Chapter 7
Varieties of Infiniteness in the Existence of Infinitely Many Primes

Victor Pambuccian

Abstract By providing quantifier-free axioms systems, without any form of induction, for a slight variation of Euclid's proof and for the Goldbach proof for the existence of infinitely many primes, we highlight the fact that there are two distinct and very likely incompatible concepts of infiniteness that are part of the theorems proved. One of them is the concept of cofinality, the other is the concept of equinumerosity with the universe.

7.1 Introduction

After looking at various proofs for the same result, in his essay [7], David Hilbert wrote

> These specific executions show how various methods of proof are applicable to the same problem; they also suggest to us the necessity to study the essence of mathematical proof itself if such questions as those of decidability by finitely many operations should be answered at all.[1]

Hilbert's suggestion, to look at various "methods of proof" and to study "the essence of mathematical proof itself" will be applied here to two proofs of the infinitude of primes, one going back to a letter Christian Goldbach wrote to Leonhard Euler (in Latin) from Moscow on 20 (31) July 1730 (see [3, p. 32f]) regarding the co-primeness of the Fermat numbers, re-discovered in [8, 10] and used to prove the infinitude of primes (see [4] for the proof's history), and a slightly modified version of Euclid's proof, whose logical underpinnings have already been the subject of study

[1] Diese speziellen Ausführungen zeigen, wie verschiedenartige Beweismethoden auf dasselbe Problem anwendbar sind, und sollen nahelegen, wie notwendig es ist, das Wesen des mathematischen Beweises an sich zu studieren, wenn man solche Fragen, wie die nach der Entscheidbarkeit durch endlich viele Operationen, mit Erfolg aufklären will.

V. Pambuccian (✉)
School of Mathematical and Natural Sciences, Arizona State University - West Campus,
P. O. Box 37100, Phoenix, AZ 95069-7100, USA
e-mail: pamb@asu.edu

F. Ferreira et al. (eds.), *Axiomatic Thinking II*,
https://doi.org/10.1007/978-3-030-77799-9_7

by Andrew Arana in [1, 2]. Studying the proofs themselves will inform us what the minimal assumptions are that are needed to carry out the deductions. We will find out, in the process, that, while on an informal level, the two proofs prove the *same result*, at the formal level, they prove *two different, very likely incompatible results*, that the kinds of infinity each finds the collection of primes to display are essentially different.

In what follows, we will first provide an axiomatic analysis of the two proofs, in the sense described by Hilbert in [6]:

> By the axiomatic analysis of a mathematical truth I understand an investigation, which does not aim to discover new or more general theorems relative to that truth, but rather aims to clarify the position of that theorem inside the system of known truths and their mutual logical connections in such a way that one can indicate exactly which conditions are necessary and sufficient for justifying that truth.[2]

The problem regarding the assumptions needed to prove the cofinality of prime numbers has been recently treated in [1, 2], where the main concern is to distinguish a *pure* proof of the cofinality of primes from one that is not pure. Euclid's proof, slightly modified to ensure that it proves cofinality, is found to be *pure*, and an axiom system that allows one to reason along the lines of Euclid's proof is presented in [1, 2]. The axiom systems presented in the two papers contain the axiom of induction, as well as the requirement that the product of all primes less than a certain given number exists.

The proofs we will present in this paper can also be considered to be *pure*, in the sense that they use only notions and axioms that belong to elementary number theory. If one thinks of purity in terms of Hilbert's [5, pp. 315–316] comment that

> In modern mathematics such criticism is raised very often, where the aim is to preserve the purity of method, i.e. to prove theorems if possible using means that are suggested by the content of the theorem.[3]

Then one cannot say that they are pure, for neither the exponential function that appears in the proof based on the co-primality of the Fermat numbers nor the existence of a number divisible by all primes $\leq x$ are "suggested by the content of the theorem".

