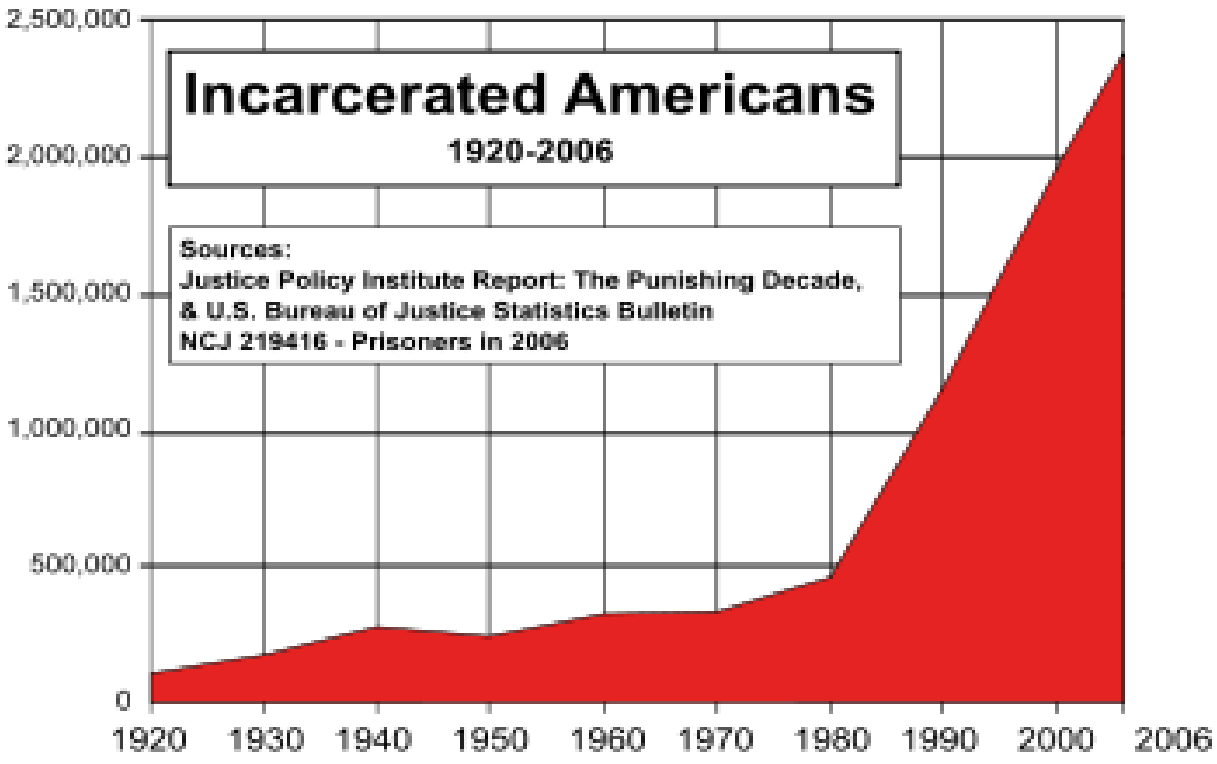
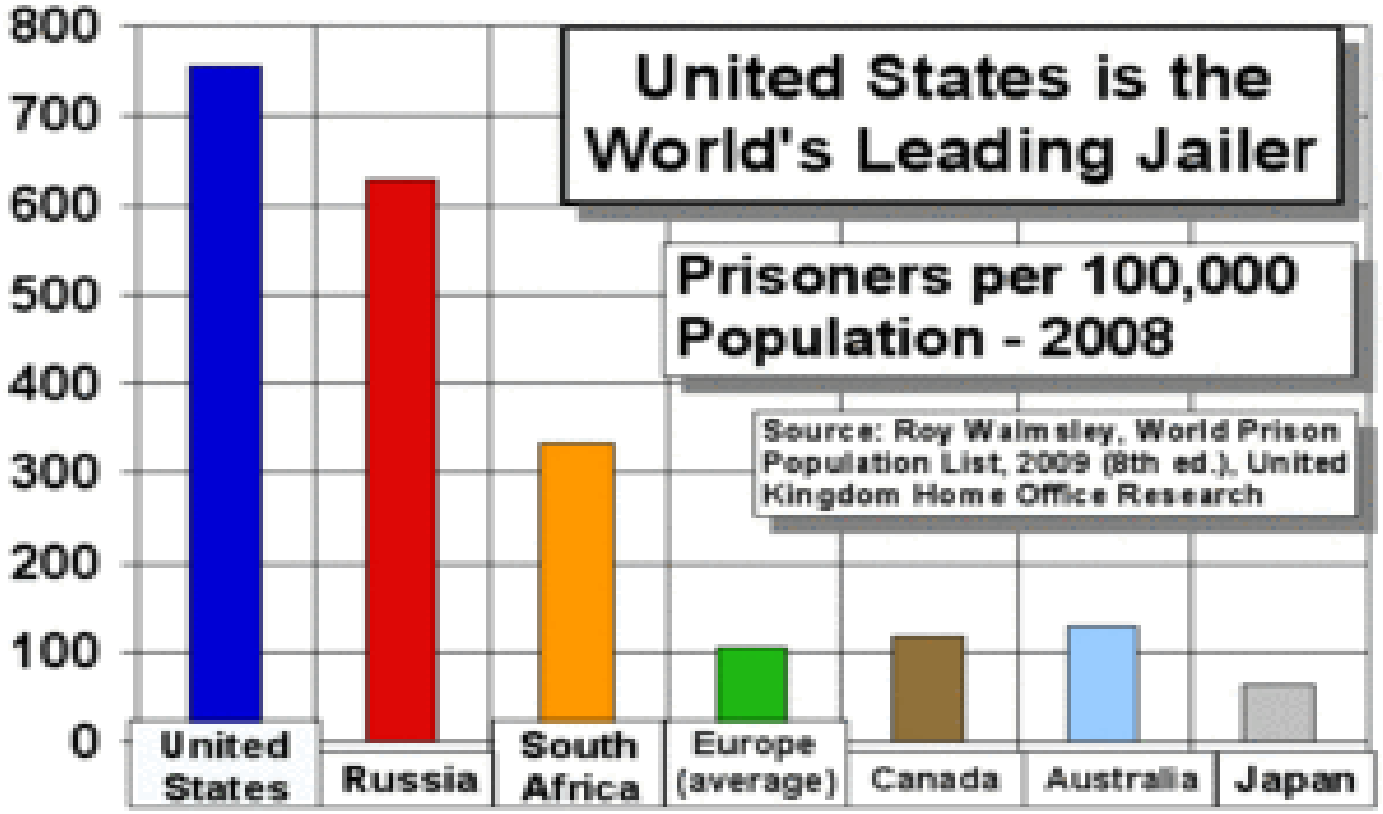

