L211 Logic and Mathematics

1. Lecture

Norbert PREINING
preining@jaist.ac.jp
www.preining.info/L211/index-en.html

2014-10-7

Self-introduction

Logic and Mathematics

Aims of the course

Ideas and concepts of mathematics are infiltrated deeply into our science and technology. Highly abstract notions of mathematics can sometimes find unexpected applications. This lecture will explain them by looking back the development of logic and mathematics, and will discuss also the current of modern mathematics.

Acquisition of basic understanding of fundamental mathematical and logical concepts.

Content

1. evolution of basic concepts in mathematics,
2. mathematical language, truth, and proofs,
3. development of mathematical logic, and
4. the current of modern mathematics

Lesson plan

	Mon 5.unit		Wed 4.unit
10/07	Examples of Math	10/08	What is Math?
10/13	*no lecture*	10/15	What are proofs?
10/20	Induction	10/22	Induction
10/27	Number systems	10/29	(infinite) sets
11/03	*no lecture*	11/05	set theory
11/10	Axiomatic method	11/12	Geometry
11/17	Functions	11/19	Graphs
11/24	Computational models	11/26	Verification
12/01	Review	12/03	Reserve day

Evaluation

- Homework
- Reports (mid-term, final)
- Contribution in class

Contact

In case of question, please contact me at:

PREINING Norbert
preining@jaist.ac.jp
Multidisciplinary Research Center 3F
C2-302a

Background of the students

What is math and logic for you?

When you think back to mathematics in your junior and high school times, what is the first thing you remember?
Please select 2 from the following:

1. Mathematics was fun
2. Mathematics was boring
3. From now on, Mathematics will be even more important
4. At the current point, there are no new things in Mathematics
5. Even though we don't see it, Mathematics is everywhere
6. Mathematics is not needed, is not useful

Today's plan

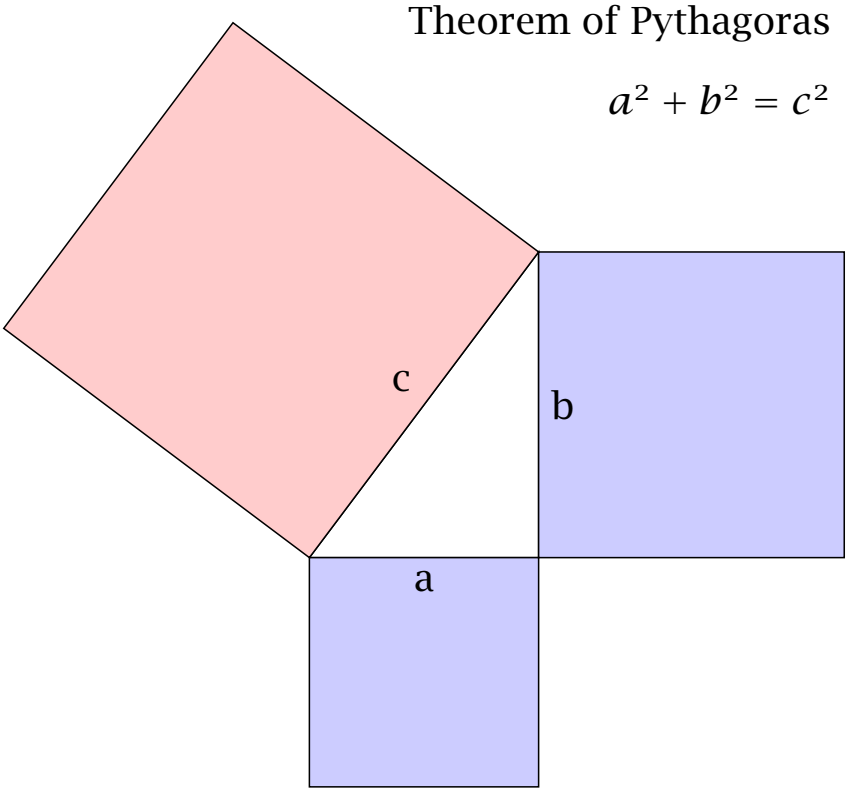
- Mathematics in the 20^{th} century
- Usefulness of Mathematics
- History

1st Example

Fermat's Last Theorem

Theorem of Pythagoras

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



Solutions for the Pythagoras equation

$$a = 1, \quad b = 2 \quad \rightarrow \quad c = \sqrt{5} = 2.23607\ldots$$

Special solution $a = 3, \quad b = 4 \quad \rightarrow \quad c = ?\,5$

Integer solution

Fermat's Last Theorem

Pierre de Fermat

- French, 1607/8–1665
- number theory, analysis, esp. functional analysis
- amateur mathematician (?) Hardly any proofs by him – or maybe hardly any left?

