Euclid's Proof of the Infinity of the Set of Prime Numbers and its Application to the Problem of the Infinity of the Set of Twin Prime Numbers, Denise Vella-Chemla, September 2025

Everyone knows Euclid's proof of the infinity of the set of prime numbers (see its translation in the Appendix).

Let's try using an argument similar to Euclid's to prove the infinity of the set of twin prime numbers.

1. Statement

Two prime numbers whose difference is 2 are called twin primes.

Examples:

- 3 and 5 are twin prime numbers.
- 29 and 31 are twin prime numbers.

The twin prime conjecture states that there are infinitely many pairs of twin primes.

We will call the "pair of twins" [1] the even number (which, except for 4 between 3 and 5, is always equally divisible by 3) that is between two twin primes. The "even" of the twin primes 3 and 5 is 4, that of 29 and 31 is 30.

We will now attempt to prove the twin prime conjecture using an argument similar to Euclid's to prove the infinitude of the set of prime numbers.

2. Euclid and the infinity of the set of pairs of twins

Let us call $\mathcal{P}$ the set of prime numbers.

Suppose that the set $\mathcal{PP} = \{k \mid k-1 \in \mathcal{P} \text{ et } k+1 \in \mathcal{P}\}$, i.e., the set of pairs of twin primes, is finite. Let us provide the extension definition of $\mathcal{PP}$:

$$\mathcal{PP} = \{4, 6, 12, 18, 30, 42, \ldots, \mathrm{pp}_{\max}\}.$$

We call $\mathrm{pp}_{\max}$ the largest element of $\mathcal{PP}$, i.e., the largest pair of twin primes. $\mathrm{pp}_{\max} - 1$ and $\mathrm{pp}_{\max} + 1$ are two prime numbers.

Let's calculate

$$\mathrm{Prod}_+ = \left(\prod_{\substack{p \in \mathcal{P} \\ p \leq \mathrm{pp}_{\max}+1}} p \right) + 1$$

[1] There is the wish to make a pun here, because of the sounding similarity of the words pair-père in french (even and father in english so the pun doesn't work.

and

$$\mathrm{Prod}_- = \left(\prod_{\substack{p \in \mathcal{P} \\ p \leq \mathrm{pp}_{\max}+1}} p \right) - 1$$

which are the successor and predecessor of the product of all prime numbers less than the prime number $\mathrm{pp}_{\max} + 1$.

In Euclid's proof, there are two possibilities for Prod_+ and Prod_-. Let, in the first case, they are two prime numbers (the first has remainder $+1$ in any Euclidean division by a prime number p with $p \leq \mathrm{pp}_{\max} + 1$, and the second has remainder $p - 1$ in any Euclidean division by a prime number p with $p \leq \mathrm{pp}_{\max} + 1$. Let, in the second case, each of them has a prime divisor that is not in the set $\mathcal{PP}$, let p be the prime divisor of Prod_+ and q be the prime divisor of Prod_-.

In the first case, we have found a number $\displaystyle\prod_{\substack{p \in \mathcal{P} \\ p \leq \mathrm{pp}_{\max}+1}} p$, which is an even number between two primes, and which does not belong to the set $\mathcal{PP}$, which contradicts the hypothesis that $\mathcal{PP}$ is a finite set of even primes. But in the second case, we cannot deduce that we have found a new even of primes, because we know nothing about the prime divisors p and q. We cannot therefore extend Euclid's proof of the infinity of the set of prime numbers to prove the infinity of the set of pairs of twin primes.

3. Proof of the infinity of the set of pairs of twin primes using a countable infinity of congruence systems

There are infinitely many prime numbers; the set of prime numbers is again denoted $\mathcal{P}$.