The axiom systems will contain only what is really needed to carry the respective proofs through. Both axiom systems will consist entirely of quantifier-free axioms.

When understood in the sense of *cofinality*, the existence of infinitely many primes states that, for any given number x, there is a prime number larger than x. When understood in the sense of *equinumerosity with the universe*, it states that there exists

---

[2] Unter der axiomatischen Erforschung einer mathematischen Wahrheit verstehe ich eine Untersuchung, welche nicht dahin zielt, im Zusammenhange mit jener Wahrheit neue oder allgemeinere Sätze zu entdecken, sondern die vielmehr die Stellung jenes Satzes innerhalb des Systems der bekannten Wahrheiten und ihren logischen Zusammenhang in der Weise klarzulegen sucht, daß sich sicher angeben läßt, welche Voraussetzungen zur Begründung jener Wahrheit notwendig und hinreichend sind.

[3] In der modernen Mathematik wird solche Kritik sehr häufig geübt, wobei das Bestreben ist, die Reinheit der Methode zu wahren, d.h. beim Beweise eines Satzes wo möglich nur solche Hülfsmittel zu benutzen, die durch den Inhalt des Satzes nahe gelegt sind.

a definable function τ, with $\tau(x) > 1$ for all x, such that, for all x, $\tau(x)$ is a prime number and $\tau(x) = \tau(y) \rightarrow x = y$ holds. One can think of τ as an injective function from the natural numbers to the prime numbers.

7.2 The Axiom System and Some Basic Facts for the First Proof

The language for the proof based on the co-primeness of Fermat numbers consists of $0, 1, +, \cdot, -, <, \left[\frac{x}{y}\right], 2^x, \pi$—in which 0 and 1 are individual constants, $+$, $\cdot$, and $-$ are binary operations ($x - y$ taking arbitrary values for $x \leq y$), $<$ is a binary relation, $\left[\frac{x}{y}\right]$ is a binary operation, 2^x and π are unary operations. We will also use the defined relation $|$ with $n \mid m \Leftrightarrow \left[\frac{m}{n}\right] \cdot n = m$ as well as the defined relation $\leq$, with $x \leq y \Leftrightarrow x < y \vee x = y$. Here $[\frac{x}{y}]$ will stand for the greatest integer $\leq \frac{x}{y}$, whenever $y \neq 0$, and for an arbitrary value if $y = 0$, 2^x for "2 to the power x", and $\pi(x)$ for the smallest prime number that divides x, for $x > 1$, and for an arbitrary value for $x \leq 1$. We will denote by $\overline{n}$ the term $1 + (1 + \ldots 1)) \ldots)$, where 1 shows up n times, where n is a natural number. The terms $\overline{n}$ will be referred to as *numerals*. The axioms are

A 1 $(x + y) + z = x + (y + z)$,

A 2 $x + y = y + x$,

A 3 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

A 4 $x \cdot y = y \cdot x$,

A 5 $x \cdot (y + z) = x \cdot y + x \cdot z$,

A 6 $x + 0 = x \wedge x \cdot 0 = 0$,

A 7 $x \cdot 1 = x$,

A 8 $(x < y \wedge y < z) \rightarrow x < z$,

A 9 $\neg x < x$,

A 10 $x < y \vee x = y \vee y < x$,

A 11 $x < y \rightarrow x + z < y + z$,

A 12 $(0 < z \wedge x < y) \rightarrow x \cdot z < y \cdot z$,

A 13 $x < y \rightarrow x + (y - x) = y$,

A 14 $0 < 1 \wedge (0 < x \rightarrow 1 \leq x)$,

A 15 $0 \leq x$,

A 16 $0 < x \rightarrow \left(\left(\left[\frac{y}{x}\right] \cdot x < y \wedge y - \left[\frac{y}{x}\right] \cdot x < x\right) \vee \left[\frac{y}{x}\right] \cdot x = y\right)$,

A 17 $0 < x \rightarrow 1 < 2^x$,

A 18 $2^x \cdot 2^y = 2^{x+y}$,

A 19 $x < y \rightarrow 2^{2^x} + 1 \mid 2^{2^y} - 1$,

A 20 $1 < x \wedge x \mid 2^y \rightarrow \overline{2} \mid x$,

A 21 $1 < x \rightarrow (1 < \pi(x) \wedge \pi(x) \mid x)$,

A 22 $1 < x \wedge 1 < p \wedge p \mid x \rightarrow \pi(x) \leq p$.

