Lecture Notes

Kyle Chui

2022-01-04

Contents

1 Lecture 1

1.1 Overview of This Course

"Ancient" history of mathematics

- Egyptian mathematics (c. 3200 BCE – 300 BCE): Number system in base 10, fractions.
- Babylonian mathematics (c. 3300 BCE – 500 BCE): Place-value sexagesimal number system, roots of algebra.
- Greek mathematics (c. 700 BCE – 400 CE): Deduction method, geometry, roots of number theory.
- Mathematics in Asia (c. 1100 BCE – 1200 CE): Roots of number theory and algebra.
- Polynomial equations.
- Development of calculus, infinite series (16^{th}–17^{th} centuries CE).

1.2 The Beginnings

What is "Mathematics"?

1. Logical-deductive mathematics (initiated by the Greeks). This is not the generally accepted view of "mathematics" anymore.
2. Abstract counting problems: "mathematical" exercises without a direct practical use.
3. Practical counting problems: Bookkeeping for bureaucracy, inventories of goods and harvest, calculations involving lengths and areas for farming purposes, etc.
4. Development of a number system.

> **Note.** We will see later that 2–4 all occur almost simultaneously.

1.3 Egyptian Mathematics

Most writing was done on papyrus, which doesn't preserve well, so we don't have much evidence from this period.

1.3.1 Egyptian Number System

The Egyptians had a base 10 number system, with a new Hieroglyphic symbol for each power of 10. This number system is *not* place valued. One simply adds all the symbols to get the number. For instance $\cap\cap\cap|||| = 34$. By comparison, our modern number system is place-valued, which means that the position of each digit matters, i.e. $254 \neq 452$.

1.3.2 Egyptian Arithmetic

Summation is extremely easy, you just write the numbers next to each other to get their sum. Multiplication was done via consecutive doubling and adding. We do this by decomposing one number into powers of 2, and then distributing the other number across this sum. Because of this method, Egyptians had tablets with powers of 2, and tablets with consecutive doublings of many numbers.

We also have sources of:

- Fractions—The Egyptians used almost exclusively fractions of the form $\frac{1}{n}$ (aside from $\frac{2}{3}$ and $\frac{3}{4}$) and used sums of these to express more general fractions.

- Notation—Since any fraction can be written as the sum of fractions of the form $\frac{1}{n}$, any general fraction could be written by just writing $\frac{1}{n}$ fractions next to each other.
- Algebra—We have evidence that they solved some linear and second order (quadratic) equations.
- Geometry—Though limited, we have evidence that the Egyptians could calculate areas and volumes of triangles, circles, pyramids, etc.

However we see no evidence for a general theory for solving these questions, and all of the problems that we know of are elementary and mostly practical. The earliest "advanced" mathematical resources from the Egyptians are from around 1900 BCE, and are predated by Babylonian mathematics.

2 Lecture 2

2.1 Babylonian Mathematics

The Babylonians, in comparison to the Egyptians:

- had a more advanced number system,
- solved more difficult problems,
- solved more abstract ("useless") problems.

Hence people often view the Babylonians in Mesopotamia as being the starting point of "serious" mathematics.

Mesopotamia was located between the Tigris and Euphrates rivers, and its name means "the land between the rivers". Historical texts from Mesopotamia are unusually well-preserved, because texts were made by making impressions on clay tablets, which hardened and preserve well.

2.1.1 Babylonian Number System

The Babylonian number system was a *sexagesimal* (base 60), place-valued system.

Note.

- The number zero didn't exist just yet! So instead of writing "20", they would just write "2", and figure out what number it took from context.
- They also had fractions, but didn't have a symbol for a decimal point, so they again guessed based on context.
- Furthermore, since there is no zero, there was no way of distinguishing between $1 \cdot 60^2 + 30 \cdot 1$, or $1 \cdot 60 + 30 \cdot \frac{1}{60}$, etc.

Later on in Mesopotamia, we see the first usage of the number zero (300 BCE), but only as a place holder to solve the aforementioned issues. This was also done by the Mayans around 400 CE. It was not until 600 CE that the number zero was invented in India, and carried its full weight as a "number".

Note. There are still remnants of the Babylonian sexagesimal number system in the modern day.

- Time: Hours and minutes are divided into 60 pieces
- Angle measurements are still done in multiples/factors of 60, i.e. 360°.

