A First Course in Abstract Algebra by Anderson & Feil

Noah Lewis

November 15, 2025

Contents

1 The Natural Numbers

Problem 1

Prove using mathematical induction that for all positive integers n,

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

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

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

Thus:

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

Problem 3

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

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

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

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

for any positive integer n.

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

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

Thus:

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

Problem 4

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

Solution

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

Problem 5

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

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

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

Thus:

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

Problem 7

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

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

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

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

Thus

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

∎

Problem 12

Consider the sequence a_n defined inductively as follows:

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

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

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

and

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

So $k = n$ is:

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

Then:

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

∎

Problem 14

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

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

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

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

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

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

Proof.

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

∎

Proof. Let $k = 0$ then, $\binom{n}{0} = \frac{n!}{(n-0)!(0!)} = \frac{n!}{n!} = 1 \in \mathbb{Z}$. Let $k = n$ then, $\binom{n}{n} = \frac{n!}{(n-n)!(n!)} = \frac{n!}{n!} = 1 \in \mathbb{Z}$. Assume this

holds for $n-1$, thus for all k where $0 \leq k \leq n-1$:

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

Then:

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

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

Proof. Let $n = 0$. Then:

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

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

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

Then:

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

∎

Problem 15

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

Solution

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

Problem 16

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

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

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

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

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

2 The Integers

Problem 3

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

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

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

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

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

Problem 4

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

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

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

Problem 5

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

Proof. Suppose p is prime.

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

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

Problem 6

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

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

Problem 7

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

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

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

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

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

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

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

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

Solution (b):

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

Problem 9

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

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

Problem 10

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

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

and

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

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

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

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

Solution:

Let

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

Exponents of each prime factor:

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

Minimum exponent for each prime:

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

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

Multiply the primes raised to the minimum exponents:

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

The gcd of 360 and 900 is 180.

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

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

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

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

Problem 11

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

Solution

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

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

and

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

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

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

where s_i is the larger of n_i and m_i.

Problem 12

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

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

Proof. We prove the general case first.

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

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

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

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

This is the ith prime factor of the lcm. ∎

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

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

∎

Problem 13

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

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

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

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

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

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

Problem 18

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

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

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

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

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

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

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

Solution 18 (b):

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

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

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

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

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

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

Problem 19

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

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

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

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

3 Modular Arithmetic

Problem 2

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

Solution

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

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

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

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

Problem 4

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

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

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

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

Problem 5

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

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

Problem 6

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

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

Problem 7

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

Solution:

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

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

Problem 9

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

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

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

Showing that $[xb] = [yc]$ ∎

Problem 10

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

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

Problem 13

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

Solution:

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

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

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

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

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

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

Problem 14

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

Solution:

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

4 Polynomials with Rational Coefficients

Problem 2

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

Solution:

When $x^2 - 3x + 2$ is divided by $2x + 1$, the quotient is $\frac{1}{2}x - \frac{7}{4}$ and the remainder is $\frac{15}{4}$. To verify:

$$\begin{aligned}(2x+1)\left(\frac{1}{2}x - \frac{7}{4}\right) + \frac{15}{4} &= x^2 - \frac{7}{2}x + \frac{1}{2}x - \frac{7}{4} + \frac{15}{4} \\ &= x^2 - 3x + 2\end{aligned}$$

Clearly, in this example the remainder is not in $\mathbb{Z}[x]$. Therefore, the Division Theorem does not hold in $\mathbb{Z}[x]$. Moreover, the quotient and remainder are unique as guaranteed by the Division Theorem in $\mathbb{Q}[x]$.

