# 18.781 Theory of Numbers

## Problem Set 1

**Official Solutions**

February 13, 2026

## Contents


1 §1.2 #27 2

2 §1.2 #36 3

3 §1.2 #43 4

4 §1.2 #45 5

5 §1.3 #5 7

6 §1.3 #21 9

7 §1.3 #26 11

8 §1.4 #3 12

9 §1.4 #4 13

10 §1.4 #8 14


## Disclaimer

This document contains the official solutions to Problem Set 1 of the Spring 2026 edition of 18.781 Theory of Numbers. While carefully proofread, all errors, typos, and omissions are mine alone. Please email allenees@mit.edu should you have any questions or concerns. All references made herein refer to Niven and Montgomery's *An Introduction to the Theory of Numbers*, 5th edition.

# 1 §1.2 #27

**Problem** (§1.2 #27)
Find positive integers $a$ and $b$ satisfying the equation $(a, b) = 10$ and $[a, b] = 100$ simultaneously. Find all solutions.

*Solution.* The only solutions are

$$(a, b) \in \{(10, 100), (20, 50), (50, 20), (100, 10)\}.$$

By Theorem 1.13, we have

$$1000 = 100 \cdot 10 = [a, b](a, b) = |ab| = ab,$$

so $a$ and $b$ are positive factors of 1000. Since $(a, b) = 10$, there exist some positive integers $x, y$ such that

$$a = 10x, \qquad b = 10y, \qquad (x, y) = 1.$$

This immediately gives $1000 = ab = 10x \cdot 10y = 100xy$, so $xy = 10$ and $(x, y) = 1$. The only such possibilities are

$$(x, y) \in \{(1, 10), (2, 5), (5, 2), (10, 1)\},$$

which gives

$$(a, b) \in \{(10, 100), (20, 50), (50, 20), (100, 10)\}.$$

One verifies that each pair satisfies $[a, b] = 100$. ■

**Remark 1.** *The main idea in this problem is using the properties of* greatest common divisor *and* least common multiple *concurrently. Theorem 1.13 directly provides the relation* $(a, b)[a, b] = |ab|$*, and we use Theorem 1.7 that*

$$1 = \left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = \left(\frac{10x}{10}, \frac{10y}{10}\right) = (x, y).$$

**Theorem** (Theorem 1.7)
If $d \mid a$ and $d \mid b$ and $d > 0$, then

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b).$$

If $(a, b) = g$, then

$$\left(\frac{a}{g}, \frac{b}{g}\right) = 1.$$

**Theorem** (Theorem 1.13)
If $m > 0$, $[ma, mb] = m[a, b]$. Also $[a, b] \cdot (a, b) = |ab|$.

# 2 §1.2 #36

**Problem** (§1.2 #36)
Prove that $(a, b, c) = ((a, b), c)$.

*Proof.* To show this, we show that $(a, b, c) \mid ((a, b), c)$ and $((a, b), c) \mid (a, b, c)$ by Theorem 1.1(4).

Theorem 1.4 characterizes the greatest common divisor of two numbers $a$ and $b$ as the positive common divisor of $a$ and $b$ that is divisible by every common divisor. Suppose $g = (a, b, c)$. Then $g \mid a$ and $g \mid b$ (i.e., $g$ is a common divisor of $a$ and $b$), so the theorem implies that $g \mid (a, b)$. But $g \mid c$ as well, so $g$ is a common divisor of $(a, b)$ and $c$. The theorem implies that $g \mid ((a, b), c)$.

To show $((a, b), c) \mid (a, b, c)$, let $g = ((a, b), c)$. Then $g \mid (a, b)$ and $g \mid c$. But $g \mid (a, b)$ implies that $g \mid a$ and $g \mid b$. Thus, $g \mid (a, b, c)$. ■

**Remark 2.** *A common way to prove that $x = y$ is showing both $x \mid y$ and $y \mid x$ and that $x, y > 0$ by Theorem 1.1(4). The positivity condition is guaranteed because the greatest common divisor is by definition positive.*

**Theorem** (Theorem 1.1(4))
$a \mid b$ and $b \mid a$ imply $a = \pm b$.

**Theorem** (Theorem 1.4)
The greatest common divisor $g$ of $b$ and $c$ can be characterized in the following two ways: (1) It is the least positive value of $bx + cy$ where $x$ and $y$ range over all integers; (2) it is the positive common divisor of $b$ and $c$ that is divisible by every common divisor.

