# A First Course in Abstract Algebra
# Part 1

Noah Lewis

September 2, 2025

## Contents



## 1 Chapter 1: The Natural Numbers (Theory)

**Axiom 1** (The Well-ordering Principle)**.** *Every non-empty subset of* $\mathbb{N}$ *has a least element.*

**Theorem 1** (Principle of Mathematical Induction)**.** *Suppose* $X$ *is a subset of* $\mathbb{N}$ *that satisifes the following criteria:*

1. $1 \in X$*, and*
2. *If* $k \in X$ *for all* $k < n$*, then* $n \in X$*.*

*Then* $X = \mathbb{N}$*.*

**Theorem 2** (Well Ordering Implies Mathematical Induction)**.** *The Well-ordering Principles implies the Principle of Mathematical Induction.*

## 2 Chapter 1: The Natural Numbers (Quick Excersizes)

**Quick Excerisize 1**

What is the set $X$ in this proof? Because?

**Solution:**

The set $X$ is the natural numbers. The base case is 1 and prove inductively it follows for $n > 1$.

**Quick Excerisize 2**

Verify that the inequality $a_{n+1} \leq 2a_n$ holds for $n = 1$ and $n = 2$.

Solution:

$a_{n+1} \leq 2_a n \iff 1 \leq 2(1) = 1 \leq 2$

$a_{n+1} \leq 2_a n \iff 2 \leq 2(1) = 2 \leq 2$

## 3 Chapter 1: The Natural Numbers (Problems)

**Problem 1**

Prove using mathematical induction that for all positive integers $n$,

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

*Proof.* Let $n = 1$ then $\frac{n(n+1)}{2} = \frac{1(1+1)}{2} = \frac{1(2)}{2} = 1$. Assume the formula is true for some integer $k = n - 1$, thus:

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

Thus:

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

□

Problem 3

You probably recall from your previous mathematical work the *triangle inequality:* for any real numbers $x$ and $y$,

$$|x + y| \leq |x| + |y|$$

Accepts this as given (or see a calculus text to recall how it is proved). Generalize the triangle inequality, by proving that

$$|x_1 + x_2 + \cdots + x_n \leq |x_1| + |x_2| + \cdots |x_n|,$$

for any positive integer $n$.

*Proof.* For $n = 1$, trivially $|x_1| \leq |x_1|$. For $n = 2$, $|x_1 + x_2| \leq |x_1| + |x_2|$ by the triangle inequality. Now assume the formula holds for $k = n - 1$, thus:

$$|x_1 + x_2 + \cdots + x_{n-1}| \leq |x_1| + |x_2| + \cdots |x_{n-1}|$$

Thus:

$$\begin{aligned}
&|x_1 + x_2 + \cdots + x_{n-1} + x_n| \\
&\leq |(x_1 + x_2 + \cdots + x_{n-1}) + x_n| \\
&\leq |x_1 + x_2 + \cdots + x_{n-1}| + |x_n| && \text{triangle inequality} \\
&\leq |x_1| + |x_2| + \cdots + |x_n|
\end{aligned}$$

□

Problem 4

Given a positive integer $n$, recall that $n! = 1 \cdot 2 \cdot 3 \cdots$ (this is read as $n$ factorial). Provide an inductive definition for $n!$. (It is customary to actually start this defintion at $n = 0$, setting $0! = 1$)

**Solution**

We can define $n!$ as follows. If $n <= 1$, then $n! = 1$. If $n > 1$, then $n! = n(n - 1)!$.

Problem 5

Prove that $2^n < n!$ for all $n \geq 4$.

*Proof.* Let $n = 4$, then $2^4 = 16 < 4! = 24$. Assume the inequality holds for $k = n - 1$, thus:

$$2^{n-1} < (n - 1)!$$

Thus:

$$\begin{aligned}
&2^{n-1} \cdot 2 < (n - 1)! \cdot n \quad \text{Note: } 2 < 4 \leq n \\
&2^n < n!
\end{aligned}$$

□

Problem 7

Prove the familiar geometric progression formula. Namely, suppose that $a$ and $r$ are real numbers with $r \neq 1$. Then show that:

$$a + ar + ar^2 + \cdots + ar^{n-1} = \frac{a - ar^n}{1 - r}$$

*Proof.* Let $n = 1$, then $a = \frac{a-ar^n}{1-r} = \frac{a-ar}{1-r} = \frac{a(1-r)}{1-r} = a$. Assume the formula holds for $k = n-1$, thus:

$$a + ar + ar^2 + \cdots + ar^{n-2} = \frac{a - ar^{n-1}}{1 - r}$$

Thus

$$\begin{aligned}
&a + ar + ar^2 + \cdots + ar^{n-2} + ar^{n-1} \\
&= \frac{a - ar^{n-1}}{1 - r} + ar^{n-1} \\
&= \frac{a - ar^{n-1}}{1 - r} + \frac{(1 - r)ar^{n-1}}{1 - r} \\
&= \frac{a - ar^{n-1} + (1 - r)(ar^{n-1})}{1 - r} \\
&= \frac{a - ar^{n-1} + ar^{n-1} - ar^n}{1 - r} \\
&= \frac{a - ar^n}{1 - r}
\end{aligned}$$