Problem 3

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

1. 0 roots: $x^3 - 2 = 0$. x would have to satisfy $x^3 = 2$. Clearly no integer cubed equals 2 (so $n = 1$ is impossible). Suppose there exists a rational number in lowest terms $x = \frac{m}{n}$ with $|n| > 1$. Then $(\frac{m}{n})^3 = 2 \iff m^3 = 2n^3$. But this implies $n^3 \mid m^3$, so $n \mid m$, which contradicts that $\gcd(m, n) = 1$. Thus there is no rational root.
2. 1 root: $(x - 0)(x - 0)(x - 0) = 0$. Justification is obvious by root theorem.
3. 2 roots: $(x - 1)(x - 1)(x - 2) = 0$. Justification is obvious by root theorem.
4. 3 roots: $(x - 1)(x - 2)(x - 3) = 0$. Justification is obvious by root theorem.

Problem 4

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

Proof. Let f be a degree 3 polynomial with two roots, a, b such that $a \neq b$. We can express f in the form

$$f = (x-a)(x-b)l$$

where $l = (x-c)$ is another linear factor. If $c \neq a$ and $c \neq b$, then f has three distinct roots a, b, c, contradicting that f has only two roots. Therefore, $c = a$ or $c = b$, meaning one of the roots is repeated. ∎

Problem 6

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

Proof. Solving $f(x) = q$ is equivalent to solving $l = f - q = 0$. Now $\deg(l) = \deg(f)$ since $\deg(f) > \deg(q)$. By the Root Theorem, every root divides l, reducing its degree by 1. Since $\deg(l)$ is finite, the number of roots is finite. ∎

Problem 8

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

Theorem 1 (GCD Identity 4.7)**.** *If d is a gcd of polynomials f and g, then there exists polynomials a and b so that $d = af + bg$.*

Proof. Let $f, g \in \mathbb{Q}[x]$. By 4.5, there exists a last nonzero remainder r_{n-1} such that $r_{n-2} = q_{n-1}r_{n-1}$ and $r_{n-1} \neq 0$. This remainder r_{n-1} is the $\gcd(f, g)$. From the division steps in the algorithm, each remainder can be expressed as a linear combination of f and g. Thus there exist polynomials $a, b \in \mathbb{Q}[x]$ such that $r_{n-1} = af + bg$. By Theorem 4.6, any other gcd of f and g differs from r_{n-1} by a nonzero rational constant. Therefore, every gcd of f and g in $\mathbb{Q}[x]$ can be expressed as a linear combination of f and g. ∎

Problem 9

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

Proof. Consider the set of all linear combinations of the polynomials f, g:

$$S = \{fa + gb \,:\, a, b \in \mathbb{Q}[x]\}$$

We must show the $\gcd(f, g)$ belongs to this set. By the Well-ordering Principle, S contains an element d which has the smallest positive degree. Since $d \in S$:

$$d = fa_0 + gb_0$$

For some $a_0, b_0 \in \mathbb{Q}[x]$. Applying the Division Theorem to d, f we get $f = dq + r$. We now show $r = 0$. But:

$$r = f - dq = f - (fa_0 + gb_0)q = f(1 - qa_0) + g(-qb_0)$$

So $r \in S$. Because $\deg(r) < \deg(d)$, and d has the smallest degree of S, we must have $r = 0$. A similar argument shows $d \mid g$.

Now suppose c divides both f and g. Then $f = nc$ and $g = mc$ for some $n, m \in \mathbb{Q}[x]$. Then any linear combination of f and g is also a multiple of c:

$$fa + gb = nca + mcb = c(na + mb)$$

So $c \mid d$. Thus d is the gcd of f and g. ∎

Problem 10

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

Proof. ($\rightarrow$) Suppose $p \in \mathbb{Q}[x]$ has a multiplicative inverse. Let q be the multiplicative inverse of p such that $pq = 1$. Clearly $q \neq 0$. If $\deg(p) > 0$ then $\deg(pq) > 0$, but $\deg(pq) = \deg(1) = 0$. Thus $\deg(p) = 0$.