# 3 §1.2 #43

**Problem** (§1.2 #43)
Prove that $a \mid bc$ if and only if $\dfrac{a}{(a,b)} \,\Big|\, c$.

*Proof.* ( $\Longrightarrow$ ) Suppose $a \mid bc$. Let $d = (a, b)$. There exist integers $s, t$ such that $a = ds$ and $b = dt$. Then we have $ds \mid dtc$, which implies $s \mid tc$ by Theorem 1.1(6). Moreover, $(s, t) = 1$, so Theorem 1.10 implies $s \mid c$. By definition, there exists some integer $x$ such that $sx = c$. But $s = a/d$ is an integer and

$$\frac{a}{d}x = c,$$

so $a/d \mid c$.

( $\Longleftarrow$ ) Let $d = (a, b)$, and suppose $a/d \mid c$. By definition, there exists some integer $x$ such that $a/d \cdot x = c$. Then $a \cdot bx/d = bc$, and $b/d$ is an integer. Thus $a \mid bc$. ■

**Remark 3.** *This is an* if and only if *statement, so one needs to prove both implications. The main idea of this problem is to use Theorem 1.10, which gives the result that $c \mid a$ when $c \mid ab$ provided that $(b, c) = 1$. Luckily, the solution to §1.2 #27 (Problem 1) suggests a way to force $(b, c) = 1$ (by using Theorem 1.7).*

**Theorem** (Theorem 1.1(6))
If $m \neq 0$, $a \mid b$ implies and is implied by $ma \mid mb$.

**Theorem** (Theorem 1.10)
If $c \mid ab$ and $(b, c) = 1$, then $c \mid a$.

# 4 §1.2 #45

**Problem** (§1.2 #45)

Prove that any positive integer $a$ can be uniquely expressed in the form

$$a = 3^m + b_{m-1}3^{m-1} + b_{m-2}3^{m-2} + \cdots + b_0$$

where each $b_j = 0$, 1, or $-1$.

*Proof.* The division algorithm gives unique integers $q$ and $r$ such that $a = 3q + r$ and $0 \leq r < 3$ (i.e., $r \in \{0, 1, 2\}$). We show that there exist integers $q'$ and $r'$ such that $a = 3q' + r'$ and $r' \in \{-1, 0, 1\}$. We construct $q'$ and $r'$ from $q$ and $r$.

- When $r \in \{0, 1\}$, take $q' = q$ and $r' = r$.
- When $r = 2$, take $q' = q + 1$ and $r' = -1$.

Note that $q' > 0$ because $a > 0$. We repeatedly apply this *modified division algorithm* to obtain two sequences of numbers $q_0, q_1, q_2, \ldots$ and $b_0, b_1, b_2, \ldots$ such that

$$\begin{aligned} a &= 3q_0 + b_0, \\ q_0 &= 3q_1 + b_1, \\ q_1 &= 3q_2 + b_2, \\ &\vdots \end{aligned}$$

such that $q_0, q_1, q_2, \ldots$ are all positive and $b_0, b_1, b_2 \ldots \in \{-1, 0, 1\}$. The sequence $q_0, q_1, q_2, \ldots$ is a strictly decreasing sequence of positive integers, so the algorithm terminates after $m$ iterations when $q_{m-1} = 0$. Thus we have that

$$\begin{aligned} a &= 3q_0 + b_0 \\ &= 3(3q_1 + b_1) + b_0 = 3^2 q_1 + 3b_1 + b_0 \\ &= 3^2(3q_2 + b_2) + 3b_1 + b_0 = 3^3 q_2 + 3^2 b_2 + 3b_1 + b_0 \\ &= \cdots \\ &= 3^{m-1}(3q_{m-1} + b_{m-1}) + 3^{m-2}b_{m-2} + \cdots + 3b_1 + b_0 \\ &= 3^m + 3^{m-1}b_{m-1} + 3^{m-2}b_{m-2} + \cdots + 3b_1 + b_0. \end{aligned}$$

