Rational Points on Curves of Genus 2: Experiments and Speculations

Michael Stoll
Universität Bayreuth

Schloss Dagstuhl, May 25, 2009
Curves of Genus 2

A curve of genus 2 over $\mathbb{Q}$ is given by an equation

$$C : y^2 = f_6 x^6 + f_5 x^5 + f_4 x^4 + f_3 x^3 + f_2 x^2 + f_1 x + f_0$$

with $f_j \in \mathbb{Z}$, such that $(f_6, f_5) \neq (0, 0)$
and the polynomial on the right does not have multiple roots.

A rational point on this curve $C$
is a pair of rational numbers $(\xi, \eta)$ satisfying the equation.

In addition, there can be rational points “at infinity”,
corresponding to the square roots of $f_6$ in $\mathbb{Z}$.

We denote the set of rational points on $C$ by $C(\mathbb{Q})$.

Theorem (Mordell’s Conjecture, proved by Faltings). $C(\mathbb{Q})$ is finite.
The Questions

Consider curves of genus 2 over $\mathbb{Q}$:

$$C : y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$$

with $f_j \in \mathbb{Z}$, and of size $\max_j |f_j| \leq N$.

**Question.**
What can we say about $C(\mathbb{Q})$, the set of rational points on $C$, as $N$ grows?

- How many rational points are there on average?
- What is the distribution of the number of points?
- What is the largest number of rational points?
- How are the sizes of the points distributed?
- How large can the points get?
The condition that the point \( \left( \frac{a}{b}, \frac{c}{b^3} \right) \) is on \( C \) translates into a linear condition on the coefficients \( f_j \):

\[
a^6 f_6 + a^5 b f_5 + a^4 b^2 f_4 + a^3 b^3 f_3 + a^2 b^4 f_2 + ab^5 f_1 + b^6 f_0 = c^2
\]

The curves satisfying this correspond to points in the intersection of a coset of a 6-dimensional lattice in \( \mathbb{R}^7 \) with a cube of side length \( 2N \).

We can estimate the size of this set by the volume of the corresponding slice of the cube, divided by the covolume of the lattice.

We obtain for the average number of points with \( x = \frac{a}{b} \):

\[
\mathbb{E}(a:b)(N) \sim \frac{\gamma(a:b)}{\sqrt{N}} \quad \text{as } N \to \infty.
\]

with \( \gamma(a:b) \) of order \( H(a:b)^{-3} \),

where \( H(a:b) = \max\{|a|, |b|\} \) is the height of \( x \).
Heuristics (2)

We let

$$\gamma(H) = \sum_{(a:b) \in \mathbb{P}^1(Q)} \gamma(a : b) = \gamma - O\left(\frac{1}{H}\right)$$

where

$$\gamma = \sum_{(a:b) \in \mathbb{P}^1(Q)} H(a : b) = \lim_{H \to \infty} \gamma(H) \approx 4.79991.$$ 

We obtain for the average number of points with $H(x) \leq H$:

$$\mathbb{E}_{\leq H}(N) \sim \frac{\gamma(H)}{\sqrt{N}} \quad \text{as } N \to \infty.$$
A First Conjecture

Naive approach gives

$$E_{\leq H}(N) = \frac{\gamma(H)}{\sqrt{N}} + o(N^{-1/2})$$

for $H \ll N^{6/5-\varepsilon}$.

Let $E(N)$ denote the average number of rational points.

**Corollary.**

$$\liminf_{N \to \infty} \sqrt{N} \cdot E(N) \geq \gamma.$$

**Conjecture 1.**

$$\lim_{N \to \infty} \sqrt{N} \cdot E(N) = \gamma.$$

Can the exponent $6/5$ be improved? How far?

Stephan Baier: Using quadratic Gauss sum, gets $7/5 - \varepsilon$. 
Large Points (1)

If we accept Conjecture 1, then we should expect about

\[(\gamma - \gamma(H))2^7N^{13/2} = O(H^{-1}N^{13/2})\]

curves of size \(\leq N\) that have points of height \(\geq H\).

