Problems In Mathematics for Computer Science

Son To
<son.trung.to@gmail.com>

Leadoo Marketing Technologies

22^{nd} May, 2021

v0.2

Preface

This is a research project in which I try to read the notes and solve all the problems from [1]

Contents

Preface i

Contents ii

I Notes 1

1 What is a Proof? 3
1.1 Propositions . . . 3
1.2 Predicates . . . 3
1.3 The Axiomatic Method . . . 4
1.4 Our axioms . . . 4
1.4.1 Logical deductions . . . 4
1.4.2 Patterns of Proof . . . 4
1.5 Proving an Implication . . . 4
1.5.1 Method #1: $P \Rightarrow Q$ . . . 4
1.5.2 Method #2: Contrapositive: $\neg Q \Rightarrow \neg P$ . . . 4
1.6 Proving an "if and only if" . . . 4
1.6.1 Method #1: Prove each statement implies the other . . . 4
1.6.2 Method #2: Construct a chain of iffs . . . 4
1.7 Proof by Cases . . . 4
1.8 Proof by Contradiction . . . 5

2 The Well Ordering Principle (WOP) 7

II Problems and Exercises 11

1 What is a Proof? 13

2 The Well Ordering Principle (WOP) 25

Bibliography 27

Part I

Notes

Chapter 1

What is a Proof?

1.1 Propositions

Definition 1.1. A *proposition* is a statement (communication) that is either true or false.

Claim 1.1.1. $\forall\ n \in \mathbb{N}$, $p ::= n^2 + n + 41$ *is prime*

Question: Is this claim true or false?

Claim 1.1.2. *No polynomial with integer coefficients can map all nonnegative numbers into primes, unless it's a constant.*

Question: Is this true or false?

Claim 1.1.3 (Euler's Conjecture)**.** $\forall a, b, c, d \in \mathbb{Z}^+.\ a^4 + b^4 + c^4 \neq d^4$

Claim 1.1.4. $313(x^3 + y^3) = z^3$ *has no solution when* $x, y, z \in \mathbb{Z}^+$

Claim 1.1.5 (Four Color Theorem)**.** *Every map can be colored with* 4 *colors so that adjacent regions have different colors.*

Claim 1.1.6 (Fermat's Last Theorem)**.** $\forall a, b, c \in \mathbb{Z}^+\ \forall n > 2, n \in \mathbb{Z}.\ a^n + b^n \neq c^n$

Claim 1.1.7 (Goldbach)**.** *Every even integer greater than* 2 *is the sum of two primes.*

1.2 Predicates

Definition 1.2. A *predicate* is a proposition whose truth depends on the value of one or more variables.

If P is a predicate, then $P(n)$ is either *true* or *false*, depending on the value of n.

1.3 The Axiomatic Method

Definition 1.3. A *proof* is a sequence of logical deductions from a set of axioms and previous proved propositions that concludes with the proposition in question.

- *Theorems*
- *Lemma*
- *Corollary*

⇒ Axiomatic Method

1.4 Our axioms

1.4.1 Logical deductions

Keywords: *Logical deductions(inference rules), antecedents, conclusion, modus ponens*

1.4.2 Patterns of Proof

Many proofs follow specific templates... Many special techniques later on.

1.5 Proving an Implication

Definition 1.4. *Implications* means $P \Rightarrow Q$

1.5.1 Method #1: $P \Rightarrow Q$

1.5.2 Method #2: Contrapositive: $\neg Q \Rightarrow \neg P$

1.6 Proving an "if and only if"

1.6.1 Method #1: Prove each statement implies the other

1.6.2 Method #2: Construct a chain of iffs

1.7 Proof by Cases

Amusing theorem

Theorem 1.7.1. *Every collection of 6 people includes a club of 3 people or a group of 3 strangers.*

Proof. The proof is by case analysis. Let x be one of those 6 people. Among 5 other people, there are two scenarios:

1. At least 3 people have met x
2. At least 3 people have not met x

We argue that these two cases are exhaustive since we are dividing the 5 people into two groups: those who have met x and those who have not.

Case 1: Suppose that at least 3 people have met x
This is divided further more into two subcases:

Case 1.1: No pairs among those people have met each other. In this case, they form a group of at least 3 strangers. Thus, the theorem holds in this subcase.

Case 1.2: At least one pair in those people have met. Adding x to such pair forms a club of at least 3 people. The theorem is proved in this subcase.

This implies that the theorem holds for Case 1.

Case 2: Suppose that at least 3 people have not met x
This again splits the case into two subcases:

Case 2.1: All pairs among those people have met each other. In this case, they form a club of at least 3 people. Thus the theorem holds in this subcase.

Case 2.2: At least one pair in those people have not met. Adding x to such pair forms a group of at least 3 strangers. The theorem holds in this subcase.

This implies that the theorem holds for Case 2.

