Many curves with few rational points

Michael Stoll
Universität Bayreuth

Selmer Groups, Descent and the Distribution of Ranks
University of Warwick

25 September 2012

The Goal

We consider (again) hyperelliptic curves with a marked Weierstrass point (simply 'curves' in this talk), ordered by height as in Manjul's talk.

Definition.
We denote by $N(C)$ the number of pairs of rational non-Weierstrass points on a curve C.

We denote by $\lambda(g, N)$ the lower density of curves of genus g with $N(C) \leq N$.

We want to obtain lower bounds on $\lambda(g, N)$ that are as large as possible.

To achieve this, we will combine the results of Bhargava-Gross with Chabauty's method.

Chabauty

We will use the following version of the Chabauty-Coleman method (M. Stoll, *Independence of rational points on twists of a given curve*, Compositio Math. **142**, 1201–1214 (2006)).

Lemma.
Let C be a curve of genus g with Jacobian of Mordell-Weil rank $r < g$.
Let p be an odd prime and $\mathcal{C}$ the given curve considered over $\mathbb{Z}_p$.
Assume that the image of $C(\mathbb{Q})$ in $\mathcal{C}(\mathbb{F}_p)$ consists of smooth points
and contains at most n pairs of points
that do not lift to a Weierstrass point in $C(\mathbb{Q}_p)$.
Then

$$N(C) \leq n + r + \left\lfloor \frac{r}{p-2} \right\rfloor .$$

Chabauty at 2

We will also want to use the prime 2.

Lemma.
Let C be a curve of genus g with Jacobian of Mordell-Weil rank $r < g$.
Let $\mathcal{C}$ be the given curve considered over $\mathbb{Z}_2$.
Assume that the image of $C(\mathbb{Q})$ in $\mathcal{C}(\mathbb{F}_2)$ consists of smooth points
and contains at most n points
that do not lift to a Weierstrass point in $C(\mathbb{Q}_2)$.
Then

$$N(C) \leq n + r + \left\lfloor \frac{r}{2} \right\rfloor .$$

In both cases (odd p and $p = 2$), we have to bound r and n.

Obtaining Bounds: Rank

Now we want to estimate the lower density of curves such that for some prime, Chabauty gives us the desired bound on $N(C)$.

Bhargava-Gross gives a bound on r:

Proposition.
The lower density of curves of genus g with Jacobian of Mordell-Weil rank $\leq r$ is

$$\geq 1 - \frac{2}{2^{r+1} - 1}.$$

Proof.
Otherwise, the contribution of ranks $> r$ would make the average of 2^{rank} larger than 3.

Obtaining Bounds: Points mod p

To bound n, we consider curves such that all non-smooth $\mathbb{F}_p$-points on the special fibre of the given model over $\mathbb{Z}_p$ are regular.

Then (for odd p) the number n is (at most) the number of $a \in \mathbb{F}_p$ such that $f(a)$ is a non-zero square.

This leads to a density of curves with $n \le m$ given by

$$\nu(g,p,m) \begin{cases} = \displaystyle\sum_{n=0}^{m} \binom{p}{n} \Big(\frac{p-1}{2p}\Big)^n \Big(\frac{p-1}{2p} + \frac{p-1}{p^2} + \frac{p-1}{p^3}\Big)^{p-n} & \text{if } 3 \le p \le g\,, \\ \ge \displaystyle\sum_{n=0}^{m} \binom{p}{n} \Big(\frac{p-1}{2p}\Big)^n \Big(\frac{p-1}{2p} + \frac{p-1}{p^2}\Big)^{p-n} & \text{if } g < p \le 2g\,. \end{cases}$$

Obtaining Bounds: Points mod 2

When $p = 2$, we obtain the following densities $\nu(g, 2, m)$
of curves with at most m points mod 2
not lifting to a Weierstrass point over $\mathbb{Q}_2$.

$$\nu(g, 2, 0) = \frac{1}{4}, \qquad \nu(g, 2, 1) = \frac{1}{2}, \qquad \nu(g, 2, 2) = \frac{9}{16}.$$

We write $\bar{\nu}(g, p, m) = 1 - \nu(g, p, m)$;
this is (an upper bound for) the density of 'bad' curves for p.