A1–A15 are the axioms of an established theory, PA^- (see [9]). A16 states the possibility of Euclidean division with remainder. The meaning of A17 and A18 is obvious. A21 states that, for all $x > 1$, $\pi(x)$ is a non-trivial divisor of x while A22 states that $\pi(x)$ is the smallest non-trivial divisor of x.

Here are some basic properties one can prove from our axioms.

Lemma 7.1 *If $a < b$, then $a + 1 \leq b$.*

Proof By A15, A13, and A6, we have $0 < b - a$. By A14, we have $1 \leq b - a$. By A13 and A11, we get $a + 1 \leq b$.

Lemma 7.2 *If $z \neq 0$ and $a \cdot x = z$, then $a = [\frac{z}{x}]$.*

Proof By A16, $\left[\frac{z}{x}\right] \cdot x \leq z$. If $\left[\frac{z}{x}\right] \cdot x = z$, then we have $\left[\frac{z}{x}\right] \cdot x = a \cdot x$. By A15, A6 and the fact that $z \neq 0$, we have $0 < x$. By A10, we have $[\frac{z}{x}] < a \vee \left[\frac{z}{x}\right] = a \vee a < \left[\frac{z}{x}\right]$. If $\left[\frac{z}{x}\right] < a$ were the case, then, by A12, we would have $\left[\frac{z}{x}\right] \cdot x < a \cdot x$, and similarly if $a < \left[\frac{z}{x}\right]$ were the case. Thus $\left[\frac{z}{x}\right] = a$.

If $\left[\frac{z}{x}\right] \cdot x < z$, then, by A10, A12, and the fact that $x \neq 0$, we have that $\left[\frac{z}{x}\right] < a$. By A16,

$$z - \left[\frac{z}{x}\right] \cdot x < x. \tag{7.1}$$

Since $[\frac{z}{x}] < a$, we get, by Lemma 7.1,

$$\left[\frac{z}{x}\right] + 1 \leq a. \tag{7.2}$$

By (7.1), A13, A5, A2, A4, and (7.2), $z < x + \left[\frac{z}{x}\right] \cdot x = x \cdot (1 + \left[\frac{z}{x}\right]) \leq a \cdot x = z$, contradicting A9.

Thus, the definition of $a \mid b$ could be rephrased as "there exists a u such that $a \cdot u = b$". This should not be interpreted as an introduction of the existential quantifier through the back door. Although we will make free use of this observation in the sequel, there is no need for it in the proofs that follow. Indeed, a first draft of this paper carried the proofs without use of Lemma 7.2. The proofs were just longer and typographically cumbersome.

Lemma 7.3 $x \mid y \wedge y \mid z \rightarrow x \mid z$.

Proof To prove this, let us first notice that, if $z \neq 0$ and $a \cdot x = z$, then, by Lemma 7.2, $a = [\frac{z}{x}]$. Since $x \mid y$ and $y \mid z$ amount to $\left[\frac{y}{x}\right] \cdot x = y$ and $\left[\frac{z}{y}\right] \cdot y = z$, we have $\left[\frac{z}{y}\right] \cdot \left(\left[\frac{y}{x}\right] \cdot x\right) = z$. By A3 and Lemma 7.2 we conclude that $x \mid z$.

We can prove that

Lemma 7.4 *For* $1 < x$, $\pi(x)$ *is* irreducible, *i.e.* $a \cdot b = \pi(x) \rightarrow (a = 1 \vee b = 1)$.

