Number Theory

Sudip Sinha

2019-07-27

Math Circle @ QTM

Outline

Section 1
Introduction and Logic

Introduction and motivation

1. What is number theory?

2. Why do we study number theory?

3. Why do we want to *prove* ideas?

4. More importantly, what constitutes a *proof*?

5. Inductive vs deductive reasoning.

Inductive reasoning

- **Inductive reasoning** derives general propositions from specific examples.
- **Caution**: *We can never be sure, our conclusion(s) can be wrong!* ☹
- *Example* 1:

1. We throw lots of things, very often.
2. In all our experiments, the things fell down and not up.
3. So we conclude that likely, things always fall down.

How we may be wrong:

1. An iron nail under a big magnet moves up (given that it is sufficiently close).
2. A helium balloon goes up.

Inductive reasoning: problems

- *Example* 2: You ask your parent for a candy and (s)he buys it for you. You ask for a fancy shoe, and (s)he buys it. Now you ask for a Lamborghini $\cdots$.

- *Example* 3 (*Black swan*): In the 16th century, it was believed (in Europe) that swans are always white. But in 1697, Dutch explorers led by Willem de Vlamingh became the first Europeans to see black swans, in Western Australia.

- *Example* 4: $\frac{1}{1} = 1, \frac{2}{2} = 1, \frac{3}{3} = 1, \cdots$; so clearly $\frac{n}{n} = 1$ for every integer n.

- *Example* 5: Illusions, e.g. drawings by *M. C. Escher*.

