Number Theory 1

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 ....
- *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: $\frac{1}{1} = 1, \frac{2}{2} = 1, \frac{3}{3} = 1, \ldots$; 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

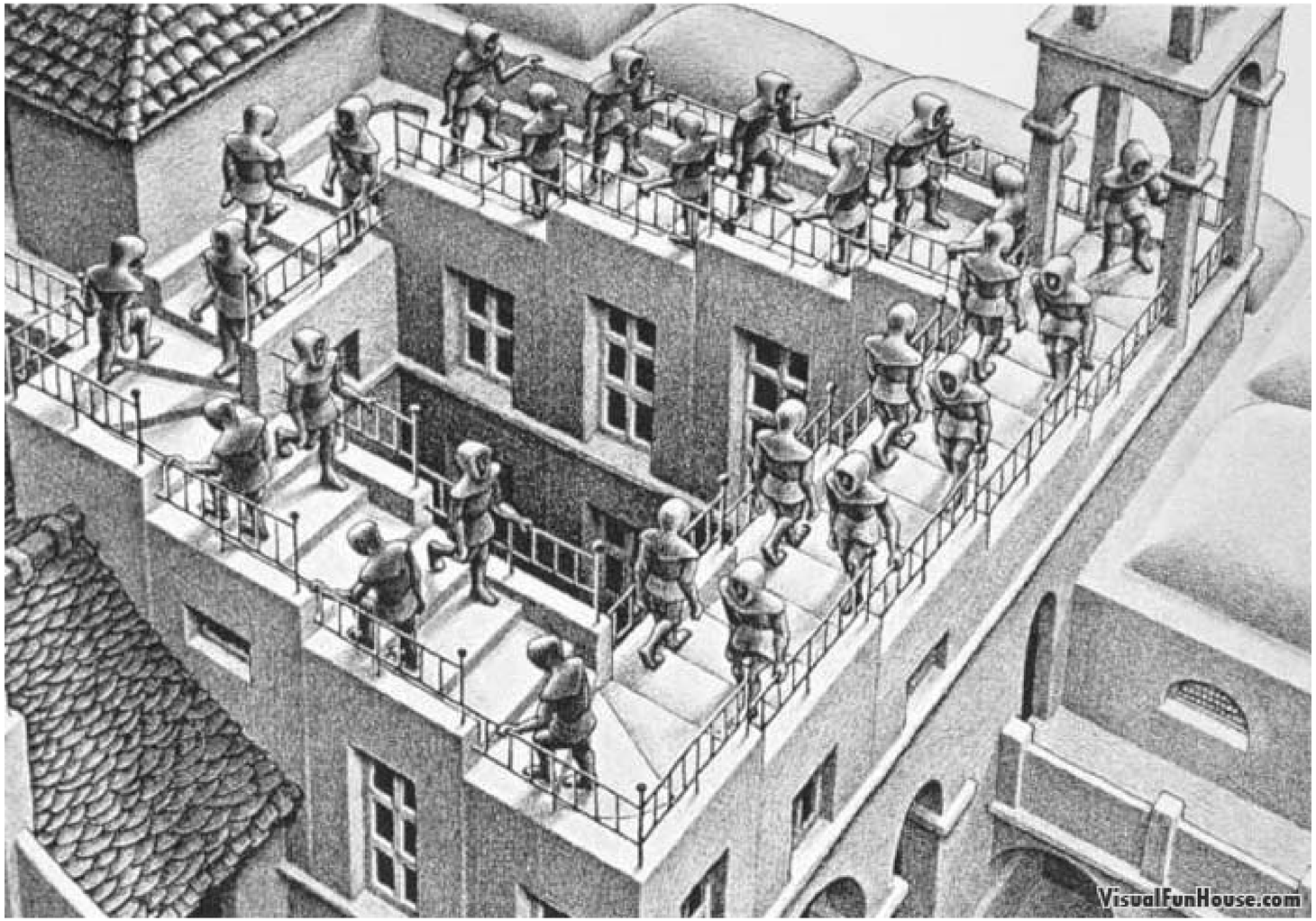

Figure 1 Ascending and Descending, M. C. Escher

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	$(\neg P)$	$(\neg Q)$	$(P \wedge Q)$	$(P \vee Q)$	$(P \to Q)$	$((\neg Q) \to (\neg P))$
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	$(P \to Q)$	$(Q \to P)$	$((P \to Q) \wedge (Q \to P))$	$(P \leftrightarrow Q)$
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 $\equiv (P_1 \rightarrow (P_2 \wedge P_3))$
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 $(P_2 \wedge P_3)$ 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) $((P \to Q) \leftrightarrow ((\neg P) \vee Q))$.
- ▷ (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) $((P \to Q) \leftrightarrow ((\neg Q) \to (\neg P)))$.