□

Problem 12

Consider the sequence $a_n$ defined inductively as follows:

$$a_1 = 5, a_2 = 7, a_{n+2} = 3a_{n+1} - 2a_n$$

*Proof.* Let $n = 1$, then $a_1 = 5 = 3+2^n = 3+2^1 = 5$. Let $n = 2$, then $a_2 = 7 = 3+2^n = 3+2^2 = 7$ Assume the formula holds for $k < n$ thus:

$$a_{n-1} = 3 + 2^{n-1}$$

and

$$a_{n-2} = 3 + 2^{n-2}$$

So $k = n$ is:

$$a_n = 3a_{n-1} - 2a_{n-2} = 3(3 + 2^{n-1}) - 2(3 + 2^{n-2})$$

Then:

$$\begin{aligned}
&3(3+2^{n-1})-2(3+2^{n-2})\\
&=9+3\cdot 2^{n-1}-6-2\cdot 2^{n-2}\\
&=3+3\cdot 2^{n-1}-2^{n-1}\\
&=3+2\cdot 2^{n-1}\\
&=3+2^n
\end{aligned}$$

□

**Problem 14**

In this problem you will prove some results about the binomial coefficients, using induction. Recall that:

$$\binom{n}{k}=\frac{n!}{(n-k)!k!}$$

where $n$ is a positive integer, and $0\le k\le n$.
(a) Prove that

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

$n\ge 2$ and $k<n$. Hint: You do not need induction to prove this. Bear in mind that $0!=1$.
(b) Verify that $\binom{n}{0}=1$ and $\binom{n}{n}=1$. Use these facts, together with part a, to prove by induction on $n$ that $\binom{n}{k}$ is an integer, for all $k$ with $0\le k\le n$. (Note: You may have encountered $\binom{n}{k}$ as the count of the number of $k$ element subsets of a set of $n$ objects; it follows that from this $\binom{n}{k}$ is an integer. What we are asking for here is an inductive proof based on algebra.)
(c) Use part a and induction to prove the Binomical Theorem: For non-negative $n$ and variables $x$, $y$,

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$$

*Proof.*

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

□

*Proof.* Let $k = 0$ then, $\binom{n}{0} = \frac{n!}{(n-0)!(0!)} = \frac{n!}{n!} = 1 \in \mathbb{Z}$. Let $k = n$ then, $\binom{n}{n} = \frac{n!}{(n-n)!(n!)} = \frac{n!}{n!} = 1 \in \mathbb{Z}$. Assume this holds for $n-1$, thus for all $k$ where $0 \leq k \leq n-1$:

$$\binom{n-1}{k} \in \mathbb{Z}$$

Then:

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

Since each of these terms exist in $\mathbb{Z}$ their sum $\binom{n}{k}$ is in $\mathbb{Z}$ since the integers are closed over addition. □

*Proof.* Let $n = 0$. Then:

$$(x+y)^0 = 1 = \sum_{k=0}^{0} \binom{0}{k} x^k y^{0-k} = \binom{0}{0} x^0 y^0 = 1 \cdot 1 \cdot 1 = 1$$

Assume the formula holds for $n-1$, thus:

$$\sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k} = (x+y)^{n-1}$$

Then:

$$\begin{aligned}
(x+y)^n &= (x+y)^{n-1} \cdot (x+y)s \\
&= \left(\sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k}\right) \cdot (x+y) \\
&= x \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k} + y \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{(n-1)-k} \\
&= \sum_{k=1}^{n} \binom{n-1}{k-1} x^k y^{n-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k=0}^{n} \left(\binom{n-1}{k-1} + \binom{n-1}{k}\right) x^k y^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}
\end{aligned}$$

□

**Problem 15**

Criticize the following "proof" showing that all cows are the same color.
It suffices to show that any herd of $n$ cows has the same color. If the herd has but one cow, then trivially all the cows in the herd have the same color. Now suppose that we have a herd of n cows and $n > 1$. Pick out a cow and remove it from the herd, leaving $n-1$ cows; by the induction hypothesis these cows all have the same color. Now put the cow back and remove another cow. (We can do so because $n > 1$.) The remaining $n-1$ again must all be the same color. Hence, the first cow selected and the second cow selected have the same color as those not selected, and so the entire herd of n cows has the same color.

**Solution**

The proof selects a different set of $n-1$ cows each time.

**Problem 16**

Prove the converse of Theorem 1.1; that is, prove that the Principle of Mathematical Induction implies the Well-ordering Princple. (This shows that these two principles are logically equivalent, and so from an axiomatic point of view it doesn't matter which we assume is an axiom for the natural numbers.)