Problems with inductive reasoning: Illusion #1

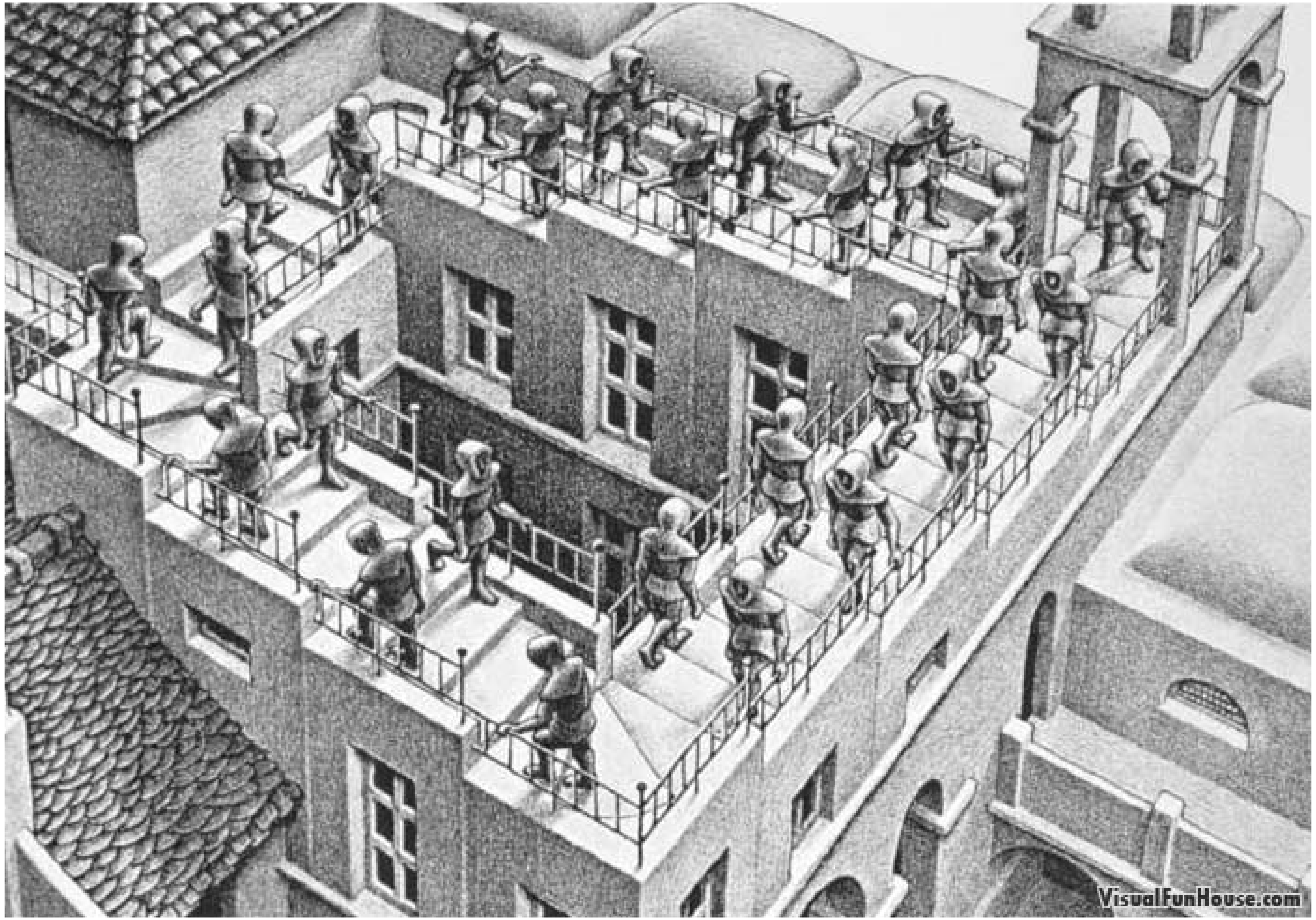

Figure 1 Ascending and Descending, M. C. Escher

Problems with inductive reasoning: Illusion #2

Figure 2   Waterfall, M. C. Escher

Deductive reasoning

- **Deductive reasoning** is deriving a logically certain conclusion from one or more premises.
- We do *NOT* question the premises. But *if the premises are correct, then all conclusions are correct.* ☺
- *Example*: Question: Do $\mathbf{Q_1}$ and $\mathbf{Q_2}$ *imply* $\mathbf{Q_3}$?
  - ($\mathbf{Q_1}$) All men are mortal. (First premise)
  - ($\mathbf{Q_2}$) Socrates is a man. (Second premise)
  - ($\mathbf{Q_3}$) Therefore, Socrates is mortal. (Conclusion)
- *Example*: Question: Does $\mathbf{P_1}$ and $\mathbf{P_2}$ *imply* $\mathbf{P_3}$?
  - ($\mathbf{P_1}$) Borogoves are mimsy whenever it is brillig.
  - ($\mathbf{P_2}$) It is now brillig, and this thing is a borogove.
  - ($\mathbf{P_3}$) Hence this thing is mimsy.
- We do not *need* an inherent *meaning* of the terms.

Inductive vs deductive reasoning

Criteria	Inductive reasoning	Deductive reasoning
Basis	evidence	logic
Questions	everything (arguments and premises)	only the arguments, not premises
Direction	*bottom-up*	*top-down*
Natural to humans?	yes	no
Requires *meaning*s of terms?	yes	no
Applicability	good in practice	good for theory
Examples	science, statistics and machine learning	logic, mathematics

Logic

- *Logic* is a *language* to formalize deductive reasoning.
- Logic comprises of the following elements.
  - propositions
  - connectives (not, and, or, implies, iff)
  - quantifications (for all, there exists)
  - values (true, false)
  - a way to assign propositions to a value
- **Important**: The propositions in the following section are not necessarily true. Please be mindful.

Logic: elementary *propositions*

- Elementary *propositions*, represented by P, Q, etc, are statements saying something.
- Examples:
  - $P_1 \equiv n$ is an integer
  - $P_2 \equiv n$ is *not* an integer
  - $P_3 \equiv 2n$ is even
  - $P_4 \equiv n = \frac{1}{2}$
  - $Q_1 \equiv$ Socrates is a man
  - $Q_2 \equiv$ Socrates is smart

Logic: compound *propositions*

- Compound *propositions* are elementary propositions connected by connectives.
- *Connectives*:
  - not ($\neg$, or $\sim$): $\neg P$ is called the negation of P.
  - and ($\wedge$)
  - or ($\vee$)
  - implies ($\rightarrow$, or $\Longrightarrow$)
  - iff ($\leftrightarrow$, or $\Longleftrightarrow$, or $\equiv$)
- Examples:

1. $(\neg P_1) \equiv$ not (n is an integer) $\equiv$ (n is *not* an integer)
2. $(P_1 \vee P_2) \equiv$ (n is an integer) or (n is *not* an integer)
3. $(Q_1 \wedge Q_2) \equiv$ (Socrates is a man) and (Socrates is smart)
4. $((\neg P_1) \leftrightarrow P_2) \equiv$ not (n is an integer) if and only if (n is *not* an integer)
5. $(P_1 \rightarrow P_3) \equiv$ (n is an integer) implies ($2n$ is even)
6. $(P_4 \rightarrow P_3) \equiv$ ($n = \frac{1}{2}$) implies ($2n$ is even)

Truth tables

- Question: How do we find the value of a compound propositions?
- Exercise: Fill up the table. Think carefully about what the '?'s should be.

