (8^{11})^{41}(8)^5 \equiv 8^5 \equiv 16 \pmod{23}$.

Exercise (4.20)**.** Find the remainder upon division of 314^{519} by 31.

Note $314 \equiv 4 \pmod{31}$ and that $4^5 \equiv 1 \pmod{31}$. Then $314^{159} \equiv (4^5)^{31}(4)^4 \equiv 4^4 \equiv 8 \pmod{31}$. So the remainder is 8.

Theorem (4.21)**.** *Let n and m be natural numbers that are relatively prime, and let a be an integer. If $x \equiv a \pmod{n}$ and $x \equiv a \pmod{m}$, then $x \equiv a \pmod{nm}$.*

Proof. Suppose $x \equiv a \pmod{n}$, $x \equiv a \pmod{m}$, and $(n, m) = 1$. By definition of congruence we have $n \mid x - a$ and $m \mid x - a$. Since $(n, m) = 1$, by Theorem 1.42 we have $nm \mid x - a$. Then by definition of congruence we have $x \equiv a \pmod{nm}$. □

Exercise (4.22)**.** Find the remainder when 4^{72} is divided by 91.

$4^3 \equiv 1 \pmod{7}$ and $4^6 \equiv 1 \pmod{13}$. Then $4^{72} \equiv 1 \pmod{7}$ and $4^{72} \equiv 1 \pmod{13}$. Since $(7, 13) = 1$ we have $4^{72} \equiv 1 \pmod{91}$. So the remainder when 4^{72} is divided by 91 is 1.

Week 21

Exercise (4.23)**.** Find the natural number $k < 117$ such that $2^{117} \equiv k \pmod{117}$.

$2^{12} \equiv 1 \pmod{117}$. Then $2^{117} = (2^{12})^9(2)^9 \equiv 2^9 \equiv 44 \pmod{117}$.

Theorem (4.24)**.** *Let a and b be numbers and let n be a natural number. Then*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i}b^i$$

Proof. We prove by induction. Let $P(u)$ be the theorem statement for when $n = u$. Consider $n = 1$. Then

$$(a+b)^1 = \sum_{i=0}^{1} \binom{1}{i} a^{1-i}b^i = \binom{1}{0} a^1b^0 + \binom{1}{1} a^0b^1 = a + b$$

Hence, $P(1)$ holds. For the inductive step, suppose $P(m)$ is true. Then

$$\begin{aligned}(a+b)^{m+1} &= (a+b)(a+b)^m \\ &= (a+b)\sum_{i=0}^{m} \binom{m}{i} a^{m-i}b^i \\ &= \sum_{i=0}^{m+1} k_i a^{m+1-i}b^i\end{aligned}$$

The second to last line holds by the inductive hypothesis. Consider the term $k_j a^{m+1-j}b^j$ for some $j \in \{0, 1, \ldots, m+1\}$. First suppose $1 \leq j \leq m$. Then we have

$$\begin{aligned}k_j a^{m+1-j}b^j &= a\binom{m}{j} a^{m-j}b^j + b\binom{m}{j-1} a^{m-(j-1)}b^{j-1} \\ &= \left(\binom{m}{j}\binom{m}{j-1}\right) a^{m+1-j}b^j \\ &= \binom{m+1}{j} a^{m+1-j}b^j\end{aligned}$$

Hence, $k_j = \binom{m+1}{j}$. Now consider the case where $j = 0$. Then

$$\begin{aligned}k_0 a^{m+1} &= a\binom{m}{0} a^m \\ &= \binom{m+1}{0} a^{m+1}\end{aligned}$$

Hence, $k_0 = \binom{m+1}{0}$. Now consider the case where $j = m+1$. Then

$$\begin{aligned}k_{m+1} b^{m+1} &= b\binom{m}{m} b^m \\ &= \binom{m+1}{m+1} b^{m+1}\end{aligned}$$

Hence, $k_{m+1} = \binom{m+1}{m+1}$. In all cases, $k_j = \binom{m+1}{j}$. Therefore, $P(m+1)$ holds. □

