Introduction to Abstract Mathematics

Benjamin Howard
Robert Gross

Notation:

- $\mathbb{Z}^+$ or $\mathbb{Z}^{>0}$ denotes the set $\{1, 2, 3, \ldots\}$ of positive integers,
- $\mathbb{Z}^{\geq 0}$ is the set $\{0, 1, 2, \ldots\}$ of nonnegative integers,
- $\mathbb{Z}$ is the set $\{\ldots, -1, 0, 1, 2, \ldots\}$ of integers,
- $\mathbb{Q}$ is the set $\{a/b : a \in \mathbb{Z}, b \in \mathbb{Z}^+\}$ of rational numbers,
- $\mathbb{R}$ is the set of real numbers,
- $\mathbb{C}$ is the set $\{x + iy : x, y \in \mathbb{R}\}$ of complex numbers,
- $Y \subset X$ means that Y is a subset of X,
- $x \in X$ means that x is an element of the set X,
- $|X|$ denotes the cardinality of a set X,
- if A and B are sets then
$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$$
is the Cartesian product of A and B.

Contents

CHAPTER I

Mathematical Induction

1. The irrationality of $\sqrt{2}$

Theorem 1.1 (Pythagoras)**.** *There is no $x \in \mathbb{Q}$ satisfying $x^2 = 2$.*

Proof. To get a contradiction, assume there is an $x \in \mathbb{Q}$ such that $x^2 = 2$. If we write $x = a/b$ as a quotient of two integers $a, b \in \mathbb{Z}$ with $b > 0$, then

$$x^2 = 2 \implies (a/b)^2 = 2 \implies a^2 = 2b^2.$$

Now stare at the last equality

$$a^2 = 2b^2 \tag{1.1}$$

and consider how many times the prime 2 appears in the prime factorization of each side. For any nonzero integer m, the prime 2 appears in the prime factorization of m^2 twice as many times as it appears in the prime factorization of m itself. In particular for any nonzero m the prime 2 appears in the prime factorization of m^2 an *even* number of times. Thus the prime factorization of the left hand side of (1.1) has an even number of 2's in it. What about the right-hand side? The prime factorization of b^2 has an even number of 2's in it, and so the prime factorization of the right hand side of (1.1) has an odd number of 2's. This is a contradiction, and so no such x can exist. □

It's worth pausing to remark on a property of positive integers used in the proof. When we talk about "how many times the prime 2 appears in the prime factorization" of a number we are using the fact that every positive integer can be factored in a unique way as a product of primes. This is true, but at the moment we have done nothing to justify this assertion. This deficiency will be addressed later, in Theorem 5.3.

Exercise 1.2. Prove there is no $x \in \mathbb{Q}$ satisfying $x^3 = 5$.

Exercise 1.3. Prove there is no $x \in \mathbb{Q}$ satisfying $x^2 = 15$.

Exercise 1.4. Suppose $m \in \mathbb{Z}^+$ is not a perfect square. Show that $\sqrt{m}$ is irrational.

2. The Principle of Induction

Axiom 2.1 (Well-Ordering Property of $\mathbb{Z}^+$)**.** *Every nonempty subset of $\mathbb{Z}^+$ has a smallest element.*

Theorem 2.2 (Principle of Induction)**.** *Suppose*

$$P(1), P(2), P(3), \ldots$$

is a sequence of statements with the following properties:

(*a*) *$P(1)$ is true,*
(*b*) *for every $k \in \mathbb{Z}^+$, $P(k) \implies P(k+1)$.*

Then, $P(n)$ is true for every $n \in \mathbb{Z}^+$.

Proof. We must show that $P(n)$ is true for every $n \in \mathbb{Z}^+$. To get a contradiction, suppose not. Then there is some $m \in \mathbb{Z}^+$ such that the statement $P(m)$ is false. Consider the set

$$S = \{n \in \mathbb{Z}^+ : P(n) \text{ is false}\}.$$

We know that $P(m)$ is false, and so $m \in S$. In particular $S \neq \emptyset$. By the Well-Ordering Property of $\mathbb{Z}^+$, the set S contains a smallest element, which we will call m_0. We know that $P(1)$ is true, and so $1 \notin S$. In particular $m_0 \neq 1$, and so $m_0 > 1$. Thus $m_0 - 1 \in \mathbb{Z}^+$ and it makes sense to consider the statement $P(m_0 - 1)$. As $m_0 - 1 < m_0$ and m_0 is the *smallest* element of S, $m_0 - 1 \notin S$. Of course this implies that $P(m_0 - 1)$ is true. Now taking $k = m_0 - 1$ in the implication $P(k) \implies P(k+1)$ we deduce that $P(m_0)$ is true, and so $m_0 \notin S$. But m_0 was defined to be the smallest element of S, and in particular $m_0 \in S$. This contradiction completes the proof. □

Theorem 2.3. *For every $n \in \mathbb{Z}^+$*

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof. Let $P(n)$ be the statement that we want to prove:

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

First, consider the case $n = 1$. The statement $P(1)$ asserts

$$1 = \frac{1(1+1)}{2},$$

and this is obviously true. Next we assume that $P(k)$ is true for some $k \in \mathbb{Z}^+$ and try to deduce that $P(k+1)$ is true. So, suppose that $P(k)$ is true. This means that

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

and adding $k+1$ to both sides and simplifying results in

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

Comparing the first and last expressions in this sequence of equalities, we find that $P(k+1)$ is also true. We have now proved that $P(k) \implies P(k+1)$, and so by induction $P(n)$ is true for all $n \in \mathbb{Z}^+$. □

Proposition 2.4. *If $n \in \mathbb{Z}^+$ and $x \neq 1$, then*

$$1 + x + x^2 + x^3 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

Definition 2.5. Define the *Fibonacci numbers* $f_1, f_2, f_3, \ldots$ by the recursion relations $f_1 = 1$, $f_2 = 1$, and

$$f_n = f_{n-1} + f_{n-2}$$

whenever $n > 2$ (so the Fibonacci numbers are $1, 1, 2, 3, 5, 8, 13, 21, \ldots$).

Proposition 2.6. *For every $n \in \mathbb{Z}^+$*

$$f_1 + f_3 + f_5 + \cdots + f_{2n-1} = f_{2n}.$$

The principle of induction can be slightly generalized. The following proposition shows that there's no reason you have to start the induction at the statement $P(1)$. If you can prove that $P(n_0)$ is true and that $P(k) \implies P(k+1)$ for all $k \geq n_0$, then $P(n_0), P(n_0+1), \ldots$ are all true.

Theorem 2.7. *Fix an integer $n_0 \in \mathbb{Z}$ and suppose we are given statements*

$$P(n_0), P(n_0+1), P(n_0+2), \ldots$$

satisfying

(a) *$P(n_0)$ is true,*

(b) *for every $k \geq n_0$, $P(k) \implies P(k+1)$.*

Then $P(n)$ is true for every $n \geq n_0$.

Proof. Define a new sequence of statements $Q(1), Q(2), \ldots$ by

$$\begin{aligned} Q(1) &= P(n_0) \\ Q(2) &= P(n_0+1) \\ &\vdots \\ Q(k) &= P(n_0+k-1) \\ &\vdots \end{aligned}$$

We will now use induction to prove that $Q(1), Q(2), \ldots$ are all true. Recall that we are assuming that $P(n_0)$ is true, and therefore $Q(1)$ is true. Now assume that $Q(k)$ is true for some k. Then of course $P(n_0+k-1)$ is also true. But $P(n_0+k-1) \implies P(n_0+k)$, and $P(n_0+k) = Q(k+1)$. Therefore $Q(k+1)$ is true. By induction the statements $Q(1), Q(2), \ldots$ are all true, and therefore $P(n_0), P(n_0+1), \ldots$ are also all true. □

Exercise 2.8. Use induction to prove that $n < 2^n$ for every $n \in \mathbb{Z}^+$.

Exercise 2.9. Prove the following statement: for every $n \in \mathbb{Z}^+$ the integer

$$10^{n+2} - 2 \cdot 10^n + 7$$

is divisible by 3.

Exercise 2.10. Prove that

$$\sum_{i=1}^{n} i^2 = \frac{n(2n+1)(n+1)}{6}$$

for every $n \in \mathbb{Z}^+$.

Exercise 2.11. Prove that

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$$

for every $n \in \mathbb{Z}^+$.

Exercise 2.12. Suppose that n is a positive integer. Prove that

$$\sum_{k=1}^{2n} (-1)^k k = n.$$

Exercise 2.13. Prove that $3^{4n} - 1$ is divisible by 5 for all $n \in \mathbb{Z}^+$.

Exercise 2.14. Prove that $2^{2n+1} + 1$ is divisible by 3 for every $n \in \mathbb{Z}^+$.

Exercise 2.15. Prove that

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

for every $n \in \mathbb{Z}^+$.

Exercise 2.16. Prove that

$$1 + 3 + 5 + \cdots + (2n-1) = n^2$$

for every $n \in \mathbb{Z}^+$.

Exercise 2.17. Prove that for every $n \in \mathbb{Z}^+$

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

Exercise 2.18.

(a) Prove that $2^n < n!$ for all integers $n \geq 4$.
(b) Prove that $3^n < n!$ for all integers $n \geq 7$.

Exercise 2.19. Prove $5 \cdot 2^n \leq 3^n$ for all integers $n \geq 4$.

Exercise 2.20. Let n be a positive integer. Show that the Fibonacci numbers satisfy

$$\sum_{k=1}^{n} f_k = f_{n+2} - 1.$$

Exercise 2.21. Let n be a positive integer. Show that

$$\sum_{k=1}^{n} f_k^2 = f_n f_{n+1}.$$

Exercise 2.22. Prove that $f_n f_{n+1} - f_{n-1} f_{n+2} = (-1)^{n+1}$ if $n \geq 2$.

Exercise 2.23. Define the *harmonic numbers* H_n by the formula

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}.$$

Prove that

$$\sum_{k=1}^{n-1} H_k = nH_n - n.$$

Exercise 2.24. Prove that

$$\sum_{k=1}^{n} kH_k = \frac{n(n+1)H_n}{2} - \frac{n(n-1)}{4}.$$

Exercise 2.25. Let n be a positive integer. Using l'Hôpital's rule and induction, prove that

$$\lim_{x\to\infty} \frac{x^n}{e^x} = 0.$$

You may assume that the formula is true when $n = 0$.

Exercise 2.26. Define the *gamma function* by the formula

$$\Gamma(n) = \int_0^\infty x^{n-1}e^{-x}\,dx.$$

You may assume without proof that the integral converges if n is a positive integer.

(a) Use integration by parts and the previous exercise to prove $\Gamma(n+1) = n\Gamma(n)$ for all $n \in \mathbb{Z}^+$.

(b) Now use induction to prove that $\Gamma(n+1) = n!$ for all $n \in \mathbb{Z}^+$.

Exercise 2.27. Find a value of N such that $2n^2 < 2^n$ for all $n \geq N$.

Exercise 2.28. Suppose that n is a positive integer. Prove using induction and l'Hôpital's Rule that

$$\lim_{x\to 0} x(\log x)^n = 0,$$

where $\log x$ is the natural logarithm of x.

Exercise 2.29. Suppose that n is a positive integer. Prove using induction and integration by parts that

$$\int_0^1 (1-x^2)^n\,dx = \frac{2^{2n}(n!)^2}{(2n+1)!}.$$

Exercise 2.30. Let n be a positive integer. Prove using induction that $\dfrac{(2n)!}{2^n n!}$ is always an integer.

Exercise 2.31. Let n be a positive integer, and α any nonnegative real number. Prove by induction that

$$(1+\alpha)^n \geq 1 + n\alpha + \frac{n(n-1)}{2}\alpha^2.$$

Be sure in your proof to indicate where you used the fact that $\alpha \geq 0$, because the result is false if α is negative.

Exercise 2.32. Suppose that n is a positive integer. Prove that $n^3 + 2n$ is a multiple of 3.

Exercise 2.33. Define a sequence of real numbers by $x_1 = 1$, and

$$x_n = \sqrt{x_{n-1} + 1}$$

for all $n > 1$. Prove that $x_n \leq x_{n+1}$ for all $n \in \mathbb{Z}^+$.

Exercise 2.34. If n is any nonnegative integer, write $g_n = 2^{2^n} + 1$. Prove using induction that

$$g_0 g_1 g_2 \cdots g_{n-1} = g_n - 2.$$

The numbers g_n were first studied by the mathematician Pierre de Fermat, who conjectured that they are always prime. If your calculator is sufficiently good, you can verify that g_5 in fact is not prime. When you consider that $g_5 = 4294967297$, it's hard to blame Fermat for being unable to notice that it is not prime.

Exercise 2.35. Let n be a nonnegative integer, and a any positive real number. Prove that

$$\int_0^1 x^a (\log x)^n \, dx = \frac{(-1)^n n!}{(a+1)^{n+1}}.$$

3. The Principle of Strong Induction

Theorem 3.1 (Principle of Strong Induction)**.** *Suppose $P(1), P(2), P(3), \dots$ is a sequence of statements with the following properties:*

(a) *$P(1)$ is true,*

(b) *for every $k \in \mathbb{Z}^+$, if $P(1), P(2), \dots, P(k)$ are all true then $P(k+1)$ is also true.*

Then $P(n)$ is true for every $n \in \mathbb{Z}^+$.

First proof of strong induction. The first proof of strong induction mimics the proof of weak induction. We must show that $P(n)$ is true for every $n \in \mathbb{Z}^+$. To get a contradiction, suppose not. Then there is some $m \in \mathbb{Z}^+$ such that the statement $P(m)$ is false. Consider the set

$$S = \{n \in \mathbb{Z}^+ : P(n) \text{ is false}\}.$$

We know that $P(m)$ is false, and so $m \in S$. In particular $S \neq \emptyset$. By the Well-Ordering Property of $\mathbb{Z}^+$, the set S contains a smallest element, which we will call m_0. Of course $1, 2, \dots, m_0 - 1 \notin S$, which implies that $P(1), P(2), \dots, P(m_0 - 1)$ are all true.

By hypothesis $P(1)$ is true, and so $1 \notin S$. In particular $m_0 \neq 1$. Therefore $m_0 > 1$ and we may take $k = m_0 - 1$ to see that

$$P(1), P(2), \dots, P(m_0 - 1) \text{ all true} \implies P(m_0) \text{ is true.}$$

Therefore $m_0 \notin S$. We now have that m_0 is both in S and not in S, a contradiction. □

Second proof of strong induction. The second proof of strong induction is a bit sneaky. We will use the weak form of induction to prove the strong form of induction. Here is the trick: for each $n \in \mathbb{Z}^+$ let $Q(n)$ be the statement

$$\text{“}P(1), P(2), \dots, P(n) \text{ are all true.”}$$

We will now use weak induction to prove that $Q(1), Q(2), \dots$ are all true. Recall we are *assuming* that $P(1)$ is true. As the statement $Q(1)$ asserts “$P(1)$ is true,” $Q(1)$ is also true. Now suppose that $Q(k)$ is true for some $k \in \mathbb{Z}^+$. Then $P(1), \dots, P(k)$ are all true, and so by hypothesis $P(k+1)$ is also true. Therefore $P(1), P(2), \dots, P(k+1)$ are all true, which means precisely that $Q(k+1)$ is true. We have now proved that $Q(k) \implies Q(k+1)$, and hence by weak induction $Q(1), Q(2), \dots$ are all true. But certainly if $Q(n)$ is true then $P(n)$ is true, and so $P(1), P(2), \dots$ are also all true. □

Definition 3.2. Suppose $n \in \mathbb{Z}^+$ with $n > 1$.

(a) We say that n is *composite* if there exist $a, b \in \mathbb{Z}^+$ such that $1 < a, b < n$ and $n = ab$.

(b) We say that n is *prime* if whenever $n = ab$ with $a, b \in \mathbb{Z}^+$, either $a = 1$ or $b = 1$.

By convention 1 is neither prime nor composite.

Theorem 3.3. *Suppose $n \in \mathbb{Z}^+$. There exist prime numbers $p_1, \dots, p_s$ such that $n = p_1 \cdots p_s$. In words: every positive integer can be factored as a product of primes.*

Proof. We will use the strong form of induction. Let $P(n)$ be the following statement: there exist prime numbers $p_1, \dots, p_s$ such that $n = p_1 \cdots p_s$. The statement $P(1)$ asserts that 1 can be written as a product of prime numbers. This is true for a reason that is either subtle or trivial: the number 1 is the *empty product* of prime numbers. If you multiply together no prime numbers at all (so take $s = 0$) the result is 1. Therefore $P(1)$ is true.

Now assume that we have some $k \in \mathbb{Z}^+$ for which $P(1), P(2), \dots, P(k)$ are all true. In other words we assume that $1, 2, 3, 4, \dots, k$ can all be factored as a product of primes.We must show that $P(k+1)$ is also true, that is, that $k+1$ can be factored as a product of primes.

Case 1: Assume that $k+1$ is prime. Then $k+1$ is certainly a product of prime numbers, so $P(k+1)$ is true.

Case 2: Assume that $k+1$ is composite. Then there are $a, b \in \mathbb{Z}^+$ such that $k+1 = ab$ and $a, b < k+1$. The induction hypothesis tells us that a and b can each be factored as a product of primes, and so there are prime numbers $p_1, \dots, p_s$ such that $a = p_1 \cdots p_s$, and prime numbers $q_1, \dots, q_t$ such that $b = q_1 \cdots q_t$. But this implies that

$$k + 1 = ab = p_1 \cdots p_s \cdot q_1 \cdots q_t$$

is also a product of prime numbers, and so $P(k+1)$ is also true.

By strong induction, we are done. □

Proposition 3.4. *The n^{th} Fibonacci number f_n satisfies $f_n \leq 2^n$.*

Proof. The proof is by strong induction. Let $P(n)$ be the statement $f_n \leq 2^n$. As $f_1 = 1$, clearly $P(1)$ is true. Now assume that we have some $k \in \mathbb{Z}^+$ such that $P(1), \dots, P(k)$ are *all* true. We must prove that $P(k+1)$ is also true. So, we are assuming *all* of the inequalities

$$\begin{aligned} f_1 &\leq 2^1 \\ f_2 &\leq 2^2 \\ &\vdots \\ f_{k-1} &\leq 2^{k-1} \\ f_k &\leq 2^k \end{aligned}$$

and must use these to deduce

$$f_{k+1} \leq 2^{k+1}. \tag{3.1}$$

Case 1: First suppose that $k > 1$. In this case we may use the equality

$$f_{k+1} = f_k + f_{k-1}$$

(this equality does not hold for $k = 1$, as the Fibonacci number f_0 is not even defined). Combining this with the final two inequalities in the list above we see that

$$f_{k+1} = f_k + f_{k-1}$$

$$\begin{aligned} &\le 2^k + 2^{k-1} \\ &\le 2^k + 2^k \\ &= 2 \cdot 2^k \\ &= 2^{k+1}. \end{aligned}$$

This proves (3.1) when $k > 1$.

Case 2: Now suppose that $k = 1$. In this case (3.1) asserts that $f_2 \le 2^2$, and this is obvious from $f_2 = 1$.

By strong induction $P(n)$ is true for all $n \in \mathbb{Z}^+$. □

Exercise 3.5. Prove that $f_n \le (\frac{5}{3})^n$.

Exercise 3.6. Find a value of N such that $(\frac{3}{2})^n < f_n$ for all $n \ge N$.

Exercise 3.7. Define $a_1, a_2, \ldots$ by $a_1 = 1$, $a_2 = 3$, and

$$a_n = a_{n-1} + a_{n-2}$$

for $n > 2$. Prove $a_n < (7/4)^n$ for every $n \in \mathbb{Z}^+$.

Exercise 3.8. Define $b_1, b_2, \ldots$ by $b_1 = 11$, $b_2 = 21$, and

$$b_n = 3b_{n-1} - 2b_{n-2}$$

for $n > 2$. Prove that $b_n = 5 \cdot 2^n + 1$ for every $n \in \mathbb{Z}^+$.

Exercise 3.9. Let

$$\alpha = \frac{1+\sqrt{5}}{2} \qquad \beta = \frac{1-\sqrt{5}}{2}$$

be the two real roots of the quadratic equation $x^2 - x - 1 = 0$. Prove that the n^{th} Fibonacci number satisfies

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Exercise 3.10. Define $a_1, a_2, a_3, \ldots$ by $a_1 = 2$, and

$$a_{n+1} = a_n^2 + a_{n-1}^2 + \cdots + a_1^2$$

for $n \ge 1$. Prove that $a_n > 3^n$ for $n \ge 4$.

Exercise 3.11. Suppose that n is a positive integer. Prove using induction, integration by parts, and l'Hôpital's Rule that

$$\int_0^1 (-\log x)^n \, dx = n!$$

where, as usual, $\log x$ refers to the natural logarithm of x. You will need l'Hôpital's rule because this is an improper integral; the integrand is not defined at $x = 0$.

4. The Binomial Theorem

Definition 4.1. Given integers $0 \le k \le n$ we define the *binomial coefficient*

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

If $k < 0$ or $k > n$, we define $\binom{n}{k}$ to be 0.

Note the easy equalities $\binom{n}{0} = 1$, $\binom{n}{n} = 1$, and $\binom{n}{k} = \binom{n}{n-k}$.