*Proof.* Assume that the principle of mathematical induction holds. Let $G \subseteq \mathbb{N}$ be nonempty. For contradiction, suppose $G$ has no least element. Define $P(n)$ to be the statement: "Nothing $\leq n$ is in $G$."

If $1 \in G$, then 1 would be the least element of $G$, a contradiction. So $1 \notin G$ and $P(1)$ is true.

Assume $P(n)$ holds meaning no element of $G$ is $\leq n$. If $n+1 \in G$, then $n+1$ would be the least element of $G$, a contradiction. Therefore $n+1 \notin G$, and hence $P(n+1)$ holds.

By induction, $P(n)$ holds for all $n \in \mathbb{N}$. So no element of $\mathbb{N}$ is in $G$, so $G = \emptyset$, contradicting the assumption that $G$ is nonempty. □

# 4 Chapter 2: The Integers (Theory)

**Theorem 3** (Division Theorem for $\mathbb{Z}$)**.** *Let $a$, $b \in \mathbb{Z}$, with $a \neq 0$. Then there exist unique integers $q$ and $r$ (called the quotient and remainder respectively), with $0 \leq r \leq |a|$, such that $b = aq + r$.*

**Lemma 1.** *Suppose that $a$, $b$, $q$, $r$ are integers and $b = aq + r$. Then $\gcd(b, a) = \gcd(a, b)$.*

**Theorem 4.** *Euclid's Algorithm compute $\gcd(b, a)$.*

**Theorem 5** (The GCD Identity for Integers)**.** *Given integers $a$ and $b$ (not both zero), there exist $x$ and $y$ for which $\gcd(b, a) = ax + by$.*

**Corollary 1.** *The* gcd *of two integers (not both zero) is the least positive linear combination of them.*

**definition 1.** *An integer $p$ (other than $\pm 1$) is irreducible if whenver $p = ab$, then $a$ or $b$ is $\pm 1$.*

**Theorem 6.** *If $p$ is prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some $i$.*

**Theorem 7.** *An integer is prime if and only if it is irreducible.*

**Theorem 8** (Fundamental Theorem of Arithmetic)**.** *Every non-zero integer (other than $\pm 1$) is either irreducible or a product of irreducibles.*

**Theorem 9** (Unique Factorization Theorem for Integers)**.** *If an integer $x = a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_n$ where the $a_i$ and $b_j$ are all irreducible, then $n = m$ and $b_j$ may be rearranged so that $a_i = \pm b_i$, for $i = 1, 2, \ldots, n$.*

# 5 Chapter 2: The Integers (Problems)

**Problem 3**

Prove that the set of all linear combinations of $a$ and $b$ are precisely the multiple of $\gcd(a, b)$.

*Proof.* Let $a, b$ be integers such that $a \neq 0$ or $b \neq 0$. We know $ax + by = \gcd(a, b)$ for some $x, y \in \mathbb{Z}$. Let $t$ be an arbitrary integer. Then $t(ax + by) = t(\gcd(a, b))$. It follows that $a(tx) + b(ty) = t(\gcd(a, b))$ Showing that any integer multiple $t$ of the $\gcd(a, b)$ is equivalent to some linear combination of $a, b$.

Let $a$, $b$, $x$, and $y$ be arbitrary integers. Let $d = \gcd(a, b)$. It follows that $d \mid a$ and $d \mid b$. Then $a = dt$ for some $t \in \mathbb{Z}$ and $b = df$ for some $f \in \mathbb{Z}$. Then:

$$ax + by = dtx + dfy = d(tx + fy)$$

So any linear combination of $a$ and $b$ is a multiple of the $\gcd(a, b)$. □

**Problem 4**

Two numbers are said to be relatively prime if their gcd is 1. Prove $a, b$ relatively prime if and only if every integer can be written as a linear combination of $a$ and $b$.

*Proof.* $\rightarrow$ Suppose $a, b \in \mathbb{Z}$ are relatively prime. Let $d \in \mathbb{Z}$. Since $a, b$ are relatively prime $\gcd(a, b) = ax+by = 1$ where $x, y \in \mathbb{Z}$. Then $d(\gcd(a, b)) = d(ax+by) = a(dx)+b(dy) = d(1) = d$.

$\leftarrow$ Suppose every integer can be written as a linear combination of $a$ and $b$. In particular $1 = ax + by$ for some $x, y \in \mathbb{Z}$. Then $\gcd(a, b) = 1 = ax + by$ so $a$ and $b$ are relatively prime. $\square$

**Problem 5**

Prove Theorem 2.6. That is, use induction to prove that if the prime $p$ divides $a_1 a_2 \cdots a_n$, then $p$ divides $a_i$ for some $i$.

*Proof.* Suppose $p$ is prime.

Base case: If $p \mid a_1 a_2$ by definition of being prime $p \mid a_1$ or $p \mid a_2$.

