0. Introduction: What is Number Theory?

Number Theory is (of course) primarily the Theory of Numbers: ordinary whole numbers (integers). It is, arguably, the oldest branch of mathematics. Integer solutions to Pythagoras's equation

$$a^2 + b^2 = c^2$$

have been found, systematically listed with all the arithmetic carried out in base 60, on ancient Babylonian clay tablets. There are several different flavours of Number Theory, distinguished more by the methods used than by the problems whose solutions are sought. These are

- *Elementary* Number Theory: using elementary methods only;
- *Analytic* Number Theory: using analysis (real and complex), notably to study the distribution of primes;
- *Algebraic* Number Theory: using more advanced algebra, and also studying *algebraic numbers* such as $1 + \sqrt[3]{2} + \sqrt[17]{17}$;
- *Geometric* Number Theory: using geometric, algebraic and analytic methods; also known as *arithmetic algebraic geometry*.

Andrew Wiles used a vast array of new techniques and previously known results in arithmetic algebraic geometry to solve Fermat's Last Theorem, whose statement is entirely elementary (see below). This is typical of progress in Number Theory, where there have been many cases of entirely new mathematical theories being created to solve specific, and often quite elementary-seeming problems.

This module is mostly elementary with some analytic and algebraic parts. The algebraic approach is pursued further in the module MA3A6 (Algebraic Number Theory). The geometric approach is pursued further in the module MA426 (Elliptic Curves).

Number Theory starts out with simple questions about integers: simple to state, if not to answer. Here are three types of question:

- *Diophantine Equations* are equations to which one seeks integers solutions (or sometimes rational solutions). For example,

(1) $x^2 + y^2 = z^2$ has infinitely many integral solutions (so-called Pythagorean triples); later, we will see how to find them all.

(2) $x^n + y^n = z^n$ has *no* nonzero integer solutions when $n \geq 3$. This is Fermat's Last Theorem, which we will certainly not be proving in these lectures, though we will prove the case $n = 4$.

(3) $y^2 = x^3 + 17$ has exactly 8 integer solutions (x, y), $x = -2, -1, 2, 4, 8, 43, 52$ and one further value which you can find for yourselves. Proving that there are no more solutions is harder; using Sage you can solve this as follows:

```
sage: EllipticCurve([0,17]).integral_points()
```

(4) Every positive integer n can be written as a sum of four squares (including 0), for example

$$47 = 1 + 1 + 9 + 36 = 1^2 + 1^2 + 3^2 + 6^2,$$

but not all may be written as a sum of 2 or 3 squares. Which?

```
sage: sum_of_k_squares(4,47)
```

We will answer the two- and four-square problems later, with a partial answer for three squares.

- Questions about primes, for example

(1) There are infinitely many primes (an ancient result proved in Euclid.)

(2) Is every even number (greater than 2) expressible as the sum of two primes? This was conjectured by Goldbach in 1746 and still not proved, though it has been verified for numbers up to 4×10^{18}; the "weak form" of the conjecture, that every odd number greater than 5 is a sum of three primes, was proved in 2013 by the Peruvian Harald Helfgott.

(3) Are all the Fermat numbers $F_n = 2^{2^n} + 1$ prime (as Fermat also claimed)? Certainly not: the first four are ($F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$) but then $F_5 = 641 \times 6700417$, $F_6 = 274177 \times 67280421310721$, $F_7 = 59649589127497217 \times 5704689200685129054721$, and no more prime values have been discovered in the sequence.

```
sage: [(2^2^n+1).factor() for n in range(9)]
```

(4) How many primes end in the digit 7? Infinitely many? Of the 664579 primes less than 10 million, the number which end in the digits 1, 3, 7 and 9 respectively are 166104, 166230, 166211, and 166032 (that is, 24.99%, 25.01%, 25.01% and 24.98%). What does this suggest?

```
sage: pc=dict([(d,0) for d in range(10)])
sage: for p in prime_range(10^7): pc[p%10]+=1
sage: [(d,pc[d],100.0*pc[d]/sum(pc.values()))
        for d in [1,3,7,9]]
```

(5) Are there infinitely many so-called *prime pairs*: primes which differ by only 2, such as $(3, 5)$, $(71, 73)$ or $(1000000007, 1000000009)$?

- Efficient algorithms for basic arithmetic: many modern applications of Number Theory are in the field of cryptography (secure communication of secrets, such as transmitting confidential information over the Internet). These application rely on the fact that the following two questions, which seem trivial from the theoretical points of view, are not at all trivial when asked about very large numbers with dozens or hundreds of digits:

(1) Primality Testing: given a positive integer n, determine whether n is prime;
(2) Factorization: given a positive integer n, determine the prime factors of n.

In this module, we will study a variety of such problems, mainly of the first two types, while also laying the theoretical foundations to further study.

Basic Notation. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ will denote, as usual, the sets of integers, rational numbers, real numbers and complex numbers. The integers form a ring, the others sets are fields.

$\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 1\}$ is the set of *natural numbers* (positive integers).

$\mathbb{N}_0 = \{n \in \mathbb{Z} \mid n \geq 0\}$ is the set of non-negative integers.

$\mathbb{P}$ will denote the set of (positive) prime numbers: integers $p > 1$ which have no factorization $p = ab$ with $a, b > 1$.

Divisibility: for $a, b \in \mathbb{Z}$ we write $a|b$, and say a *divides* b, when b is a multiple of a:

$$a|b \iff \exists c \in \mathbb{Z} : b = ac.$$

If a does not divide b we write $a \not| b$. The divisibility relation gives a partial order on $\mathbb{N}$ with 1 as the "least" element and no "greatest element".

Congruence: for $a, b, c \in \mathbb{Z}$ with $c \neq 0$ we write $a \equiv b \pmod{c}$ and say that a is congruent to b modulo c if $c|(a-b)$:

$$a \equiv b \pmod{c} \iff c|(a-b).$$

Divisibility and congruence will be studied in detail later.