Lemma (A)**.** *If k and m are natural numbers such that $1 \leq k \leq m$, then*

$$\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k-1}$$

Proof. By definition, the right hand side is equivalent to

$$\begin{aligned}
\binom{m}{k} + \binom{m}{k-1} &= \frac{m!}{k!(m-k)!} + \frac{m!}{(k-1)!(m-k+1)!} \\
&= \frac{m!(m-k+1)}{k!(m-k)!(m-k+1)} + \frac{m!k}{k(k-1)!(m-k+1)!} \\
&= \frac{(m+1)! - m!k}{k!(m+1-k)!} + \frac{m!k}{k!(m+1-k)!} \\
&= \frac{(m+1)!}{k!((m+1)-k)!} \\
&= \binom{m+1}{k}
\end{aligned}$$

Hence, the right hand side and left hand side are equivalent. □

Lemma (4.25)**.** *If p is prime and i is a natural number less than p, then p divides $\binom{p}{i}$.*

Proof. We prove by inducting on i. Let $P(u)$ be the lemma statement for when $i = u$. Consider the case $P(1)$. Then $\binom{p}{1} = p$ and $p \mid p$. This concludes the base case. For the inductive step suppose $P(k-1)$ is true where $k - 1 < p$. By Lemma A we know $\binom{p}{k} = \binom{p+1}{k} - \binom{p}{k-1}$. Moreover, by the inductive hypothesis we know $p \mid \binom{p}{k-1}$. By algebra, note that

$$\binom{p}{k-1}\frac{p+1}{k} = \binom{p+1}{k}$$

Since $p \mid \binom{p}{k-1}$ then $p \mid \binom{p}{k-1}(p+1)$. For the sake of contradiction, suppose $p \nmid \binom{p}{k-1}\frac{p+1}{k}$. Then by Theorem 2.46 we have $\left(\binom{p}{k-1}\frac{p+1}{k}, p\right) = 1$. Moreover, since we are assuming $k < p$ and p is prime it follows $(k, p) = 1$. Since $\left(\binom{p}{k-1}\frac{p+1}{k}, p\right) = 1$ and $(k, p) = 1$ by Theorem 1.43 it follows $\left(\binom{p}{k-1}(p+1), p\right) = 1$ but this contradicts the fact that $p \mid \binom{p}{k-1}(p+1)$. Hence, $p \mid \binom{p}{k-1}\frac{p+1}{k}$. Then $p \mid \binom{p+1}{k}$. Then because $p \mid \binom{p+1}{k}$ and $p \mid \binom{p}{k-1}$ by Theorem 1.32 it follows $p \mid \binom{p}{k}$. Hence, $P(k)$ holds. It follows $P(j)$ holds for all j where $1 \leq j \leq p-1$. □

Lemma (B)**.** *Suppose $m, n \in \mathbb{Z}$ such that $0 \leq m \leq n$ and $n \geq 1$. Then $\binom{n}{m} \in \mathbb{Z}$ and $\binom{\{n}{m\} \in \mathbb{N}}$*

Proof. We prove by inducting on n. Let $P(u)$ be the lemma statement for when $n = u$. For the base case consider when $n = 1$. Then $\binom{1}{0}$ and $\binom{1}{1}$ are both equal to one. Then $\binom{1}{0}, \binom{1}{1} \in \mathbb{N}$. Hence, $P(1)$ holds. For the inductive step, suppose $P(k-1)$ holds. Take $j \in \mathbb{Z}$ such that $0 \leq j \leq k$. If $j = 0$, then $\binom{k}{0} = 1 \in \mathbb{Z}$ and $1 \geq 1$. Otherwise $1 \leq j \leq k$ and equivalently $0 \leq j - 1 \leq k - 1$. It follows $\binom{k-1}{j}$ and $\binom{k-1}{j-1}$ well-defined. Moreover, they are natural numbers by the inductive hypothesis. Then their sum must also be a natural number by closure of addition of natural numbers. Moreover, by Lemma A we know

$$\binom{k-1}{j} + \binom{k-1}{j-1} = \binom{k}{j}$$

so then $\binom{k}{j} \in \mathbb{N}$. Hence, $P(k)$ holds. This concludes the induction. $\square$

Theorem (Fermat's Little Theorem, Version II)**.** *If p is a prime and a is an integer, then $a^p \equiv a \pmod{p}$.*