Assume the Theorem holds for $n - 1$ so if $p \mid a_1 a_2 \cdots a_{n-1}$ then $p \mid a_i$ for some $i$. Now suppose $p \mid a_1 a_2 \cdots a_{n-1} a_n$. Let $c = a_1 a_2 \cdots a_{n-1}$, then $p \mid c \cdot a_n$. By definition of being prime $p \mid c$ by the induction hypothesis or $p \mid a_n$. $\square$

**Problem 6**

Suppose that $a$ and $b$ are positive integers. If $a + b$ is prime, prove that $\gcd(a, b) = 1$.

*Proof.* We've already proved $n$ is prime iff $n$ is irreducible. Suppose $a + b$ is prime and for contradiction $\gcd(a, b) = x > 1$. Since $a + b$ is prime it has no factors other than itself and 1. Since $\gcd(a, b) = x > 1$ then $x \mid a$ and $x \mid b$. Furthermore, $a = tx$ and $b = yx$ for some $t, y \in \mathbb{Z}$. Then $a + b = tx + yx = x(t + y)$ a contradiction since $a + b$ is prime. $\square$

**Problem 7**

(a) A natural number greater than 1 that is not prime is called composite. Show that for any $n$, there is a run of $n$ consecutive composite numbers. Hint: Think Factorial.
(b) Therefore, there is a string of 5 consecutive composite numbers starting where?

*Proof.* Let $T = \{2, 3, \ldots, n + 1\}$ and let $i$ be an element in $T$. Now let

$$d = i + (n + 1)!.$$

First notice $2 \leq i \leq n + 1$. Then:

$$((i + 1) + (n + 1)!) - (i + (n + 1)!) = 1$$

Showing consecutive values of $i$ produce consecutive values of $d$. Since $2 \leq i \leq n+1$, we have $i \mid (n+1)!$. Then:

$$\begin{aligned} d &= i + (n+1)! \\ &= i\left(1 + \frac{(n+1)!}{i}\right) \end{aligned}$$

Clearly $d$ is a composite number since it has been factored into 2 integers greater than 1. Thus, the $n$ values of $d$ produce a sequence of $n$ consecutive composite numbers. □

**Solution (b):**

$$722 = 2 \cdot 361, 723 = 3 \cdot 241, 724 = 2 \cdot 362, 725 = 5 \cdot 145, 726 = 2 \cdot 363$$

**Problem 9**

Notice that $\gcd(30, 50) = 5\gcd(6, 10) = 5 \cdot 2$. In fact, this is always true; prove that if $a > 0$, then $\gcd(ab, ac) = a \cdot \gcd(b, c)$.

*Proof.* Let $p = \gcd(ab, ac) = abx + acy$. Since $a \mid p$ there exists $r$ such that $p = ar$. So $ar = abx + acy$ and dividing by $a$ gives $r = bx + cy$. Since $a > 0$ and $ar = \gcd(ab, ac) > 0$ it follows that $r > 0$. Thus $r$ is a positive linear combination of $b$ and $c$. Suppose, for contradiction, there exists $d$ that is a positive linear combination of $b$ and $c$, and $d < r$. So $d = bu + cv$ for some integers $u, v$. Since $a > 0$ it follows that $ad > 0$. But then $ad = abu + acv$ and $ad < ar = p$ contrdicting the minimality of $p$. Therefore $r = \gcd(b, c)$. It follows that $\gcd(ab, ac) = ar = a \cdot \gcd(b, c)$. □

**Problem 10**

Suppose two integers $a$ and $b$ have been factored into primes as follows:

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

and

$$b = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

where the $p_i$'s are primes, and the exponents $m_i$ and $n_i$ are non-negative integers. It is the case that

$$\gcd(a, b) = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$$

where $s_i$ is the smaller of $n_i$ and $m_i$. Show this with $a = 360 = 2^3 \cdot 3^2 \cdot 5$ and $b = 2^2 3^2 5^2$. Now prove this fact in general.

**Solution:**

Let

$$a = 360 = 2^3 \cdot 3^2 \cdot 5^1, \quad b = 2^2 \cdot 3^2 \cdot 5^2.$$

**Exponents of each prime factor:**

| Prime $p_i$ | Exponent in $a$ ($n_i$) | Exponent in $b$ ($m_i$) |
|---|---|---|
| 2 | 3 | 2 |
| 3 | 2 | 2 |
| 5 | 1 | 2 |

**Minimum exponent for each prime:**

$$s_i = \min(n_i, m_i)$$

| Prime $p_i$ | $s_i = \min(n_i, m_i)$ |
|---|---|
| 2 | 2 |
| 3 | 2 |
| 5 | 1 |

**Multiply the primes raised to the minimum exponents:**

$$\gcd(a, b) = 2^2 \cdot 3^2 \cdot 5^1 = 4 \cdot 9 \cdot 5 = 180.$$

The gcd of 360 and 900 is 180.

