Formalizing Mordell ?

Michael Stoll
Universität Bayreuth

The Mordell conjecture $2 \cdot 3 \cdot 17$ years later
MIT
July 12, 2024

Prologue: a Challenge

Challenge:

Given $C > 0$, find (or prove the existence of)
a nice curve $X/\mathbb{Q}$ of genus $g \geq 2$ such that $\#X(\mathbb{Q}) \geq C \cdot g$!

- $C = 321$ ($g = 2$; St., Elkies)
- $C = 8$ ($g \to \infty$<, hyperelliptic; Mestre(?))
- $\#X(\mathbb{Q}) \leq (8r + 33)g$ (hyperelliptic, $r = \operatorname{rk} J(\mathbb{Q}) \leq g - 3$; St.)
- Unlikely intersection heuristic: $\#X(\mathbb{Q}) \ll g + r$

Challenge′:

Beat $C = 8$ for $g \to \infty$!

Proof Assistants

A proof assistant or interactive theorem prover (ITP)
is a piece of computer software that

❶ allows to construct a proof in a formal language

❷ and checks it for correctness.

There are various such systems around (list not exhaustive):

- Isabelle (1986)
- Coq/Rocq (1989)
- Agda (1999; 2007: Agda 2)
- Lean (2013; 2021: Lean 4)

Lean has a large cohesive and actively developed library Mathlib
that contains definitions, statements and proofs
comprising most ungergraduate and quite some higher-level mathematics.

What are they good for?

There are various (potential) benefits.

- Establish correctness of difficult proofs
  - ⋆ Four Color Theorem (Gonthier$^+$, 2005, Coq)
  - ⋆ Kepler Conjecture (Hales$^+$, 2014, Isabelle/HOL Light)
  - ⋆ A result on liquid vector spaces (Commelin$^+$, 2022, Lean)
- Establish a unified database of mathematical definitions and results
- Enable large-scale collaboration on mathematical projects without the need of establishing trust beforehand or checking each other's work
  - ⋆ Polynomial Freiman-Ruzsa Conjecture over $\mathbb{F}_2$ (Tao$^+$, 2023, Lean)
  - ⋆ Reduce FLT to 1980s mathematics (Buzzard$^+$, 2024–, Lean)
  - ⋆ $\mathrm{BB}(5) = 47\,176\,870$ (July 2024, 40 000 lines in Coq)
- Avoid mistakes in one's research

Motivation

Corollary 9.10. *Suppose that C/k is a smooth projective curve of genus 2 given by an integral Weierstrass model $\mathcal{C}$ such that there are three nodes in the special fiber of $\mathcal{C}$. We say that $\mathcal{C}$ is split if the two components A and E of the special fiber of $\mathcal{C}^{\min}$ are defined over $\mathfrak{k}$; otherwise $\mathcal{C}$ is nonsplit. Let $v(\Delta) = m_1 + m_2 + m_3$ as above and set $M = m_1m_2 + m_1m_3 + m_2m_3$.*

$\vdots$

(c) *If two of the nodes lie in a quadratic extension of $\mathfrak{k}$ and are conjugate over $\mathfrak{k}$ and one is $\mathfrak{k}$-rational, then*

$$\beta = \begin{cases} \dfrac{m_1}{M} \max\left\{ \left\lfloor \dfrac{m_1^2}{2} \right\rfloor + m_1m_3, \left\lfloor \dfrac{m_3^2}{2} \right\rfloor + m_1 \left\lfloor \dfrac{m_3}{2} \right\rfloor \right\} & \text{if } \mathcal{C} \text{ is split,} \\ \dfrac{m_1}{2} & \text{if } \mathcal{C} \text{ is nonsplit and } m_1 \text{ is even,} \\ 0 & \text{otherwise,} \end{cases}$$

where m_3 corresponds to the rational node (and $m_1 = m_2$).

Motivation

Proof. The proof of (a) follows easily from Proposition 9.4.

