Diophantus of Alexandria ($\approx 210 - 280$ AD) wrote a book called "Arithmetica" which discussed equations to be solved over the integers or rationals.

Example 19.1. Problem 24 of Book VI, asks to split the number 6 into two (rational) parts, say y and $6 - y$ so that the product of those parts is the difference of a cube minus its (rational) cube root. In other words, find $x, y \in \mathbb{Q}$ such that $y(6 - y) = x^3 - x$.
Trivial solutions include $(x, y) = (0, 0)$ and $(1, 6)$. A nontrivial solution is $(x, y) = (17/9, 26/27)$.

Definition 19.2. A *Diophantine equation* is a polynomial equation (or system of polynomial equations) in n unknowns, for which the desired solutions are restricted to $\mathbb{Z}$ or $\mathbb{Q}$.

19.3. Problems:

- Determine whether or not solutions exist.
- Determine the number of solutions.
- Find a solution efficiently.
- Find all solutions efficiently.

19.4 Linear diophantine equations $ax + by = c$, $a, b, c \in \mathbb{Z}$.

19.5 Simplest non-linear diophantine equation $ax^2 + by = c$.
Example. $3x^2 + 10y = 37$.

Exercise 19.6. Let p be an odd prime, let $n \in \mathbb{Z}_{>1}$ and let $a, b \in \mathbb{Z}$ be such that $p \nmid a$. Write down an efficient algorithm which, given a solution to $ax^2 \equiv b \mod p$, computes a solution to $ax^2 \equiv b \mod p^n$.

19.7 General quadratic diophantine equation $ax^2 + bxy + cy^2 = d$.
This equation reduces to the *Pell equation* $X^2 + DY^2 = N$. The next chunk of the course will be on Pell equations and how to find solutions to them using continued fractions.

Example 19.8. The smallest non-trivial integer solution of $x^2 - 61y^2 = 1$ is (found in the 12th century!)

$$(x, y) = (1766319049, 226153980).$$

19.8 Geometric Methods For example, the $\mathbb{Z}$ solutions to the Pythagoras equation $x^2 + y^2 = z^2$ are in 1-1 correspondence with $\mathbb{Q}$ solutions to $X^2 + Y^2 = 1$. Geometric methods can be used to determine all solutions. Later in the course we will study a generalisation of these geometric methods when we study *elliptic curves*.

19.9 Hilbert's 10th problem. Is there a algorithm to determine whether or not a given Diophantine equation has a solution?
Answer: No (Yuri Matiyasevich, Julia Robinson, Martin Davis, Hilary Putnam, 1950–1970).