Sets, relations and functions

Huan Long
Shanghai Jiao Tong University

- Basic set theory
- Relation
- Function

Brief History of Set Theory

- Georg Cantor(1845-1918)
  - German mathematician
  - Founder of set theory

- Bertrand Russell(1872-1970)
  - British philosopher, logician, mathematician, historian, and social critic.

- Ernst Zermelo(1871-1953)
  - German mathematician, foundations of mathematics and hence on philosophy

- David Hilbert (1862-1943)
  - German mathematician, one of the most influential and universal mathematicians of the 19th and early 20th centuries.

- Kurt Gödel(1906-1978)
  - Austrian American logician, mathematician, and philosopher. ZFC not $\vdash \neg$CH .

- Paul Cohen(1934-2007)
  - American mathematician, 1963: ZFC not $\vdash$ CH,AC .

Problem	Brief explanation	Status
1st	The continuum hypothesis (that is, there is no set whose cardinality is strictly between that of the integers and that of the real numbers)	Proven to be impossible to prove or disprove within Zermelo–Fraenkel set theory with or without the Axiom of Choice (provided Zermelo–Fraenkel set theory is consistent, i.e., it does not contain a contradiction). There is no consensus on whether this is a solution to the problem.
2nd	Prove that the axioms of arithmetic are consistent.	There is no consensus on whether results of Gödel and Gentzen give a solution to the problem as stated by Hilbert. Gödel's second incompleteness theorem, proved in 1931, shows that no proof of its consistency can be carried out within arithmetic itself. Gentzen proved in 1936 that the consistency of arithmetic follows from the well-foundedness of the ordinal ε_0.
3rd	Given any two polyhedra of equal volume, is it always possible to cut the first into finitely many polyhedral pieces that can be reassembled to yield the second?	Resolved. Result: no, proved using Dehn invariants.
4th	Construct all metrics where lines are geodesics.	Too vague to be stated resolved or not.[n 2]
5th	Are continuous groups automatically differential groups?	Resolved by Andrew Gleason, depending on how the original statement is interpreted. If, however, it is understood as an equivalent of the Hilbert–Smith conjecture, it is still unsolved.
6th	Mathematical treatment of the axioms of physics	Partially resolved depending on how the original statement is interpreted.[13] In particular, in a further explanation Hilbert proposed two specific problems: (i) axiomatic treatment of probability with limit theorems for foundation of statistical physics and (ii) the rigorous theory of limiting processes "which lead from the atomistic view to the laws of motion of continua." Kolmogorov's axiomatics (1933) is now accepted as standard. There is some success on the way from the "atomistic view to the laws of motion of continua."[14]
7th	Is a^b transcendental, for algebraic $a \neq 0,1$ and irrational algebraic b ?	Resolved. Result: yes, illustrated by Gelfond's theorem or the Gelfond–Schneider theorem.
8th	The Riemann hypothesis ("the real part of any non-trivial zero of the Riemann zeta function is ½") and other prime number problems, among them Goldbach's conjecture and the twin prime conjecture	Unresolved.
9th	Find the most general law of the reciprocity theorem in any algebraic number field.	Partially resolved.[n 3]
10th	Find an algorithm to determine whether a given polynomial Diophantine equation with integer coefficients has an integer solution.	Resolved. Result: impossible, Matiyasevich's theorem implies that there is no such algorithm.
11th	Solving quadratic forms with algebraic numerical coefficients.	Partially resolved.[15]
12th	Extend the Kronecker–Weber theorem on abelian extensions of the rational numbers to any base number field.	Unresolved.
13th	Solve 7-th degree equation using algebraic (variant: continuous) functions of two parameters.	The problem was partially solved by Vladimir Arnold based on work by Andrei Kolmogorov.[n 4]
14th	Is the ring of invariants of an algebraic group acting on a polynomial ring always finitely generated?	Resolved. Result: no, a counterexample was constructed by Masayoshi Nagata.
15th	Rigorous foundation of Schubert's enumerative calculus.	Partially resolved.
16th	Describe relative positions of ovals originating from a real algebraic curve and as limit cycles of a polynomial vector field on the plane.	Unresolved, even for algebraic curves of degree 8.
17th	Express a nonnegative rational function as quotient of sums of squares.	Resolved. Result: yes, due to Emil Artin. Moreover, an upper limit was established for the number of square terms necessary.
18th	(a) Is there a polyhedron that admits only an anisohedral tiling in three dimensions? (b) What is the densest sphere packing?	(a) Resolved. Result: yes (by Karl Reinhardt). (b) Widely believed to be resolved, by computer-assisted proof (by Thomas Callister Hales). Result: Highest density achieved by close packings, each with density approximately 74%, such as face-centered cubic close packing and hexagonal close packing.[n 5]
19th	Are the solutions of regular problems in the calculus of variations always necessarily analytic?	Resolved. Result: yes, proven by Ennio de Giorgi and, independently and using different methods, by John Forbes Nash.
20th	Do all variational problems with certain boundary conditions have solutions?	Resolved. A significant topic of research throughout the 20th century, culminating in solutions for the non-linear case.
21st	Proof of the existence of linear differential equations having a prescribed monodromic group	Partially resolved. Result: Yes, no, open depending on more exact formulations of the problem.
22nd	Uniformization of analytic relations by means of automorphic functions	Resolved.
23rd	Further development of the calculus of variations	Too vague to be stated resolved or not.