2.1.2 Babylonian Algebra

This notation was also used to solve basic algebra questions, but we don't know how exactly these problems were solved (probably the same method as the Egyptians, guess and check). It is believed that math problems were given to students in order to train them in literacy, numeracy, and applications to administration. The Babylonians also knew about the quadratic formula, although it was described in words as opposed to being given as an equation. Furthermore, although they knew of the quadratic formula, they did not have negative numbers, and so found only one solution to quadratic equations. This is the first instance we know of where a civilization has an "algorithmic" solution to a problem.

2.1.3 Babylonian Geometry

We have some sources of Babylonian geometry that indicate that they knew of the Pythagorean Theorem. One example of this is the "IM 67118" tablet, which gives the sides of a rectangle given its area and diagonal

length. There is a tablet called "Plimpton 322" that contains Pythagorean triples, or integer triplets a, b, c satisfying $a^2 + b^2 = c^2$.

3 Lecture 3

Another tablet titled "YBC7289" contains approximations for $\sqrt{2}$ and $\frac{1}{\sqrt{2}}$ that has an error of less than 1 in 2 million.

3.1 Greek Mathematics

Note. A lot of "Greek" mathematicians did not come from what is nowadays Greece, but rather the old Hellenistic empire (which was larger).

3.1.1 The Theorem of Pythagoras

Probably the oldest "mathematical theorem", known (in some form) to:

- Egyptians
- Babylonians
- Chinese
- Indians
- Greeks

before Pythagoras.

What we know about Pythagoras with (quasi-)certainty

- He existed (~580 BCE–500 BCE)
- He was born in Samos (modern day Turkey)
- He left no writings himself
- He founded a school in Croton (c. 540 BCE)
  - We say "school" but it was more like a sect, with strict rules and secrecy
  - Their central belief was "All is number", and that every number has a meaning
  - The number 10 was a "holy number", often drawn as a triangle
  - Theory of music based on whole fractions
  - Largely responsible for introducing "rigorous" mathematics
  - They viewed "pure" mathematics as the opposite of "applied" mathematics

Theorem — *Pythagorean Theorem*
Given a right triangle with legs a and b and hypotenuse c, we have

$$a^2 + b^2 = c^2.$$

Definition. *Pythagorean Triples*
Triples (a, b, c) that satisfy $a^2 + b^2 = c^2$ are called *Pythagorean triples*.

General Formula: For positive integers p, q, r such that $p \geq q$, we can use the following equations:

$$\begin{aligned} a &= (p^2 - q^2)r \\ b &= 2pqr \\ c &= (p^2 + q^2)r \end{aligned}$$

"Facts":

- Less general formulas were known to Pythagoras' school, Plato, Babylonians...
- The first statement *and* proof of this formula is from Euclid's "Elements", book 10

3.1.2 Rational points on the circle

Finding rational points on the unit circle with rational coordinates is actually very related to finding Pythagorean triples.

4 Lecture 4

4.1 Rational Points on the Circle

Observation. If $a^2 + b^2 = c^2$, then

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

Hence rational points on the unit circle correspond to Pythagorean triples.

4.2 Chord-Tangent Construction

- The idea is most likely due to Diophantos, circa 250 CE.
- Worked out in detail in the 17^{th} century (Lagrange, Euler, etc.).
- Take a line through $(-1, 0)$ to (x, y) with slope t. The equation of this line is thus $y = t(x + 1)$.
- We claim that R has rational coordinates if and only if t is rational.

Proof. ($\Rightarrow$) Suppose $R = (x_0, y_0)$, with $x_0, y_0 \in \mathbb{Q}$. The slope of the line can be computed to be $\frac{y_0}{1+x_0} = t$. Thus t is rational.
($\Leftarrow$) Suppose t is rational. Since the line intersects the unit circle, we have

$$\begin{aligned} x^2 + y^2 &= 1 \\ x^2 + t(x+1)^2 &= 1 \\ x^2 + tx^2 + 2tx + t &= 1 \\ (1+t)x^2 + (2t)x + (t-1) &= 0. \end{aligned}$$

Observation: If x_0, x_1 are solutions of $ax^2 + bx + c = 0$, then we know that we can factor into $a(x - x_0)(x - x_1) = 0$. Thus by equating coefficients, we see that x_0 is rational if x_1 is rational.