The *converse* of $(P \to Q)$ is $(Q \to P)$, 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 $\mathbb{N} = \{1, 2, 3, \ldots\}$.

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, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, 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 $a^2 + b^2 = c^2$.

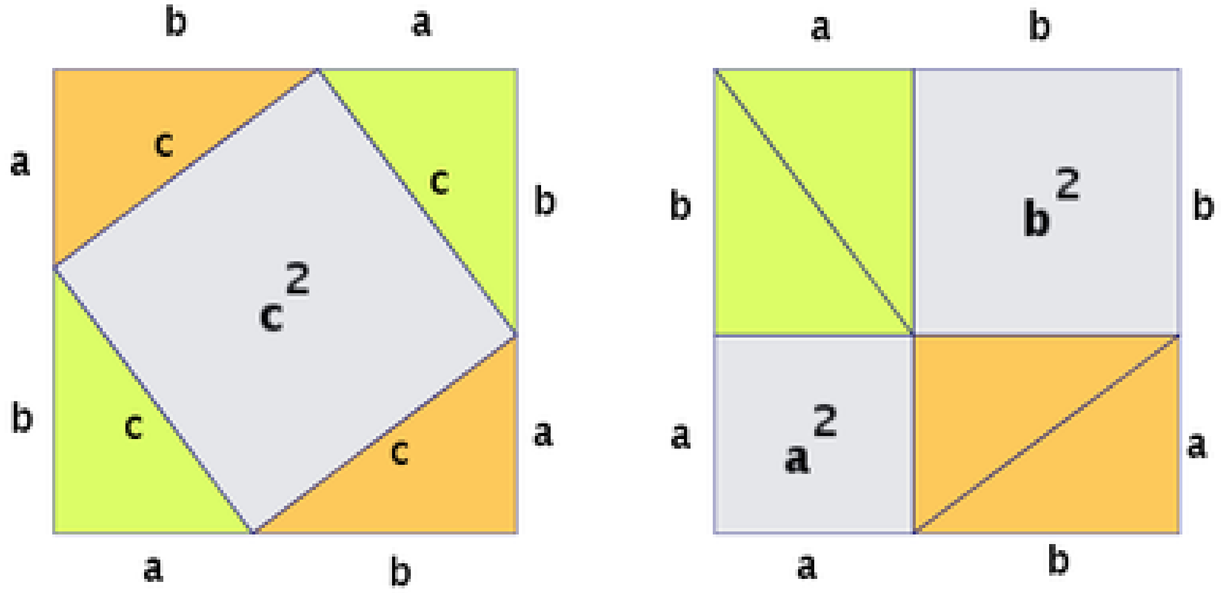

Figure 3 Pythagoras's art

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.

□

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 (Euclid) *$\sqrt{2}$ 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. □

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.

Geometric series

Proposition (Finite geometric series) *The sum of the finite geometric series is given by the formula*

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

Proof.

$$\begin{aligned} \text{Let} \qquad S &= \quad 1 + r + r^2 + \cdots + r^{n-1}, \\ \text{so} \qquad rS &= \qquad r + r^2 + \cdots + r^{n-1} + r^n. \end{aligned}$$

Subtracting, $(1 - r)S = 1 - r^n$.

□

Proposition (Infinite geometric series) *For $|r| < 1$, the sum of the infinite geometric series is given*

$$1 + r + r^2 + \cdots = \frac{1}{1 - r}.$$

Exercises

1. Prove that there exist positive integers n and m such that $n^2 + m^2 = 100$. Hint: $3^2 + 4^2 = 5^2$.

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

   a. What is the length of the diagonal? $\sqrt{l^2 + b^2 + h^2}$.
   b. By what factor must each side be scaled so that the length of the diagonal is doubled? 2.

3. Represent the repeating decimals as rational numbers.

   a. 0.2222…
   b. 42.2888…
   c. 0.9999…

   Method 1: $n = 0.9 + 0.09 + 0.009 + \cdots = 0.9(1 + 10^{-1} + 10^{-2} + \cdots) = 0.9 \cdot \frac{1}{1-0.1} = 1$.