*Proof.* Let $a = \prod_{i=1}^{r} p_i^{n_i}$ and $b = \prod_{i=1}^{r} p_i^{m_i}$. For each prime $p_i$, define $s_i = \min(n_i, m_i)$ and let $c_i = p_i^{s_i}$.

First note that the gcd will have the common prime factors of $a$ and $b$. A prime not common to both would not divide both.

Let $f_i = p_i^{s_i+1}$ for the $i$th prime number appearing in $a$ and $b$. Then $f_i > p_i^{m_i}$ or $f_i > p_i^{n_i}$ so $f_i \nmid p_i^{m_i}$ or $f_i \nmid p_i^{n_i}$. So $c_i$ is the largest power of $p_i$ dividing the $i$th prime of both numbers.

Since the primes are independent, the greatest common divisor of $a$ and $b$ is $\gcd(a, b) = \prod_{i=1}^{r} c_i = \prod_{i=1}^{r} p_i^{s_i}$. □

Problem 11

The **least common multiple** of natural numbers $a$ and $b$ is the smallest positive common multiple of $a$ and $b$. That is, if $m$ is the least common mulitple of $a$ and $b$, then $a \mid m$ and $b \mid m$, and if $a \mid n$ and $b \mid n$ then $n \geq m$. We will write $lcm(a, b)$ for the least common mulitple of $a$ and $b$. Can you find a formula for the lcm of the type given for the gcd in the previous excersize.

**Solution**

Suppose two integers $a$ and $b$ have been factored into primes as follows:

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

and

$$b = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

where the $p_i$'s are primes, and the exponents $m_i$ and $n_i$ are non-negative integers. It is the case that

$$lcm(a, b) = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$$

where $s_i$ is the larger of $n_i$ and $m_i$.

Problem 12

Show that if $\gcd(a,b) = 1$, then $lcm(a,b) = ab$.
In general, show that:

$$lcm(a,b) = \frac{ab}{\gcd(a,b)}$$

*Proof.* We prove the general case first.

Let $a = \prod_{i=1}^{r} p_i^{n_i}$ and $b = \prod_{i=1}^{r} p_i^{m_i}$. So

$$ab = \prod_{i=1}^{r} p_i^{n_i+m_i}.$$

Now inspecting the $i$th prime in $ab$ we get $p_i^{n_i+m_i}$. Then looking at the gcd's $i$th prime we get $p_i^{\min\{n_i,m_i\}}$. Suppose wlog that $n_i \geq m_i$. Then

$$\frac{p_i^{n_i+m_i}}{p_i^{\min\{n_i,m_i\}}} = \frac{p_i^{n_i+m_i}}{p_i^{m_i}} = p_i^{n_i+m_i-m_i} = p_i^{n_i} = p_i^{\max\{n_i,m_i\}}.$$

This is the $i$th prime factor of the $lcm$. □

*Proof.* Suppose that for each prime $p_i$, $p_i$ divides $a$ or $b$ but not both. Then for the $i$th prime factor $p_i$, either $n_i = 0$ or $m_i = 0$. Then:

$$\frac{p_i^{n_i+m_i}}{p_i^{\min\{n_i,m_i\}}} = \frac{p_i^{n_i+m_i}}{p_i^{0}} = p_i^{n_i+m_i-0} = p_i^{n_i+m_i} = p_i^{\max\{n_i,m_i\}}.$$

□

Problem 13

Prove that if $m$ is a common multiple of both $a$ and $b$, then $lcm(a,b) \mid m$.

*Proof.* Suppose $m$ is a common multiple of both $a$ and $b$. Then there exist integers $l$ and $f$ such that $m = la$ and $m = fb$. Let the $i$th prime factor of $a, b, l, f$ be $p_i^{n_i}$, $p_i^{m_i}$, $p_i^{t_i}$, $p_i^{s_i}$ respectively. Then the $i$th prime factor of $m$ is

$$m = la = p_i^{n_i+t_i}, \quad m = fb = p_i^{m_i+s_i}.$$

Let the $i$th prime factor of $\operatorname{lcm}(a,b)$ be $p_i^{\max\{n_i,m_i\}}$. Then, in either case, we have

$$n_i + t_i = m_i + s_i \geq \max\{n_i, m_i\}.$$

So each $p_i^{\max\{n_i,m_i\}}$ divides the corresponding prime factor of $m$. □

Problem 18

(a) Show that in Euclid's Algorithm, the remainders are at least halved after two steps. That is $r_{i+2} < 1/2 r_i$.

(b) Use part a to find the maximum number of steps required for Euclid's algorithm. (Figure this in terms of the maximum of $a$ and $b$).

