Hilbert's Hotel and other encounters with infinity

Barry Mazur

I want to thank Minhyong Kim and the organizing committee of the International Centre for Mathematical Sciences-London Mathematical Society UK Mathematics Undergraduate Colloquium (May 2022) for inviting me to talk. Here are rough notes I made in preparation for it.

How do we measure infinity? How do we compare infinite sets? If someone tells you that "it is equally likely for a prime number to have residue $+1$ as it is likely for it to have residue -1 modulo 4"—forgetting any proof of this claim for the moment—in how many ways might one formulate (correct) rigorous mathematical statements that are in accord with that claim?

I will elaborate on such questions. E.g., on the notion of density of a subset contained in an infinite set: what this might mean, in hopes of launching a general discussion.

1. Density Questions

$$\text{infinite set} \longrightarrow S \subset T \longleftarrow \text{infinite set}$$

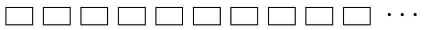
What might the density of a subset contained in an infinite set mean?

Of course a related, perhaps prior, question is:

What is an infinite set?

2. Infinite Real Estate

You might be familiar with the virtues of that unending corridor of rooms in Hilbert's Hotel:



Even if every room is occupied and some new guest arrives looking for a room: no problem: the manager ask all the guests to move to the next room in the corridor, leaving the first room free for the new guest.

3. Defining Infinity:

Here are four possible definitions of *infinite set*—they are all minor variants of one another. (The first is due to Dedekind and resonates with that curious corridor in *Hilbert's Hotel*.)

What do we think is the difference between these four possible definitions of *infinite set* given below?

Recall the concepts: **injective** and **surjective** map.

A map $f : X \longrightarrow Y$ is **injective** (synonym: "**one-one into**") if f sends no two different elements of the set X to the same element of the set Y.

I.e., if for $x, x' \in X$ we have

$$\{x \neq x'\} \implies \{f(x) \neq f(x')\}.$$

I.e., no collapsing:

$$\begin{tikzcd} x \arrow[dr, "f"'] & & x' \arrow[dl, "f"] \\ & z & \end{tikzcd}$$

An example:

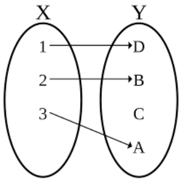


Figure 1. injective

A map $f : X \longrightarrow Y$ is **surjective** (synonym: "**onto**") if every element $y \in Y$ is in the image of X under the map f; i.e.,

$$\forall y \in Y \; \exists x \in X \text{ such that } f(x) = y.$$

An example:

Now for the four different candidate-definitions of this concept "infinite set":

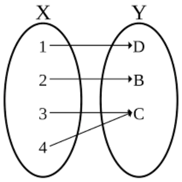


FIGURE 2. surjective

Definition ∞_1 : A set S is **infinite** if there exists an *injective* mapping $f : S \to S$ (i.e., from the set S to *itself*) that is not surjective (equivalently: is not a one:one correspondence between the set S and itself).[1]

Definition ∞_2 : A set S is **infinite** if there exists a *surjective* mapping $f : S \to S$ (i.e., from the set S to *itself*) that is not injective (equivalently: is not a one:one correspondence between the set S and itself).

Definition ∞_3 : A set S is **infinite** if there exists an injective mapping of the set $\mathbf{N}$ of natural numbers into S.

(The set of natural numbers is what you think it is: $\mathbf{N} := \{1, 2, 3, 4, \dots\}$, even though the ancients were dubious about the number 1 as being in the same category as the other whole numbers. To actually *define*[2] this set $\mathbf{N}$ without making use of the *dot-dot-dots* requires some apparatus—e.g., mathematical induction.)

Definition ∞_4 : A set S is **infinite** if there exists an surjective mapping of the set S onto $\mathbf{N}$.

We could also pass the buck by defining an infinite set as simply... an *in*-finite set, i.e., a *non-finite set.* E.g., it is a set S such that any finite subset of S has a non-empty complement in S. So, what is a finite set?

4. DEFINITION OR CHARACTERIZATION?

Within the appropriate axiomatic set-theoretic context, the four definitions of “infinite set” are equivalent, so we have a choice:

- We can choose one of them as our primary definition, and the other three can be thought of as ‘characterizations’ of the then-defined concept—infinite set.

