1 On the abc Conjecture

1.1 Introduction

Problems that directly relate the additive and multiplicative structure in $\mathbb{Z}$ tend to look deceptively simple and harshly difficult. (Goldbach's conjecture, Twin prime conjecture, FLT)

The abc conjecture gives a lower bound for rad of integer sums.

In general, bounds of the form $c < f(\mathrm{rad}(abc))$ are far from trivial (see Mahler's theorem).

More precisely, the abc conjecture states that for some $\epsilon > 0$ there is a constant K_ϵ such that for all coprime positive integers a, b, c with $a + b = c$ we have $c < K_\epsilon \,\mathrm{rad}(abc)^{1+\epsilon}$.

We know that the condition $\epsilon > 0$ is necessary.

1.2 Relevance

If the abc conjecture is true, it

- guarantees there a *simple* proof of Falting's theorem (general equation $f(x, y) = 0$ with $f \in \mathbb{Q}[x, y]$ with $\deg f \geq 4$ has only finitely many solutions in $\mathbb{Q}$)
- gives a master key for ternary Diophantine equations
- gives many results in the theory of elliptic curves
- implies FLT for large exponents
- gives an asymptotic formula for counting squarefree values of polynomials $f(t) \in \mathbb{Z}[t]$ as we evaluate at $t = 1, 2, \ldots,$ as shown by Granville (1998)
- warrants the infinitude of non-Wieferich primes (p such that $p^2 \nmid 2^{p-1} - 1$)
- power values imply power factoriation:

  If abc($\mathbb{Q}^{\leq k}$) holds, then for $k \geq 2$ there is a constant $M = M(k)$ such that if a **monic** polynomial $f(t \in \mathbb{Z}[t])$ of **degree** k satisfies the condition that $f(1)$, $f(2)$, $\ldots$, $f(M)$ are all powers of integers, then $f(x) = (t + b)^k$ for some $b \in \mathbb{Z}$.
- gives applications to Erdös-Ulam problem about rational distance sets:

  A **rational distance set** $U \subseteq \mathbb{R}^2$ is a set such that for all $x, y \in U$ we have $\|x - y\|_2 \in \mathbb{Q}$. For instance, $\mathbb{Q}$ in the X-axis is a rational distance set.

1.3 Is the field of meromorphic functions easy?

For k a field with an absolute value, we write $\mathfrak{M}_k$ for the field of (possibly transcendental) meromorphic functions on k.

Vojta formulated a conjecture in the 1980 by which number fields have arithmetic analogous to that of the fields.q

For example, in case of curves, Faltings theorem is analogous to the Picard-Berkovich theorem.

Vojta's dictionary is intimately related to the abc conjecture.

1.4 Elliptic Curves

Definition 1.1. An elliptic curve over $\mathbb{Q}$ is a smooth, geometrically connected, projective curve over $\mathbb{Q}$ of genus 1 with a distinguished $\mathbb{Q}$-rational point.

There are two integers attached to every elliptic curve: Δ_E, the absolute value of the minimal discriminant, and N_E, the conductor of E, where N_E divides Δ_E and they have the same prime factors.

It can be shown that all elliptic curves over $\mathbb{Q}$ are modular (see Wiles et al). The are some curves $X_0(N)$ over $\mathbb{Q}$ such that each curve can be reconstructed from the given integer N. They are well-understood and support the modular theory.