Proof Suppose $\pi(x) = a \cdot b$, with $a \neq 1$ and $b \neq 1$. Then, by A14, A15, A6, and A21, $1 < a$ and $1 < b$. . Since $a \cdot b = \pi(x)$ implies that $a \mid \pi(x)$, and since $\pi(x) \mid x$, we have, by Lemma 7.3, also $a \mid x$. By A22 we should have $\pi(x) < a$ or $\pi(x) = a$. Since $\pi(x) = a \cdot b$ and $1 < b$, we have, by A12 and A4, $a < \pi(x)$. This contradiction proves that one of a or b must be 1.

A19 states that $2^{2^x} + 1$ divides $2^{2^y} - 1$ whenever $x < y$. If $y = x + \overline{n}$, then we can prove A19 from the other axioms, but, in general, the difference between y and x does not need to be a numeral.

The infinity of primes, which we will prove, is in the form of the equinumerosity of a set of primes with the universe, the function $\tau(x)$ being in our case a term, namely, $\pi(2^{2^x} + 1)$. It is the statement

IP $\pi(2^{2^x} + 1) = \pi(2^{2^y} + 1) \rightarrow x = y$.

7.3 Proof of the Infinity of Primes Based on the Co-Primeness of the Fermat Numbers

Let $F_n = 2^{2^n} + 1$. If $2^0 = 0$, then, by A18 and A6, we should have $2^x = 0$ for all x, contradicting A17 and A14. Thus, by A15, $0 < 2^0$. By A18, $2^0 \cdot 2^0 = 2^{0+0}$, and, since $0 + 0 = 0$ by A6, we have $2^0 \cdot 2^0 = 2^0$. Since $0 < 2^0$, by A14, we have either $2^0 = 1$ or $1 < 2^0$. If $1 < 2^0$ were the case, then, by A12 and A7, we would have $2^0 < 2^0 \cdot 2^0$, which contradicts A9. Thus $2^0 = 1$. Notice that, by A17, A15, A14, and A8, $1 < 2^{2^n}$, for all n, so that, by A11, $\overline{2} < F_n$, for all n. By A19, $F_n \mid F_m - \overline{2}$ for all $n < m$. Thus $\pi(F_m) \neq \pi(F_n)$ for all $m \neq n$. For, suppose, for some $n < m$, we had $\pi(F_m) = \pi(F_n)$, and let α denote that common value. Notice that, by A13, A10, and A11, we have, for $x > 1$, $(x + 1) - \overline{2} = x - 1$. Thus $\alpha \mid F_m$ (by A21) and, by Lemma 7.3, $\alpha \mid F_m - \overline{2}$. Thus, for some u and v, $\alpha \cdot u = F_m$ and $\alpha \cdot v = F_m - \overline{2}$. By A10 and A11, we have $v < u$. By A13, $v + (u - v) = u$, and thus, by A5, $\alpha \cdot v + \alpha \cdot (u - v) = \alpha \cdot u$, which means that $(F_m - \overline{2}) + \alpha \cdot (u - v) = F_m$. By A13 and A10, we get $\alpha \cdot (u - v) = \overline{2}$. This implies $\alpha \mid \overline{2}$. We also have, by A20, that $\overline{2} \mid F_m - 1$, and thus, given Lemma 7.3, $\alpha \mid F_m - 1$. Repeating the argument that has led us from $\alpha \mid F_m$ and $\alpha \mid F_m - \overline{2}$ to conclude that $\alpha \mid \overline{2}$ with 1 instead of $\overline{2}$, we get that $\alpha \mid F_m$ and $\alpha \mid F_m - 1$ imply $\alpha \mid 1$. However, since $1 < F_m$, we have, by A21, $1 < \alpha$, so, by A12 and A9, we cannot have $\alpha \mid 1$.