   Method 2: Let $n = 0.9999\ldots$. Then $10n = 9.9999\ldots$. Subtracting, $9n = 9$, so $n = 1$.

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.

□

Exercise *Try to prove the motivating examples by mathematical induction.*

Telescoping series

Exercise *Simplify each of the following sums to express it as a simple fraction:*

i. $\frac{1}{1\cdot 2}$

ii. $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}$

iii. $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}$

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

Prove your result.

Solution

$$
\begin{aligned}
S &= \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} \\
&= \frac{2-1}{1\cdot 2} + \frac{3-2}{2\cdot 3} + \frac{4-3}{3\cdot 4} + \cdots + \frac{(n+1)-n}{n(n+1)} \\
&= \left(\frac{1}{1}-\frac{1}{2}\right) + \left(\frac{1}{2}-\frac{1}{3}\right) + \left(\frac{1}{3}-\frac{1}{4}\right) + \cdots + \left(\frac{1}{n}-\frac{1}{n+1}\right) \\
&= 1-\frac{1}{n+1} = \frac{n}{n+1}
\end{aligned}
$$

□

Section 4
Primes

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.
   i. $13 \mid 52$. T $(52 = 4 \cdot 13)$. ii. $27 \mid 9$. F $(9 < 27)$. iii. $-3 \mid 9$. T $(9 = (-3) \cdot (-3))$.

2. Let a be an integer. Is the following true? Prove your claim.
   i. $a \mid a$. T $(a = 1 \cdot a)$. ii. $1 \mid a$. T $(a = a \cdot 1)$. iii. $a \mid 0$. T $(0 = 0 \cdot a)$.

Properties of |

Let $a, b, c, d, m, n, \in \mathbb{Z}$. Check if the following are true. Prove your claim.

1. If $a \mid b$ and $a \mid (b + c)$, then $a \mid c$. T ($b = q_1 a$ and $b + c = q_2 a$, so $c = (q_2 - q_1)a$).
2. If $a \mid b$ and $c \mid d$, then $ac \mid bd$. T ($b = q_1 a$ and $d = q_2 c$, so $bd = (q_1 q_2)(ab)$).
3. If $ab \mid c$, then $a \mid c$ and $b \mid c$. T ($c = qab$, so $c = (qb)a$ and $c = (qa)b$).
4. If $a \mid c$ and $b \mid c$, then $ab \mid c$. F ($a = 2, b = 6, c = 6$).
5. If $a \mid bc$, then $a \mid b$ or $a \mid c$. F ($a = 6, b = 3, c = 2$).
6. If $a \mid b^2$, then $a \mid b$. F ($a = 4, b = 2$).
7. (Transitivity) If $a \mid b$ and $b \mid c$, then $a \mid c$. T ($b = q_1 a$ and $c = q_2 b$, so $c = (q_2 q_1)a$).
8. (Linear combination) If $d \mid a$ and $d \mid b$, then $d \mid (ma + nb)$.
   T ($a = q_1 d$ and $b = q_2 d$, so $ma + nb = (mq_1 + nq_2)d$).

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 $n \geq 2$, $n^3 + 1$ is *not* prime.

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

Counting primes

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

Proof. Suppose that $\mathbb{P} = \{p_1, p_2, ..., p_n\}$ 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. □

Corollary *Any two consecutive integers are coprime (have no common factor except 1).*

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).*

Exercises

1. Let n be a natural number. Prove that every factor of $(n! + 1)$ other than 1 is strictly greater than n.

2. Let $n \geq 3$. Prove that there exists a prime p such that $n < p < n!$.

3. Find a million consecutive composite numbers. Explain your reasoning.
   Think about $1000001! + j$, where $j = 2, 3, \ldots, 1000002$.

4. Consider the following numbers of the form $p^2 - 1$, where p is prime.
   For example, $5^2 - 1 = 24, 7^2 - 1 = 48, 11^2 - 1 = 120$.
   Each of these numbers is divisible by 12.
   Prove or provide a counterexample to the following statement:
   If $p > 3$ is prime, then $24 \mid (p^2 - 1)$.
   Firstly, $p^2 - 1 = (p - 1)(p + 1)$. Now, $p - 1, p, p + 1$ are consecutive numbers, so one of them must be divisible by 3, and it cannot be p. So 3 is a factor of $p^2 - 1$. Moreover, $p - 1$ and $p + 1$ are consecutive even numbers, so one of them must be divisible by 4 and the other by 2. Therefore $p^2 - 1$ must be divisible by $2 \cdot 3 \cdot 4 = 24$.