We already know that $x_1 = -1$ is a solution to our equation, so we know that x must be rational. Since $y = t(x_0 + 1)$, it must be rational as well, so R has rational coordinates. □

If we actually solve the equation, we get the point R has coordinates $(-1, 0)$ or $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$. If we write $t = \frac{p}{q}$ for integers p, q, then we have

$$x_0 = \frac{p^2 - q^2}{p^2 + q^2}, y_0 = \frac{2pq}{p^2 + q^2}.$$

Thus we may convert this into a true Pythagorean triple via

$$\begin{aligned} a &= (p^2 - q^2)r \\ b &= 2pqr \\ c &= (p^2 + q^2)r \end{aligned}$$

Note. The general takeaway from this proof is that you can use "known" points to help you deduce properties of certain "unknown" points. In this case, we found an intersection point between a line and a circle, using that we are given the other intersection point.

5 Lecture 5

5.1 Irrational Numbers

Claim. The square root of 2 is irrational.

Lemma. If a^2 is even, then so is a.

Proof. We proceed via proof by contrapositive. Suppose a is odd, so $a = 2k+1$ for some $k \in \mathbb{Z}$. Then

$$a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Hence a^2 is odd. □

Proof. Suppose towards a contradiction that $\sqrt{2}$ is rational, so $\sqrt{2} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ where $q \neq 0$. We may also assume that the greatest common factor of p, q is 1, since we otherwise could have pulled the factor out. Hence

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

Since p^2 is even, p must be even, and so $p = 2k$ for some $k \in \mathbb{Z}$. Thus

$$(2k)^2 = 2q^2$$
$$4k^2 = 2q^2$$
$$2k^2 = q^2.$$

Since q^2 is even, so must q. However, this contradicts our assumption that the greatest common factor of p and q is 1. □

The original Greek conclusion was that "geometric quantities" were different from "numbers". They used rational numbers to "describe" irrational numbers. This later led to the "theory of proportions" and the method of exhaustion, which inspired Dedekind cuts.

Note. The theorem of Pythagoras also gives a notion of *distance* between points in the plane, e.g.

$$d((x_1, y_1), (x_2, y_2)) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

5.2 Greek Geometry

The most important resource for Greek geometry is Euclid's "The Elements".

- It was written circa 300 BCE
- It consists of 465 theorems and proofs in 13 books
- Mostly comprised of works from earlier mathematicians
- Main contributions:
  - The deductive method
  - Unified framework for "Euclidean geometry".

Facts about Euclid:

- Lived in Alexandria
- Called the "father of geometry"

6 Lecture 6

6.1 Greek Geometry

6.1.1 The Deductive Method

The "Elements" from Euclid is the first mathematical text where statements are derived step by step, starting from axioms ("postulates") following certain rules ("common notions").

(1) Definitions: It starts with 23 definitions, i.e. of "point", "line", "parallel lines", "circle", etc.

(2) Postulates ("Ruler–Compass Construction"):

(a) To draw a straight line from any point to any point.

(b) To produce a finite straight line continuously into a straight line.

(c) To describe a circle with any center and distance ("radius").

(d) All right angles are equal to each other.

(e) If a straight line falling on two straight lines makes the interior angles on the same sides less than two right angles, then the two straight lines, if produced indefinitely, meet on the side which the angles are less than two right angles.

(3) Common Notions:

(a) Things which are equal to the same thing are also equal to each other ("Transitivity of equality").

(b) If equals are added to equals, the wholes are equal.

(c) If equals are subtracted from equals, the remainders are equal.

(d) Things which coincide with one another are equal to one another.

(e) The whole is greater than the part.

> **Note.** The word "equal" means "have the same length/area/volume", whereas the word "coincide" is when two objects are "really the same".

Note. Often, Euclid uses "visually obvious" assumptions that are not mentioned in the postulates.

Example. *Proposition I.35 of the "Elements"*
"Parallelograms with the same base and the same height are equal".

Note. Some of the proofs are flawed because they make visual assumptions of the layouts of problems, rather than use equations and variables.

7 Lecture 7

In the 19^{th} century, mathematicians started to develop "non-Euclidean" geometries by adjusting the 5^{th} postulate.

Fact. Assuming the first four postulates, the fifth postulate is equivalent to the following: "In a plane, there exactly one line parallel to a given line through a given point".

Adjustments

1) There are no such lines (spherical geometry)

2) There are more than one such lines (hyperbolic geometry)

7.1 The Regular Polyhedra (the Platonic Solids)

There are the:

- Tetrahedron
- Cube
- Octahedron
- Dodecahedron
- Icosahedron

As far as we know, they were the first entirely described and proven that they are the only regular solids by Theaetetos, circa 400 BCE.