This proves the *existence* of the expansion, but we still have to prove the *uniqueness*. To this end, suppose we have two expansions of $a$; that is,

$$3^m + b_{m-1}3^{m-1} + \cdots + b_0 = a = 3^n + b'_{n-1}3^{n-1} + b'_{n-2}3^{n-2} + \cdots + b'_0$$

for some integers $m, n \geq 0$ and $b_{m-1}, \ldots, b_0, b'_{n-1}, \ldots, b'_0 \in \{-1, 0, 1\}$. Without loss of generality suppose $m \geq n$. Then

$$0 = 3^m - 3^n + \sum_{j=n+1}^{m-1} b_j 3^j + \sum_{i=0}^{n-1} (b_i - b'_i)3^i,$$

or that

$$3^m = 3^n - \sum_{j=n+1}^{m-1} b_j 3^j + \sum_{i=0}^{n-1} (b'_i - b_i)3^i.$$

We first prove $m = n$. Suppose for the sake of contradiction that $m > n$. Taking the absolute value of both sides and applying the triangle inequality yields

$$\begin{aligned}
|3^m| &= \left| 3^n - \sum_{j=n+1}^{m-1} b_j 3^j + \sum_{i=0}^{n-1} (b'_i - b_i)3^i \right| \\
&\leq 3^n + \sum_{j=n+1}^{m-1} |b_j|\, 3^j + \sum_{i=0}^{n-1} |(b'_i - b_i)|\, 3^i \\
&\leq 2 \cdot 3^n + \sum_{j=n+1}^{m-1} 2 \cdot 3^j + \sum_{i=0}^{n-1} 2 \cdot 3^i \\
&= 2\left(1 + 3 + 3^2 + \cdots + 3^{m-1}\right) \\
&= 2 \cdot \frac{3^m - 1}{2} \\
&= 3^m - 1,
\end{aligned}$$

which is clearly absurd. (Here we use the fact that $|b_j| \leq 2$ and $|b'_i - b_i| \leq 2$ for all appropriate $i$ and $j$). Thus $m = n$. From then the expansion becomes

$$0 = \sum_{i=0}^{m-1} (b_i - b'_i)3^i.$$

Take the largest index $k \in \{0, \ldots, m-1\}$ for which $b_k - b'_k \neq 0$. In other words,

$$0 = \sum_{i=0}^{k} (b_i - b'_i)3^i.$$

We then have

$$0 \neq (b'_k - b_k)3^k = \sum_{i=0}^{k-1} (b_i - b'_i)3^i.$$

Taking the absolute value of both sides and applying the triangle inequality again yields

$$\begin{aligned}
|b'_k - b_k|3^k &= \left| \sum_{i=0}^{k-1} (b_i - b'_i)3^i \right| \\
&\leq \sum_{i=0}^{k-1} |b_i - b'_i|3^i \\
&\leq 2\left(1 + 3 + 3^2 + \cdots + 3^{k-1}\right) \\
&= 2 \cdot \frac{3^k - 1}{2} \\
&= 3^k - 1.
\end{aligned}$$

This implies $|b'_k - b_k| \leq 1 - 3^{-k}$, for which the only possibility is $|b'_k - b_k| = 0$. However, this means $b_k - b'_k = 0$, our required contradiction. Therefore, the required expansion is unique. ■

**Remark 4.** *This problem is an exercise on adapting the division algorithm. It is important to not only show* existence *but also* uniqueness.

# 5 §1.3 #5

**Problem** (§1.3 #5)
Prove that an integer is divisible by 11 if and only if the difference between the sum of the digits in the odd places and the sum of the digits in the even places is divisible by 11.

*Proof.* The key fact to observe is the following.

**Lemma 5**
If $i \geq 0$ is an even integer, then $11 \mid 10^i - 1$. If $i \geq 0$ is an odd integer, then $11 \mid 10^i + 1$.

Let $a$ be an integer. Write

$$a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

where each $0 \leq a_i \leq 9$ is an integer for each $i \in \{0, \ldots, k\}$. Assume without loss of generality that $k$ is odd. Now by Lemma 5, for every $i \in \{1, \ldots, k\}$ there exists some $n_i$ such that

$$10^i = \begin{cases} 11n_i + 1 & \text{if } i \text{ is even,} \\ 11n_i - 1 & \text{if } i \text{ is odd.} \end{cases}$$

