Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

January 23, 2023

What we have seen last week

- Hasse diagram
- Division network of positive integers
- Prime numbers
- Prime factorization $\nu_p : \mathbb{Z}_+ \to \mathbb{N}$
- Translation between $(\mathbb{Z}_+, \cdot, 1, |)$ and $(\mathbb{N}, +, 0, \leqslant)$

Today's topics

- Infinitude of primes
- Perfect numbers and Mersenne primes
- Prime number theorem
- Gaps between primes

Infinitude of primes

Infinitude of primes

Theorem 6.1 (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. □

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

Infinitude of primes

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

$a, 2a, 3a, \cdots \rightarrow$ at most one.

Infinitude of primes

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

Theorem 6.2 (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.

Infinitude of primes

Theorem 6.2 (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 $a = 3$, $b = 4$.

Another method (for specific cases): Quadratic Reciprocity Theorem

Infinitude of primes

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

Infinitude of primes

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

Theorem 6.3 (Green-Tao, 2008)

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

$k=1$: ∞-many primes

$a_1, a_2, \cdots, a_k$

$a_i - a_{i-1}$ is a constant.

$a, a+d, a+2d, \cdots, a+(k-1)d.$ $\in \mathbb{P}$

common difference

length k.

Infinitude of primes

Look at this sequence

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

0^2+1 1^2+1 2^2+1 3^2+1 4^2+1 5^2+1 6^2+1

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

Infinitude of primes

Look at this sequence

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

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

Look at this sequence

$$\underset{2^1-1}{3}, \underset{2^3-1}{7}, 15, \underset{2^5-1}{31}, 63, \underset{2^7-1}{127}, \underset{2^8-1}{255}, \cdots$$

$$\underset{2^2-1}{3}, \underset{2^4-1}{15}, \underset{2^6-1}{63}, \underset{2^8-1}{255}$$

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).

Perfect numbers and Mersenne primes

Mersenne primes are closed related to perfect numbers.

Definition 6.4

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 $1 < p$
- Say n is ***abundant*** if the sum of its *proper* divisors $> n$.
  e.g. $12 < 1+2+3+4+6 = 16$, 18, 20, 24, 30, 36, ...

Perfect numbers and Mersenne primes

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 6.5 (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. open conjecture

Distribution of primes

Prime counting

Although there are infinitely many prime numbers, the number of primes below a given bound is finite.

Definition 6.6

The ***prime counting function*** $\pi(x)$ takes a positive real number as input and outputs the number of primes no larger than x.

Example 6.7

- $\pi(\frac{3}{2}) = 0$ since there is no prime $\leqslant \frac{3}{2}$.
- $\pi(3\sqrt{5}) = \pi(6) =$ 3
- $\pi(24) =$ 9

$3\sqrt{5} = \sqrt{45}$

$36 < 45 < 49$

2, 3, 5

2, 3, 5, 7, 11, 13, 17, 19, 23

Q: How to test if n is prime

$\rightsquigarrow$ "primality test"

Distribution of primes

Question (Open)

Can we have an asymptotic formula for $\pi(x)$? Namely, can we find a simple function $f(x)$ such that $\pi(x) \sim f(x)$, i.e.

$$\lim_{x \to \infty} \frac{\pi(x)}{f(x)} = 1?$$

Furhtermore, can we bound the "error" $|\pi(x) - f(x)|$ in terms of x?

Prime number theorem

Theorem 6.8 (Prime number theorem)

Let $\log(\cdot)$ *be the natural logarithm. Then we have* $\pi(x) \sim \frac{x}{\log(x)}$.

First conjectured by Adrien-Marie Legendre (1797 or 1798) and Carl Friedrich Gauss (1792 or 1793). Studied by Pafnuty Chebyshev (1848 and 1850) and Bernhard Riemann (1859). Finally proved by Jacques Hadamard and Charles Jean de la Vallée Poussin (1896) through a study of the Riemann zeta function $\zeta(s)$. After that, several different proofs of it were found.

Prime number theorem

We know that $\pi(1\text{ million}) = 78498$ while $\frac{1\text{ million}}{\log(1\text{ million})} \approx 72382$. You may find the error a bit large.

A much better approximation is given by the ***logarithmic integral***:

$$\mathrm{Li}(x) := \int_2^x \frac{\mathrm{d}\,t}{\log t} \qquad (x \geqslant 2).$$

Indeed, we have $\mathrm{Li}(1\text{ million}) \approx 78627$. The error is smaller than $\frac{\sqrt{1\text{ million}}\log(1\text{ million})}{8\pi} \approx 550$.

$$\lim_{x\to\infty} \frac{x}{\log x} \Big/ \mathrm{Li}(x) = 1$$

Prime number theorem

One important consequence of the ***Riemann hypothesis*** is that

Corollary 6.9 (Lowell Schoenfeld, 1976)

If Riemann hypothesis is true, then for all $x \geqslant 2657$,

$$|\pi(x) - \mathrm{li}(x)| \leqslant \frac{\sqrt{x}\log(x)}{8\pi}.$$

Here $\mathrm{li}(x)$ only differ from $\mathrm{Li}(x)$ by a small constant $\mathrm{li}(2) = 1.045\cdots$.

Gaps between primes

Another direction is to consider the gaps between primes.

The first fact is: the gap between primes can be arbitrarily large.

see: HW 2

Gaps between primes

Another direction is to consider the gaps between primes.

The first fact is: the gap between primes can be arbitrarily large.

Then it is natural to ask: how small could the gap be? Note that every pair of consecutive integers must contain an even number. Hence, the only pair of primes having gap 1 is $(2, 3)$.

Gaps between primes

Another direction is to consider the gaps between primes.

The first fact is: the gap between primes can be arbitrarily large.

Then it is natural to ask: how small could the gap be? Note that every pair of consecutive integers must contain an even number. Hence, the only pair of primes having gap 1 is $(2, 3)$.

How about gap 2?

Definition 6.10

Two primes p, q are called ***twin primes*** if $|p - q| = 2$.

Gaps between primes

Question (Open)

Are there infinitely many twin primes?

$|p-q| = 2$ or $(\leqslant 2)$

The best results so far are:

Theorem 6.11

There infinitely many pairs of primes (p, q) *such that*

$\lvert p - q \rvert \leqslant 70$ *million*	*(Yitang Zhang, 2013)*
$\lvert p - q \rvert \leqslant 600$	*(James Maynard, 2013)*
$\lvert p - q \rvert \leqslant 246$	*(D. H. J. Polymath, 2014)*

After Class Work

Reading materials

- There are many ways to prove ***Euclid's theorem on infiniteness of prime numbers***. If you are interested in, you can start from ***Wikipedia*** or ***ProofWiki***. It is worth mentioning that one method is to show the series $\sum_{p \text{ is prime}} \frac{1}{p}$ of reciprocals of prime numbers ***diverges***.
- The method people used to attack the ***twin prime conjecture*** as well as many other questions in number theory is called the ***Sieve theory***, a central method in ***analytic number theory***.
- We will discuss the divisor sets and multiplicative functions in next lecture. Please read pp. 64–49 of the textbook.