The prime number theorem

Definition *For every natural number n, define $\pi(n)$ to be the number of primes less than or equal to n.*

Example $\pi(7) = 4$, *because there are 4 primes less than or equal to 7, namely* $2, 3, 5, 7$.

Theorem $\pi(n) \to \frac{n}{\log(n)}$ *as* $n \to \infty$.

Here log *is the natural logarithm function.*

Remark *The prime number theorem tell us how the primes are distributed on a grand scale, but it does not tell us precisely which numbers will be prime and which will not.*

Landau's problems, 1912

1. Goldbach's conjecture states that every even integer greater than 2 can be expressed as the sum of two primes.

2. A *twin prime* is a prime number that is either 2 less or 2 more than another prime number — for example, either member of the *twin prime pair* $(41, 43)$. The twin prime conjecture states that there are infinitely many primes p such that $p + 2$ is also prime.

3. Legendre's conjecture states that there is a prime number between n^2 and $(n + 1)^2$ for every natural number n.

4. The near-square primes conjecture states that there are infinitely many primes of the form $n^2 + 1$.

More conjectures

1. A *Mersenne prime* is a prime of the form $2^n - 1$, e.g.

   i. Show that if $2^n - 1$ is prime, then n has to be prime.
   ii. Give a counterexample to show that the converse is not true.

   The Mersenne prime conjecture states that there are infinitely many Mersenne primes.

2. A *perfect number* is a positive integer that is equal to the sum of its proper positive divisors, e.g. 6, 28, 496. There are two questions.

   i. Are there infinitely many perfect numbers?
   ii. Are there any odd perfect numbers?

Generating primes — some attempts

1. Trying to find a function.

   i. Fermat numbers: $F(n) = 2^{2^n} + 1$.
   Euler showed that $F(5)$ is composite after a century.
   ii. Euler: $f(n) = n^2 + n + 41$.
   Show that $f(40)$ and $f(41)$ are both composite.
   iii. Mersenne numbers: For p prime, define $M(p) = 2^p - 1$.
   Counterexample: $M(11)$ is composite.

2. Trying to find a sequence which gives infinitely many primes.

   i. Near-square prime conjecture: $g(n) = n^2 + 1$
   ii. Dirichlet prime number theorem: The sequence given by $D(n) = an + b$ has infinitely many prime numbers if a and b are coprime.

Status of research for primes

1. Identifying primes: solved — AKS primality test (Agrawal, Kayal, & Saxena, 2004).
2. Constructing primes: open.
3. Fast factorization: open.
4. Twin primes: substantial progress by Yitang Zhang in 2013, as well as by James Maynard, Terence Tao.

Section 5
The Euclidean algorithm

GCD and LCM

Definition *Let $a, b \in \mathbb{Z}, a \neq 0 \neq b$. The greatest common divisor* (gcd) *of a and b is the largest $d \in \mathbb{N}$ for which $d \mid a$ and $d \mid b$. We write $d = \gcd(a, b)$.*
Numbers whose gcd *is 1 are called coprime.*
Let $a, b \in \mathbb{Z}, a \neq 0 \neq b$. The least common multiple (lcm) *of a and b is the smallest $m \in \mathbb{N}$ for which $a \mid m$ and $b \mid m$. We write $m = \operatorname{lcm}(a, b)$.*

Exercises

1. Calculate the gcd and lcm of the following sets of numbers:
   i. $\{1331, 2431\}$
   ii. $\{-60, 207\}$
   iii. $\{15, 20, 48\}$
   iv. $\left\{2^2 \cdot 3^2 \cdot 5^2,\ 5^3 \cdot 11 \cdot 17^2,\ 2 \cdot 5^2 \cdot 17\right\}$

2. Let $n > 1$ be an natural number. Calculate the gcd and lcm of the following sets of numbers:
   i. $\{n, 3n\}$.
   ii. $\{n, n+1\}$.
   iii. $\left\{n^2 - 1, n + 1\right\}$
   iv. $\{n-1, n+1\}$ for n even.
   v. $\{n-1, n+1\}$ for n odd.