Incarcerated Americans
1920-2006
Sources:
Justice Policy Institute Report: The Punishing Decade,
& U.S. Bureau of Justice Statistics Bulletin
NCJ 219416 - Prisoners in 2006
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
1920
1930
1940
1950
1960
1970
1980
1990
2000
2006


United States is the World's Leading Jailer
Prisoners per 100,000 Population - 2008
Source: Roy Walmsley, World Prison Population List, 2009 (8th ed.), United Kingdom Home Office Research
800
700
600
500
400
300
200
100
0
United States
Russia
South Africa
Europe (average)
Canada
Australia
Japan

- Rudolf Schlesinger: If you are innocent, you want to be tried in Europe; if you are guilty, you want to be tried in the United States.

Topics

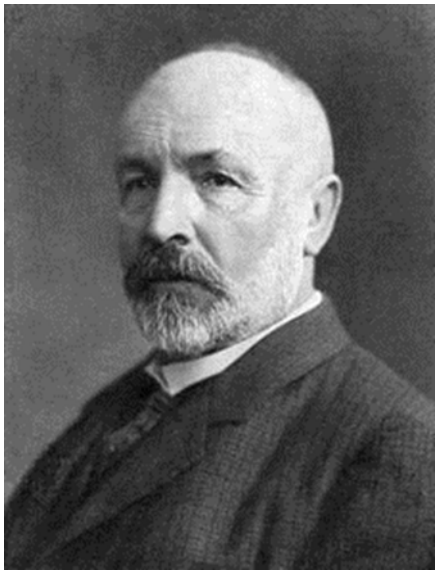
- Proof ‘in the field’: arrest and probable cause. *Scott v. Harris*.
- Plea bargaining and torture.
- Trial by mathematics?
- Jury trial; origins and purposes of the jury; eyewitness testimony; detection of truthfulness.

