Elementary Number Theory

Modular Arithmetic and the Power of Primes.

Loh Kwong Weng

1 April 2024

Introduction - What is Number Theory?

- Number theory is the study of natural numbers, $\mathbb{N} = \{1, 2, 3, ...\}$, from which we can build everything else.

$$\mathbb{N} \xrightarrow{-} \mathbb{Z} \xrightarrow{\div} \mathbb{Q} \xrightarrow{\text{Real analysis}} \mathbb{R} \xrightarrow{\sqrt{-1}} \mathbb{C}$$

- The building blocks of natural numbers are called **primes**, numbers that cannot be written as a product of two smaller numbers.

Exercise

Verify if $91, 101, 111, 121$ are primes.

- Despite its deceptively simple definition, the study of primes can go to incredible depths, and yet most parts of primes still appear mysterious!

> God made the integers, all the rest is the work of man.
>
> Leopold Kronecker (1823-1891)

Prime factorisation

Why are primes the building blocks of natural numbers? The reason lies within the following theorem, known as the Fundamental Theorem of Arithmetic.

Theorem

Fundamental Theorem of Arithmetic Every integer $N > 1$ can be uniquely decomposed into product of primes. In other words, there exists primes $p_1, p_2, \cdots, p_n$ and integers $\alpha_1, \cdots \alpha_n$ such that

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

Example

Factorise $91, 92, 93, 94$.

Finitely many primes?

This raises a question — is there only finitely many primes? The answer is no, and I would like to share an elegant proof by Euclid back in 2000 years ago.

Euclid's proof

We use proof by contradiction. Suppose there are only finitely many primes, say $p_1, p_2, \cdots, p_n$. Now consider

$$M = p_1 p_2 \cdots p_n + 1.$$

This number is larger than any of $p_1, p_2, \cdots p_n$, but it isn't divisible by any of them, so M must be a prime! This contradicts our assumption that there are only finitely many primes.

Divisibility

When working in integers, addition, substraction and multiplication makes perfect sense. What about division? Well, not always. To find out when division makes sense, we use the notion divisibility.

Definition

We say that an integer b is divisible by some integer a, $a|b$, when there exists an integer n such that $b = na$.

What if division fails? Recall how we dealt with it in primary school — take the remainder. This is known as the Euclidean Algorithm:

$$b = na + m$$

for some integers n, m, where $0 \leq m < a$.

Modular Arithmetic

Definition

We say that two integers a, b are congruent modulo n, $a \equiv b \pmod{n}$ if $n|a-b$. In other words, they leave the same remainder when divided by n.

Addition, substraction and multiplication in $\pmod{n}$ is easy — Perform the calculations like integers, then take the result modulo n. However, there's a caveat with division:

Multiplicative inverse

For any integer a coprime to n, there exists a unique multiplicative inverse a^{-1} such that $a \cdot a^{-1} \equiv 1 \pmod{n}$.

The interesting fact is that inverses behave just like fractions! As an exercise, find the multiplicative inverse of $2, 3, 4, 5, 6$ modulo 13, then find $\frac{4}{5} + \frac{2}{3} \pmod{13}$.

Problems

Now, let's try some problems on number theory.

1. Find all integer solutions to $a^2 + b^2 + 1 = 2024$.
2. (Wilson's theorem) Let p be a prime. Show that $(p-1)! \equiv -1 \pmod{p}$.
3. Let f be a polynomial in integer coefficients. Then $f(x+d) \equiv f(x) \pmod{d}$ for any $x \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$.
4. (Chinese Remainder Theorem) Let m, n be coprime positive integers. Then for any integers a, b there exist a unique integer $0 \leq c < mn$ such that $c \equiv a \pmod{m}$ and $c \equiv b \pmod{n}$. (Hint: consider when $(a, b) = (0, 1), (1, 0)$ first.)
5. Prove that for any positive integer n, there exists n consecutive positive integers, with none of them being a perfect square.

LCM and GCD

Definition

- Least common multiple (LCM) of two integers a, b is the smallest positive integer c such that $a|c$ and $b|c$.
- Greatest common divisor (GCD) of two integers a, b is the largest positive integer c such that $c|a$ and $c|b$.

$\gcd(a, b)$ can be efficiently obtained by repeatedly applying Euclidean Algorithm. Now let's prove the following two results:

Problem

- *Prove that* $lcm(a, b) \cdot \gcd(a, b) = ab$ *for any integer* a, b. *(Hint : Consider prime factorisation)*
- *(Bezout's Lemma) Prove that there exists integers* x, y *such that* $ax + by = \gcd(a, b)$.

Primality Test

How do we check if a number p is prime? The naive way is to check for all $1 \leq a < p$ if $a|p$, which will take $p-1$ operations. One way to optimise this is to note that we only need to check a up to $\sqrt{p}$ (Why?)

Now, consider if we want to generate all primes less than N. Using the above method, we need to check if each of $1, 2, \cdots, N$ is prime, which will take $O(N\sqrt{N})$ time. To optimise this we can use the following:

Sieve of Eratosthenes

Suppose we want to find all primes in the set $\{1, 2, 3, \cdots N\}$. For $a = 1, 2, \ldots, N$, if a is prime then we mark all multiples of a less than N as non-primes. This will take

$$\frac{N}{2} + \frac{N}{3} + \cdots \frac{N}{N} \approx N \ln N$$

operations.

Number-theoretic functions

Number-theoretic function is any function that maps to natural numbers. Here are some common ones:

Example

Let $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ be a positive integers. Then

- The number of positive integer divisors of N,

$$d(N) = \prod_{i=1}^{m} (\alpha_i + 1) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1)$$

- The sum of positive integer divisors of N,

$$\sigma(N) = \prod_{i=1}^{m} (1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i})$$

Try proving why the above results are true.

Euler function & Euler's Theorem

Euler function, $\phi(N)$ is the number of positive integers less than N and coprime to N,

$$\phi(N) = N \cdot \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

Now we present the Euler theorem:

Theorem

Let a be an integer coprime to N. Then $a^{\phi(N)} \equiv 1 \pmod{N}$.

In fact, this theorem generalises the Fermat's Little Theorem, from primes to natural numbers.

In the next slide, we'll try to understand how the RSA algorithm works — It'll require most things we've learnt previously!

The RSA algorithm (Rivest, Shamir, Adleman)

Suppose person A wants to send a message m to B. The RSA public key cryptography can be used to encrypt the message. Here's the procedure:

1. B generates two large primes p, q and compute $N = pq$.
2. B chooses some integer x coprime to $\phi(N) = (p-1)(q-1)$, and computes $y = x^{-1} \pmod{\phi(N)}$
3. B publishes N, x as its public key.
4. A computes $m^x \pmod{N}$ and sends it to B. Here $0 < m < N$ and $(m, N) = 1$, where m is the integer A wants to send.
5. B computes

$$(m^x)^y = m^{xy} = m^{k\phi(N)+1} \equiv m \pmod{N}$$

The effectiveness of this algorithm lies in the difficulty to factorise N and compute $\phi(N)$, so another person can never obtain y from N, x alone.