We have proved the theorem. □

1.8 Proof by Contradiction

Theorem 1.8.1. $\sqrt{2}$ *is irrational*

Proof. We use proof by contradiction. Suppose $\sqrt{2}$ is rational, then $\sqrt{2} = \frac{p}{q}$, where p and q are integers that have no common factors. Then $2 = \frac{p^2}{q^2}$, which means $p^2 = 2q^2$. Since p^2 is even, p must be even (easily proved by contradiction again). W.l.o.g, assume $p = 2k$ for some integer k. Then $4k^2 = 2q^2 \Rightarrow q^2 = 2k^2$, which implies that q is also even. However, this contradicts the fact that p and q have no common factors. Therefore $\sqrt{2}$ is irrational. □

Chapter 2

The Well Ordering Principle (WOP)

Every nonempty set of nonnegative integers has a smallest element.

Claim 2.0.1. *$\sqrt{2}$ is irrational implies the well ordering principle has been assumed.*

Proof. Assume by contradiction that $\sqrt{2} = \frac{m}{n}$ where it cannot be rewritten in the lowest common denominator. Let $\mathbb{C}$ be the set of all numerators of such fractions. By assumption, $\mathbb{C}$ is non-empty as $m \in \mathbb{C}$. By WOP, there exists a smallest element m_0. By definition of $\mathbb{C}$, there exists $n_0 > 0, n \in \mathbb{Z}$ such that

$$\frac{m_0}{n_0} \in \mathbb{C}$$

By definition of $\mathbb{C}$, there must be an integer $k > 1$ such that

$$\frac{\frac{m_0}{k}}{\frac{n_0}{k}} = \frac{m_0}{n_0}$$

Therefore, $\frac{m_0}{k} \in \mathbb{C}$. But then $\frac{m_0}{k} < m_0$, contradicting that m_0 is the smallest element in $\mathbb{C}$. Therefore, $\mathbb{C} = \emptyset$, meaning there is no fractions that cannot be written in the lowest common denominator. □

Claim 2.0.2.

$$\sum_{1}^{n} i = n(n+1)/2 \tag{2.1}$$

Proof. The proof is by contradiction. Suppose that there is a set of $\mathbb{C}$ such that,

$$\mathbb{C} = \left\{ n \in \mathbb{N} \;\middle|\; \sum_{1}^{n} i \neq n(n+1)/2 \right\}$$

By assumption, $\mathbb{C}$ is a non-empty set of non-negative integers. By WOP, there is the smallest element $n_0 \in \mathbb{C}$ such that 2.1 is satisfied when $n < n_0$. Since 2.1 is true when $n = 0$, it follows that $n_0 > 0$. Therefore, the equation 2.1 must hold true for all $0 < n_0 - 1 < n_0$; this means that,

$$1 + 2 + \ldots + n_0 - 1 = \frac{(n_0 - 1)n_0}{2}$$

Adding n_0 to both sides,

$$1 + 2 + \ldots + (n_0 - 1) + n_0 = \frac{n_0(n_0 + 1)}{2}$$

Therefore, the equation 2.1 holds true for n_0, but this contradicts that $n_0 \in \mathbb{C}$. □

Unique Factorization Theorem, also known as *Prime Factorization Theorem* and the *Fundamental Theorem of Arithmetic*, states that every integer greater than one has a unique expression as a product of prime numbers.

Claim 2.0.3. *Every positive integer greater than one can be factored as a product of primes.*

Proof. Let $\mathbb{C}$ be the set of all positive integers greater than one that cannot be factored as a product of primes. Suppose by contradiction that $\mathbb{C} \neq \emptyset$. By WOP, there exists a smallest $c_0 \in \mathbb{C}$ such that $c_0 = c_1 \times c_2$ where c_1 and c_2 are nonnegative and non-prime integers. Since $c_1, c_2 \notin \mathbb{C}$, they are factored as a product of primes,

$$c_1 \times c_2 = p_{11}p_{21} \cdots \; p_{k1}p_{12}p_{22} \cdots \; p_{j2}$$

for some postive integers k, j. However, this implies that c_0 can be factored into a product of primes, contradicting that $c_0 \in \mathbb{C}$. □

Definition 2.1 (***Well-ordered of a set***)**.** A set of real numbers is *well ordered* when EACH of its NONEMPTY SUBSETS HAS a minimum element.

Remark 2.1. The set of *nonnegative integers* is well ordered. So is $r\mathbb{N}$

The set of *nonnegative rationals* has minimal element but is *not* well ordered.

Remark 2.2. Well ordering commonly comes up in computer science as a method for proving that computations won't run forever.

