FOUR PROOFS OF EUCLID'S THEOREM

Aidan Rocke
aidanrocke@gmail.com

June 22, 2021

ABSTRACT

Many scientists are familiar with Euclid's theorem of the infinitude of primes. But, some proofs are more insightful than others. In this article, I shall expand upon four different proofs which emphasise different aspects of the infinitude of primes.

1 Euler's proof of the infinitude of primes

A proof by Euler relies on the fundamental theorem of arithmetic, that each integer has a unique prime factorisation.

His proof is as follows:

$$\prod_{p \in \mathbb{P}} \frac{1}{1-\frac{1}{p}} = \prod_{p \in \mathbb{P}} \sum_{k \geq 0} \frac{1}{p^k} = \sum_{n} \frac{1}{n} \tag{1}$$

Now, since the Harmonic series diverges and $\frac{p}{p-1} \leq 2$ we must conclude that there are infinitely many primes.

2 Erdős' proof

Erdős' insight is that if there were finitely many primes there would not be enough to generate infinitely many integers. To be precise, let's suppose the set of primes $\mathbb{P}$ is finite so we have $\mathbb{P} = {p_i}_{i=1}^k$ and each integer N may be expressed as:

$$N = \prod_{i=1}^{K} p_i^{\alpha_i} \tag{2}$$

and as α_i is either odd or even, we may express N as:

$$N = \big(\prod_{i=1}^{K} p_i^{e_i}\big) \cdot s^2 \tag{3}$$

where $e_i \in \{0,1\}$ so $\prod_{i=1}^{K} p_i^{e_i}$ is square-free.

Now, since $s \leq \sqrt{N}$ and there are only 2^k possible products $\prod_{i=1}^{K} p_i^{e_i}$ we may conclude that:

$$\forall n \leq N, n \in [1, 2^k \cdot \sqrt{N}] \implies N \leq 2^k \cdot \sqrt{N} \tag{4}$$

which brings us to a contradiction as there are infinitely many integers. Although this concludes the proof, it is worth adding that $\prod_{i=1}^{K} p_i^{e_i}$ may express at most k bits of information which suggests the possibility of an information-theoretic proof.

3 Chaitin's proof of the infinitude of primes

3.1 Lemma: Almost all integers are incompressible

Given that $\mathbb{N}$ is countable and the space of binary strings of finite length $\{0,1\}^*$ is also countable, we may construct a bijection from $\mathbb{N}$ to $\{0,1\}^*$. It follows that every positive integer has a unique binary encoding.

Moreover, almost all positive integers are incompressible since:

$$\forall n \in \mathbb{N}^* \forall k < n, |x \in 0, 1^* : K(x) \geq n - k| \geq 2^n(1 - 2^{-k}) \tag{5}$$

where $|x| = n$, the binary length of x, which may be understood as the machine-code representation of an integer.

Proof:

Let's suppose an integer with binary encoding x has an algorithmic complexity $K(x) \leq n - k$. Given that the number of binary strings of binary length less than $n - k$ is $2^{n-k} - 1 < 2^{n-k}$ we have:

$$2^n - 2^{n-k} = 2^n(1 - 2^{-k}) \tag{6}$$

integers with an algorithmic complexity greater than or equal to $n - k$. As an immediate consequence, for $n > k \geq 10$, more than 99.9% of integers have an algorithmic complexity greater than $n - k$ so less than 1% of integers are compressible.

3.2 Chaitin's proof of Euclid's theorem

Each integer $n \in \mathbb{N}$ may be described by its prime factorisation:

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} \tag{7}$$

so $\pi(n) = k$ assuming that some exponents α_i equal zero.

Given that $p_i \geq 2$,

$$\forall i \in [1, k], \alpha_i \leq \log_2 n \tag{8}$$

and so any exponent may be described using $\log_2 \log_2 n$ bits.

Now, assuming that the value of $\log_2 \log_2 n$ is known the integer n may be described using:

$$k \cdot \log_2 \log_2 n \tag{9}$$

bits.

However, given that most integers are incompressible there are integers of binary length $l = \log_2 n$ which can't be described in fewer than l bits. So we may deduce that:

$$\pi(n) \cdot \log_2 \log_2 n \geq \log_2 n \tag{10}$$

for almost all positive integers $n \in \mathbb{N}$.

This allows us to deduce a useful lower bound on the prime counting function for almost all n:

$$\pi(n) \geq \frac{\log_2 n}{\log_2 \log_2 n} \tag{11}$$

which implies that there are infinitely many prime numbers.

4 Euclid's theorem via the irrationality of Archimedes' constant

If we let $\alpha = -x^2$ where $|\alpha| < 1$,

$$\sum_{n=0}^{\infty} \alpha^n = \frac{1}{1-\alpha} \tag{12}$$

Given that $\arctan(x) = \int_0^x \frac{dx}{1+x^2}$, if we combine the integral form of $\arctan(x)$ with (10) we have:

$$\arctan(x) = \int_0^x \frac{dx}{1+x^2} = \sum_{k=0}^{\infty}(-1)^k \int_0^x x^{2k}dx = \sum_{k=0}^{\infty} \frac{(-1)^k \cdot x^{2k+1}}{2k+1} \tag{13}$$

so for $x = 1$,

$$\frac{\pi}{4} = \arctan(1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + ... \tag{14}$$

Upon closer inspection, (11) simplifies to:

$$\frac{\pi}{4} = \sum_{n=0}^{\infty} \frac{\chi(n)}{n} \tag{15}$$

where $\chi(n) = 0$ if $n \mod 2 = 0$, $\chi(n) = 1$ if $n \mod 4 = 1$ and $\chi(n) = -1$ if $n \mod 4 = 3$.
Now, we may observe:

$$\sum_{n=0}^{\infty} -\frac{1}{p^n} = \frac{1}{1-(-\frac{1}{p})} = \frac{1}{1+\frac{1}{p}} = \frac{p}{p+1} \tag{16}$$

Finally, since $\chi(p = 2) = 0$ and for $p > 2$, $p \mod 4$ is either 1 or 3 we may define:

$$P = \{p \in \mathbb{P} : p \equiv 1 \pmod 4\} \tag{17}$$

$$P' = \{p \in \mathbb{P} : p \equiv 3 \pmod 4\} \tag{18}$$

so (13) may be expressed as:

$$\sum_{n=0}^{\infty} \frac{\chi(n)}{n} = (\prod_{p \in P} \frac{p}{p-1}) \cdot (\prod_{p \in P'} \frac{p}{p+1}) \tag{19}$$

and therefore:

$$\frac{\pi}{4} = \frac{3}{4} \cdot \frac{5}{4} \cdot \frac{7}{8} \cdot \frac{11}{12} ... \tag{20}$$

where each numerator is an odd prime and each denominator is the nearest multiple of 4 with respect to the numerator. It follows that if there were only finitely many primes, π would be a rational number. QED.

References

References:

[1] Debnath, Lokenath (2010), The Legacy of Leonhard Euler: A Tricentennial Tribute, World Scientific.

[2] Aigner, Martin; Ziegler, Günter (2009). Proofs from THE BOOK (4th ed.). Berlin, New York: Springer-Verlag.

[3] Gregory Chaitin. META MATH! The Quest for Omega. Arxiv. 2004.

[4] Lance Fortnow. Kolmogorov Complexity. 2000.