What is a *set* ?

- By *Georg Cantor* in 1870s:

  *A **set** is an unordered collection of objects.*

  - The objects are called the *elements*, or *members*, of the set. A set is said to *contain* its elements.

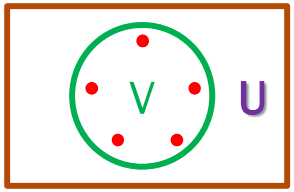
- Notation: $a \in A$
  - Meaning that: a is an element of the set A, or,

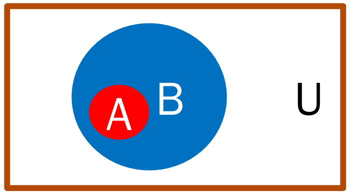
  Set A contains a .

- Important:
  - Duplicates do not matter.
  - Order does not matter.

Basic notions

- $a \in A$ a is an element of the set A.
- $a \notin A$ a is NOT an element of the set A.
- **Set of sets** {{a,b},{1, 5.2}, k}
- $\emptyset$ the empty set, or the null set, is set that has no elements.
- $A \subseteq B$ subset relation. Each element of A is also an element of B.
- $A = B$ equal relation. $A \subseteq B$ and $B \subseteq A$.
- $A \neq B$
- $A \subset B$ strict subset relation. If $A \subseteq B$ and $A \neq B$
- $|A|$ cardinality of a set, or the number of distinct elements.
- **Venn Diagram**





Examples

- $a \in \{a, e\ i, o, u\}$
- a ∉{{a}}
- Ø ∉Ø
- Ø ∈ {Ø} ∈ {{Ø}}
- {3,4,5}={5,4,3,4}
- Ø⊆S
- Ø ⊂{Ø }
- S ⊆S
- |{3, 3, 4, {2, 3},{1,2,{f}} }|=4

Set Operations

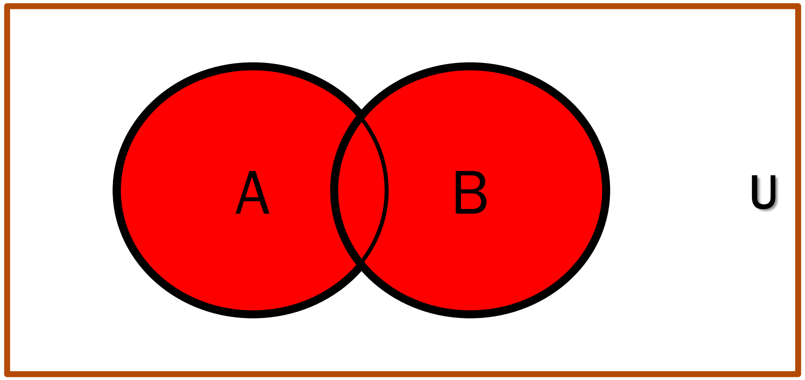
- Union
- Intersection
- Difference
- Complement
- Symmetric difference
- Power set

Union

- **Definition** Let A and B be sets. The union of the sets A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A or in B, or both.

