

# 1 Historical Background

**Theorem 1.1.**  $x^n + y^n = z^n$  has no solutions in  $\mathbb{Z}$  for  $n > 2$ .

*Proof.* Recall that the polynomial  $f(z) = z^n + 1$  has the factorization,

$$f(z) = \prod_{i=0}^{n-1} (z + \zeta_n^i)$$

where  $\zeta_n = e^{2\pi i/n}$  is a primitive  $n^{\text{th}}$ -root of unity. Thus,

$$x^n + y^n = \prod_{i=0}^{n-1} (x + \zeta_n^i y)$$

□

## 2 Number Fields

## 3 The Class Group

## 4 Cyclotomic Fields

## 5 The Case of Regular Primes

## 6 Elliptic Curves and Modularity

## 7 Wiles' proof