Exercises

1. Let $x, y \in \mathbb{Z}$ and let $a \in \mathbb{N}$. Prove that $\gcd(ax, ay) = a \cdot \gcd(x, y)$.

2. Reason why $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$.

3. You have to fill a 16×7 floor with square tiles. What is the largest size of tiles you can use?
   Can you express your answer as a linear combination of 16 and 7?
   Can you draw a diagram of what you did? Please do this!

4. You have to fill a 64×28 floor with square tiles. What is the largest size of tiles you can use?

5. You have tiles of size 4×6. What is the smallest square room you can fill with these tiles?

The Euclidean algorithm

Definition (Euclidean algorithm)

1. *Use Division Theorem to find q_1 and r_1 such that $a = q_1 b + r_1$.*
2. *Let $a = b$ and $b = r_1$ and use the Division Theorem again to find q_2 and r_2 such that $b = q_2 r_1 + r_2$.*
3. *Repeat Step 2 until we get $r_k = 0$. Then the* gcd *is q_k.*

Exercises: Use the Euclidean algorithm to find the gcd of the following sets.

i. $\{42823, 6409\}$.

ii. $\{2k + 1, k\}$.

iii. $\{7k + 14, 3k + 6\}$.

iv. $\{n! + 1, (n + 1)! + 1\}$.

Some key points about the Euclidean algorithm

1. It is fast. The number of steps required are at most $\log_2(ab)$ to find $\gcd(a, b)$.
   See code here: https://repl.it/@SudipSinha/GCDEuclid.

2. The order of the arguments do not matter. (Why?)

3. We can express the gcd as a linear combination of the arguments. (How?)
   This is called Bézout's identity and very useful (we will soon see why).

Lemma (Bézout's identity) *Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. Then there exists $m, n \in \mathbb{Z}$ such that $ma + nb = d$.*

Proof. Follows from extended Euclidean algorithm. □

Solutions of equations

Do the following equations have a solution? If so, how many?

1. $2x + 2y = 1$.
2. $x + y = 1$.
3. $x + y = 1, x - y = 1$.
4. $x + y = 1, x - y = 1, 3x + 2y = 1$.
5. $ax + by = 1$.
6. $x^2 + y^2 = 1$.
7. $x^2 + y^2 = 1, x + y = 1$.
8. $x^3 + y^3 + z^3 = 33$.
   See this and this.

Linear Diophantine equations

1. René Descartes' unified geometry and algebra into what is known as analytical geometry.

2. In 2D analytical geometry, equations of the form $ax + by = c$, where $a, b, c \in \mathbb{R}$ is given and $x, y \in \mathbb{R}$ has to be found, represent a straight line in the *Cartesian plane*.
   Every point that lies on the line satisfies the equation.
   This equation has infinitely many solutions.

3. What can we now say about the same equation if we have $a, b, c \in \mathbb{Z}$ and need $x, y \in \mathbb{Z}$? This is called a linear Diophantine equations in two variables.

4. In general, a Diophantine equation is a polynomial equation, usually in two or more unknowns, such that only integer solutions are sought or studied. These are named after the Greek mathematician/philosopher Diophantus of Alexandria ($\sim$ 200 - 300 AD).

Which linear Diophantine equations have solutions?

Lemma (Euclid's lemma) *Let $a, b, d \in \mathbb{Z}$. If $d \mid ab$ and $\gcd(d, a) = 1$, then $d \mid b$.*

Proof. Since $\gcd(d, a) = 1$, by Bézout's identity we can find $m, n \in \mathbb{Z}$ such that $1 = md + na$. This implies $b = mdb + nab = (mb)d + n(ab)$. Since d divides both terms on the right hand side, d must divide b. □

Theorem *Let $a, b, c \in \mathbb{Z}$. Then the equation $ax + by = c$ has integral solutions iff $\gcd(a, b) \mid c$.*

Proof. Let $d = \gcd(a, b)$. So $d \mid a$ and $d \mid b$. That is, there exists $q_1, q_2 \in \mathbb{Z}$ such that $a = q_1 d$ and $b = q_2 d$.

($\Longrightarrow$) Let (x_0, y_0) be a solution. Then $c = ax_0 + by_0 = q_1 dx_0 + q_2 dy_0 = (q_1 x_0 + q_2 y_0)d$.