($\leftarrow$) Suppose $\deg(p) = 0$. It follows that $p \in \mathbb{Q}$. Then let $a, b \in \mathbb{Z}$ such that $p = \frac{a}{b}$. We know $a \neq 0$ since $\deg(p) \neq -\infty$. Let $q = \frac{b}{a}$, then $pq = \frac{a}{b} \cdot \frac{b}{a} = 1$. ∎

Problem 11

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

Proof. Clearly $g \neq 0$ since division by 0 is undefined. Suppose, for contradiction, that g is non-constant. That is, $\deg(g) > 0$. Consider $f \in \mathbb{Q}[x]$ such that $f \neq 0$ and $\deg(f) < \deg(g)$. Since $g \mid f$, there exists $c \in \mathbb{Q}[x]$ such that $f = c \cdot g$. But $\deg(f) < \deg(g)$ and $\deg(f) = \deg(c) + \deg(g) \geq \deg(g)$, a contradiction. Thus g is a non-zero constant polynomial. ∎

Problem 12

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

Proof. Let $f(x) = x^3$ and $g(x) = x$. Clearly as polynomials $f \neq g$. Now check each $a \in \mathbb{Z}_3$:

$$0^3 \equiv 0, \quad 1^3 \equiv 1, \quad 2^3 \equiv 2 \pmod 3.$$

Thus $f(a) \equiv g(a) \pmod 3$ for all $a \in \mathbb{Z}_3$, so f and g are equal as functions. ∎

Problem 13

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

Proof. Let $f(x) = 2x^2 + 2x^4 \in \mathbb{Z}_4[x]$. Now check each element in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$:

$$\begin{aligned}
f(0) &= 2 \cdot 0^2 + 2 \cdot 0^4 = 0, \\
f(1) &= 2 \cdot 1^2 + 2 \cdot 1^4 = 2 + 2 = 4 \equiv 0 \pmod 4, \\
f(2) &= 2 \cdot 2^2 + 2 \cdot 2^4 = 8 + 32 = 40 \equiv 0 \pmod 4, \\
f(3) &= 2 \cdot 3^2 + 2 \cdot 3^4 = 18 + 162 = 180 \equiv 0 \pmod 4.
\end{aligned}$$

Therefore $f(a) = 0$ for all $a \in \mathbb{Z}_4$, but $f(x)$ is not the zero polynomial. ∎

5 Factorization of Polynomials

Problem 1

Prove Theorem 5.1: A polynomial in $\mathbb{Q}[x]$ of degree greater than zero is either irreducible or the product of irreducibles.

Proof. Let f be a polynomial with degree greater than 0. We proceed by induction on the degree of f.

(**Base Case**) A polynomial of degree one is irreducible.

(**Induction Step**) Suppose the theorem holds for all polynomials of degree $m < n$. If f of degree n is irreducible, we are done. Suppose f is not irreducible; then $f = l \cdot g$ where $l, g \in \mathbb{Q}[x]$ and $\deg(l), \deg(g) < \deg(f)$. By the induction hypothesis, l and g can be expressed as a product of irreducible polynomials. Therefore, f can also be expressed as a product of irreducibles. ∎

Problem 2

Prove Theorem 5.2: A polynomial in $\mathbb{Q}[x]$ is irreducible if and only if it is prime.

Proof. Let f be an arbitrary polynomial in $\mathbb{Q}[x]$.

($\rightarrow$) Suppose f is irreducible and $f \mid lg$. Furthermore, suppose f does not divide l. We must show that $f \mid g$. Suppose that d is a common divisor of f and l. Then, because f is irreducible, d must be equal to f or a unit. Because f does not divide l, it must be that $\gcd(f, l) = 1$. So by the GCD identity there exist $x, y \in \mathbb{Q}[x]$ such that $1 = lx + fy$. Multiplying both sides by g gives

$$g = lgx + fgy.$$

Since f divides both terms on the right-hand side, it follows that $f \mid g$, as required.

