1
How Many Prime Numbers Are There?

The answer to the question of how many prime numbers exist is given by the fundamental theorem:

There exist infinitely many prime numbers.

I shall give several proofs of this theorem (plus three variants) by famous, but also by forgotten, mathematicians. Some proofs suggest interesting developments; other proofs are just clever or curious. There are of course more (... but not quite infinitely many) proofs of the existence of infinitely many primes.

I. Euclid's Proof

Euclid's Proof. Suppose that $p_1 = 2 < p_2 = 3 < \cdots < p_r$ are all the primes. Let $P = p_1 p_2 \cdots p_r + 1$ and let p be a prime dividing P; then p cannot be any of $p_1, p_2, \ldots, p_r$, otherwise p would divide the difference $P - p_1 p_2 \cdots p_r = 1$, which is impossible. So this prime p is still another prime, and $p_1, p_2, \ldots, p_r$ would not be all the primes. □

Euclid's proof is pretty simple; however, it does not give any information about the new prime found in each stage, only that it is at most equal to the primes already found. Thus, it may be that $P = p_1 p_2 \cdots p_n + 1$ is itself a prime (for some n), or that it is composite (for other indices n). I shall examine this and similar questions in Section VIII of this chapter.

Euclid's proof has of course many variants. Here is one: Let $q_1 = 3$, $q_2 = q_1 - 1 = 2$, $q_3 = q_1 q_2 - 1 = 5$; more generally let q_{n+1} be a prime dividing $Q = q_1 q_2 \cdots q_n - 1$. Then q_{n+1} is differ-

P. Ribenboim, *The New Book of Prime Number Records*

ent from $q_1, \ldots, q_n$, so the process may be continued and gives a proof that there are infinitely many primes.

Another very elegant variant was given by Kummer in 1878.

Kummer's Proof. Suppose that there exist only finitely many primes $p_1 < p_2 < \cdots < p_r$. Let $N = p_1 p_2 \cdots p_r > 2$. The integer $N - 1$, being a product of primes, has a prime divisor p_i in common with N; so, p_i divides $N - (N - 1) = 1$, which is absurd! □

This proof, by an eminent mathematician, is like a pearl, round, bright, and beautiful in its simplicity.

A proof similar to Kummer's was given in 1890 by Stieltjes, another great mathematician.

Stieltjes' Proof. Assume that $p_1, p_2, \ldots, p_r$ are the only existing primes. Let $N = p_1 p_2 \cdots p_r$ and let $N = mn$ be any factorization of N (with $1 \leq m, n$). Each prime p_i divides one, but not both, numbers m, n. Then $m + n$ is not divisible by any of the existing primes, which is absurd since $m + n \neq 1$. □

II. Goldbach Did It Too!

The idea behind the proof is very simple and fruitful. It is enough to find an infinite sequence of natural numbers $a_1, a_2, \ldots, a_n, \ldots$, greater than 1, that are pairwise relatively prime (i.e., without a common prime factor). So, if q_1 is a prime dividing a_1, if q_2 is a prime dividing a_2, etc., then $q_1, q_2, \ldots$ are all different.

The point is that the greatest common divisor is calculated by successive euclidean divisions and this does not require knowledge of the prime factors of the numbers.

Nobody seems to be the first to have a good idea—especially if it is simple. I thought it was due to Pólya and Szegö (see their book, 1924). E. Specker called my attention to the fact that Pólya used an exercise by Hurwitz (1891). But, W. Narkiewirz just told me that in a letter to Euler (July 20/31, 1730), Goldbach wrote the proof given below using Fermat numbers—this may well be the only written proof of Goldbach.