P	Q	$(\neg P)$	$(P \wedge Q)$	$(P \vee Q)$	$(P \rightarrow Q)$	$(P \leftrightarrow Q)$
T	T					
T	F					
F	T				?	
F	F				?	

Truth tables

P	Q	$(\neg P)$	$(\neg Q)$	$(P \wedge Q)$	$(P \vee Q)$	$(P \rightarrow Q)$	$((\neg Q) \rightarrow (\neg P))$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	F	F
F	T	T	F	F	T	T	T
F	F	T	T	F	F	T	T

P	Q	$(P \rightarrow Q)$	$(Q \rightarrow P)$	$((P \rightarrow Q) \wedge (Q \rightarrow P))$	$(P \leftrightarrow Q)$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

- Truth tables evaluate the values of the expression for each values of the elementary propositions.
- Two propositions are equivalent if their truth table outputs are the same.

Thinking *logic*ally about mathematical statements

- Every mathematical statement can be broken down into their constituent propositions.
- Example

1. Original statement: if the product of two integers is even, then each of them is even.
2. Analysis: if the product of two integers n and m is even, then m is even and n is even.
3. Writing this down logically.
   - $P_1 \equiv$ the product of two integers n and m is even
   - $P_2 \equiv m$ is even
   - $P_3 \equiv n$ is even
   - Statement $\equiv (P_1 \rightarrow (P_2 \land P_3))$
4. Question: is the above statement true or false? How can you prove it?
5. Note: The part before the implication is called the antecedent, and the part after is called the consequent. In this example, P_1 is the antecedent and $(P_2 \land P_3)$ is the consequent.

Quantifiers

There are two quantifiers.

- ▷ Universal quantifier a.k.a. for every ($\forall$).
  Example 1: Every man has a head.
  Example 2: Every natural number is even.

- ▷ Existential quantifier a.k.a. there exists ($\exists$).
  Example 1: There is a man who can survive without breathing for an hour.
  Example 2: There exists a natural number which is the sum of its factors (except itself).

Exercise: Analyze the following statements logically.

1. Every odd number has a odd factor.

2. (Fermat's last theorem) No three positive integers a, b, and c satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2.

Tautologies

Let P, Q, and R be propositions. Verify the following using truth tables.

- (idempotence) $(P \leftrightarrow (P \wedge P))$, and $(P \leftrightarrow (P \vee P))$.
- (commutativity) $((P \wedge Q) \leftrightarrow (Q \wedge P))$, and $((P \vee Q) \leftrightarrow (Q \vee P))$.
- (associativity) $(((P \wedge Q) \wedge R) \leftrightarrow (P \wedge (Q \wedge R)))$, and $(((P \vee Q) \vee R) \leftrightarrow (P \vee (Q \vee R)))$.
- (distributivity) $((P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R)))$, and $((P \wedge (Q \vee R)) \leftrightarrow ((P \wedge Q) \vee (P \wedge R)))$.
- (identity) $((P \wedge T) \leftrightarrow P)$, $((P \vee F) \leftrightarrow P)$; $((P \wedge F) \leftrightarrow F)$, $((P \vee T) \leftrightarrow T)$.
- (involution) $((\neg(\neg P)) \leftrightarrow P)$.
- (implication) $((P \rightarrow Q) \leftrightarrow ((\neg P) \vee Q))$.
- (de Morgan's laws) $((\neg(P \wedge Q)) \leftrightarrow ((\neg P) \vee (\neg Q)))$, and $((\neg(P \vee Q)) \leftrightarrow ((\neg P) \wedge (\neg Q)))$.
- (contrapositive) $((P \rightarrow Q) \leftrightarrow ((\neg Q) \rightarrow (\neg P)))$.