> **Note.** If you take a regular polyhedron and create new vertices at the center of each face, you can construct another regular polyhedron.

Via the above described method, you can construct the octahedron from the cube.

8 Lecture 8

8.1 Ruler and Compass Constructions

Even though it was "abstract", Greek mathematics was largely guided by geometric intuition. Most of their geometry is built on constructions with ruler (straight lines) and compass (circles).

They typically constructed:

- Perpendicular lines
- Bisection of an angle
- Square root of a given length
- Circle through three points

Fact. Given points $P_1, \dots, P_n$ in the plane, we can construct with ruler and compass exactly those points whose coordinates can be obtained from the P_i's using $+, -, \times, \div, \sqrt{}$.

Famous impossible problems that the Greeks tried to solve:

- Doubling the cube
- Trisecting an angle
- Squaring the circle

All of the above were proven impossible in the 19^{th} century with modern techniques.

8.2 Conic Sections

We obtain conic sections by finding the intersection between two cones (one inverted) and a plane. We think that these curves were invented by Menaechmos, circa 400 BCE. From this we get our equations for conic sections:

- Hyperbola: $\dfrac{x^2}{a^2} - \dfrac{y^2}{b^2} = 1$.
- Ellipse: $\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1$.
- Parabola: $y = ax^2$.

8.3 Higher Degree Curves

> **Note.** The Greeks did not have "equations".

8.3.1 Cissoid of Diocles

Another graph that has a nice mathematical description, but is impossible to construct with just a ruler and compass. It has the equation

$$y^2(1+x) = (1-x)^3. \qquad (0 \le x \le 1)$$

Fact. Both conic sections and the cissoid can be used to solve the doubling of the cube, i.e. to construct $\sqrt[3]{2}$.

9 Lecture 9

9.1 Greek Number Theory

Fact. The basics of number theory are contained in the Elements, mostly connected to the "Euclidean algorithm".

- The only other major advancement in the Greek empire: Diophantos (circa 250 AD, Alexandria), who studied Diophantine equations
- Later, there are much more advances in India, China, the Middle East, etc.

9.1.1 Polygonal, Prime, Perfect Numbers

Polygonal numbers were studied by the Pythagoreans. We start with triangular numbers, which are just equilateral triangles consisting of dots, like ∴. They go $1, 3, 6, 10, \ldots$. Square numbers are what you think they are, just perfect squares. The pentagonal numbers start $1, 5, 12, 22, \ldots$.

Note. While interesting, the polygonal numbers don't seem to have many uses. They are also given by quadratic equations, i.e.the n^{th} pentagonal number is given by

$$P_n = \frac{3n^2 - n}{2}.$$

9.1.2 Prime Numbers

Definition. *Prime*
A number is *prime* if it is only divisible by 1 and themselves.

Note. The Greeks called them "numbers with no rectangular representations", where a rectangular representation was a drawing of n dots that wasn't just a line of dots.

Euclid proved that there are infinitely many prime numbers, "Prime numbers are more than any assigned multitude of primes".

Proof. Suppose towards a contradiction that there are finitely many primes, say $p_1, \ldots, p_n$. Then observe that $p_1 p_2 \cdots p_n + 1$ is not divisible by any p_i for $i = 1, \ldots, n$, and so must be prime. Hence there must be infinitely many primes. □

9.1.3 Perfect Numbers

Definition. *Perfect Numbers*
A *perfect* number is a number that equals the sum of its divisors (excluding itself).

For example, $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 7 + 14$.
Fact. We know that k is an even perfect number if and only if k takes the form

$$k = 2^{n-1}(2^n - 1)$$

for $n \in \mathbb{N}$ and $2^n - 1$ is prime (Mersenne prime).

Open Problems

- Are there any odd perfect numbers?
- Are there infinitely many even perfect numbers/Mersenne primes (51 known)?

10 Lecture 10

10.1 The Euclidean Algorithm

This algorithm is used to find the greatest common divisor of two numbers. It was most likely known before Euclid, but it first appears in the Elements.

10.1.1 Performing the Algorithm

We wish to find $\gcd(a, b)$ where $a, b \in \mathbb{Z}$.

- Construct $a_1 = \max(a, b) - \min(a, b)$ and $b_1 = \min(a, b)$. Note that $\gcd(a, b) = \gcd(a_1, b_1)$.
- Repeat this until $a_n = b_n$, at which point $\gcd(a, b) = a_n$.