Claim 2.0.4. *For any nonnegative integer n the set of integers greater than or equal to $-n$ is well ordered.*

Proof. Let $\mathbb{C}$ be any nonempty set of integers greater than or equal to $-n$. Adding n to all elements in $\mathbb{C}$, the set becomes $\mathbb{C} + n$. By WOP, $\mathbb{C} + n$ is well ordered. By definition, every nonempty set of $\mathbb{C} + n$ has the smallest element m. Then every nonempty set of $\mathbb{C}$ has the smallest element $m - n$. □

Definition 2.2 (**Lower bound, Upper bound**). A *lower bound* (respectively, *upper bound*) for a set S of real numbers is a number b such that $b \leq s$ (respectively, $b \geq s$) for every $s \in S$.

Well ordered sets' definition lead to two corollaries,

Corollary 2.0.1. *Any set of integers with a lower bound is well ordered.*

Proof. Let $\mathbb{B}$ be an arbitrary set of integers with a lower bound b. Then $\mathbb{B} - b$ has a lower bound 0. By WOP, $\mathbb{B} - b$ is well ordered. Therefore $\mathbb{B}$ is well ordered. □

Corollary 2.0.2. *Any nonempty set of integers with an upper bound has a maximal element.*

Proof. Let $\mathbb{B}$ be an arbitrary nonempty set of integers with an upper bound $\lceil b \rceil$. Then $-\mathbb{B}$ must have a lower bound $-\lceil b \rceil$. By the above Corollary 2.0.1, $-\mathbb{B}$ is well ordered and has a minimal element. Hence $\mathbb{B}$ has a maximal element. □

Finite sets are yet another routine example of well ordered sets.

Remark 2.3. Note that *finite* is the basis for WOP.

Lemma 2.1. *Every nonempty finite set of real numbers is well ordered.*

Proof. If a nonempty set of real numbers is finite, its number of subsets is also finite. Therefore it is sufficient to prove that every such finite set of real numbers has a minimal element.

We shall prove by contradiction using WOP on the *size* of finite sets.

Suppose we have a set $\mathbb{C}$ of n positive integers where finite sets of size n real numbers have no minimal element. For the sake of our argument, $\mathbb{C} \neq \emptyset$. By WOP, $\mathbb{C}$ has a minimal element n_0. We argue that $n_0 > 1$ since a set of real numbers with one single element has minimal element as the one element itself.

Now let $\mathbb{S}$ be a finite set of real numbers which satisfies $\mathbb{C}$. Then $\mathbb{S}$ must have at least n_0 elements. Let $r_1 \in \mathbb{S}$. By assumption, $\mathbb{S}$ has no minimal elements. Removing r_1 from $\mathbb{S}$ means that the set now has a minimal element r_0 since $n_0 - 1 \notin \mathbb{C}$. But then this means that $\min(r_0, r_1)$ is the minimal element of $\mathbb{S}$, contradicting that $\mathbb{S}$ has no minimal element. □

$$\mathbb{F} = \left\{0, \frac{1}{2}, \frac{2}{3}, \ldots, \frac{n}{n+1}, \ldots\right\}$$

We claim that $\mathbb{F}$ is well ordered whose minimal element is the smallest numerator.

Lemma 2.2. $\mathbb{N} + \mathbb{F}$ *is well ordered.*

Proof. Let $\mathbb{S}$ be any nonempty subset of $\mathbb{N} + \mathbb{F}$.

Let $\mathbb{S}_n = \{n \in \mathbb{N} \mid (n + f) \in \mathbb{S} \text{ for some } f \in \mathbb{F}\}$. By definition of $\mathbb{S}$, $\mathbb{S}_n$ is nonempty. By WOP, there exists a minimal $n_0 \in \mathbb{S}_n$.

Then by definition of $\mathbb{S}_n$, $\mathbb{S}_f = \{f \in \mathbb{F} \mid (n_0 + f) \in \mathbb{S}\}$ is nonempty. By WOP, there exists a minimal $f_0 \in \mathbb{S}_f$.

We argue that $n_0 + f_0$ is the smallest element in $\mathbb{S}$. For any arbitrary $(n + f) \in \mathbb{S}$, $n + f \geq n_0 + f \geq n_0 + f_0$ where $n_0 + f_0 \in \mathbb{S}$. Therefore, $\mathbb{N} + \mathbb{F}$ is well ordered. □

Remark 2.4. $\mathbb{N} + \mathbb{F}$ provides a hint of the rich collection of well ordered sets. For example, in $\mathbb{N} + \mathbb{F}$ every element greater than or equal to 1 can be the first element in a strictly decreasing sequence of arbitrary finite length. For example,

$$
\begin{aligned}
&1, 0. \\
&1, \frac{1}{2}, 0. \\
&1, \frac{2}{3}, \frac{1}{2}, 0. \\
&1, \frac{3}{4}, \frac{2}{3}, \frac{1}{2}, 0. \\
&\quad\vdots
\end{aligned}
$$

It is impossible to find an infinite decreasing sequence in $\mathbb{N} + \mathbb{F}$.