($\leftarrow$) Suppose f is prime. Furthermore, suppose f has been factored as $f = lg$. Then $f \mid lg$, and so, without loss of generality, $f \mid l$. Thus, $l = fx$, and so $f = fxg$. Cancelling f gives $1 = xg$, and so both x and g must be degree 0 polynomials. This shows that the factorization $f = lg$ is trivial, as required. ∎

Problem 3

Prove Corollary 5.3: If an irreducible polynomial in $\mathbb{Q}[x]$ divides a product $f_1 f_2 f_3 \dots f_n$, then it divides one of f_i.

Proof. Let f be an irreducible polynomial in $\mathbb{Q}[x]$. Furthermore, suppose $f \mid f_1 f_2 f_3 \dots f_n$. We proceed by induction on n.

(**Base Case**) If $f \mid f_1 f_2$, then by the definition of being prime, $f \mid f_1$ or $f \mid f_2$.

(**Induction Step**) Assume the statement holds for $n - 1$; that is, if $f \mid f_1 f_2 \cdots f_{n-1}$, then $f \mid f_i$ for some $i < n$. Now suppose $f \mid f_1 f_2 \cdots f_{n-1} f_n$. Let $c = f_1 f_2 \cdots f_{n-1}$, so $f \mid c f_n$. By the definition of being prime, $f \mid c$ or $f \mid f_n$. By the induction hypothesis, if $f \mid c$, then $f \mid f_i$ for some $i < n$. Thus, in either case, f divides one of the f_i. ∎

Problem 4

Use Gauss's Lemma to determine which of the following are irreducible in $Q[x]$:

$$4x^3 + x - 2, 3x^3 - 6x^2 + x - 2, x^3 + x^2 + x - 1$$

Proof. If $f(x) = 4x^3 + x - 2$ can be factored then one of the factors is of the form $(ax + b)$ where $a, b \in \mathbb{Z}$. The only possible factors are $(4x \pm 1)$, $(4x \pm 2)$, $(2x \pm 2)$, $(2x \pm 1)$, $(x \pm 2)$, $(x \pm 1)$. This implies roots of $\pm\frac{1}{4}, \pm\frac{1}{2}, \pm 2, \pm 1$. By inspection this is not the case. Since f is irreducible in $\mathbb{Z}[x]$ by Gauss's Lemma f is irreducible in $Q[x]$. ∎

Proof. Let $f(x) = 3x^3 - 6x^2 + x - 2$. By inspection $x = 2$ is a root thus by the Root Theorem f is not irreducible in $\mathbb{Q}[x]$. ∎

Proof. If $f(x) = x^3 + x^2 + x - 1$ can be factored then one of the factors is of the form $ax + b$. The only possible factor is $(x \pm 1)$. By inspection this is not the case. Since f is irreducible in $\mathbb{Z}[x]$ by Gauss's Lemma f is irreducible in $Q[x]$. ∎

Problem 6

Prove the Rational Root Theorem 5.6.

Theorem 2 (Ration Root Theorem 5.6)**.** *Suppose that $f = a_0 + a_1 x + \cdots + a_n x^n$ is a polynomial in $\mathbb{Z}[x]$, and $\frac{p}{q}$ is a rational root; that is, p and q are integers, $q \neq 0$, and $f\left(\frac{p}{q}\right) = 0$. We may as well assume also that $gcd(p, q) = 1$. Then q divides the integer a_n, and p divides a_0.*

Proof. We first show $q \mid a_n$. Plugging in $\frac{p}{q}$ shows

$$f\left(\frac{p}{q}\right) = a_0 + a_1\frac{p}{q} + \cdots + a_n\left(\frac{p}{q}\right)^n = 0.$$

Then multiplying through by q^n shows

$$a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n = 0$$

Solving for $a_n p^n$ shows

$$a_n p^n = -a_0 q^n - a_1 p q^{n-1} - a_2 p^2 q^{n-2} - \cdots - a_{n-1} p^{n-1} q$$

