A Dirichlet Theorem for Rank 1 Elliptic Curves

Keith Merrill, Brandeis University

June 25, 2020

This is based on joint work with Lior Fishman, David Lambert, Tue Ly, and David Simmons.

My thanks to the organizers and staff for persevering in these difficult times and making this conference a success.

Diophantine Approximation

The field of Diophantine approximation can be viewed as an attempt to turn the *qualitative* aspect of density into a *quantitative* notion.

As a motivating example, let's consider the classical situation of the density of the rationals in the real numbers. What does it mean to quantify that density?

Dirichlet's Theorem

Theorem (Dirichlet, Strong Form)

For every $\alpha \in \mathbb{R}$ and every $N \geq 1$, there exists a pair $(p, q) \in \mathbb{Z} \times \mathbb{N}$ for which

$$|q\alpha - p| < \frac{1}{N}, \quad 1 \leq q \leq N.$$

Corollary (Dirichlet, Weak Form)

For every irrational α, there exist infinitely many rationals p/q such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

We can obviously always find rationals which are closer and closer to α, but doing so generally requires larger and larger denominators. The idea here is to force rationals with large denominator to be correspondingly much closer.

The exponent of 2 which appears in the corollary can be interpreted as a measure of the *quantitative* density of the rationals–indeed, for almost every irrational α, it cannot be replaced by something strictly larger if the corollary is to remain true.

Elliptic Curves

An *elliptic curve* is formally a smooth *curve* (a smooth projective variety of dimension 1) which has genus 1 and a specified basepoint, which we denote by O.

For our purposes, however, we can consider elliptic curves as defined by an equation

$$y^2 = x^3 + ax + b.$$

It's generally more convenient to think of the projectivization of the curve given by

$$\{[x : y : z] \ : \ y^2z = x^3 + axz^2 + bz^3\}, \quad O = [0 : 1 : 0].$$

We will be concerned with elliptic curves *defined over* $\mathbb{Q}$, in which case we assume $a, b \in \mathbb{Q}$.

The set $E(\mathbb{C})$

We can consider the set of complex points on the curve, thought of as sitting inside $\mathbb{P}^2(\mathbb{C})$.

Given a complex lattice Λ, consider the associated *Weierastrass $\wp$-function*

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

For all $z \in \mathbb{C} \setminus \Lambda$ we have

$$\wp'(z;\Lambda)^2 = 4\wp(z;\Lambda)^3 - g_2\wp(z;\Lambda) - g_3,$$

where g_2 and g_3 are quantities associated to Λ.

The set $E(\mathbb{C})$

Theorem (Silverman, VI, Prop. 3.6b)

Let Λ a complex lattice, and g_2 and g_3 its associated quantities. Then

$$E : y^2 = 4x^3 - g_2 x - g_3.$$

is an elliptic curve, and the map

$$\varphi : \mathbb{C}/\Lambda \to E \subset \mathbb{P}^2(\mathbb{C}), \quad z \mapsto [\wp(z;\Lambda) : \wp'(z;\Lambda) : 1]$$

is a complex analytic isomorphism of complex Lie groups.

Moreover, by the Uniformization Theorem, *every* elliptic curve arises in this way. They correspond exactly to complex tori.

The set $E(\mathbb{R})$

Moreover, if our elliptic curve is defined with real coefficients, then we can visualize the set $E(\mathbb{R})$ as the restriction of the map φ. In fact, this map is precisely the exponential map of the real locus, viewed as a compact real Lie group.

$$\exp_E : \mathbb{R} \to E(\mathbb{R}) \subset \mathbb{P}^2(\mathbb{R}), \quad z \mapsto [\wp(z;\Lambda) : \wp'(z;\Lambda) : 1]$$

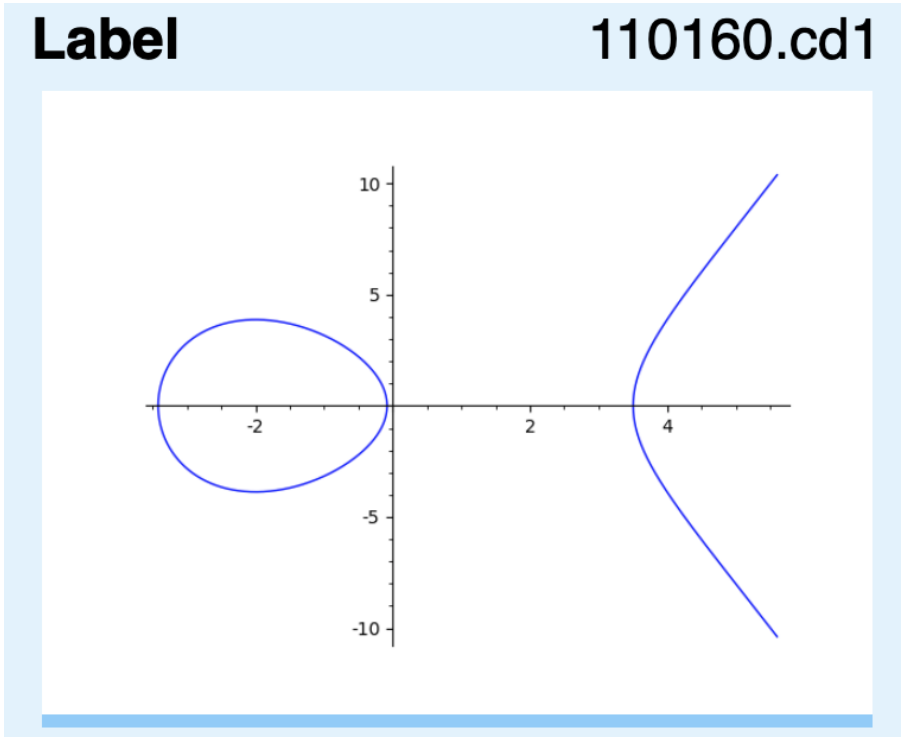
(Here we need to know that because E is defined over $\mathbb{R}$, Λ is invariant under complex conjugation, which forces the values $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$ to be real).