$$A \cup B=\{x \mid x \in A \text{ or } x \in B\}$$

- Example: $\{1,3,5\} \cup \{1,2,3\}=\{1,2,3,5\}$
- Venn Diagram representation

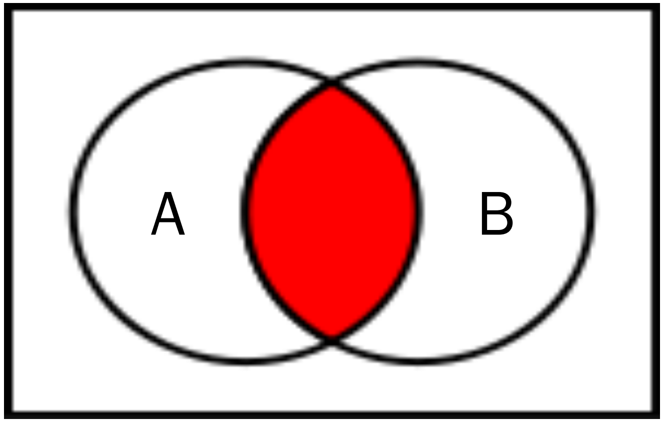


Intersection

- **Definition** Let A and B be sets. The intersection of the sets A and B, denoted by $A \cap B$, is the set that containing those elements in both A and B.

$$A \cap B=\{x \mid x \in A \text{ and } x \in B\}$$

- Example: $\{1,3,5\} \cap \{1,2,3\}=\{1,3\}$
- Venn Diagram Representation

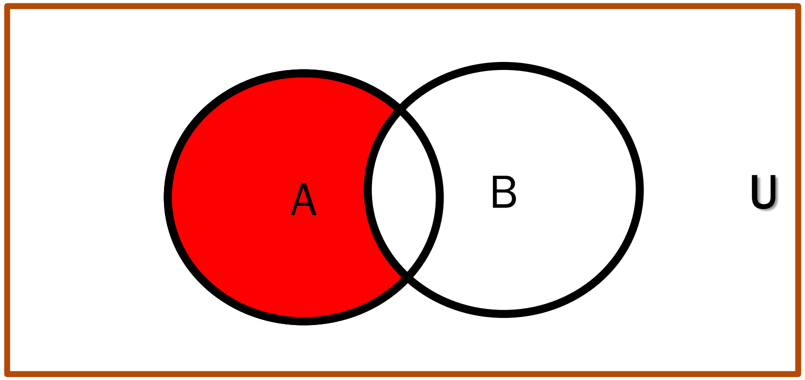


Difference

- **Definition** Let A and B be sets. The difference of the sets A and B, denoted by A - B, is the set that containing those elements in A but not in B.

$$A - B = \{x |\ x \in A\ but\ x \notin B\} = A \cap \bar{B}$$

- Example: {1,3,5}-{1,2,3}={5}
- Venn Diagram Representation

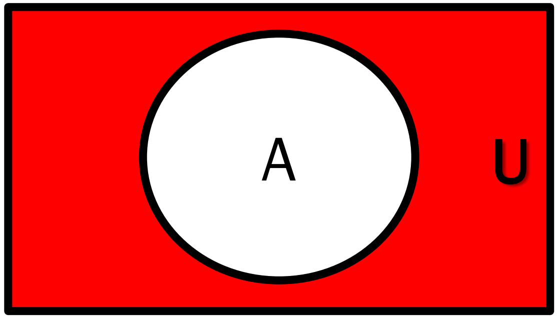


Complement

- **Definition** Let U be the universal set. The complement of the sets A, denoted by $\bar{A}$ or $-A$, is the complement of with respect to U.

$$\bar{A} = \{x \mid x \notin A\} = U - A$$

- Example: -E = O
- Venn Diagram Representation



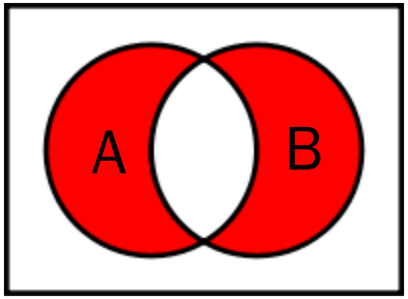
Symmetric difference

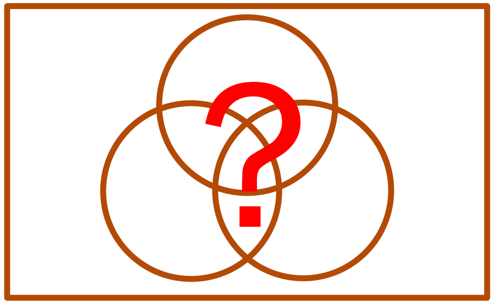
- **Definition** Let A and B be sets. The symmetric difference of A and B, denoted by $A \oplus B$, is the set containing those elements in either A or B, but not in their intersection.

