

1. *Problem involving divisibility*
 - a. Students attacking this problem don't seem to realize that the greatest common divisor of two positive integers not only
 - i. divides them, and
 - ii. is the largest of their common divisors, but
 - iii. is actually *divisible* by each of their common divisors.
 - b. The chain of theorems in number theory that leads to that is roughly this.
 - i. First, elementary considerations lead to the existence of the greatest common divisor and properties (i) and (ii).
 - ii. Second, the Euclidean algorithm is developed, and shows that the greatest common divisor is the sum of integral multiples of the two numbers.
 - iii. Third, that property is used to show the uniqueness of prime factorization: the *fundamental theorem of arithmetic*.
 - iv. Fourth, unique factorization allows us to express the greatest common divisor in terms of the prime factorization of the numbers: it's the product of the same primes, each raised to the smaller of the corresponding powers.
 - v. This trivially implies property (iii).
 - c. Similar results, except for the Euclidean algorithm, hold for least common multiples.
 - d. In this course, you *are* expected to apply results from standard undergraduate courses.
2. I started responding to questions about the *Axiom of Choice* (AC) unit.
 - a. The AC was first recognized as a convenient method of proof around 1890. By about 1900 it was described as a principle of proof possibly independent of other commonly used principles: it either required proof itself, or should be explicitly stated as an assumption. But many doubted its validity.
 - b. Ernst Zermelo stated it explicitly in [1904] 1970 and used it to prove that every set S has a well-ordering: that is for each S there is a partial ordering relation with respect to which each nonempty subset of S has a minimum element.
 - c. In [1900] 2000 Hilbert proposed, as one of his famous problems, that of finding a well-ordering for the set of real numbers. Well-orderings are important in general because they permit an analog of the standard techniques of definition and proof by recursion, hence a powerful tool in analysis.
 - d. For decades, some mathematicians doubted the validity of the AC, some tried to prove it from other axioms, and some tried to refute it (prove its negation) from other axioms.
 - e. In 1938, Kurt Gödel showed that it could not be refuted from the axioms of Zermelo–Fraenkel set theory (ZF).

- i. Those axioms are expressible in a formal language that uses the Boolean connectives $\&$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$; variables; the equality sign $=$; quantifiers $\forall$, $\exists$ ranging over those variables; and parentheses as necessary.
- ii. Gödel invented a notion of *constructibility* of a set x . He considered relativizing the open sentences of the ZF language by changing all phrases $\forall x$ and $\exists x$ to phrases equivalent to $(\forall \text{ constructible } x)$ and $(\exists \text{ constructible } x)$. He showed that
 - (1) the relativizations of all ZF axioms are provable in ZF, and
 - (2) if a conclusion is derivable from some hypotheses under the ZF rules of proof, then the relativization of the conclusion is derivable from the relativizations of the hypotheses under those same rules, and
 - (3) the relativization R of the AC is provable in ZF.
- iii. It follows from (1) and (2) that the relativizations of all theorems of ZF are also theorems of ZF. In particular, if the negation $\neg \text{AC}$ were provable, so would be its relativization, which is just $\neg R$.
- iv. Thus, if ZF is consistent, then $\neg \text{AC}$ is not a theorem of ZF.
- f. The status of AC itself relative to ZF remained unsettled until on 4 July 1963, Paul Cohen showed that if ZF is consistent, then AC is not a theorem of ZF. That is, AC is *independent* of ZF. Ever since then, 4 July has been known as *independence day*!
 - i. Cohen's *forcing* method, although related to Gödel's earlier work, was revolutionary, and for me very difficult to understand.
 - ii. Soon after Cohen's announcement, others began to reformulate his argument in a more accessible Boolean form. For references, see Moore 1982, 304–305. This form is much more succinctly described, but it requires one piece of knowledge covered only in advanced analysis texts.
 - iii. The Boolean argument first shows that for each member B of a certain class of lattices there is a function φ_B that maps the open sentences of ZF and lists of values for their variables to elements of B . These lattices have a negation operation $\sim$ satisfying familiar laws such as $\sim(a \wedge b) = (\sim a) \vee (\sim b)$, and contain the joins and meets of certain infinite subsets: they are Boolean algebras of a certain type. The function φ_B enjoys some properties analogous to those in Gödel's earlier argument:
 - (1) if a is a ZF axiom, then $\varphi_B(a)$ is the maximum element $\top$ of B ;
 - (2) if a conclusion b is derivable from some hypotheses under the ZF rules of proof, and $\varphi_B(a) = \top$ for each hypothesis a , then $\varphi_B(b) = \top$.
 - iv. It follows that $\varphi_B(b) = \top$ for all ZF theorems b , for any Boolean algebra B in this class.
 - v. You can think of such a B as a set of truth values, including not just the maximum element $\top$ but the minimum element $\bot$ and lots of others.