Proposition 4.2 (Pascal's relation)**.** *If $0 < k < n+1$ then*

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

Proposition 4.3. *If $n \in \mathbb{Z}^+$ and $0 \le k \le n$ then $\binom{n}{k} \in \mathbb{Z}$.*

Theorem 4.4 (Binomial Theorem)**.** *For any $n \in \mathbb{Z}^{\ge 0}$ and any $x, y \in \mathbb{R}$ we have*

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

Proof. The proof is by induction. In the base case $n = 0$ the desired equality is

$$(x+y)^0 = \binom{0}{0} x^0 y^0,$$

which is obvious, as both sides are equal to 1. Now suppose that

$$(x+y)^n = \binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \cdots + \binom{n}{n} x^0 y^n \tag{4.1}$$

for some $n \ge 0$. We must prove the equality

$$(x+y)^{n+1} = \binom{n+1}{0} x^{n+1} y^0 + \binom{n+1}{1} x^n y^1 + \cdots + \binom{n+1}{n+1} x^0 y^{n+1}.$$

Multiplying both sides of (4.1) by $x + y$ results in

$$\begin{aligned}
&(x+y)^{n+1} \\
&= (x+y) \cdot \left[\binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \cdots + \binom{n}{n-1} x^1 y^{n-1} + \binom{n}{n} x^0 y^n \right] \\
&= x \cdot \left[\binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n} x^0 y^n \right] \\
&\quad + y \cdot \left[\binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \cdots + \binom{n}{n-1} x^1 y^{n-1} + \binom{n}{n} x^0 y^n \right] \\
&= \left[\binom{n}{0} x^{n+1} y^0 + \binom{n}{1} x^n y^1 + \binom{n}{2} x^{n-1} y^2 + \cdots + \binom{n}{n} x^1 y^n \right] \\
&\quad + \left[\binom{n}{0} x^n y^1 + \binom{n}{1} x^{n-1} y^2 + \cdots + \binom{n}{n-1} x^1 y^n + \binom{n}{n} x^0 y^{n+1} \right].
\end{aligned}$$

Notice that the final expression contains two terms involving the monomial $x^n y^1$, two terms involving the monomial $x^{n-1}y^2$, and so on, down to two terms involving the monomial $x^1 y^n$. Collecting together like terms and rearranging results in

$$\begin{aligned}(x+y)^{n+1} &= \binom{n}{0}x^{n+1}y^0 + \left[\binom{n}{0}+\binom{n}{1}\right]x^n y^1 + \left[\binom{n}{1}+\binom{n}{2}\right]x^{n-1}y^2 + \\ &\quad \cdots + \left[\binom{n}{n-1}+\binom{n}{n}\right]x^1 y^n + \binom{n}{n}x^0 y^{n+1}.\end{aligned}$$

Using Pascal's relation and the equalities

$$\binom{n}{0} = 1 = \binom{n+1}{0} \quad \text{and} \quad \binom{n}{n} = 1 = \binom{n+1}{n+1},$$

this simplifies to the desired equality

$$\begin{aligned}(x+y)^{n+1} &= \binom{n+1}{0}x^{n+1}y^0 + \binom{n+1}{1}x^n y^1 + \binom{n+1}{2}x^{n-1}y^2 + \\ &\quad \cdots + \binom{n+1}{n}x^1 y^n + \binom{n+1}{n+1}x^0 y^{n+1}.\end{aligned}$$

□

In the exercises, you were asked to prove the formula

$$\sum_{i=1}^{n} i^2 = \frac{n(2n+1)(n+1)}{6}$$

using induction. A disadvantage to the inductive proof is that it gives no indication of *how* one would ever have found the formula in the first place. Here is how the binomial theorem can be used to derive, rather than merely prove, this formula. Let's start by using the binomial theorem to expand

$$\begin{aligned}(x+1)^3 &= x^3 + \binom{3}{1}x^2 + \binom{3}{2}x + 1 \\ &= x^3 + 3x^2 + 3x + 1,\end{aligned}$$

so that

$$(x+1)^3 - x^3 = 3x^2 + 3x + 1.$$

Now let x vary over the set $\{1, 2, \ldots, n\}$ and write out the resulting equalities:

$$\begin{aligned}2^3 - 1^3 &= 3\cdot 1^2 + 3\cdot 1 + 1 \\ 3^3 - 2^3 &= 3\cdot 2^2 + 3\cdot 2 + 1 \\ 4^3 - 3^3 &= 3\cdot 3^2 + 3\cdot 3 + 1 \\ &\vdots \\ (n-1)^3 - (n-2)^3 &= 3\cdot(n-2)^2 + 3\cdot(n-2) + 1 \\ n^3 - (n-1)^3 &= 3\cdot(n-1)^2 + 3\cdot(n-1) + 1 \\ (n+1)^3 - n^3 &= 3\cdot n^2 + 3\cdot n + 1.\end{aligned}$$

If we add together all of these equalities, most of the terms on the left hand side cancel out leaving

$$(n+1)^3 - 1 = 3 \cdot (1^2 + 2^2 + 3^2 + \cdots + n^2) + 3 \cdot (1 + 2 + 3 + \cdots + n) + n,$$

or, solving for $1^2 + 2^2 + 3^2 + \cdots + n^2$,

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

Finally, we substitute in the known formula

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

and simplify the result:

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

Note that in order to derive the formula for $1^2 + 2^2 + \cdots + n^2$ it was important that we already knew the formula for $1 + 2 + \cdots + n$. Now that we know both of these formulas, we can continue on to derive the formula

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4} \tag{4.2}$$

(stated earlier in the exercises) in a similar way. Starting from the binomial expansion

$$\begin{aligned} (x+1)^4 &= x^4 + \binom{4}{1}x^3 + \binom{4}{2}x^2 + \binom{4}{3}x + 1 \\ &= x^4 + 4x^3 + 6x^2 + 4x + 1, \end{aligned}$$

we deduce the equality

$$(x+1)^4 - x^2 = 4x^3 + 6x^2 + 4x + 1.$$

Letting x vary over the set $\{1, 2, 3 \ldots, n\}$ and adding together all of the resulting formulas yields

$$(n+1)^4 - 1 = 4(1^3 + 2^3 + \cdots + n^3) + 6(1^2 + 2^2 + \cdots + n^2) + 4(1 + 2 + \cdots + n) + n,$$

which we rewrite as

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

Substituting in the known formulas for $1^2 + 2^2 + \cdots + n^2$ and $1 + 2 + \cdots + n$, and then simplifying the result, gives (try it!) the formula (4.2).

Exercise 4.5. Derive a formula for $\sum_{i=1}^{n} i^4$.

Exercise 4.6. Derive a formula for $\sum_{i=1}^{n} i^5$.

Exercise 4.7. Prove that

$$\binom{r}{m}\binom{m}{k} = \binom{r}{k}\binom{r-k}{m-k}$$

where $r \geq m \geq k \geq 0$.

Exercise 4.8.

(a) What is the coefficient of x^3y^4 in the expansion of $(2x+y)^7$?
(b) What is the coefficient of $x^{12}y^6$ in the expansion of $(x^3-3y)^{10}$?
(c) What is the coefficient of $x^{11}y^6$ in the expansion of $(x^3-3y)^{10}$?

Exercise 4.9. Prove

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

Exercise 4.10. Prove

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0.$$

Exercise 4.11. Suppose that $a, n \in \mathbb{Z}^+$. Prove that the product

$$(a+1)(a+2)(a+3)\cdots(a+n)$$

is divisible by $n!$.

Exercise 4.12. Suppose $m \geq 0$. Prove that

$$\binom{m}{m} + \binom{m+1}{m} + \cdots + \binom{n}{m} = \binom{n+1}{m+1}$$

for all $n \geq m$.

Exercise 4.13. Let n be a positive integer. Prove that $\binom{3n}{n}$ is a multiple of 3.

Exercise 4.14. If f is a function, let Df be its derivative. For $n \in \mathbb{Z}^+$ let

$$f^{(n)} = \underbrace{D\cdots D}_{n \text{ times}} f$$

be the n^{th} derivative of f. In this notation the usual product rule from calculus says that

$$(fg)^{(1)} = fg^{(1)} + f^{(1)}g.$$

Using the product rule, prove the formula for the n^{th} derivative of a product

$$(fg)^{(n)} = \sum_{k=0}^{n}\binom{n}{k} f^{(n-k)}g^{(k)}.$$

Exercise 4.15. Prove that for any integer $m \geq 2$

$$\binom{2m}{2} = 2\binom{m}{2} + m^2$$

Exercise 4.16. Prove that for any integer $n \geq 2$

$$\binom{m+n}{k} = \sum_{i=0}^{m}\binom{m}{i}\cdot\binom{n}{k-i}$$

Exercise 4.17. Prove that

$$\sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k} = \binom{a+b}{n}$$

where $a \geq n \geq 0$ and $b \geq n \geq 0$.

CHAPTER II

Arithmetic

1. Divisibility and the GCD

Definition 1.1. Given integers m and n, we say that m *divides* n (or that n is a *multiple* of m) if there exists a $q \in \mathbb{Z}$ such that $n = mq$. We often write $m \mid n$ to mean that m divides n.

Definition 1.2. Given two integers a and b, not both 0, their *greatest common divisor* $\gcd(a, b)$ is defined to be the largest integer that divides both a and b. We say that a and b are *relatively prime* (or *coprime*) if $\gcd(a, b) = 1$.

Exercise 1.3. What is $\gcd(-100, 75)$?

Exercise 1.4. Suppose $a, b, c \in \mathbb{Z}$. For each of the following claims, give either a proof or a counterexample.

(a) If $a \mid b$ and $b \mid c$ then $a \mid c$.
(b) If $a \mid bc$ then either $a \mid b$ or $a \mid c$.
(c) If $a \mid c$ and $b \mid c$ then $ab \mid c$.

Exercise 1.5. Suppose $b, c \in \mathbb{Z}^+$ are relatively prime and a is a divisor of $b + c$. Prove that

$$\gcd(a, b) = 1 = \gcd(a, c).$$

Exercise 1.6. Let f_n be the n^{th} Fibonacci number.

(a) Show that any common divisor of f_{n+1} and f_{n+2} is also a divisor of f_n.
(b) Now use induction to prove that $\gcd(f_n, f_{n+1}) = 1$ for all $n \in \mathbb{Z}^+$.

Exercise 1.7. In an earlier exercise we defined $g_n = 2^{2^n} + 1$, and proved that

$$g_0 g_1 g_2 \cdots g_{n-1} = g_n - 2.$$

Suppose now that a and b are unequal positive integers. Prove that $\gcd(g_a, g_b) = 1$.

2. The Division Algorithm

Theorem 2.1 (Division algorithm)**.** *Suppose $a, b \in \mathbb{Z}$ with $b > 0$. There are unique integers q and r that satisfy $a = bq + r$ and $0 \le r < b$.*

Proof. There are two things to prove here. First the existence of integers q and r with the desired properties, and then the uniqueness of q and r.

First we prove the existence of q and r. Look at the infinite list

$$\ldots,\ a - 2b,\ a - b,\ a,\ a + b,\ a + 2b,\ a + 3b,\ a + 4b,\ \ldots$$

The first claim is that this list contains a nonnegative element: if $a \ge 0$ then this is clear, while if $a < 0$ then

$$a + b \cdot (-a) = a(1 - b) \ge 0.$$

shows that $a + b \cdot (-a)$ is a nonnegative element of the list.

Let

$$S = \{a + bx : x \in \mathbb{Z} \text{ and } a + bx \geq 0\}$$

be the set of nonnegative elements in the list above. We have just agreed that $S \neq \emptyset$. I claim that the set S has a smallest element. If $0 \in S$ then 0 is the smallest element of S. If $0 \notin S$ then S is a nonempty subset of $\mathbb{Z}^+$, and the well-ordering property of $\mathbb{Z}^+$ then implies that S has a smallest element. In any case, we now know that S has a smallest element, which we call r.

The integer r, like every element of S, has the form $r = a + bx$ for some $x \in \mathbb{Z}$. If we set $q = -x$ then

$$a + bx = r \implies a - bq = r \implies a = bq + r$$

as desired. The only thing left to check is that $0 \leq r < b$. The inequality $0 \leq r$ is clear, because $r \in S \implies r \geq 0$. To prove that $r < b$, we of course use the fact that $r = a + bx$ is the smallest element of S. As

$$a + b(x - 1) < a + bx$$

we must have $a + b(x - 1) \notin S$. Therefore $a + b(x - 1) < 0$, and then

$$\begin{aligned} a + b(x - 1) < 0 &\implies a + bx - b < 0 \\ &\implies r - b < 0 \\ &\implies r < b. \end{aligned}$$

Now we prove the uniqueness of q and r. This means the following: suppose we have another pair of integers q' and r' that also satisfy $a = bq' + r'$ with $0 \leq r' < b$. We must show that $q = q'$ and $r = r'$. If we subtract one of

$$\begin{aligned} a &= bq + r \\ a &= bq' + r' \end{aligned}$$

from the other we arrive at $0 = b(q - q') + (r - r')$. This implies that $r' - r = b(q - q')$. Now from the inequalities

$$-b < -r \leq r' - r \leq r' < b$$

we deduce $-b < r' - r < b$, and dividing through by b shows that $-1 < q' - q < 1$. As $q' - q \in \mathbb{Z}$, the only possibility is $q' - q = 0$. Therefore $q' = q$, and from the relation $r' - r = b(q' - q)$ we deduce also that $r' = r$. □

Exercise 2.2. Find the quotient, q, and the remainder, r, in the division algorithm when

(a) $a = 17$ and $b = 5$,
(b) $a = 5$ and $b = 8$,
(c) $a = -31$ and $b = 5$.

Exercise 2.3. Prove that if n is a perfect square then n must have the form $4k$ or $4k + 1$. Hint: write $n = m^2$ for some $m \in \mathbb{Z}^+$. When m is divided by 4 there are four possible remainders. Consider each case separately.

3. Euclid's Algorithm

Euclid's algorithm is a simple and quick method to compute greatest common divisors. Start with $a, b \in \mathbb{Z}^+$ and repeatedly apply the division algorithm

$$\begin{aligned}
a &= bq_1 + r_1 && 0 \le r_1 < b \\
b &= r_1 q_2 + r_2 && 0 \le r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && 0 \le r_3 < r_2 \\
r_2 &= r_3 q_4 + r_4 && 0 \le r_4 < r_3 \\
r_3 &= r_4 q_5 + r_5 && 0 \le r_5 < r_4 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n && 0 \le r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}$$

As the remainders form a decreasing sequence of nonnegative integers

$$b > r_1 > r_2 > r_3 > r_4 > \cdots$$

they must eventually reach 0, which justifies the final line $r_{n-1} = r_n q_{n+1}$. We are interested in the last nonzero remainder, r_n.

Lemma 3.1. *If $c \in \mathbb{Z}$ divides both a and b then c divides r_n.*

Lemma 3.2. *If $c \in \mathbb{Z}$ divides r_n then c divides both a and b.*

Theorem 3.3. *The last nonzero remainder in Euclid's algorithm is* $\gcd(a, b)$*. Furthermore, for any $c \in \mathbb{Z}$ we have*

$$c \mid \gcd(a, b) \iff c \textit{ is a common divisor of } a \textit{ and } b.$$

Proof. Taken together, Lemma 3.1 and 3.2 show that for any $c \in \mathbb{Z}$

$$c \mid r_n \iff c \text{ is a common divisor of } a \text{ and } b. \tag{3.1}$$

As r_n divides itself, the implication $\implies$ of (3.1) shows that r_n is a common divisor of a and b. Now suppose that c is any common divisor of a and b. The implication $\impliedby$ of (3.1) implies that c divides r_n, and in particular $c \le r_n$. Thus $r_n = \gcd(a, b)$. The final claim

$$c \mid \gcd(a, b) \iff c \text{ is a common divisor of } a \text{ and } b$$

is now just a restatement of (3.1). □

The following proposition can be proved very efficiently using Euclid's algorithm: just perform Euclid's algorithm on a and b, and then multiply everything in sight by x.

Proposition 3.4. *For any $a, b, x \in \mathbb{Z}^+$ we have*

$$\gcd(ax, bx) = \gcd(a, b) \cdot x.$$

Proposition 3.5. *Suppose $a, b \in \mathbb{Z}^+$. If we set $d = \gcd(a, b)$, then a/d and b/d are relatively prime.*

Exercise 3.6. Use Euclid's algorithm to compute

(a) $\gcd(83, 13)$
(b) $\gcd(21, 96)$

(c) $\gcd(75, -21)$
(d) $\gcd(735, 1421)$
(e) $\gcd(-397, -204)$

Exercise 3.7. Let n and k be positive integers. Show that $\gcd(n, nk + 1) = 1$.

4. The equation $ax + by = \gcd(a, b)$

Definition 4.1. Suppose $a, b \in \mathbb{Z}$. A *$\mathbb{Z}$-linear combination* of a and b is an integer of the form $ax + by$ for some $x, y \in \mathbb{Z}$.

Suppose we want to express $\gcd(75, 21)$ as a $\mathbb{Z}$-linear combination of 75 and 21. In other words, we seek $x, y \in \mathbb{Z}$ satisfying

$$75x + 21y = \gcd(75, 21).$$

First perform Euclid's algorithm on 75 and 21:

$$\begin{aligned} 75 &= 21 \cdot 3 + 12 \\ 21 &= 12 \cdot 1 + 9 \\ 12 &= 9 \cdot 1 + 3 \\ 9 &= 3 \cdot 3. \end{aligned}$$

This shows that $\gcd(75, 21) = 3$. Now start at the top and work down, expressing each successive remainder as a $\mathbb{Z}$-linear combination of 75 and 21:

$$\begin{aligned} 12 &= 75 - 21 \cdot 3 \\ 9 &= 21 - 12 \\ &= 21 - (75 - 21 \cdot 3) \\ &= -75 + 21 \cdot 4 \\ 3 &= 12 - 9 \\ &= (75 - 21 \cdot 3) - (-75 + 21 \cdot 4) \\ &= 75 \cdot 2 - 21 \cdot 7. \end{aligned}$$

Thus we have the desired solution $x = 2$, $y = -7$ to

$$75x + 21y = \gcd(75, 21).$$

There are many other solutions to this equation; for example $x = -5$, $y = 18$ also works. Euclid's algorithm yields *one* solution.

Lemma 4.2. *If $m, n \in \mathbb{Z}$ are $\mathbb{Z}$-linear combinations of a and b, then $m + n$ is also a $\mathbb{Z}$-linear combination of a and b.*

Lemma 4.3. *Suppose $m \in \mathbb{Z}$ is a $\mathbb{Z}$-linear combination of a and b. Then cm is a $\mathbb{Z}$-linear combination of a and b for every $c \in \mathbb{Z}$.*

Theorem 4.4. *Suppose $a, b \in \mathbb{Z}^+$. Then there are $x, y \in \mathbb{Z}$ such that*

$$ax + by = \gcd(a, b).$$

Proof. Start by performing Euclid's algorithm on a and b:

$$\begin{aligned}
a &= bq_1 + r_1 & 0 &\le r_1 < b\\
b &= r_1q_2 + r_2 & 0 &\le r_2 < r_1\\
r_1 &= r_2q_3 + r_3 & 0 &\le r_3 < r_2\\
r_2 &= r_3q_4 + r_4 & 0 &\le r_4 < r_3\\
r_3 &= r_4q_5 + r_5 & 0 &\le r_5 < r_4\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n & 0 &\le r_n < r_{n-1}\\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

The first line can be rewritten as $r_1 = a - bq_1$ which shows that r_1 is a $\mathbb{Z}$-linear combination of a and b. The second line can be rewritten as $r_2 = b - r_1q_2$. Clearly $b = a \cdot 0 + b \cdot 1$ is a $\mathbb{Z}$-linear combination of a and b, and $-r_1q_2$ is a $\mathbb{Z}$-linear combination of a and b by Lemma 4.3, and so r_2 is also a $\mathbb{Z}$-linear combination of a and b by Lemma 4.2. The third line of Euclid's algorithm can be rewritten as

$$r_3 = r_1 - r_2q_2.$$

As we have already shown that r_1 and r_2 are $\mathbb{Z}$-linear combinations of a and b, so is r_3 (again by Lemmas 4.2 and 4.3). Continuing in this way we eventually find that $r_1, r_2, \dots, r_n$ are all $\mathbb{Z}$-linear combinations of a and b. In particular $r_n = \gcd(a, b)$ is a $\mathbb{Z}$-linear combination of a and b, as desired. □

Next, we remove the restriction $a, b > 0$ from Theorem 4.4.

Corollary 4.5. *If $a, b \in \mathbb{Z}$ are not both 0 then there are $x, y \in \mathbb{Z}$ such that*

$$ax + by = \gcd(a, b).$$

Proof. We know from Theorem 4.4 that the claim is true when $a > 0$ and $b > 0$. The remaining cases are treated as follows.

(a) Suppose $a > 0$ and $b < 0$. Then $-b > 0$, and so there are $x, y \in \mathbb{Z}$ such that

$$ax + (-b)y = \gcd(a, -b).$$

As $\gcd(a, -b) = \gcd(a, b)$, this can be rewritten as

$$ax + b(-y) = \gcd(a, b).$$

(b) Suppose $a < 0$ and $b > 0$; or that $a < 0$ and $b < 0$. These cases are proved using the same idea as the first case.

(c) Suppose $a = 0$ and $b > 0$. Then $\gcd(a, b) = b$, and so

$$a \cdot 0 + b \cdot 1 = \gcd(a, b).$$

(d) Suppose $a = 0$ and $b < 0$. Then $\gcd(a, b) = -b$, and so

$$a \cdot 0 + b \cdot (-1) = \gcd(a, b).$$

(e) Suppose $a > 0$ and $b = 0$; or that $a < 0$ and $b = 0$. These cases are treated in the same way as the previous two cases.

□

Lemma 4.6. *Suppose $a, b, m \in \mathbb{Z}$ with a, b not both zero. If $\gcd(a, b) \mid m$, then there is an integer solution to $ax + by = m$.*

Lemma 4.7. *Suppose $a, b, m \in \mathbb{Z}$ with a, b not both zero. If there is an integer solution to $ax + by = m$, then $\gcd(a, b) \mid m$.*

Theorem 4.8. *Suppose $a, b, m \in \mathbb{Z}$ with at least one of a, b nonzero. The equation $ax + by = m$ has a solution with $x, y \in \mathbb{Z}$ if and only if $\gcd(a, b) \mid m$. In other words:*

$$m \text{ is a } \mathbb{Z}\text{-linear combination of } a \text{ and } b \iff \gcd(a, b) \mid m.$$

Proof. Combine Lemmas 4.6 and 4.7. □

The proposition has an elegant proof based on Corollary 4.5.

Proposition 4.9. *Suppose $a, b, c \in \mathbb{Z}^+$, and $\gcd(a, b) = 1$.*

(*a*) *If $a \mid bc$, show that $a \mid c$.*
(*b*) *If $a \mid c$ and $b \mid c$, show that $ab \mid c$.*

Exercise 4.10. For each pair $a, b \in \mathbb{Z}$ below find $x, y \in \mathbb{Z}$ satisfying

$$ax + by = \gcd(a, b).$$

(a) $a = 83$, $b = 13$
(b) $a = 21$, $b = 96$
(c) $a = 75$, $b = -21$
(d) $a = 735$, $b = 1421$
(e) $a = -397$, $b = -204$
(f) $a = 1024$, $b = 238$

Exercise 4.11. For each of the following equations, either find an integer solution or show that no solution exists.

(a) $204x + 157y = 4$
(b) $501x - 42y = 3$
(c) $87x + 12y = -14$
(d) $-422x - 316y = 12$

Exercise 4.12. Find the smallest positive integer in the set

$$\{120x + 192y : x, y \in \mathbb{Z}\}.$$

Exercise 4.13. Suppose $a, b \in \mathbb{Z}^+$ and set $\ell = \frac{ab}{\gcd(a,b)}$.

(a) Show that ℓ is a common multiple of a and b.
(b) If m is any common multiple of a and b, show that m/ℓ is an integer.
(c) Deduce that

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

and that for any $m \in \mathbb{Z}$

$$m \text{ is a common multiple of } a \text{ and } b \iff m \text{ is a multiple of } \operatorname{lcm}(a, b).$$

Exercise 4.14. Suppose $a, b, x \in \mathbb{Z}^+$. Prove that $\operatorname{lcm}(ax, bx) = \operatorname{lcm}(a, b) \cdot x$.

Exercise 4.15. Suppose $a, b \in \mathbb{Z}^+$ are coprime, d is any integer, and we are given a pair of integers (x_0, y_0) such that

$$ax_0 + by_0 = d.$$

The goal of this exercise is to find *all* solutions to $ax + by = d$.

(a) First, suppose we have $x, y \in \mathbb{Z}$ such that $ax + by = 0$. Show that $a \mid y$ and $b \mid x$, and deduce that $(x, y) = (kb, -ka)$ for some $k \in \mathbb{Z}$.

(b) Now show that the set of solutions to $ax + by = d$ is exactly the set of pairs

$$(x, y) = (x_0 + kb, y_0 - ka)$$

with $k \in \mathbb{Z}$.

(c) Find all integer solutions to $500x + 131y = 5$.

Exercise 4.16 (The McNugget problem). Suppose your local McDonald's sells McNuggets in boxes of size a and size b, with $\gcd(a, b) = 1$. If $d \geq ab$, use the previous exercise to show that it is possible to order *exactly* d McNuggets. In other words, show that

$$ax + by = d$$

has a solution with $x \geq 0$ and $y \geq 0$.

5. The Fundamental Theorem of Arithmetic

Proposition 5.1. *Suppose $b, c \in \mathbb{Z}$ and p is a prime. Then*

$$p \mid bc \implies p \mid b \text{ or } p \mid c.$$

Corollary 5.2. *Let p be a prime and suppose $a_1, \ldots, a_n$ are nonzero integers. If p divides the product $a_1 \cdots a_n$ then p divides some a_i.*

Theorem 5.3 (Fundamental Theorem of Arithmetic)**.** *Suppose N is any positive integer. There are prime numbers $p_1, \ldots, p_k$ such that $N = p_1 \cdots p_k$. Furthermore, suppose we have another list of prime numbers $q_1, \ldots, q_\ell$ such that $N = q_1 \cdots q_\ell$. Then $k = \ell$ and, after possibly reordering the q_i's,*

$$p_1 = q_1, \quad p_2 = q_2, \quad \ldots \quad , p_k = q_k.$$

Proof. The existence of prime factorizations was the content of Theorem 3.3, and so we need only prove the uniqueness. Suppose N has two prime factorizations

$$N = p_1 \cdots p_k$$

and

$$N = q_1 \cdots q_\ell.$$

Without loss of generality we may assume that $k \leq \ell$. The above equalities obviously imply

$$p_1 \cdots p_k = q_1 \cdots q_\ell. \tag{5.1}$$

As p_1 divides the left hand side, Corollary 5.2 implies that p_1 divides some q_i. After reordering the list $q_1, \ldots, q_\ell$, we may assume that $p_1 \mid q_1$. As q_1 is prime, its only positive divisors are 1 and q_1, and we deduce that $p_1 = q_1$.

