The projective line minus three fractional points

Bjorn Poonen

University of California at Berkeley

July 13, 2006

(grew out of discussions with many people at the Spring 2006 MSRI program on Rational and Integral Points on Higher-Dimensional Varieties, especially Frédéric Campana, Jordan Ellenberg, and Aaron Levin)

1. 3 kinds of integral points
   - Darmon's M-curves
   - Campana's orbifolds
   - Almost integral points

2. Counting points of bounded height
   - Counting functions
   - Heuristics
   - Theorems and conjectures
   - Consequences

Motivation: a generalized Fermat equation

- Let
$$S(\mathbb{Z}) := \left\{ (x,y,z) \in \mathbb{Z}^3 : \begin{array}{l} x^2 + y^3 = z^7 \\ \gcd(x,y,z) = 1 \end{array} \right\}.$$
- Then
$$S(\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Q}) := \mathbb{Q} \cup \left\{ \frac{1}{0} \right\}$$
$$(x,y,z) \mapsto \frac{x^2}{z^7} \qquad \left(= 1 - \frac{y^3}{z^7} \right).$$
induces a bijection
$$\frac{S(\mathbb{Z})}{\text{sign}} \leftrightarrow \left\{ q \in \mathbb{P}^1(\mathbb{Q}) : \begin{array}{l} \text{num}(q) \text{ is a square} \\ \text{num}(q-1) \text{ is a cube} \\ \text{den}(q) \text{ is a } 7^{\text{th}} \text{ power} \end{array} \right\}.$$
- Darmon and Granville applied Faltings' theorem to covers of $\mathbb{P}^1$ ramified only over $\{0, 1, \infty\}$ to prove that the right hand side is finite, and hence deduce that $S(\mathbb{Z})$ is finite.

Geometric interpretation

- Define a $\mathbb{Z}$-scheme

$$S := \left(x^2 + y^3 = z^7 \text{ in } \mathbb{A}^3\right) - \{(0,0,0)\}.$$

- Then the morphism

$$\begin{array}{ccc} S & & (x, y, z) \\ \downarrow & & \downarrow \\ \mathbb{P}^1 & & x^2/y^7 \end{array}$$

  has multiple fibers above 0, 1, ∞, having multiplicities 2, 3, 7, respectively.

- So $S \to \mathbb{P}^1$ factors through a stack $\tilde{\mathbb{P}}^1 := [S/\mathbb{G}_m]$ that looks like $\mathbb{P}^1$ except that the points 0, 1, ∞ have been replaced by a 1/2-point, a 1/3-point, and a 1/7-point, respectively. Points in $S(\mathbb{Z})$ map to $\tilde{\mathbb{P}}^1(\mathbb{Z}) \subset \mathbb{P}^1(\mathbb{Z}) = \mathbb{P}^1(\mathbb{Q})$.

- Moral: Multiple fibers impose conditions on images of integral points.

Numerator with respect to a point

- We saw that a fiber of multiplicity 2 above $0 \in \mathbb{P}^1(\mathbb{Q})$ imposes the condition that $\operatorname{num}(q)$ be a square.
- What condition is imposed, say, by a fiber of multiplicity 2 above the point $3/5 \in \mathbb{P}^1(\mathbb{Q})$?
- Answer: The value of $\operatorname{num}_{3/5}(a/b) := |5a - 3b|$ should be a square.

In general:

Definition (Numerator with respect to the point c/d)

For $c/d \in \mathbb{P}^1(\mathbb{Q})$, define $\operatorname{num}_{c/d}(a/b) := |ad - bc|$.

Examples

- If $c \in \mathbb{Z}$, then $\operatorname{num}_c(a/b) = \operatorname{num}(a/b - c)$.
- $\operatorname{num}_\infty(q) = \operatorname{den}(q)$.

Darmon's M-curves

- M-curve data:
  points $P_1, \ldots, P_N \in \mathbb{P}^1(\mathbb{Q})$, with
  multiplicities $m_1, \ldots, m_N \in \{2, 3, \ldots\} \cup \{\infty\}$.
- An M-curve may be denoted formally by $\mathbb{P}^1 - \Delta$, where

$$\Delta := \sum_{i=1}^{N} \left(1 - \frac{1}{m_i}\right) [P_i].$$

  (It is really a kind of stack.)
- Define the Euler characteristic

$$\chi(\mathbb{P}^1 - \Delta) := \chi(\mathbb{P}^1) - \deg \Delta$$
$$= 2 - \sum_{i=1}^{\infty} \left(1 - \frac{1}{m_i}\right).$$

Definition (Integral points in Darmon's sense)

$(\mathbb{P}^1 - \Delta)(\mathbb{Z}) := \{q \in \mathbb{P}^1(\mathbb{Q}) : \text{num}_{P_i}(q) \text{ is an } m_i\text{-th power } \forall i\}$
Note: "∞-th power" means unit (i.e., ± 1).

