Example 59. (Euclid) There are infinitely many primes.

Proof. Assume (for contradiction) there is only finitely many primes: $p_1, p_2, \ldots, p_n$.
Consider the number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.
Each prime p_i divides $N - 1$ and so p_i does not divide N.
Thus any prime dividing N is not on our list. Contradiction. □

Historical note. This is not necessarily a proof by contradiction, and Euclid (300BC) himself didn't state it as such. Instead, one can think of it as a constructive machinery of producing more primes, starting from any finite collection of primes.

A variation. Can we replace $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ in the proof with $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1$? Yes! (If $n \geqslant 2$.)

Playing with numbers.

$2 + 1 = 3$ is prime. $2 \cdot 3 + 1 = 7$ is prime. $2 \cdot 3 \cdot 5 + 1 = 31$ is prime. $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ is prime. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ is prime. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ is not prime.

Let $P_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ where p_i is the ith prime. If P_n is prime, it is called a primorial prime. We have just checked that P_1, P_2, P_3, P_4, P_5 are primes but that P_6 is not a prime.

The next primorial primes are $P_{11}, P_{75}, P_{171}, P_{172}$. It is not known whether there are infinitely P_n which are prime.

More shamefully, it is not known whether there are infinitely many P_n which are not prime.

See, for instance: http://mathworld.wolfram.com/PrimorialPrime.html

Example 60. $(p, p+2)$ is a twin prime pair if both p and $p+2$ are primes.

Just making sure. $(2,3)$ is the only pair $(p, p+1)$ with p and $p+1$ both prime. (Why?!)

Some twin prime pairs. $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, $(71,73)$, $(101,103)$, ...

Largest known one: $\underbrace{3756801695685}_{3 \cdot 5 \cdot 43 \cdot 347 \cdot 16785299} \cdot 2^{666669} \pm 1$ ($200,700$ decimal digits; found 2011)

Twin prime conjecture. Euclid already conjectured in 300 BCE that there are infinitely many twin primes. Despite much effort, noone has been able to prove that in more than 20 centuries.

Recent progress. It is now known that there are infinitely many pairs of primes (p_1, p_2) such that the gap between p_1 and p_2 is at most 246 (the break-through in 2013 due to Yitang Zhang had $7 \cdot 10^7$ instead of 246).

The following two famous results say a bit more about the infinitude of primes.

- **Bertrand's postulate**: for every $n > 1$, the interval $(n, 2n)$ contains at least one prime.

  conjectured by Bertrand in 1845 (he checked up to $n = 3 \cdot 10^6$), proved by Chebyshev in 1852

  Comment.

  Advanced comment. Let $\pi(x)$ be the number of primes $\leqslant x$. It follows from Betrand's postulate that

  $$\pi(2^n) \geqslant n.$$

  To prove that, note that 2 is a prime and that each of the (disjoint!) intervals $(2,4)$, $(4,8)$, $(8,16)$, ..., $(2^{n-1}, 2^n)$ contains at least one prime.

  This is a very poor bound. For instance, we find $\pi(2^{20}) \geqslant 20$ where 2^{20} is a little bigger than 10^6. Compare that to the actual numbers in the next item.

- **Prime number theorem**: up to x, there are roughly $x/\ln(x)$ many primes

  proportion of primes up to 10^6: $\frac{78,498}{10^6} = 7.850\%$ vs the estimate $\frac{1}{\ln(10^6)} = \frac{1}{6\ln(10)} = 7.238\%$

  proportion of primes up to 10^9: $\frac{50,847,534}{10^9} = 5.085\%$ vs the estimate $\frac{1}{\ln(10^9)} = 4.825\%$

  proportion of primes up to 10^{12}: $\frac{37,607,912,018}{10^{12}} = 3.761\%$ vs the estimate $\frac{1}{\ln(10^{12})} = 3.619\%$

  Advanced comment. Let $\pi(x)$ be the number of primes $\leqslant x$. Then the PNT states that

  $$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

  Comment. Chebyshev actually tried to prove the PNT (and succeeded in showing that the quotient in the above limit is bounded, for large x, by constants close to 1). However, the PNT was not proved until 1896 by Hadamard and, independently, de la Vallée Poussin, who both used new ideas due to Riemann.

Theorem 61. The gaps between primes can be arbitrarily large.

Proof. Indeed, for any integer $n > 1$,

$$n! + 2, \quad n! + 3, \quad \ldots, \quad n! + n$$

is a string of $n - 1$ composite numbers. Why are these numbers all composite!? $\square$

Comment. Notice, however, how very large (compared to the gap) the numbers brought up in the proof are!

Armin Straub
straub@southalabama.edu