So generically, we expect that rational points on a curve of size \(N\) will have height \(\ll N^{13/2+\varepsilon}\).

Conjecture 2.

Given \(\varepsilon > 0\), there is \(B_\varepsilon > 0\) and a Zariski-open subset \(\emptyset \neq U_\varepsilon \subset \mathbb{A}^7\) such that the rational points on every curve of size \(\leq N\) whose coefficient vector is in \(U_\varepsilon\) have height \(\leq B_\varepsilon N^{13/2+\varepsilon}\).
Large Points (2)

It is, however, likely that there are families of curves with larger points.

A naive dimension count predicts a family with points of height $\gg N^9$ (maybe not over $\mathbb{Q}$).

Still, we can hope that the following is true.

**Conjecture 3.**
There are $\kappa > 0$ and $B > 0$ such that every rational point on a genus 2 curve of size $N$ has height $\leq BN^\kappa$.

Andrew Granville:
True under ABC with $\kappa = 1/2$ for quadratic twists of a fixed curve.

Su-Ion Ih: Conjecture 3 follows from Vojta’s Conjecture.
Nils Bruin and I have found (very likely) all rational points on all genus 2 curves of size $N \leq 3$. Records:

<table>
<thead>
<tr>
<th>size of curves</th>
<th>$N = 1$</th>
<th>$N = 2$</th>
<th>$N = 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>max. $H(P)$</td>
<td>145</td>
<td>10,711</td>
<td>209,040</td>
</tr>
<tr>
<td>max. $H(P)/N^{13/2}$</td>
<td>145.00</td>
<td>118.34</td>
<td>165.55</td>
</tr>
</tbody>
</table>

Using an efficient implementation of point search (ratpoints), I have found all rational points of height $< 16384$ on all genus 2 curves of size $N \leq 10$.

The graph on the next slide compares the counts for points in the height brackets $2^n \leq H < 2^{n+1}$ with the heuristic prediction.
#pts

10
1

data

N = 10
N = 9
N = 8
N = 7
N = 6
N = 5
N = 4
N = 3
N = 2
N = 1
Observations

- Overall good agreement with heuristic prediction.
- “Too many” relatively large points.

The deviation might be related to the existence of families with “overly large” points.

Note that agreement is good in the range $H \leq N^{3/2}$. 
Number of Points

The following graph shows the number of curves of size $\leq N$ with at least a given number of point pairs.

Under the assumption that the events 
“there is a rational point with $x$-coordinate $x_0$” 
are independent for all $x_0$, one arrives at a prediction for these numbers.

It turns out that the assumption must be wrong.
Another Conjecture

It appears that there is a fairly constant probability that a curve with at least \( m \) point pairs actually has at least \( m + 1 \).

This leads to the following.

**Conjecture 4.**
There is some \( B > 0 \) such that

\[
\#C(\mathbb{Q}) \leq B \log(2N + 1)
\]

for curves of size \( \leq N \).

The next two slides show the best curves known to me with respect to number of points versus size.
The points marked Elkies/Stoll 2009 come from several families constructed by Noam Elkies using K3 surfaces.

One of them represents the current record for the number of rational points on a genus 2 curve over $\mathbb{Q}$:

The curve

$$y^2 = 82342800 x^6 - 470135160 x^5 + 52485681 x^4 + 2396040466 x^3 + 567207969 x^2 - 985905640 x + 247747600$$

has at least 642 rational points!

The previous record was 588 points, due to Keller and Kulesz.
Some Remarks

From the data, it looks like we might have

$$\max\{\#C'(\mathbb{Q}) : C \text{ of size } \leq N\} \gg \log(2N + 1).$$

However, Caporaso, Harris and Mazur show that the Weak Lang Conjecture implies that \(\#C'(\mathbb{Q})\) is bounded.

We observe that the rank of the group of rational points on the Jacobian variety of the curve also grows with the number of rational points on the curve. (Compare next slide.)

So if we assume that the rank is bounded, our data and the CHM result can be reconciled.