With $\mathcal{H} = \{\text{A1} - \text{A22}\}$, we have proved that

Theorem 7.5 $\mathcal{H} \vdash$ **IP**.

7.4 Euclid's Proof for the Cofinality of Primes

For the formalization of Euclid's proof, slightly modified by Arana, of the cofinality of primes, the language will contain $0, 1, +, \cdot, -, <, \left[\frac{x}{y}\right], \pi$, with the same intended interpretation as above, as well as the unary operation ϵ, with $\epsilon(x)$ to be read, for $x > 1$, as a multiple of each prime $\leq x$, an arbitrary number for $x = 1$ and for $x = 0$. Besides A1–A16, A21, A22, we need the following axiom:

A 23 $1 < x \wedge \pi(x) = x \wedge x \leq z \rightarrow x \mid \epsilon(z)$.

In this setting, one can prove the cofinality of primes, that is:

CP $1 < x \rightarrow x < \pi(\epsilon(x) + 1)$.

To see this, notice that, by A10, if that is not the case, then $x = \pi(\epsilon(x) + 1)$ or $\pi(\epsilon(x) + 1) < x$. So, if we denote $\pi(\epsilon(x) + 1)$ by u, then, by A21, we have $u \mid \epsilon(x) + 1$. Since $u = x \vee u < x$ and $\pi(u) = u$ (since u is irreducible by Lemma 7.4), by A23, we have $u \mid \epsilon(x)$. By A13, A10, A11, and A5, we get $u \mid 1$, which contradicts the fact that $1 < u$. With $\mathcal{E} = \{\text{A1} - \text{A16}, \text{A21} - \text{A23}\}$, we have proved that

Theorem 7.6 $\mathcal{E} \vdash$ **CP**.

If we want to have a description of ϵ that comes closer to "the product of all primes $\leq x$", we need to add the following two axioms:

A 24 $1 < x \wedge \pi(x) = x \wedge z < x \rightarrow x \not\mid \epsilon(z)$

A 25 $1 < x \wedge \pi(x) = x \wedge (z < x \vee z = x) \rightarrow x^2 \not\mid \epsilon(z)$.

These, however, have no role to play in the proof of **CP**, which is why we did not adopt them as axioms for our proof.

7.5 Comparing Notions of Infinity

We have come to our main point, namely, the observation that **IP** and **CP** are fundamentally different statements, that none is stronger than the other. To make our statement precise, let $\mathcal{T}$ be a theory in a language either containing $0, 1, +, \cdot, <, \left[\frac{x}{y}\right], \pi$

or one in which these notions can be defined in terms of the primitive notions of $\mathcal{T}$, which proves A1–A16, A21, A22. We say that $\mathcal{T}$ proves that *the number of primes is equinumerous with the universe* if it satisfies

IP$_0$ There exists a function τ, definable in $\mathcal{T}$, with $\mathcal{T} \vdash 1 < \tau(x)$, $\mathcal{T} \vdash \pi(\tau(x)) = \tau(x)$, and $\mathcal{T} \vdash \tau(x) = \tau(y) \to x = y$.

We say that $\mathcal{T}$ proves the *cofinality of primes* if

CP$_0$ $\mathcal{T} \vdash (\forall x)(\exists y)\, x < y \wedge \pi(y) = y$.

One could think that any theory $\mathcal{T}$ which proves **IP$_0$** must also prove **CP$_0$** by reasoning informally as follows: All the $\pi(\tau(j))$ for $1 \leq j \leq x$ cannot be $\leq x$ by the pigeonhole principle, so there is a j such that $x < \pi(\tau(j))$. However, the pigeonhole principle is a very powerful statement, when looked at with formal eyeglasses. It is usually proved by using the induction axiom (see [9, p. 68]) and there is no reason to believe that for $\mathcal{T} = \mathcal{H}$ one could prove the particular instance of the pigeonhole principle scheme corresponding to $\tau(x) = \pi(2^{2^x} + 1)$.

