History

Before Greeks (Euclid, Pythagoras): Knew $a^2 + b^2 = c^2$ for right triangles, but without proof. Believed π is rational!

Euclid: Took five intuitively obvious statements as axioms (postulates) of Geometry; proved everything else from it.

For many years people tried to prove the fifth postulate from the first four, w/o success.

Recently (20th century?): proved fifth postulate independent of first four; i.e., can neither prove or disprove it; how? Found model for first four + negation of fifth − called Noneuclidean Geometry (spherical, hyperbolic). Hilbert found gaps in Euclid, but fixed everything, and made it completely rigorous (points, lines undefined terms; can use cups and chairs instead).

Other branches of math became rigorous too. But paradoxes existed.

Example 1. Some sets can be elements of themselves: S = set of all sets with $\geq$ two elements. Q: $|S| > 2$? Yes. Q: $S \in S$? According to def of S, yes.

Russell's paradox: Let T = set of all sets R s.t. $R \notin R$.

Q: $T \in T$? Ans: Y and N both give contradiction!

So early 20th century: lots of work establishing precise and rigorous foundations for all of mathematics: Axiomatic Systems for every branch of math.

Why axioms? **1**. Must accept somethings w/o pf − can't expect to prove everything. **2**. Need precise def of what is a pf. **3**. Need to be able to check validity of any given pf; i.e., must have algorithm for checking correctness of proofs.

Axioms for Arithmetic: PA–Peano Axioms.

Axioms for Set Theory: ZFC (Zermelo-Frankel Axioms, + axiom of Choice). All branches of mathematics could be expressed in language of set theory, L_{ST}.

People were optimistic that Axiomatic Systems were the perfect approach.

Hilbert's "dream": Prove mathematics is consistent. In particular, prove arithmetic is consistent. Also prove arithmetic is complete: every true statement can be proved in PA.

Gödel's Theorems: Good news and bad news

Good news:

Theorem 1. (Completeness Theorem = Soundness + Adequacy) $\Gamma \vdash A$ iff $\Gamma \models A$.

Bad news:

Theorem 2. If PA axioms are consistent, then there are true statements in arithmetic that cannot be proved from PA. Furthermore, for any decidable set of axioms containing PA, the same conclusion holds.

Idea: This sentence is not provable.

Theorem 3. PA axioms cannot be proven (within PA) to be consistent.

Q: What do the above thms imply about models of PA? Ans: That the standard model is not the only model!

Example 2. A nonstandard model of arithmetic.

Domain: $D = \{(a, b)|(a \in \mathbb{N} \wedge b = 0) \vee (a \in \mathbb{Z} \wedge b \in \mathbb{Q} \wedge b > 0)\}$.

0: $(0, 0)$.

S: $S(a, b) = (a + 1, b)$.

$<$: $(a, b) < (c, d)$ iff $b < d$ or $b = d \wedge a < c$.

$+$: $(a, b) + (c, d) = (a + b, c + d)$.

$\times$: $(a, b) \times (c, d) = (ab, ac + bd)$.

Remark. It's not just that PA axioms are not well-chosen – they *are* well-chosen:

Theorem 4. (Löwenheim-Skolem) Any set of first order axioms that has an infinite model has both countable and uncountable models.

So models are never unique: whatever interpretation we're trying to "capture" with axioms, will always have "nonstandard" models.

Example 3. Continuum Hypothesis (CH): $\forall S \subset \mathbb{R}$ s.t. $|S| = |\mathbb{N}| \vee |S| = |\mathbb{R}|$.

Obviously either CH or ($\neg$ CH) is true in $\mathbb{R}$. But:

Gödel(1938): CH is consistent with ZFC.

Cohen (1963): ($\neg$ CH) is consistent with ZFC.