[1] This definition is given in Richard Dedekind’s (1888) essay “Was sind und was sollen die Zahlen?”

[2] And here, the late middle English sense of the word ‘define’ (to *bring to an end*) fits neatly.

- We can simply say: these are all equivalent and any one can serve as “the” definition.

The relationship between these choices depend on the ambient axiomatic context in which are working. For example, if you accept the ‘Axiom of Choice’ then if a set is infinite following Definition ∞_2 it is also infinite following Definition ∞_1.[3]

The question, then, (*What is an infinite set?*) depends on the choice: definition versus characterization. The same holds for the question:

What *are*[4] Prime Numbers?

As for the power of definition to provide ‘focus,’ consider the two equivalent definitions of prime number (given by (1) and (2) below)—where one is left to make the choice of regarding one of these as ‘definition’ and the other as ‘characterization’:

A prime number p is a (whole) number greater than one

(1) that is not expressible as the product of two smaller numbers. I.e., is *unfactorable.*

or

(2) that has the property that if it divides a product of two numbers, it divides one of them.

If you choose (2) as the fundamental definition you are placing the notion of prime number in the broader context of ‘prime’-ness as it applies to number systems more general than the ring of ordinary numbers—and more specifically in the context of *prime ideals* of a general ring. So choosing (2) as definition casts (1) as a specific feature that characterizes prime numbers, thanks to the theorem that guarantees the equivalence of these two formulations. Going the other route—i.e., focusing on (1), the unfactorable quality of prime number, would then cast (2) as a basic more general feature also *characterizing* prime-ness.

[3] For an excellent account of the issues that Dedekind confronted in his essay see *Notes on Richard Dedekind’s “Was sind und was sollen die Zahlen?” by David Joyce,* `https://mathcs.clarku.edu/~djoyce/numbers/dedekind.pdf`

[4] ‘and what should be’—following the tone of Dedekind’s *“Was sind und was sollen die Zahlen?”*

5. What prime numbers **are there**?

5.1. **New primes are discovered every few days. . . .** *One week ago today:* A record prime of 50001 digits was computed:

$$10^{50000} + 65859$$

is the smallest prime with 50001 digits[5].

5.2. **Proofs that there are infinitely many primes.**

(1) *The* classical proof: . . . is the one in Euclid's *Elements*[6]

It proves that the set of prime numbers is "non-finite." E.g., if you already know that $2, 3, 5, 7$, and 11 are primes, for example, then Euclid's proof notes that there exists yet another prime

$$\leq 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \ + \ 1 \ = 2311.$$

Well, 2311 is, in fact, a prime not on your list, but. . . so is 13.

(2) *Far out proofs:*
Following Euler, the Riemann zeta function $\zeta(s)$ which has its additive and multiplicative formats—for $Re(s) > 1$:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \ = \ \prod_{p \text{ prime}} \big(1 - \frac{1}{p^s}\big)^{-1.}$$

For $s = 2n$ (with n any positive integer) Euler proved that

$$\zeta(2n) = \prod_{p \text{ prime}} \big(1 - \frac{1}{p^{2n}}\big)^{-1} = r_n \cdot \pi^{2n} \tag{5.1}$$

where r_n is some (positive) rational number[7].

Now,

[5] `https://www.multiprecision.org/downloads/ecpp/cert-50000.bz2` in PARI/GP format and `https://www.multiprecision.org/downloads/ecpp/cert-50000.primo.bz2` in Primo format as converted by PARI/GP code written by J. Asuncion, who is also the author of the fastECPP implementation in PARI/GP.

[6] "Elements" —'Στοιχεîα'—is quite a stark title. "Elements" of what?

[7] $\boxed{r_n := (-1)^{n+1} \frac{2^{2k-1}}{(2k)!} \cdot B_{2n}}$ where B_{2n} is the $2n$th Bernoulli number.