Part II

Problems and Exercises

Chapter 1

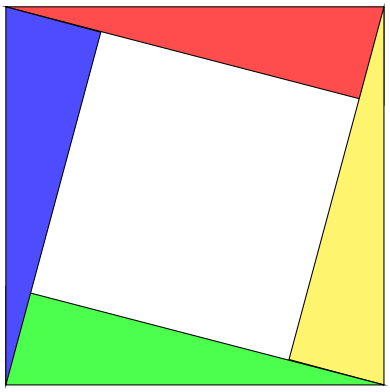
What is a Proof?

There are many problems in this chapter in which we will use this specific Lemma. So we state it here for convenience.

Lemma 1.1 (Unique prime factorization/Fundamental Theorem of Algebra)**.** *Every natural number can be expressed as a unique product of primes.*

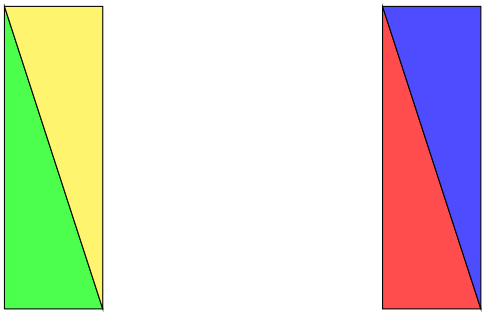
Problem 1.1.

(a) Colors of the triangles are arbitrary since I do not remember the exact ones in the text.



The middle square is a square of $(b-a) \times (b-a)$

(b) [*Possible Errata:* Arrange the same shapes so they form two rectangles, both $a \times b$.]



We prove by construct a chain of iffs.

$$\begin{aligned} & (b-a)^2 = c^2 - 2ab \\ \Leftrightarrow \quad & a^2 + b^2 - 2ab = c^2 - 2ab \\ \Leftrightarrow \quad & a^2 + b^2 = c^2 \end{aligned}$$

(c) The equation would still hold true since $a = b$ is not a requirement for the proof. In fact, note that if $a = b$, the area of the bigger square in **(a)** will now be exactly equal to the sum of area of all triangles inside it, which is equal to the sum of area of two smaller squares in **(b)**. That is, $c^2 = a^2 + b^2$.

(d) Some assumptions about right triangles, squares and lines are,

- 4 identical right triangles.
- For every 2 points, there is a line.

Problem 1.2.

(a) Mistake:

$$\sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1}$$

The right-hand side of this equation is undefined while the left-hand side is defined.

(b) Suppose $1 = -1$, then

$$\begin{aligned} & 0 = 0 \\ \Rightarrow \quad & 1^2 - 1^2 = 1 + 1 \\ \Rightarrow \quad & (1-1)(1+1) = 1 + 1 \end{aligned}$$

At this stage, we cancel off $1 + 1$ on each side since they are non-zero, the equation then becomes,

$$\begin{aligned} \Rightarrow \quad & 1 - 1 = 1 \\ \Rightarrow \quad & 1 + 1 = 1 \\ \Rightarrow \quad & 2 = 1 \end{aligned}$$

where the second equation is by the antecedent $1 = -1$. Hence, we have proved $2 = 1$.

(c) We shall prove the following lemma,

Lemma 1.2.1. *If $r, s > 0$, then $\sqrt{rs} = \sqrt{r}\sqrt{s}$*

Proof. Assume $r, s > 0$. For every positive integer x, there is one $\sqrt{x} > 0$ such that $x = (\sqrt{x})^2$; therefore,

$$(\sqrt{r})^2(\sqrt{s})^2 = rs \tag{1.1}$$

By commutative and associative property of multiplication,

$$(\sqrt{r})^2(\sqrt{s})^2 = (\sqrt{r}\sqrt{s})^2 \tag{1.2}$$

which leads to

$$(\sqrt{r}\sqrt{s})^2 = rs \tag{1.3}$$

Since $rs > 0$, there is also one $\sqrt{rs} > 0$ such that $(\sqrt{rs})^2 = rs$. Therefore,

$$(\sqrt{r}\sqrt{s})^2 = (\sqrt{rs})^2 \tag{1.4}$$

Since $\sqrt{r}\sqrt{s} > 0$ and $\sqrt{rs} > 0$, we conclude

$$\sqrt{r}\sqrt{s} = \sqrt{rs} \tag{1.5}$$

□

Problem 1.3.

(a) Mistake,

$$3 > 2$$
$$3\log_{10}(1/2) > 2\log_{10}(1/2)$$

since $\log_{10} n \; \forall 0 < n < 1$ is always negative.

(b) Wrong because all arithmetic operations must be done on numbers with the same currency, so that they will be in the same field.

