Infinitude of primes

Infinitude of primes

As early as the ancient Greek period, mathematicians already knew that there are infinitely many prime numbers.

Theorem 2.4.1 (Euclid)

There are infinitely many prime numbers.

Theorem 2.4.1 (Euclid)

There are infinitely many prime numbers.

Euclid's proof. Suppose for the sake of contradiction that there are only finitely many prime numbers, say

$$p_1, p_2, \cdots, p_n.$$

Then consider $P = p_1 \cdots p_n + 1$. By the 2-out-of-3 principle, P must be coprime to each prime p_i. This is impossible since $P > 1$ must have a prime divisor. $\square$

Theorem 2.4.1 (Euclid)

There are infinitely many prime numbers.

So the Hasse diagram of divisibility of positive integers is an *infinite* dimensional diagram!

One may further ask if there are infinitely many prime numbers in a specific sequence.

One may further ask if there are infinitely many prime numbers in a specific sequence.

Theorem 2.4.2 (Infinitude of primes in arithmetic progression)

If a, b are coprime positive integers, then there are infinitely many prime numbers in the arithmetic progression

$$a, a+b, a+2b, \cdots$$

Note that the coprime condition is necessary, otherwise each term in the arithmetic progression will be a multiple of $\gcd(a, b)$ and hence can contain at most one prime number.

Theorem 2.4.2 (Infinitude of primes in arithmetic progression)

If a, b are coprime positive integers, then there are infinitely many prime numbers in the arithmetic progression

$$a, a + b, a + 2b, \cdots$$

Note that the coprime condition is necessary, otherwise each term in the arithmetic progression will be a multiple of $\gcd(a, b)$ and hence can contain at most one prime number.

The proof of the theorem is beyond the scope of this course. However, some special cases can be proved using variants of Euclid's proof. For example, see problem 4 from Chapter 2 in the textbook for the case $a = 3, b = 4$.

Instead of consider primes in arithmetic progression, one can also consider arithmetic progressions in primes.

Instead of consider primes in arithmetic progression, one can also consider arithmetic progressions in primes.

Theorem 2.4.3 (Green-Tao, 2008)

The set of prime numbers contains infinitely many arithmetic progressions of length k, for all positive integer k.

Example 2.4.4 (Landau's problem 4)

Look at this sequence n^2+1

$$1, 2, 5, 10, 17, 26, 37, \cdots$$

they are squares plus one. It seems there are infinitely many primes in this sequence. But no one knows how to prove.

Example 2.4.5 (Mersenne primes)

Look at this sequence $2^n - 1$

$$3, 7, 15, 31, 63, 127, 255, \cdots$$

they are powers of 2 minus one. Primes in this sequence are called *Mersenne primes*. How many Mersenne primes are there? No one knows. As of now, only 51 Mersenne primes are found, the largest one is $2^{82589933} - 1$ (GIMPS 2018).

Mersenne primes are closed related to perfect numbers.

Definition 2.4.6

Let n be a positive integer.

- Say n is *perfect* if the sum of its *proper* divisors $= n$.
  e.g. $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$, 496, 8128, 33550336, ...
- Say n is *deficient* if the sum of its *proper* divisors $< n$.
  e.g. all primes are deficient
- Say n is *abundant* if the sum of its *proper* divisors $> n$.
  e.g. $12 < \underbrace{1 + 2 + 3 + 4 + 6}_{= 16}$, 18, 20, 24, 30, 36, ...

Let n be a positive integer. We will use M_n to denote the candidate of Mersenne prime $2^n - 1$. We will see later than for M_n to be a prime, n has to be a prime.

Theorem 2.4.7 (Euclid-Euler)

An even natural number N is perfect if and only if it has the form $N_p := 2^{p-1}M_p$, where M_p is a Mersenne prime.

This theorem tells us that even perfect numbers are one-one corresponding to Mersenne primes. It is still unknown whether there is any odd perfect numbers.