- History: Origins of the idea of ‘beyond a reasonable doubt’.
- Comparison: How other countries do it. Is there a problem with the common law method?

Proof: from Cantor to Gödel

- Homework assignment (due in class next Thursday, Oct. 18):
  - Write out a clear exposition of the following argument, filling in the gaps as indicated.

Cantor and Dedekind



Stage 1

- November 29, 1873. Cantor writes to Dedekind with a puzzle that he can't answer: Is it possible to correlate the positive real numbers one-to-one with the positive integers? You might (he says) think the answer is obviously no, because the reals form a continuum. But so do the rationals, and it is easy to see that they can be enumerated.

Enumeration of the Rationals

- We have seen the proof (please write out a sketch): zig-zag through the (positive) lattice points of the plane.

Dedekind's Answer (by December 2)

- He can't answer the question; however: the question has no practical interest; so it does not deserve much effort.

- Cantor agrees – but still, it would be 'nice' to have a proof that the reals cannot be enumerated, since that would give a new proof of the existence of transcendental numbers.

Stage 2

- 7 December, 1873: Cantor proves that the reals cannot be enumerated; a simplified proof follows on 9 December. Dedekind congratulates him, and also sends a simplified proof (which crosses in the mail). Cantor's proof is submitted for publication later that month.

The Diagonal Argument
[NOT Cantor's original proof]

- Homework (extra credit): Write out Cantor's original proof.

(You will need the following fact about the reals: Every bounded infinite sequence of real numbers has a limit point.)

Cantor's argument: Assume we have an enumeration $(a_1, a_2, \ldots)$ of the reals in (0,1).

Then in any given sub-interval (α, β) there exists a real number η not in the enumeration.

Sketch of Cantor's Proof

- Let α' and β' be the first two numbers in the enumeration to appear in (α, β); without loss of generality, let $\alpha' < \beta'$. Let α'' and β'' be the next two numbers in the enumeration to appear in (α', β'); repeat. If the process terminates, we are left with an entire interval in which no number in the enumeration appears, and we are done. If the process does not terminate, we have a bounded increasing sequence $(\alpha', \alpha'', \alpha''', \ldots)$ and a bounded decreasing sequence $(\ldots, \beta''', \beta'', \beta')$. Now consider the limit points, and complete the proof.

Stage 3: What to make of this?

- C's proof gives us two kinds of infinites – some are as 'big' as the integers; others [give examples] are as 'big' as the reals.
- Question 1: Is there anything in between?
  - Conjecture: No. ("Continuum hypothesis" – Hilbert's first problem, and extremely hard.)
- Question 2: Is there anything bigger than the reals?
  - Conjecture: there are more points in the real plane than on the real line.

- Cantor thinks about this question for nearly four years until he writes again to Dedekind (20 June, 1877).
- He produces essentially the argument we saw in class. To the point (x,y) where

  x = .abcde…

  y = .pqrst…

correlate the point z:

z = .apbqcrdset …

- Dedekind's reply: the proof contains a gap, since the decimal representation of the reals is not unique. (We saw this in class:

  .3500000… = .349999999…).

Homework (easy): show by an example why Dedekind is correct, i.e. that Cantor's correlation is not one-to-one.

Homework (a bit harder): repair Cantor's argument.

- Cantor is quite perplexed by his discovery. '*Je le vois, mais je ne le crois pas*.'
- Cantor's proofs are highly complicated. For example (extra-credit homework): try to show that the cardinality of (0,1) = the cardinality of [0,1) (i.e. that there exists a bijection between the two sets).

[NB: by definition, two sets have the same cardinality if there is a bijection – i.e. a map that is one-to-one and onto – between them.]

Stage 4.

- Problem: Is it possible to get sets that are 'larger' than the cardinality of the real numbers? (So far we have not managed to do so: Cantor was stuck.)
- Can we *generalize* the diagonal argument? What about Cantor's proof using converging sequences? It is not obvious how: neither proof suggests a way forward.
- Maybe we should ask instead: How are the reals related to the integers?