Proof. Let $P(u)$ be the theorem statement for when $a = u$. We prove $P(u)$ is true for all natural numbers first. Consider $P(1)$. Then $1^p \equiv 1 \pmod{p}$. Then $P(1)$ holds. For the inductive step, assume $P(m)$ holds. Then we show $p \mid (m+1)^p - (m+1)$. Note that

$$\begin{aligned}(m+1)^p - (m+1) &= \left(\sum_{i=0}^{p} \binom{p}{i} m^{p-i}\right) - m - 1 \\ &= \binom{p}{0} m^p - m + \binom{p}{1} m^{p-1} + \binom{p}{2} m^{p-2} + \cdots + \binom{p}{p-1} m^1 + 1 - 1 \\ &= m^p - m + \sum_{i=1}^{p-1} \binom{p}{i} m^{p-i}\end{aligned}$$

Note $p \mid m^p - m$ by the inductive hypothesis and $p \mid \binom{p}{i} m^{p-i}$ for all $i \in \{1, 2, \ldots, p-1\}$ by Lemma 4.25. Then $p \mid (m+1)^p - (m+1)$. Hence, $(m+1)^p \equiv m + 1 \pmod{p}$. Hence, $P(m+1)$ holds. This concludes the induction.

It follows if $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$. If $a = 0$ then the theorem still holds since $0^p = 0$. Now consider the case where $a < 0$. First consider when $p = 2$. Then we have to show $a^2 \equiv a \pmod{2}$. If $a \equiv 0 \pmod{2}$ then $a^2 \equiv 0 \pmod{2}$. Hence $a \equiv a^2 \pmod{2}$. If $a \equiv 1 \pmod{2}$ then $a^2 \equiv 1 \pmod{2}$. Hence, $a \equiv a^2 \pmod{2}$. Now suppose $p \neq 2$. Then p is odd since p is prime. Since $a < 0$ then $-a > 0$. Then $(-a)^p \equiv -a \pmod{p}$. Since p is odd $-(a^p) = (-a)^p$. Then we have $-a^p \equiv -a \pmod{p}$. Then $a^p \equiv a \pmod{p}$. Hence, the theorem holds for any integer a. $\square$

Question (4.27)**.** The numbers $1, 5, 7$, and 11 are all the natural numbers less than or equal to 12 that are relatively prime to 12, so $\phi(12) = 4$.

(1) $\phi(7) = 6$.
(2) $\phi(15) = 8$.
(3) $\phi(21) = 12$
(4) $\phi(35) = 24$

Theorem (31)**.** *Let n be a natural number and let $x_1, x_2, \ldots, x_{\phi(n)}$ be the distinct natural numbers less than or equal to n that are relatively prime to n. Let a be a non-zero integer relatively prime to n and let i and j be different natural numbers less than or equal to $\phi(n)$. Then $ax_i \not\equiv ax_j \pmod{n}$.*

Proof. We prove the contrapositive. Suppose $ax_i \equiv ax_j \pmod{n}$. Then $n \mid ax_i - ax_j$. Since $(a, n) = 1$, by Theorem 1.41 it follows $n \mid x_i - x_j$. Then $x_i \equiv x_j \pmod{n}$. Note $1 \leq x_i, x_j \leq n$. Then $0 \leq |x_i - x_j| \leq n - 1$. Since $n \mid x_i - x_j$ it follows $|x_i - x_j| = 0$. Then $x_i = x_j$. Since $x_1, x_2, \ldots, x_{\phi(n)}$ are distinct natural numbers it follows $i = j$. $\square$

Theorem (4.31)**.** *Let n be a natural number and let $x_1, x_2, \ldots, x_{\phi(n)}$ be the distinct natural numbers less than or equal to n that are relatively prime to n. Let a be a non-zero integer relatively prime to n and let i and j be different natural numbers less than or equal to $\phi(n)$. Then $ax_i \not\equiv ax_j \pmod{n}$.*

Proof. We prove the contrapositive. Suppose $ax_i \equiv ax_j \pmod{n}$. Then $n \mid ax_i - ax_j$. Since $(a, n) = 1$, by Theorem 1.41 it follows $n \mid x_i - x_j$. Then $x_i \equiv x_j \pmod{n}$. Note $1 \leq x_i, x_j \leq n$. Then $0 \leq |x_i - x_j| \leq n - 1$. Since $n \mid x_i - x_j$ it follows $|x_i - x_j| = 0$. Then $x_i = x_j$. Since $x_1, x_2, \ldots, x_{\phi(n)}$ are distinct natural numbers it follows $i = j$. □