It now follows from (5.1) that

$$p_2 \cdots p_k = q_2 \cdots q_\ell.$$

The left hand side is visibly divisible by p_2, and repeating the argument of the paragraph above shows that, after possibly reordering the q_i's, $p_2 = q_2$. This leaves us with

$$p_3 \cdots p_k = q_3 \cdots q_\ell.$$

Repeating this process, we eventually find that $p_1 = q_1$, $p_2 = q_2$, and so on down to $p_{k-1} = q_{k-1}$, at which point we are left with the equality

$$p_k = q_k \cdots q_\ell.$$

From this we deduce $k = \ell$ (otherwise we have found a nontrivial factorization of the prime p_k, which is absurd), leaving $p_k = q_k$. □

Theorem 5.4 (Euclid). *There are infinitely many prime numbers.*

Proof. To get a contradiction, suppose there are only finitely many primes numbers, and list them (in no particular order) as $p_1, p_2, \ldots, p_k$. Now set

$$N = p_1 p_2 \cdots p_k + 1$$

and let q be any prime divisor of N. By hypothesis, $p_1, \ldots, p_k$ is a complete list of *all* prime numbers, and so q must appear in this list. If we now rewrite the definition of N as

$$N - p_1 p_2 \cdots p_k = 1,$$

we find that q divides the left hand side, and so $q \mid 1$. But this contradicts $q > 1$. □

Exercise 5.5. Prove that there are infinitely many primes of the form $4k - 1$. Hint: suppose there are only finitely many, say $p_1, \ldots, p_k$. What can you say about the prime factorization of $N = 4p_1 \cdots p_k - 1$?

Exercise 5.6. Suppose $a, b \in \mathbb{Z}^+$ are relatively prime. If m and n are any positive integers, show that a^m and b^n are again relatively prime.

Exercise 5.7. Suppose that a, b, and c are positive integers satisfying $\gcd(a, b) = 2$ and $\gcd(a, c) = 3$. What can you say about $\gcd(a, bc)$?

Exercise 5.8. Suppose that a, b, and c are positive integers satisfying $\gcd(a, b) = 2$ and $\gcd(a, c) = 4$. What can you say about $\gcd(a, bc)$?

Exercise 5.9. Suppose that a, b, and c are positive integers satisfying $\gcd(a, b) = 2$ and $\gcd(a, c) = 4$. What can you say about $\gcd(a^2, bc)$?

Exercise 5.10. Let n be a positive integer. Prove that if $18 \mid n^3$, then $18 \mid n^2$. (Note that it is quite possible for 18 not to divide n, for example if $n = 6$.)

CHAPTER III

Complex numbers, sets, and functions

1. The complex numbers

Definition 1.1. If X and Y are sets, the *Cartesian product* of X and Y is the set

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

Definition 1.2. The *complex numbers* are the set $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ with addition and multiplication defined by the rules

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

and

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

We usually write $x + iy$ to mean the complex number (x, y). Then the rules for addition and multiplication become

$$(x_1 + iy_1) + (x_2 + iy_2) = (x_1 + x_2) + i(y_1 + y_2)$$

and

$$(x_1 + iy_1) \cdot (x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2).$$

In particular, note that $i \cdot i = -1$.

Definition 1.3. If $z = x + iy$ is a complex number define

(a) the *real part* $\mathrm{Re}(z) = x$ and *imaginary part* $\mathrm{Im}(z) = y$,
(b) the *complex conjugate* $\overline{z} = x - iy$,
(c) and the *absolute value* $|z| = \sqrt{x^2 + y^2}$.

Note that $|z|$, $\mathrm{Re}(z)$, and $\mathrm{Im}(z)$ are real numbers, and that $|z| \geq 0$.

Proposition 1.4. *Suppose that $z_1, z_2, w \in \mathbb{C}$. Then*

(*a*) $z_1 \cdot z_2 = z_2 \cdot z_1$,
(*b*) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$,
(*c*) $\overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2$,
(*d*) $w\overline{w} = |w|^2$.

Proposition 1.5 (Triangle inequality)**.** *For any $z_2, z_2 \in \mathbb{C}$ we have*

$$|z_1 + z_2| \leq |z_1| + |z_2|.$$

Any complex number z may be written in *polar form* $z = r[\cos(\theta) + i\sin(\theta)]$ with $r \in \mathbb{R}^{\geq 0}$ and $\theta \in \mathbb{R}$.

Proposition 1.6. *Given two complex numbers in polar form*

$$z_1 = r_1[\cos(\theta_1) + i\sin(\theta_1)]$$
$$z_2 = r_2[\cos(\theta_2) + i\sin(\theta_2)],$$

the product has polar form

$$z_1z_2 = r_1r_2[\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)].$$

The next proposition, due to Euler, is proved using the power series expansions of e^x, $\sin(x)$, and $\cos(x)$. Note that taking $\theta = \pi$ yields the famous formula

$$e^{i\pi} = -1.$$

Proposition 1.7 (Euler's formula)**.** *For any $\theta \in \mathbb{R}$, we have*

$$e^{i\theta} = \cos(\theta) + i\sin(\theta).$$

Proposition 1.8 (DeMoivre's Theorem)**.** *Given a $z \in \mathbb{C}$ in polar form*

$$z = r \cdot [\cos(\theta) + i\sin(\theta)]$$

and any $n \in \mathbb{Z}^+$, we have $z^n = r^n \cdot [\cos(n\theta) + i\sin(n\theta)]$.

Exercise 1.9. Compute the real and imaginary parts of $(7-5i)^{-1}$.

Exercise 1.10. Suppose that z and w are complex numbers. Prove that

$$|z-w| \geq \Big||z| - |w|\Big|.$$

Exercise 1.11. Find two different complex numbers z and w such that $z^2 = w^2 = i$. Express your answer both in terms of trigonometric functions and in terms of radicals.

Exercise 1.12. Find three different complex numbers z, w, and u, so that $z^3 = w^3 = u^3 = i$. Express your answer both in terms of trigonometric functions and in terms of radicals.

2. Roots of unity

Let $2\pi\mathbb{Z}$ denote the set of all integer multiples of 2π, so that

$$2\pi\mathbb{Z} = \{2\pi k : k \in \mathbb{Z}\} = \{\ldots, -4\pi, -2\pi, 0, 2\pi, 4\pi, 6\pi, \ldots\},$$

and note the equivalence

$$r \cdot e^{i\theta} = 1 \iff r = 1 \text{ and } \theta \in 2\pi\mathbb{Z} \tag{2.1}$$

(as 1 has distance $r = 1$ from the origin, and is at angle $\theta = 2\pi k$ from the real axis). Let's now use this observation, together with Proposition 1.8, to find all complex solutions to the equation

$$z^3 = 1.$$

Any such solution can be written in polar form $z = re^{i\theta}$, and then

$$1 = z^3 = r^3 e^{i\cdot 3\theta}.$$

By (2.1), this happens precisely when $r^3 = 1$ and $3\theta \in 2\pi\mathbb{Z}$. As $r \in \mathbb{R}^{\geq 0}$, the relation $r^3 = 1$ is equivalent to $r = 1$. The relation $3\theta \in 2\pi\mathbb{Z}$ means precisely that $3\theta = 2\pi k$ for some $k \in \mathbb{Z}$, and so $\theta = 2\pi k/3$. We deduce that the solutions to $z^3 = 1$ consist of the set

$$\{e^{2\pi ik/3} : k \in \mathbb{Z}\} = \{\ldots, e^{-4\pi i/3}, e^{-2\pi i/3}, 1, e^{2\pi i/3}, e^{4\pi i/3}, e^{6\pi i/3}, e^{8\pi i/3}, \ldots\}.$$

At first glance, it looks as though this set is infinite, but in fact there are many repetitions in the list. For example

$$e^{6\pi i/3} = e^{2\pi i} = 1,$$

and

$$e^{8\pi i/3} = e^{6\pi i/3} e^{2\pi i/3} = e^{2\pi i/3}.$$

In fact, the list above is precisely the three complex numbers 1, $e^{2\pi i/3}$, and $e^{4\pi i/3}$ written again and again. Thus

$$\{z \in \mathbb{C} : z^3 = 1\} = \{1, e^{2\pi i/3}, e^{4\pi i/3}\}.$$

We can write this concisely by abbreviating $\zeta = e^{2\pi i/3}$, so that

$$\{z \in \mathbb{C} : z^3 = 1\} = \{1, \zeta, \zeta^2\}.$$

The same analysis will allow us to find all solutions to $z^n = 1$.

Definition 2.1. Given $n \in \mathbb{Z}^+$, an n^{th} *root of unity* is a $z \in \mathbb{C}$ such that $z^n = 1$. The set of all n^{th} roots of unity is denoted

$$\mu_n = \{z \in \mathbb{C} : z^n = 1\}.$$

The calculation done above shows that $\mu_3 = \{1, \zeta, \zeta^2\}$ where $\zeta = e^{2\pi i/3}$.

Theorem 2.2. *Suppose $n \in \mathbb{Z}^+$ and set $\zeta = e^{2\pi i/n}$. Then*

$$\mu_n = \{\zeta^k : k \in \mathbb{Z}\}.$$

Proof. First we prove the inclusion $\{\zeta^k : k \in \mathbb{Z}\} \subset \mu_n$. If $z \in \{\zeta^k : k \in \mathbb{Z}\}$ then there is some $k \in \mathbb{Z}$ such that $z = \zeta^k$. Therefore

$$z^n = (\zeta^k)^n = (e^{2\pi k i/n})^n = e^{2\pi k i} = 1,$$

which proves that $z \in \mu_n$. Now we prove the inclusion $\mu_n \subset \{\zeta^k : k \in \mathbb{Z}\}$. Suppose $z \in \mu_n$, so that $z^n = 1$. If we write $z = re^{i\theta}$ in polar coordinates then

$$1 = z^n = r^n e^{in\theta},$$

and (2.1) now implies $r^n = 1$ and $n\theta \in 2\pi\mathbb{Z}$. If follows that $r = 1$, and that there is some $k \in \mathbb{Z}$ such that $n\theta = 2\pi k$. Therefore

$$z = re^{i\theta} = e^{2\pi k i/n} = (e^{2\pi i/n})^k = \zeta^k,$$

proving that $z \in \{\zeta^k : k \in \mathbb{Z}\}$. □

Proposition 2.3. *If $z \in \mu_n$ then $\{z^k : k \in \mathbb{Z}\} = \{1, z, z^2, \ldots, z^{n-1}\}$.*

Combining Theorem 2.2 with Proposition 2.3 shows that, if we set $\zeta = e^{2\pi i/n}$,

$$\mu_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}.$$

Definition 2.4. Given an n^{th} root of unity $z \in \mu_n$, the *order* of z is the smallest $d \in \mathbb{Z}^+$ such that $z^d = 1$. In other words, z has order d if $z^d = 1$ but $z^m \neq 1$ for every $1 \leq m < d$. A *primitive* n^{th} *root of unity* is a $z \in \mu_n$ of order n.

Proposition 2.5. *If $z \in \mu_n$ then the order of z is a divisor of n.*

Proposition 2.6. *Suppose z is a root of unity of order d. Then for any $n \in \mathbb{Z}$*

$$z^n = 1 \iff d \mid n.$$

Theorem 2.7. *Suppose z is a root of unity of order d. Then for any $k \in \mathbb{Z}$, z^k has order $d/\gcd(d,k)$.*

Proof. Set

$$d_0 = d/\gcd(d,k) \qquad \text{and} \qquad k_0 = k_0/\gcd(d,k)$$

and recall (Chapter II, Proposition 3.5) that $\gcd(d_0, k_0) = 1$. We want to prove that z^k is a root of unity of order d_0. Let's first check that $(z^k)^{d_0} = 1$. This is clear from the calculation

$$(z^k)^{d_0} = z^{kd_0} = z^{kd/\gcd(d,k)} = (z^d)^{k_0} = 1^{k_0} = 1.$$

We next have to show that d_0 is the *smallest* positive integer such that $(z^k)^{d_0} = 1$. So, suppose we have another positive integer $f \in \mathbb{Z}^+$ such that $(z^k)^f = 1$. Then

$$(z^k)^f = 1 \implies z^{fk} = 1.$$

As z has order d by hypothesis, Proposition 2.6 implies $d \mid fk$, and so there is a $c \in \mathbb{Z}$ such that $fk = dc$. Dividing both sides by $\gcd(d,k)$ shows that

$$\frac{fk}{\gcd(d,k)} = \frac{dc}{\gcd(d,k)} \implies f \cdot k_0 = d_0 \cdot c.$$

In particular $d_0 \mid fk_0$. But now recall (Chapter II, Proposition 4.9) that whenever $\gcd(d_0, k_0) = 1$ we have

$$d_0 \mid fk_0 \implies d_0 \mid f.$$

In particular $d_0 \le f$. This proves that d_0 is the smallest positive integer such that $(z^m)^{d_0} = 1$, and shows that z^k has order d_0. □

Corollary 2.8. *Let $\zeta = e^{2\pi i/n}$. For any $k \in \mathbb{Z}$, ζ^k has order $n/\gcd(n,k)$. In particular, ζ^k is a primitive n^{th} root of unity if and only if $\gcd(n,k) = 1$.*

Exercise 2.9. Compute the order of every element of μ_n for $n = 5, 6, 7, 8, 9, 10$.

Exercise 2.10. Set

$$z = \frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

Show that z is a root of unity, find its order, and express z^{100} in the form $a + bi$.

Exercise 2.11. Prove that if $z \in \mathbb{C}$ satisfies both $z^a = 1$ and $z^b = 1$ then

$$z^{\gcd(a,b)} = 1.$$

Exercise 2.12. Prove that if $z \in \mathbb{C}$ is a root of unity then $\overline{z} = z^{-1}$.

Exercise 2.13.

(a) Let $w = 3 + 19i$. Compute the real and imaginary parts of $1/w$.

(b) Let

$$z = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}.$$

Compute the real and imaginary parts of z^{50}.

Exercise 2.14. Suppose that w is a primitive 3rd root of unity and z is a primitive 5th root of unity. Show that wz is a primitive 15th root of unity.

Exercise 2.15. Suppose that w is a primitive 9th root of unity and z is a primitive 5th root of unity. Show that wz is a primitive 45th root of unity.

Exercise 2.16. Fix an $n \in \mathbb{Z}^+$.

(a) Suppose $n > 1$. Prove that the sum of all n^{th} roots of unity is equal to 0. Hint: Factor the polynomial $x^n - 1$.
(b) Show that the product of all n^{th} roots of unity is 1 if n is odd, and is -1 if n is even.

Exercise 2.17. Suppose p is a prime number. Show that there are $p^n - p^{n-1}$ primitive p^n-th roots of unity.

Exercise 2.18. Let p be a prime and suppose $n \in \mathbb{Z}^+$. Show that $z \in \mu_{p^{n+1}}$ has order p^{n+1} if and only if z^p has order p^n.

Exercise 2.19. Suppose $d, n \in \mathbb{Z}^+$.

(a) Prove that $d \mid n \implies \mu_d \subset \mu_n$.
(b) Now prove that $\mu_d \subset \mu_n \implies d \mid n$.

Exercise 2.20. Suppose that a and b are roots of unity of orders m and n, respectively, with $\gcd(m, n) = 1$. Prove that ab has order mn. Show by example that the claim is false if the hypothesis $\gcd(m, n) = 1$ is omitted.

3. Operations on sets

Definition 3.1. Suppose A and B are sets. Define

(a) the *union* $A \cup B = \{x : x \in A \text{ or } x \in B\}$
(b) the *intersection* $A \cap B = \{x : x \in A \text{ and } x \in B\}$
(c) the *difference* $A \setminus B = \{x \in A : x \notin B\}$
(d) the *complement* $A^c = \{x : x \notin A\}$.

Proposition 3.2. *The operations of union and intersection are commutative:*

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A.$$

Proof. For any x we have

$$\begin{aligned} x \in A \cup B &\iff x \in A \text{ or } x \in B \\ &\iff x \in B \text{ or } x \in A \\ &\iff x \in B \cup A. \end{aligned}$$

This proves that $A \cup B = B \cup A$, and the proof of $A \cap B = B \cap A$ is similar (just replace *or* by *and*). □

Proposition 3.3. *The operations of union and intersection are associative:*

$$(A \cup B) \cup C = A \cup (B \cup C)$$
$$(A \cap B) \cap C = A \cap (B \cap C).$$

Proposition 3.4. *For any sets A and B we have $A \setminus B = A \cap B^c$.*

Proposition 3.5 (De Morgan's laws)**.** *For any sets A and B*

$$(A \cup B)^c = A^c \cap B^c$$
$$(A \cap B)^c = A^c \cup B^c.$$

Proposition 3.6 (Distributive laws)**.** *For any sets A, B, and C we have*

(*a*) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(*b*) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Exercise 3.7. Given sets A, B, and C, prove

(a) $A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C)$

(b) $A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C)$.

Exercise 3.8.

(a) Prove that if $A \cup B = A$ and $A \cap B = A$ then $A = B$.

(b) Give a counterexample to the claim $(A \smallsetminus B) \cup B = A$.

Exercise 3.9.

(a) Find a counterexample to $A \cap (B \cup C) = (A \cap B) \cup C$.

(b) Find a counterexample to $A \cup (B \cap C) = (A \cup B) \cap C$.

Exercise 3.10. For each of the following statements either provide a proof or a counterexample.

(a) $(A \cup B) \cap A^c = B \smallsetminus A$

(b) $(A \cup B) \cap C = A \cup (B \cap C)$

(c) $A \times (B \smallsetminus C) = (A \times B) \smallsetminus (A \times C)$

(d) $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$

(e) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

Exercise 3.11. For each of the following statements either provide a proof or a counterexample.

(a) $A \smallsetminus (A \smallsetminus B) = B$

(b) $A \smallsetminus (B \smallsetminus A) = A \smallsetminus B$

(c) $A \cap (B \smallsetminus C) = (A \cap B) \smallsetminus (A \cap C)$

(d) $A \cup (B \smallsetminus C) = (A \cup B) \smallsetminus (A \cup C)$

(e) $(A \cap B) \cup (A \smallsetminus B) = A$

(f) $(A \smallsetminus B) \cap C = (A \cap C) \smallsetminus (B \cap C)$.

Exercise 3.12. For each of the following statements either provide a proof or a counterexample.

(a) If $C \subset A$ and $C \subset B$ then $C \subset A \cup B$

(b) If $C \subset A \cup B$ then $C \subset A$ and $C \subset B$

(c) If $C \subset A$ or $C \subset B$ then $C \subset A \cup B$

(d) If $C \subset A \cup B$ then $C \subset A$ or $C \subset B$

(e) If $C \subset A$ and $C \subset B$ then $C \subset A \cap B$

(f) If $C \subset A \cap B$ then $C \subset A$ and $C \subset B$

(g) If $C \subset A$ or $C \subset B$ then $C \subset A \cap B$

(h) $A \subset C$ and $B \subset D \implies (A \times B) \subset (C \times D)$

Exercise 3.13. Given sets A and B define the *symmetric difference*

$$A \triangle B = (A \cup B) \smallsetminus (A \cap B).$$

(a) Prove that $A \triangle B = (A \smallsetminus B) \cup (B \smallsetminus A)$.

(b) Find a set X with the property $X \triangle A = A$ for every set A.

(c) Prove that

$$(A \triangle B) \triangle C = A \triangle (B \triangle C).$$

4. Functions

We give an informal definition of the word “function.” Suppose X and Y are sets. A *function* $f : X \to Y$ is a rule that assigns to every element $x \in X$ an element $f(x) \in Y$. The set X is called the *domain* of f, and the set Y is called the *codomain* of f.

For example we have the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$, and the function $f : (0, 1) \to \mathbb{R}$ defined by $f(x) = 1/x$. We ***cannot*** talk about the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 1/x$, as the rule provided fails to associate an element of the codomain to $0 \in \mathbb{R}$. In other words, $f(0)$ is not defined. This problem could be fixed by shrinking the proposed domain: the function $f : \mathbb{R} \smallsetminus \{0\} \to \mathbb{R}$ defined by $f(x) = 1/x$ is perfectly fine. Similarly we ***cannot*** talk about the function $f : \mathbb{R} \to [0, 1]$ defined by $f(x) = \cos(x)$, as the rule given fails to associate to $\pi \in \mathbb{R}$ an element of the codomain $[0, 1]$. In other words, $f(\pi) \notin [0, 1]$. This problem is easily fixed by enlarging the codomain: the function $f : \mathbb{R} \to [-1, 1]$ defined by $f(x) = \cos(x)$ is perfectly fine.

Definition 4.1. Let $f : X \to Y$ be a function.

(a) We say that f is *injective* if for every $x_1, x_2 \in X$

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

(b) We say that f is *surjective* if for every $y \in Y$ there exists some $x \in X$ such that $f(x) = y$.

(c) We say that f is *bijective* if f is both injective and surjective.

The definition of injective can be rephrased by replacing the implication

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

by its contrapositive

$$f(x_1) = f(x_2) \implies x_1 = x_2.$$

Thus an equivalent (and more useful) definition of injective is: $f : X \to Y$ is injective if for every $x_1, x_2 \in X$ we have $f(x_1) = f(x_2) \implies x_1 = x_2$.

If $f : X \to Y$ is injective then given any $y \in Y$ there is *at most* one solution to $f(x) = y$. Indeed, if x_1 and x_2 are two solutions then $f(x_1) = y = f(x_2) \implies x_1 = x_2$. If $f : X \to Y$ is surjective then for every $y \in Y$ the equation $f(x) = y$ has *at least* one solution. If $f : X \to Y$ is bijective then for every $y \in Y$ the equation $f(x) = y$ has *exactly* one solution.

Definition 4.2. Suppose X, Y, Z are sets, and we have functions $f : X \to Y$ and $g : Y \to Z$. The *composition* $g \circ f : X \to Z$ is the function

$$(g \circ f)(x) = g(f(x)).$$

Theorem 4.3. *Composition of functions is associative: given three functions*

$$\begin{aligned} f &: A \to B \\ g &: B \to C \\ h &: C \to D \end{aligned}$$

we have $(h \circ g) \circ f = h \circ (g \circ f)$.

Proof. For any $a \in A$ we have both

$$\big((h \circ g) \circ f\big)(a) = (h \circ g)(f(a)) = h(g(f(a)))$$

and

$$\big(h \circ (g \circ f)\big)(a) = h((g \circ f)(a) = h(g(f(a))).$$

Therefore $(h \circ g) \circ f = h \circ (g \circ f)$. □

Definition 4.4. For any set X define the *identity function* $\mathrm{id}_X : X \to X$ by $\mathrm{id}_X(x) = x$.

Proposition 4.5. *For any function $f : X \to Y$ we have $\mathrm{id}_Y \circ f = f$ and $f \circ \mathrm{id}_X = f$.*

Definition 4.6. Suppose $f : X \to Y$ is a function. A function $g : Y \to X$ is called an *inverse* of f if it satisfies both relations

$$f \circ g = \mathrm{id}_Y \qquad g \circ f = \mathrm{id}_X.$$

We say that f is *invertible* if it admits an inverse.

Theorem 4.7. *Suppose $f : X \to Y$ is a function and $g, h : Y \to X$ are inverses of f. Then $g = h$.*

Proof. This follows from the sneaky calculation

$$g = \mathrm{id}_X \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ \mathrm{id}_Y = h.$$

□

Thus if $f : X \to Y$ has an inverse, it has a *unique* inverse. The inverse is usually denoted by $f^{-1} : Y \to X$, and satisfies (by definition)

$$f \circ f^{-1} = \mathrm{id}_Y \qquad f^{-1} \circ f = \mathrm{id}_X.$$

Equivalently, $f(f^{-1}(y)) = y$ for every $y \in Y$, and $f^{-1}(f(x)) = x$ for every $x \in X$.