$$A \oplus B=\{x \mid (x \in A \vee x \in B) \wedge x \notin A \cap B\}$$

$$=(A-B) \cup (B-A)$$

- Venn Diagram: $A \oplus B$ $\qquad\qquad$ $A \oplus B \oplus c$





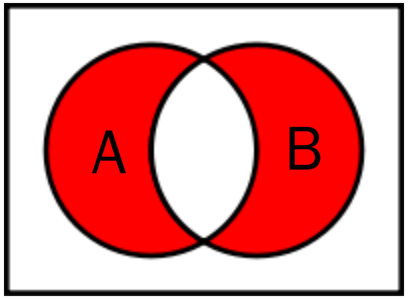
Symmetric difference

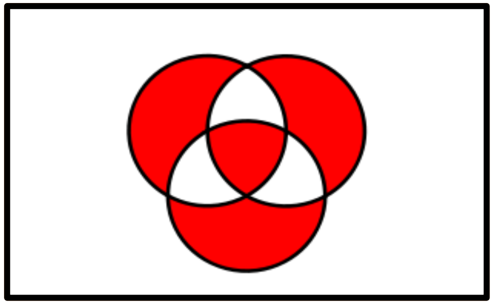
- **Definition** Let A and B be sets. The symmetric difference of A and B, denoted by $A \oplus B$, is the set containing those elements in either A or B, but not in their intersection.

$$A \oplus B=\{x \mid (x \in A \vee x \in B) \wedge x \notin A \cap B\}$$

$$=(A-B) \cup (B-A)$$

- Venn Diagram: $A \oplus B$ $\quad$ $A \oplus B \oplus c$





The Power Set

- Many problems involves testing all combinations of elements of a set to see if they satisfy some property. To consider all such combinations of elements of a set S, we build a new set that has its members all the subsets of S.
- Definition: Given a set S, the power set of S is the set of all subsets of the set S. The power set of S is denoted by P(S) or $\wp S$.
- Example:
  - $P(\{0,1,2\})=\{\phi, \{0\},\{1\},\{2\}, \{0,1\},\{0,2\},\{1,2\},\{0,1,2\} \}$
  - $P(\emptyset)=\{\emptyset\}$
  - $P(\{\emptyset\})=\{\emptyset,\{\emptyset\}\}$

Set Identities

1. Identity laws

$$A \cup \emptyset = A \qquad A \cap U = A$$

2. Domination laws

$$A \cup U = U \qquad A \cap \emptyset = \emptyset$$

3. Idempotent laws

$$A \cup A = A \qquad A \cap A = A$$

Set Identities (Cont.)

4. Complementation law

$$\overline{(\overline{A})} = A$$

5. Commutative laws

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

6. Associative laws

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

Set Identities (Cont.)

7. Distributive laws

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

8. De Morgan's laws

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Set Identities (Cont.)

9. Absorption laws

$$A \cup (A \cap B) = A$$

$$A \cap (A \cup B) = A$$

10. Complement laws

$$A \cup \bar{A} = U$$

$$A \cap \overline{A} = \emptyset$$

Example

Theorem 1 (De Morgan's Law). $\overline{S \cap T} = \bar{S} \cup \bar{T}$ *or* $S \cap T = \overline{\bar{S} \cup \bar{T}}$

Proof. (Proved by Venn Diagram)

$$\begin{aligned} x \in \overline{S \cap T} &\Rightarrow x \notin S \cap T \\ &\Rightarrow \text{ either } x \notin S \text{ or } x \notin T \\ &\Rightarrow \text{ either } x \in \bar{S} \text{ or } x \in \bar{T} \\ &\Rightarrow x \in \bar{S} \cup \bar{T} \\ x \in \bar{S} \cup \bar{T} &\Rightarrow \text{ reverse steps} \end{aligned}$$