Theorem (4.32–Euler's Theorem)**.** *If a and n are integers with $n > 0$ and $(a, n) = 1$, then*

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

Proof. Let a and n be integers with $n > 0$ and $(a, n) = 1$. Define the sets A and B as

$$A = \{x_1, x_2, \ldots, x_{\phi(n)}\}$$
$$B = \{ax_1, ax_2, \ldots, ax_{\phi(n)}\}$$

where the numbers $x_1, x_2, \ldots, \phi(n)$ are the numbers relatively prime to n. Now we define the map $f\colon \{1, 2, \ldots, \phi(n)\} \to \{1, 2, \ldots, \phi(n)\}$ as $f(i) = j$ where $ax_i \equiv x_j \pmod{n}$ for some $j \in \{1, 2, \ldots, \phi(n)\}$. First we show f is well-defined. Consider some $i \in \{1, 2, \ldots, \phi(n)\}$. Then by the division algorithm we have $ax_i = nq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r \leq n - 1$. By Theorem 1.33 we have $(ax_i, n) = (n, r)$. Since $(a, n) = 1$ and $(x_i, n) = 1$ by Theorem 1.43 it follows $(ax_i, n) = 1$. Then $(n, r) = 1$. Since $(n, r) = 1$ and $0 \leq r \leq n - 1$, it follows $r = x_j$ for some $j \in \{1, 2, \ldots, \phi(n)\}$. Hence, f is well-defined.

Now we show f is injective. Suppose $i \neq j$ and let $f(i) = k$ and $f(j) = \ell$. For the sake of contradiction suppose $k = \ell$. Then we have $x_k \equiv x_\ell \pmod{n}$. Moreover, since $f(i) = k$ and $f(j) = \ell$ we have $ax_i \equiv x_k \pmod{n}$ and $ax_j \equiv x_\ell \pmod{n}$. Then by repeated application of transitivity and commutativity of congruence we have $ax_i \equiv ax_j \pmod{n}$. This contradicts Theorem 4.31 It follows f is in fact injective.

Now we show f is surjective. For the sake of contradiction suppose f is not surjective. Then the image of B under f is a proper subset of A. Then $|\mathrm{im}(f)| \leq \phi(n) - 1$ but we know $|B| = \phi(n)$. Then by the pigeonhole principle there exists k such that for some $i \neq j$ $f(i) = f(j) = k$. However, this contradicts the injectivity of f. Hence, f is surjective. It follows f is a bijection.

Notice by definition of f we have $ax_i \equiv x_{f(i)} \pmod{n}$ for all $i = 1, 2, \ldots, \phi(n)$. Then

$$ax_1 \cdot ax_2 \cdots ax_{\phi(n)} \equiv x_{f(1)} \cdot x_{f(2)} \cdots x_{f(\phi(n))} \pmod{n}$$

and since f is a bijection from B to A we have

$$x_{f(1)} \cdot x_{f(2)} \cdots x_{f(\phi(n))} \equiv x_1 \cdot x_2 \cdots x_{\phi(n)} \pmod{n}$$

Then by transitivity of congruence we have

$$ax_1 \cdot ax_2 \cdots ax_{\phi(n)} \equiv x_1 \cdot x_2 \cdots x_{\phi(n)} \pmod{n}$$

Note $(x_i, n) = 1$ for all i and by repeated application (finitely many) of Theorem 1.43 it follows $(x_1 x_2 \cdots x_{\phi(n)}, n) = 1$. Then by Theorem 1.45 we have

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

□

Corollary (4.33–Fermat's Little Theorem)**.** *If p is a prime and a is an integer relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Since a and p are relatively prime, we can apply Euler's Theorem. Then we have $a^{\phi(p)} \equiv 1 \pmod{p}$. If p is prime, then by definition of a prime number for all integers k where $1 \leq k < p$, $p \nmid k$ so then by Theorem 2.46 we have $(p, k) = 1$. It follows $\phi(p) = p - 1$. Then $a^{p-1} \equiv 1 \pmod{p}$. □

Exercise (4.34)**.** Compute each of the following without the aid of a calculator or computer.