*Proof.* Theorem 2.3 shows that the remainders form a strictly decreasing sequence of integers. Three steps of the algorithm are shown below.

$$\begin{aligned} \text{step 1: } b_{n-2} &= a_{n-2} \cdot q_{n-2} + r_{n-2} \\ \text{step 2: } b_{n-1} &= a_{n-1} \cdot q_{n-1} + r_{n-1} \\ \text{step 3: } b_n &= a_n \cdot q_n + r_n \end{aligned}$$

Now for the $i$th iteration $b_i = a_{i-1}$ and $a_i = r_{i-1}$. Then:

$$\begin{aligned} \text{step 1: } b_{n-2} &= a_{n-2} \cdot q_{n-2} + r_{n-2} \\ \text{step 2: } a_{n-2} &= r_{n-2} \cdot q_{n-1} + r_{n-1} \\ \text{step 3: } r_{n-2} &= r_{n-1} \cdot q_n + r_n \end{aligned}$$

Notice, in step 3, a larger $q_n$ implies a smaller $r_n$. So in the worst case $q_n = 1$. So $r_{n-2} = r_{n-1} + r_n \iff r_n = r_{n-2} - r_{n-1}$. Now since $r_n < r_{n-1}$ then $r_{n-2} - r_{n-1} < r_{n-1} \iff r_{n-2} < 2r_{n-1}$. So $\frac{1}{2} r_{n-2} < r_{n-1}$. Now since $r_n < r_{n-2} - r_{n-1}$ then $r_n < r_{n-2} - \frac{1}{2} r_{n-2} = \frac{1}{2} r_{n-2}$. □

**Solution 18 (b):**

Let $c = \max\{a, b\}$. From part (a), we know that after every two steps, the remainder is at most half of the remainder two steps before:

$$r_{i+2} < \frac{1}{2} r_i$$

Let $k$ be the number of "two-step pairs" needed for the remainder to drop below 1. Then

$$\frac{c}{2^k} < 1 \implies 2^k > c \implies k > \log_2 c$$

Since each $k$ corresponds to two iterations, the maximum number of iterations of Euclid's algorithm is

$$\text{max steps} \leq 2k \leq 2 \log_2 c$$

Problem 19

Recall from Excersize 1.13 the definition of the binomial coefficient $\binom{n}{k}$. Suppose that $p$ is a positive prime integer, and $k$ is an integer with $1 \leq k \leq p-1$. Prove that $p$ divides binomial coefficient $\binom{p}{k}$.

*Proof.* By Exercise 1.13, we know that $\binom{p}{k} \in \mathbb{Z}$. Using the factorial definition:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1)!}{k \cdot (k-1)!(p-k)!} = \frac{p}{k}\binom{p-1}{k-1}.$$

Since $p$ is prime and $1 \leq k \leq p-1$, we have $\gcd(p,k) = 1$, so $k$ divides $\binom{p-1}{k-1}$. Therefore, $p$ divides $\binom{p}{k}$. □

# 6 Chapter 3: Modular Arithmetic (Theory)

**definition 2.** *For any positive integer $m$ and integer $a$, the residue of $a$ modulo $m$ is the remainder one obtains when dividing $a$ by $m$ in the Division Theorem.*

**definition 3.** *Given an integer $a$, the set of all integers with the same residue (mod $m$) as $a$ is called the residue class (mod $m$) of $a$ and denoted $[a]_m$.*

**definition 4.** *If $[a]_m = [b]_m$ we say that $a$ and $b$ are congruent modulo $m$, and write $a \equiv b (mod\ n)$.*

**Theorem 10.**

$$[a]_m = \{a + km : k \in \mathbb{Z}\}$$

**Theorem 11.** *Two integers $x$ and $y$, have teh same residue (mod $m$) if and only if $x - y = km$ for some integer $k$.*

**definition 5.**

$$[a]_m + [b]_m = [a+b]_m$$
$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

# 7 Chapter 3: Modular Arithmetic (Problems)

**Problem 2**

Determine the elements of $\mathbb{Z}_{15}$ that have multiplicative inverses. Give an example of an equation of the form $[a]X = [b]$ ($[a] \neq 0$) that has no solution in $\mathbb{Z}_{15}$.