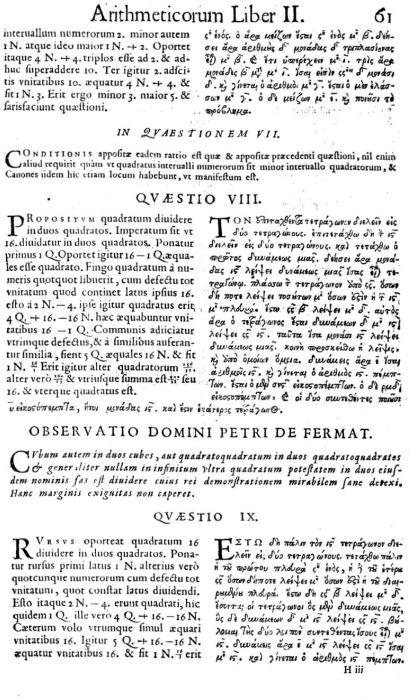
Source: Wikipedia

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.

AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V. C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adsciti vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 2. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVAESTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones idem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$. Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

ὁ εἰκοσιπεντέλτα, ἴσου μοναδὶ ις̄. καὶ ἔσται ἑτέρας πεζάγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadrates & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sanè detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oportet quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{32}{5}$ erit

H iii

Diophantine - Arithmetic

Source: Wikipedia

DIOPHANTINE EQUATIONS

- integer coefficients
- multiple variables
- multi-dimensional equations

linear equation

$$ax + by = c \quad \text{for } a, b, c \text{ integers } (\in \mathbb{Z})$$

a, b, c requirements? – c is divisor of a and b GCD

Pythagoras' Theorem

quadratic equation

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

Solvable as Diophantine equations: $(3, 4, 5)$ etc

cubic equation

$$x^3 + y^3 = z^3$$

???

n-ary equation

$$x^n + y^n = z^n$$

???

Fermat's Conjecture

In 1637, Fermat wrote in the margin of *Diophantine analysis*

> Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

> It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.

Fermat's Conjecture

Which means ...

Conjecture

If $n > 2$, then $x^n + y^n = z^n$ does not have integer solutions.

In 1995, Andrew Wiles finally gave a proof of this conjecture.

History of the Fermat Conjecture

$$x^n + y^n = z^n$$

For a proof, it suffices to consider prime n.

- $n = 4$: Fermat
- $n = 3$: Euler (1770)
- $n = 5$: Legendre, Dirichlet (~1825)
- $n = 7$: Lamé (1839)
- till 1993, all primes $< \sim 4.000.000$
- ...Wiles

Wiles' proof

- 1955: Taniyama-Shimura-Weil conjecture
- 1984: relation to ellliptic curves
- 1986: Ken Ribet, epsilon conjecture
- Wiles worked alone since 1986 in search for a proof
- June 1993: 3-day lecture at the Issac Newton Institute for Mathematical Sciences
- August 1993: various errors and holes found in the proof
- 1993–1995: Wiles and Richard Taylor are fixing the proof
- May 1995: publication in the Annals of Mathematics

Since Fermat 358 years have passed ...