Campana's orbifolds: motivation

- Suppose $\pi\colon S \to \mathbb{P}^1$ is such that the fiber above 0 consists of two irreducible components, one of multiplicity 2 and one of multiplicity 5.
- If $s \in S(\mathbb{Z})$, then $\pi(s)$ is again restricted: its numerator is of the form $u^2 v^5$.
- Equivalently, in the prime factorization of $\operatorname{num}(\pi(s))$, every exponent is a nonnegative integer combination of 2 and 5.
- In particular (but not equivalently), $\operatorname{num}(\pi(s))$ is a squareful integer, i.e., $p_1^{e_1} \cdots p_r^{e_r}$ with all $e_i \geq 2$.

More generally:

Definition

An integer a is called *m-powerful* if in its prime factorization all (nonzero) exponents are $\geq m$.
An integer a is called *∞-powerful* if $a = \pm 1$.

Definition (Integral points in Campana's sense)

For an M-curve $\mathbb{P}^1 - \Delta$, define

$$(\mathbb{P}^1 - \Delta)_C(\mathbb{Z}) := \{q \in \mathbb{P}^1(\mathbb{Q}) : \operatorname{num}_{P_i}(q) \text{ is } m_i\text{-powerful } \forall i\}$$

Example

Let $\Delta = \frac{1}{2}[0] + \frac{1}{2}[3] + [\infty]$. Then

$$(\mathbb{P}^1 - \Delta)_C(\mathbb{Z}) = \left\{ \frac{a}{b} \in \mathbb{P}^1(\mathbb{Q}) : \begin{array}{l} a \text{ is squareful,} \\ a - 3b \text{ is squareful, and} \\ b = 1 \end{array} \right\}$$
$$= \{a \in \mathbb{Z} : a, a-3 \text{ are both squareful}\}$$

Almost integral points

Definition (Height and penalty)

For an M-curve $\mathbb{P}^1 - \Delta$ and $q = a/b \in \mathbb{P}^1(\mathbb{Q})$, define

$$H(q) := \max\left(|a|, |b|\right)$$

$$\operatorname{penalty}_{\mathbb{P}^1-\Delta}(q) := \prod_{i=1}^{N} \prod_{\substack{p \text{ such that} \\ m_i \nmid v_p(\operatorname{num}_{P_i}(q))}} p^{1-\frac{1}{m_i}}.$$

Remark: If Δ consists of whole points, then log(penalty) is the "truncated counting function" in Vojta's "more general *abc* conjecture".

Fix a real number $r \in [0, \deg \Delta]$ ("tolerance level").

Definition (Almost integral points)

$$(\mathbb{P}^1 - \Delta + r)(\mathbb{Z}) := \left\{ q \in \mathbb{P}^1(\mathbb{Q}) : \operatorname{penalty}_{\mathbb{P}^1-\Delta}(q) \le H(q)^r \right\}$$

Also define $\chi(\mathbb{P}^1 - \Delta + r) := \chi(\mathbb{P}^1 - \Delta) + r$.

Counting points of bounded height

- We will study when the set of integral points (in each of the three senses) is finite.
- When it is infinite, we will measure it by counting points of bounded height.

Definition (Counting functions)

$$(\mathbb{P}^1 - \Delta)(\mathbb{Z})_{\le B} := \left\{ q \in (\mathbb{P}^1 - \Delta)(\mathbb{Z}) : H(q) \le B \right\}.$$
$$(\mathbb{P}^1 - \Delta)_C(\mathbb{Z})_{\le B} := \left\{ q \in (\mathbb{P}^1 - \Delta)_C(\mathbb{Z}) : H(q) \le B \right\}.$$
$$(\mathbb{P}^1 - \Delta + r)(\mathbb{Z})_{\le B} := \left\{ q \in (\mathbb{P}^1 - \Delta + r)(\mathbb{Z}) : H(q) \le B \right\}.$$

Heuristics for Darmon's M-curves

Δ	$(\mathbb{P}^1 - \Delta)(\mathbb{Z})$	$\#(\mathbb{P}^1 - \Delta)(\mathbb{Z})_{\leq B}$
0	$\left\{ \frac{a}{b} : \gcd(a,b) = 1 \right\}$	$\sim B^2$
$\left(1 - \frac{1}{m}\right)[\infty]$	$\left\{ \frac{a}{b} : b \text{ is } m^{\text{th}} \text{ power} \right\}$	$\sim B \cdot B^{1/m}$
$\sum \left(1 - \frac{1}{m_i}\right)[P_i]$	$\left\{ \frac{a}{b} : \cdots \right\}$	$\sim B^{\chi}?$

Heuristic:

- In the case $\Delta = \left(1 - \frac{1}{m}\right)[\infty]$, the probability that a point satisfies the condition at ∞ is $\sim \frac{B \cdot B^{1/m}}{B^2} = \frac{1}{B^{1-1/m}}$.
- If conditions at different points are independent, the count for $\Delta = \sum \left(1 - \frac{1}{m_i}\right)[P_i]$ should be

$$\sim B^2 \left(\frac{1}{B^{1-1/m_1}} \right) \cdots \left(\frac{1}{B^{1-1/m_N}} \right) = B^{\chi}.$$

Heuristics for Darmon's M-curves

Δ	$(\mathbb{P}^1 - \Delta)(\mathbb{Z})$	$\#(\mathbb{P}^1 - \Delta)(\mathbb{Z})_{\le B}$
0	$\left\{ \frac{a}{b} : \gcd(a,b) = 1 \right\}$	$\sim B^2$
$\left(1 - \frac{1}{m}\right)[\infty]$	$\left\{ \frac{a}{b} : \ b \text{ is } m^{\text{th}} \text{ power} \right\}$	$\sim B \cdot B^{1/m}$
$\sum \left(1 - \frac{1}{m_i}\right)[P_i]$	$\left\{ \frac{a}{b} : \cdots \right\}$	$\sim B^{\chi}$?

Heuristic:

- In the case $\Delta = \left(1 - \frac{1}{m}\right)[\infty]$, the probability that a point satisfies the condition at ∞ is $\sim \frac{B \cdot B^{1/m}}{B^2} = \frac{1}{B^{1-1/m}}$.
- If conditions at different points are independent, the count for $\Delta = \sum \left(1 - \frac{1}{m_i}\right)[P_i]$ should be

$$\sim B^2 \left(\frac{1}{B^{1-1/m_1}} \right) \cdots \left(\frac{1}{B^{1-1/m_N}} \right) = B^{\chi}.$$

Heuristics for Campana's orbifolds and for almost integral points

We use two facts.

Fact (Erdős-Szekeres 1935)

The number of m-powerful integers in $[1, B]$ *is* $\sim B^{1/m}$ *as* $B \to \infty$.

(In fact, they proved a more precise asymptotic formula.)

Since the number of m-powerful integers up to B is (up to a constant factor) the same as the number of m^{th} powers up to B, the asymptotic behavior of $\#(\mathbb{P}^1 - \Delta)_C(\mathbb{Z})_{\leq B}$ should match that of $\#(\mathbb{P}^1 - \Delta)(\mathbb{Z})_{\leq B}$.

Fact

For $r \in [0, 1]$, *the number of integers in* $[1, B]$ *whose radical is* $< B^r$ *is* $B^{r+o(1)}$ *as* $B \to \infty$.

This gives an analogous prediction for $\#(\mathbb{P}^1 - \Delta + r)(\mathbb{Z})_{\leq B}$.

Theorems and conjectures

	Darmon $\mathbb{P}^1 - \Delta$	Campana $(\mathbb{P}^1 - \Delta)_C$	Almost integral $\mathbb{P}^1 - \Delta + r$
$\chi > 0$	$\sim B^\chi$ (Beukers)	$\sim B^\chi$?	$B^{\chi+o(1)}$?
$\chi = 0$	$(\log B)^{O(1)}$ (Mordell-Weil)	$(\log B)^{O(1)}$?	$B^{o(1)}$?
$\chi < 0$	finite (Siegel, Faltings, Darmon-Granville)	finite? (Campana)	finite?

All are true if $N \leq 2$.

Theorems and conjectures

	Darmon $\mathbb{P}^1 - \Delta$	Campana $(\mathbb{P}^1 - \Delta)_C$	Almost integral $\mathbb{P}^1 - \Delta + r$
$\chi > 0$	$\sim B^\chi$ (Beukers)	$\sim B^\chi$?	$B^{\chi+o(1)}$?
$\chi = 0$	$(\log B)^{O(1)}$ (Mordell-Weil)	$(\log B)^{O(1)}$?	$B^{o(1)}$?
$\chi < 0$	finite (Siegel, Faltings, Darmon-Granville)	finite? (Campana)	finite?

All are true if $N \leq 2$.

Theorems and conjectures

	Darmon $\mathbb{P}^1 - \Delta$	Campana $(\mathbb{P}^1 - \Delta)_C$	Almost integral $\mathbb{P}^1 - \Delta + r$
$\chi > 0$	$\sim B^\chi$ (Beukers)	$\sim B^\chi$?	$B^{\chi+o(1)}$?
$\chi = 0$	$(\log B)^{O(1)}$ (Mordell-Weil)	$(\log B)^{O(1)}$?	$B^{o(1)}$?
$\chi < 0$	finite (Siegel, Faltings, Darmon-Granville)	finite? (Campana)	finite?

All are true if $N \leq 2$.