Theorem 4.8. *A function $f : X \to Y$ is invertible if and only if it is bijective.*

Proof. Suppose that f is invertible, so there is an inverse $f^{-1} : Y \to X$. First we prove that f is injective: for any $x_1, x_2 \in X$ we have

$$\begin{aligned} f(x_1) = f(x_2) &\implies f^{-1}(f(x_1)) = f^{-1}(f(x_2)) \\ &\implies x_1 = x_2. \end{aligned}$$

This proves the injectivity. Now for surjectivity suppose $y \in Y$. If we set $x = f^{-1}(y)$ then

$$f(x) = f(f^{-1}(y)) = y.$$

This prove that f is surjective, and completes the proof that f is bijective.

Now assume that f is bijective. This means that for every $y \in Y$ the equation $f(x) = y$ has a unique solution. We define a function $g : Y \to X$ as follows: for every $y \in Y$ let $g(y) \in X$ be the unique element of X satisfying $f(g(y)) = y$. The function g is defined in such a way that $f(g(y)) = y$ for every $y \in Y$, and so $f \circ g = \mathrm{id}_Y$. Now suppose $x \in X$, and set $y = f(x)$. Then the two equalities $f(x) = y$ and $f(g(y)) = y$ together with the injectivity of f tell us

$$f(g(y)) = f(x) \implies g(y) = x \implies g(f(x)) = x.$$

This proves that $g \circ f = \mathrm{id}_X$, and shows that g is an inverse of f. □

Exercise 4.9. Compute the inverse of the function $f : \mathbb{C} \smallsetminus \{1\} \to \mathbb{C} \smallsetminus \{2\}$ defined by $f(z) = (2z-1)/(z-1)$

Exercise 4.10. For each of the following functions either compute the inverse or show that no inverse exists.

(a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = (5x-2)/12$
(b) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$
(c) $f : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ defined by $f(x) = x^2$
(d) $f : \mathbb{C} \to \mathbb{C}$ defined by $f(x) = x^2$
(e) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 2n$.
(f) $f : \mathbb{R} \smallsetminus \{1\} \to \mathbb{R} \smallsetminus \{1\}$ defined by $f(x) = \frac{x+1}{x-1}$
(g) $f : \mathbb{C} \smallsetminus \{1\} \to \mathbb{C} \smallsetminus \{2\}$ defined by $f(z) = (2z-1)/(z-1)$

Exercise 4.11. For each of the following functions $f : X \to Y$, is f injective? Surjective? Bijective?

(a) $f : \mathbb{Z} \to \mu_5$ defined by $f(n) = e^{2\pi i n/5}$
(b) $f : \mathbb{Z} \to \mu_{10}$ defined by $f(n) = e^{2\pi i n/5}$.
(c) $f : \mu_3 \to \mu_3$ defined by $f(z) = z^3$
(d) $f : \mu_5 \to \mu_5$ defined by $f(z) = z^3$
(e) $f : \mu_9 \to \mu_3$ defined by $f(z) = z^3$
(f) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined by $f(x, y) = x - y$
(g) $f : \mathbb{Z} \to \mathbb{Z}$ defined by

$$f(n) = \begin{cases} n+2 & \text{if } n \text{ is even} \\ 2n+1 & \text{if } n \text{ is odd} \end{cases}$$

Exercise 4.12. Find a function $f : \mathbb{Z} \to \mathbb{Z}$ which is

(a) neither injective nor surjective.
(b) injective but not surjective.
(c) surjective but not injective.

Exercise 4.13. Suppose we have functions $f : A \to B$ and $g : B \to C$.

(a) Prove that if f and g are both injective then so is $g \circ f$.
(b) Prove that if f and g are both surjective then so is $g \circ f$.
(c) It follows from the previous two parts that if f and g are bijective then so is $g \circ f$. Is the converse

$$g \circ f \text{ bijective} \implies f \text{ and } g \text{ bijective}$$

true? Prove or give a counterexample.

Exercise 4.14. Give an example of functions $f : X \to Y$ and $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ but f is not invertible.

Exercise 4.15. Given two subsets A and B of $\mathbb{C}$, consider the function $f : A \to B$ defined by $f(z) = z^5$. Find examples of A and B for which

(a) f is a bijection
(b) f is injective but not surjective
(c) f is surjective but not injective.

Exercise 4.16. Suppose that $f : A \to B$ and $g : B \to C$ are functions.

(a) Prove that if $g \circ f$ is injective then f is injective.
(b) Prove that if $g \circ f$ is surjective then g is surjective.

Exercise 4.17. Suppose we have functions $f : A \to B$ and $g : B \to C$ with inverses $f^{-1} : B \to A$ and $g^{-1} : C \to B$. Prove that $g \circ f$ is invertible, and

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Exercise 4.18. Define a function $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ by the formula

$$f(a,b) = \begin{cases} \binom{a}{b} & \text{if } a \geq b \\ \binom{b}{a} & \text{if } a < b. \end{cases}$$

Decide if f is surjective, injective, both, or neither.

Exercise 4.19. Define a function $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ by the formula

$$f(a,b) = \binom{a+b}{b}.$$

Decide if f is surjective, injective, both, or neither.

Exercise 4.20. Suppose that $f : \mathbb{C} \to \mathbb{C}$ is a surjection. Define a new function $g : \mathbb{C} \to \mathbb{C}$ by the formula $g(x) = 2f(x+1)$. Show that $g(x)$ is a surjection.

Exercise 4.21. Determine if each of the following functions is injective, surjective, both, or neither:

(a) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(x) = \dfrac{x}{x^2+1}$,
(b) $g : \mathbb{Z} \to \mathbb{Q}$ defined by $g(x) = \dfrac{x}{x^2+1}$.

5. Image and preimage

Definition 5.1. Suppose $f : X \to Y$ is a function, and that $A \subset X$ and $B \subset Y$.

(a) The *image of A under f* is the set

$$f(A) = \{f(a) : a \in A\}.$$

(b) The *preimage of B under f* is the set

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

The image of X under f, $f(X)$, is often simply called *the image of f*.

The definition of preimage and image can be restated as follows

- for every $x \in X$,

$$x \in f^{-1}(B) \iff f(x) \in B,$$

- for every $y \in Y$,

$$y \in f(A) \iff \exists a \in A \text{ such that } y = f(a).$$

Proposition 5.2. *Suppose $f : X \to Y$ is a function.*

(a) *If* $A \subset B$ *are subsets of* X *then* $f(A) \subset f(B)$.
(b) *If* $C \subset D$ *are subsets of* Y *then* $f^{-1}(C) \subset f^{-1}(D)$.

Exercise 5.3. Let $\zeta = e^{2\pi i/6}$, and define $f : \mathbb{Z} \to \mu_6$ by $f(n) = \zeta^n$. Compute each of the following sets:
(a) $f(\{2k : k \in \mathbb{Z}\})$
(b) $f(\{5k : k \in \mathbb{Z}\})$
(c) $f^{-1}(\{\zeta\})$
(d) $f^{-1}(\{1, \zeta, \zeta^3\})$.

In all of the following exercises, X **and** Y **are sets and** $f : X \to Y$ **is a function.**

Exercise 5.4. For each of the following statements, provide a proof or a counterexample.
(a) If A, B are subsets of X then $f(A \cup B) = f(A) \cup f(B)$.
(b) If A, B are subsets of X then $f(A \cap B) = f(A) \cap f(B)$.
(c) If C, D are subsets of Y then $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
(d) If C, D are subsets of Y then $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.
Hint: at least one of them is false.

Exercise 5.5. Suppose that f is surjective. Prove that every $A \subset X$ satisfies

$$Y \smallsetminus f(A) \subset f(X \smallsetminus A).$$

Show by example that the claim is false if we omit the hypothesis that f is surjective.

Exercise 5.6.
(a) Suppose $B \subset Y$. Prove or give a counterexample to each of the inclusions

$$B \subset f(f^{-1}(B)) \qquad f(f^{-1}(B)) \subset B.$$

(b) Suppose f is surjective, and $B \subset Y$. Prove that $f(f^{-1}(B)) = B$.
(c) Suppose $A \subset X$. Prove or give a counterexample to each of the inclusions

$$A \subset f^{-1}(f(A)) \qquad f^{-1}(f(A)) \subset A.$$

(d) Suppose f is injective, and $A \subset X$. Prove that $f^{-1}(f(A)) = A$.

Exercise 5.7.
(a) Suppose that $A, B \subset X$, and that f is injective. Prove that

$$f(A) \subset f(B) \implies A \subset B.$$

(b) Show that the previous claim is false if we omit the hypothesis that f is injective.
(c) Suppose that $C, D \subset Y$, and that f is surjective. Prove that

$$f^{-1}(C) \subset f^{-1}(D) \implies C \subset D.$$

(d) Show that the previous claim is false if we omit the hypothesis that f is surjective.

Exercise 5.8. Suppose $A_1, A_2 \subset X$. Prove or give a counterexample:

$$f(A_1 \smallsetminus A_2) = f(A_1) \smallsetminus f(A_2).$$

Exercise 5.9. Suppose $f^{-1}(f(A)) = A$ holds for *every* $A \subset X$. Prove that f is an injection.

Exercise 5.10. Suppose we are given functions $f, g : \mathbb{R} \to \mathbb{R}$ satisfying

$$g(x) = f(3x + 2).$$

(a) If $f([2, 5]) = [10, 20]$, what is $g([0, 1])$?
(b) If $f^{-1}([-10, 10]) = [0, 2]$, what is $g^{-1}([-10, 10])$?

CHAPTER IV

Congruences and the ring $\mathbb{Z}/n\mathbb{Z}$

1. Equivalence relations and partitions

Let X be a set. We will settle for an intuitive definition of what it means to have a *relation* on X: a relation R on X is a property that may or may not hold between two elements of X. We write xRy to mean that the relation R does hold between x and y. For example $<$ ("less than") is a relation on $\mathbb{R}$, and we write $x < y$ to mean that the relation holds. Another example would be the relation R on $\mathbb{Z}$ defined by xRy if and only if $x^2 = y^2$. Thus $-2R2$ since $(-2)^2 = 2^2$, but $3 \not R\, 5$ since $3^2 \neq 5^2$. Relations satisfying certain properties are customarily denoted by $\sim$ instead of R, and are called equivalence relations:

Definition 1.1. Let X be a set and let $\sim$ be a relation on X. We say that $\sim$ is an *equivalence relation* if it satisfies the following three properties:
(reflexivity): every $a \in X$ satisfies $a \sim a$,
(symmetry): for all $a, b \in X$, we have $a \sim b \implies b \sim a$,
(transitivity): for all $a, b, c \in X$, if $a \sim b$ and $b \sim c$ then $a \sim c$.

Definition 1.2. Let X be a set and let $\sim$ be an equivalence relation on X. For any $a \in X$ define the *equivalence class of* a by

$$[a] = \{x \in X : x \sim a\}.$$

Note that, by definition of $[a]$, $b \in [a] \iff b \sim a$.

Example 1.3. Define a relation $\sim$ on $\mathbb{R}$ by

$$a \sim b \iff a^2 = b^2.$$

Let's first check that $\sim$ is an equivalence relation. For any $a \in \mathbb{R}$ we obviously have $a^2 = a^2$, and so $a \sim a$. Therefore $\sim$ is reflexive. For any $a, b \in \mathbb{R}$

$$a \sim b \implies a^2 = b^2 \implies b^2 = a^2 \implies b \sim a,$$

proving that $\sim$ is symmetric. Finally, for any $a, b, c \in \mathbb{R}$

$$\begin{aligned} a \sim b \text{ and } b \sim c &\implies a^2 = b^2 \text{ and } b^2 = c^2 \\ &\implies a^2 = c^2 \\ &\implies a \sim c. \end{aligned}$$

That proves the transitivity. Next, what is the equivalence class of, say, 13? From the definitions

$$\begin{aligned} [13] &= \{x \in \mathbb{R} : x \sim 13\} \\ &= \{x \in \mathbb{R} : x^2 = 13^2\} \\ &= \{13, -13\}. \end{aligned}$$

Similarly for every $a \in \mathbb{R}$

$$\begin{aligned}[a] &= \{x \in \mathbb{R} : x \sim a\} \\ &= \{x \in \mathbb{R} : x^2 = a^2\} \\ &= \{a, -a\}.\end{aligned}$$

Definition 1.4. Fix a positive integer n. Define a relation on $\mathbb{Z}$, called *congruence modulo n*, by

$$a \equiv b \pmod{n} \iff n \text{ divides } a - b.$$

Proposition 1.5. *For every $n \in \mathbb{Z}^+$, congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

Theorem 1.6. *For all $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$*

$$a \equiv b \pmod{n} \iff \begin{array}{c} a \text{ and } b \text{ leave the same remainder} \\ \text{when divided by } n. \end{array}$$

Proof. ($\Longleftarrow$) Assume that a and b both have remainder r when divided by n. Then there are $q_1, q_2 \in \mathbb{Z}$ satisfying

$$\begin{aligned} a &= nq_1 + r \\ b &= nq_2 + r. \end{aligned}$$

Subtracting these equations shows that

$$a - b = n(q_1 - q_2).$$

Therefore $n \mid a - b$ and so $a \equiv b \pmod{n}$.

($\implies$) Assume that $a \equiv b \pmod{n}$, so that n divides $a - b$. By the division algorithm there are $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ satisfying

$$\begin{aligned} a &= nq_1 + r_1 \qquad 0 \le r_1 < n \\ b &= nq_2 + r_2 \qquad 0 \le r_2 < n. \end{aligned}$$

Subtraction shows that

$$a - b = n(q_1 - q_2) + (r_1 - r_2)$$

and so

$$(a - b) - n(q_1 - q_2) = r_1 - r_2.$$

The left hand side is divisible by n, and therefore also $r_1 - r_2$ is divisible by n. But using the inequalities $0 \le r_1 < n$ and $0 \le r_2 < n$ we see that

$$-n < -r_2 \le r_1 - r_2 \le r_1 < n.$$

Thus $-n < r_1 - r_2 < n$ and so

$$-1 < \frac{r_1 - r_2}{n} < 1.$$

But we know that $(r_1 - r_2)/n$ is an integer, so it must be 0. Thus $r_1 = r_2$, and a and b leave the same remainder when divided by n. □

Example 1.7. Let's compute the equivalence classes for the equivalence relation congruence modulo 3 on $\mathbb{Z}$. We have

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv 0 \pmod 3\} \\
&= \{x \in \mathbb{Z} : x \text{ leaves the same remainder as 0 when divided by 3}\} \\
&= \{x \in \mathbb{Z} : x \text{ leaves remainder 0 when divided by 3}\} \\
&= \{\dots, -3, 0, 3, 6, \dots\}
\end{aligned}$$

$$\begin{aligned}
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\} \\
&= \{x \in \mathbb{Z} : x \text{ leaves the same remainder as 1 when divided by 3}\} \\
&= \{x \in \mathbb{Z} : x \text{ leaves remainder 1 when divided by 3}\} \\
&= \{\dots, -2, 1, 4, 7, \dots\}
\end{aligned}$$

$$\begin{aligned}
[2] &= \{x \in \mathbb{Z} : x \equiv 2 \pmod 3\} \\
&= \{x \in \mathbb{Z} : x \text{ leaves the same remainder as 2 when divided by 3}\} \\
&= \{x \in \mathbb{Z} : x \text{ leaves remainder 2 when divided by 3}\} \\
&= \{\dots, -1, 2, 5, 8, \dots\}
\end{aligned}$$

$$\begin{aligned}
[3] &= \{x \in \mathbb{Z} : x \equiv 3 \pmod 3\} \\
&= \{x \in \mathbb{Z} : x \text{ leaves the same remainder as 3 when divided by 3}\} \\
&= \{x \in \mathbb{Z} : x \text{ leaves remainder 0 when divided by 3}\} \\
&= \{\dots, -3, 0, 3, 6, \dots\}
\end{aligned}$$

$$\begin{aligned}
[4] &= \{x \in \mathbb{Z} : x \equiv 4 \pmod 3\} \\
&= \{x \in \mathbb{Z} : x \text{ leaves the same remainder as 4 when divided by 3}\} \\
&= \{x \in \mathbb{Z} : x \text{ leaves remainder 1 when divided by 3}\} \\
&= \{\dots, -2, 1, 4, 7, \dots\} \\
&\vdots
\end{aligned}$$

In particular note that

$$\begin{gathered}
\cdots = [-3] = [0] = [3] = [6] = \cdots \\
\cdots = [-2] = [1] = [4] = [7] = \cdots \\
\cdots = [-1] = [2] = [5] = [8] = \cdots
\end{gathered}$$

and so there are only three equivalence classes: $[0], [1], [2]$.

The following proposition will be needed later, to prove Proposition 3.5.

Proposition 1.8. *Fix $n \in \mathbb{Z}^+$. If $a, b, a', b' \in \mathbb{Z}$ satisfy*

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

then

(*a*) $a + b \equiv a' + b' \pmod n$
(*b*) $ab \equiv a'b' \pmod n$.

Proposition 1.9. *Let X be a set and let $\sim$ be an equivalence relation on X. For any $a, b \in X$ the following are equivalent:*

- $b \sim a$,
- $b \in [a]$,
- $[b] = [a]$.

Definition 1.10. Let X be any set. A *partition* of X is a collection $\mathcal{C}$ of subsets of X having the following properties:

(a) for every $x \in X$ there is a $B \in \mathcal{C}$ such that $x \in B$,
(b) every $B \in \mathcal{C}$ is nonempty,
(c) given any $B, B' \in \mathcal{C}$ either $B = B'$ or $B \cap B' = \emptyset$.

The elements $B \in \mathcal{C}$ are called the *blocks* of the partition.

Remark 1.11. Let $\mathcal{C}$ be a partition of X. For each $x \in X$ we know from the first property of a partition that there is some $B \in \mathcal{C}$ such that $x \in B$. Suppose there is another $B' \in \mathcal{C}$ such that $x \in B'$ as well. Then $x \in B \cap B'$ which implies that $B \cap B' \neq \emptyset$. By the third property of a partition we deduce that $B = B'$. To summarize: for every $x \in X$ there is a *unique* $B \in \mathcal{C}$ such that $x \in B$.

Example 1.12. Take X to be the set $X = \{1, 2, 3, \dots, 10\}$. As a partition of X we could take the collection $\mathcal{C} = \{B_1, B_2, B_3, B_4\}$ in which

$$\begin{aligned} B_1 &= \{4, 5, 8, 9\} \\ B_2 &= \{1, 2, 10\} \\ B_3 &= \{3\} \\ B_4 &= \{6, 7\}. \end{aligned}$$

More succinctly

$$\mathcal{C} = \Big\{\{4, 5, 8, 9\}, \{1, 2, 10\}, \{3\}, \{6, 7\}\Big\}.$$

Example 1.13. Go back to the equivalence classes for the equivalence relation $a \equiv b \pmod 3$. Recall that there are three equivalence classes

$$\begin{aligned} [0] &= \{\dots, -3, 0, 3, 6, \dots\} \\ [1] &= \{\dots, -2, 1, 4, 7, \dots\} \\ [2] &= \{\dots, -1, 2, 5, 8, \dots\}. \end{aligned}$$

Instead of using the clunky phrase *the equivalence classes for the equivalence relation* $a \equiv b \pmod 3$, most people would refer to these three subsets of $\mathbb{Z}$ as the *congruence classes modulo* 3. Note that $\mathcal{C} = \{[0], [1], [2]\}$ is a partition of $\mathbb{Z}$: every integer is contained in one of $[0], [1], [2]$; each of $[0]$, $[1]$, $[2]$ is nonempty; and the three blocks do not overlap, in the sense that for any $[a], [b] \in \mathcal{C}$ either $[a] = [b]$ or $[a] \cap [b] = \emptyset$

Proposition 1.14. *Given any equivalence relation $\sim$ on a set X, the collection of all equivalence classes $\mathcal{C} = \{[a] : a \in X\}$ is a partition of X.*

The upshot of the proposition is that any equivalence relation on a set X induces a partition of X. There is way to reverse this construction. Starting from a partition $\mathcal{C}$ of X one can define an equivalence relation on X as follows. We know from Remark 1.11 that for every $x \in X$ there is a unique $B \in \mathcal{C}$ such that $x \in B$. Not very creatively, we will refer to this B as the *block containing x*. Now define a relation $\sim$ on X by

$$a \sim b \iff \text{(the block containing } a) = \text{(the block containing } b).$$

We will see in a moment that $\sim$ is an equivalence relation. As an example, let's return to the partition

$$\mathcal{C} = \Big\{\{4,5,8,9\},\{1,2,10\},\{3\},\{6,7\}\Big\}$$

of the set $X = \{1,2,3,\ldots,10\}$ considered earlier. What is the associated equivalence relation? Two elements of X are equivalent if and only if they lie in the same block of the partition. Thus $4 \sim 8$, $2 \sim 10$, $3 \sim 3$, $7 \sim 6$, etc., while $5 \not\sim 3$, $6 \not\sim 2$, etc.

Proposition 1.15. *As above let X be a set and let $\mathcal{C}$ be a partition of X. The relation $\sim$ on X defined by*

$$a \sim b \iff \textit{(the block containing } a) = \textit{(the block containing } b).$$

is an equivalence relation.

Exercise 1.16. Define a relation on μ_{10} by

$$z_1 \sim z_2 \iff \text{(the order of } z_1) = \text{(the order of } z_2).$$

Verify that $\sim$ is an equivalence relation, and determine the associated partition of μ_{10} (this means write down the blocks of the partition explicitly).

Exercise 1.17. Define a relation on μ_{10} by

$$z_1 \sim z_2 \iff \text{(the order of } z_1^4) = \text{(the order of } z_2^4).$$

Verify that $\sim$ is an equivalence relation, and determine the associated partition of μ_{10}.

Exercise 1.18. Let $f : X \to Y$ be a function, and for every $y \in Y$ let $A_y = f^{-1}(\{y\})$. The set A_y is called the *fiber* over y. Prove that $\{A_y : y \in Y \text{ and } A_y \neq \emptyset\}$ is a partition of X.

Exercise 1.19. Define a relation $\sim$ on $\mathbb{R} \times \mathbb{R}$ by setting $(a,b) \sim (c,d)$ if there is a nonzero real number λ such that $(a,b) = (\lambda c, \lambda d)$. Prove that $\sim$ is an equivalence relation.

Exercise 1.20. Let $M_2(\mathbb{R})$ denote the set of 2×2 matrices with real entries. We say that two matrices $A, B \in M_2(\mathbb{R})$ are *similar* if there is an invertible matrix T such that $AT = TB$. Show that similarity of matrices is an equivalence relation.

Exercise 1.21. If $a \equiv b \pmod{n}$, prove that $\gcd(a,n) = \gcd(b,n)$.

2. The Chinese Remainder Theorem

The idea behind the Chinese Remainder Theorem is best illustrated by an example. Suppose our goal is to find a number $z \in \mathbb{Z}$ that satisfies the pair of congruences

$$z \equiv 5 \pmod 7$$
$$z \equiv 3 \pmod 9.$$

Let's suppose we have a solution, z, and see what it might look like. The two congruences above imply that there are $a, b \in \mathbb{Z}$ such that

$$z = 5 + 7a$$
$$z = 3 + 9b,$$

and so $7a + 5 = 9b + 3$. If we rewrite this equality as

$$7a + 9(-b) = -2$$

then we are in a situation familiar to us from our earlier discussion of Euclid's algorithm. In fact, as $\gcd(7, 9) = 1$ we know that this equation must have a solution, and it isn't hard to find one. Using Euclid's algorithm we first find

$$7(4) + 9(-3) = 1,$$

and multiplying by -2 gives

$$7(-8) + 9(6) = -2.$$

Thus if we set

$$a = -8 \qquad b = -6$$

we have the desired relation $7a + 9(-b) = -2$. Now just undo the reasoning that got us here. If we let

$$z = 5 + 7a = 5 + 7 \cdot (-8) = -51$$
$$z = 3 + 9b = 3 + 9 \cdot (-6) = -51$$

then we arrive at the solution

$$-51 \equiv 5 \pmod 7$$
$$-51 \equiv 3 \pmod 9.$$

Can we use this processes to solve *any* pair of congruences? Not quite. It was important for the argument that $\gcd(7, 9) = 1$. The Chinese Remainder Theorem generalizes this argument.