- Theorem: the positive reals in (0,1) can be correlated one-to-one with the subsets (finite and infinite) of the positive integers.
  - [Fact: Any real number can be represented as an infinite binary decimal, .0010111001…, and every such binary decimal determines a real.]
- Homework: Show that every binary decimal determines a subset of the positive integers, and vice versa. (You can ignore the 'Dedekind objection' about unique representation.)

Stage 5.

- If the reals are all the subsets of the integers, and if the reals have greater cardinality than the integers, then can we generalize *that* fact?

  – Some notational jargon:
    - If X is a set, then P(X) (the 'power set') is the set of all subsets of X.
    - {x| f(x)} is notation for: 'the set of all x satisfying f(x)'

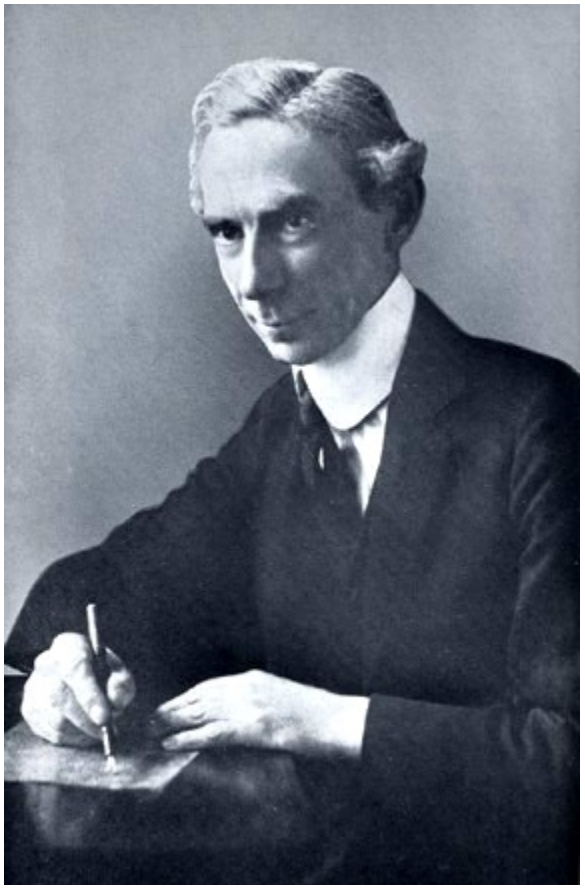
Cantor's Theorem

- Conjecture: For any set X, it is never possible to establish a bijection ϕ between the elements of X and the elements of P(X).
- Sketch of Proof. (Extremely important: Write out the details, and make sure you understand the argument!)
  - Experiment first with finite sets; you will quickly persuade yourself that the conjecture is correct. The difficulty is to prove it for arbitrary, infinite sets. Try to solve this yourself before looking at the hint at the end of these slides.

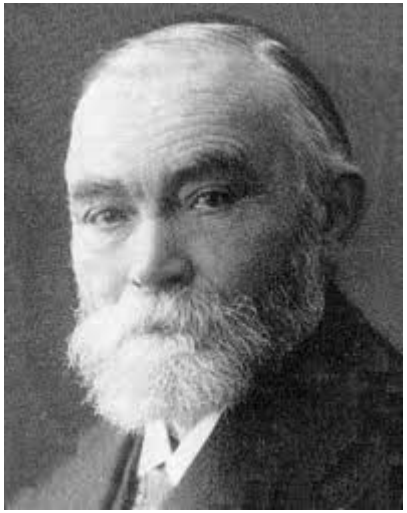
Stage 6. Two Big Problems.

- Cantor's Theorem gives us an infinite hierarchy of ever-larger infinite numbers. Does this even make sense? (Many mathematicians thought not – especially Kronecker, and also Poincaré.)
- How can we be sure that Cantor's theory is not self-contradictory?
- **Russell's Paradox** (which he got from Cantor's Theorem): Consider the set of all sets that do not belong to themselves.