(1) $12^{49} \pmod{15}$. Note that $12 \equiv -3 \pmod{15}$ and $(-3)^5 \equiv -3 \pmod{15}$. Then $12^{49} \equiv (-3)^{45}(-3)^4 \equiv (-3)^9(-3)^4 \equiv (-3)^{13} \equiv (-3)^2(-3)^3 \equiv (-3)^5 \equiv -3 \equiv 12 \pmod{15}$.
(2) $139^{112} \pmod{27}$. Since $(139, 27) = 1$, we can apply Euler's Theorem. Then $\phi(27) = 27(1 - 1/3) = 18$. Then $139^{112} \equiv 139^4 \equiv 4^4 \equiv 13 \pmod{27}$

Theorem (4.36)**.** *Let p be a prime and let a be an integer such that $1 \leq a < p$. Then there exists a unique natural number b less than p such that $ab \equiv 1 \pmod{p}$.*

Proof. Let p be a prime and let a be an integer such that $1 \leq a < p$. Since $a < p$ and p is prime, it follows a and p are relatively prime for all a. Then by Fermat's Little Theorem it follows $a^{p-1} \equiv 1 \pmod{p}$. Since $p \geq 2$ it follows $a(a^{p-2}) \equiv 1 \pmod{p}$ where $a, a^{p-2} \in \mathbb{Z}$. By Theorem 3.14 there exists unique integer $b \in \{0, 1, \ldots, p-1\}$ such that $a^{p-2} \equiv b \pmod{p}$. Since $a^{p-2} \equiv b \pmod{p}$ then $1 \equiv a \cdot a^{p-2} \equiv ab \pmod{p}$. □

Exercise (4.37)**.** Let p be a prime. Show that the natural numbers 1 and $p - 1$ are their own inverses modulo p.

Proof. Let p be prime. Then $(1)(1) \equiv 1 \pmod{p}$. Hence, 1 is its own inverse modulo p. Then $(p-1)(p-1) = p^2 - 2p + 1 \equiv 1 \pmod{p}$. Hence, $p - 1$ is its own inverse modulo p. □

Theorem (4.38)**.** *Let p be a prime and let a and b be integers such that $1 < a, b < p - 1$ and $ab \equiv 1 \pmod{p}$. Then $a \neq b$.*

Proof. For the sake of contradiction suppose $a = b$ and $ab \equiv 1 \pmod{p}$. Then $a^2 \equiv 1 \pmod{p}$. Then $p \mid a^2 - 1$ so $p \mid (a-1)(a+1)$. By Theorem 2.47 it follows either $p \mid a - 1$ or $p \mid a + 1$. Suppose $2 \leq a \leq p - 2$. Then $1 \leq a - 1 \leq p - 3$ and $3 \leq a + 1 \leq p - 1$. It follows $p \nmid a - 1$ and $p \nmid a + 1$. This is a contradiction. Hence, $a \neq b$. □

Exercise (4.39)**.** Find all pairs of numbers a and b in $\{2, 3, \ldots, 11\}$ such that $ab \equiv 1 \pmod{13}$.

$2 \cdot 7 \equiv 1 \pmod{13}$, $3 \cdot 9 \equiv 1 \pmod{13}$, $4 \cdot 10 \equiv 1 \pmod{13}$, $5 \cdot 8 \equiv 1 \pmod{13}$, $6 \cdot 11 \pmod{13}$.

Theorem (4.40)**.** *If p is a prime larger than 2, then $2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod{p}$*

Proof. Let $S = \{2, 3, \ldots, p-2\}$. Then define the binary relation $\sim$ on S as $a \sim b$ if and only if either $ab \equiv 1 \pmod{p}$ or $a = b$. Now we show $\sim$ is an equivalence relation. By construction of the relation, $\sim$ is reflexive. Now suppose $a \sim b$. If $ab \equiv 1 \pmod{p}$ then $ba \equiv 1 \pmod{p}$ by commutativity of multiplication of natural numbers. If $a = b$ then $b = a$ by commutativity of equality. It follows $\sim$ is commutative. Now we show $\sim$ is transitive.