The *converse* of $(P \rightarrow Q)$ is $(Q \rightarrow P)$, and they have no relation to each other.
Exercise: Find an example for which the proposition is true but its converse is not.

Proof methods

- Direct proof of $P \to Q$: Start with P and logically arrive at Q.
- Proof by contrapositive of $P \to Q$: Direct proof of $((\neg Q) \to (\neg P))$.
- Proof by contradition of a general proposition P: Consider that P is false. Logically show that this leads to an absurdity.
- Proof by induction (more on this later).
- Proof by construction.
- Proof by exhaustion.
- Probabilistic proof.
- Combinatorial proof.
- Nonconstructive proof.

Guidelines for proofs

Note: Proving a proposition is an art. There is no algorithms, only rules of thumb.

- To prove an existential proposition true, we need to find just one instance (*example*) for which the proposition is true.
- To prove an universal proposition false, we need to find just one instance (*counterexample*) for which the statement is false.
- It is sometimes easier to prove the contrapositive of a proposition.
- To prove a uniqueness proposition, proofs by contradiction is usually more convenient.
- Sometimes it is pragmatic to break down a proof into two or more cases.

Product of odd numbers

Before we use a term in mathematics, we try to define it as clearly as possible.

Definition (Even and odd numbers)

An integer n is called even if there exists an integer k such that $n = 2k$.

An integer n is called odd if there exists an integer k such that $n = 2k + 1$.

1. What can we say about the product of two odd numbers?
   Prove your claim.

2. If the product of two numbers is odd, can we say anything about the numbers?
   Prove your claim.

Section 2
Number systems

Natural numbers and integers

1. From ancient times, humans have been able to identify the natural numbers.
   In modern mathematics, the *set* of natural numbers is represented by $\mathbb{N} = \{1, 2, 3, \cdots\}$.

2. We can add/subtract, and multiply/divide any two natural numbers.

3. Are these all the numbers there can be?

4. Question: Are the natural numbers closed under addition/subtraction?
   (Being closed with respect to an operation means that the result is also in the given set.)

   a. I had 4 objects, and I gave 4 objects to Luci. How many objects do I now have?
   b. I owed Luci 20 \$, but I have 4 \$ with me. How much do I have?

5. This gives rise to the integers, $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$, which are closed under addition/subtraction.

6. From now on, we shall forget about subtraction, because subtracting an integer is essentially adding the negative of that integer.

Rational numbers

1. Note that the set of natural numbers is contained within the set of integers.
   In set theory, we say "$\mathbb{N}$ is a subset of $\mathbb{Z}$", and denote this by $\mathbb{N} \subset \mathbb{Z}$.

2. Are the integers closed with respect to multiplication/division?

3. This gives rise to the set of rational numbers, $\mathbb{Q} = \left\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\right\}$.

4. And now we can forget about division since it is simply multiplication with the inverse of the number.

5. Is that all we have?

6. Let's go on a journey.

Time Travel adventures: Part 1

Date: around 550 BC
Place: Pythagoras's office in Samos, Greece
Stage: Pythagoras has recently claimed that he has proved a major equality about the sides of right-angled triangles. We go there to investigate his claims.

Unfortunately, a lot of people have been trying do the same, so he has a filtering mechanism in place. We need to answer the following question to get in:

1. What is the area of a rectangle of dimensions $a \times b$?

2. What is the area of a right angled triangle of base b and height h?
   But of course, now he wants a proof of that fact.
   (Remember that Pythagoras is a geometer, so he is very happy with a geometric proof.)

3. What is the sum of angles of a triangle?

Once we answer these question, we get to see Pythagoras's proof.

Time Travel adventures: Part 1

Unfortunately, he believes that those who want to understand his work must themselves discover it. All he gives us is the following picture.
On the other side is scribbled $a^2 + b^2 = c^2$.