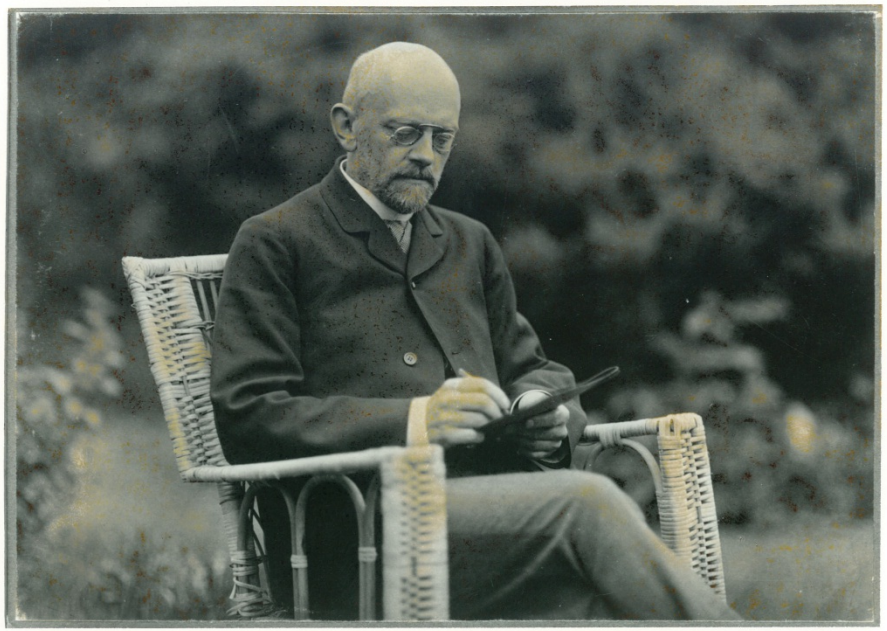
Bertrand Russell



Gottlob Frege



David Hilbert
(1862-1943)



Hilbert's Idea ("Proof Theory")

- Two (related) problems:
  - How do we defend Cantor's theory of the infinite, and show that it is free of contradiction?
  - How, in general, do we show that a mathematical proof contains no 'gaps'?

- Hilbert's Insight: Cantor talks about 'infinite sets' and 'infinite numbers' – but the *words* he uses are *finite* objects. So (inspired by Hilbert's work on axioms of geometry):
- Can we fully specify the *language* of infinite set-theory, write down its *axioms* and a set of (syntactic!) *inference rules*, and then, by studying this formal calculus, show:

  - That it suffices for higher mathematics ('completeness'); and,
  - That one can never derive the formula, 1=0 (i.e. that the formal system is syntactically consistent)?
- NB: the derivations in the system are purely mechanical, syntactic, a matter of manipulating symbols – we are not interested in their 'meaning.'

1920s and Proof Theory

- Controversy with Brouwer, Weyl; the 'Grundlagenstreit'
- Early successes in showing consistency of various simple sub-systems; by 1925 a proof of the consistency of analysis appears in reach. Main researchers:
  - David Hilbert
  - Paul Bernays
  - Wilhelm Ackermann
  - John von Neumann

Kurt Gödel

- 1931 – First Incompleteness Theorem.
- Suppose you have a syntactic machine M that is capable of answering truthfully any question of mathematics (i.e. consistency and completeness are satisfied).
- This machine is itself a mathematical object, and can be given a mathematical description.

Gödel's Idea:

- Ask the machine M to prove the following theorem:
  - 'Machine M will never be able to prove this sentence.'
- Now we have a dilemma. If M proves the sentence, then M has proved a falsehood (and we lose consistency). But if M cannot prove the sentence, then the sentence is true (and we lose completeness).

Two Consequences:
1. Early Computation

- Hilbert's Program (at least as originally formulated) cannot be carried through.
- Subtler forms of consistency proof (e.g. in the work of Gentzen) are still possible.
- There remains Hilbert's question about decidability (the *Entscheidungsproblem*): Given a set of axioms, can we decide whether a given formula is derivable?

Alan Turing and J. von Neumann

2. What about Proof?

- Two concepts of proof?
  - ‘gapless,’ fully-formalized proofs, executable by a digital computer;
  - ‘informal’ proofs and arguments, as given by mathematicians.

- What is the relationship between them?

Hint on Cantor's Theorem

Suppose we have such a ϕ. Then consider the set $Y = \{x \mid x \text{ is not a member of } \phi(x)\}$. Because ϕ is a bijection, for some z in X, we have $Y = \phi(z)$. Now ask: Is z a member of Y? QED.