Now we group the odd places and even places and write

$$\begin{aligned} a &= a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &= \left(a_k \cdot 10^k + a_{k-2} \cdot 10^{k-2} + \cdots a_1 \cdot 10\right) + \left(a_{k-1} \cdot 10^{k-1} + \cdots + a_2 \cdot 10^2 + a_0\right) \\ &= a_k(11n_k - 1) + a_{k-2}(11n_{k-2} - 1) + \cdots a_1(11n_1 - 1) \\ &\quad + a_{k-1}(11n_{k-1} + 1) + \cdots + a_2(11n_2 + 1) + a_0 \\ &= 11(a_k n_k + a_{k-2}n_{k-2} + \cdots + a_1 n_1) - (a_k + a_{k-2} + \cdots + a_1) \\ &\quad + 11(a_{k-1}n_{k-1} + a_{k-3}n_{k-3} + \cdots + a_0) + (a_{k-1} + a_{k-3} + \cdots + a_0) \\ &= 11(a_k n_k + a_{k-1}n_{k-1} + \cdots + a_1 n_1) + \big((a_{k-1} + a_{k-3} + \cdots + a_0) - (a_k + a_{k-2} + \cdots + a_1)\big), \end{aligned}$$

($\implies$) Suppose $11 \mid a$. But $11 \mid 11(a_k n_k + a_{k-1}n_{k-1} + \cdots + a_1 n_1)$, so 11 divides the difference, which is precisely

$$(a_{k-1} + a_{k-3} + \cdots + a_0) - (a_k + a_{k-2} + \cdots + a_1).$$

($\impliedby$) Suppose

$$11 \mid (a_{k-1} + a_{k-3} + \cdots + a_0) - (a_k + a_{k-2} + \cdots + a_1).$$

But $11 \mid 11(a_k n_k + a_{k-1}n_{k-1} + \cdots + a_1 n_1)$, so 11 divides the sum, which is $a$.

It remains to prove Lemma 5.

*Proof of Lemma 5.* Suppose that $i \geq 0$ is even. Then $i = 2n$ for some integer $n$. Then factoring gives

$$\begin{aligned} 10^i - 1 &= 10^{2n} - 1 \\ &= (10 + 1)\left(10^{2n-1} - 10^{2n-2} + \cdots + 10 - 1\right), \end{aligned}$$

from which we immediately see that $11 = 10 + 1$ is a divisor of $10^i - 1$.

Now suppose $i \geq 0$ is odd. Then $i = 2n + 1$ for some integer $n$. Then factoring gives

$$\begin{aligned} 10^i + 1 &= 10^{2n+1} + 1 \\ &= (10 + 1)\left(10^{2n} - 10^{2n-1} + \cdots - 10 + 1\right), \end{aligned}$$

from which we immediately see that $11 = 10 + 1$ is a divisor of $10^i + 1$. ■

The proof is finished. ■

**Remark 6.** *Proving this divisibility rule suggests that we look at the base-10 expansion of $a$, which motivates Lemma 5. The important part of this problem is proving Lemma 5 and recognizing that if $d \mid x$ and $d \mid y$, then $d$ divides any integer linear combination of $x$ and $y$, including the sum and difference (cf. Theorem 1.1(c)).*

**Theorem** (Theorem 1.1(c))
$a \mid b$ and $a \mid c$ imply $a \mid (bx + cy)$ for any integers $x$ and $y$.

# 6 §1.3 #21

**Problem** (§1.3 #21)
Prove that $[a,b,c](ab,bc,ca) = |abc|$.

*Proof.* By the fundamental theorem of arithmetic, write

$$a = \pm \prod_p p^{\alpha(p)},$$
$$b = \pm \prod_p p^{\beta(p)},$$
$$c = \pm \prod_p p^{\gamma(p)},$$

for exponents $\alpha(p)$, $\beta(p)$, and $\gamma(p)$. By §1.2 #36 (Problem 2) we see that

$$\begin{aligned}(ab,bc,ca) &= ((ab,bc),ca)\\ &= \left(\left(\prod_p p^{\alpha(p)+\beta(p)}, \prod_p p^{\beta(p)+\gamma(p)}\right), \prod_p p^{\gamma(p)+\alpha(p)}\right)\\ &= \left(\prod_p p^{\min(\alpha(p)+\beta(p),\beta(p)+\gamma(p))}, \prod_p p^{\gamma(p)+\alpha(p)}\right)\\ &= \prod_p p^{\min(\min(\alpha(p)+\beta(p),\beta(p)+\gamma(p)),\gamma(p)+\alpha(p))}\\ &= \prod_p p^{\min(\alpha(p)+\beta(p),\beta(p)+\gamma(p),\gamma(p)+\alpha(p))}.\end{aligned}$$

On the other hand,

$$[a,b,c] = \prod_p p^{\max(\alpha(p),\beta(p),\gamma(p))}.$$

The key fact here is the following.