Then factoring out q shows

$$a_n p^n = -q(a_0 q^{n-1} + a_1 p q^{n-2} + \cdots + a_{n-1} p^{n-2})$$

Since $\gcd(p, q) = 1$, it follows that $q \nmid p^n$. Thus $q \mid a_n$. We now show $p \mid a_0$. In the previous part it was shown that

$$a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n = 0$$

Solving for $a_0 q^n$ shows

$$a_0 q^n = -(a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n)$$

We can then factor out p so

$$a_0 q^n = -p(a_1 q^{n-1} + a_2 p q^{n-2} + \cdots + a_n p^{n-1})$$

Since $\gcd(p, q) = 1$, it follows that $p \nmid q^n$. Thus $p \mid a_0$. ∎

Problem 7

Use the Rational Root Theorem 5.6 to factor

$$2x^3 - 17x^2 - 10x + 9$$

Solution:

Using the Root Theorem we find the following possible roots

$$\text{Candidates} = \{\pm\frac{9}{1}, \pm\frac{9}{2}, \pm\frac{3}{1}, \pm\frac{3}{2}, \pm\frac{1}{1}, \pm\frac{1}{2}\}$$

Inspection shows that 9 and $\frac{1}{2}$ are roots. Dividing $2x^3 - 17x^2 - 10x + 9$ by $(x-9)(x-\frac{1}{2})$ gives us $(2x+2)$. Thus

$$2x^3 - 17x^2 - 10x + 9 = (x-9)(x-\frac{1}{2})(2x+2)$$

Problem 9

Use the Rational Root Theorem 5.6 (applied to $x^3 - 2$) to argue that $\sqrt[3]{2}$ is irrational.

Proof. For contradiction, suppose $\sqrt[3]{2}$ is a rational root for $x^3 - 2$. Since $\sqrt[3]{2}$ is rational it can be expressed as $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $\gcd(a,b) = 1$. By the Rational Root Theorem 5.6 it follows that $a \mid -2$ and $b \mid 1$. There exists $k_1, k_2 \in \mathbb{Z}$ such that $-2 = ak_1$ and $1 = bk_2$. Then

$$\sqrt[3]{2} = \frac{\frac{-2}{k_1}}{\frac{1}{k_2}} = \frac{-2k_2}{k_1}$$

It follows that $2 = \frac{-8k_2^3}{k_1^3}$. Multiplying by k_1^3 and dividing by 2 shows that k_1 is even. Rewriting $k_1 = 2k_3$ where $k_3 \in \mathbb{Z}$ we get

$$2 = \frac{-8k_2^3}{(2k_3)^3} \iff 2(2k_3)^3 = -8k_2^3 \iff 16k_3^3 = -8k_2^3.$$

Dividing by 8 shows that k_2 is even, contradicting that $\gcd(a,b) = 1$. ∎

Proof. For contradiction, suppose $\sqrt[3]{2}$ is a rational root of $x^3 - 2$. Then we can write $\sqrt[3]{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$. By the Rational Root Theorem 5.6 any rational root $\frac{a}{b}$ must satisfy $a \mid -2$ and $b \mid 1$. Thus the only possible rational roots are

$$\pm 1, \quad \pm 2.$$

Inspection shows that no combination works. Thus $\sqrt[3]{2}$ is irrational. ∎

Problem 10

Suppose that α is a real number (which might not be rational), and suppose that it is a root of a polynomial $p \in \mathbb{Q}[x]$; that is, $p(\alpha) = 0$. Suppose further that p is irreducible in $\mathbb{Q}[x]$. Prove that p has a minimal degree in the set

$$\mathcal{F} = \{f \in \mathbb{Q}[x] : f(\alpha) = 0 \text{ and } f \neq 0\}$$

Proof. Suppose there exists $g \in \mathbb{Q}[x]$ such that $\deg(g) < \deg(p)$. By the Division Theorem there exists $q, r \in \mathbb{Q}[x]$ such that $p = gq + r$ and $\deg(r) < \deg(g)$. Then

$$0 = p(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = 0 + r(\alpha) = r(\alpha),$$

thus $r(\alpha) = 0$.