(c) Since $a = b$, $a - b = 0$, and therefore we cannot cancel $a - b$ on both sides since we cannot divide each side by 0.

Problem 1.4. The questionable step is from step 2 to step 3, namely,

$$\begin{aligned} a+b &\overset{?}{\geq} 2\sqrt{ab} \\ a^2+2ab+b^2 &\overset{?}{\geq} 4ab \end{aligned}$$

Assume that $a, b < 0$. Then even though the first inequality is false, the second inequality is true, which will lead to all subsequent inequalities to be true. Therefore, we have just "proved" that arithmetic mean is at least as large as geometric mean for all negative numbers a, b!

To fix this,

$$\begin{aligned} \frac{a+b}{2} &\geq \sqrt{ab} \\ a+b-2\sqrt{ab} &\geq 0 \\ (\sqrt{a}-\sqrt{b})^2 &\geq 0 \end{aligned}$$

This ensures that $a, b \geq 0$ so that the last inequality can be defined.

Problem 1.5.
The reasoning is wrong because of the implicit assumption on Monday.

Assumption 1.5.1. *If Albert didn't give the quiz **before** Monday, by Midnight Sunday, we know the quiz has to be on Monday.*

The contrapositive of this statement is,

Assumption 1.5.2 (equivalent to 1.5.1)**.** *If the quiz is not on Monday, then Albert gave the quiz **before** Monday.*

This is a false assumption since we know Albert gives out his quiz on next week. This collapses the chain of arguments and therefore the reasoning is false.

Problem 1.6.
We prove by case analysis. Let $x = \log_7 n \; \forall n \in \mathbb{Z}^+$ so that $7^x = n$. We argue that there are two scenarios,

1. x is an integer
2. x is a non-integer

These cases are clearly exhaustive.

Case 1: x is an integer
We use a certain fact called the fundamental theorem of algebra,

Fact 1.6.1. *All positive integers are products of unique primes.*

Therefore, for all n that are a product of $7s$ (e.g, 7, 7^2, 7^3, ...), x is an integer.

Case 2: x is a non-integer

We prove by contradiction. Assume x is rational, then $x = \frac{p}{q}$ for all integers $p, q \in \mathbb{Z}^+$ that do not share common factor such that $7^{\frac{p}{q}} = n$. Then $n^q = 7^p$. By fact 1.6.1, $n = 7^k$ for some positive integer k, which means $7^{qk} = 7^p$. Then $\frac{p}{q} = k$, which contradicts the fact p and q do not share a common factor. We conclude that x is irrational.

Problem 1.7.

Case 1: $r \geq s$

$$max(r, s) + min(r, s) = r + s$$

Case 2: $r < s$

$$max(r, s) + min(r, s) = s + r = r + s$$

Problem 1.8.
We claim that,

Predicate 1.8.1. *An irrational number powered to an irrational number can be rational.*

We prove by case analysis. Let's consider $\sqrt{2}^{\sqrt{2}}$ to be one of the two cases,

1. $\sqrt{2}^{\sqrt{2}}$ is rational
2. $\sqrt{2}^{\sqrt{2}}$ is irrational

In case 1, we have the conclusion. In case 2, suppose $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, then

$$x^y = \sqrt{2}^{(\sqrt{2})^2} = (\sqrt{2})^2 = 2$$

Therefore, we conclude that an irrational number powered to an irrational number can be rational.

Problem 1.9.
We prove $|r + s| \leq |r| + |s|$ $\forall r, s \in \mathbb{R}$ by case analysis.

Case 1: $r > 0$, $s > 0$

$$(r + s) = r + s$$

Case 2: $r > 0$, $s < 0$

$$|r + s| \leq r - s$$

There are two subcases in this one,

Case 2.1: $r + s \geq 0$

$$r + s < r - s$$

Case 2.2: $r + s < 0$

$$-r - s < r - s$$

Case 3: $r < 0$, $s > 0$
Very similar to the case above, interchange the role of r, s.

Case 4: $r < 0$, $s < 0$
Then $-(r + s) = -r - s = (-r) + (-s)$.

Problem 1.10.

(a) We prove by case analysis. Without loss of generality, assume $z = a + b$ and $d = z + c$ where $a, b, c, d \in \mathbb{Z}^+$, then one of the following four cases happens,

Case 1: z is odd and c is odd

z is odd IFF one and only one of the summands is even and the other is odd. In this case, d is even if one of a, b, c is even.

Case 2: z is even and c is even

For z to be even, there are two sub-cases,

Case 2.1: Both a and b are evens

d is even if all of a, b, c are even.

Case 2.2: Both a and b are odds

d is even if one and only one of a, b, c is even.

Case 3: z is even and c is odd

d is odd in this case.

Case 4: z is odd and c is even

d is also odd in this case.

We conclude that d is even IFF either one and only one of a, b, c is even or all a, b, c are evens.