Theorem 2.1 (Chinese Remainder Theorem)**.** *Suppose we are given $m, n \in \mathbb{Z}^+$ and $c, d \in \mathbb{Z}$. If $\gcd(m, n) = 1$ then there is a $z \in \mathbb{Z}$ satisfying*

$$z \equiv c \pmod m$$
$$z \equiv d \pmod n.$$

Proof. The proof is essentially contained in the example above. As $\gcd(m, n) = 1$ there are $x, y \in \mathbb{Z}$ satisfying $mx + ny = d - c$. Now rewrite this equality as $mx + c = -ny + d$, and let z be the common value of the two sides:

$$z = mx + c$$
$$z = -ny + d.$$

From these two equalities we see that $z - c$ is divisible by m, and that $z - d$ is divisible n. Hence

$$\begin{aligned} z &\equiv c \pmod{m} \\ z &\equiv d \pmod{n}. \end{aligned}$$

□

Now reconsider the example

$$\begin{aligned} z &\equiv 5 \pmod{7} \\ z &\equiv 3 \pmod{9}. \end{aligned}$$

Having found the solution

$$\begin{aligned} -51 &\equiv 5 \pmod{7} \\ -51 &\equiv 3 \pmod{9} \end{aligned} \tag{2.1}$$

we can ask for *all* solutions. I claim that for any $z \in \mathbb{Z}$

$$\begin{array}{l} z \equiv 5 \pmod{7} \\ z \equiv 3 \pmod{9} \end{array} \iff z \equiv -51 \pmod{63}. \tag{2.2}$$

First we prove the implication ($\Longleftarrow$). Suppose $z \equiv -51 \pmod{63}$. Then $z + 51$ is a multiple of $63 = 7 \cdot 9$, which implies that $z + 51$ is a multiple both of 7 and of 9. Therefore

$$\begin{aligned} z &\equiv -51 \pmod{7} \\ z &\equiv -51 \pmod{9}. \end{aligned}$$

Now using (2.1) and the transitivity of $\equiv$, we deduce

$$\begin{aligned} z &\equiv 5 \pmod{7} \\ z &\equiv 3 \pmod{9}. \end{aligned}$$

Now for the implication ($\Longrightarrow$). Suppose

$$\begin{aligned} z &\equiv 5 \pmod{7} \\ z &\equiv 3 \pmod{9}. \end{aligned}$$

Using the transitivity of $\equiv$ we find

$$\begin{array}{r} z \equiv 5 \pmod{7} \\ -51 \equiv 5 \pmod{7} \end{array} \Longrightarrow z \equiv -51 \pmod{7}.$$

and

$$\begin{array}{r} z \equiv 3 \pmod{9} \\ -51 \equiv 3 \pmod{9} \end{array} \Longrightarrow z \equiv -51 \pmod{9}.$$

These congruences imply that $z + 51$ is divisible by both 7 and 9. As $z + 51$ is a common multiple of 7 and 9, it is a multiple of

$$\operatorname{lcm}(7, 9) = \frac{63}{\gcd(7, 9)} = 63.$$

We have now proved that $z + 51$ is a multiple 63, and so $z \equiv -51 \pmod{63}$. Going back to the original problem

$$\begin{array}{l} z \equiv 5 \pmod{7} \\ z \equiv 3 \pmod{9} \end{array} \iff z \equiv -51 \pmod{63}$$

$$\begin{aligned}&\iff z \in \{\dots, -114, -51, 12, 75, \dots\}\\ &\iff z \in \{63q + 12 : q \in \mathbb{Z}\}.\end{aligned}$$

Theorem 2.2. *Suppose we are given $m, n \in \mathbb{Z}^+$ and $c, d \in \mathbb{Z}$. If $\gcd(m, n) = 1$ and we have found a $z_0 \in \mathbb{Z}$ such that*

$$\begin{aligned}z_0 &\equiv c \pmod{m}\\ z_0 &\equiv d \pmod{n}\end{aligned}$$

then for any $z \in \mathbb{Z}$

$$\begin{matrix} z \equiv c \pmod{m} \\ z \equiv d \pmod{n} \end{matrix} \iff z \equiv z_0 \pmod{mn}.$$

Proof. We first prove ($\Longleftarrow$). Suppose that $z \equiv z_0 \pmod{mn}$. Then mn divides $z - z_0$, which implies that both m and n divide $z - z_0$. Therefore

$$\begin{aligned}z &\equiv z_0 \pmod{m}\\ z &\equiv z_0 \pmod{n}.\end{aligned}$$

Of course by hypothesis

$$\begin{aligned}z_0 &\equiv c \pmod{m}\\ z_0 &\equiv d \pmod{n},\end{aligned}$$

and so the transitivity of $\equiv$ implies that

$$\begin{aligned}z &\equiv c \pmod{m}\\ z &\equiv d \pmod{n}.\end{aligned}$$

Now we prove ($\Longrightarrow$). Assume that

$$\begin{aligned}z &\equiv c \pmod{m}\\ z &\equiv d \pmod{n}.\end{aligned}$$

By hypothesis we have

$$\begin{aligned}z_0 &\equiv c \pmod{m}\\ z_0 &\equiv d \pmod{n},\end{aligned}$$

and so by the transitivity of $\equiv$ we deduce that

$$\begin{aligned}z &\equiv z_0 \pmod{m}\\ z &\equiv z_0 \pmod{n}.\end{aligned}$$

This implies that $z - z_0$ is a multiple of both m and n, and so $z - z_0$ is a multiple of the least common multiple

$$\operatorname{lcm}(m, n) = \frac{mn}{\gcd(m, n)} = mn.$$

But if $z - z_0$ is a multiple of mn then $z \equiv z_0 \pmod{mn}$. □

Exercise 2.3. Find all solutions to the pair of congruences

$$\begin{aligned}z &\equiv 38 \pmod{60}\\ z &\equiv 7 \pmod{11}.\end{aligned}$$

Exercise 2.4. Find all $z \in \mathbb{Z}$ satisfying the congruences

$$\begin{aligned} z &\equiv 1 \pmod 5 \\ z &\equiv 2 \pmod 7 \\ z &\equiv 3 \pmod 9. \end{aligned}$$

Exercise 2.5. Use the Chinese Remainder Theorem to find the smallest positive *odd* integer n so that n has a remainder of 11 when divided by 13, and a remainder of 14 when divided by 17.

Exercise 2.6. A band of 17 pirates has stolen a chest of gold coins. When they try to divide the coins into equal portions, 3 coins are left over. In the ensuing brawl over what to do with the remaining coins, 1 pirate is thrown overboard. The remaining 16 pirates again attempt to divide the coins into equal portions, but this time there are 10 coins left over. In the ensuing brawl over what to do with the remaining coins, another pirate is thrown overboard. The remaining 15 pirates attempt to divide the coins evenly, and this time they are successful. What is the least number of coins that could be in the pirates' chest?

3. Arithmetic in $\mathbb{Z}/n\mathbb{Z}$

To avoid ambiguity, we use the notation $[a]_n = \{x \in \mathbb{Z} : x \equiv a \pmod n\}$ for the congruence class of a modulo n. For example $[3]_5 = \{\dots, -2, 3, 8, \dots\}$.

Definition 3.1. For any $n \in \mathbb{Z}^+$ define

$$\mathbb{Z}/n\mathbb{Z} = \{[a]_n : a \in \mathbb{Z}\}.$$

For example $\mathbb{Z}/5\mathbb{Z} = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$. In order to fully understand the structure of $\mathbb{Z}/n\mathbb{Z}$ we must make a digression on the meaning of the phrase "well-defined." This is best done by example.

Example 3.2. Define a function $f : \mathbb{Q} \to \mathbb{Z}$ by $f(a/b) = b$. There is something wrong with the previous sentence. On the one hand $f(1/2) = 2$. On the other hand $f(2/4) = 4$. But $1/2 = 2/4$, so $2 = f(1/2) = f(2/4) = 4$. What happened? The definition of f is ambiguous. There is more than one way to express a given rational number in the form a/b, and the definition of f depends on which expression one chooses. In such a situation we say that f is *not well-defined*. As a result, the first sentence simply fails to define a function. There is no such function f.

Example 3.3. Define a function $f : \mathbb{R} \to \mathbb{Z}$ as follows: for $x \in \mathbb{R}$ we define $f(x)$ to be the first digit to the right of the decimal point in the decimal expansion of x. As with the previous example, this definition is bogus: the number 1 has two decimal expansions, $1 = 1.00\dots$ and $1 = 0.99\dots$. So is $f(1) = 0$ or is $f(1) = 9$? The rule defining f is ambiguous, and there simply is no such function. This f is not well-defined.

The issues in the previous two examples show up all the time when dealing with $\mathbb{Z}/n\mathbb{Z}$. For example, suppose we try to define $f : \mathbb{Z}/8\mathbb{Z} \to \mathbb{R}$ by

$$f([a]_8) = 3^a.$$

This simply doesn't make sense: for example $[2]_8 = [10]_8$, so what is $f([2]_8)$? Is it 3^2 or is it 3^{10}? The definition is ambiguous, and f is not well-defined. *There is no such function!* But, we can define $f : \mathbb{Z}/8\mathbb{Z} \to \mathbb{C}$ by

$$f([a]_8) = i^a.$$

This is ok. If $[a]_8 = [a']_8$, then $a \equiv a' \pmod 8$, and so there is a $q \in \mathbb{Z}$ such that $a = a' + 8q$. Therefore

$$i^a = i^{a'+8q} = i^{a'} \cdot i^{8q} = i^{a'},$$

where the last equality follows from $i^4 = 1$. This f *is* well-defined, since

$$[a]_8 = [a']_8 \implies i^a = i^{a'}.$$

Example 3.4. Suppose we try to define

$$f : \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \to \mathbb{C}$$

by

$$f([a]_5, [b]_5) = e^{2\pi i(a+b)/5}.$$

I claim this is well-defined. To see this suppose $([a]_5, [b]_5) = ([a']_5, [b']_5)$. Then $[a]_5 = [a']_5$ and $[b]_5 = [b']_5$. Therefore $a \equiv a' \pmod 5$ and $b \equiv b' \pmod 5$, and so there are $s, t \in \mathbb{Z}$ such that $a = a' + 5s$ and $b = b' + 5t$. This implies

$$e^{2\pi i(a+b)/5} = e^{2\pi i(a'+5s+b'+5t)/5} = e^{2\pi i(a'+b')/5} \cdot e^{2\pi i(s+t)} = e^{2\pi i(a'+b')/5}$$

Note that the last equality follows from $e^{2\pi i(s+t)} = 1$, as $e^{2\pi i k} = 1$ for any $k \in \mathbb{Z}$. To be clear: to verify that f is well-defined we had to check that

$$([a]_5, [b]_5) = ([a']_5, [b']_5) \implies e^{2\pi i(a+b)/5} = e^{2\pi i(a'+b')/5}.$$

The following proposition is really just a restatement of Proposition 1.8.

Proposition 3.5. *Fix an* $n \in \mathbb{Z}^+$.

(a) *The function*

$$\oplus : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

defined by $[a]_n \oplus [b]_n = [a + b]_n$ *is well-defined.*

(b) *The function*

$$\odot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

defined by $[a]_n \odot [b]_n = [a \cdot b]_n$ *is well-defined.*

The two functions $\oplus$ and $\odot$ just defined are called *addition* and *multiplication*, respectively. In practice we'll just write $+$ and $\cdot$ instead of $\oplus$ and $\odot$, so that addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ are defined by

$$[a]_n + [b]_n = [a + b]_n \qquad [a]_n \cdot [b]_n = [a \cdot b]_n.$$

For $k \in \mathbb{Z}^{\geq 0}$ we may now define

$$[a]_n^k = \underbrace{[a]_n \cdots [a]_n}_{k \text{ times}} = [\, \underbrace{a \cdots a}_{k \text{ times}} \,]_n = [a^k]_n.$$

What is $\mathbb{Z}/n\mathbb{Z}$ good for? Here are some simple examples.

Example 3.6. In grade school, you learned a rule to compute remainders after dividing by 3: the remainder when 46925 is divided by 3 is the same as the remainder of $4+6+9+2+5 = 26$, which is the same as the remainder of $2 + 6 = 8$ which is 2. Why does this work? Because $[10]_3 = [1]_3$, so

$$\begin{aligned}[46925]_3 &= [4 \cdot 10^4 + 6 \cdot 10^3 + 9 \cdot 10^2 + 2 \cdot 10 + 5]_3 \\ &= [4]_3 \cdot [10]_3^4 + [6]_3 \cdot [10]_3^3 + [9]_3 \cdot [10]_3^2 + [2]_3 \cdot [10]_3 + [5]_3\end{aligned}$$

$$\begin{aligned}&= [4]_3 + [6]_3 + [9]_3 + [2]_3 + [5]_3\\&= [4+6+9+2+5]_3\\&= [26]_3.\end{aligned}$$

Now repeat

$$\begin{aligned}[26]_3 &= [2\cdot 10 + 6]_3\\&= [2]_3\cdot[10]_3 + [6]_3\\&= [2]_3 + [6]_3\\&= [2+6]_3\\&= [8]_3.\end{aligned}$$

But of course $[8]_3 = [2]_3$, so $[46925]_3 = [2]_3$.

Example 3.7. In the spirit of the previous example, we can devise a test for divisibility by 11 by exploiting the fact that $[10]_{11} = [-1]_{11}$. Suppose we want to compute the remainder when 3624 is divided by 11. Here's what you do. Reverse the order of the digits, then add them together but alternate the signs in the sum, starting with a + sign in front: $4-2+6-3=5$. I claim that 5 is the remainder when 3624 is divided by 11. Why does this work? Because

$$\begin{aligned}[3624]_{11} &= [3\cdot 10^3 + 6\cdot 10^2 + 2\cdot 10 + 4]_{11}\\&= [3]_{11}\cdot[10]_{11}^3 + [6]_{11}\cdot[10]_{11}^2 + [2]_{11}\cdot[10]_{11} + [4]_{11}\\&= [3]_{11}\cdot[-1]_{11}^3 + [6]_{11}\cdot[-1]_{11}^2 + [2]_{11}\cdot[-1]_{11} + [4]_{11}\\&= [4]_{11} - [2]_{11} + [6]_{11} - [3]_{11}\\&= [4-2+6-3]_{11}\\&= [5]_{11}.\end{aligned}$$

Example 3.8. I claim there are no integers $x, y \in \mathbb{Z}$ satisfying $3x^2 - 5y^2 = 1$. Here's why: To get a contradiction, suppose there are such x and y. Then we can reduce everything modulo 5 to obtain $[3x^2 - 5y^2]_5 = [1]_5$. As $[5]_5 = [0]_5$, this simplifies to $[3]_5 \cdot [x]_5^2 = [1]_5$. But $\mathbb{Z}/5\mathbb{Z}$ has only five elements, and we can check by brute force that none of those elements satisfy the stated equation:

$$\begin{aligned}[3]_5\cdot[0]_5^2 &= [0]_5\\ [3]_5\cdot[1]_5^2 &= [3]_5\\ [3]_5\cdot[2]_5^2 &= [2]_5\\ [3]_5\cdot[3]_5^2 &= [2]_5\\ [3]_5\cdot[4]_5^2 &= [3]_5.\end{aligned}$$

This is a contradiction. In other words, $3x^2 - 5y^2 = 1$ has no solutions in $\mathbb{Z}/5\mathbb{Z}$, so it has no solutions in $\mathbb{Z}$.

Example 3.9. What is the remainder when $\sum_{k=1}^{100} k!$ is divided by 6? We argue as follows. If $k \geq 6$ then $k! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdots k$ is clearly divisible by 6, so $[k!]_6 = [0]_6$. This allows us to simplify

$$[1!]_6 + [2!]_6 + \cdots + [100!]_6 = [1!]_6 + [2!]_6 + [3!]_6 + [4!]_6 + [5!]_6.$$

But each of 3!, 4!, and 5! is divisible by both 2 and 3, and so are each are divisible by 6. This leaves

$$[1!]_6 + [2!]_6 + \cdots + [100!]_6 = [1!]_6 + [2!]_6 = [3]_6.$$

So the remainder is 3.

Example 3.10. What is the remainder when 5^{335} is divided by 13? Working in $\mathbb{Z}/13\mathbb{Z}$, first note that $[5^2] = [25] = [-1]$. Squaring both sides of $[5^2] = [-1]$ shows that $[5^4] = [1]$. Now use the division algorithm to write $335 = 4 \cdot 83 + 3$, and compute

$$\begin{aligned} [5^{335}] &= [5^4]^{83} \cdot [5]^3 \\ &= [5]^3 \\ &= [5]^2 \cdot [5] \\ &= [-1] \cdot [5] \\ &= [-5] \\ &= [8]. \end{aligned}$$

So the remainder is 8.

It's possible to prove the following proposition using induction, but doing so is more confusing than it is helpful. Your best bet is just to think about it until it's obvious.

Proposition 3.11 (The Pigeonhole Principle)**.** *Suppose we are given finite sets A and B of cardinality $|A|$ and $|B|$, respectively. Let $f : A \to B$ be any function.*

(a) *If f is injective then $|A| \leq |B|$.*
(b) *If f is surjective then $|A| \geq |B|$.*
(c) *If f is bijective then $|A| = |B|$.*
(d) *If $|A| = |B|$ then f is injective if and only if f is surjective.*

Consider the function $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ defined by $f([z]_6) = ([z]_2, [z]_3)$. First, we should check that this is well-defined: if $[z]_6 = [z']_6$ then $z \equiv z' \pmod 6$ and so there is a $q \in \mathbb{Z}$ such that $z = z' + 6q$. This equality implies

$$\begin{aligned} z &\equiv z' \pmod 2 \\ z &\equiv z' \pmod 3 \end{aligned}$$

and so $[z]_2 = [z']_2$ and $[z]_3 = [z']_3$. Therefore

$$[z]_6 = [z']_6 \implies ([z]_2, [z]_3) = ([z']_2, [z']_3)$$

and f is well-defined. By tabulating the values of f

$$\begin{aligned} f([0]_6) &= ([0]_2, [0]_3) \\ f([1]_6) &= ([1]_2, [1]_3) \\ f([2]_6) &= ([0]_2, [2]_3) \\ f([3]_6) &= ([1]_2, [0]_3) \\ f([4]_6) &= ([0]_2, [1]_3) \\ f([5]_6) &= ([1]_2, [2]_3) \end{aligned}$$

we see that f is a bijection.

Suppose we instead define $f : \mathbb{Z}/100\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ by

$$f([z]_{100}) = ([z]_4, [z]_{25}).$$

Is this still a well-defined bijection? You can check that this is well-defined by the same argument just used, but if we want to prove that f is bijective we'll need a method better than tabulating all values of f by brute force. The better method is to use the Chinese Remainder Theorem to prove that f is surjective, and then invoke the Pigeonhole Principle to show that f is also injective. To illustrate the method let's try to find a $[z]_{100} \in \mathbb{Z}/100\mathbb{Z}$ satisfying

$$f([z]_{100}) = ([3]_4, [12]_{25}).$$

Using the methods of the previous section, the congruences

$$\begin{aligned} z &\equiv 3 \pmod 4 \\ z &\equiv 12 \pmod{25} \end{aligned}$$

are equivalent to the single congruence

$$z \equiv -213 \pmod{100}.$$

As $87 \equiv -213 \pmod{100}$, we deduce

$$\begin{aligned} 87 &\equiv 3 \pmod 4 \\ 87 &\equiv 12 \pmod{25} \end{aligned}$$

and so

$$f([87]_{100}) = ([87]_4, [87]_{25}) = ([3]_4, [12]_{25}).$$

This argument can be generalized to prove that f is surjective. Fix a $([c]_4, [d]_{25}) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$. By the Chinese Remainder Theorem, there is a $z \in \mathbb{Z}$ satisfying

$$\begin{aligned} z &\equiv c \pmod 4 \\ z &\equiv d \pmod{25}, \end{aligned}$$

and so

$$f([z]_{100}) = ([z]_4, [z]_{25}) = ([c]_4, [d]_{25}).$$

This proves that f is surjective, and as the domain and codomain of f each have $100 = 4 \cdot 25$ elements, f is injective as well, by the Pigeonhole Principle.

Proposition 3.12 (Chinese Remainder Theorem II). *Suppose $m, n \in \mathbb{Z}^+$ are relatively prime. The function*

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

defined by $f([z]_{mn}) = ([z]_m, [z]_n)$ is well-defined, and is a bijection.

Exercise 3.13. Prove that $3x^3 - 7y^3 + 21z^3 = 2$ has no integer solutions.

Exercise 3.14. Determine if each of the following functions is well-defined. For those that are well-defined, determine if they are injective, surjective, both, or neither:

(a) $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ defined by $f([x]_2) = [3x]_4$
(b) $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ defined by $f([x]_2) = [2x]_4$
(c) $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$ defined by $f([a]_5) = [a^2]_{15}$
(d) $f : \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ defined by $f([a]_{15}) = ([a]_3, [a]_3)$
(e) $f : \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \to \mu_3$ defined by $f([a]_6, [b]_{15}) = e^{2\pi i(a+b)/3}$

(f) $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$ defined by $f([x]_3) = [x^3]_9$.

Exercise 3.15. Suppose $m, n \in \mathbb{Z}^+$.

(a) Prove that the rule $f([a]_{mn}) = ([a]_m, [a]_n)$ determines a well-defined function $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m \times \mathbb{Z}/n\mathbb{Z}$.

(b) Find an example of m and n for which the function in part (a) is not a bijection.

Exercise 3.16. Suppose $m, n \in \mathbb{Z}^+$ with $m \mid n$. Prove that the function

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

defined by $f([a]_n) = [a]_m$ is well-defined. Is it injective? Surjective? Prove or give a counterexample.

Exercise 3.17. Consider the bijection

$$f : \mathbb{Z}/150\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$$

defined by $f([z]_{150}) = ([z]_3, [z]_{50})$ Find the unique $[z]_{150} \in \mathbb{Z}/150\mathbb{Z}$ such that $f([z]_{150}) = ([2]_3, [48]_{50})$.

Exercise 3.18. What is the remainder when $1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$ is divided by 4?

Exercise 3.19. Prove that $53^{103} + 103^{53}$ is divisible by 39, and that $111^{333} + 333^{111}$ is divisible by 7.

Exercise 3.20. Prove that $7^{100} \equiv 1 \pmod 5$ and $7^{100} \equiv 1 \pmod 6$. Deduce that $7^{100} \equiv 1 \pmod{30}$.

Exercise 3.21. Prove that $5^{2n} + 13^n - 2$ is divisible by 3 for every $n \in \mathbb{Z}^+$.

Exercise 3.22. Prove that there are infinitely many primes congruent to -1 modulo 4. Hint: suppose there are only finitely many and call them $p_1, \ldots, p_k$. Now show that $N = 4p_1 \cdots p_k - 1$ has a prime factor $q \equiv -1 \pmod 4$ not found in the list $p_1, \ldots, p_k$.

Exercise 3.23. Consider the function $f : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ defined by $f(x) = [2x]$.

(a) What is the image of f?

(b) Compute $f^{-1}(B)$ for each of

$$B = \{[0]\} \qquad B = \{[1], [2]\} \qquad B = \{[0], [2]\} \qquad B = \{[0], [2], [4]\}.$$

(c) Compute $f(A)$ for each of

$$A = \mathbb{Z}^+ \qquad A = \{x \in \mathbb{Z} : x \text{ is even}\} \qquad A = \{x \in \mathbb{Z} : x \text{ is odd}\}.$$

Exercise 3.24.

(a) Consider $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$ defined by

$$f([a]_3) = [a^3]_9.$$

Prove that this function is well-defined.

(b) Consider $f : \mathbb{Z}/3\mathbb{Z} \to \mu_9$ defined by

$$f([a]_3) = e^{2\pi i a^3/9}.$$

Prove that this function is well-defined.

Exercise 3.25. Suppose we have functions $f : A \to A$, and $g : A \to A$. Suppose in addition that $f \circ g : A \to A$ is a bijection.

(a) Assuming that A is finite, prove that f and g are both bijections.

(b) Show by example that if A is infinite then f and g need not be bijections.

