NUMBER THEORY

UNIT 0 INTRODUCTION

The history of number theory dates back to almost as far as the history of mathematics. As its name implies, number theory is the study of the properties of ‘numbers’. For most of the time we shall be dealing with positive integers.

Before we proceed, let us have a feeling of what number theory is about. Listed below are some number theory problems.

- Find the last two digits of 17^{2002}.

- Let n be a natural number. If $2n$ has 28 positive divisors and $3n$ has 30, how many does $6n$ have?

- Show that a natural number N is divisible by 3 if and only if its sum of digits is divisible by 3.

- Prove that there are infinitely many prime numbers.

- Show that the sequence 11, 111, 1111, … contains no perfect squares.

- Find the remainder when 1234^{5678} is divided by 13.

- Find all integers x, y such that $15x^2 - 7y^2 = 9$.

- (IMO 1959) Prove that the fraction $\dfrac{21n+4}{14n+3}$ is irreducible for every natural number n.

- (USAMO 1976) Find all positive integers a, b, c such that $a^2 + b^2 + c^2 = a^2b^2$.

- (APMO 1993) Find all positive integers n such that the equation $x^n + (2+x)^n + (2-x)^n = 0$ has an integer solution.

By now we have a general idea of what 'number theory' is in mind. It concerns things like prime numbers, multiples, divisors, perfect squares, remainders, digits, and so on. Most of these terms are not at all new. So number theory is not a monster nor a stranger; it concerns things that we are familiar with and which are so common in our life; it involves concepts which we have been learning since we were small.

Before we go further let's have some warm-up with our mind. For each of the following group of numbers, find the odd one out. For sure there can be many different answers provided that each one is well justified, but try to find one that appears to be the most reasonable and natural.

(1) 101, 103, 105, 107, 109

(2) 1488, 2566, 3972, 4567, 5080

(3) 2285, 5075, 6228, 7995, 9030

(4) 123, 456, 789, 2345, 6789

(5) 13, 17, 25, 39, 45

There are many different ways to classify people (according to gender, age, nationality, ethnic group, personality, occupation, etc). Analogously, there are many different ways to classify numbers. In fact, these are well illustrated by the examples above.

In (1), you would probably have chosen 105, because all the rest are prime numbers. This gives a way of classifying positive integers — into prime numbers and composite numbers (the number 1 is defined to be neither prime nor composite). The prime numbers are important in the sense that they 'generate' all the positive integers (just like elements 'generate' all the compounds in the world); we learned in primary school that every integer greater than 1 can be written as a product of prime factors, e.g. $180 = 2^2 \times 3^2 \times 5$. Indeed, in many cases we have to consider the prime factorizations of integers in solving problems.

In (2) 4567 is the odd one out: it is an odd number while the rest are all even. The classification of integers into odd and even is one of the simplest and we learnt it at a very early age.

An alternative (but equivalent) interpretation of this classification is according to whether the numbers are divisible by 2 or not. Again, divisibility is another familiar subject that we know for long and which we will see in later units.

Having the concept of divisibility in mind, (3) and (4) become easy. For (3), 6228 is the odd one out, as all the others are divisible by 5 while 6228 is not. For (4), 2345 is the odd one out: it is not divisible by 3 but all the rest are multiples of 3. How do we know that a number is divisible by 3 or 5? Well, we learnt that in primary school. A number is divisible by 5 if and only if its last digit is 0 or 5, while a number is divisible by 3 if and only if its sum of digits is divisible by 3. The explanation to the former is quite simple, but that of the latter needs some arguments, which we will soon study.

How about (5)? Which is the odd one out? Using the above classifications into odd/even numbers or primes or multiples of certain integers does not seem to work. (Of course you can argue like, 17 is the odd one out because it is the only number which is divisible by 17, but definitely this is not a good answer.) But if we divide each of the numbers by 4, we find that 39 leaves a remainder of 3 while all others leave a remainder of 1. Hence 39 is the odd one out. This is the intuitive concept of congruence (or modular arithmetic). According to the remainders upon division by 4, we can classify the integers into four types. Of course, there is no need to restrict ourselves to the case of division by 4, we can divide by any positive integer. (In fact, the concept of congruence is also very useful in other areas of mathematics outside number theory.)

In addition to divisibility and congruence, another main area that we shall study is Diophantine equations. Diophantine was a mathematician of the 2nd century. Diophantine equations are equations in which integer solutions are to be sought. For instance, we want to find positive integers a, b, c satisfying $a+b+c=abc$. It can be shown that the only solutions are permutations of (1, 2, 3). However, if a, b, c can be any integers (not necessarily positive), then there will be infinitely many solutions, such as (0, 1, –1), (0, 2, –2), etc.

In solving for Diophantine equations many techniques and concepts in number theory have to be applied. Usually the difficult part of the problem is not to find out the solutions, but rather to show that those found are all the solutions.

In addition we will also look at some special types of numbers, such as twin primes, Fermat primes and Pythagorean triples. Many questions will pop up when we study these numbers, and some of them remain unsolved to date.