- noting that *if there were only finitely many prime numbers*, then

$$\prod_{p \text{ prime}} (1 - \frac{1}{p^{2n}})^{-1} \tag{5.2}$$

  would be a *rational* number, and

- comparing Equation 5.1 with:

  Theorem 5.3. *(Lindemann-Weierstrass) π is transcendental,*

  and

- choosing n to be some positive number you like:

  $n = 1$ or $n = 2$, or ... $n =$ a million,

  we get:

- a contradiction, since Equation 5.2 would be rational and $r_n \cdot \pi^{2n}$ is irrational.

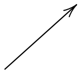
Therefore, for any choice of n, we get:

Corollary 5.4 ($\{Proof_n\}$)**.** *There are infinitely many prime numbers.*

Query 1. (1) *Assuming that these proofs aren't circular (and I'm guessing that they aren't) would you consider them to actually be different proofs for different choices of positive integer n?*

(2) *Which, if any, of the definitions above of the concept "infinite" do these proofs rely on?*

6. Prime Number Races



That is the title of a wonderful article[8] by Andrew Granville and Greg Martin that explains in detail the race between, for example, the team of

[8] https://arxiv.org/pdf/math/0408319.pdf

prime numbers congruent to 1 mod 4 (color them blue) and the team congruent to -1 mod 4 (color them red).

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

Primes congruent to 1 mod 4 (blue)—versus—Primes congruent to -1 mod 4 (red)

$$\{\text{ Score for primes } < 100\}: \qquad 11 \quad \text{to} \quad 13$$

The race is very close, but the team of Primes congruent to -1 mod 4 is ahead. This is often the case for larger packets of prime numbers:

$$\{\text{ Score for primes } < 100,000\}: \qquad 4783 \quad \text{to} \quad 4808$$

If you choose a prime 'at random' and ask what the probability is that you've got a 'red' prime or a 'blue' prime the answer is $1/2$ thanks to a theorem of Dirichlet. Much more specifically,

$$\lim_{X\to\infty} \frac{|\{\text{red primes } < X\}|}{|\{\text{primes } < \mathrm{X}\}|} = \lim_{X\to\infty} \frac{|\{\text{blue primes } < X\}|}{|\{\text{primes } < \mathrm{X}\}|} = \frac{1}{2}. \tag{6.1}$$

So, the race is tight, and even tighter given

- a conjecture[9] that for 100% of the positive integers X the number of red primes less than X exceeds the number of blue primes less than X,

and

- a theorem of Littlewood that says that there will be cutoffs X arbitrarily large for which the number of blue primes less than X exceeds the number of red primes less than X.

This discussion might lead us to the general question:

7. What ways are there to measure the 'density' of a subset S of the set $\mathcal{P}$ of prime numbers?

Such a notion, **density** should b e defined on lots of (but not necessarily all) subsets

$$S \mapsto \delta(S) \in [0,1] \subset \mathbb{R},$$

[9] beginning with some comments of Tschebyscheff in a letter to the mathematician Fuss. This was sharpened and made explicit as a conjecture in 1962 by Knapowski and Turán. See the discussion in the article *Prime Number Races* of Granville and Martin cited above.

should at least have these basic properties:

(1) The density of the full set of primes $\mathcal{P}$ (in $\mathcal{P}$) is 1: $\delta(\mathcal{P}) = 1$.
(2) The density of any finite set of primes (is defined, and) is 0.
(3) *Density is finitely additive:* Let $S_1, S_2 \subset \mathcal{P}$ be disjoint subsets of primes and $S_3 := S_1 \cup S_2$ their union. If two out of the three subsets S_1, S_2, S_3 have defined densities then the third one has a defined density too: and

$$\delta(S_1) + \delta(S_2) = \delta(S_3).$$

7.1. **Natural Density:** The most natural definition one can think of that might be called the density of a subset S of primes is:

$$\delta_{\text{natural}}(S) := \lim_{X \to \infty} \frac{|\{p \in S; p \leq X\}|}{|\{p \in \mathcal{P}; p \leq X\}|}, \tag{7.1}$$

if that limit exists. (E.g., this has already appeared in Equation 6.1 above.) And δ_{natural} satisfies all the requirements in the axioms above.

Note that "natural density" depends *only* on the structure of $\mathcal{P}$ viewed as an ('abstract') ordered set, and not at all on the placement of the prime numbers within the set of real numbers.