10.1.2 Consequences of the Euclidean Algorithm

- Given $a, b \in \mathbb{Z}^+$, there exist integers $m, n \in \mathbb{Z}$ such that

$$am + bn = \gcd(a, b).$$

> **Note.** If you "work backwards" through the Euclidean Algorithm, you see that $\gcd(a, b)$ is a linear combination of a and b.

- If a prime number p divides ab, then p divides a or p divides b.

  Proof. Suppose p does not divide a. We claim that p divides b. Since p is prime and does not divide a, we have $\gcd(p, a) = 1$. Hence there exist $m, n \in \mathbb{Z}^+$ such that $mp + na = 1$. Multiplying both sides by b, we have

$$mpb + nab = 1.$$

  Since p divides ab, we have $ab = kp$ for some $k \in \mathbb{Z}$. Hence

$$mpb + nkp = b$$
$$p(mb + nk) = b.$$

  Therefore p divides b. □

- Each positive integer has a unique factorization into primes.

10.2 Greek Number Systems

- There were different number systems in different parts of the Hellenistic realm.
- They are usually decimal (base 10).
- They are usually *not* place-valued.

Example. *Acrophonic System*

- Symbols for 1, 5, 10, 100, 1000, and *sometimes* for 50, 500, etc.
- Not place-valued, just add symbols.
- Lead to "Roman numerals", which were used in Europe till the late Middle Ages (~1500).

Example. *Alphabetic System (most common)*

- 27 letters of the alphabet were used for 1–9, 10–90, and 100–900.
- This was used for numbers up to 999, and it becomes similar to a place-valued system.
- The symbol **M** was used to represent "multiplication by 10000".

11 Lecture 11

11.1 Infinity in Greek Mathematics

- Greek mathematicians (back then) were "afraid" of infinity.
- They did not believe that actual "infinite processes" exist.

Example. *Zeno's Paradoxes*

- Attributed to Zeno of Elea (~450 BCE).
- Not clear what his intentions were.
- Sources: Aristotle.

Achilles and the Tortoise Paradox

- Achilles runs faster than the tortoise.
- For the race, the tortoise gets a head start.
- Intuitively, Achilles should catch up to the tortoise, but in order to catch up to the tortoise he first must reach where the tortoise currently is, and in that time the tortoise will have already moved on. Hence Achilles will never overtake the tortoise.

Dichotomy Paradox

- Motion cannot exist because what is moved has to first arrive at the halfway point before reaching the destination.
- Before reaching the halfway point, it must reach the halfway point to the halfway point, and so on and so forth.

Note. By trying to avoid ∞, the Greeks laid the foundations of a rigorous treatment of it.

Eudoxus of Knidos

- Lived around 375 BCE.
- Developed both the "theory of proportions" and "method of exhaustion".
- For example, he described a "quantity" (real number) by its position among rational numbers.
- His works are contained in Book V of the Elements.

11.2 Theory of Proportions

Example. *Describing the quantity $\sqrt{2}$ with rational numbers*Observe that $\sqrt{2}$ is determined by two sets:

$$L_{\sqrt{2}} = \left\{r \in \mathbb{Q} \mid r^2 < 2\right\},$$
$$U_{\sqrt{2}} = \left\{r \in \mathbb{Q} \mid r^2 > 2\right\}.$$

Namely, $\sqrt{2}$ is the *unique* quantity so that every rational number in $L_{\sqrt{2}}$ is smaller than it, and every rational number in $U_{\sqrt{2}}$ is larger than it.

Often used in the following way: "Two quantities λ_1 and λ_2 are equal if every rational length less than λ_1 is also less than λ_2, and vice versa". Using the notation from the example above, we have

$$L_{\lambda_1} = L_{\lambda_2}.$$

Note. If we only have one side of the inequality, we can define $\lambda_1 \leq \lambda_2$.

There are two main viewpoints for irrational numbers:

- Geometric: we find some way to express these values as a length or area.
- Arithmetic: we need some kind of "infinite" description of the quantity.

Until the 19^{th} century, the overall belief was that "geometry is a better foundation for mathematics". Later on, there were more rigorous definitions of convergence, which led to other non-geometric axiomatic systems and "set theory" became the foundation for mathematics.