($\Longleftarrow$) Since $d \mid c$, there exists $q_0 \in \mathbb{Z}$ such that $c = q_0 d$. Moreover, by Bézout's identity, there exists $m, n \in \mathbb{Z}$ such that $ma + nb = d$. Multiplying by q_0, we have $(q_0 m)a + (q_0 n)b = q_0 d = c$, so $(x, y) = (q_0 m, q_0 n)$ is a solution. □

Towards a general solution

Theorem (General solution from particular solution) *Let $a, b, c \in \mathbb{Z}$. If (x_0, y_0) be a particular solution to the linear Diophantine equation $ax + by = c$, then the general solution is given by $\left\{\left(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k\right) : k \in \mathbb{Z}\right\}$.*

Proof. Since (x_0, y_0) is a particular solution, $ax_0 + by_0 = c$. If (x, y) is a general solution, we have $ax + by = c = ax_0 + by_0$, which gives $a(x - x_0) = -b(y - y_0)$.

TODO □

A simple problem

For the first sixth of his life, Diophantus was a boy. After another twelfth of his life, Diophantus grew beard. One-seventh of this life after this, Diophantus married. Five years after his marriage, Diophantus's son was born. Diophantus's son died at a relatively young age. Four years after his son died, Diophantus himself died. The total number of years the son lived is one-half the total number of years Diophantus lived.

Write one or more equations that express the information in the riddle algebraically. Then solve the equation(s) to determine the following:

i. The total number of years Diophantus lived.
ii. The number of years Diophantus was a boy.
iii. The age at which Diophantus grew a beard.
iv. The age at which Diophantus got married.
v. Diophantus's age when his son was born.
vi. Diophantus's age when his son died.

Exercise *Find the general solution of the Diophantine equation* $42823x + 6409y = 17$.

Exercise *Find a solution of the Diophantine equation* $6x + 10y + 45z = 1$.

Section 6
Modular arithmetic

Modular arithmetic

Modular arithmetic was developed by Carl Friedrich Gauss in his book Disquisitiones Arithmeticae, written in 1798 when he was 21 and first published in 1801 when he was 24 years old.

Definition *Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If $n \mid (a - b)$, then a and b are said to be congruent modulo n, symbolized by $a \equiv b \pmod{n}$ or $a \equiv_n b$.*
To reduce a modulo n means to find the remainder when a is divided by n.

Exercises

1. Is $22 \equiv_{12} 10$? Is $321 \equiv_{12} 7$?
2. Reduce 41 and -39 modulo 10.
3. Find particular solutions (both positive and negative) of the congruence equations. Can you also give general solutions?
   i. $x \equiv_{20} 15$ $\{15 + 20k : k \in \mathbb{Z}\}$ ii. $x \equiv_9 0$ $\{9k : k \in \mathbb{Z}\}$ iii. $x \equiv_{35} 37$ $\{2 + 35k : k \in \mathbb{Z}\}$.

Question: How many ways can you write 37 in the form $q \cdot 8 + r$, where $q, r \in \mathbb{Z}$?
Revision: Division theorem.

Equivalent definitions

Theorem *The following are equivalent.*

i. $a \equiv_n b$.

ii. $n \mid (a - b)$.

iii. $\exists k \in \mathbb{Z}$ *such that* $a = b + kn$.

iv. *a and b leave the same remainder when divided by n.*

Proof. i $\iff$ ii: By definition.

ii $\iff$ iii: $n \mid (a - b)$ mean $\exists k \in \mathbb{Z}$ such that $a - b = kn$, so $a = b + kn$. The other direction can be shown by going backward instead of forward.

iii $\iff$ iv: Let $\exists k \in \mathbb{Z}$ such that $a = b + kn$, and division theorem gives $b = qn + r$ $(0 \leq r < n)$. Then $a = b + kn = (qn + r) + kn = (q + k)n + r$.

On the other hand, suppose we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder r $(0 \leq r < n)$. Then $a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$, whence $n \mid (a - b)$. □

Can the congruence relation be seen as equality?

Let $n, k \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$. Which of the following are true? Prove or give a counterexample.

1. (reflexivity) $a \equiv_n a$.
2. (symmetry) If $a \equiv_n b$, then $b \equiv_n a$.
3. (transitivity) If $a \equiv_n b$ and $b \equiv_n c$, then $a \equiv_n c$.
4. (addition) If $a \equiv_n b$ and $c \equiv_n d$, then $a + c \equiv_n b + d$.
5. (multiplication) If $a \equiv_n b$ and $c \equiv_n d$, then $ac \equiv_n bd$.
6. (addition) If $a \equiv_n b$, then $a + c \equiv_n b + c$.
7. (multiplication) If $a \equiv_n b$, then $ac \equiv_n bc$.
8. (division) If $ac \equiv_n bc$, then $a \equiv_n b$.
9. (exponentiation) If $a \equiv_n b$, then $a^k \equiv_n b^k$.