Either $\deg(r) = 0$ or $\deg(r) > 0$. Suppose $\deg(r) = 0$, then since $r(\alpha) = 0$, r is the zero polynomial. Since $\deg(p) = \deg(g) + \deg(q)$ and $\deg(g) < \deg(p)$, it follows that $\deg(q) > 0$. Thus p has been factored into two polynomials with degree greater than 0, contradicting the irreducibility of p.

Now, suppose $\deg(r) > 0$. We can repeatedly apply the Division Theorem to form a sequence of decreasing remainders by their degrees.

For example, continuing where we left off, we divide p by r and by the Division Theorem obtain $r_1, q_1 \in \mathbb{Q}[x]$ such that

$$p = rq_1 + r_1.$$

Then $\deg(r_1) < \deg(r) < \deg(g)$.

If at any point a remainder r is a scalar, it must be the zero polynomial and we contradict the irreducibility of p. On the other hand, if the sequence never ends, then we contradict the finiteness of the degree of p. ∎

Problem 12

Construct polynomials of arbitrarily large degree, which are irreducible in $\mathbb{Q}[x]$.

Solution

$$\mathscr{F} = \{f \mid f = x^n - 2\}$$

By Eisenstein's Cirterion all $f \in \mathscr{F}$ are irreducible in $\mathbb{Z}[x]$. By Gauss's Lemma they are irreducible in $\mathbb{Q}[x]$.

Problem 13

(a) Prove that the equation $a^2 = 2$ has no ration solutions; that is, prove that $\sqrt{2}$ is irrational. (This part is a repeat of exercise 2.14.)
(b) Generalize part a,k by proving that $a^n = 2$ has no rational solutions, for all positive integers $n \geq 2$.

Proof. Let $p = 2$ and apply Eisenstein's Criterion to $a^2 - 2 = 0$. Clearly 2 is prime, $2 \mid -2$, $2 \nmid 1$, and $2^2 \nmid -2$. Thus there is no rational root. ∎

Proof. Same logic as before. ∎

Problem 14

Let $f \in \mathbb{Z}[x]$ and n an integer. Let g be the polynomial defined by $g(x) = f(x + n)$. Prove that f is irreducible in $\mathbb{Z}[x]$ if and only if g is irreducible in $\mathbb{Z}[x]$.

Proof. Let $y = x - n$, so that $f(x + n) = g(y) = g(x - n)$.

($\rightarrow$) Suppose f is irreducible in $\mathbb{Z}[x]$. For contradiction suppose g is reducible: $g = pl$ where $p, l \in \mathbb{Z}[x]$. Then

$$f(x) = g(x - n) = p(x - n)l(x - n),$$

contradicting the irreducibility of f. Thus g is irreducible in $\mathbb{Z}[x]$.

($\leftarrow$) Suppose g is irreducible in $\mathbb{Z}[x]$. For contradiction suppose f is reducible: $f = pl$ where $p, l \in \mathbb{Z}[x]$. Then

$$g(x) = f(x + n) = p(x + n)l(x + n),$$

contradicting the irreducibility of g. Thus f is irreducible in $\mathbb{Z}[x]$. ∎

Problem 15

(a) Apply Eisenstein's criterion 5.7 to check that the following polynomials are irreducible

$$5x^3 - 6x^2 + 2x - 14 \text{ and } 4x^5 + 5x^3 - 15x + 20$$

(b) Make the substition $x = y + 1$ to the polynomial $x^5 + 5x + 4$ that appears in Example 5.1. Show that the resulting polynomial is irreducible.
(c) Use the same technique as in part b to find a substitution $x = y + m$ so you can conclude the polynomial

$$x^4 + 6x^3 + 12x^2 + 10x + 5$$

is irreducible.
(d) Show that this technique works in general: Prove that if $f(x) \in \mathbb{Z}[x]$, then $f(x)$ is irreducible if and only if $f(y + m)$ is.