12 Lecture 12

Note. In 1858, Dedekind used this theory of proportions to define the reals using "Dedekind cuts". For example, he defined $\sqrt{2}$ to be $(L_{\sqrt{2}}, U_{\sqrt{2}})$.

12.1 Method of Exhaustion

This theory was also developed by Eudoxus, and generalizes the theory of proportions to higher dimensions. For example, you could approximate the area of a circle or volume of a pyramid via a bunch of intermediary steps, i.e. circumscribed polygons etc.

Theorem. The area of a circle of radius r is proportional to r^2.

Proof. Assume by contradiction the area is *not* proportional to r^2, then by taking a polygon "close enough" to the circle, it would fail for the polygon. Hence we have arrived at a contradiction. □

Note.

- Rather than taking an infinite limit, such proofs by contradiction only need finitely many steps.
- This is very much reminiscent of modern (ε, δ) proofs.

Archimedes (250 BCE) from Syracuse (Sicily)

- Known for physics (particularly mechanics) and mathematics.
- Applied and refined the method of exhaustion with great success.
- Manuscript of him was discovered in 1906, revealing *how* he discovered many of his results.
  - "*not* with an immediate perfect proof, rather first with intuition and lots of trial and error".
  - A document describing the philosophy of math.
- Approximated π to $3.1408 < \pi < 3.1429$.
- According to legend, he died during the Roman siege of Syracuse during in 212 BCE after angering a Roman soldier by refusing to leave his home until he finished his math problem, telling the soldier "Don't disturb my circles!".

13 Lecture 13

13.1 Ancient Chinese Mathematics

The ancient Chinese civilization centered around the "Yellow River", which is the 6^{th} longest river in the world.

13.1.1 Numbers and Patterns

- Compared to many other civilizations, the Chinese had a great interest in numbers and patterns.
- Numbers were believed to have cosmic significance. For instance, "1" is often related to water, and "9" to fire.
- Interesting patterns of numbers were also often given divine significance.
- One very famous example is the "Lo Shu Magic Square" (c. 650 BCE). Every row, column, and diagonal sums to the same number (15).
  - There are several legends surrounding this square, usually involving a turtle (an animal regarded as symbolizing the world, the universe, immortality, wisdom, etc.)
  - One such legend was that the river God kept flooding the Yellow River. It was due to a turtle with the magic square on its back that the emperor realized that he had to make 15 offerings to appease the river God.
  - The magic square is unique, aside from mirroring and rotating.

13.1.2 Chinese Number System

Already around 2000 BCE, the Chinese had a decimal place-value system!

They arranged bamboo rods to represent the numbers 1 to 9, and then placing them in columns, the different places corresponded to different powers of 10.

> **Note.** There is still no "0", so there's no way to express numbers such as 102.

13.1.3 Resources

- The Chinese usually wrote on bamboo, so we have limited resources. Fortunately, we have *some* resources dating back to 200 BCE. We have "Jiuzhang Suanshu", or "Nine Chapters on the Mathematical Art", written most likely over a long period of time between 1000 BCE to 250 AD by many different authors.
- Most of the problems discussed in this book are practical, revolving around solving real-world problems. They found *general* methods for solving problems, rather than solutions to specific problems.
- The book covers:
  - Arithmetic operations with positive integers, fractions, and some "special" irrational numbers. We even see negative numbers (usually in the context of debt)!
  - It contains an approximation of $\pi \approx 3.14159$, using an approximation of the circle with a regular polygon of 192 vertices. We actually know the author for this part, Liu Hui (c. 250 AD).
  - The Pythagorean Theorem.
  - Solving linear systems of equations, with what is basically Gaussian elimination.

13.1.4 Chinese Remainder Theorem

Very useful for solving Diophantine equations and systems of congruence equations, which first appeared in "Sunzi Suanjing", or "Mathematical Manual of Sun Zi", c. 400 AD.

14 Lecture 14

The stated problem was: "Find a number that leaves remainders 2 on division by 3, 3 on division by 5, and 2 on division by 7".

Explanation. If we count by threes and have remainder 2, put down 140. If we count by fives and have remainder 3, put down 63. If we count by sevens and have remainder 2, put down 30. Add them all to get 233, and subtract 210 to get the answer (23).