Finding remainders

Lesson: Congruences cannot be seen as equality relation.

Exercises

1. Find the remainders when 2^{50} and 41^{65} are divided by 7. Hint: $2^3 = 8 \equiv_7 1$ and $41 \equiv_7 -1$.

2. What is the remainder when the following sum is divided by 4?

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5.$$

3. What is the remainder when the following sum is divided by 12?

$$1! + 2! + 3! + \cdots + 99! + 100!.$$

4. Prove the following.
   i. $39 \mid (53^{103} + 103^{53})$.
   ii. $7 \mid (111^{333} + 333^{111})$.
   iii. $41 \mid (2^{20} - 1)$.
   iv. $89 \mid (2^{44} - 1)$.
   v. $97 \mid (2^{48} - 1)$.

5. For $n \in \mathbb{N}$, prove the following divisibility statements:
   i. $13 \mid (3^{n+2} + 4^{2n+1})$.
   ii. $7 \mid (5^{2n} + 3 \cdot 2^{5n-2})$.

Equivalence relations

Definition *Any relation which is reflexive, symmetric, and transitive is called an equivalence relation.*

Example *Congruence relation is an equivalence relation.*

Exercise *Give other examples and non-examples of equivalence relations.*

Definition *A partition of a set is a grouping of the set's elements into non-empty, disjoint subsets.*

Example

i. *Even and odd numbers partition the set of integers. It corresponds to the relation* $\equiv_2$.

ii. *The sets* $[0] = \{3k : k \in \mathbb{Z}\}, [1] = \{3k + 1 : k \in \mathbb{Z}\}, [2] = \{3k + 2 : k \in \mathbb{Z}\}$ *partition the set of integers. It corresponds to the relation* $\equiv_3$.

iii. *In general, the relation* $\equiv_n$ *generates the partition* $[0], [1], [2], ..., [n - 1]$, *where* $[i] = \{i + kn : k \in \mathbb{Z}\}$.

Theorem *There is a one-to-one correspondence between equivalence relations and set partitions.*

Congruence classes

1. Representation
2. Arithmetic

Division

Theorem *If* $ca \equiv_n cb$, *then* $a \equiv_{\frac{n}{d}} b$, *where* $d = \gcd(c, n)$.

Proof. By hypothesis, we can write $c(a - b) = ca - cb = kn$ for some integer k. Knowing that $\gcd(c, n) = d$, there exist coprime integers r and s satisfying $c = dr, n = ds$. When these values are substituted in the displayed equation and the common factor d canceled, the net result is $r(a - b) = ks$. Hence, $s \mid r(a - b)$ and $gcd(r, s) = 1$. Euclid's lemma yields $s \mid (a - b)$, which may be recast as $a \equiv_s b$; in other words, $a \equiv_{\frac{n}{d}} b$. □

Corollary *If* $ca \equiv_n cb$ *and* $\gcd(c, n) = 1$, *then* $a \equiv_n b$.

Definition *Let* $n \in \mathbb{N}$ *and* $a \in \mathbb{Z}$. *Then the multiplicative inverse of a modulo n is an integer x such that* $ax \equiv_n 1$.

Solve the following congruences equations.

i. $x + 8 \equiv_{10} 0$.

ii. $3x \equiv_{12} 0$.

iii. $7 + 3x \equiv_{10} 0$.

iv. $4x + 6 \equiv_{10} 0$.

v. $1 + 8x \equiv_{10} 0$.

Positional representations of numbers

Numbers can be represented in various positional systems. These usually change the base from 10 to another number. Following is a list of commonly used bases. For more information see the Wikipedia article on positional notation.

1. Base 10 (decimal): Used almost universally by humans (with exceptions).
   Here $d_n \cdots d_2 d_1 d_0 = d_n \cdot 10^n + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$, where $d_i \in \{0, 1, \ldots, 9\}, i \in \{0, \ldots, n\}$.