**Solution**

| | [0] | [1] | [2] | [3] | [4] | [5] | [6] | [7] | [8] | [9] | [10] | [11] | [12] | [13] | [14] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [0] | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| [1] | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| [2] | 0 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 1 | 3 | 5 | 7 | 9 | 11 | 13 |
| [3] | 0 | 3 | 6 | 9 | 12 | 0 | 3 | 6 | 9 | 12 | 0 | 3 | 6 | 9 | 12 |
| [4] | 0 | 4 | 8 | 12 | 1 | 5 | 9 | 13 | 2 | 6 | 10 | 14 | 3 | 7 | 11 |
| [5] | 0 | 5 | 10 | 0 | 5 | 10 | 0 | 5 | 10 | 0 | 5 | 10 | 0 | 5 | 10 |
| [6] | 0 | 6 | 12 | 3 | 9 | 0 | 6 | 12 | 3 | 9 | 0 | 6 | 12 | 3 | 9 |
| [7] | 0 | 7 | 14 | 6 | 13 | 5 | 12 | 4 | 11 | 3 | 10 | 2 | 9 | 1 | 8 |
| [8] | 0 | 8 | 1 | 9 | 2 | 10 | 3 | 11 | 4 | 12 | 5 | 13 | 6 | 14 | 7 |
| [9] | 0 | 9 | 3 | 12 | 6 | 0 | 9 | 3 | 12 | 6 | 0 | 9 | 3 | 12 | 6 |
| [10] | 0 | 10 | 5 | 0 | 10 | 5 | 0 | 10 | 5 | 0 | 10 | 5 | 0 | 10 | 5 |
| [11] | 0 | 11 | 7 | 3 | 14 | 10 | 6 | 2 | 13 | 9 | 5 | 1 | 12 | 8 | 4 |
| [12] | 0 | 12 | 9 | 6 | 3 | 0 | 12 | 9 | 6 | 3 | 0 | 12 | 9 | 6 | 3 |
| [13] | 0 | 13 | 11 | 9 | 7 | 5 | 3 | 1 | 14 | 12 | 10 | 8 | 6 | 4 | 2 |
| [14] | 0 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Elements with multiplicative inverses are [1],[2],[4],[7],[8],[11],[13], and [14].

Example of an equation of the form $[a]X = [b]$ ($[a] \neq 0$) that has no solution.

$$[3]X = [5]$$

**Problem 4**

Find an example in $\mathbb{Z}_6$ where $[a][b] = [a][c]$, but $[b] \neq [c]$. How is this related to the existence of multiplicative inverses in $\mathbb{Z}_6$?

Example where $[a][b] = [a][c]$, but $[b] \neq [c]$:

$$[2][2] = [2][5] = [4]$$

You cannot assume that if $[a][b] = [a][c]$ then $[b] = [c]$. This is only true if $[a]$ has a multiplicative inverse.

**Problem 5**

If $\gcd(a, b) = 1$ then the GCD identity 2.4 garuntees that there exists integers $u$ and $v$ such that $1 = au + mv$. Show that in this case, $[u]_m$ is the multiplicate inverse of $[a]_m$ in $\mathbb{Z}_m$.

*Proof.* By Theorem 3.2 if $x - y = km$ for some integer $k$ then $x$,$y$ are in the same residue (mod $m$). Now $1 = au + mv \iff au = -mv + 1$. Then $x - y = (-mv + 1) - 1 = (-v)m$. Thus $[au]_m = [1]_m$ and therefore $[a]_m \cdot [u]_m = [1]$. □

**Problem 6**

Now use essentially the reverse of the argument from Excersize 5 to show that if $[a]$ has a multiplicative inverse in $\mathbb{Z}_m$, then $\gcd(a, m) = 1$.

*Proof.* Suppose $[a]_m$ has a multiplicative inverse $[b]_m$ in $\mathbb{Z}_m$. Then $[a] \cdot [b] = [ab] = [1]$. By Theorem 3.2, $ab - 1 = km$. But $ab - km = 1$ so $ab + m(-k) = 1$. Therefore $\gcd(a, m) = 1$. □

**Problem 7**

According to what you have shown in Excersize 5 and 6, which elements of $\mathbb{Z}_{24}$ have multiplicative inverses? What are the inverses for each of those elements? (The answer is somewhat suprising.)

**Solution:**

The following have multiplicate inverses in $\mathbb{Z}_{24}$.

1. $[1]_{24}$
2. $[5]_{24}$
3. $[7]_{24}$
4. $[11]_{24}$
5. $[13]_{24}$
6. $[17]_{24}$
7. $[19]_{24}$
8. $[23]_{24}$

Problem 9

Prove that the multiplication on $\mathbb{Z}_m$ as defined in the text is well defined, as claimed in Section 3.2.

*Proof.* Consider $[a]$ and $[b]$. Let $x, y$ be elements in $[a]$ and $b, c$ be elements in $[b]$. We need to show $[xb] = [yc]$. But $x, y \in [a]$ implies $x - y = k_1 m$ for some integer $k_1$. Also $b, c \in [b]$ implies $b - c = k_2 m$ for some integer $k_2$. Then:

$$\begin{aligned} & xb - yc \\ =&(k_1 m + y)(k_2 m + c) - yc \\ =&k_1 k_2 m^2 + k_1 mc + k_2 my + yc - yc \\ =&k_1 k_2 m^2 + k_1 mc + k_2 my \\ =&m(k_1 k_2 m + k_1 c + k_2 y) \end{aligned}$$

Showing that $[xb] = [yc]$ □

Problem 10

Prove that if all non-zero $\mathbb{Z}_m$ have multiplicative inverses, then multiplicative cancellation holds: that is, if $[a][b] = [a][c]$, then $[b] = [c]$.