Basic set theory

Relation

Function

Ordered Pairs

- In set theory {1,2}={2,1}
- What if we need the object <1,2> that will encode more information:
  - 1 is the first component
  - 2 is the second component
- Generally, we say

$$<x, y> =<u, v> \quad \text{iff} \quad x=u \wedge y=v$$

Cartesian Product

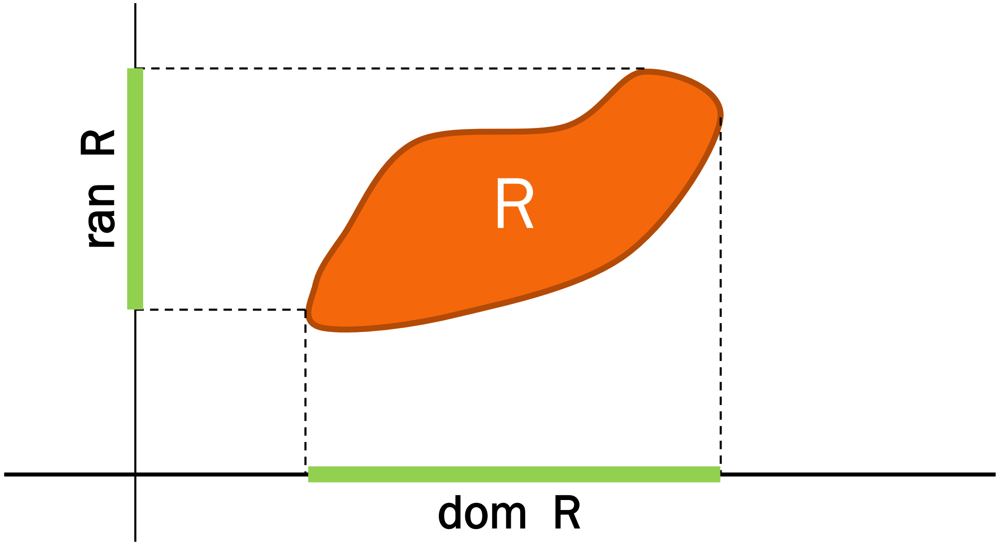
- $A \times B = \{<x,y> \mid x \in A \wedge y \in B\}$ is the Cartesian product of set A and set B.
- Example

  $A=\{1,2\}$ $B=\{a,b,c\}$

  $A \times B = \{<1,a>,<1,b>,<1,c>,$
  $<2,a>,<2,b>,<2,c>\}$

Relation

- **Definition** A **relation** is a set of ordered pairs.
- **Examples**
  - $<=\{<x,y>\in R\times R \mid x \text{ is less than } y\}$
  - $M=\{<x,y>\in People\times People \mid x \text{ is married to } y\}$



A relation as a subset of the plane

More about the binary relation

Let R denote any binary relation on a set x, we say:

- R is reflexive, if $(\forall a \in x)(aRa)$;
- R is symmetric, if $(\forall a, b \in x)(aRb \rightarrow bRa)$;
- R is transitive , if $(\forall a, b, c \in x)[(aRb \wedge bRc) \rightarrow (aRc)]$;

Equivalence relation

- **Definition** R is an **equivalence relation** on A iff R is a binary relation on A that is
  - Reflexive
  - Symmetric
  - Transitive

Partition

- **Definition** A ***partition*** π of a set A is a set of nonempty subsets of A that is disjoint and exhaustive. i.e.
  (a) no two different sets in π have any common elements, and
  (b) each element of A is in some set in π.

Equivalence class

- If R is an equivalence relation on A, then the quotient set (equivalence class) A/R is defined as

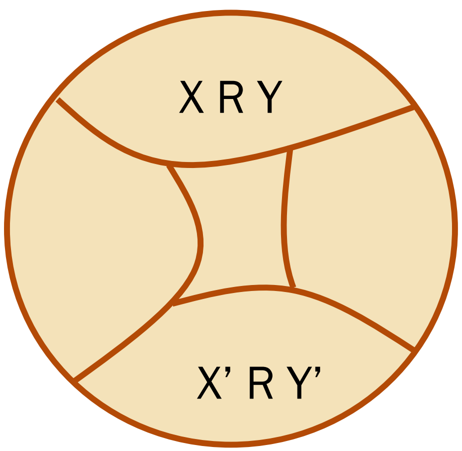
$$A/R=\{ [x]_R \mid \in A \}$$

Where A/R is read as “A modulo R”

- The ***natural map*** (or canonical map) $\alpha:A\to A/R$ **defined by**

$$\alpha(x)= [x]_R$$

- **Theorem** Assume that R is an equivalence relation on A. Then the set $\{[x]_R \mid x \in A\}$ of all equivalence classes is a partition of A.



Examples

- Let $\omega = \{0,1,2,\ldots\}$; and $m \sim n \Leftrightarrow m - n$ is divisible by 6.