(b) We shall first prove a lemma,

Lemma 1.10.1. *If x is even, x^2 is a multiple of 4. If x is odd, x^2 is one more than a multiple of 4.*

Proof. If x is even, $x = 2k$ for some integer k, then $x^2 = 4k^2$. If x is odd, $x = 2m + 1$ for some integer m, then $x^2 = 4(m^2 + m) + 1$. □

Suppose,

$$w^2 + x^2 + y^2 = z^2$$

for all $w, x, y, z \in \mathbb{Z}^+$. We shall prove the statement,

Theorem 1.10.1. *z is even IFF all w, x, y are even.*

Proof. We shall prove by case analysis. Assume if w, x, y are even, then $w = 2i, x = 2j, y = 2k$ for some integer i, j, k; if w, x, y are odd, then $w = 2m + 1, x = 2n + 1, y = 2l + 1$ for some integer m, n, l. Then one of the following four cases happen,

Case 1: All w, x, y are odd

$$\begin{aligned} z^2 &= (2m+1)^2 + (2n+1)^2 + (2l+1)^2 \\ &= 4(m^2 + n^2 + l^2 + m + n + l) + 3 \end{aligned}$$

Case 2: One of w, x, y is even

$$\begin{aligned} z^2 &= (2i)^2 + (2n+1)^2 + (2l+1)^2 \\ &= 4(i^2 + n^2 + l^2 + n + l) + 2 \end{aligned}$$

Case 3: Two of w, x, y are even

$$\begin{aligned} z^2 &= (2i)^2 + (2j)^2 + (2l+1)^2 \\ &= 4(i^2 + j^2 + l^2 + l) + 1 \end{aligned}$$

Case 4: All of w, x, y are even

$$\begin{aligned} z^2 &= (2i)^2 + (2j)^2 + (2k)^2 \\ &= 4(i^2 + j^2 + k^2) \end{aligned}$$

Therefore, if either one and only one of w, x, y is even or all of w, x, y are even, then z^2 is even, which implies z is even. Conversely, if z is even, by the above lemma, z^2 does not exist in Case 2. We conclude that z is even IFF all of w, x, y are even. □

Problem 1.11.
We want to prove the theorem,

Theorem 1.11.1. *There exists an irrational number a such that $a^{\sqrt{3}}$ is rational.*

Proof. We prove by case analysis. The number $x = \sqrt[3]{2}^{\sqrt{3}}$ must be one of the two cases,

Case 1: x is rational.
In this case, $a = \sqrt[3]{2}$ and a is irrational.

Case 2: x is irrational.
Let $a = \sqrt[3]{2}^{\sqrt{3}}$. Then a is irrational such that,

$$\begin{aligned} a^{\sqrt{3}} &= (\sqrt[3]{2})^{(\sqrt{3})^2} \\ &= (\sqrt[3]{2})^3 \\ &= 2 \end{aligned}$$

We conclude that there exists an irrational a such that $a^{\sqrt{3}}$ is rational. □

Problem 1.12. The proof is by contradiction. Suppose a is odd, then $a = 2k+1$ for some integer k, then for all $n > 0$,

$$a^n = (2k+1)^n = \sum_{i=1}^{n} \mathrm{C}_i^n (2k)^i + 1 = 2\left(\sum_{i=1}^{n} \mathrm{C}_i^n 2^{i-1} k^i\right) + 1$$

Therefore, a^n is odd, a contradiction. We conclude that if a^n is even, a is even.

Problem 1.13. Assume by contradiction that both a and $b > \sqrt{n}$. Then, since $a, b \geq 0$,

$$a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$$

which contradicts the antecedent $a \cdot b = n$.

Problem 1.14.

(a) Suppose by contradiction $n = 2k + 1$ for some integer k, then $n^2 = 4(k^2 + k) + 1$ is odd. Therefore, n must be even.

(b) Suppose by contradiction either $n = 3l + 1$ or $n = 3l + 2$ for some integer l, then either $n^2 = 3(3l^2 + 2l) + 1$ or $n^2 = 3(3l^2 + 2l + 1) + 1$, contradicting the antecedent n^2 is a multiple of 3. Therefore, n must be a multiple of 3.

Problem 1.15. Let $n = 4$ and $m = 8$. Then $16 = 4^2$ is a multiple of 8, but 4 is not a multiple of 8. If $m < n$, $n = mk + l$ for some integer k and $l < m$, and we will prove that if n^2 is a multiple of m, then n is a multiple of m.

Proof. We will prove by contradiction. Suppose $n = mk + l$ for some positive integer k and $m < n$ and $l < m$, then $n^2 = m(mk^2 + 2kl) + l^2 < 2m(mk^2 + 2kl)$. Therefore, n^2 is not a multiple of m, a contradiction. □

Problem 1.16.
We can generalize the proof to only for some nonnegative integer n. For example, $\sqrt{4} = 2$ is rational. $\sqrt{3}$, however, is irrational. Using Problem 1.14 **(b)**, we can easily prove such statement.