Let us look what it would mean for $\mathcal{H}$ to prove **CP$_0$**. It would mean that we knew of a term $\theta(x)$ in the language $0, 1, +, \cdot, <, \left[\frac{x}{y}\right], 2^x, \pi$, such that $\mathcal{H}$ would prove $x < \pi(\theta(x))$. Now, there is no axiom in $\mathcal{H}$ which could help with the size of $\pi(x)$, so it appears to be hopeless to try to find such a term $\theta(x)$.

What would it mean for $\mathcal{E}$ to satisfy **IP$_0$**? It would mean that we knew of some function $\tau(x)$, such that $\mathcal{E} \vdash \pi(\tau(x)) = \tau(x)$ and $\mathcal{E} \vdash \tau(x) = \tau(y) \to x = y$. $\mathcal{E}$ is almost certainly too weak to prove any such result.

We are thus led to the following:

Conjecture $\mathcal{E}$ does not satisfy **IP$_0$** and $\mathcal{H}$ does not satisfy **CP$_0$**.

Acknowledgements This paper was written while the author enjoyed the hospitality of Yerevan State University as a Fulbright Scholar. I thank Gurgen Asatryan for fruitful conversations on the subject of this paper and an anonymous referee for many improvements.

References

1. A. Arana. L'infinité des nombres premiers: une étude de cas de la pureté des méthodes. *Études Philosophiques*, 97: 193–213, 2011.
2. A. Arana. Purity in arithmetic: some formal and informal issues. In G. Link, editor, *Formalism and beyond. On the nature of mathematical discourse*, pages 315–335. De Gruyter, Berlin, 2014.
3. P. H. Fuss. *Correspondance mathématique et physique de quelques célèbres géomètres du XVI-IIème siècle précédé d'une notice sur les travaux de Léonard Euler, tant imprimeés qu'ineédits et publiée sous les auspices de l'Académie impériale des sciences de Saint-Pétersbourg*. L'imprimerie de l'Académie impériale des sciences, St.-Pétersbourg, 1843.

4. R. Haas. Goldbach, Hurwitz, and the infinitude of primes: weaving a proof across the centuries. *Mathematical Intelligencer*, 36: 54–60, 2014.
5. M. Hallett and U. Majer, editors. *David Hilbert's Lectures on the Foundations of Geometry, 1891–902*. Springer-Verlag, Berlin, 2004.
6. D. Hilbert. Über den Satz von der Gleichheit der Basiswinkel im gleichschenkligen Dreieck. *Proceedings of the London Mathematical Society*, 35: 50–68, 1903.
7. D. Hilbert. Axiomatisches Denken. *Mathematische Annalen*, 78: 405–415, 1918. [English translation by J. Fang in *Philosophia Mathematica*, 7 (No. 1–2): 1–12, 1979].
8. A. Hurwitz. *Übungen zur Zahlentheorie, 1891–1918*, volume 32 of *Schriftenreihe der ETH-Bibliothek*. ETH Zürich University Archives, Zürich, 1999. Transcribed by Barbara Aquilino, prepared by Herbert Funk and Beat Glaus.
9. R. Kaye. *Models of Peano Arithmetic*. Oxford University Press, Oxford, 1991.
10. H. Scheffler. *Beiträge zur Zahlentheorie, insbesondere zur Kreis- und Kugelteilung mit einem Nachtrage zur Theorie der Gleichungen*. F. Foerster, Leipzig, 1891.

Victor Pambuccian got his Ph. D. in mathematics in 1993 at the University of Michigan and is mathematics professor at the West campus of Arizona State University. His research has been largely on the axiomatic foundation of geometry, with a few incursions into weak arithmetics. He has also translated poetry from several languages, and is the editor and translator of *Something is still present and isn't, of what's gone. A bilingual anthology of avant-garde and avant-garde inspired Rumanian poetry*. Aracne editrice, Rome, 2018.