Nineteen proofs there are infinitely many primes

(each in nineteen seconds)

Carl Joshua Quines

July 24, 2019

In all proofs, p is a prime. Many proofs use contradiction, assuming there are finitely many primes $p_1, p_2, \ldots, p_k$.

1. (Hermite) The smallest prime divisor of $n! + 1$ is greater than n.
2. (Euclid) Multiply all the primes and add 1. This number is relatively prime to each prime, contradiction.
3. (Kummer) If the product of all the primes was N, then some prime p divides both N and $N - 1$, so it also divides 1, contradiction.
4. (Scimone) Let N be the product of all the primes. But $\sum \frac{N}{p}$ is relatively prime to each one.
5. (Pinasco) Do the sieve of Eratosthenes. The density of integers removed after removing k primes is $(1-1/p_1)(1-1/p_2)\cdots(1-1/p_k)$, by the Chinese remainder theorem. This is less than 1, so one of the remaining integers is prime.
6. (Goldbach) The numbers $F_n = 2^{2^n} + 1$ satisfy $F_{n+1} - 2 = F_0 F_1 \cdots F_n$, so any two are relatively prime. Choose a prime divisor of each F_n.
7. (Saidak) Let $a_1 = 2$, and define $a_n = a_{n-1}\,(a_{n-1} + 1)$. As a_{n-1} and $a_{n-1} + 1$ are relatively prime, their product has more prime factors than a_{n-1}.
8. (in Engel) The numbers $a_n = 2^{2^{n+1}} + 2^{2^n} + 1$ satisfy $a_n = \left(2^{2^n} - 2^{2^{n-1}} + 1\right) a_{n-1}$. The two factors are relatively prime, so a_n has at least n prime factors.
9. (Wunderlich) Let $a_n = 2^n - 1$, and observe $\gcd(a_m, a_n) = a_{(m,n)}$. So $a_{p_1}, \ldots, a_{p_k}$ are pairwise relatively prime. There are only k primes, so each a_{p_i} has only one prime factor. But $a_{11} = 23 \cdot 89$.
10. (Euler) If the product of all primes was N, then $\phi(N) = \prod p_i - 1 \geq 2^{k-1} \geq 2$. So some integer less than N is relatively prime to N, and also each prime.
11. (IMO 1971/3) Consider $2^{(p_1-1)(p_2-1)\cdots(p_k-1)} - 3$. By Fermat's little theorem, this is $-2 \bmod p_i$, so it is relatively prime to each prime.
12. (Folklore) Let p be the largest prime. Some prime q divides $2^p - 1$. Then $2^p \equiv 1 \pmod{q}$, hence $p \mid q - 1$ so $q > p$, contradiction.

13. (Euler) By unique factorization,

$$\prod_p \left(1 - \frac{1}{p}\right)^{-1} = \prod_p \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \sum_{n=1}^{\infty} \frac{1}{n},$$

which diverges, so the leftmost product can't be finite.

14. (Euler) Using similar manipulations and a well-known identity, we get

$$\prod_p \left(1 - \frac{1}{p^2}\right)^{-1} = \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots\right) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

But π^2 is irrational, so the leftmost product can't be finite.

15. (Whang) By de Polignac's formula,

$$\nu_p(n!) = \sum_{e=1}^{\infty} \left\lfloor \frac{n}{p^e} \right\rfloor \le \sum_{e=1}^{\infty} \frac{n}{p^e} = \frac{n}{p-1} \le n \implies \prod_p p^{\nu_p(n!)} \le \prod_p p^n.$$

This is $n!$ on the left and $(p_1 p_2 \cdots p_k)^n$ on the right. But by Stirling's approximation, $n!$ grows larger than any constant raised to n.

16. (Erdős) Each positive integer less than N be written as ab^2, where a is squarefree and $b^2 < N$. There are 2^k choices for a, as it's a product of distinct primes, and $\sqrt{N}$ choices for b, so $2^k\sqrt{N}$ choices in total. For large N, this is less than N.

17. (Perott) Let k be the number of primes less than N. The number of squarefree integers less than N is at least

$$N - \sum_{p \le N} \left\lfloor \frac{N}{p^2} \right\rfloor \ge N\left(1 - \sum_{p \le N} \frac{1}{p^2}\right) > N\left(1 - \sum_{n=2}^{\infty} \frac{1}{n^2}\right) > \frac{N}{3}.$$

But there are at most 2^k squarefree integers. So $k > \log_2 \frac{N}{3}$.

18. (Thue) Say $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} < 2^m$ for some m. Then $e_1, e_2, \ldots, e_k < m$, so there are at most m^k possibilities for n. For large enough m, $m^k < 2^m$, contradiction.

19. (Mercer) Let $a + b\mathbb{Z}$ be the set of integers congruent to a modulo b. Let $N(p) = (1 + p\mathbb{Z}) \cup (2 + p\mathbb{Z}) \cup \cdots \cup ((p-1) + p\mathbb{Z})$. Then

$$\{-1, 1\} = N(p_1) \cap N(p_2) \cap \cdots \cap N(p_k),$$

but the intersection of two $a + b\mathbb{Z}$s is either empty or is another $a + b\mathbb{Z}$ itself.

Notes

Meštrović in his article "Euclid's theorem on the infinite of primes: A historical survey of the proofs (300 B.C.–2017)" provides references for each of these proofs, and 163 more of them.

Pinasco's proof counts the number of integers less than N after removing k primes using the principle of inclusion–exclusion; here the proof is adapted as a density argument instead.

The ninth proof is cited in Engel's book *Problem Solving Strategies* to be from a "recent German contest", though I couldn't find which one.

IMO 1971 Problem 3 is actually about finding an infinite set of positive integers of the form $2^n - 3$, each pair of which are relatively prime. The problem itself proves there are infinitely many primes, but this adaptation proves it more directly.

I first saw the thirteenth proof from *Proofs from the Book* by Aigner and Ziegler. They don't cite a specific source, citing the result as folklore.

The last proof is Mercer's adaptation of Furstenburg's topological proof, written without mentioning any topological stuff. The original proof was constructing a topology on the integers, where the open sets are $a + b\mathbb{Z}$; the conclusion follows from the fact that the intersection of two open sets is an open set.

Thanks to Kevin Chang for inspiring me to do this.