Number Theory

Number theory has been studied since ancient times, and a lot of early number theory was included in Euclid's Elements. It deals with properties of numbers, in particular the integers. Common questions include questions of whether equations have integer solutions, for example, the famous *Fermat's Last Theorem*, proved in 1995? by Andrew Wiles states that there are no non-trivial integer solutions to the equation $a^n + b^n = c^n$ for any $n > 2$. It also deals with properties of divisibility (and more generally, modular arithmetic) and prime numbers. Number theory is divided up into different areas based on the methods used.

Elementary Number Theory

This deals with basic algebra purely number-theoretic concepts, such as primes, divisibility and *modular arithmetic*. Modular arithmetic is the arithmetic of clocks, where two numbers are considered essentially the same (*congruent modulo* n) if their difference is a multiple of n. For example, 8 is congruent to 3 modulo 5 because $8 - 3 = 5$ is a multiple of 5.

Modular arithmetic is important in computer science. For example, the RSA encryption algorithm encodes the message m as m^e modulo n for some fixed integer e, where n is the public key, which is a product of two primes p and q, which form the private key. Without knowing p and q, it is difficult to determine the original message from the encrypted message, but knowing p and q, a theorem known as *Fermat's little theorem* can be used to calculate m.

Algebraic Number Theory

This uses algebraic methods for studying properties of numbers. In particular, it considers extensions of the integers by adding solutions to algebraic equations. This is useful for finding integer solutions to certain polynomial equations. By adding numbers to the integers, we can hope that the polynomials will factorise in these extended integers, making it easier to find integer solutions. A difficulty is that standard properties such as unique prime factorisation no longer apply.

Analytic Number Theory

This uses methods from analysis to prove number theoretic results. Many of these results concern asymptotic properties (approximations that become more accurate for large numbers) of numbers, for example, the proportion of the numbers from 1 to N that are prime is approximately $\frac{1}{\log N}$, with the approximation becoming more and more accurate as N gets larger. Other problems ask questions like Warings problem "Can every positive integer be writen as a sum of k nth powers, for some fixed k (depending on n)? That is, can we write $m = a_1^n + a_2^n + \cdots + a_k^n$?" Explicit bounds for the number k required were calculated by analytic methods involving certain integrals.

One of the most important objects of study in analytic number theory is the Riemann zeta function, defined as $\zeta(x)$ is the sum of $\frac{1}{n^x}$ over all positive integers n, so for example $\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \cdots$ (which can be shown to equal $\frac{\pi^2}{6}$ using Fourier analysis). This function is related to prime numbers because $\zeta(x)$ can be factored as the product of $\frac{1}{1-\left(\frac{1}{p}\right)^x}$ for all prime numbers p. Studying this function gives a lot of information about the distribution of the prime numbers. One of the most important open problems in mathematics is the *Riemann Hypothesis* which is a conjecture about the zeros of this function. There is a $1,000,000 prize offered for anyone who can prove this hypothesis. It would have many important consequences in number theory.