Suppose $a \sim b$ and $b \sim c$. There are four cases. First suppose $ab \equiv 1 \pmod{p}$ and $bc \equiv 1 \pmod{p}$. Then $ab \equiv bc \pmod{p}$. Then $p \mid b(a-c)$ but $b < p$ so $p \mid (a-c)$. Since $a, c \in S$ it follows $0 \leq |a-c| \leq p-4$. We must have $a = c$. Then $a \sim c$. Second suppose $ab \equiv 1 \pmod{p}$ and $b = c$. Then by substitution $ac \equiv 1 \pmod{p}$ so $a \sim c$. Third suppose $a = b$ and $bc \equiv 1 \pmod{p}$. Then by substitution we have $ac \equiv 1 \pmod{p}$. Then $a \sim c$. Fourth suppose $a = b$ and $b = c$. Then $a = c$. Then $a \sim c$. In all four cases, $a \sim c$; hence, $\sim$ is transitive. Since $\sim$ is reflexive, commutative, and transitive, $\sim$ is a equivalence relation.

By the lemma, the set of equivalence classes (as defined in the Lemma) partition S. Let $\overline{S}$ be the set of equivalence classes,

$$\overline{S} = \{C_{a_1}, C_{a_2}, \ldots, C_{a_n}\}$$

We know $\overline{S}$ is finite since S is finite. Now we show $|C_a| = 2$ for all $a \in S$. We know $a \in C_a$. Moreover, there exists $b \in S$ such that $ab \equiv 1 \pmod{p}$ where $a \neq b$ by Theorem 4.38. Then $a, b \in C_a$. Let $c \in C_a$. Then $a \sim c$. Then either $ac \equiv 1 \pmod{p}$ or $a = c$. If $ac \equiv 1 \pmod{p}$, then $ac \equiv bc \pmod{p}$ which implies $p \mid a(b-c)$. Since $a < p$ it follows $(a, p) = 1$ so then $p \mid (b-c)$ by Theorem 1.41. But $0 \leq |b-c| \leq p-4$. Hence, $b = c$. Therefore, either $c = a$ or $c = b$. Hence, $|C_a| = 2$ for all $a \in S$. Then $n = (p-3)/2$.

Consider the product $2 \cdot 3 \cdots (p-2)$. Then we have

$$\begin{aligned} 2 \cdot 3 \cdots (p-2) &= \prod_{i=1}^{n} \left(\prod_{x \in C_{a_i}} x \right) \\ &\equiv \prod_{i=1}^{n} (1) \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

Note the first congruence holds by definition of the equivalence class. □

Lemma. *Given an equivalence relation on a set S, the set of equivalence classes form a partition on S.*

Proof. First recall a partition is a collection of non-empty disjoint subsets of S such that union of the collection is the whole set S. Moreover, an equivalence relation is a binary relation that is reflexive, commutative, and transitive. Now suppose we have an equivalence relation $\sim$ on a set S. Let $a \in S$. Then the equivalence class of a, which we denote as C_a, is defined as

$$C_a = \{b \in S \mid a \sim b\}$$

Now we show the collection of equivalence classes form a partition on S. Note, since $\sim$ is reflexive, it follows $a \sim a$ so then $a \in C_a$ for all $a \in S$. Then C_a is non-empty for all a. Moreover, it follows $S = \cup_{a \in S} C_a$. Now we show equivalence classes are disjoint. Formally, we show that if $C_a \cap C_b \neq \varnothing$ then $C_a = C_b$. We show that $C_a \subset C_b$ and $C_b \subset C_a$. However, it suffices to show $C_a \subset C_b$ since a and b are arbitrary. Let $u \in C_a \cap C_b$. Let $x \in C_a$. Note that $b \sim u$, $u \sim a$, and $a \sim x$. Then by two applications of transitivity we have $b \sim x$. It follows $x \in C_b$. Hence, $C_a \subset C_b$. An analogous argument shows $C_b \subset C_a$. Hence, $C_a = C_b$. It follows equivalence classes are disjoint. Since we have shown equivalence classes are non-empty and disjoint and their union is the whole set S, the collection of equivalence classes form a partition on S. □