Putting It All Together

To see how this works, let us consider the case $g = 4,\ N = 3$.

We can bound $N(C)$ by 3 in the following cases.

$$\begin{aligned}
p = 2: &\quad (r, m) = (0,3), (1,2), (2,0) \\
p = 3: &\quad (r, m) = (0,3), (1,1) \\
p = 5: &\quad (r, m) = (0,3), (1,2), (2,1) \\
p = 7: &\quad (r, m) = (0,3), (1,2), (2,1), (3,0)
\end{aligned}$$

This gives us lower bounds for the density assuming the rank is bounded:

$$\begin{aligned}
r = 0: &\quad \geq 1 - \bar{\nu}(4,2,3)\bar{\nu}(4,3,3)\bar{\nu}(4,5,3)\bar{\nu}(4,7,3) &&\geq 0.99437 \\
r = 1: &\quad \geq 1 - \bar{\nu}(4,2,2)\bar{\nu}(4,3,1)\bar{\nu}(4,5,2)\bar{\nu}(4,7,2) &&\geq 0.94901 \\
r = 2: &\quad \geq 1 - \bar{\nu}(4,2,0)\bar{\nu}(4,5,1)\bar{\nu}(4,7,1) &&\geq 0.49460 \\
r = 3: &\quad \geq 1 - \bar{\nu}(4,7,0) &&\geq 0.01542
\end{aligned}$$

Putting It All Together (2)

Taking differences, we see that we get densities of at least

$0.99437 - 0.94901 = 0.04536$	that work for $r = 0$, but not for $r \geq 1$
$0.94901 - 0.49460 = 0.45441$	that work for $r \leq 1$, but not for $r \geq 2$
$0.49460 - 0.01542 = 0.47918$	that work for $r \leq 2$, but not for $r \geq 3$
$0.01542 - 0.00000 = 0.01542$	that work for $r \leq 3$, but not for $r \geq 4$

Using the bound coming from Bhargava-Gross, we finally obtain

$$\lambda(4,3) \geq 0.04536 \cdot 0 + 0.45441 \cdot \frac{1}{3} + 0.47918 \cdot \frac{5}{7} + 0.01542 \cdot \frac{13}{15} = 0.50711\,.$$

A Table

Proceeding in this way, we obtain the following table of lower bounds on $\lambda(g, N)$.

$g \backslash N$	0	1	2	3	4	5	$\cdots$	∞
2	0	0.083	0.195	0.257	0.284	0.289	$\cdots$	0.289
3	0	0.097	0.260	0.476	0.641	0.695	$\cdots$	0.708
4	0	0.100	0.275	0.507	0.719	0.818	$\cdots$	0.865
5	0	0.105	0.289	0.528	0.735	0.837	$\cdots$	0.935
6	0	0.105	0.290	0.531	0.739	0.841	$\cdots$	0.968
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
∞	0	0.106	0.294	0.538	0.745	0.847	$\cdots$	1.000

The Majority

Working a bit harder, we can improve the bound

$$\lambda(3,3) \geq 0.476$$

to

$$\lambda(3,3) > 1/2\,.$$

This gives:

Theorem.
If $g \geq 3$, then a majority of all curves have at most 7 rational points.

Large Genus

To say something about asymptotics as $g \to \infty$,
we want to use fairly large primes.

So we have to get rid of the 'n' in the estimate

$$N(C) \leq n + r + \left\lfloor \frac{r}{p-2} \right\rfloor .$$

For this we try to make sure the the image of $C(\mathbb{Q})$ in $\mathcal{C}(\mathbb{F}_p)$
only hits Weierstrass points.

2-Descent

If C has good reduction at p, then

$$J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \cong J(\mathbb{F}_p)/2J(\mathbb{F}_p)\,.$$

If
$$f(x) = h_1(x)h_2(x)\cdots h_d(x)$$
is the factorisation mod p of the defining polynomial,
then the map $C(\mathbb{F}_p) \to J(\mathbb{F}_p)/2J(\mathbb{F}_p)$ is given by

$$(\xi, \eta) \longmapsto \big((h_1(\xi), h_2(\xi), \ldots, h_d(\xi)\big) \in \big(\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2\big)^d\,.$$

We look for f such that the image is nontrivial for all $\xi \in \mathbb{F}_p$.