Consider the infinity of congruence systems defined as follows:

$$\begin{cases} x_1 & \equiv & 0 \pmod 2 \ ; \\ x_2 & \equiv & 0 \pmod 3 \ ; \\ x_3 & \equiv & 0 \vee 2 \vee 3 \pmod 5 \ ; \\ x_5 & \equiv & 0 \vee 2 \vee 3 \vee 4 \vee 5 \pmod 7 \ ; \\ \quad \vdots & & \\ x_k & \equiv & 0 \vee 2 \vee 3 \vee \ldots \vee p_k - 2 \pmod{p_k} \ ; \\ \quad \vdots & & \end{cases}$$

In the system above, the symbol $\vee$ represents the combinatorial disjunction of all congruence systems that can be written by considering in each system only a single number to be taken from each disjunction of numbers.

We can number each of the systems in question by putting them in bijection with $\mathbb{N}$ (lexicographic numbering according to the usual order on integers applied to disjunctions of remainders).

Now, each of these systems allows, by applying the Chinese remainder theorem, to obtain at least one (in fact, infinitely many) solution to the congruence system in question. This number x is a

pair of twin primes because it satisfies the equation

$$(x-1)(x+1) \not\equiv 0 \pmod{\prod_{p_k \in \mathcal{P}} p_k},$$

which makes $x-1$ and $x+1$ both prime.

There are therefore at least countably infinite pairs of twin primes.

For examples (finite but infinitely completable by congruences to the solution, according to all prime numbers greater than the largest prime number used in the system of a finite number of congruences) of such congruence systems, see the note
Relative Goldbach Conjecture versus Absolute Infinity of the Set of Pairs of Twin Primes ,
which shows that the problem of the infinitude of the set of twin primes is the "absolute" variant of Goldbach's conjecture: to find a pair of twin primes, we seek a solution to a system of congruence of the form $(x-1)(x+1) \not\equiv 0 \pmod{p_k, \forall p_k \in \mathcal{P}}$ while to find a Goldbach decomposing system of n greater than $\sqrt{n}$, we seek a solution of a congruence system of the form $x(n-x) \not\equiv 0 \pmod{p_k, \forall p_k \in \mathcal{P} \cap [2..\sqrt{n}]}$.

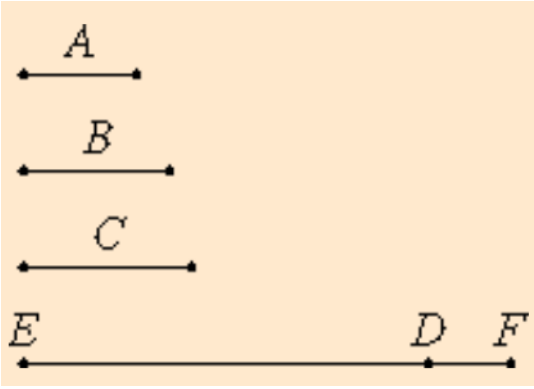
For the proof of this last assertion, please refer to the note

proof of the characterization of Goldbach decomposites greater than $\sqrt{n}$ of an even number n .

Appendix: Euclid's Proof of the Infinity of the Set of Prime Numbers

Proposition 20 of book IX *of Euclid's Elements*:

The prime numbers are more numerous than any possible multitude that would be assigned to their set.
Let A, B, and C be three prime numbers.
I say that there are more of prime numbers than just A, B, and C.
Let DE be the smallest number measured by both A, B, and C. Let the unit DF be added to DE.



Then EF is either a prime number or a composite number.
First, suppose EF is a prime number. Then A, B, C and EF are prime numbers, which is more than just A, B, C.

(VII.31) Now, suppose EF is composite. Then EF is measured by some prime number. Suppose EF is measured by the prime number G.
I say that G is not equal to any of the numbers A, B, and C.
Suppose it could be. Now, A, B and C measure DE, so G also measures DE. But it also measures EF. Therefore, G, being a number, measures their remainder, the unit DF, which is absurd.
Therefore G is not equal to any of the numbers A, B, and C. And by hypothesis, G is a prime number. Therefore, the numbers A, B, C, and G are prime numbers, which is more than the initial multitude of prime numbers that was assigned to only the numbers A, B, and C.
Therefore, the prime numbers are greater in number than any possible multitude that can be assigned to them.