Problem 1.17.
We shall prove by contradiction. Let $\log_4 6 = \dfrac{m}{n}$ for some integer m, n in its simpliest form such that $4^{\frac{m}{n}} = 6$. Then

$$2^{2\frac{m}{n}} = (2 \cdot 3)$$

Powering to n on both sides, we have,

$$2^{2m} = (2 \cdot 3)^n$$

Dividing both sides by 2^n, we have,

$$2^{2m-n} = 3^n$$

By unique factorization of primes, this cannot happen unless both $2m - n = 0$ and $n = 0$, but this implies that $m = n = 0$. Hence, this is a contradiction.

We conclude that $\log_4 6$ is irrational.

Problem 1.18.
We shall prove by contradiction. Note that,

$$(\sqrt{3} + \sqrt{2})(\sqrt{3} - \sqrt{2}) = 3 - 2 = 1$$

Therefore, $\sqrt{3} + \sqrt{2}$ is rational/irrational IFF $\sqrt{3} - \sqrt{2}$ is rational/irrational since $\sqrt{3} + \sqrt{2} = \dfrac{1}{\sqrt{3} - \sqrt{2}}$. Suppose $\sqrt{3} + \sqrt{2}$ is rational, then $\sqrt{3} - \sqrt{2}$ is also rational, but then,

$$(\sqrt{3} + \sqrt{2}) + (\sqrt{3} - \sqrt{2}) = 2\sqrt{3}$$

Since we know that $2\sqrt{3}$ is irrational, this is a contradiction. Therefore, $\sqrt{3} + \sqrt{2}$ is irrational.

Problem 1.19.
Let us first re-state the lemma,

Lemma 1.19.1. *Let the coefficients of the polynomial*

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{m-1} x^{m-1} + x^m$$

be integers. Then any real root of the polynomial is either integer or irrational.

(a) Let $\sqrt[m]{k} = x_0$, where x_0 is a real root of the polynomial. Suppose $\sqrt[m]{k}$ is rational, then by the lemma, x_0 must be an integer, which implies that $k = x_0^m$. Therefore, $\sqrt[m]{k}$ is irrational whenever $k \neq x_0^m$ for some integer x_0.

(b) We shall first prove a lemma,

Lemma 1.19.2. *If a prime p is a factor of some power of an integer, then it is also a factor of that integer.*

Proof. We prove by contradiction. Suppose p is not a factor of some integer, by unique prime factorization, it cannot be a factor of some power of that integer as well. We conclude that the lemma must hold. □

We shall prove the first lemma in this problem by direct proof. Suppose the real root of the polynomial is x_0. Then x_0 is either rational or irrational. Let $x_0 = \frac{r}{s}$ for some integer r, s in the lowest term possible. Hence,

$$\begin{aligned} a_0 + a_1\left(\frac{r}{s}\right) + a_2\left(\frac{r}{s}\right)^2 + \ldots + a_{m-1}\left(\frac{r}{s}\right)^{m-1} + \left(\frac{r}{s}\right)^m &= 0 \\ a_0 s^m + a_1 r s^{m-1} + a_2 r^2 s^{m-2} + \ldots + a_{m-1} r^{m-1} s &= -r^m \\ s(a_0 s^{m-1} + a_1 r s^{m-2} + a_2 r^2 s^{m-3} + \ldots + a_{m-1} r^{m-1}) &= -r^m \end{aligned}$$

By unique prime factorization, $s = pk$ where p is a prime and k is some integer. This implies r^m is divisible by p. By the lemma proved above, this means r is also divisible by p. But this contradicts that r and s are in its simpliest form. Therefore, it must be the case that $s = \pm 1$ or x_0 is irrational. We conclude that any real root of the polynomial is either integer or irrational.

Problem 1.20.
Let $x = \log_9 12$. We shall prove that x is irrational by contradiction. Assume that $x = \frac{p}{q}$ in the lowest term possible for some integer p, q. Then,

$$3^{\left(2\frac{p}{q}\right)} = (2^2 \cdot 3)$$

Powering both sides to q, we have,

$$3^{2p} = (2^{2q} \cdot 3^q)$$

Dividing both sides by 3^q, yielding,

$$3^{2p-q} = 2^q$$

By unique prime factorization lemma, the last equation is impossible unless both powers on both sides equal to 0, but this implies that $p = q = 0$. Therefore, x must be irrational.