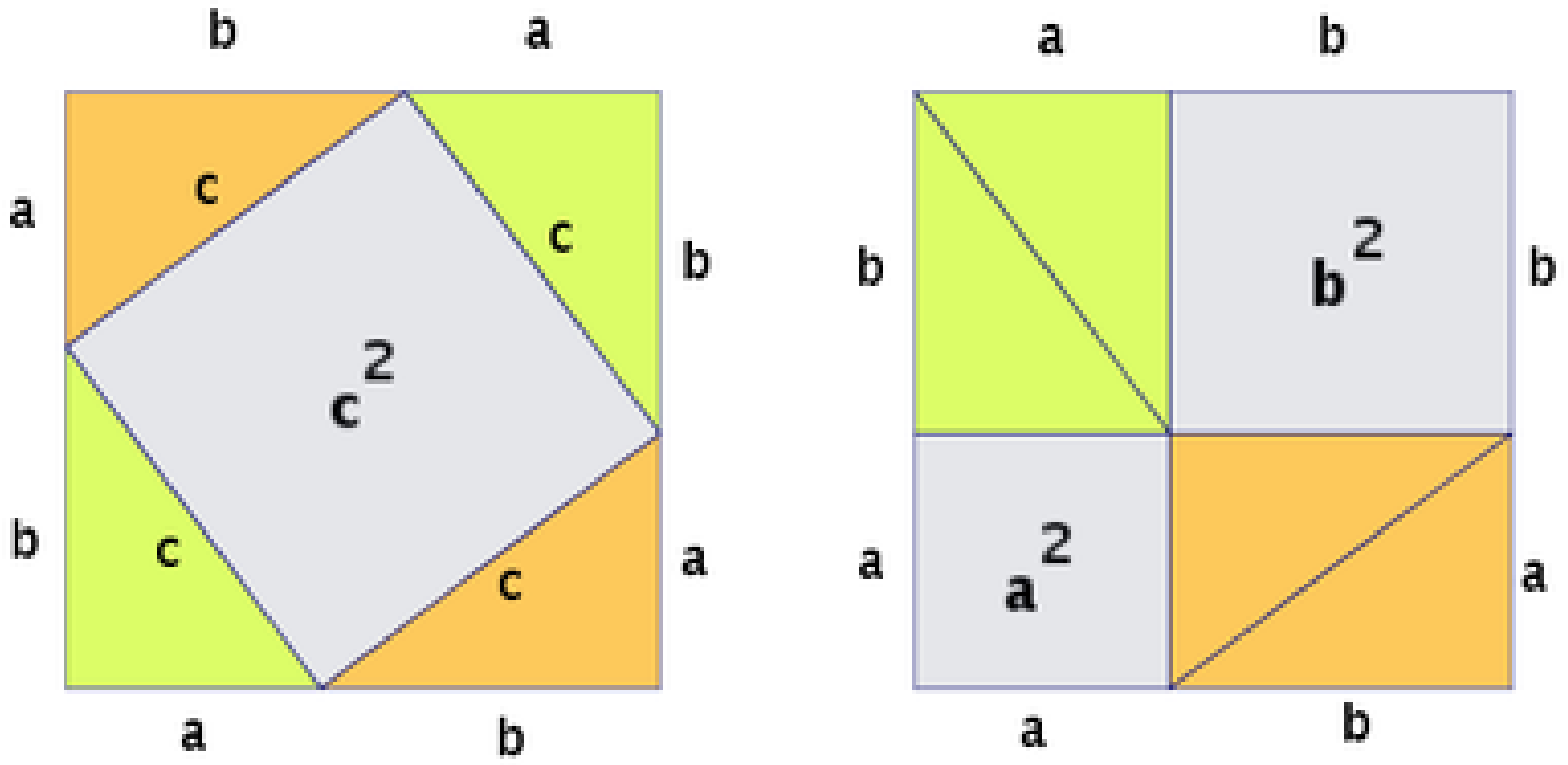

Figure 3 Pythagoras's art

Length of hypotenuse of a right-angled triangle

1. Using the Pythagoras formula, Find the length of the hypotenuse of a right-angled triangle of base and height equaling 1.

2. Is the above length rational?
   How can you be sure?

We start with a lemma

Lemma *Let n be an integer. The n^2 is even iff n is even.*

Proof Note that this is a $\iff$ statement. So we can break it into two parts.

Before we look at the individual directions, let us note that when p is an integer, so are p^2, $2p$, $2p^2$, and $2p^2 + 2p$.

($\Longleftarrow$) We use a direct proof for this direction.

