BUNTES

Angus McAndrew
Apr 6, 2018

Belyi's Theorem, Effective Mordell, and ABC

We begin with one of the most famous results in arithmetic geometry.

Theorem (Mordell Conjecture) [Faltings]

Let C be an algebraic curve of genus ≥ 2 over a number field K. Then $C(K)$ is finite.

There are many proofs, Faltings' being the original and most famous.

Remark: Faltings' proof is not effective.
That is, it cannot predict the number of points or give any bounds.

Today we'll show how this theorem follows from a (much harder) conjecture, but how this nonetheless gives new insight into the question of effectiveness.

Specifically, we'll show that
ABC conjecture $\Rightarrow$ Mordell conjecture

"Mordell is as easy as ABC!"
- Zagier (apparently)

Conjecture (ABC): Let $A, B, C \in \mathbb{Z}$ s.t. $\gcd(A, B, C) = 1$ and $A + B + C = 0$.

Then for all $\varepsilon > 0$ there exists a constant K_ε s.t.

$$N(A, B, C) > K_\varepsilon \, H(A, B, C)^{1-\varepsilon}$$

where

- $N(A, B, C) = \prod_{p \mid ABC} p$ (or $\operatorname{rad}(ABC)$)
- $H(A, B, C) = \max(|A|, |B|, |C|)$.

This is a remarkably deep statement about the integers.
Something surprising about how one compares the additive and multiplicative structures of the integers.

For our purpose (to connect it to curves and Mordell) we'd like to remove the dependence on integrality and coprimality, by making it scaling invariant.

We now define

- $H(A, B, C) = \prod_{v \text{ place of } \mathbb{Q}} \max(|A|_v, |B|_v, |C|_v)$
- $N(A, B, C) = \prod_{p \in I} p$

where $I = \left\{ p \text{ prime} \mid \max(|A|_p, |B|_p, |C|_p) > \min(|A|_p, |B|_p, |C|_p) \right\}$.

Sanity exercises:

- $H(\lambda A, \lambda B, \lambda C) = H(A, B, C)$ for $\lambda, A, B, C \in \mathbb{Q}^\times$ and same for $N(\dots)$
- If $A, B, C \in \mathbb{Z}$ s.t. $\gcd(A, B, C) = 1$, one recovers the original definitions

Since we have $A+B+C=0$ and our fns are scaling invariant, they only depend on $r = -A/B$.
We'll also reformulate it over an arbitrary number field K.

Note that to satisfy the hypotheses of the conjecture, we require
$r \in \mathbb{P}^1_K \setminus \{0, 1, \infty\}$.

We now define

- $H(r) = \prod_v \max(1, |r|_v)$
- $N(r) = \prod_{p \in I} p$,
  where $I = \{p \text{ prime} \mid \max(\mathrm{val}_p(r), \mathrm{val}_p(\frac{1}{r}), \mathrm{val}_p(r-1)) > 0\}$

Remark: In fact this new height is off from the old one by a constant factor, but since ABC allows for a constant factor this won't trouble us.

Motivation: ABC ⇒ Fermat Bound

One can see this simply by assuming a solution $x^n + y^n = z^n$ $(n > 3)$
and setting
$$(A, B, C) = (x^n, y^n, z^n).$$
Then
$$N(A,B,C) = \prod_{p \mid ABC} p \leq |xyz| < \max(|x|^3, |y|^3, |z|^3) = H(A,B,C)^{3/n}.$$

So setting $\varepsilon = 1 - \frac{3}{n}$, for (A,B,C) s.t. $H(A,B,C)$ is sufficiently large, we get a contradiction to ABC.
Thus ABC gives us a bound on possible solutions to the Fermat equation, reducing the remainder of the problem to finite computation.

Let us phrase this in the following alternate way.
Let

$$F_n : \quad x^n + y^n + z^n = 0 \qquad \text{be the Fermat curve}$$

Consider the function $f : F_n \longrightarrow \mathbb{P}^1$

$$(x:y:z) \longmapsto -\left(\frac{x}{y}\right)^n,$$

ramified over $0, 1, \infty$.

Note: - $\deg(f) = n^2$
- each of $0, 1, \infty$ has n preimages in $F_n(\bar{\mathbb{Q}})$.

The idea now is that $N(A,B,C)$ is measuring ramification, while $H(A,B,C)$ is a height fn.
The note above tells us that each of $0, 1, \infty$ contributes a factor of $O(H(A,B,C)^{n/n^2})$ to $N(A,B,C)$.

So in this formulation, what we used was the existence of a rational fn f such that

$$\#\{P \in C(\bar{\mathbb{Q}}) \mid f(P) \in \{0,1,\infty\}\} < \deg(f).$$

Exercise: If C has genus 0 or 1, no such f can exist.
(Hint: Use Riemann-Hurwitz).

ABC ⇒ Mordell Bound

We begin with a technical proposition.