For the other cases, note that in the nonsplit case some power of Frobenius acts as negation on the component group $\Phi(\bar{\mathfrak{k}})$, so the only elements of $\Phi(\mathfrak{k})$ are elements of order 2 in $\Phi(\bar{\mathfrak{k}})$, which correspond to $[B_{m_1/2} - C_{m_2/2}]$ if m_1 and m_2 are even $\big($where μ takes the value $\frac{1}{4}(m_1 + m_2)\big)$, and similarly with the obvious cyclic permutations.

In the situation of (c), we must have $m_1 = m_2$. If $P = [(P_1) - (P_2)] \in J(k)$ and $P_1 \in C(\bar{k})$ maps to one of the conjugate nodes, then P_2 must map to the other, so all $P \in J(k)$ must map to a component of the form $[B_i - C_j]$ or $[D_i - D_j]$. Now the result in the split case follows from a case distinction depending on whether $m_1 \leq m_3$ or not. In the nonsplit case, the only element of order 2 that is defined over $\mathfrak{k}$ is $[B_{m_1/2} - C_{m_1/2}]$ if it exists.

In the situation of (d), the group $\Phi(\mathfrak{k})$ is of order 3 (generated by $[E - A]$) in the split case and trivial in the nonsplit case. □

Motivation

Proof. The proof of (a) follows easily from Proposition 9.4.

For the other cases, note that in the nonsplit case some power of Frobenius acts as negation on the component group $\Phi(\bar{\mathfrak{k}})$, so the only elements of $\Phi(\mathfrak{k})$ are elements of order 2 in $\Phi(\bar{\mathfrak{k}})$, which correspond to $[B_{m_1/2} - C_{m_2/2}]$ if m_1 and m_2 are even $\big($where μ takes the value $\frac{1}{4}(m_1 + m_2)\big)$, and similarly with the obvious cyclic permutations.

In the situation of (c), we must have $m_1 = m_2$. If $P = [(P_1) - (P_2)] \in J(k)$ and $P_1 \in C(\bar{k})$ maps to one of the conjugate nodes, then P_2 must map to the other, so all $P \in J(k)$ must map to a component of the form $[B_i - C_j]$ or $[D_i - D_j]$. Now the result in the split case follows from a case distinction depending on whether $m_1 \leq m_3$ or not. In the nonsplit case, the only element of order 2 that is defined over $\mathfrak{k}$ is $[B_{m_1/2} - C_{m_1/2}]$ if it exists.

In the situation of (d), the group $\Phi(\mathfrak{k})$ is of order 3 (generated by $[E - A]$) in the split case and trivial in the nonsplit case. $\square$

Motivation

There are actually two mistakes in the statement and proof (but one is not visible here).

It would be nice to be able to avoid such mistakes!

Goal: Be able to formalize my papers!

Problem: Lean+Mathlib is very far away from this.

(**But:** See `https://github.com/MichaelStollBayreuth/Weights`)

New Goal: Teach more arithmetic geometry to Lean!

For example: Get a proof of Mordell's Conjecture into Mathlib!

Quick Live Demo

```
import Mathlib

open Nat

theorem infinitely_many_primes : ∀ n : ℕ, ∃ p > n, p.Prime := by
  intro n
  let N := n ! + 1
  let p := N.minFac -- smallest prime divisor of `N = n! + 1`
  use p -- this will be the witness for the existential statement
  have hp : p.Prime := by -- first show that `p` is prime
    apply minFac_prime -- `N.minFac` is prime if `N ≠ 1`
    have : n ! ≠ 0 := factorial_ne_zero n
    omega -- tactic for solving linear arithmetic on `ℕ` and `ℤ`
  constructor -- split the conjunction
  · -- prove `p > n`
    by_contra! h -- assume that `p ≤ n`
    have hdvd : p ∣ n ! := (Prime.dvd_factorial hp).mpr h
    have hdvd' : p ∣ N := minFac_dvd N
    have : p ∣ 1 := (Nat.dvd_add_iff_right hdvd).mpr hdvd'
    exact hp.not_dvd_one this -- contradiction to `¬ p ∣ 1`
  · exact hp -- use proof of `p.Prime`
```

Disclaimer

I have only very recently started to think about this.

