ELLIPTIC CURVES: MOTIVATION

A fundamental question is whether an equation with integer coefficients

$$F(x_1, \ldots, x_n) = 0 \qquad (1)$$

has integer solutions; F is a polynomial in variables $x_1, \ldots, x_n$ with integer coefficients.

1. Does (1) have solutions in the integers?

2. Does (1) have solutions in the rationals?

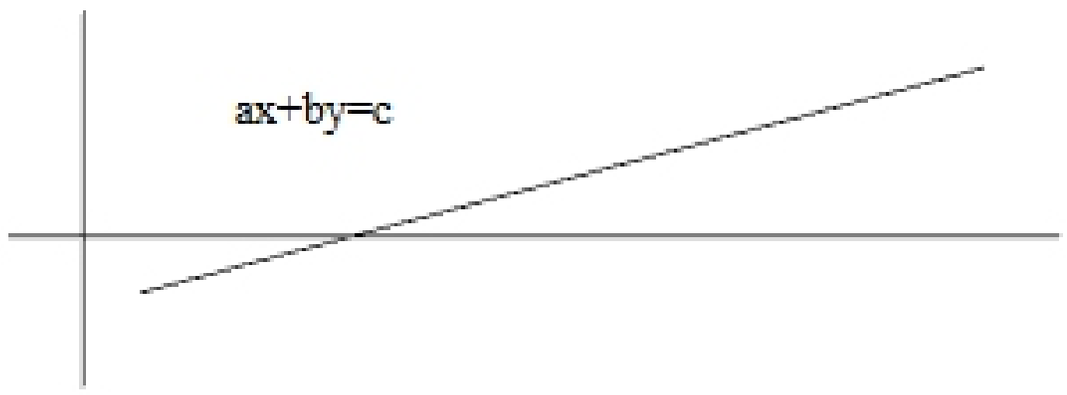
3. Does (1) have infinitely many solutions in the integers?

4. Does (1) have infinitely many solutions in the rationals?

A two variable equation $F(x, y) = 0$ forms a curve in the plane. So we are seeking geometric-arithmetic methods to find solutions.

LINEAR EQUATIONS

$$ax + by = c, \quad a, b, c \in Z$$



- In the integers it has a solution if and only if gcd$(a, b)|c$, in which case it has infinitely many solutions.

- In the rationals it has infinitely many solutions.

EXAMPLES

- $2x+3y=13$ has a solution in the integers. Namely, $x=2, y=3$. It also has solutions in the rationals. For each rational value of x the corresponding value of y is $\frac{13-2x}{3}$.

- $4x-6y=13$ has no solution in the integers, because $\gcd(4,6)=2 \not| 13$. But it has solutions in the rationals.

- Pythagorean triples (X,Y,Z) are triples of integers satisfying $X^2+Y^2=Z^2$. E.g., $(3,4,5)$. This is equivalent to solving $x^2+y^2=1$ in the rationals. The solutions are $x=\frac{1-t^2}{1+t^2}, y=\frac{2t}{1+t^2}$.

- For $n \geq 3$, $X^n+Y^n=Z^n$ has no solution in the integers (Fermat's conjecture). This is equivalent to saying that $x^n+y^n=1$ has no solution in the rationals, for $n \geq 3$.