Solution (a): Consider $2 \nmid 5$. Also $2 \mid -6, 2, -14$. Finally $2^2 = 4 \nmid -14$ satisfying parts a, b, c of Eisenstein's criterion respectively. Thus $5x^3 - 6x^2 + 2x - 14$ is irreducible in $\mathbb{Z}[x]$.

Consider $5 \nmid 4$. Also $5 \mid 5, -15, 20$. Finally $5^2 = 25 \nmid 20$ satisfying parts a, b, c of Eisenstein's criterion respectively. Thus $4x^5 + 5x^3 - 15x + 20$ is irreducible in $\mathbb{Z}[x]$.

Solution (b): Substituting $x = y + 1$ into $x^5 + 5x + 4$ gives

$$(y + 1)^5 + 5(y + 1) + 4 = y^5 + 5y^4 + 10y^3 + 10y^2 + 10y + 10.$$

Consider $5 \nmid 1$. Also $5 \mid 5, 10, 10, 10, 10$. Finally $5^2 = 25 \nmid 10$ satisfying parts a, b, c of Eisenstein's criterion respectively. Thus the polynomial is irreducible in $\mathbb{Z}[y]$, and so $x^5 + 5x + 4$ is irreducible in $\mathbb{Z}[x]$.

Solution (c): Substituting $x = y + 1$ into $x^4 + 6x^3 + 12x^2 + 10x + 5$ gives

$$(y + 1)^4 + 6(y + 1)^3 + 12(y + 1)^2 + 10(y + 1) + 5 = y^4 + 10y^3 + 36y^2 + 56y + 34.$$

Consider $2 \nmid 1$. Also $2 \mid 10, 36, 56, 34$. Finally $2^2 = 4 \nmid 34$ satisfying parts a, b, c of Eisenstein's criterion respectively. Thus $y^4 + 10y^3 + 36y^2 + 56y + 34$ is irreducible in $\mathbb{Z}[y]$.

Proof. ($\longrightarrow$) Let $x = y + m$. Suppose $f(x)$ is irreducible. For contradiction, suppose $f(y + m)$ is reducible. Thus $f(y + m) = g(y)\, l(y)$ for some $g(y), l(y) \in \mathbb{Z}[y]$. But $x = y + m$, so $f(x) = g(x - m)\, l(x - m)$. Thus $f(x)$ is reducible, which is a contradiction.

($\longleftarrow$) Let $x = y + m$. Suppose $f(y + m)$ is irreducible. For contradiction, suppose $f(x)$ is reducible. Thus $f(x) = g(x)\, l(x)$ for some $g(x), l(x) \in \mathbb{Z}[x]$. But $x = y + m$, so $f(y + m) = g(y + m)\, l(y + m)$. Thus $f(y + m)$ is reducible, which is a contradiction. ∎

Problem 16

Prove Theorem 5.7 (Eisenstein's criterion).

Theorem 3 (Eisenstein's Criterion)**.** *Suppose that $f \in \mathbb{Z}[x]$, and*

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

Let p be a prime integer, and suppose that

1. *p divides a_k, for $0 \leq k < n$,*
2. *p does not divide a_n, and*
3. *p^2 does not divide a_0*

Then f is irreducible in $\mathbb{Z}[x]$.

Proof. Suppose for contradiction that f is reducible. Then there exist polynomials $g, l \in \mathbb{Z}[x]$ such that $f = gl$:

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = gl.$$

Now p either divides the constant term of g or l; otherwise it would not divide the constant term of f. Furthermore, if p divides the constant term of both, then p^2 would divide the constant term of f, which is impossible. Suppose w.l.o.g. that p divides the constant term of g and p does not divide the constant term of l. The constant term of l cannot be zero; otherwise the constant term of f would be zero.