  Then $\sim$ is an equivalence relation on ω. The quotient set $\omega/\sim$ has six members:

  $[0] = \{0,6,12,\ldots\}$,

  $[1] = \{1,7,13,\ldots\}$,

  ……

  $[5] = \{5,11,17,\ldots\}$

- Clique (with self-circles on each node) : a graph in which every edge is presented. Take the existence of edge as a relation. Then the equivalence class decided by such relation over the graph would be clique.

Ordering relations

- Linear order/total order
  - transitive
  - trichotomy
- Partial order
  - reflexive
  - anti-symmetric
  - transitive
- Well order
  - total order
  - every non-empty subset of S has a least element in this ordering.

- Basic set theory
- Relation
- Function

Function

- **Definition** A **function** is a relation F such that for each x in *dom* F there is only one y such that $x\,F\,y$. And y is called the value of F at x.
- **Notation** $F(x)=y$
- **Example** $f(x) = x^2$ $f : R \to R$, $f(2) = 4$, $f(3) = 9$, etc.
- **Composition** $(f \circ g)(x)=f(g(x))$
- **Inverse** The inverse of $\boldsymbol{F}$ is the set

  $$F^{-1}=\{<u,v> \mid v\,\boldsymbol{F}\,u\}$$

  F^{-1} is not necessarily a function (why?)

Special functions

- We say that *F is a function from A into B* or that *F maps A into B* (written $F: A \to B$) iff F is a function, *dom* $F=A$ and *ran* $F \subseteq B$.
  - If, in addition, *ran* $F=B$, then F is a function from A ***onto*** B. F is also named a ***surjective function***.
  - If, in addition, for any $x \in dom\ F$, $y \in dom\ F$, with $x \neq y$, $F(x) \neq F(y)$, then F is an ***injective function***. or ***one–to-one*** (or ***single-rooted***).
  - F is ***bijective function*** : f is surjective and injective.

References

- Main References
  - Herbert B. Enderton, *Elements of Set Theory*, ACADEMIC PRESS, 1977
  - Yiannis Moschovakis, *Notes on Set Theory (Second Edition)*, Springer, 2005
  - Keith Devlin, *The Joy of Sets: Fundamentals of Contemporary Set Theory*, Springer-Verlag, 1993
  - Kenneth H. Rosen, *Discrete Mathematics and Its Applications (Sixth Edition)*, 2007
  - 沈恩绍，*集论与逻辑*，科学出版社，（集合论部分），2001

Thank you

Hilbert's twenty-three problems are:

Problem	Brief explanation
1st	The continuum hypothesis (that is, there is no set whose cardinality is strictly between that of the integers and that of the real numbers)
2nd	Prove that the axioms of arithmetic are consistent.
3rd	Given any two polyhedra of equal volume, is it always possible to cut the first into finitely many polyhedral pieces which can be reassembled to yield the second?
4th	Construct all metrics where lines are geodesics.
5th	Are continuous groups automatically differential groups?
6th	Mathematical treatment of the axioms of physics
7th	Is a^b transcendental, for algebraic $a \neq 0,1$ and irrational algebraic b ?
8th	The Riemann hypothesis ("the real part of any non-trivial zero of the Riemann zeta function is ½") and other prime number problems, among them Goldbach's conjecture and the twin prime conjecture
9th	Find the most general law of the reciprocity theorem in any algebraic number field.
10th	Find an algorithm to determine whether a given polynomial Diophantine equation with integer coefficients has an integer solution.
11th	Solving quadratic forms with algebraic numerical coefficients.
12th	Extend the Kronecker–Weber theorem on abelian extensions of the rational numbers to any base number field.
13th	Solve 7-th degree equation using continuous functions of two parameters.
14th	Is the ring of invariants of an algebraic group acting on a polynomial ring always finitely generated?
15th	Rigorous foundation of Schubert's enumerative calculus.
16th	Describe relative positions of ovals originating from a real algebraic curve and as limit cycles of a polynomial vector field on the plane.
17th	Express a nonnegative rational function as quotient of sums of squares.
18th	(a) Is there a polyhedron which admits only an anisohedral tiling in three dimensions? (b) What is the densest sphere packing?
19th	Are the solutions of regular problems in the calculus of variations always necessarily analytic?
20th	Do all variational problems with certain boundary conditions have solutions?
21st	Proof of the existence of linear differential equations having a prescribed monodromic group
22nd	Uniformization of analytic relations by means of automorphic functions
23rd	Further development of the calculus of variations

Sp