**Lemma 7**
For each $p$,

$$\min(\alpha(p)+\beta(p),\beta(p)+\gamma(p),\gamma(p)+\alpha(p)) + \max(\alpha(p),\beta(p),\gamma(p)) = \alpha(p)+\beta(p)+\gamma(p).$$

*Proof of Lemma 7.* Suppose $\min(\alpha(p)+\beta(p),\beta(p)+\gamma(p),\gamma(p)+\alpha(p)) = \alpha(p)+\beta(p)$. Then

$$\alpha(p)+\beta(p) \le \beta(p)+\gamma(p) \quad \text{and} \quad \alpha(p)+\beta(p) \le \gamma(p)+\alpha(p).$$

This immediately implies $\gamma(p) \ge \alpha(p)$ and $\gamma(p) \ge \beta(p)$, so $\max(\alpha(p),\beta(p),\gamma(p)) = \gamma(p)$. ∎

Hence

$$[a,b,c](ab,bc,ca) = \prod_p p^{\min(\alpha(p)+\beta(p),\beta(p)+\gamma(p),\gamma(p)+\alpha(p))+\max(\alpha(p),\beta(p),\gamma(p))} = \prod_p p^{\alpha(p)+\beta(p)+\gamma(p)} = |abc|,$$

as desired. ∎

**Remark 8.** *Important of note is the fundamental theorem of arithmetic. This problem generalizes the two-dimensional case that*

$$(a, b) = \prod_p p^{\min(\alpha(p),\beta(p))},$$
$$[a, b] = \prod_p p^{\max(\alpha(p),\beta(p))},$$

*so*

$$[a, b](a, b) = \prod_p p^{\min(\alpha(p),\beta(p))+\max(\alpha(p),\beta(p))} = \prod_p p^{\alpha(p)+\beta(p)} = ab,$$

*which is Theorem 1.13.*

**Theorem** (Fundamental Theorem of Arithmetic, Theorem 1.16)
The factoring of any integer $n > 1$ into primes is unique apart from the order of the prime factors.

# 7 §1.3 #26

**Problem** (§1.3 #26)
Prove that there are infinitely many primes of the form $4n+3$; of the form $6n+5$. (H)

*Proof.* We first prove that there are infinitely many primes of the form $4n+3$. Suppose for the sake of contradiction that the number of primes of the form $4n+3$ is finite; say $p_1, p_2, \ldots, p_r$ are the only $r$ such primes. Consider

$$N = 4p_1p_2\cdots p_r - 1.$$

Clearly $N$ is of the form $4n+3$. If $N$ is prime, then we achieved our desired contradiction. If $N$ is composite, then some odd prime $p$ divides $N$ since $N$ is odd. Certainly $p \neq p_i$ for any $i \in \{1, \ldots, r\}$; if $p = p_i$ and $p \mid N$ and $p \mid 4p_1p_2\cdots p_r$, then $p$ divides the difference $\pm 1$, which is clearly absurd. Therefore, $p$ is not of the form $4n+3$. Since $p$ is odd, $p$ is of the form $4n+1$. This means that all prime factors of $N$ are of the form $4n+1$. But any product of numbers of the form $4n+1$ has the form $4n+1$ (i.e., the product of numbers of the form $4n+1$ is closed under multiplication) as

$$(4n+1)(4m+1) = 16nm + 4(n+m) + 1 = 4(4nm+n+m) + 1.$$

Therefore, $N$ is of the form $4n+1$, our required contradiction.