4. Rings and the units of $\mathbb{Z}/n\mathbb{Z}$

Definition 4.1. A *ring* is an ordered triple $(R, +, \cdot)$ in which R is a set and

$$+ : R \times R \to R$$

and

$$\cdot : R \times R \to R$$

are functions satisfying the following properties:

(a) $a + b = b + a$ for all $a, b \in R$,
(b) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$,
(c) there is an element $0_R \in R$, called the *additive identity*, satisfying $a + 0_R = a$ for all $a \in R$,
(d) for every $a \in R$ there is an element $-a \in R$, called the *additive inverse of* a, such that $a + (-a) = 0_R$,
(e) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$,
(f) for all $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

We usually just say “Let R be a ring” instead of the cumbersome “Let $(R, +, \cdot)$ be a ring.” Note the properties that are not included as axioms. We do not assume that multiplication is commutative: it is possible that $a \cdot b \neq b \cdot a$. We do not assume that there is a multiplicative identity $1_R \in R$ (see below), and we do not assume that elements $a \in R$ have multiplicative inverses: in general a^{-1} has no meaning (but see below). We also do not assume that R has a cancellation law: in general $ab = ac$ does *not* imply $b = c$.

Definition 4.2. A *commutative ring* is a ring R satisfying $ab = ba$ for all $a, b \in R$.

Definition 4.3. A *ring with* 1 is a ring R possessing a multiplicative identity: an element $1_R \in R$ satisfying $a \cdot 1_R = a = 1_R \cdot a$ for every $a \in R$.

Example 4.4. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}/n\mathbb{Z}$ with the usual notions of $+$ and $\cdot$ are all commutative rings with 1.

The ring $\mathbb{Z}/6\mathbb{Z}$ provides a good example of the failure of cancellation to hold: in $\mathbb{Z}/6\mathbb{Z}$ we have

$$[2]_6 \cdot [4]_6 = [2]_6 \cdot [1]_6,$$

but, obviously, you cannot cancel the $[2]_6$ to deduce that $[4]_6 = [1]_6$.

Example 4.5. If R is any ring and $n \in \mathbb{Z}^+$ we define $M_n(R)$ to be the set of all $n \times n$ matrices with entries in R. Then $M_n(R)$ is a ring under the usual addition and multiplication of matrices. If R is a ring with 1 then so is $M_n(R)$. The multiplicative identity in $M_n(R)$ is the matrix

$$I_n = \begin{pmatrix} 1_R & & & \\ & 1_R & & \\ & & \ddots & \\ & & & 1_R \end{pmatrix}$$

with 1_R along the diagonal and 0_R in all other entries. The ring $M_n(R)$ is not commutative (at least if $n > 1$).

Example 4.6. Suppose R is a commutative ring with 1. We denote by $R[x]$ the ring of all polynomials with coefficients in R. So $\mathbb{R}[x]$ is the ring of polynomials with real coefficients, $\mathbb{Q}[x]$ is the ring of polynomials with rational coefficients, etc....

Example 4.7. The set $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ of even integers is a commutative ring under the usual addition and multiplication, but is not a ring with 1.

Example 4.8. The set $\mathbb{Z}^+$ with its usual addition and multiplication is not a ring, as it has no additive identity. Even though $\mathbb{Z}^{\geq 0}$ has an additive identity, it is still not a ring. For example 3 has no additive inverse in $\mathbb{Z}^{\geq 0}$. Similarly $\mathbb{R}^{\geq 0}$ is not a ring.

In all that follows, R is a ring.

Proposition 4.9. *For every $a \in R$ we have $a \cdot 0_R = 0_R = 0_R \cdot a$.*

One of the ring axioms asserts the existence of an additive identity 0_R, but there is no axiom saying that R cannot have more than one additive identity. Is it possible for R to have two distinct additive identities? According to the following lemma, no.

Lemma 4.10. *If 0_R and $0_R'$ are additive identities of R then $0_R = 0_R'$.*

Lemma 4.11. *Suppose $a \in R$ and $b, c \in R$ are additive inverses of a. Then $b = c$.*

Definition 4.12. Let R be a ring with 1. An element $a \in R$ is a *unit* if there is an $a^{-1} \in R$, called the *multiplicative inverse* of a, satisfying

$$a \cdot a^{-1} = 1_R = a^{-1} \cdot a.$$

The set of all units in R is denoted $R^\times$.

Example 4.13.

(a) As every nonzero real number has a multiplicative inverse, $\mathbb{R}^\times = \mathbb{R} \smallsetminus \{0\}$.
(b) Similarly, if $z \in \mathbb{C}$ is nonzero then $z^{-1} = \overline{z}/|z|^2$ is a multiplicative inverse of z, so $\mathbb{C}^\times = \mathbb{C} \smallsetminus \{0\}$.
(c) The units in $\mathbb{Z}$ are $\mathbb{Z}^\times = \{\pm 1\}$.
(d) From linear algebra we know that

$$M_n(\mathbb{R})^\times = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}.$$

Lemma 4.14. *If 1_R and $1_R'$ are multiplicative identities of R then $1_R = 1_R'$.*

Lemma 4.15. *Suppose R is a ring with 1 and $a \in R$ is a unit. Then the multiplicative inverse of a is unique.*

Proposition 4.16 (Cancellation law for units)**.** *Suppose R is a ring with 1, and that $a, b \in R$ and $c \in R^\times$. Then*

$$ca = cb \iff a = b.$$

Similarly

$$ac = bc \iff a = b.$$

Our next task is to determine the set $(\mathbb{Z}/n\mathbb{Z})^\times$. Let's start by examining $\mathbb{Z}/10\mathbb{Z}$. Is $[2]_{10}$ a unit? Suppose $[2]_{10}$ has a multiplicative inverse, say $[2]_{10} \cdot [x]_{10} = [1]_{10}$. This implies $2x \equiv 1 \pmod{10}$, and so $2x = 1 + 10q$ for some $q \in \mathbb{Z}$. But then $1 = 2(x - 5q)$ shows that 1 is a multiple of 2, a contradiction. So $[2]_{10} \notin (\mathbb{Z}/10\mathbb{Z})^\times$. What about $[7]_{10}$? This is a unit, and we can find its multiplicative inverse as follows. First we use Euclid's algorithm to solve

$$7x + 10y = 1.$$

This is possible as $\gcd(7, 10) = 1$, and by the usual method we compute

$$7 \cdot 3 - 10 \cdot 2 = 1.$$

Now reduce modulo 10 to obtain $[7]_{10} \cdot [3]_{10} = [1]_{10}$. Thus $[7]_{10}^{-1} = [3]_{10}$.

Proposition 4.17. *Fix $n \in \mathbb{Z}^+$. For every $a \in \mathbb{Z}$*

$$[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \gcd(a, n) = 1.$$

Corollary 4.18. *If p is a prime then*

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{[1]_p, [2]_p, \ldots, [p-1]_p\}.$$

The use of multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$ allows us to solve some simple types of congruences. for example, suppose we want to find all $x \in \mathbb{Z}$ such that

$$9x \equiv 4 \pmod{22}.$$

Noting that $\gcd(9, 22) = 1$, we use Euclid's algorithm to find that

$$9x + 22y = 1$$

has $x = 5$, $y = -2$ as a solution. By reducing the equality $9 \cdot 5 - 22 \cdot 2 = 1$ modulo 22 we find $[9]_{22} \cdot [5]_{22} = [1]_{22}$. Thus $[9]_{22}^{-1} = [5]_{22}$, and from this it follows that

$$[9]_{22} \cdot [x]_{22} = [4]_{22} \iff [x]_{22} = [5]_{22} \cdot [4]_{22}.$$

Thus

$$9x \equiv 4 \pmod{22} \iff x \equiv 20 \pmod{22}.$$

Exercise 4.19.

(a) Compute the multiplicative inverse of $[17] \in \mathbb{Z}/21\mathbb{Z}$, if it exists.
(b) Compute the multiplicative inverse of $[35] \in \mathbb{Z}/97\mathbb{Z}$, if it exists.
(c) Find all $x \in \mathbb{Z}$ satisfying $35x \equiv 7 \pmod{97}$.

Exercise 4.20.

(a) List the elements of $(\mathbb{Z}/9\mathbb{Z})^\times$ and $(\mathbb{Z}/27\mathbb{Z})^\times$.
(b) Suppose p is a prime and $n \in \mathbb{Z}^+$. Find a formula for $|(\mathbb{Z}/p^n\mathbb{Z})^\times|$.

Exercise 4.21. Find all solutions to the system of congruences

$$\begin{aligned} 3x &\equiv 7 \pmod{8} \\ 12x &\equiv -2 \pmod{17} \\ -5x &\equiv 1 \pmod{9}. \end{aligned}$$

Exercise 4.22. Fix $p \in \mathbb{Z}^+$.

(a) Suppose p is prime and $x^2 \equiv 1 \pmod{p}$. Prove that $x \equiv \pm 1 \pmod{p}$.

(b) Show by example that the previous statement is false without the hypothesis that p is prime.

Exercise 4.23. Prove *Wilson's theorem*: if p is a prime then

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

Hint: look for cancellation in the product $[1]\cdot[2]\cdot[3]\cdots[p-1]$.

5. Fermat's Little Theorem

Let R be a ring with 1.

Lemma 5.1. *If $a, b \in R^\times$ then $ab \in R^\times$.*

Fix a $u \in R^\times$. By the preceding lemma $x \in R^\times \implies ux \in R^\times$, so we may define a function "multiplication by u"

$$\mathrm{mult}_u : R^\times \to R^\times \tag{5.1}$$

by $\mathrm{mult}_u(x) = ux$.

Lemma 5.2. *For any $u \in R^\times$ the function $\mathrm{mult}_u : R^\times \to R^\times$ is a bijection.*

As $\gcd(3,7) = 1$ we have $[3] \in (\mathbb{Z}/7\mathbb{Z})^\times$, and Lemma 5.2 implies that the function

$$\mathrm{mult}_{[3]} : (\mathbb{Z}/7\mathbb{Z})^\times \to (\mathbb{Z}/7\mathbb{Z})^\times$$

defined by $\mathrm{mult}_{[3]}([x]) = [3x]$ is a bijection. This can also be seen by direct computation:

$$\begin{aligned}
\mathrm{mult}_{[3]}([1]) &= [3\cdot 1] = [3] \\
\mathrm{mult}_{[3]}([2]) &= [3\cdot 2] = [6] \\
\mathrm{mult}_{[3]}([3]) &= [3\cdot 3] = [2] \\
\mathrm{mult}_{[3]}([4]) &= [3\cdot 4] = [5] \\
\mathrm{mult}_{[3]}([5]) &= [3\cdot 5] = [1] \\
\mathrm{mult}_{[3]}([6]) &= [3\cdot 6] = [4],
\end{aligned}$$

which makes it clear that multiplication by [3] simply permutes the elements of $(\mathbb{Z}/7\mathbb{Z})^\times$. This allows us to do the magical calculation

$$\begin{aligned}
&[3^6]\cdot[1]\cdot[2]\cdot[3]\cdot[4]\cdot[5]\cdot[6] \\
&\quad = \quad [3\cdot 1]\cdot[3\cdot 2]\cdot[3\cdot 3]\cdot[3\cdot 4]\cdot[3\cdot 5]\cdot[3\cdot 6] \\
&\quad = \quad [3]\cdot[6]\cdot[2]\cdot[5]\cdot[1]\cdot[4].
\end{aligned}$$

The final expression is just $[6!]$ written out of order, and so

$$[3^6]\cdot[6!] = [6!]. \tag{5.2}$$

Now reread Lemma 5.1. As $[1], \ldots, [6] \in (\mathbb{Z}/7\mathbb{Z})^\times$, we also have

$$[6!] = [1]\cdot[2]\cdot[3]\cdot[4]\cdot[5]\cdot[6] \in (\mathbb{Z}/7\mathbb{Z})^\times.$$

Multiplying both sides of (5.2) by $[6!]^{-1}$ results in

$$[3^6] = [1],$$

and we have proved (in an admittedly roundabout way)

$$3^6 \equiv 1 \pmod{7}.$$

This is a special case of the following result, known as Fermat's Little Theorem.

Theorem 5.3 (Fermat, 1640)**.** *Suppose p is a prime and a is an integer such that $p \nmid a$. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. As we assume $p \nmid a$, we have $\gcd(p, a) = 1$, and so $[a] \in (\mathbb{Z}/p\mathbb{Z})^\times$. Let

$$\mathrm{mult}_{[a]} : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

be the function "multiplication by $[a]$" defined by $\mathrm{mult}_{[a]}([x]) = [ax]$. By Lemma 5.2 this function is a bijection, and so multiplication by $[a]$ simply permutes the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$. In other words

$$\Big\{[a \cdot 1], [a \cdot 2], [a \cdot 3], \ldots, [a \cdot (p-1)]\Big\} = \Big\{[1], [2], [3], \ldots, [(p-1)]\Big\}.$$

If we multiply together all the elements in set on the left, then multiply together all the elements in set on the right, and then set the two results equal to one another we find

$$[a^{p-1}] \cdot [1] \cdot [2] \cdots [p-1] = [1] \cdot [2] \cdots [p-1]. \tag{5.3}$$

Lemma 5.1 implies that

$$[1] \cdot [2] \cdots [(p-1)] \in (\mathbb{Z}/p\mathbb{Z})^\times,$$

and multiplying both sides of (5.3) by the multiplicative inverse results in

$$[a^{p-1}] = [1].$$

Of course this is equivalent to $a^{p-1} \equiv 1 \pmod{p}$. □

Corollary 5.4. *Suppose p is a prime. For every $a \in \mathbb{Z}$*

$$a^p \equiv a \pmod{p}.$$

Lemma 5.5. *For any $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ there is a $d \in \mathbb{Z}^+$ such that $[a^d] = [1]$.*

Definition 5.6. The *order* of $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ is the smallest positive integer d such that $[a^d] = [1]$.

Proposition 5.7. *Suppose $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ has order d, and that $m \in \mathbb{Z}$. Then*

$$[a^m] = [1] \iff d \mid m.$$

Corollary 5.8. *If p is prime then every $[a] \in (\mathbb{Z}/p\mathbb{Z})^\times$ has order dividing $p - 1$.*

Corollary 5.8, which is really a restatement of the Little Fermat Theorem, can be used to compute the orders of elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ fairly quickly. For example, suppose we want to compute the order of $[8] \in (\mathbb{Z}/23\mathbb{Z})^\times$. By Corollary 5.8 the order must be a divisor of 22, and so is one of 1, 2, 11, or 22. It clearly isn't 1, as $[8^1] = [5]$. Similarly $[8^2] = [64] = [-5]$ shows that the order isn't 2. To compute $[8^{11}]$ we use the method of successive squaring: squaring both sides of $[8^2] = [-5]$ shows that

$$[8^4] = [8^2]^2 = [-5]^2 = [25] = [2],$$

and squaring both sides again shows that

$$[8^8] = [8^4]^2 = [2]^2 = [4].$$

From this we easily find

$$[8^{11}] = [8^8] \cdot [8^2] \cdot [8] = [4] \cdot [-5] \cdot [8] = [1].$$

Thus $[8]$ has order 11 in $(\mathbb{Z}/23\mathbb{Z})^\times$.

Exercise 5.9. Compute

(a) the order of $[5] \in (\mathbb{Z}/11\mathbb{Z})^\times$,
(b) the order of $[2] \in (\mathbb{Z}/17\mathbb{Z})^\times$,
(c) the order of $[5] \in (\mathbb{Z}/103\mathbb{Z})^\times$.

Exercise 5.10. Define a relation $\sim$ on $(\mathbb{Z}/15\mathbb{Z})^\times$ by $[a] \sim [b]$ if and only if the order of $[a]$ equals the order of $[b]$. Verify that $\sim$ is an equivalence relation, and write down the associated partition of $(\mathbb{Z}/15\mathbb{Z})^\times$.

Exercise 5.11. Define a relation $\sim$ on $(\mathbb{Z}/15\mathbb{Z})^\times$ by $[a] \sim [b]$ if and only if the order of $[a^2]$ equals the order of $[b^2]$. Verify that $\sim$ is an equivalence relation, and write down the associated partition of $(\mathbb{Z}/15\mathbb{Z})^\times$.

Exercise 5.12. Compute the order of every element of $(\mathbb{Z}/23\mathbb{Z})^\times$.

Exercise 5.13. Let p be a prime.

(a) Suppose $0 < k < p$. Use the relation

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

to prove $\binom{p}{k} \equiv 0 \pmod{p}$.

(b) Deduce $(x+y)^p \equiv x^p + y^p \pmod{p}$ for all $x, y \in \mathbb{Z}$.
(c) Use (b) and induction to prove $n^p \equiv n \pmod{p}$ for every $n \in \mathbb{Z}^+$.
(d) Use (c) to give a new proof of the Little Fermat Theorem.

Exercise 5.14. Suppose that p is a prime, and $a \equiv b \pmod{p}$. Prove that

$$a^p \equiv b^p \pmod{p^2}.$$

Hint: use the binomial theorem and the fact (see the previous exercise) that p divides the binomial coefficient $\binom{p}{k}$ for $0 < k < p$.

Exercise 5.15.

(a) If $\gcd(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$. Hint: first show

$$a^{12} \equiv 1 \pmod{5}$$
$$a^{12} \equiv 1 \pmod{7}.$$

(b) If $\gcd(a, 42) = 1$, show that $a^6 - 1$ is divisible by 168.
(c) If $\gcd(a, 133) = 1$ and $\gcd(b, 133) = 1$, show that $133 \mid (a^{18} - b^{18})$.

Exercise 5.16. Suppose p and q are distinct primes. Show that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Exercise 5.17. Suppose that p and q are distinct primes. Show that

$$pn^{q-1} + qn^{p-1} \equiv p + q \pmod{pq}$$

for every $n \in \mathbb{Z}$ with $\gcd(n, pq) = 1$.

Exercise 5.18. Prove that $11^{12n+6} + 1$ is divisible by 13 for every $n \in \mathbb{Z}^+$.

Exercise 5.19. Suppose p is an odd prime and k is an integer with $0 < k < p$. Prove that

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

CHAPTER V

Polynomial arithmetic

1. Integral domains and fields

Definition 1.1. The *trivial ring* is the ring $\{0\}$ consisting of a single element, 0, with addition and multiplication defined by $0 + 0 = 0$ and $0 \cdot 0 = 0$.

Note that the trivial ring is a ring with 1. The sole element 0 of the trivial ring is a multiplicative identity, since $0 \cdot a = a = a \cdot 0$ for every $a \in \{0\}$. The following proposition shows that the trivial ring is characterized as the unique ring with 1 in which $1_R = 0_R$.

Proposition 1.2. *Let R be a ring with 1. If $1_R = 0_R$, then R is the trivial ring.*

Definition 1.3. An *integral domain R* is a nontrivial commutative ring with 1, such that for all $a, b \in R$

$$ab = 0_R \implies a = 0_R \text{ or } b = 0_R.$$

The definition of integral domain may be restated by replacing the above implication by its contrapositive: an *integral domain R* is a nontrivial commutative ring with 1, such that for all $a, b \in R$

$$a \neq 0_R \text{ and } b \neq 0_R \implies ab \neq 0_R.$$

The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all integral domains. The ring $\mathbb{Z}/12\mathbb{Z}$ is not an integral domain, as $[3]_{12} \cdot [4]_{12} = [0]_{12}$. The ring $M_2(\mathbb{R})$ is not an integral domain for (at least) two reasons. First, it is not even commutative. Second,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Proposition 1.4 (Cancellation law)**.** *Let R be an integral domain and suppose $ab = ac$ for some $a, b, c \in R$. If $a \neq 0_R$ then $b = c$.*

Definition 1.5. A *field* is a nontrivial commutative ring with 1 in which every nonzero element has a multiplicative inverse.

For example, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields, but $\mathbb{Z}$ is not. If F is a nontrivial commutative ring with 1 then F is a field if and only if $F^\times = F \smallsetminus \{0_F\}$.

Proposition 1.6. *If F is a field then F is an integral domain.*

Proposition 1.7. *Suppose $p > 1$ is an integer. The following are equivalent:*

(*a*) *p is prime,*
(*b*) *$\mathbb{Z}/p\mathbb{Z}$ is a field,*
(*c*) *$\mathbb{Z}/p\mathbb{Z}$ is an integral domain.*

Let R be a commutative ring with 1, and recall that $R[x]$ denotes the ring of polynomials with coefficients in R. Every nonzero $f(x) \in R[x]$ can be written in the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $a_n \neq 0$. The nonnegative integer n is called the *degree* of f, and is denoted $\deg(f)$. By convention, the zero polynomial has degree $-\infty$. For any polynomial $f(x) \in R[x]$ we have $\deg(f) \in \{-\infty\} \cup \mathbb{Z}^{\geq 0}$.

Definition 1.8. Let R be a commutative ring with 1 and suppose $a(x), b(x) \in R[x]$. We say that $a(x)$ *divides* $b(x)$, and write $a(x) \mid b(x)$, if there is a $q(x) \in R[x]$ such that $b(x) = a(x) \cdot q(x)$.

In general the degree of polynomials is not terribly well-behaved. One would like to have a nice formula like

$$\deg(f \cdot g) = \deg(f) + \deg(g), \tag{1.1}$$

but this is false in general. For example in $(\mathbb{Z}/6\mathbb{Z})[x]$ we have

$$\begin{aligned}(3x^5+1)\cdot(4x^2+x) &= 12x^7 + 3x^6 + 4x^2 + x\\ &= 3x^6 + 4x^2 + x\end{aligned}$$

which has degree 6, not 7 (note that the coefficients here are in $\mathbb{Z}/6\mathbb{Z}$, so $12 = 0$; from now on, if it clear from the context that we are working in $(\mathbb{Z}/n\mathbb{Z})[x]$, we will write *e.g.* $3x^6 + 4x^2 + x$ instead of the clunky $[3]_n x^6 + [4]_n x^2 + [1]_n x$). It is clear that in the above example, (1.1) failed because the coefficients of x^5 and x^2 multiplied together to give 0, causing the x^7 term to disappear. This unpleasant phenomenon cannot happen if the coefficients lie in an integral domain.

Proposition 1.9. *If R is an integral domain and $f(x), g(x) \in R[x]$ then*

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

Corollary 1.10. *If R is an integral domain and $a(x), b(x) \in R[x]$ with $b(x) \neq 0$, then*

$$a(x) \mid b(x) \implies \deg(a) \leq \deg(b).$$

Corollary 1.11. *If R is an integral domain, then so is $R[x]$. In particular, if F is a field, then $F[x]$ is an integral domain.*

The integral domain $\mathbb{Z}$ can be enlarged into the field $\mathbb{Q}$ by allowing the formation of fractions. In a similar way, the integral domain $\mathbb{Q}[x]$ can be enlarged to a field by allowing quotients of polynomials such as

$$\frac{x^3 + 2x + 1}{(x^2-1)(3x+2)}.$$

Such quotients of polynomials are called *rational functions*. More generally, if F is any field, we denote by $F(x)$ the field of rational functions with coefficients in F. Thus

$$F(x) = \left\{ \frac{a(x)}{b(x)} : a(x), b(x) \in F[x] \text{ and } b(x) \neq 0 \right\}.$$

Exercise 1.12.

(a) Show that if R is an integral domain then $R^\times = R[x]^\times$ (in words: the units in $R[x]$ are precisely the units in R, viewed as constant polynomials).

(b) Find a unit in $(\mathbb{Z}/4\mathbb{Z})[x]$ of degree ≥ 1.

Exercise 1.13. Prove that every *finite* integral domain is a field. Hint: Let R be a finite integral domain. If $r \in R$ is nonzero, show that the function $\mathrm{mult}_r : R \to R$ defined by $\mathrm{mult}_r(x) = rx$ is a bijection. Why does this imply that $r \in R^\times$?

2. The division algorithm for polynomials

Theorem 2.1 (Division algorithm for polynomials)**.** *Suppose F is a field and $a(x), b(x) \in F[x]$ with $b(x) \neq 0$. There are unique $q(x), r(x) \in F[x]$ such that*

$$a(x) = b(x)q(x) + r(x)$$

and $\deg(r) < \deg(b)$.