Week 23

Theorem (4.41)**.** *If p is prime then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. Suppose p is a prime. Then the integers $1, \ldots, p-1$ have an inverse modulo p by theorem 4.38. Note that the inverse is unique and each number is the inverse of its inverse. Thus we have partition the set $\{2, \ldots, p-2\}$ into pairs so that their product is congruent to 1 modulo p. It follows $(p-1)! \equiv (1)(p-1) \equiv p-1 \equiv -1 \pmod{p}$. □

Theorem (4.42)**.** *If n is a natural number such that $(n-1)! \equiv -1 \pmod{n}$ then n is prime.*

Proof. For the sake of contradiction suppose n is composite. Then there exists $k \mid n$ and $k < n$. So $k \mid (n-1)!$ and $k \equiv 1 \pmod{n}$. This means $k \mid 1$ so n must be prime. □

Exercise (E)**.** Make a conjecture about the value of $\phi(p)$ for a prime p. Prove your conjecture.

Conjecture. *If p is prime then $\phi(p) = p-1$.*

Proof. Let p be prime. Then by definition $k \nmid p$ for all $1 < k < p$. Then $(k, p) = 1$. Moreover, $(1, p) = 1$ but $(p, p) \neq 1$. Then we have $(j, p) = 1$ for $j = 1, 2, \ldots, p-1$. Hence, $\phi(p) = p-1$. □

Exercise (F)**.** Make a conjecture about the value of $\phi(p^k)$ for a prime p and natural numbers k. Prove your conjecture.

Conjecture. *If p is prime and $k \in \mathbb{N}$ then $\phi(p^k) = p^k - p^{k-1}$.*

Proof. Note for some natural number n that $(n, p) = 1$ if and only if $(n, p^k) = 1$. Then the only numbers in $\{1, 2, \ldots, p^k - 1\}$ that are not relatively prime to p^k are multiples of p. Then there are $p^k/p = p^{k-1}$ multiples of p. But this includes p^k so there are $p^{k-1} - 1$ multiples of p in $\{1, 2, \ldots, p^k - 1\}$. Then $\phi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1}$. □

Theorem (G)**.** *If n is a natural number and A is a complete residue system modulo n, then the number of numbers in A that are relatively prime to n is equal to $\phi(n)$.*

Proof. Let $x_1, x_2, \ldots, x_{\phi(n)}$ be the numbers that are relatively prime to n. Let $A = \{a_1, \ldots, a_n\}$. Since A is a CRS it follows for every x_i there is $j \in \{1, \ldots, n\}$ such that $x_i \equiv a_j \pmod{n}$. Since $(n, x_i) = 1$ it follows $(a_j, n) = 1$ by Theorem 4.3. Then the number of elements in A that are relatively prime to n is at least $\phi(n)$. Now consider some $a_i \in A$ that is relatively prime to n. Then by the division algorithm we have $a_i = nq + r_i$ where $0 \leq r_i \leq n-1$. Then $1 = (a_i, n) = (n, r_i)$. Hence $r_i = x_j$ for some $j \in \{1, 2, \ldots, \phi(n)\}$. It follows for $a_i \equiv x_j \pmod{n}$. It follows the number of elements in A that are relatively prime to n is at most $\phi(n)$. Hence, the number of elements in A that are relatively prime to n is $\phi(n)$. □

Theorem (H)**.** *If n is a natural number, k is an integer, and m is an integer relatively prime to n, then the set of n integers*

$$\{k, k+m, \ldots, k+(n-1)m\}$$

is a complete residue system modulo n.

Proof. First we show no two are pairwise congruent. Suppose $k + im \equiv k + jm \pmod{n}$ where $i, j \in \{0, 1, \ldots, n-1\}$. then $n \mid m(i-j)$. Since n and m are relatively prime it follows $n \mid i-j$. Moreover, $0 \leq |i-j| \leq n-1$. It follows $i = j$. Hence, no two elements are pairwise congruent. Moreover, there are n elements. Then by Theorem 3.17 it follows the set is a complete residue system modulo n. □

Exercise (I)**.** Did on paper. You can use the principle of inclusion and exclusion to find the total number.