Similarly, we show that there is an infinite number of primes of the form $6n+5$. Suppose for the sake of contradiction that the number of primes of the form $6n+5$ is finite; say $p_1, p_2, \ldots, p_r$ are the only $r$ such primes. Consider

$$N = 6p_1p_2\cdots p_r - 1.$$

Clearly $N$ is of the form $6n+5$. If $N$ is prime, then we achieved our desired contradiction. If $N$ is composite, then some odd prime $p \neq 3$ divides $N$ since $N$ is odd. For the same reason as above, $p \neq p_i$ for any $i \in \{1, \ldots, r\}$. Therefore, $p$ is not of the form $6n+5$, so $p$ is of the form $6n+1$. (Why can't $p$ be of the form $6n+a$, where $a \in \{2, 3, 4\}$?) But the product of numbers of the form $6n+1$ is closed under multiplication. Therefore, $N$ is of the form $6n+1$, our required contradiction. ■

**Remark 9.** *This problem is mainly an exercise at emulating and generalizing Euclid's proof of the infinitude of primes.*

**Theorem** (Theorem 1.17)
The number of primes is infinite. That is, there is no end to the sequence of primes $2, 3, 5, 7, 11, 13, \ldots$.

# 8 §1.4 #3

**Problem** (§1.4 #3)

(a) By comparing the coefficient of $z^k$ in the polynomial identity

$$\sum_{k=0}^{m+n} \binom{m+n}{k} z^k = (1+z)^{m+n} = (1+z)^m (1+z)^n$$
$$= \left( \sum_{k=0}^{m} \binom{m}{k} z^k \right) \left( \sum_{k=0}^{n} \binom{n}{k} z^k \right)$$

show that

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

(b) Let $\mathscr{U}$ and $\mathscr{V}$ be disjoint sets containing $m$ and $n$ elements, respectively, and put $\mathscr{S} = \mathscr{U} \cup \mathscr{V}$. Show that the number of subsets $\mathscr{A}$ of $\mathscr{S}$ that contain $k$ elements and that also have the property that $\mathscr{A} \cap \mathscr{U}$ contains $i$ elements is $\binom{m}{i}\binom{n}{k-i}$. Interpret this identity combinatorially.

(c) Show that for $n \geqslant 0$,

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

*Proof.* (a) The $z^k$ coefficient is the sum of all possible combinations of products of $z^{k_1}$ and $z^{k_2}$ terms such that $k_1 + k_2 = k$. More precisely,

$$\binom{m+n}{k} = \sum_{\substack{k_1 \in \{0,\dots,m\} \\ k_2 \in \{0,\dots,n\} \\ k_1+k_2=k}} \binom{m}{k_1}\binom{n}{k_2} = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}.$$

(b) For a subset $\mathscr{A} \subseteq \mathscr{S}$, we have

$$\mathscr{A} = \mathscr{A} \cap \mathscr{S} = \mathscr{A} \cap (\mathscr{U} \cup \mathscr{V}) = (\mathscr{A} \cap \mathscr{U}) \cup (\mathscr{A} \cap \mathscr{V}).$$

Thus, to construct $\mathscr{A}$ we first choose $i$ elements from $\mathscr{U}$ and the remaining $k-i$ elements from $\mathscr{V}$. The number of ways for the former and the latter are $\binom{m}{i}$ and $\binom{n}{k-i}$, respectively, so the total number is $\binom{m}{i}\binom{n}{k-i}$. Therefore, the identity states that the total number of subsets $\mathscr{A}$ that contain $k$ elements with any number of elements in $\mathscr{U}$ is $\binom{m+n}{k}$.

(c) Fix any $n \geqslant 0$ and take $m = n$. Using the symmetry $\binom{n}{k} = \binom{n}{n-k}$ for any $k \in \{0, \dots, n\}$ part (a) implies

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n},$$

as required.

The proof is complete. ∎

# 9 §1.4 #4

**Problem** (§1.4 #4)

(a) Suppose that $\mathscr{S}$ contains $2n$ elements, and that $\mathscr{S}$ is partitioned into $n$ disjoint subsets each one containing exactly two elements of $\mathscr{S}$. Show that this can be done in precisely

$$(2n-1)(2n-3)\cdots 5\cdot 3\cdot 1 = \frac{(2n)!}{2^n n!}$$

ways.

(b) Show that $(n+1)(n+2)\cdots(2n)$ is divisible by $2^n$, but not by $2^{n+1}$.

*Proof.* (a) Let $s_1, \ldots, s_{2n}$ be the elements of $\mathscr{S}$.

We can view the partitioning of $\mathscr{S}$ into $n$ disjoint subsets of two elements equivalently as $n$ matchings, where each matching is a pair of two elements. At each of the $n$ iterations, we find a match for the unmatched element with the largest index.