Problem 1.21.
Let $x = \log_{12} 18$. We shall prove that x is irrational by contradiction. Assume that $x = \dfrac{p}{q}$ in the lowest term possible for some integer p, q. Then,

$$(2^2 \cdot 3)^{\frac{p}{q}} = (3^2 \cdot 2)$$

Powering both sides to q,

$$(2^2 \cdot 3)^p = (2 \cdot 3^2)^q$$

Equivalently,

$$2^{2p} \cdot 3^p = 2^q \cdot 3^{2q}$$

Finally, dividing both sides by $2^q 3^p$ yields,

$$2^{2p-q} = 3^{2q-p}$$

By unique prime factorization lemma, this is impossible unless $p = q = 0$, but this contradicts x is rational. We conclude that x is irrational.

Problem 1.22.
The unsatisfiable equation is $a^3 = 7^2 b^3$. Assume $\sqrt[3]{7^2} = \dfrac{a}{b}$ for some integer a, b in the lowest term possible. By lemma 1.19.2, since 7 is a factor of a^3, 7 is also a factor of a, but this means that 7 is also a factor b^3 and, by implication, b. This contradicts that a and b are in the lowest term possible. Hence, the equation is not satisfied.

Problem 1.23.
From the problems above, it is easy to show that $2 \log_2 3$ is irrational.

Problem 1.24.

(a) The proof relies first on the fact that $1 < \sqrt{2} < 2$. This is because $\sqrt{2} > 0$, $1 > 0$, $(\sqrt{2})^2 - 1^2 = 2 - 1 > 0$ and $(\sqrt{2})^2 - 2^2 = 2 - 4 < 0$. From here, $0 < \sqrt{2} - 1 < 1$, and $0 < (\sqrt{2} - 1)q < q \ \forall q \in \mathbb{N}$. Pick the smallest positive integer q such that $\sqrt{2}q \in \mathbb{N}$. Hence, $(\sqrt{2} - 1)q$ must be a nonnegative integer. We find a positive integer q' such that $0 < q' < q$ and we can still find a nonnegative integer, contradicting the original assumption of q being the smallest positive integer possible. We see that this is the case with $q' ::= (\sqrt{2} - 1)q$.

(b) I prefer this proof because,

- There are less computations.
- Relying only on basic assumptions about numbers.
- More abstractions lead to general results and proof methods.

- Optimization method.

Problem 1.25.

(a) Let $Q(n)$ be the polynomial without the constant term $c \in \mathbb{N}$. By definition, $q(n) = Q(n) + q(0)$ and $Q(n) = nQ'(n)$. Then for all $m \in \mathbb{Z}$,

$$\begin{aligned} q(cm) &= Q(cm) + q(0) \\ &= cQ'(m) + c \\ &= c[Q'(m) + 1] \end{aligned}$$

Therefore, $q(cm)$ is a multiple of c.

(b) Assume $c > 1$. Since $n = cm$, as $n \to \infty$, $m \to \infty$ and there will be an infinite many $q(n) \in \mathbb{Z}$ that are not primes since they all are multiples of c.

(c) It is sufficient to consider the case $0 \leq c \leq 1$. Then observe that $q(0) = c$, which is not a prime.

We conclude that for every nonconstant polynomial q there must be an $n \in \mathbb{N}$ such that $q(n)$ is not prime.

Chapter 2

The Well Ordering Principle (WOP)

Problem 2.1. We shall prove the following statement,

Lemma 2.1.1. *Every amount of postage that can be assembled using only* 10 *cent and* 15 *cent stamps is divisible by* 5*.*

Proof. Let the notation "$j \mid k$" indicate the integer j is a divisor of integer k, and let $S(n)$ mean that exactly n cents postage can be assembled using only 10 and 15 cent stamps. Then the proof shows that

$$S(n) \quad \text{IMPLIES} \quad 5 \mid n, \qquad \text{for all nonnegative integers n.} \tag{2.1}$$

Let C be the set of *counterexamples* to (2.1), namely

$$C ::= \{n \mid S(n) \text{ DOES NOT IMPLY } 5 \mid n \text{ for some } n \in S(n)\}$$

Assume for the purpose of obtaining a contradiction that $C \neq \emptyset$. By WOP, there exists a smallest $m \in C$. This m must be positive because $5 \mid 0$.

But if $S(m)$ holds and m is positive, then $S(m-10)$ or $S(m-15)$ must hold, because for all positive $m = 10i + 15j$ for either $i > 0$ or $j > 0$; if $i > 0$, $(m-10) \in S(m-10)$; if $j > 0$, $(m-15) \in S(m-15)$.

So suppose $S(m-10)$ holds. Then $5 \mid m-10$, because $(m-10) \notin C$.

But this means that $5 \mid m$, contradicting the fact that m is a counterexample.

Next, if $S(m-15)$ holds, we arrive at a contradiction the same way.

Since we get a contradiction in both cases, we conclude that $C = \emptyset$, which proves that (2.1) holds. □

Bibliography

[1] Eric Lehman, Tom Leighton, and Albert Meyer. *Mathematics for Computer Science*. MIT OCW, 2018.