Theorem (J)**.** *Let m and n be relatively prime. Then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. Consider the set of numbers $\{0, 1, \ldots, mn\}$. We can partition the set into subsets $A_1, A_2, \ldots, A_n$ where for $j \in \{1, 2, \ldots, n\}$, A_j is defined as

$$A_j = \{in + j \mid 0 \leq i \leq m - 1\}$$

Note there are $n - \phi(n)$ numbers less than or equal to n that are not relatively prime to n. Denote these numbers as $y_1, y_2, \ldots, y_{n-\phi(n)}$. Then consider A_{y_k} for $k \in \{1, 2, \ldots, n - \phi(n)\}$. Then

$$A_{y_k} = \{in + y_k \mid 0 \leq i \leq m - 1\}$$

Since y_k is not relatively prime to n we have $(y_k, n) = d$ where $d > 1$. Since $d \mid y_k$ and $d \mid in$, it follows $d \mid (in + y_k)$. It follows all elements in A_{y_k} are not relatively prime to n for all $k = 1, 2, \ldots, \phi(n)$.

Note there are $\phi(n)$ numbers less than or equal to n that are relatively prime to n. Denote these numbers as $x_1, x_2, \ldots, x_{\phi(n)}$. Then consider A_{x_ℓ} for $\ell \in \{1, 2, \ldots, \phi(n)\}$. Then

$$A_{x_\ell} = \{in + x_\ell \mid 0 \leq i \leq m - 1\}$$

Since x_ℓ is relatively prime to n we have $(x_\ell, n) = 1$. Note that for all $i \in \{0, 1, \ldots, m - 1\}$ the number $in + x_\ell$ is of the form after performing the division algorithm when dividing by n since $0 \leq x_\ell \leq n - 1$. It follows $(in + x_\ell, n) = (n, \ell)$. Since $(n, x_\ell) = 1$ it follows $(in + x_\ell, n) = 1$ for all i. Then all elements in A_{x_ℓ} are relatively prime to n.

Now we show for all $\ell = 1, 2, \ldots, \phi(n)$, there are $\phi(m)$ elements in A_{x_ℓ} that are also relatively prime to m. Fix ℓ. Then A_{x_ℓ} is of the form

$$A_{x_\ell} = \{x_\ell, 1n + x_\ell, 2n + x_\ell, \ldots, (m - 1)n + x_\ell\}$$

Note there are m elements in A_{x_ℓ}. We show that A_{x_ℓ} is a complete residue system modulo m. Note there are m elements so by Theorem 3.17 it suffices to show no two elements are congruent. Suppose for some $i, j = 0, 1, \ldots, m - 1$ that we have $in + x_\ell \equiv jn + x_\ell \pmod{m}$. Then $m \mid n(i - j)$. Since m and n are relatively prime, by Theorem 1.41 it follows $m \mid (i - j)$ but $0 \leq |i - j| \leq m - 1$ so then $i = j$. Then no two elements are congruent so A_{x_ℓ} is a complete residue system modulo m. Then by Theorem G, it follows there are $\phi(m)$ elements in A_{x_ℓ} that are relatively prime to m.

In total we have if $(n, i) \neq 1$ and $i \leq n$ then A_i contains no elements relatively prime to n. If $(n, i) = 1$ and $i \leq n$ then all elements of A_i are relatively prime to n. Moreover, of all the elements in A_i, only $\phi(m)$ of them are in addition relatively prime to m. In total, there are at least $\phi(n)\phi(m)$ elements in A that are relatively prime to both n and m. If $(z, n) = 1$ and $(z, m) = 1$ then $(z, nm) = 1$ so then there are at least $\phi(n)\phi(m)$ elements relatively prime to nm. Moreover, if an element say u is relatively prime to nm. Then we have $(u, mn) = 1$. Moreover, since $(n, m) = 1$, by Theorem 2.28 it follows $(u, mn) = (u, m)(u, n)$. Then it must be $(u, m) = (u, n) = 1$. Hence, there are exactly $\phi(n)\phi(m)$ elements relatively prime to nm. Hence, $\phi(mn) = \phi(m)\phi(n)$. □

Exercise (K)**.** Compute the following.

(1) $\phi(5) = 4$.
(2) $\phi(7) = 6$.

(3) $\phi(35) = 24$.
(4) $\phi(45) = \phi(3)^2\phi(5) = 16$
(5) $\phi(98) = 42$
(6) $\phi(5^6 11^4 17^{10}) = \phi(5)^6\phi(11)^4\phi(17)^{10} = 4^6 10^4 16^{10}$.