Proof. First we prove the existence of $q(x)$ and $r(x)$. Define a subset of $F[x]$ by

$$S = \{a(x) - b(x)q(x) : q(x) \in F[x]\}.$$

Among all elements of S choose one of smallest degree, $r(x)$. In other words, $r(x) \in S$, and for any $s(x) \in S$ we have $\deg(r) \leq \deg(s)$ As $r(x) \in S$, there is some $q(x) \in F[x]$ such that $r(x) = a(x) - b(x)q(x)$. We must show that $\deg(r) < \deg(b)$. Suppose not, so that $\deg(r) \geq \deg(b)$, and write

$$\begin{aligned} r(x) &= r_m x^m + \cdots r_1 x + r_0 \\ b(x) &= b_n x^n + \cdots + b_1 x + b_0 \end{aligned}$$

with $r_m \neq 0$ and $b_n \neq 0$, so that $m = \deg(r)$ and $n = \deg(b)$. Recall we are assuming that $m \geq n$, and because F is a field $b_n \in F^\times$. Therefore we may consider the polynomial

$$\begin{aligned} r(x) - \frac{r_m}{b_n} x^{m-n} \cdot b(x) &= a(x) - b(x)q(x) - \frac{r_m}{b_m} x^{m-n} \cdot b(x) \\ &= a(x) - b(x)\left[q(x) - \frac{r_m}{b_n} x^{m-n}\right]. \end{aligned} \tag{2.1}$$

From the final expression, it is clear that (2.1) lies in S. Now look at the left hand side of (2.1). The term of highest degree in $r(x)$ is $r_m x^m$. The term of highest degree in $\frac{r_m}{b_n} x^{m-n} \cdot b(x)$ is

$$\frac{r_m}{b_n} x^{m-n} \cdot b_n x^n = r_m x^m.$$

When you subtract the two, the terms involving x^m cancel out, leaving only terms involving $x^{m-1}, x^{m-2}, \ldots, x, x^0$. Thus the polynomial (2.1) has degree strictly less than $m = \deg(r)$. We have now shown that (2.1) is a polynomial in S of degree strictly smaller than the degree of $r(x)$, contradicting the choice of $r(x)$. This contradiction shows that $\deg(r) < \deg(b)$.

Now for uniqueness. Suppose we have $r(x), q(x) \in F[x]$ and $r'(x), q'(x) \in F[x]$ satisfying

$$\begin{aligned} a(x) &= b(x)q(x) + r(x) \\ a(x) &= b(x)q'(x) + r'(x) \end{aligned}$$

and

$$\deg(r) < \deg(b) \qquad \deg(r') < \deg(b).$$

We want to show that $q(x) = q'(x)$ and $r(x) = r'(x)$. From

$$0_F = a(x) - a(x) = b(x) \cdot [q(x) - q'(x)] + [r(x) - r'(x)]$$

we see that

$$r(x) - r'(x) = b(x) \cdot [q'(x) - q(x)],$$

and so

$$\deg(r - r') = \deg(b) + \deg(q' - q).$$

As each of $r(x)$ and $r'(x)$ have degree strictly less than the degree of $b(x)$, we must have $\deg(r-r') < \deg(b)$. Therefore

$$\deg(q'-q) = \deg(r-r') - \deg(b) < 0.$$

The only way this can happen is if $\deg(q'-q) = -\infty$, and so $q'(x) - q(x) = 0_F$. From this it follows that $r'(x) - r(x) = 0_F$, and we have now shown that $q'(x) = q(x)$ and $r'(x) = r(x)$. □

Exercise 2.2. For each field F and each pair $a(x), b(x) \in F[x]$, find $q(x), r(x) \in F[x]$ such that $a(x) = b(x)q(x) + r(x)$ and $\deg(r) < \deg(b)$.

(a) $F = \mathbb{Q}$, $a(x) = x^5 + 2x^2 - 2$, $b(x) = x^3 + 7x + 1$.
(b) $F = \mathbb{Q}$, $a(x) = x^4 + 3x + 2$, $b(x) = 2x^2 + x - 1$.
(c) $F = \mathbb{Z}/3\mathbb{Z}$, $a(x) = x^5 + x^3 + x + 1$, $b(x) = x^2 + x + 1$.
(d) $F = \mathbb{Z}/7\mathbb{Z}$, $a(x) = x^3 + 6$, $b(x) = 2x^2 + 1$.
(e) $F = \mathbb{Z}/11\mathbb{Z}$, $a(x) = 2x^6 - 1$, $b(x) = 5x^2 + x + 1$.
(f) $F = \mathbb{Z}/5\mathbb{Z}$, $a(x) = -x^5 + x^3 + 2x + 1$, $b(x) = 3x + 4$.
(g) $F = \mathbb{Z}/7\mathbb{Z}$, $a(x) = 9x^5 - 4x^3 + 1$, $b(x) = 5x^2 + 2$.
(h) $F = \mathbb{Z}/13\mathbb{Z}$, $a(x) = x^3 + x^2 + 1$, $b(x) = x + 11$.
(i) $F = \mathbb{Z}/19\mathbb{Z}$, $a(x) = x^4 + 18$, $b(x) = 7x^2 + 7$.

3. Euclid's Algorithm for polynomials

For the rest of this subsection we fix a field F and two nonzero polynomials $a(x), b(x) \in F[x]$. Euclid's algorithm for polynomials is exactly what you think it is. By repeatedly applying the division algorithm we obtain

$$\begin{aligned}
a(x) &= b(x)q_1(x) + r_1(x) & \deg(r_1) &< \deg(b)\\
b(x) &= r_1(x)q_2(x) + r_2(x) & \deg(r_2) &< \deg(r_1)\\
r_1(x) &= r_2(x)q_3(x) + r_3(x) & \deg(r_3) &< \deg(r_2)\\
&\vdots\\
r_{n-3}(x) &= r_{n-2}(x)q_{n-1}(x) + r_{n-1}(x) & \deg(r_{n-1}) &< \deg(r_{n-2})\\
r_{n-2}(x) &= r_{n-1}(x)q_n(x) + r_n(x) & \deg(r_n) &< \deg(r_{n-1})\\
r_{n-1}(x) &= r_n(x)q_{n+1}(x).
\end{aligned}$$

We are interested in the last nonzero remainder $r_n(x)$.

Definition 3.1. A *greatest common divisor* of $a(x)$ and $b(x)$ is a polynomial $d(x) \in F[x]$ satisfying the following properties:

(a) $d(x)$ is a common divisor of $a(x)$ and $b(x)$;
(b) if $f(x) \in F[x]$ is any common divisor of $a(x)$ and $b(x)$ then $f(x) \mid d(x)$.

Definition 3.2. We say that nonzero polynomials $a(x), b(x) \in F[x]$ are *relatively prime* (or *coprime*) if 1_F is a greatest common divisor of $a(x)$ and $b(x)$.

Proposition 3.3. *The last nonzero remainder in Euclid's algorithm is a greatest common divisor of $a(x)$ and $b(x)$.*

As an example, take $F = \mathbb{Z}/7\mathbb{Z}$ and define $a(x), b(x) \in F[x]$ by

$$\begin{aligned} a(x) &= x^5 + 2x^2 + 3x + 1 \\ b(x) &= x^4 + 2x^3 + 4. \end{aligned}$$

Then Euclid's algorithm is

$$\begin{aligned} x^5 + 2x^2 + 3x + 1 &= (x^4 + 2x^3 + 4) \cdot (x - 2) + (4x^3 + 2x^2 - x + 2) \\ x^4 + 2x^3 + 4 &= (4x^3 + 2x^2 - x + 2) \cdot (2x + 3) + (3x^2 - x + 5) \\ 4x^3 + 2x^2 - x + 2 &= (3x^2 - x + 5) \cdot (-x + 5) + (-5x + 5) \\ 3x^2 - x + 5 &= (-5x + 5) \cdot (5x + 1) \end{aligned}$$

and the last nonzero remainder, $-5x + 5$, is a greatest common divisor of $a(x)$ and $b(x)$. Now we must address a subtle question. Do the polynomials $a(x), b(x) \in F[x]$ have any other greatest common divisors? The answer is yes, but once we know one greatest common divisor it is easy to find all the rest. We will see in a moment (Proposition 3.7) that the other greatest common divisors of $a(x)$ and $b(x)$ are obtained by multiplying $-5x + 5$ by elements of $F^\times$. For example

$$2 \cdot (-5x + 5) = -3x + 3$$

is also a greatest common divisor of $a(x)$ and $b(x)$, and so is

$$4 \cdot (-5x + 5) = x - 1.$$

It is customary, but not essential, to multiply by a unit in F to make the greatest common divisor monic (a polynomial is *monic* if the leading coefficient is 1). Thus most people would say that $x - 1$, rather than $-5x + 5$, is the greatest common divisor of $a(x)$ and $b(x)$.

Definition 3.4. Two polynomials $a(x), b(x) \in F[x]$ are *associate* if there is a $\lambda \in F^\times$ such that $a(x) = \lambda \cdot b(x)$. We write $a(x) \sim b(x)$ to indicate that $a(x)$ and $b(x)$ are associate.

Proposition 3.5. *The relation $\sim$ is an equivalence relation on the set $F[x]$.*

Proposition 3.6. *Given polynomials $a(x), b(x) \in F[x]$*

$$a(x) \sim b(x) \iff a(x) \mid b(x) \text{ and } b(x) \mid a(x).$$

Proposition 3.7. *Suppose $a(x), b(x) \in F[x]$.*

(a) *If $d(x)$ and $e(x)$ are both greatest common divisors of $a(x)$ and $b(x)$, then $d(x) \sim e(x)$.*
(b) *If $d(x)$ is a greatest common divisor of $a(x)$ and $b(x)$, then so is every associate of $d(x)$.*

Theorem 3.8. *Let $d(x)$ be a greatest common divisor of $a(x)$ and $b(x)$. There are $s(x), t(x) \in F[x]$ such that*

$$a(x)s(x) + b(x)t(x) = d(x).$$

Proof. Let's say that a polynomial $f(x) \in F[x]$ is an $F[x]$*-linear combination* of $a(x)$ and $b(x)$ if there are $s(x), t(x) \in F[x]$ such that

$$a(x)s(x) + b(x)t(x) = f(x).$$

First we perform Euclid's algorithm on $a(x)$ and $b(x)$:

$$\begin{aligned} a(x) &= b(x)q_1(x) + r_1(x) & \qquad \deg(r_1) &< \deg(b) \\ b(x) &= r_1(x)q_2(x) + r_2(x) & \qquad \deg(r_2) &< \deg(r_1) \end{aligned}$$

$$\begin{aligned} r_1(x) &= r_2(x)q_3(x) + r_3(x) && \deg(r_3) < \deg(r_2) \\ &\vdots \\ r_{n-2}(x) &= r_{n-1}(x)q_n(x) + r_n(x) && \deg(r_n) < \deg(r_{n-1}) \\ r_{n-1}(x) &= r_n(x)q_{n+1}(x). \end{aligned}$$

Arguing as in the proof of Theorem 4.4, each successive remainder $r_k(x)$ is an $F[x]$-linear combination of $a(x)$ and $b(x)$. In particular $r_n(x)$ is an $F[x]$-linear combination of $a(x)$ and $b(x)$, and so there are $s_0(x), t_0(x) \in F[x]$ such that

$$a(x)s_0(x) + b(x)t_0(x) = r_n(x).$$

As $r_n(x)$ and $d(x)$ are both greatest common divisors of $a(x)$ and $b(x)$, Proposition 3.7 implies $r_n(x) \sim d(x)$. Therefore there is a $\lambda \in F^\times$ such that $d(x) = \lambda \cdot r_n(x)$. Now we set $s(x) = \lambda \cdot s_0(x)$ and $t(x) = \lambda \cdot t_0(x)$, and multiply both sides of

$$a(x)s_0(x) + b(x)t_0(x) = r_n(x)$$

by λ to obtain the desired equality $a(x)s(x) + b(x)t(x) = d(x)$. □

Let's go back to the example $F = \mathbb{Z}/7\mathbb{Z}$ and

$$\begin{aligned} a(x) &= x^5 + 2x^2 + 3x + 1 \\ b(x) &= x^4 + 2x^3 + 4. \end{aligned}$$

We saw above that $x - 1$ is a greatest common divisor of $a(x)$ and $b(x)$, and that Euclid's algorithm on $a(x)$ and $b(x)$ is

$$\begin{aligned} a(x) &= b(x) \cdot (x-2) + (4x^3 + 2x^2 - x + 2) \\ b(x) &= (4x^3 + 2x^2 - x + 2) \cdot (2x+3) + (3x^2 - x + 5) \\ 4x^3 + 2x^2 - x + 2 &= (3x^2 - x + 5) \cdot (-x+5) + (-5x+5) \\ 3x^2 - x + 5 &= (-5x+5) \cdot (5x+1). \end{aligned}$$

Writing each successive remainder in terms of $a(x)$ and $b(x)$, we find

$$\begin{aligned} 4x^3 + 2x^2 - x + 2 &= a(x) - b(x)(x-2) \\ 3x^2 - x + 5 &= b(x) - (4x^3 + 2x^2 - x + 2) \cdot (2x+3) \\ &= b(x) - [a(x) - b(x)(x-2)] \cdot (2x+3) \\ &= a(x)(5x+4) + b(x)(2x^2 - x + 2) \\ -5x + 5 &= (4x^3 + 2x^2 - x + 2) - (3x^2 - x + 5) \cdot (-x+5) \\ &= [a(x) - b(x)(x-2)] \\ &\quad -[a(x)(5x+4) + b(x)(2x^2 - x + 2)] \cdot (-x+5) \\ &= a(x)(5x^2 + 2) + b(x)(2x^3 + 3x^2 - x - 1) \end{aligned}$$

and so

$$a(x) \cdot (5x^2 + 2) + b(x) \cdot (2x^3 + 3x^2 - x - 1) = -5x + 5$$

If we multiply everything through by 4 we obtain

$$a(x) \cdot (6x^2 + 1) + b(x) \cdot (x^3 + 5x^2 + 3x + 3) = x - 1.$$

Definition 3.9. A *least common multiple* of $a(x)$ and $b(x)$ is a polynomial $m(x) \in F[x]$ satisfying the following properties:

(a) $m(x)$ is a common multiple of $a(x)$ and $b(x)$;
(b) if $f(x) \in F[x]$ is any common multiple of $a(x)$ and $b(x)$ then $m(x) \mid f(x)$.

Exercise 3.10. Let $d(x)$ be a greatest common divisor of $a(x)$ and $b(x)$, and set

$$m(x) = \frac{a(x)b(x)}{d(x)}.$$

Show that $m(x)$ is a least common multiple of $a(x)$ and $b(x)$.

Exercise 3.11. Suppose $m(x)$ is a least common multiple of $a(x)$ and $b(x)$, and $f(x) \in F[x]$ is any polynomial. Then

$$f(x) \text{ is a least common multiple of } a(x) \text{ and } b(x) \iff f(x) \sim m(x).$$

Exercise 3.12. In $(\mathbb{Z}/3\mathbb{Z})[x]$, compute a greatest common divisor $d(x)$ of

$$\begin{aligned} a(x) &= x^8 + x^7 + x^6 - x^4 - x^3 + x + 1 \\ b(x) &= x^5 + x^4 + x^3 + x^2 - 1 \end{aligned}$$

and find polynomials $s(x), t(x) \in (\mathbb{Z}/3\mathbb{Z})[x]$ such that

$$a(x)s(x) + b(x)t(x) = d(x).$$

Exercise 3.13. Find polynomials $s(x), t(x) \in (\mathbb{Z}/13\mathbb{Z})[x]$ satisfying

$$(6x^5 + x + 2) \cdot s(x) + (3x^4 - x^2 + 1) \cdot t(x) = 1,$$

or show that no such polynomials exist.

Exercise 3.14. Define polynomials in $(\mathbb{Z}/3\mathbb{Z})[x]$ by

$$\begin{aligned} a(x) &= x^3 + 2x^2 + 2 \\ b(x) &= x^2 + x + 1. \end{aligned}$$

Find $s(x), t(x) \in (\mathbb{Z}/3\mathbb{Z})[x]$ satisfying

$$a(x) \cdot s(x) + b(x) \cdot t(x) = x,$$

or prove that no such $s(x), t(x)$ exist.

4. Unique factorization of polynomials

Let F be a field.

Definition 4.1. Suppose $a(x) \in F[x]$ is a nonconstant polynomial.

(a) We say that $a(x)$ is *irreducible* if for every factorization

$$a(x) = s(x) \cdot t(x)$$

with $s(x), t(x) \in F[x]$, either $\deg(s) = 0$ or $\deg(t) = 0$ (in other words, either $s(x)$ or $t(x)$ is a nonzero constant).

(b) We say that $a(x)$ is *factorizable* if there is some factorization

$$a(x) = s(x) \cdot t(x)$$

with $s(x), t(x) \in F[x]$ and

$$0 < \deg(s) < \deg(a) \qquad 0 < \deg(t) < \deg(a).$$

Every nonconstant polynomial is either irreducible or factorizable. By convention a constant polynomial is neither irreducible nor factorizable.

Proposition 4.2. *Every $a(x) \in F[x]$ of degree 1 is irreducible.*

Suppose that $a(x) \in F[x]$ is irreducible. What do the divisors of $a(x)$ look like? If $d(x) \mid a(x)$ then there is a $q(x) \in F[x]$ such that $a(x) = d(x)q(x)$. By definition of irreducible either $\deg(d) = 0$ or $\deg(q) = 0$. If $\deg(d) = 0$ then $d(x)$ is a constant polynomial, which is clearly nonzero as $d(x)q(x) \neq 0$. In other words $d(x) = d_0$ for some $d_0 \in F^\times$. But this means that $d(x) \sim 1_F$. If $\deg(q) = 0$ then $q(x)$ is a constant polynomial, so $q(x) = q_0$ for some $q_0 \in F^\times$. But now $a(x) = d(x) \cdot q_0$ shows that $a(x) \sim d(x)$. What we have proved is that if $a(x)$ is irreducible then

$$d(x) \mid a(x) \implies d(x) \sim 1_F \text{ or } d(x) \sim a(x).$$

Proposition 4.3. *Suppose $a(x), b(x) \in F[x]$ are associates. Then $a(x)$ is irreducible if and only if $b(x)$ is irreducible.*

The following result, which asserts that every nonconstant polynomial can be factored as a product of irreducible polynomials, is proved using (strong) induction on the degree of the polynomial.

Proposition 4.4. *Given any nonconstant polynomial $a(x) \in F[x]$, there are irreducible polynomials $p_1(x), \ldots, p_m(x) \in F[x]$ such that*

$$a(x) = p_1(x) \cdots p_m(x).$$

Recall an old result: if $p, a, b \in \mathbb{Z}^+$ with p prime, and if $p \mid ab$, then either $p \mid a$ or $p \mid b$. The following is the analogous statement for polynomials.

Proposition 4.5. *Suppose $p(x), a(x), b(x) \in F[x]$ with $p(x)$ irreducible. Then*

$$p(x) \mid a(x)b(x) \implies p(x) \mid a(x) \text{ or } p(x) \mid b(x).$$

Proposition 4.5 has the following strengthened form, which will be needed in the proof of the Fundamental Theorem of Arithmetic for Polynomials.

Corollary 4.6. *Suppose $p(x), a_1(x), \ldots, a_n(x) \in F[x]$ with $p(x)$ irreducible. If $p(x)$ divides the product $a_1(x) \cdots a_n(x)$ then $p(x) \mid a_i(x)$ for some $1 \leq i \leq n$.*

We saw above that every polynomial in $F[x]$ can be factored as a product of irreducible polynomials. Now we are ready to prove the *uniqueness* of the factorization.

Theorem 4.7 (Fundamental Theorem of Arithmetic for Polynomials)**.** *Let $a(x) \in F[x]$ be a nonconstant polynomial. There are irreducible polynomials*

$$p_1(x), \ldots, p_m(x) \in F[x]$$

such that

$$a(x) = p_1(x) \cdots p_m(x).$$

If $a(x) = q_1(x) \cdots q_n(x)$ is another factorization of $a(x)$ into irreducibles then $m = n$ and, after possibly reordering $q_1(x), \ldots, q_m(x)$,

$$\begin{aligned} p_1(x) &\sim q_1(x) \\ p_2(x) &\sim q_2(x) \\ &\vdots \\ p_m(x) &\sim q_m(x). \end{aligned}$$

Proof. The existence part of the proof was Proposition 4.4, so we only need to prove the uniqueness of the factorization. Suppose $a(x) \in F[x]$ is nonconstant and admits two factorizations into irreducible polynomials

$$a(x) = p_1(x) \cdots p_m(x)$$

and

$$a(x) = q_1(x) \cdots q_n(x).$$

Without loss of generality we may assume that $m \le n$.

From the equality

$$p_1(x) \cdots p_m(x) = q_1(x) \cdots q_n(x)$$

it is clear that $p_1(x)$ divides the product $q_1(x) \cdots q_n(x)$, and so Corollary 4.6 tells us that $p_1(x)$ divides at least one of $q_1(x), \ldots, q_n(x)$. After reordering the $q_i(x)$'s we may assume that $p_1(x) \mid q_1(x)$. As $q_1(x)$ is irreducible, either $p_1(x) \sim 1_F$ or $p_1(x) \sim q_1(x)$. The first possibility cannot occur: if $p_1(x) \sim 1_F$ then $p_1(x)$ is a constant polynomial, and constant polynomials are not irreducible. Therefore $p_1(x) \sim q_1(x)$ and so there is a $\lambda_1 \in F^\times$ such that $p_1(x) = \lambda_1 q_1(x)$. Therefore

$$\lambda_1 q_1(x) p_2(x) \cdots p_m(x) = q_1(x) \cdots q_n(x).$$

Canceling $q_1(x)$ from both sides (recall $F[x]$ is an integral domain, so the cancellation law holds) we arrive at

$$\lambda_1 p_2(x) \cdots p_m(x) = q_2(x) \cdots q_n(x).$$

Now repeat this process. The previous equality implies that $p_2(x)$ divides one of $q_2(x), \ldots, q_n(x)$, and after reordering we may assume $p_2(x) \mid q_2(x)$. As above, this implies $p_2(x) \sim q_2(x)$, so there is a $\lambda_2 \in F^\times$ such that $p_2(x) = \lambda_2 q_2(x)$. Therefore

$$\lambda_1 \lambda_2 p_3(x) \cdots p_m(x) = q_3(x) \cdots q_n(x).$$

Repeating this process shows that, after reordering the $q_i(x)$'s,

$$p_1(x) \sim q_1(x) \qquad p_2(x) \sim q_2(x) \qquad \cdots \qquad p_m(x) \sim q_m(x)$$

and

$$\lambda_1 \lambda_2 \cdots \lambda_m = q_{m+1}(x) \cdots q_n(x)$$

for some $\lambda_1, \ldots, \lambda_m \in F^\times$. If $n > m$ then the product on the right is a nonempty product of polynomials of degree > 0. Therefore

$$0 = \deg(\lambda_1 \cdots \lambda_m) = \deg(q_{m+1}) + \cdots + \deg(q_n) > 0,$$

a contradiction. Thus $m = n$ and we are dome. □

Exercise 4.8. Suppose $a(x), b(x), c(x) \in F[x]$ with $a(x)$ and $b(x)$ relatively prime.

(a) Assume $a(x) \mid c(x)$ and $b(x) \mid c(x)$. Show that $a(x)b(x) \mid c(x)$.

(b) Assume $a(x) \mid b(x)c(x)$. Show that $a(x) \mid c(x)$.

Exercise 4.9. Find two different ways to factor $x^2 + x + 8 \in (\mathbb{Z}/10\mathbb{Z})[x]$ as a product of monic polynomials of degree one.

5. Roots of polynomials

Let F be a field. The first step to understanding how to factor polynomials into irreducibles is to understand the connection between factorization and finding roots.

Definition 5.1. Suppose $a(x) \in F[x]$ and $\alpha \in F$. We say that α is a *root* (or *zero*) of $a(x)$ if $a(\alpha) = 0_F$.