- vi. Now, Cohen's followers analyzed his forcing method and identified a certain Boolean algebra B , already studied in some detail in advanced analysis texts, for which $\varphi_B(\text{AC}) \neq \top$.
- vii. All these arguments of Cohen's followers can be carried out within ZF. Thus if AC were a theorem of ZF then in ZF one could prove both $\varphi_B(\text{AC}) = \top$ and $\varphi_B(\text{AC}) \neq \top$. That is, if ZF is consistent, AC is not a theorem of ZF.

3. *Early objections to the axiom of choice*

- a. This discussion is based mainly on Moore 1982, chapter 1.
- b. During the 1800s, as mathematicians developed rigorous proofs of theorems in algebra and analysis, they often employed some version of the axiom of choice without noticing it. As a first example, consider the first proof of the equivalence of continuity and sequential continuity for real functions, due to Cantor but published in Heine 1872, 183 (routine exercise 2 in the *Axiom of choice* notes). As a second, consider Richard Dedekind's proof that

$$(\forall n \in \mathbf{N}) [Z_n \leq \Sigma] \Rightarrow \mathbf{N} \leq \Sigma, \quad \text{where } Z_n = \{m \in \mathbf{N} : m < n\}$$

in Dedekind [1888] 1963, subsection 159. Ewald's 1996 translation begins,

The proof...—however obvious it may appear—is more complicated. If every system Z_n is similarly mappable into Σ , then to every number n there corresponds a similar mapping α_n of Z_n such that $\alpha_n[Z_n] \subseteq \Sigma$. From the existence of such a series of mappings α_n , regarded as given, but respecting which nothing further is assumed, we derive....

Dedekind tacitly selected one element α_n from each of the nonempty sets $\{e \in \Sigma^{Z_n} : e \text{ is injective}\}$, then constructed from those an injection from $\mathbf{N}$ to Σ . A pioneering study of the foundations of arithmetic, this work exerted enormous influence.

- c. Giuseppe Peano, who frequently examined weaknesses in the statements and proofs of familiar theorems, noted curtly in [1890, 210](#), a paper on the existence of solutions of differential equations, that infinitely many choices of that sort are not justified. Having just published an equally influential study of foundations of arithmetic, he was certainly familiar with Dedekind's argument. This is evidently the first published objection to that type of argument.
- d. In Bettazzi 1892, 176, a paper on continuity of real functions, Peano's junior colleague Rodolfo Bettazzi at the Military Academy in Turin published a more detailed critique of such arguments:

A point can be taken arbitrarily from a given set of points, or from one of its subsets, or from a finite number of its subsets. But when one has to consider infinitely many of its subsets and to construct a subset formed by choosing in each of these subsets any point whatever (as will be the case in what follows), it does not suffice to say that one forms this set by taking a point *arbitrarily* in each of these subsets. For one cannot regard as determinate an *infinite* number of objects all chosen arbitrarily in given classes. This follows clearly when one notes that giving them arbitrarily is equivalent to defining them separately one at a time...

In order that, given an arbitrary set G , one can form a set consisting of any point whatever from each of infinitely many determinate subsets of G , the following problem must be

resolved: given a set of points, indicate a rule by means of which a set determines a point in it, *whatever the given set may be*. In the present state of set theory, no solution is known for this problem. [Translation from Moore 1982, 77.]

- e. In [1896, 512, Bettazzi](#) continued with a specific criticism of Dedekind's argument:

But since there is more than one such correspondence between *any* Z_n and Σ , and since Dedekind does not determine a *specific* one among them, then one must take any one of them *arbitrarily*, and do so for each set of correspondences between any Z_n and Σ ; that is, one must choose an object (correspondence) arbitrarily in each of the *infinite* sets, which does not seem rigorous; unless one wishes to accept as a postulate that such a choice can be carried out—something, however, which seems ill-advised to us. [Translation from Moore 1982, 26–27.]

- f. [Click here](#) for a cartoon.

- g. This topic remained under discussion in several publications. But those papers tended to mix up two questions: whether the notions of finiteness and Dedekind finiteness coincide, and whether arguments that required infinitely many arbitrary choices were valid. Another of Peano's Military Academy colleagues, Cesare Burali-Forti, provided some insight, but confused matters by improperly stating and employing a *partition principle* easily seen to be equivalent to the axiom of choice as stated in these notes: If $\mathcal{S}$ is a disjoint family of sets, then $\#\mathcal{S} \leq \bigcup \mathcal{S}$.

- h. Moreover, discussion of some closely related questions continued alongside.
- i. The theory of well-ordered sets was advanced, using involved recursion techniques.
 - ii. The arithmetic of cardinals of well-ordered sets was developed, and its results were easy to state and very satisfying.
 - iii. It appeared that some of these results might lead to contradictions such as that suggested by Cantor's theorem on cardinals of power sets.
 - iv. Cantor had conjectured years before, in 1879–1884, 550, but was unable to prove, that every set could be well-ordered. That result would greatly simplify the theory of cardinal arithmetic.
 - v. In his famous [1900] 2000 paper on mathematical problems that should guide twentieth-century research, Hilbert posed the proof of Cantor's conjecture as part of the very first problem statement.
- i. In 1902 Beppo Levi instilled some order into these discussions by recognizing the partition principle as a specific assumption, an easy consequence of the well-ordering conjecture, which had not been proved and was therefore to be avoided. [Click here](#) for his original text. Levi then reproved a result of F. Bernstein (substantial problem 9b in the *Cardinals II* unit) without using the partition principle, which Bernstein had originally employed. Levi was also Peano's junior colleague at Turin, but probably not a close one.
- j. Russell's [1902] 1970 antinomy, publicized widely in 1903, clarified this situation somewhat, too. It showed that antinomies should be studied independently of well-ordering and cardinals.