Since n is even, there is an integer p such that $n = 2p$. Now, $n^2 = (2p)^2 = 4p^2 = 2(2p^2)$, so n^2 is even.

($\Longrightarrow$) We prove this by proving the contrapositive.

Suppose n is *not* even, that is, n is odd. Then we can write $n = 2p + 1$ for some integer p. Then $n^2 = (2p + 1)^2 = 4p^2 + 4p + 1 = 2(2p^2 + 2p) + 1$, so n^2 is also odd.

$\square$

Remark: A *lemma* is a proposition that leads to a bigger result, which are usually called *theorems*. *Corollaries* are applications or minor modifications of theorems that are themselves quite important. From a *logic*al viewpoint, there is no difference between lemmas, propositions, theorems, or corollaries.

Rationality of $\sqrt{2}$

Theorem *$\sqrt{2}$ is not rational.*

Proof We prove this by contradiction.

Suppose $\sqrt{2}$ is rational. Then it can be written in the form $\frac{p}{q}$, where p, q are integers with $q \neq 0$. Assume that p and q have no common factors, for if they do, we can reduce the fraction to its lowest terms and then call the numerator p and the denominator q.
Squaring and simplifying, we get

$$p^2 = 2q^2. \tag{1}$$

This means p^2 is even. By the previous lemma, p is also even. Therefore, there exists an integer r such that $p = 2r$, and so $p^2 = 4r^2$.
Putting this in equation (1), we get $4r^2 = 2q^2$, which is the same as $2r^2 = q^2$. This means that q^2, and thus q, is even.
But we had assumed that p and q have no common factors. Thus we have a contradiction.
Therefore, our supposition must be wrong, and it must be that $\sqrt{2}$ is not rational. $\square$

Real numbers

1. We showed that if we desire closure with respect to solutions of algebraic equations, we end up with numbers which may not be rational.

2. *Algebraic* numbers are numbers that are solutions of algebraic equations. For example, $\sqrt{2}$ is the solution of the algebraic equation $x^2 = 2$, and is thus algebraic.

3. It can be shown that there are numbers that are not solutions of any algebraic equation. Such numbers are called *transcendental* numbers. Example: π.

4. All rational numbers are algebraic. But the converse is not true, e.g. $\sqrt{2}$.

5. The set of all algebraic and transcendental numbers is called the set of *real* numbers.

6. The set of real numbers that are not rational is called the set of *irrational* numbers.

7. Closure with respect to square roots of negative number gives us an even bigger set, called the *complex* numbers.

Exercises

1. Prove that there exist positive integers n and m such that $n^2 + m^2 = 100$.

2. Assume that we have a rectangular box of dimensions $l \times b \times h$.

   a. What is the length of the diagonal?
   b. By what factor must each side be scaled so that the length of the diagonal is doubled?

3. Use the following formula for the sum of an infinite geometric series:

$$a + ar + ar^2 + \cdots = \frac{a}{1 - r} \quad , \qquad if |r| < 1$$

   a. Represent the repeating decimal $0.2222\cdots$ as a ratio of two integers.
   b. Represent the repeating decimal $42.2888\cdots$ as a ratio of two integers.
   c. Prove that $0.9999\cdots = 1$.

Section 3
Mathematical Induction

Motivation

Try to find expression for the following for an arbitrary natural number n.

1. $1 + 2 + 3 + \cdots + n$

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

I claim that $2^n > n$ for every natural number n. Is it true? How can we prove it?

Proving a fact for all natural numbers

1. Mathematical induction is a proof method of deductive reasoning.
   Do not confuse it with inductive reasoning.

2. Principle of mathematical induction. Suppose $P(n)$ is a statement about the natural number n. Assume that we can establish both of the following

   1. (base case) prove $P(1)$ is true, and
   2. (inductive step) for an arbitrary natural number k, if $P(k)$ is true, then $P(k+1)$ is also true.

   Then $P(n)$ is true for all natural numbers n.

Proof of $2^n > n$ using mathematical induction

Proposition $2^n > n$ *for every natural number* n*.*

Proof This is a proof by mathematical induction.

Let $P(n) \equiv 2^n > n$.

Base case $P(1) \equiv 2^1 > 1$ is true.

Inductive step Suppose $P(k)$ is true for some $k \in \mathbb{N}$. That is, suppose $2^k > k$.