So everything that follows is very preliminary
and needs some considerable fleshing-out.

Stating Mordell's Conjecture

```
theorem Mordell_Faltings {K} [Field K] [NumberField K]
    (X : NiceCurve K) (h : genus X ≥ 2) :
    Finite (Points X K) := by
  sorry
```

- Number fields are in Mathlib
- (Nice) curves not yet, but will be soon
  (two versions: schemes / function fields)
- The genus will need a bit more work
- Once curves are there, points are easy
  ($\mathrm{Mor}_{\mathrm{Spec}\,K}(\mathrm{Spec}\,K, X)$ / places with residue field $= K$)

Which Proof?

I will look at the proof via heights (Vojta, Bombieri):

- personal taste (I find it more accessible)
- it leads to further possibilities:
  - ⋆ bounds on $\#X(K)$
  - ⋆ Mordell-Lang
  - ⋆ uniformity results
- necessary material desirable for other projects

But of course, we also want to have the other results from Faltings's original paper eventually!

Why Lean+Mathlib?

We need material from various areas of mathematics.

Since we want to combine everything, we need it to be

- formalized in the same system
- in a compatible way.

Mathlib provides a unified library of definitions and results,
which is carefully designed
so that its various parts can talk to each other.

Mathlib currently contains more than 80 000 definitions
and more than 150 000 lemmas and theorems.

Reduction to Vojta's Inequality + ε

Lemma.

Let M be a finitely generated abelian group
with a quadratic form $h\colon M \to \mathbb{R}$ such that
$\#\{x \in M : h(x) \le B\} < \infty$ for all $B \in \mathbb{R}$.
Let $S \subset M$ be a subset, $C > 0$ and $\gamma < 1$ such that
for all $x, y \in S$ with $h(x) \ge C$ and $h(y) \ge Ch(x)$, we have

$$(\star) \qquad h(x+y) - h(x-y) \le 4\gamma\sqrt{h(x)h(y)}\,.$$

Then S is finite.

Think $S = X(K)$, $M = J(K)$, $h = \hat{h}$.

This should be easy to formalize (and is partly done).

Some Requirements

- M finitely generated: Mordell-Weil Theorem
  - ⋆ weak M-W: $M/2M$ finite
    - ∘ Selmer groups
    - ∘ Galois cohomology, Néron-Ogg-Shafarevich
    - ∘ finiteness statements (class group, units f.g.)
  - ⋆ weak M-W $\Rightarrow$ M-W: heights
- canonical height function satisfying Northcott
  - ⋆ heights again

Before we can do these, we need

- abelian varieties
- Jacobian varieties ($\rightsquigarrow M$)
  - ⋆ Abel-Jacobi map ($\rightsquigarrow S \hookrightarrow M$)

The Hard Part: Vojta's Inequality

About 24 pages (Chapter 11) of [Bombieri-Gubler],
using a bunch of serious algebraic geometry, e.g.,

- Riemann-Roch on X and $X \times X$
- Intersection theory on $X \times X$
- The relation between (very ample) divisors and projective embeddings, description of global sections
- Sheaf cohomology on (products of) projective spaces

plus diophantine approximation:

- Siegel's Lemma (over K)
- Roth's Lemma

Lower-Hanging Fruit?

One idea:

First do odd degree hyperelliptic curves over $\mathbb{Q}$

- Can do many things explicitly
- Theta divisor is symmetric
- Hyperelliptic involution gives another divisor on $X \times X$

Another idea:

Formalize Chabauty-Coleman

- Can bypass Mordell-Weil
- Can perhaps replace J by Pic^0
- But: need to formalize p-adic integration

Outlook

- Algebraic geometry in Mathlib is being developed
- Diophantine approximation ($\rightsquigarrow$ Roth's Theorem) as well
- Need to develop the theory of heights in Mathlib
- Based on the above, need to formalize the proof of Vojta's inequality

Optimistic time frame: A few years

Maybe better automation and/or AI methods will help speed up things

Thank You!