Prop: Let K be a number field, C/K a curve.
Let $f \in K(C)$ be a rational function of degree d.
Then for $P \in C(K) \setminus f^{-1}(0)$ we have

$$\log N_0(f(P)) < \left(1 - b_f(0)/d\right) \log H(f(P)) + O\left(\sqrt{\log H(f(P))} + 1\right)$$

Notation: • $N(r) = N_0(r) N_1(r) N_\infty(r)$

where $N_0(r) = \prod_{p \geq (r)} N_M(p)$, $N_1(r) = \prod_{p \geq (r-1)} N_M(p)$, $N_\infty(r) = \prod_{p \geq (1/r)} N_M(p)$

• $b_f(\alpha) = \sum_{f(P)=0} (e_P - 1)$

Pf: The genus 0 case follows from the fact that f is a rational function (and in fact the error term is $O(1)$). (Exercise)

For the general case we need the theory of log heights on curves.
From this we require the following

- For D a divisor on C we have a height fn $h_D(\cdot)$ (well defined up to $O(1)$)
- For $D = \sum M_k D_k$ a decomposition into irreducible divisors,
$$h_D(P) = \sum M_k h_{D_k}(P)$$
- For Δ a deg 0 divisor, $h_\Delta(P) = O\left(\sqrt{\log H(f(P))} + 1\right)$

Let $D = \mathrm{div}_0(f) = \sum M_k D_k$
$D' = \sum_{P(P)=0} (P)$ (i.e. set multiplicities to 1)
Then $b_f(0) = \deg D'$.

Then

$$\log H(f(P)) = h_D(P) + O(1) = \sum M_k h_{D_k}(P) + O(1)$$

(since $\log H(f(P))$ is also a height fn relative to D).

We now turn to $N_0(f(P))$.

Any prime occurring in this must also occur in $h_{D_k}(P)$ for some k (except for a finite set $\{p \mid p \mid f$ or p bad red. of $C\}$).

Thus

$$N_0(f(P)) < \sum h_{D_k}(P) + O(1) = h_{D'}(P) + O(1).$$

Letting $\Delta = (\deg D)D' - (\deg D')D$, we have

$$h_\Delta(P) = O\left(\sqrt{\log H(f(P))} + 1\right).$$

Thus $\log N_0(f(P)) < h_{D'}(P) + O(1)$

$$= \frac{1}{\deg D}(\deg D) h_{D'}(P) + O(1)$$

$$= \frac{1}{\deg D}(\deg D') h_D(P) + O\left(\sqrt{\log H(f(P))} + 1\right)$$

$$= \frac{1 - b_f(0)}{d} \cdot \log H(f(P)) + O\left(\sqrt{\log H(f(P))} + 1\right). \qquad \square$$

Remark: One can show the above with

$N_1(f(P))$ ... $b_f(1)$

$N_\infty(f(P))$ ... $b_f(\infty)$

By replacing f with $f-1$ and $1/f$, respectively.

Adding the 3 together we get

$$\log N_0(f(P)) N_1(f(P)) N_\infty(f(P)) < \left[\left(1 - \frac{b_0(0)}{d}\right) + \left(1 - \frac{b_f(1)}{d}\right) + \left(1 - \frac{b_f(\infty)}{d}\right)\right] \log H(f(P)) + O(\dots)$$

$$\log N(f(P)) < \frac{1}{d}\left(\#f^{-1}(0) + \#f^{-1}(1) + \#f^{-1}(\infty)\right) \log H(f(P)) + O(\dots)$$

$$< \frac{m}{d} \log H(f(P)) + O(\dots)$$

where $m = \#\{P \in C(\bar{\mathbb{Q}}) \mid f(P) \in \{0, 1, \infty\}\}$

Exponentiating, we get

$$N(f(P)) < H(f(P))^{m/d} \cdot K$$

Thm: ABC $\Rightarrow$ Mordell

Pf: Let C be a curve of genus $g \geq 2$.
Belyi's theorem gives a function

$$f: C \longrightarrow \mathbb{P}^1,$$

ramified over $\{0, 1, \infty\}$.

Exercise: By Riemann Hurwitz, $m = d + 2 - 2g$, $d = \deg(f)$, m as above.

Thus $m < d$.
Thus we can pick $0 < \varepsilon < 1 - m/d$.
Thus for sufficiently large $H(f(P))$ (i.e. all but a finite set)
we have a counterexample to ABC. □

Some important closing remarks

- Belyi's proof gives an algorithm for determining $f: C \to \mathbb{P}^1$ (ie. it is effective)
- One can also show ABC $\Rightarrow$ Siegel's Thm
- In fact, it can be shown that a particular effective form of Mordell (applied to $y^2 + y = x^5$) $\forall$ number fields K $\Rightarrow$ ABC (Related to Szpiro's Conjecture)

Elkies, "ABC Implies Mordell", Int. Math. Res. Notes. 1991
Serre, "Lectures on the Mordell-Weil Theorem", Aspects of Math E. 1989