Influence on today's life

Encryption

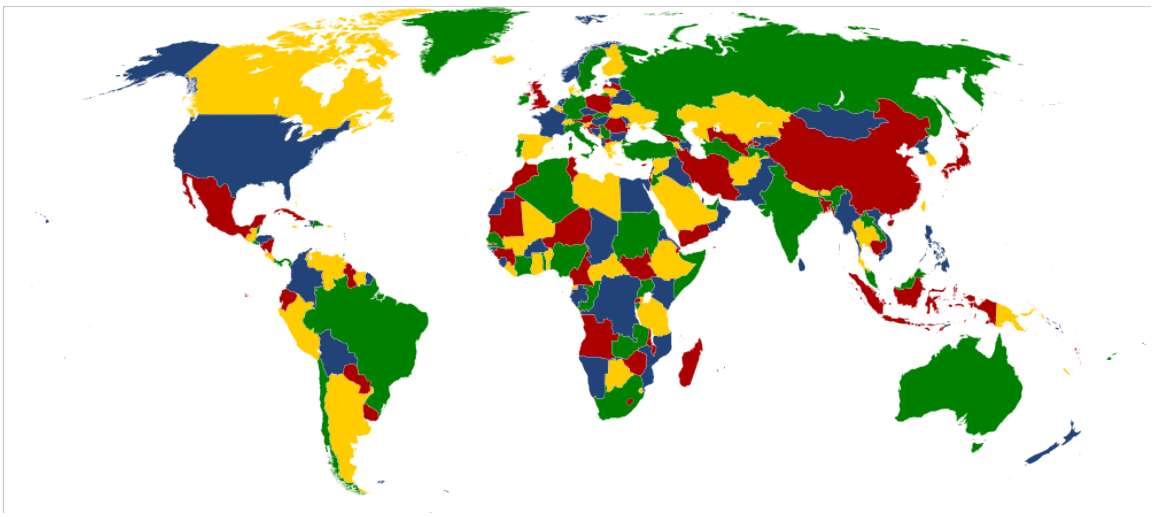
- elliptic curve cryptography
- ECDSA – elliptic curve digital signature algorithm
- Dual EC DRBG Dual Elliptic Curve Deterministic Random Bit Generator
- prime factorization

Fermat and Wiles

Source: Wikipedia

2nd Example

Four Color Theorem



To color every flat map in a way that adjacent countries have different colors, 4 colors are enough.

History of the Four Color Theorem

- 1840: Möbius conjectured the theorem
- 1890: Heawood – Five Color Theorem
- 1870-1890: Many incorrect proofs
- 1976: Appel and Haken – proof using computers

This was the first time computers were used to prove a mathematical theorem!

Proof method

Step 1

Divide all maps into a finite number of classes (at first 1936!)

traditional mathematics

Step 2

Show that if one can color one representative of a class, then all members of the class are 4-colorable.

traditional mathematics

Step 3

pick from each class one map, and try to color it

computer program

The aftermath of the proof

- various problems surfaced, in 1989 a fixed proof was published
- 1996: much faster algorith
- number of classes were considerable reduced
- 2005: proof verification with Coq (proof assistant system)
- still mathematicians are not content!

Influence on today's life

Development of proof assistant systems

Verification of proofs (and programs)

3rd Example

Gödel's Incompleteness Theorem

David Hilbert

- 1862–1943
- German mathematician
- Hilbert's 23 problems
- 1920: Hilbert Program
  Hilbert proposed to ground all existing theories to a finite, complete set of axioms, and provide a proof that these axioms were consistent.

Kurt Gödel

- 1906–1978
- Austrian-Hungarian Monarchy
- listened to Hilbert's lecture
  question of completeness
  of first-order logic
- 1930: Completeness of First Order Logic (age 24)
- 1931: Incompleteness Theorem (age 25)
- 1939-40: Russia – Japan – USA Princeton

Idea of the Incompleteness Theorem

> The sentence in the frame on this slide is wrong

A bit more formal

- Let G be a sentence of first order logic
- Let the meaning of G be "G is not correct"
- Can we prove or disprove G?
- If we could prove G, then G is correct, ...
- if G is correct, then
  "G is not correct" is correct
- this is a contradiction, so we cannot prove G

Consequences of the Incompleteness Theorem

- Halting problem
- End of Hilbert's Program
  automatization of proofs / truth is not possible
- paraconsistent logics
- various independence results
- mathematicians and logicians are still necessary!

Round up

- Mathematics is still alive!
- The 20^{th} century is often called ‘century of mathematics’
- Even simple questions can lead to very deep results
- Influence is strong
- It’s fun!

Next lecture

High school and university math – from computation to proof

Homework

The word ‘proof’ carries many meanings.

cultural, society, legal, sciences other than mathematics