Observation.

$$\begin{aligned} 140 &\equiv 2 \pmod 3 \\ 140 &\equiv 0 \pmod 5 \\ 140 &\equiv 0 \pmod 7 \\ 63 &\equiv 0 \pmod 3 \\ 63 &\equiv 3 \pmod 5 \\ 63 &\equiv 0 \pmod 7 \\ 30 &\equiv 0 \pmod 3 \\ 30 &\equiv 0 \pmod 5 \\ 30 &\equiv 2 \pmod 7 \end{aligned}$$

Notice that each one of these numbers "takes care of" exactly one of the conditions. If we add all of them together, we get the correct remainders for each of the divisions. We can then just subtract as many of the products of all the numbers as many times as possible (since 105 is congruent to 0 mod 3, 5, and 7).

It remains to see how to get the values of 140, 63, and 30.

Explanation. If we count by threes and have remainder 1, put down 70. If we count by fives and have remainder 1, put down 21. If we count by sevens and have remainder 1, put down 15.

Observation. 70 is the smallest multiple of 5 and 7 with remainder 1 after division by 3. The same rule follows for 21 and 15 (3 and 7, 3 and 5). The numbers from before are simply multiples of these values.

14.1 General Method for Chinese Remainder Theorem

To find a number m such that:

$$\begin{aligned} m &\equiv a \pmod p \\ m &\equiv b \pmod q \\ m &\equiv c \pmod r, \end{aligned}$$

perform the following:

(1)
- Find a multiple of qr with remainder 1 on division by p.
- Find a multiple of pr with remainder 1 on division by q.
- Find a multiple of pq with remainder 1 on division by r.

(2) Multiply these numbers by a, b, and c, respectively.

(3) Sum the resulting numbers.

(4) Subtract an appropriate multiple of pqr to get the *smallest* possible solution.

> **Note.** It is entirely possible that there exists *no solution* for step 1!

Fact. Step 1 is possible if p, q, and r have no common divisors. In particular,

$$\gcd(p, q) = \gcd(p, r) = \gcd(q, r) = 1.$$

This was first solved in full generality in the "Shushu Jiuzhang" or the "Mathematical Treatise in Nine Sections" of Qin Jinshao, 1247 CE.

Idea. Via the Euclidean Algorithm, there exists m, n such that

$$mqr + np = 1,$$

if $\gcd(qr, p) = 1$. Hence $mqr \equiv 1 \pmod{p}$.

Fact. We can find m by "reversing" the Euclidean Algorithm.

15 Lecture 15

Theorem — *Chinese Remainder Theorem*
If $p_1, \dots, p_k$ are relatively prime (i.e. $\gcd(p_i, p_j) = 1$ for all $i \leq i \neq j \leq k$) and $r_1 < p_1, \dots, r_k < p_k$, then there exists an integer n such that

$$n \equiv r_i \pmod{p_i}$$

for every i.

Example. Find n such that

$$\begin{aligned} n &\equiv 2 \pmod 3, \\ n &\equiv 2 \pmod 4, \\ n &\equiv 3 \pmod 5. \end{aligned}$$

We first find a multiple of $4 \cdot 5$ with remainder 1 on division by 3. In this case, 40 suffices. We then find multiples of other pairs of numbers that result on a remainder by 1 when divided by the last number, which yields 45 and 36. We then scale by their respective multiples, which gives us 80, 90, 108. Their sum is 278, and then we take it mod $3 \cdot 4 \cdot 5$ to get 38 as our final answer.

15.1 Linear Diophantine Equations

"$ax + by = c$ has an integer solutions in x, y if and only if $\gcd(a, b) \mid c$".

This was observed and used a lot in China, India, etc.

15.2 Linear Equations and Elimination

In the "Nine Chapters of Mathematical Art", (c. 200BCE–200CE), the method of Gaussian elimination (row reduction) is explained. It is used to solve *systems* of linear equations. The general form is

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n \end{aligned}$$

Idea. Subtract a multiple of each equation from the ones below to get a "triangular" system.

Note. This is only possible if we don't create rows with only zeroes, or if the matrix of coefficients is invertible.

Fact. Around the 12^{th} century China, a similar method was applied to systems of polynomial equations (not necessarily linear) in two or more variables.

General Form in 2 Unknowns

$$\begin{aligned} a_0(x)y^m + a_1(x)y^{m-1} + \cdots + a_{m-1}(x)y + a_m(x) = 0, \\ b_0(x)y^m + b_1(x)y^{m-1} + \cdots + b_{m-1}(x)y + b_m(x) = 0, \end{aligned}$$

where $a_i(x), b_i(x)$ are polynomials in x.