- k. In [1904] 1970, Ernst Zermelo proved that the axiom of choice implies that every set can be well-ordered. He recognized the axiom, in the form presented in the *Axiom of Choice* unit, as a basic principle of set theory, not derived from any simpler ones. [Click here](#) for his original text. It clear, and served to focus the controversy. Widely disseminated in published notes, that continued for at least a decade.
- 4. *Early logical controversies*
 - a. The foundations literature from 1880–1910 reveals that mathematicians then often disagreed with each other, sometimes explicitly, sometimes tacitly, about some very basic concepts and approaches, and their practices sometimes differed considerably from today's. Since at least 1950, we've all learned "by osmosis" to adhere to extremely uniform and rigid standards, and to announce loudly when we depart from them. Thus we sometimes find the earlier literature puzzling when it tacitly interprets a notion in a way different from ours, or annoying when it seems to make much ado about nothing. We must remind ourselves that today's standard approaches evolved through much discussion and experimentation. Problems and solutions that seem clear to today's eyes did not become so until appropriate techniques evolved to study them (and to dismiss irrelevant questions from consideration).
 - b. Decades later Felix Bernstein juxtaposed differing versions of the idea of a set itself, held by the very creators of set theory: Dedekind regarded a set as a completed collection, but Cantor believed that its members should be considered one at a time. Bernstein's anecdote is quoted in [Dedekind 1930–1932a](#), 449.
 - c. Since about 1890, Peano stridently advocated use of precise logical techniques to analyze such differences. Others before, particularly Dedekind and Frege, had adopted equivalent methods, but were less assertive. During the 1890s Bertrand Russell began considering such questions, and experienced a great epiphany when he met Peano in Paris at the 1900 International Congress of Philosophy. From 1903 on, Russell's work became one of the driving forces in philosophy of mathematics. See Kennedy 1973 for a vivid description: *What Russell learned from Peano*. In retrospect, using the philosopher's trick of employing catchy phrases to remind us of knotty problems, Russell mentioned just two lessons: the difference between *Socrates is mortal* and *All Greeks are mortal*, and the difference between an object a and the set $\{a\}$. Kennedy is more direct: Russell learned symbolic logic from Peano. Those lessons each had to do with the distinctions between *one* and *many*, and between a condition and its extension. Russell adopted Peano's techniques, but ultimately disagreed with him on the latter question. Peano's work made it possible to reason precisely about such questions, and to recognize where differences lay.
 - d. [Click here](#) for portraits of Russell and Peano.
 - e. Frege's [1895] 1980 review of Schröder 1890 illustrates some of these difficulties. Frege claimed that Schröder was contradictory, and demonstrated that

even slightly careless handling of predicates, extensions, membership, inclusion, the empty set, and singleton sets can lead to such contradiction. (This reminds me of the software developer's maxim that bugs in software tools usually manifest themselves in the simplest possible applications.) Frege spent pages on the distinction between a and $\{a\}$. On the other hand he rejected ([1895] 1980, 89) the idea of an empty set, with an argument akin to Cantor's set concept just mentioned: "If we burn down all the trees of a wood, we thereby burn down the wood." I regard his argument as wrong, because it doesn't make sense to speak of the wood at one time, then at another. Frege did, however, accept some of Schröder's uses of the empty set as a convenient artificial mathematical idea.

- f. Translating the 1898 work of Peano's junior colleague Mario Pieri, I must continually remind myself that without being aware of it, I learned to use the basic notions about sets in a way somewhat different from that of Peano and his followers. Careless substitution of today's usages for Pieri's can make his work appear inconsistent.
5. *Projects*
- a. *For a term paper or master's expository paper.* For each $n \in \mathbb{N}$, let AC_n stand for the statement *every indexed family of n -element sets has a choice function*. Interrelationships among these statements has been studied in detail using methods of set theory, combinatorics, and algebra. Years ago I attended a marvelous series of lectures on this subject by John Horton Conway, published in 1973. (The containing publication Mathias and Rogers 1973, is hard to locate, but available through our library.) Those, along with Sierpinski 1958, §VI.5, are a starting place. There is probably more ample research literature.
 - b. *For a term paper.* Using the accessible literature, investigate further uses of the axiom of choice in real analysis.
 - c. *For a master's expository paper, or perhaps for a term paper.* Wagon 1985 is about the Banach–Tarski "paradox," one of the most spectacular and counter-intuitive consequences of the axiom of choice. At least one other, comparable, book is available, too. A report on this subject would be intriguing. It would probably require background in advanced real analysis.