1. On the first iteration, we find a match for $x_{2n}$. There are $2n-1$ choices.
2. After finding a match for $x_{2n}$, we find a match for the next unmatched element with the largest index. There are $2n-3$ choices.
3. This continues until we finish with the $n$th match, of which there is only one choice remaining.

Therefore, the total number of ways is

$$(2n-1)(2n-3)\cdots 5\cdot 3\cdot 1.$$

On the other hand, we can view the partitioning of $\mathscr{S}$ into $n$ disjoint subsets equivalently as arrangements of $x_1, \ldots, x_{2n}$, with each arrangement giving rise to $n$ disjoint sets by picking the first two for the first subset, the next two for the second subset, and so on. There are $(2n)!$ arrangements of $x_1, \ldots, x_{2n}$, but arrangements give rise to the same partitioning regardless of

- the ordering of the $n$ subsets, of which there are $n!$ ways; and
- the ordering of the two elements $2! = 2$ in each of the $n$ subsets for $2^n$ ways.

Therefore, the total number of ways is $\dfrac{(2n)!}{2^n n!}$. Because both ways count the same number we have

$$(2n-1)(2n-3)\cdots 5\cdot 3\cdot 1 = \frac{(2n)!}{2^n n!}.$$

(b) Note that $(n+1)(n+2)\cdots(2n) = (2n)!/n!$. From the identity, we have

$$2^n\big((2n-1)(2n-3)\cdots 5\cdot 3\cdot 1\big) = \frac{(2n)!}{n!} = (n+1)(n+2)\cdots(2n),$$

so certainly $2^n \mid (n+1)(n+2)\cdots(2n)$. The corresponding factor is $(2n-1)(2n-3)\cdots 5\cdot 3\cdot 1$; each term is odd, so there are no additional factors of 2. In particular, $2^{n+1} \nmid (n+1)(n+2)\cdots(2n)$.

The proof is complete. ∎

# 10 §1.4 #8

**Problem** (§1.4 #8)

Give three proofs that

$$\sum_{m=0}^{M} \binom{m+k}{k} = \binom{k+M+1}{k+1}.$$

(a) With $k$ fixed, induct on $M$, using Theorem 1.20.

(b) Let $\mathscr{S} = \{1, 2, \ldots, k+M+1\}$. Count the number of subsets $\mathscr{A}$ of $\mathscr{S}$ containing $k+1$ elements, with the maximum one being $k+m+1$.

(c) Compute the coefficient of $z^M$ in the identity

$$(1 + z + z^2 + \cdots) \cdot \frac{1}{(1-z)^{k+1}} = \frac{1}{(1-z)^{k+2}}.$$

*Proof.* (a) We fix an integer $k$. We proceed by induction on $M$. When $M = 0$, we have

$$1 = \binom{k}{k} = \sum_{m=0}^{M} \binom{m+k}{k} = \binom{k+M+1}{k+1} = 1.$$

Now assume the proposition holds for some positive integer $M$; that is,

$$\sum_{m=0}^{M} \binom{m+k}{k} = \binom{k+M+1}{k+1};$$

we show the proposition holds for $M+1$; that is,

$$\sum_{m=0}^{M+1} \binom{m+k}{k} = \binom{k+M+2}{k+1}.$$

But the inductive hypothesis implies

$$\sum_{m=0}^{M+1} \binom{m+k}{k} = \sum_{m=0}^{M} \binom{m+k}{k} + \binom{k+M+1}{k} = \binom{k+M+1}{k+1} + \binom{k+M+1}{k}.$$

Let $\mathscr{S} = \{1, \ldots, k+M+2\}$. Any subset $\mathscr{A}$ of $\mathscr{S}$ of size $k+1$ either contains or does not contain $k+M+2$. In the first case, $\mathscr{A} = \{k+M+2\} \cup \mathscr{A}'$, where $\mathscr{A}'$ is a subset of $\{1, \ldots, k+M+1\}$ of size $k$. By Theorem 1.20, $\binom{k+M+1}{k}$ such subsets. In the second case, $\mathscr{A}$ is also a subset of $\{1, \ldots, k+M+1\}$ of size $k+1$; by Theorem 1.20, there are $\binom{k+M+1}{k+1}$ such subsets. Finally, by Theorem 1.20, the total number of subsets $\mathscr{A}$ is $\binom{k+M+2}{k+1}$, so adding the two cases give

$$\binom{k+M+1}{k+1} + \binom{k+M+1}{k} = \binom{k+M+2}{k+1},$$

which completes the proof.