Theorems and conjectures

	Darmon $\mathbb{P}^1 - \Delta$	Campana $(\mathbb{P}^1 - \Delta)_C$	Almost integral $\mathbb{P}^1 - \Delta + r$
$\chi > 0$	$\sim B^\chi$ (Beukers)	$\sim B^\chi$?	$B^{\chi+o(1)}$?
$\chi = 0$	$(\log B)^{O(1)}$ (Mordell-Weil)	$(\log B)^{O(1)}$?	$B^{o(1)}$?
$\chi < 0$	finite (Siegel, Faltings, Darmon-Granville)	finite? (Campana)	finite?

All are true if $N \leq 2$.

Theorems and conjectures

	Darmon $\mathbb{P}^1 - \Delta$	Campana $(\mathbb{P}^1 - \Delta)_C$	Almost integral $\mathbb{P}^1 - \Delta + r$
$\chi > 0$	$\sim B^{\chi}$ (Beukers)	$\sim B^{\chi}$?	$B^{\chi + o(1)}$?
$\chi = 0$	$(\log B)^{O(1)}$ (Mordell-Weil)	$(\log B)^{O(1)}$?	$B^{o(1)}$?
$\chi < 0$	finite (Siegel, Faltings, Darmon-Granville)	finite? (Campana)	finite?

All are true if $N \leq 2$.

Theorems and conjectures

	Darmon $\mathbb{P}^1 - \Delta$	Campana $(\mathbb{P}^1 - \Delta)_C$	Almost integral $\mathbb{P}^1 - \Delta + r$
$\chi > 0$	$\sim B^\chi$ (Beukers)	$\sim B^\chi$?	$B^{\chi+o(1)}$?
$\chi = 0$	$(\log B)^{O(1)}$ (Mordell-Weil)	$(\log B)^{O(1)}$?	$B^{o(1)}$?
$\chi < 0$	finite (Siegel, Faltings, Darmon-Granville)	finite? (Campana) ($\Longleftarrow$ abc)	finite? ($\Longleftrightarrow$ abc)

All are true if $N \leq 2$.

Theorems and conjectures

	Darmon $\mathbb{P}^1 - \Delta$	Campana $(\mathbb{P}^1 - \Delta)_C$	Almost integral $\mathbb{P}^1 - \Delta + r$
$\chi > 0$	$\sim B^\chi$ (Beukers)	$\sim B^\chi$?	$B^{\chi+o(1)}$?
$\chi = 0$	$(\log B)^{O(1)}$ (Mordell-Weil)	$(\log B)^{O(1)}$? $(\implies *)$	$B^{o(1)}$?
$\chi < 0$	finite (Siegel, Faltings, Darmon-Granville)	finite? (Campana) $(\impliedby abc)$	finite? $(\iff abc)$

All are true if $N \leq 2$.

* Given an elliptic curve over a number field, the ranks of its twists are uniformly bounded.

Consequences of the Campana column

Example

Consider $(\mathbb{P}^1 - \Delta)_C$ with $\Delta := \frac{1}{2}[0] + \frac{1}{2}[1] + \frac{1}{2}[\infty]$.
So $\chi = 1/2$. Then the number of solutions to

$$\begin{cases} x + y = z, \\ x, y, z \in \mathbb{Z} \cap [1, B] \text{ squareful}, \\ \gcd(x, y, z) = 1 \end{cases}$$

is $\sim B^{1/2}$?

Is the following related?

Theorem (Blomer 2005)

The number of integers in $[1, B]$ expressible as the sum of two squareful integers is

$$\frac{B}{(\log B)^{1-2^{-1/3}+o(1)}}$$

Consequences II

Example

Take $\Delta := [\infty] + \frac{1}{2}[0] + \frac{1}{2}[1]$. So $\chi = 0$. Then $\{a \in \mathbb{Z} \cap [1, B] : a, a+1 \text{ are both squareful}\} = (\log B)^{O(1)}$?

Is it $O(\log B)$?
Well known: the Pell equation $x^2 - 8y^2 = 1$ proves $\gtrsim \log B$.

Example

Take $\Delta := [\infty] + \frac{1}{2}[0] + \frac{1}{2}[1] + \frac{1}{2}[2]$. So $\chi = -1/2$. Then

$$\{a \in \mathbb{Z}_{\geq 1} : a, a+1, a+2 \text{ are all squareful}\}$$

is finite?

Conjecture (Erdős 1975)

The set in the previous example is empty.

Consequences III

Example

Take $\Delta := [0] + [\infty] + \frac{1}{2}[1]$ over $\mathbb{Z}[1/5]$. So $\chi = -1/2$. Then

$$\{n \geq 1 : 5^n - 1 \text{ is squareful}\}$$

is finite?

Can linear forms in logarithms prove this?
It seems not.