

Number Theory

Section 1.1. Euclid and Primes—Proofs of Theorems

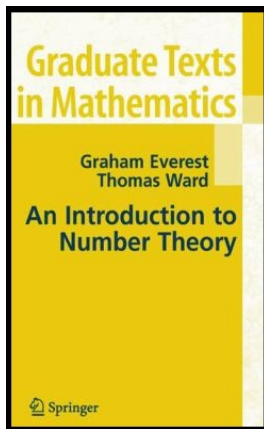


Table of contents

- 1 Theorem 1.2. Euclid's Infinite Primes Theorem, Euclid's Proof
- 2 Theorem 1.2. Euclid's Infinite Primes Theorem, Euler's Proof

Theorem 1.2

Theorem 1.2. Euclid's Infinite Primes Theorem. There are infinitely many primes.

Proof. ASSUME there are only finitely many primes, say $p_1, p_2, \dots, p_r$. Let $N = p_1 p_2 \cdots p_r + 1 > 1$. By the Fundamental Theorem of Arithmetic (Theorem 1.1), N can be expressed as a product of prime numbers and so is divisible by some prime p_k in the list $p_1, p_2, \dots, p_r$. Since p_k also divides $p_1 p_2 \cdots p_k \cdots p_r$, then p_k divides the difference $N - p_1 p_2 \cdots p_r = 1$. But $p_k > 1$ cannot divide 1, a CONTRADICTION. So the assumption that there are only finitely many primes is false and hence there are infinitely many primes, as claimed. □

Theorem 1.2

Theorem 1.2. Euclid's Infinite Primes Theorem. There are infinitely many primes.

Proof. ASSUME there are only finitely many primes, say $p_1, p_2, \dots, p_r$. Let $N = p_1 p_2 \cdots p_r + 1 > 1$. By the Fundamental Theorem of Arithmetic (Theorem 1.1), N can be expressed as a product of prime numbers and so is divisible by some prime p_k in the list $p_1, p_2, \dots, p_r$. Since p_k also divides $p_1 p_2 \cdots p_k \cdots p_r$, then p_k divides the difference $N - p_1 p_2 \cdots p_r = 1$. But $p_k > 1$ cannot divide 1, a CONTRADICTION. So the assumption that there are only finitely many primes is false and hence there are infinitely many primes, as claimed. □

Theorem 1.2

Theorem 1.2. Euclid's Infinite Primes Theorem. There are infinitely many primes.

Proof. ASSUME there are only finitely many primes, say $p_1, p_2, \dots, p_r$.

Consider the product $X = \prod_{k=1}^r \left(1 - \frac{1}{p_k}\right)^{-1}$. Since this is a finite product, the X is finite. Notice that each term can be written as the sum of a convergent geometric series:

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots$$

Notice that for any fixed $K \in \mathbb{N}$, we have

$$\frac{1}{1 - \frac{1}{p}} \geq 1 + \frac{1}{p} + \frac{1}{p^2} + \dots + \frac{1}{p^K}.$$

Theorem 1.2

Theorem 1.2. Euclid's Infinite Primes Theorem. There are infinitely many primes.

Proof. ASSUME there are only finitely many primes, say $p_1, p_2, \dots, p_r$.

Consider the product $X = \prod_{k=1}^r \left(1 - \frac{1}{p_k}\right)^{-1}$. Since this is a finite product, the X is finite. Notice that each term can be written as the sum of a convergent geometric series:

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots$$

Notice that for any fixed $K \in \mathbb{N}$, we have

$$\frac{1}{1 - \frac{1}{p}} \geq 1 + \frac{1}{p} + \frac{1}{p^2} + \dots + \frac{1}{p^K}.$$

Theorem 1.2 (continued 1)

Proof (continued). Substituting the previous inequality into the representation of X we have

$$\begin{aligned}
 X &\geq \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^K}\right) \cdot \left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots + \frac{1}{3^K}\right) \\
 &\quad \cdot \left(1 + \frac{1}{5} + \frac{1}{5^2} + \cdots + \frac{1}{5^K}\right) \cdots \left(1 + \frac{1}{p_r} + \frac{1}{p_r^2} + \cdots + \frac{1}{p_r^K}\right) \\
 &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{2^K 3^K 5^K \cdots p_r^K} \\
 &= \sum_{n \in \mathcal{N}(K)} \frac{1}{n},
 \end{aligned}$$

where $\mathcal{N}(K) = \{n \in \mathbb{N} \mid n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, 0 \leq e_i \leq K \text{ for all } i\}$. Notice that by the Fundamental Theorem of Arithmetic, the elements of $\mathcal{N}(K)$ are distinct.

Theorem 1.2 (continued 2)

Theorem 1.2. Euclid's Infinite Primes Theorem. There are infinitely many primes.

Proof (continued). Given an $n \in \mathbb{N}$, if K is large enough (and under our assumption of a finite number of primes), we have that $X \geq \sum_{n=1}^{\infty} \frac{1}{n}$. Since the harmonic series diverges to infinity, the X must be infinity, a CONTRADICTION. So the assumption that there are only finitely many primes is false and hence there are infinitely many primes, as claimed. $\square$