(b) With $k$ fixed again, let $\mathscr{A}$ be a subset of $\mathscr{S}$ containing $k+1$ elements such that its maximum element is $k+m+1$ for some $m \in \{0, \ldots, M\}$. Therefore, $\mathscr{A} = \{k+m+1\} \cup \mathscr{A}'$ for some $\mathscr{A}' \subseteq \{1, \ldots, k+m\}$ of size $k$. There

are $\binom{m+k}{k}$ such $\mathscr{A}'$ and hence of $\mathscr{A}$. Every subset of $\mathscr{S}$ of size $k+1$ has a maximum element of the form $k+m+1$ for some $m \in \{0, \ldots, M\}$, so summing $\binom{m+k}{k}$ across the same range of $m$ gives the total number of subsets of $\mathscr{S}$ of size $k+1$, which is $\binom{k+M+1}{k+1}$.

(c) We fix $k$ again. The key property to use is the expansion below.

**Lemma 10**

For any integer $k \geq 1$,

$$\frac{1}{(1-z)^{k+1}} = \sum_{m=0}^{\infty} \binom{m+k}{k} z^m$$

as a formal power series.

*Proof of Lemma 10.* We proceed by induction. For $k = 1$, we have

$$\frac{1}{1-z} = 1 + z + z^2 + z^3 + \cdots = \sum_{m=0}^{\infty} z^m.$$

Taking the formal derivative with respect to $z$ yields

$$\frac{1}{(1-z)^2} = 1 + 2z + 3z^2 + \cdots = \sum_{m=0}^{\infty} (m+1) z^m = \sum_{m=0}^{\infty} \binom{m+k}{k} z^m.$$

Now assume the proposition holds for some integer $k$; that is,

$$\frac{1}{(1-z)^{k+1}} = \sum_{m=0}^{\infty} \binom{m+k}{k} z^m = 1 + \sum_{m=1}^{\infty} \binom{m+k}{k} z^m.$$

Taking the formal derivative with respect to $z$ yields

$$\frac{k+1}{(1-z)^{k+2}} = \sum_{m=1}^{\infty} \binom{m+k}{k} m z^{m-1} = \sum_{m=0}^{\infty} \binom{m+k+1}{k} (m+1) z^m,$$

which implies

$$\frac{1}{(1-z)^{k+2}} = \sum_{m=0}^{\infty} \binom{m+k+1}{k} \frac{m+1}{k+1} z^m = \sum_{m=0}^{\infty} \binom{m+k+1}{k+1} z^m,$$

which completes the induction. ∎

Applying Lemma 10 gives

$$(1 + z + z^2 + \cdots) \cdot \sum_{m=0}^{\infty} \binom{m+k}{k} z^m = \sum_{m=0}^{\infty} \binom{m+k+1}{k} z^m.$$

The $z^M$ coefficient of the right-hand side is very much $\binom{k+M+1}{k}$. Similar to §1.4 #3 (Problem 8), the $z^M$ coefficient on the left-hand side is the sum of all possible combinations of products of $z^{m_1}$ and $z^{m_2}$ terms such that $m_1 + m_2 = M$. More precisely, this is

$$\sum_{\substack{m_1 \in \{0,\ldots,M\} \\ m_2 \in \{0,\ldots,M\} \\ m_1 + m_2 = M}} 1 \cdot \binom{m_2+k}{k} = \sum_{m=0}^{M} \binom{m+k}{k}.$$

Because the coefficients are equal we must have

$$\sum_{m=0}^{M} \binom{m+k}{k} = \binom{k+M+1}{k}.$$

The proof is complete. ■

**Remark 11.** *Since the identity starts with initial index $m = 0$, starting the base case of the induction at $M = 0$ is crucial for the complete argument. This exercise shows the variety of proofs for identities of binomial coefficients.*

**Theorem** (Theorem 1.20)
Let $\mathscr{S}$ be a set containing exactly $n$ elements. For any nonnegative integer $k$, the number of subsets of $\mathscr{S}$ containing precisely $k$ elements is $\binom{n}{k}$.