Proposition 5.2. *Suppose $a(x) \in F[x]$ and $\alpha \in F$. Then*

$$\alpha \text{ is a root of } a(x) \iff x - \alpha \text{ divides } a(x).$$

Corollary 5.3. *Suppose $a(x) \in F[x]$ has degree $n \geq 0$. Then $a(x)$ has at most n roots in F.*

Proposition 5.4. *If $a(x) \in F[x]$ has degree 2 or 3 then*

$$a(x) \text{ is irreducible} \iff a(x) \text{ has no roots in } F.$$

Consider the polynomial $a(x) = x^5 - x^3 + 2x^2 + 3x + 2 \in (\mathbb{Z}/5\mathbb{Z})[x]$. In order to factor $a(x)$ into irreducibles, the first step is to look for roots. As $\mathbb{Z}/5\mathbb{Z}$ only has five elements, this can be done by brute force. Plugging in the possible values of x we quickly find that $a(2) = 0$, and so $a(x)$ is divisible by $x - 2$. By long division we find

$$a(x) = (x - 2)(x^4 + 2x^3 + 3x^2 + 3x + 4).$$

Can we factor this any further? Yes. Plugging in different values of x we find that $x^3 + 2x^2 + 2x + 4$ has 3 as a root, so we can further divide out a factor of $x - 3$. The result is

$$a(x) = (x - 2)(x - 3)(x^3 + 3x + 2).$$

Can we factor this any further? No. There are only five elements in $\mathbb{Z}/5\mathbb{Z}$. If you plug each one into $x^3 + 3x + 2$ you will find that $x^3 + 3x + 2$ has no roots. By Proposition 5.4 the polynomial $x^3 + 3x + 2$ is irreducible.

Warning: If you have a polynomial $a(x)$ of degree 2 or 3 with no roots, then you can deduce that $a(x)$ is irreducible. If $\deg(a) > 3$ and $a(x)$ has no roots, it does *not* follow that $a(x)$ is irreducible. For example, the polynomial $a(x) = x^4 + 3x^2 + 2 \in (\mathbb{Z}/7\mathbb{Z})[x]$ has no roots, but it factors as $a(x) = (x^2 + 1)(x^2 + 2)$.

For polynomials with coefficients in $\mathbb{Z}/p\mathbb{Z}$, finding roots is simply a question of brute force. After all, $\mathbb{Z}/p\mathbb{Z}$ only has finitely many elements. For polynomials with coefficients in $\mathbb{Q}$, finding roots is done using the *rational root test.*

Theorem 5.5 (Rational root test)**.** *Suppose*

$$a(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Let $\alpha \in \mathbb{Q}$ be a root of $a(x)$ and write $\alpha = s/t$ with $s \in \mathbb{Z}$, $t \in \mathbb{Z}^+$, and $\gcd(s,t) = 1$. Then $s \mid a_0$ and $t \mid a_n$.

Proof. Using $0 = a(s/t)$ we deduce

$$0 = a_n(s/t)^n + a_{n-1}(s/t)^{n-1} + \cdots + a_2(s/t)^2 + a_1(s/t) + a_0.$$

Multiplying both sides by t^n shows

$$0 = a_n s^n + a_{n-1}s^{n-1}t + \cdots + a_2 s^2 t^{n-2} + a_1 s t^{n-1} + a_0 t^n. \tag{5.1}$$

First rewrite (5.1) as

$$a_0 t^n = -(a_n s^n + a_{n-1}s^{n-1}t + \cdots + a_2 s^2 t^{n-2} + a_1 s t^{n-1}).$$

The right hand side is divisible by s, and so $s \mid a_0 t^n$. I claim that $\gcd(s, t^n) = 1$. To see this, suppose $\gcd(s, t^n) > 1$. Then $\gcd(s, t^n)$ is divisible by some prime p, and so s and t^n are each divisible by p. But $p \mid t^n$ implies that p appears in the prime factorization of t^n. This implies that p already appeared in the prime factorization of t, and so p divides both s and t, contradicting $\gcd(s, t) = 1$. Therefore $\gcd(s, t^n) = 1$, and the divisibility $s \mid a_0 t^n$ now implies $s \mid a_0$ (see Proposition 4.9).

Similarly we may rewrite (5.1) as

$$a_n s^n = -(a_{n-1}s^{n-1}t + \cdots + a_2 s^2 t^{n-2} + a_1 s t^{n-1} + a_0 t^n).$$

The right hand side is divisible by t, and so $t \mid a_n s^n$. Repeating the argument of the preceding paragraph shows $\gcd(t, s^n) = 1$, and so $t \mid a_n$ as desired. □

Let's use the rational root test to factor

$$a(x) = x^4 - \frac{1}{3}x^3 + x^2 + \frac{2}{3}x - \frac{1}{3} \in \mathbb{Q}[x].$$

First we clear denominators

$$a(x) = \frac{1}{3}\Big(3x^4 - x^3 + 3x^2 + 2x - 1\Big)$$

and then we apply the rational root test to $3x^4 - x^3 + 3x^2 + 2x - 1$. Any root must have the form s/t with $t > 0$, $s \mid (-1)$, and $t \mid 3$. Thus $s \in \{\pm 1\}$ and $t \in \{1, 3\}$, and any root of $a(x)$ lies in the set $\{\pm 1, \pm 1/3\}$. The rational root test does not imply that all of these numbers are roots of $a(x)$, only that any root is somewhere in the above set. To find the actual roots, we just plug each each of 1, -1, $1/3$, and $-1/3$ into $a(x)$ to see which ones really are roots. We quickly find that $1/3$ is a root, and so we may factor $x - 1/3$ out of $a(x)$. Doing so shows that

$$a(x) = \left(x - \frac{1}{3}\right)(x^3 + x + 1).$$

Can this be factored any further? No. The rational root test shows that any root of $x^3 + x + 1$ lies in the set $\{1, -1\}$. Neither 1 nor -1 is actually a root, and so $x^3 + x + 1$ is irreducible by Proposition 5.4.

As another example, let's factor $a(x) = 2x^4 - 5x^3 + 7x^2 - 25x - 15 \in \mathbb{Q}[x]$. The first thing to do is check for roots. If s/t is a root of $a(x)$, reduced to lowest terms, then the rational root test tells us $s \mid 15$ and $t \mid 2$. Thus $s \in \{\pm 1, \pm 3, \pm 5, \pm 15\}$ and $t \in \{1, 2\}$. This gives 16 possibilities for s/t:

$$s/t \in \{\pm 1, \pm 3, \pm 5, \pm 15, \pm 1/2, \pm 3/2, \pm 5/2, \pm 15/2\}.$$

To find the actual roots we just plug each of the above 16 values of x into $a(x)$ and see which ones give solutions to $a(x) = 0$. By brute force, we find that the only roots of $a(x)$ are $-1/2$ and 3, and so we may factor out $x + 1/2$ and $x - 3$ from $a(x)$. After long division we find

$$a(x) = (x + 1/2)(x - 3)(2x^2 + 10)$$

or, if you prefer,

$$a(x) = (2x + 1)(x - 3)(x^2 + 5).$$

To show that this is the complete factorization into irreducibles, it only remains to show that $x^2 + 5$ is irreducible, and by the rational root test the only possible roots are s/t with $s \mid 5$ and $t \mid 1$, and so $s/t \in \{\pm 1, \pm 5\}$. None of these are roots, and so $x^2 + 5$ is irreducible by Proposition 5.4.

We could also have used the quadratic formula to show that $x^2 + 5$ has no roots in $\mathbb{Q}$. In general, if $f(x) = ax^2 + bx + c$ has complex coefficients with $a \neq 0$ then the complex roots of $f(x)$ are given by the familiar formula

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

In the case of $f(x) = x^2 + 5$, the complex roots of $f(x)$ are $\pm\sqrt{-5}$, which are not rational.

Exercise 5.6.

(a) Factor $x^4 + 2x^3 + x^2 + 3x + 2 \in \mathbb{Q}[x]$ into irreducibles.
(b) Factor $x^4 + 2x^3 + x^2 + 3x + 2 \in (\mathbb{Z}/3\mathbb{Z})[x]$ into irreducibles.
(c) Factor $2x^4 + 7x^3 + 9x^2 + 15x + 6 \in \mathbb{Q}[x]$ into irreducibles.
(d) Factor $2x^4 + 7x^3 + 9x^2 + 15x + 6 \in (\mathbb{Z}/5\mathbb{Z})[x]$ into irreducibles.

Exercise 5.7. Let F be a field. Suppose $f(x) = ax^2 + bx + c \in F[x]$ with $2a \in F^\times$, and set $\Delta = b^2 - 4ac$. Prove the following version of the quadratic formula.

(a) If there is a $\delta \in F$ such that $\delta^2 = \Delta$, then

$$\frac{-b \pm \delta}{2a}$$

are roots of $f(x)$.
(b) If there is no $\delta \in F$ such that $\delta^2 = \Delta$, then $f(x)$ has no roots in F.
(c) Use the above to find the roots of

$$3x^2 + 2x + 5 \in (\mathbb{Z}/p\mathbb{Z})[x]$$

for each prime $p \in \{7, 11, 13, 23\}$, and use this to factor $3x^2 + 2x + 5 \in (\mathbb{Z}/p\mathbb{Z})[x]$.

Hint: for (b) use the identity $4a \cdot f(x) = (2ax + b)^2 - \Delta$.

Exercise 5.8.

(a) Factor $x^4 + 1$ into irreducible factors in $\mathbb{Q}[x]$.
(b) Factor $x^4 + 1$ into irreducible factors in $\mathbb{R}[x]$.
(c) Factor $x^4 + 1$ into irreducible factors in $\mathbb{C}[x]$.

Exercise 5.9.

(a) Factor $x^4 + 1$ into irreducible factors in $(\mathbb{Z}/2\mathbb{Z})[x]$.
(b) Factor $x^4 + 1$ into irreducible factors in $(\mathbb{Z}/3\mathbb{Z})[x]$.
(c) Factor $x^4 + 1$ into irreducible factors in $(\mathbb{Z}/5\mathbb{Z})[x]$.

Exercise 5.10. List all irreducible polynomials of degree ≤ 4 in $(\mathbb{Z}/2\mathbb{Z})[x]$.

Exercise 5.11. Suppose $n \in \mathbb{Z}^+$ and $a(x), b(x) \in F[x]$ have degree $< n$. Suppose also that there are n distinct elements $z_1, \ldots, z_n \in F$ such that $a(z_i) = b(z_i)$ for all $1 \leq i \leq n$. Prove that $a(x) = b(x)$.

Exercise 5.12. For which $n > 1$ does the polynomial $f(x) = x^n + 5x + 6 \in \mathbb{Q}[x]$ have a root in $\mathbb{Q}$?

Exercise 5.13. Find all $a, b \in \mathbb{Z}/3\mathbb{Z}$ for which the polynomial $x^3 + ax + b \in (\mathbb{Z}/3\mathbb{Z})[x]$ is irreducible.

Exercise 5.14. Suppose $n > 1$. Show that $30x^n - 91$ has no rational roots.

Exercise 5.15. Let p be an odd prime.

(a) Show that the polynomial $x^{p-1} - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ factors as

$$x^{p-1} - 1 = \Big(x-1\Big) \cdot \Big(x-2\Big) \cdot \Big(x-3\Big) \cdots \Big(x-(p-2)\Big) \cdot \Big(x-(p-1)\Big).$$

(b) Deduce *Wilson's theorem*: $(p-1)! \equiv -1 \pmod{p}$.

Exercise 5.16. Suppose that $f(x), g(x) \in \mathbb{C}[x]$ are monic polynomials, with $\deg(f) = \deg(g) = n \geq 1$. Suppose also that

$$f(1) = g(1) \qquad f(2) = g(2) \qquad \cdots \qquad f(n) = g(n).$$

Show that $f(x) = g(x)$. Hint: Let $h(x) = f(x) - g(x)$. What is the degree of h? What are some of its roots?

Exercise 5.17. Suppose we remove the assumption that $f(x)$ and $g(x)$ are monic in the previous problem. Show by example that we can no longer conclude that $f(x) = g(x)$.

6. Eisenstein's criterion and the Gauss lemma

Definition 6.1. A polynomial $a(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is *primitive* if the greatest common divisor of $a_n, \ldots, a_0$ is equal to 1.

Every nonzero $a(x) \in \mathbb{Z}[x]$ can be factored as the product of a constant times a primitive polynomial in an obvious way. If $a(x) = a_n x^n + \cdots + a_1 x + a_0$ then let $d \in \mathbb{Z}$ be the greatest common divisor of the coefficients $a_n, \ldots, a_0$. The polynomial

$$A(x) = \frac{a_n}{d} x^n + \cdots + \frac{a_1}{d} x + \frac{a_0}{d}$$

is then primitive, and $a(x) = d \cdot A(x)$. More generally, suppose $a(x) \in \mathbb{Q}[x]$ is nonzero. Let $e \in \mathbb{Z}^+$ be an integer chosen so that $e \cdot a(x)$ has integer coefficients. By what was just said, we may now write $e \cdot a(x)$ as the product of a constant $d \in \mathbb{Z}$ by a primitive polynomial $A(x) \in \mathbb{Z}[x]$. Then

$$a(x) = \frac{d}{e} \cdot A(x).$$

In other words, every nonzero $a(x) \in \mathbb{Q}[x]$ can be written as the product of a nonzero rational number times a primitive polynomial in $\mathbb{Z}[x]$. For example

$$\begin{aligned} -\frac{4}{5}x^2 + \frac{2}{5}x + \frac{2}{3} &= \frac{1}{15} \cdot (-12x^2 + 6x + 10) \\ &= \frac{2}{15} \cdot (-4x^2 + 3x + 5). \end{aligned}$$

Theorem 6.2 (Gauss Lemma I)**.** *Suppose $f(x), g(x) \in \mathbb{Z}[x]$ are primitive polynomials. Then the product $f(x)g(x)$ is again primitive.*

Proof. Suppose not, so that there is some integer $d > 1$ that divides all coefficients of $f(x)g(x)$. If p is any prime divisor of d, then p divides all coefficients of $f(x)g(x)$. Given any polynomial $a(x) \in \mathbb{Z}[x]$ we denote by $\overline{a}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ the polynomial obtained by reducing all coefficients of $a(x)$ modulo p. For example if $p = 5$ and $a(x) = 7x^3 + 10x^2 - 11x + 2$ then

$$\overline{a}(x) = 2x^3 + 4x + 2 \in (\mathbb{Z}/5\mathbb{Z})[x].$$

Clearly, $\overline{f}(x)\overline{g}(x) = 0$, as all coefficients of $f(x)g(x)$ are divisible by p. But $(\mathbb{Z}/p\mathbb{Z})[x]$ is an integral domain, and so either $\overline{f}(x) = 0$ or $\overline{g}(x) = 0$. If $\overline{f}(x) = 0$ then all coefficients of $f(x)$ are divisible by p, contradicting $f(x)$ being primitive. Similarly, if $\overline{g}(x) = 0$ then all coefficients of $g(x)$ are divisible by p, contradicting $g(x)$ being primitive. In either case we arrive at a contradiction. □

Theorem 6.3 (Gauss Lemma II)**.** *Suppose $f(x) \in \mathbb{Z}[x]$ is a nonconstant polynomial that can be factored as $f(x) = a(x)b(x)$ for polynomials $a(x)$ and $b(x)$ with rational coefficients. Then there are polynomials $c(x)$ and $d(x)$ with integer coefficients such that $f(x) = c(x)d(x)$ and*

$$c(x) \sim a(x) \qquad d(x) \sim b(x).$$

Proof. Start by writing $a(x) = sA(x)$ and $b(x) = tB(x)$ for nonzero $s, t \in \mathbb{Q}$ and primitive polynomials $A(x), B(x) \in \mathbb{Z}[x]$. Then

$$f(x) = stA(x)B(x).$$

Write $st = p/q$ with $p \in \mathbb{Z}$ and $q \in \mathbb{Z}^+$, and consider the equality

$$q \cdot f(x) = p \cdot A(x)B(x).$$

By the first form of the Gauss Lemma the product $A(x)B(x)$ is primitive, and so the GCD of the coefficients of $A(x)B(x)$ is 1. Therefore the GCD of the coefficients of $pA(x)B(x)$ is p. On the other hand, if we let $r \in \mathbb{Z}^+$ be the GCD of the coefficients of $f(x)$ then the GCD of the coefficients of $qf(x)$ is qr. So $qr = p$, and hence

$$q \cdot f(x) = qr \cdot A(x)B(x).$$

Now simplify to

$$f(x) = rA(x)B(x),$$

and set

$$c(x) = rA(x) \qquad d(x) = B(x).$$

As $c(x) \sim A(x) \sim a(x)$ and $d(x) \sim B(x) \sim b(x)$, and both $c(x)$ and $d(x)$ have integer coefficients, we are done. □

Proposition 6.4. *Suppose*

$$f(x) = a_m x^m + \cdots + a_1 x + a_0$$
$$g(x) = b_n x^n + \cdots + b_1 x + b_0$$

are two polynomials with coefficients in a field F. Then the coefficient of x^k in $f(x)g(x)$ is

$$a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0.$$

Theorem 6.5 (Eisenstein's Criterion)**.** *Suppose*

$$a(x) = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Q}[x]$$

has integer coefficients, and there is a prime p satisfying

(a) $p \nmid a_n$,
(b) p *divides* $a_{n-1}, \ldots, a_0$,
(c) $p^2 \nmid a_0$.

Then $a(x)$ is irreducible.

First proof of Eisenstein's criterion. To get a contradiction, assume that $a(x)$ factors in $\mathbb{Q}[x]$ as a product of two polynomials of degree $< n$. By the second form of the Gauss Lemma, we may assume that the two factors actually have integer coefficients. Thus we have $a(x) = b(x)c(x)$ for some $b(x), c(x) \in \mathbb{Z}[x]$ of degree less than n. Write

$$b(x) = b_sx^s + \cdots + b_1x + b_0$$
$$c(x) = c_tx^t + \cdots + c_1x + c_0$$

with $s, t < n$. As $a_0 = b_0c_0$ is divisible by p either b_0 or c_0 is divisible by p, and without loss of generality we may assume that $p \mid b_0$. On the other hand, as $a_n = b_sc_t$ is not divisible by p, we must have $p \nmid b_s$.

So, as $p \mid b_0$ and $p \nmid b_s$, there is a *first* coefficient in the list $b_0, \ldots, b_s$ that is not divisible by p, say $p \nmid b_k$, with

$$k \le s < n.$$

In other words, $p \mid b_0, \ldots, b_{k-1}$ but $p \nmid b_k$. By Proposition 6.4,

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0,$$

and so

$$b_kc_0 = a_k - (b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1).$$

Now we get to the punchline: every term on the right hand side is divisible p, and so $p \mid b_kc_0$. As $p \nmid b_k$, we deduce that $p \mid c_0$. But this shows that b_0 and c_0 are both divisible by p, and hence $a_0 = b_0c_0$ is divisible by p^2, contradicting our assumptions on $a(x)$. □

Second proof of Eisenstein's criterion. To get a contradiction, assume that $a(x)$ factors in $\mathbb{Q}[x]$ as a product of two polynomials of degree $< n$. By the second form of the Gauss Lemma, we may assume that the two factors actually have integer coefficients. Thus we have $a(x) = b(x)c(x)$ for some $b(x), c(x) \in \mathbb{Z}[x]$ with

$$\deg(b) < n \qquad \deg(c) < n.$$

For a polynomial $f(x) \in \mathbb{Z}[x]$ let $\overline{f}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ denote the polynomial obtained by reducing all coefficients of $f(x)$ modulo p. Reducing the factorization $a(x) = b(x)c(x)$ modulo p shows that

$$\overline{a}(x) = \overline{b}(x)\overline{c}(x). \tag{6.1}$$

Now think about the irreducible factorization of each side. On the one hand, our hypotheses on $a(x)$ imply that

$$\overline{a}(x) = a_nx^n.$$

On the other hand, if we factor each polynomial on the right into irreducibles

$$\overline{b}(x) = p_1(x)\cdots p_s(x)$$

$$\overline{c}(x) = q_1(x) \cdots q_t(x),$$

then (6.1) implies

$$a_n x^n = p_1(x) \cdots p_s(x) q_1(x) \cdots q_t(x).$$

By the uniqueness part of the Fundamental Theorem of Arithmetic for polynomials, every one of $p_1(x), \ldots, p_s(x), q_1(x), \ldots, q_t(x)$ is associate to the irreducible polynomial x. We deduce from this that

$$\begin{aligned} \overline{b}(x) &\sim x^s \\ \overline{c}(x) &\sim x^t, \end{aligned} \tag{6.2}$$

and as

$$x^n \sim \overline{a}(x) = \overline{b}(x)\overline{c}(x) \sim x^s x^t$$

we must have $n = s + t$. Is it possible that $s = 0$? No, because then $t = n$ contradicting

$$t = \deg(\overline{c}) \leq \deg(c) < n.$$

Similarly we cannot have $t = 0$. It now follows from (6.2) that both $\overline{b}(x)$ and $\overline{c}(x)$ are divisible by x, and so their constant terms are equal to 0. This implies that if we write

$$\begin{aligned} b(x) &= b_s x^s + \cdots + b_0 \\ c(x) &= c_t x^t + \cdots + c_0 \end{aligned}$$

then b_0 and c_0 are each divisible by p, and so $a_0 = b_0 c_0$ is divisible by p^2, contradicting our hypotheses on $a(x)$. □

For example, consider the polynomial $a(x) = 3x^7 - 15x^5 + 10 \in \mathbb{Q}[x]$. We may apply Eisenstein's criterion with $p = 5$: 5 does not divide the leading coefficient, 5 divides all the other coefficients, and 5^2 does not divide the constant term. Therefore $a(x)$ is irreducible (and some would say that $a(x)$ *is Eisenstein at* 5)

Suppose we want to factor

$$a(x) = x^6 - \frac{1}{2}x^5 - \frac{3}{2}x^2 + \frac{9}{4}x - \frac{3}{4} \in \mathbb{Q}[x]$$

into irreducibles. First we clear the denominators by writing

$$a(x) = \frac{1}{4}(4x^6 - 2x^5 - 6x^2 + 9x - 3).$$

Applying the rational root test to $4x^6 - 2x^5 - 6x^2 + 9x - 3$ we quickly find that $x = 1/2$ is a root, and so is a root of $a(x)$. Factoring out $x - 1/2$ leaves

$$a(x) = \left(x - \frac{1}{2}\right)\left(x^5 - \frac{3}{2}x + \frac{3}{2}\right).$$

I claim the second term is irreducible. Indeed, clearing denominators we find

$$x^5 - \frac{3}{2}x + \frac{3}{2} = \frac{1}{2} \cdot (2x^5 - 3x + 3).$$

The polynomial $2x^5 - 3x + 3$ is Eisenstein at 3, and so is irreducible. Therefore $x^5 - \frac{3}{2}x + \frac{3}{2}$ is also irreducible, by Proposition 4.3.

Exercise 6.6.

(a) Factor $x^5 + 3x^4 - 3x^2 - 3x + 18 \in \mathbb{Q}[x]$ into irreducibles.
(b) Factor $x^5 + 3x^4 - 3x^2 - 3x + 18 \in (\mathbb{Z}/5\mathbb{Z})[x]$ into irreducibles.

(c) Factor $3x^8 - 9x^7 + 8x^4 - 24x^3 + 2x - 6 \in \mathbb{Q}[x]$ into irreducibles.

Exercise 6.7.

(a) Show that the polynomial $x^5 + x^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ has no roots in $\mathbb{Z}/2\mathbb{Z}$, and is not divisible by $x^2 + x + 1$. Deduce that $x^5 + x^2 + 1$ is irreducible.

(b) Use part (a) to prove that $x^5 + 8x^4 + 3x^2 + 4x + 7 \in \mathbb{Q}[x]$ is irreducible. Hint: If it factors in $\mathbb{Q}[x]$ then, by the Gauss Lemma, it factors in $\mathbb{Z}[x]$.

Exercise 6.8. Suppose p is a prime.

(a) Show that $\Big[(x+1)^p - 1\Big]/x \in \mathbb{Q}[x]$ is irreducible.

(b) Use part (a) to prove that

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Q}[x]$$

is irreducible.

Exercise 6.9. Show there are infinitely many integers k for which

$$x^4 + 2x^2 + k \in \mathbb{Q}[x]$$

is irreducible.