2. Base 2 (binary): Used to represent information in computers.
   Minimum base required to represent numbers and other information.
   Here $d_n \cdots d_1 d_0 = d_n \cdot 2^n + \cdots + d_1 \cdot 2^1 + d_0 \cdot 2^0$, where $d_i \in \{0, 1\}, i \in \{0, \ldots, n\}$.

3. Base 16 (hexadecimal): Useful for computing. Here $d_n \cdots d_1 d_0 = d_n \cdot 16^n + \cdots + d_1 \cdot 16^1 + d_0 \cdot 16^0$, where $d_i \in \{0, \ldots, 9, A, \ldots, F\}, i \in \{0, \ldots, n\}$.

4. Base 8 (octal): Useful for computing. Here $d_n \cdots d_1 d_0 = d_n \cdot 8^n + \cdots + d_1 \cdot 8^1 + d_0 \cdot 8^0$, where $d_i \in \{0, \ldots, 7\}, i \in \{0, \ldots, n\}$.

5. Base 60 (Babylonian): Used to write time and angles.

Tests of divisibility for *decimal* numbers

1. Test for 2: The number n must have $0, 2, 4, 6, 8$ as the units digit.
   Proof. $n = d_n \cdots d_1 d_0 = 10^n d_n + \cdots + 10 d_1 + d_0 \equiv_2 d_0$, so $2 \mid n \iff 2 \mid d_0$. □

2. Test for 5: The number n must have $0, 5$ as the units digit.
   Proof. $n = d_n \cdots d_1 d_0 = 10^n d_n + \cdots + 10 d_1 + d_0 \equiv_5 d_0$, so $5 \mid n \iff 5 \mid d_0$.. □

3. Test for 3 (similar for 9): The number n must have its sum of digits divisbile by 3.
   Proof. $n = d_n \cdots d_1 d_0 = 10^n d_n + \cdots + 10 d_1 + d_0 \equiv_3 d_n + \cdots + d_1 + d_0$. □

4. Test for 4 (similar for 25): The number n must have its last two digits divisible by 4.
   Proof. $n = d_n \cdots d_2 d_1 d_0 = 10^n d_n + \cdots + 100 d_2 + 10 d_1 + d_0 \equiv_4 d_1 \cdot 10 + d_0 = d_1 d_0$. □

5. Tests for 2^n and 5^n: The number n must have its last n digits divisible by 2^n and 5^n, respectively.
   Key idea: $10^n = 2^n 5^n$.

6. Test for 11: The number n must have its alternating sum of digits divisible by 11.
   Proof. $n = d_n \cdots d_2 d_1 d_0 = 10^n d_n + \cdots + 10 d_1 + d_0 \equiv_{11} (-1)^n d_n + \cdots + d_2 - d_1 + d_0$. □

Tests of divisibility for *decimal* numbers

1. Test for 7: The difference between twice the units digit of the number n and the number formed by the rest of the digits is divisible by 7. Repeat to get only one digit left.
   Proof. $n = 10m + d_0 \equiv_7 10m + d_0 - 3 \cdot 7 \cdot d_0 = 10(m - 2d_0)$. □

2. Test for 13: The sum of four times the units digit of the number n and the number formed by the rest of the digits must be divisible by 13. Repeat to get only two digits left.
   Proof. $n = 10m + d_0 \equiv_{13} 10m + d_0 + 3 \cdot 13 \cdot d_0 = 10(m + 4d_0)$. □

Systems of congruences and the Chinese remainder theorem

Exercise (Sunzi Suanjing, 3rd-century AD) *There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?*

We shall not see the theorem as it can be confusing. We will see how to apply it. A great explanation of using the Chinese remainder theorem is given in this video on YouTube.
Caution: For the Chinese remainder theorem to be valid, the moduli must be pairwise coprime.

Solve the following systems of congruences.

i. $x \equiv_9 3, x \equiv_{10} 7$.
   Method 1: linear Diophantine equation.
   Method 2: Chinese remainder theorem.
ii. $x \equiv_3 2, x \equiv_4 2, x \equiv_5 1$.
iii. $x \equiv_5 1, x \equiv_7 2, x \equiv_9 3, x \equiv_{11} 4$.
iv. $x^3 \equiv_{55} 3$. This can be broken down into $x^3 \equiv_5 3, x^3 \equiv_{11} 3$.

Thank you!

Bibliography

Agrawal, M., Kayal, N., & Saxena, N. (2004). PRIMES is in P. doi:10.4007/annals.2004.160.781

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