Now consider the first coefficient b_j of g with $j > 0$ that is not divisible by p. This term exists since coefficientof largest degree term of g is not divisible by p. Let c be the constant term of l, so $p \nmid c$. Then the product $b_j c$ contributes to the coefficient a_j of f. Since $p \nmid b_j$ and $p \nmid c$, it follows that $p \nmid b_j c$.

Any other contributions to a_j come from products of terms of g and l where at least one factor is divisible by p, so those terms are divisible by p. Thus the coefficient a_j of f is

$$a_j = b_j c + (\text{terms divisible by } p),$$

which is not divisible by p, contradicting the assumption that p divides a_k for all $0 \leq k < n$. ∎

Problem 17

Let p be a positive prime integer. Then the polynomial

$$\phi_p = \frac{x^p - 1}{x - 1}$$

is called a **cyclotomic polynomial**.
(a) Write out, in the usual form for a polynomial, the cyclotomic polynomials for the first three primes.
(b) Prove that all cyclotomic polynomials ϕ_p are irreducible over $\mathbb{Z}[x]$, using Eisenstein's criterion 5.7 and Exercise 15*d* for $m = 1$.

Solution (a):

$$p = 2, \frac{x^2 - 1}{x - 1} = \frac{(x-1)(x+1)}{x-1} = x + 1$$

$$p = 3, \frac{x^3 - 1}{x - 1} = \frac{(x-1)(x^2+x+1)}{x-1} = x^2 + x + 1$$

$$p = 5, \frac{x^5 - 1}{x - 1} = \frac{(x-1)(x^4+x^3+x^2+x+1)}{x-1} = x^4 + x^3 + x^2 + x + 1$$

Proof. Let $x = y + 1$. Let p be an arbitrary prime. Then consider

$$\frac{(y+1)^p - 1}{(y+1) - 1} = \frac{(y+1)^p - 1}{y}$$

We can re-express the numerator using the binomial theorem

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

Substituting into the fraction gives

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

Multiplying numerator and denominator by y^{-1}/y^{-1} gives

$$\frac{\sum_{k=0}^{p}\binom{p}{k}y^{p-k}-1}{y}\cdot\frac{y^{-1}}{y^{-1}}=\sum_{k=0}^{p}\binom{p}{k}y^{p-k-1}-y^{-1}$$

Now we re-express this summation and extract the cases $k=0, p-1, p$ to show

$$\sum_{k=0}^{p}\binom{p}{k}y^{p-k-1}-y^{-1}=y^{p-1}+\sum_{k=1}^{p-2}\binom{p}{k}y^{p-k-1}+\binom{p}{p-1}y^{0}+\binom{p}{p}y^{-1}-y^{-1}=y^{p-1}+\sum_{k=1}^{p-2}\binom{p}{k}y^{p-k-1}+\binom{p}{p-1}$$

Now y^{p-1} is the term with the highest degree and its coefficient is 1. Clearly $p \nmid 1$, satisfying part (a) of Eisenstein's criterion. Furthermore, by Chapter 2 Problem 19, since p is a positive prime integer and k is an integer with $1 \leq k \leq p-1$, we have $p \mid \binom{p}{k}$. Additionally, $p \mid \binom{p}{p-1} = p$. Thus part (b) of Eisenstein's criterion is satisfied. Now, the constant term of $\frac{(y+1)^p-1}{y}$ is p. Since $a_0 = p < p^2$, we have $p^2 \nmid a_0$, satisfying part (c) of Eisenstein's criterion. By Problem 15 part d, it follows that all cyclotomic polynomials ϕ_p are irreducible over $\mathbb{Z}[x]$. ∎