For a polynomial with d factors, the chance for this to happen is

$$\geq 1 - p\,2^{-d}\,.$$

Equidistribution

Theorem (Bhargava-Gross).
Each nontrivial element of $J(\mathbb{F}_p)/2J(\mathbb{F}_p)$ (order $= 2^{d-1}$)
has on average $2/2^{d-1}$ preimages in the Selmer group.

So excluding up to p points in the image
leads to at most a further proportion of $4p\,2^{-d}$ 'bad' curves.

The total density of 'bad' curves for the prime p is then at most

$$\frac{1}{p} + p^{-2g} \sum_{f} 5p\,2^{-d(f)} = \frac{1}{p} + O\Big(\frac{p}{\sqrt{g}}\Big) .$$

($1/p$ accounts for bad reduction.)

For $p \asymp g^{1/4}$, this is $O(g^{-1/4})$.

The Result

Taking all primes p with $\alpha\sqrt{g} < p < \beta\sqrt{g}$, we obtain the following.

Theorem.
There is $c > 0$ such that for a set of curves C of genus g of density

$$\geq 1 - e^{-c\sqrt{g}/\log g},$$

the points in $C(\mathbb{Q})$ with positive y-coordinate are independent in the Mordell-Weil group.

Corollary.
For $N < \alpha\sqrt{g} - 2$, we have $\quad \lambda(g, N) \geq 1 - e^{-c\sqrt{g}/\log g} - \frac{2}{2^{N+1}-1}$.

In particular, $\quad \liminf_{g\to\infty} \lambda(g, N) \geq 1 - \frac{2}{2^{N+1}-1}$.

So for g large, we have $\lambda(g, 2) > 1/2$.

Only One Point?

Can we also prove a positive density of curves C with $N(C) = 0$?

Recall the Chabauty estimates

$$N(C) \leq n + r + \left\lfloor \frac{r}{p-2} \right\rfloor \qquad \text{for odd } p$$

$$N(C) \leq n + r + \left\lfloor \frac{r}{2} \right\rfloor \qquad \text{for } p = 2$$

When p is odd, we cannot get rid of r in the estimate;
so we would need a positive density for $r = 0$, which we cannot (yet) prove.

But we can do something when $p = 2$!

The following argument is due to **Bjorn Poonen** (for $g \geq 4$).

Special Curves

Consider the curve

$$C_0 \colon y^2 + y = x^{2g+1} + x + 1$$

of genus g over $\mathbb{F}_2$, with Jacobian J_0.
Then $C_0(\mathbb{F}_2) = \{\infty\}$ and $J_0[2] = 0$.

For $C/\mathbb{Q}$ (with Jacobian J) in a small 2-adic neighbrbourhood of a fixed curve reducing mod 2 to C_0, we have uniformly

$$J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \xrightarrow{\cong} G = \mathbb{F}_2^g$$

and the Chabauty pairing $J(\mathbb{Q}_2) \times \Omega^1(C_{\mathbb{Q}_2}) \to \mathbb{Q}_2$ induces a perfect pairing

$$G \times \Omega^1(C_0) \longrightarrow \mathbb{F}_2 .$$

Chabauty: If Selmer $\hookrightarrow G$ and there is $\omega \in \Omega^1(C_0)$ with $\omega(\infty) \neq 0$ such that ω annihilates the image of S, then $N(C) = 0$.

Only One Point!

Equidistribution of Selmer group elements in G implies
that for $g \geq 3$, there is a positive density of C (reducing to C_0)
such that the condition is satisfied.

Since a suitable family of such curves can be defined
by 2-adic congruence conditions, we obtain:

Theorem.
For every genus $g \geq 3$,
the set of curves C with $C(\mathbb{Q}) = \{\infty\}$ has positive density.

The lower bounds we can prove in this way go to zero exponentially fast.
It would be nice to get a uniform bound!