*Proof.* Suppose all non-zero $\mathbb{Z}_m$ have multiplicative inverses. Let $[t]$ be the multiplicative inverse of $[a]$. Then $[a][b] = [a][c] \iff [t][a][b] = [t][a][c] \iff [b] = [c]$. □

Problem 13

In the integers, the equation $x^2 = a$ has a solution only when $a$ is a positive perfect square or zero. For which $[a]$ does the equation $[X]^2 = [a]$ have a solution in $\mathbb{Z}_7$? What about in $\mathbb{Z}_8$? What about in $\mathbb{Z}_9$?

**Solution:**

Elements with square roots in $\mathbb{Z}_7$:

$$[0], [1], [2], [4]$$

Elements with square roots in $\mathbb{Z}_8$:

$$[0], [1], [4]$$

Elements with square roots in $\mathbb{Z}_9$:

$$[0], [1], [4], [7]$$

Problem 14

Explain what $a \equiv b (mod\ 1)$ means.

**Solution:**

It means when elements in $[a]$ and $[b]$ are divided by 1 the remainder is equivalent. Of course this is true for any $a$ and $b$ since $\frac{a}{1} = a$ and $\frac{b}{1} = b$. So $[a] = [b] = \mathbb{Z}$.

# 8 Chapter 4: Polynomials with Rational Coefficients (Theory)

**definition 6.** *A polynomial $f \in \mathbb{Q}[x]$ is an expression of the form*

$$f = a_0 + a_1 x + a_x x^2 + \cdots + a_n x^n + \cdots$$

*where $a_i \in \mathbb{Q}$ and all but finitely many of the $a_i$'s are 0.*

**definition 7.** *We call the $a_i$'s in the previous definition coefficients of the polynomial.*

**definition 8.** *Two polynomials are equal if and only if their corresponding coefficients are equal.*

**definition 9.** *The degree of a polynomial is the largest exponent with corresponding non-zero coefficient.*

**Theorem 12.** *Let $f, g \in \mathbb{Q}[x]$. Then*

*(a) $deg(fg) = deg(f) + deg(g)$, where it is understood that $-\infty$ added to anything is $-\infty$.*

*(b) $deg(f + g)$ is less than or equal to the larger of the degrees of $f$ and $g$.*

# 9 Chapter 4: Polynomials with Rational Coefficients (Problems)

**Problem 2**

Divide the polynomial $x^2 - 3x + 2$ by the polynomial $2x + 1$, to obtain a quotient and remainder as garunteed by the Division Theorem 4.2. Note that although $x^2 - 3x + 2$ and $2x + 1$ are elements of $\mathbb{Z}[x]$, the quotient and remainder are not. Argue that this means that there is not Division Theorem for $\mathbb{Z}[x]$.

**Problem 3**

By Corollary 4.4 we know that a third-degree polynomial in $\mathbb{Q}[x]$ has at most three roots. Give four examples of third-degree polynomials in $\mathbb{Q}[x]$ that have 0, 1, 2, and 3 roots, respectively; justify your assertions. (Recall that here a root must be a rational number!)

**Problem 4**

Your example in the previous excersize of a third-degree polynomial with exactly 2 roots had one repeated root; that is, a root $a$ where $(x-a)^2$ is a factor of the polynomial. (Roots may have multiplicity greater than two of course.) Why can't a third-degree polynomial in $\mathbb{Q}[x]$ have exactly 2 roots where neither is a multiple root.

**Problem 6**

Suppose that $f \in \mathbb{Q}[x]$, $q \in \mathbb{Q}$, and $deg(f) > 0$. Use the Root Theorem 4.3 to prove that the equation $f(x) = q$ has at most finitely many solutions.

**Problem 8**

Prove that Theorem 4.7: the GCD identity for $\mathbb{Q}[x]$. Use Euclid's Algorithm 4.5, and the relationship we know between the gcd produced by the algorithm and an arbitrary gcd (Theorem 4.6).

**Problem 9**

One can also prove the GCD identity for $\mathbb{Q}[x]$ with an argument similar to the existential proof of the GCD identity for integers, found in Section 2.3. Try this approach.

**Problem 10**

We say that $p \in \mathbb{Q}[x]$ has a multiplicative inverse if there exists $q \in \mathbb{Q}[x]$ such that $pq = 1$. Prove that $p \in \mathbb{Q}[x]$ has a multiplicative inverse if and only if $deg(p) = 0$.

**Problem 11**

Suppose that $g \in \mathbb{Q}[x]$, and $g$ divides all elements of $[Q][x]$. Prove that $g$ is a non-zero constant polynomial.

**Problem 12**

Find two different polynomials in $\mathbb{Z}_3[x]$ that are equal as functions from $\mathbb{Z}_3 = \mathbb{Z}_3$.

**Problem 13**

Find a non-zero polynomial in $\mathbb{Z}_4[x]$ for which $f(a) = 0$, for all $a \in \mathbb{Z}_4$.