1. Introduction to Number theory

Number theory is to do with the study of the natural numbers,

$$\mathbb{N} = \{ 1, 2, 3, \dots \}.$$

There are two key operations on the natural numbers, addition and multiplication,

$$+ \colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \qquad \text{and} \qquad \cdot \colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}.$$

Results in number theory are statements about the interaction of the two:

$$\forall n \in \mathbb{N}, x \in \mathbb{N}, y \in \mathbb{N}, z \in \mathbb{N}\ (n > 2, x > 0, y > 0, z > 0) \implies (x^n + y^n \neq z^n)$$

This is a statement of Fermat's last Theorem.

It is a curious fact that if one forgets about multiplication and concentrates just on addition then there is a computer program to decide if the statement is true. On the contrary a famous theorem of Gödel states that it is not possible to prove every true statement in number theory. It is the interaction between addition and multiplication that makes number theory interesting.

It is very easy to state true results in number theory but it is sometime suprisingly challenging to prove them. Herein lies the charm of number theory. There are an enormous number of different techniques ranging for elementary to very sophisticated to prove results in number theory.

Let me start with an easy example of a problem which it is quite likely that no-one will ever solve. Consider the following algorithm.

Two versus three

---

(1) Pick a natural number n.
(2) If the number is one then STOP.
(3) If the number is even then divide it by two and GOTO (2).
(4) If the number is odd but not one then multiply it by three, add one and GOTO (2).

As with any algorithm the most interesting mathematical question is whether or not this algorithm stops after finitely many times or whether or not it continues for ever. To truly understand both the algorithm and the problem, it helps to look at a lot of examples; here are a couple of examples.

Suppose we pick $n = 3$. $3 \neq 1$ so we don't stop. 3 is not even so we don't divide it by 2. So we multiply by 3 and add 1 to get $3 \cdot 3 + 1 = 10$.

Using the obvious notation we get the following sequence of numbers:

$$3 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1.$$

In the end, it is a question of the proportion (or ratio) of the even numbers versus multiples of three.

There are many famous problems and results in number theory.

One striking early result is due to Fermat:

Theorem 1.1. *Every natural number is a sum of four squares.*

Here the square is allowed to be zero. We illustrate this theorem with some the first couple of examples:

$$\begin{aligned} 1 &= 1^2 + 0 + 0 + 0 \\ 2 &= 1^2 + 1^2 + 0 + 0 \\ 3 &= 1^2 + 1^2 + 1^2 + 0 \\ 4 &= 1^2 + 1^2 + 1^2 + 1^2 \\ 5 &= 2^2 + 1^2 + 0^2 + 0^2, \end{aligned}$$

and so on.

Definition 1.2. *Let a and b be two natural numbers.*

*We say that b **divides** a, denoted $b|a$, if there is a natural number c such that $a = bc$. b is called a **divisor** of a.*

Note that 1 divides every natural number, as $a = a \cdot 1$. Note that every natural number divides itself as $a = 1 \cdot a$.

Definition 1.3. *Let $p \in \mathbb{N}$ be a natural number. We say that p is **prime** if it is not equal to one and the only divisors of p are 1 and p.*

Prime numbers have fascinated mathematicians for centuries. Many results in number theory can be reduced to the case of prime numbers. For example, it suffices to check Fermat's last theorem in the case when the exponent is prime. Even though the definition of a prime number is so simple, in fact prime numbers appear quite randomly. Here is a list of the first few prime numbers:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots.$$

There are two interesting features of this sequence. It is clear that primes become more sparse as they increase; one can see this by looking at tables and it makes sense if you think about the sieve of Eratosthenes, where you know all even numbers, all multiples of three, all multiples of five, are not prime (apart from the obvious exceptions, 2, 3, 5, etc). Looking at tables of primes, Gauss guessed the number $\pi(x)$ of primes up to x is approximately given by an integral:

$$\pi(x) \simeq \int_2^x \frac{\mathrm{d}t}{\log t}.$$

In fact this is true and an accurate estimate of the error term is called the prime number theorem.

The second interesting feature is that ood primes sometimes come in pairs, 3, 5; 5, 7; 11, 13, and so on. Any pair of primes p and q such that $q - p = 2$ are called twin primes. The twin prime conjecture states that there are infinitely many twin primes.

Quite recently, Yitang Zhang made a spectacular breakthrough towards the twin prime conjecture. He proved:

Theorem 1.4. *There are infinitely many pairs of primes p and q such that $p < q$ and $q - p < 7 \times 10^7$.*

Building on this work, Tao (conducting a joint effort over the internet) and Maynard reduced the gap seventy million to 246. For the twin prime conjecture we need to get down to a gap of two. Before the work of Zhang, no finite gap was known.