We have to prove that $P(k+1)$ is true (using the supposition).

From our supposition, multiplying both sides by 2, we get $2^{k+1} > 2k$.

All we need to do now is to show that $2k \geq k + 1$.

Since $k \geq 1$, $k + k \geq ppk + 1$. Therefore $2^{k+1} > k + 1$.

We have shown that $P(k+1)$ is true. The concludes the inductive step.

By the principle of mathematical induction, $2^n > n$ is true for every postive integer n.

$\square$

Exercises

1. Try to prove the motivating examples by mathematical induction.

2. (telescoping series) Simplify each of the following sums to express it as a simple fraction:

   a. $\frac{1}{1\cdot 2}$
   b. $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3}$
   c. $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4}$
   d. $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)}$

   Prove your result.

3. Prove that the sum of the geometric series is given by the formula

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

Section 4
Divisibility

Divisibility

Definition *Let $a, d \in \mathbb{Z}$. We say that d divides a if there exists $q \in \mathbb{Z}$ such that $a = qd$.*
We write this as $d \mid a$. If d does not divide a, we write $d \nmid a$.
All integers that divide $a \in \mathbb{Z}$ are called factors of a.

Exercises

1. Which of the following is/are true? Give reasons.
   a. $13 \mid 52$
   b. $27 \mid 9$
   c. $-3 \mid 9$

2. Let a be an integer. Is the following true? Prove your claim.
   a. $a \mid a$
   b. $1 \mid a$
   c. $a \mid 0$

3. (Properties of $\mid$) Let $a, b, c, d, m, n, \in \mathbb{Z}$. Check if the following are true. Prove your claim.
   a. If $a \mid b$ and $a \mid (b + c)$, then $a \mid c$.
   b. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
   c. If $a \mid bc$, then $a \mid b$ or $a \mid c$.
   d. If $a \mid b^2$, then $a \mid b$.
   e. (Transitivity) If $a \mid b$ and $b \mid c$, then $a \mid c$.
   f. (Linear combination) If $d \mid a$ and $d \mid b$, then $d \mid (ma + nb)$.

Primes

Definition *Let $p \in \mathbb{N}, p > 1$. Then p is called prime if its only positive factors are 1 and p. A natural number $n > 1$ is called composite if it is* not *prime.*

Theorem (prime factorization) *Let $n > 1$ be a natural number. Then n can be written as a product of one or more prime numbers.*

Exercises

1. *Consecutive* integers are integers that differ by 1, such as 17 and 18.

   a. Find a pair of consecutive integers that are both prime. How many such pairs are there?
   b. Find a pair of consecutive integers that are both composite. How many such pairs are there?

2. Prove that for all $n \in \mathbb{N}$, $n^3 + 1$ is *not* prime.

3. Prove that every integer greater than 11 can be written as the sum of two composite numbers.

4. Given $f(n) = n^2 + n + 41$. Show that $f(40)$ and $f(41)$ are both composite.

Counting primes

Theorem (**Euclid, ~ 300** BC) *There are infinitely many primes.*

Proof Suppose that $\mathbb{P} = \{p_1, p_2, \cdots, p_n\}$ is a set of primes for some $n \in \mathbb{N}$.
Let $m = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n$ and $q = m + 1$. Now, q is either a prime or it is not.
If it is a prime, we have one more prime than our original set.
If it is not a prime, it must be divisible by some prime p. If $p \in \mathbb{P}$, then it would divide both m and $m+1$. Therefore it would divide the difference, that is, $p \mid 1$, which is impossible. Therefore $p \notin \mathbb{P}$.
Therefore a new prime can always be found to any given (finite) set of primes. $\square$

Remark *It is a common misconception that q is prime. For example, let $p_1 = 3$ and $p_2 = 5$. Then $p_1 \cdot p_2 + 1 = 16$, which is composite.*
Even if one considers n smallest primes, it is not true. For example, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$.

Remark *This is not a proof by contradiction. For more details, see (Hardy & Woodgold, 2009).*

Appendix

Thank you!

Bibliography

Hardy, M. & Woodgold, C. (2009). Prime Simplicity. *The Mathematical Intelligencer*, *31*(4), 44. doi:10.1007/s00283-009-9064-8