For example, we can ask for the "natural density" of any subset $\mathcal{S}$ of the set of natural numbers, and if you are willing to replace "lim" by "liminf" you have a definition of 'proportion' for any subset of natural numbers:

$$\underline{\delta}(\mathcal{S}) := \liminf_{X \to \infty} \frac{|\{n \in \mathcal{S};\ n \leq X\}|}{X}, \tag{7.2}$$

It's fascinating to compare this natural concept of proportion of subsets of prime numbers in the set of all prime numbers with notions of 'density' that do, in fact, depend on the actual positions of primes on the number line.

7.2. **Here's something that's not yet a density:** It's fascinating to compare this natural concept of proportion of subsets of prime numbers in the set of all prime numbers with notions of 'density' that do, in fact, depend on the actual positions of primes on the number line:

For each real number $x > 1$ and any set of primes S, let's define the "x**-Density**" of S to be

$$\delta_x(S) := \frac{\sum_{p \in S} p^{-x}}{\sum_{p \in \mathcal{P}} p^{-x}}. \tag{7.3}$$

What's neat about "x**-Density**" is that (for any $x > 1$) $\delta_x(S)$ is defined for every subset $S \subset \mathcal{P}$, and is finitely additive.

It has the defect, though, of assigning a *non zero density* to absolutely every nonempty subset—including finite subsets.

7.3. **Dirichlet Density.** Here's a way, due to Dirichlet, of correcting that defect:

Define the Dirichlet density, $\delta_{\text{Dirichlet}}(S)$, of a subset $S \subset \mathcal{P}$ to be the limit in Equation 7.3—*if that limit exists.*

$$\delta_{\text{Dirichlet}}(S) := \lim_{x\to 1} \delta_x(S) \tag{7.4}$$

Note that if S is any finite subset of $\mathcal{P}$ the numerator, $\sum_{p\in S} p^{-x}$, of Equation 7.3 has a finite limit as x tends to 1, while:

Lemma 7.5. *The denominator of Equation 7.3 tends to infinity as x tends to* 1*.*

So, the Dirichlet density of any finite set of primes is 0. Dirichlet density then satisfies all three requirements desired for a 'density' listed above.

7.4. **The relationship between Natural and Dirichlet Density.**

Theorem 7.6. *If a subset $S \subset \mathcal{P}$ has a natural density, then S also has a Dirichlet density, and the two densities are the same.*

8. The non-correlation of prime numbers and congruence

Equation 6.1 says that if you pick prime at random it has a residue of $+1$ (rather than -1) mod 4 fifty percent of the time. Therefore the other way too, of course: it has a residue of -1 (rather than $+1$) mod 4 fifty percent of the time.

The same sort of thing is true (proved again by Dirichlet) for any other reasonable congruence condition. Let $x \mapsto \Phi(x)$ be Euler's Phi-function. Take m any positive number. There are $\Phi(m)$ congruence classes mod m containing elements relatively prime to m.

Given such a congruence class, Dirichlet showed that the probability that a 'random prime' falls into that congruence class is

$$\frac{1}{\Phi(m)},$$

i.e., the primes are uniformly distributed over those congruence classes mod m.

9. A very new result about proportions of numbers having interesting properties

Question 9.1. *What is the proportion of integers that are the sum of two rational cubes?*

This happens frequently; e.g.. . .

$$1, 2, 6, 7, 8, 9, 12, 13, 15, 16, 17, 19, 20, 22, 26, 27, 28, 30, 31, 33, 34, 35, \ldots$$

For example:

$$6 = (17/21)^3 + (37/21)^3$$

Let $\mathcal{S}$ denote the set of such integers. Is it as 'likely' that an integer is in $\mathcal{S}$ as not?

A very recent result of Levent Alpöge, Manjul Bhargava, and Ari Shnidman—with full proofs forthcoming[10] is an important advance in that direction:

Theorem 9.2. *(Alpöge, Bhargava, Shnidman) , A positive proportion of integers are not the sum of two rational cubes, and a positive proportion of integers are*[11].

10. Welcome to Arithmetic Statistics!

These kinds of questions are both utterly traditional. . . but also are in a currently burgeoning, rapid-moving, part of number theory where the aim is to get the (statistical) 'lay of the land' regarding basic issues in number theory.

[10] See —

[11] proof forthcoming