The image of this map is the connected component of the identity $E(\mathbb{R})^0$ and its kernel is of the form $\mathbb{Z}\omega$ for some nonzero period ω.

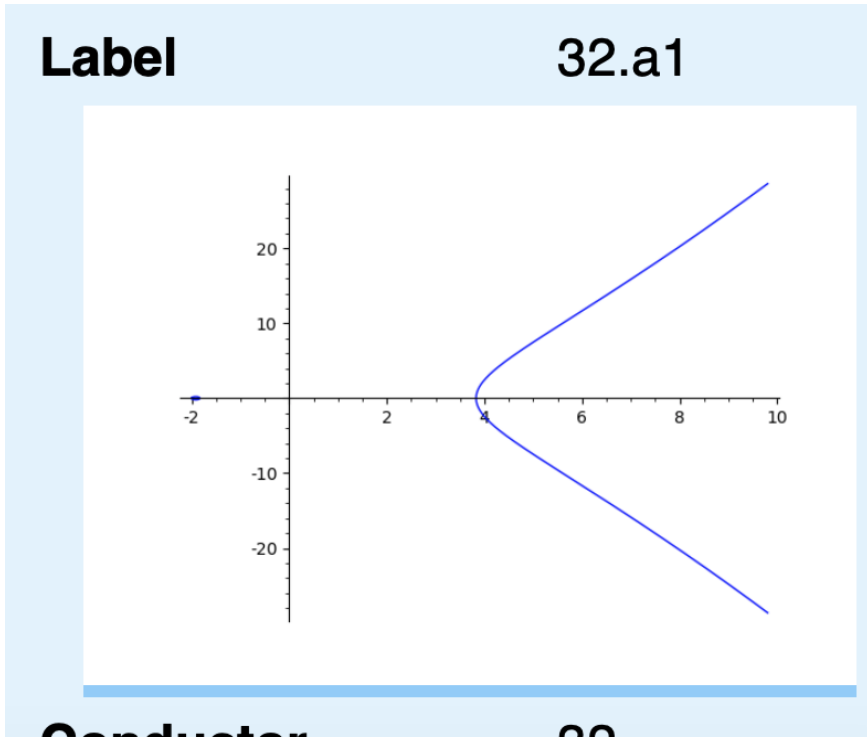
In fact, $E(\mathbb{R})$ is real-analytically isomorphic to $S^1 \times \Phi$, where Φ has order 1 or 2.

The set $E(\mathbb{R})$

Let's see some pictures. These are courtesy of `lmfdb.org`[Accessed June 21, 2020]



,



The Group Law

Elliptic curves carry an addition law which can be described as follows: given two points P, Q, we consider the line through them and take the third point of intersection; we then flip that point over the x-axis (note that in this presentation the curves are invariant under reflection). This is defined to be $P \oplus Q$.

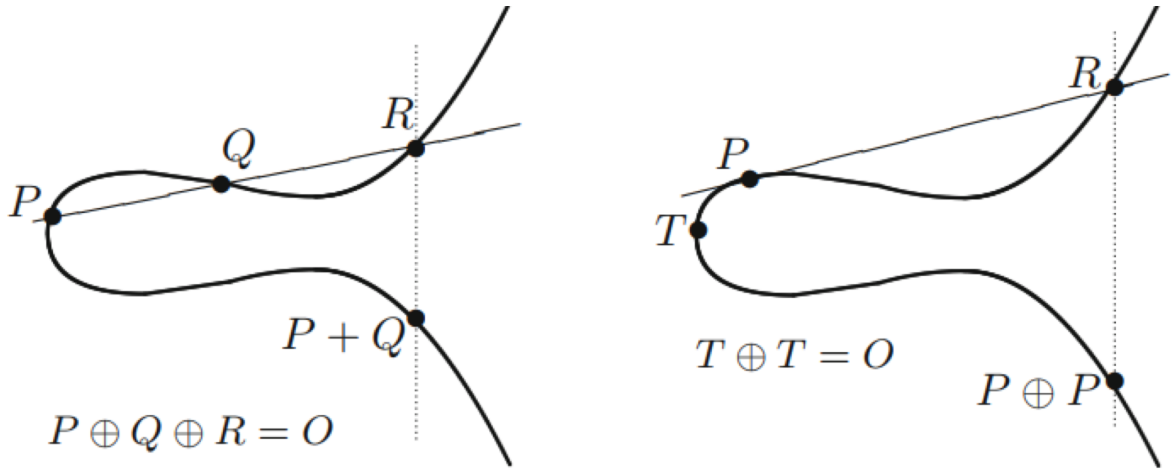


Figure 1: Elliptic curve addition (Image from [Sil09])

Image credit to Dylan Pentland of MIT, who credits Silverman.

The set $E(\mathbb{Q})$

If our curve has *rational* coefficients, then it turns out the group law respects points with rational coordinates, in that the sum of two points on the curve E with rational coefficients will again be a point with rational coefficients. While the picture of these points is maybe not as beautiful as the previous cases, we have the following incredible theorem:

Theorem (Mordell-Weil)

The group of rational points $E(\mathbb{Q})$ is a finitely-generated abelian group.

It follows immediately that we have

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \mathbb{Z}_{tor},$$

where $\mathbb{Z}_{tor}$ consists of the torsion points (i.e. finite order). We call r the *rank* of the elliptic curve.

Rational Approximation on Elliptic Curves

We can now phrase the problem we're interested in. Given an elliptic curve defined over $\mathbb{Q}$ with positive rank, the rational points on the curve are dense in $E(\mathbb{R})^0$. We want to quantify that density.

We say $P \in E(\mathbb{R})^0 \setminus E(\mathbb{Q})$ is *κ-approximable* if there exists a constant C and infinitely many $Q \in E(\mathbb{Q})$ for which

$$\text{dist}(P, Q) < C(\hat{h}(Q))^{-\kappa}.$$

Here $\hat{h}(\cdot)$ is the *canonical height* on E, which defines a positive definite quadratic form on the quotient group $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$, and "dist" is the distance inherited on E from $\mathbb{P}^2(\mathbb{R})$.

We define the *Diophantine exponent of P* to be the quantity

$$\nu_E(P) = \limsup_{\hat{h}(Q)\to\infty} \frac{-\ln(\mathrm{dist}(P,Q))}{\ln(\hat{h}(Q))},$$

and we define the *Diophantine exponent of the curve E* to be

$$\nu_E = \inf\{\nu_E(P) \ : \ P \in E(\mathbb{R})^0 \setminus E(\mathbb{Q})\}.$$

Saying that P is κ-approximable is equivalent to saying that $\nu_E(P) \geq \kappa$.
Waldschmidt has a conjecture (which we will see later) which would imply the following:

Conjecture

Let E be an elliptic curve over $\mathbb{Q}$ of rank r. Then $\nu_E \geq \frac{r}{2}$.

The Main Result

For the rank 1 case, we show stronger than this.

Theorem (Fishman, Lambert, Ly, M., Simmons)

Let $E/\mathbb{Q}$ be an elliptic curve with rank 1. Then

$$\nu_E = \frac{1}{2}.$$

Even stronger, there exists a constant C such that for every $P \in E(\mathbb{R})^0 \setminus E(\mathbb{Q})$ there exist infinitely many $Q \in E(\mathbb{Q})$ satisfying

$$\operatorname{dist}(P, Q) < C(\hat{h}(Q))^{-1/2}.$$

This can be interpreted as a uniform weak-type Dirichlet theorem for the rank 1 case. The second claim of the theorem implies that $\nu_E \geq \frac{1}{2}$. For the reverse inequality, we need to show that the set of *badly approximable* points is nonempty.

Sketch Proof

Via the use of the exponential map discussed previously, we can convert the problem of approximation on $E(\mathbb{R})^0$ to one of *inhomogeneous* approximation on the circle.

Let P be an irrational point and let Q be a generator for the free summand of $E(\mathbb{Q})$. Denote by

$$\theta := \exp^{-1}(Q), \quad \gamma := \exp^{-1}(P),$$

where we choose the unique preimages in the interval $(0, \omega)$.

Remark

We have that $\frac{\theta}{\omega} \notin \mathbb{Q}$ and that there do not exist integers p, q for which $q\frac{\theta}{\omega} + p = \frac{\gamma}{\omega}$.

The first statement follows immediately from the fact that Q has infinite order, and the second follows because P is not in the orbit of Q.

Proof–Lower Bound

It turns out that the previous remark is exactly what we need to apply a classical theorem of Minkowski:

Theorem (Minkowski)

Let $\frac{\theta}{\omega}$ any irrational number and let $\frac{\gamma}{\omega}$ any number for which $\frac{\gamma}{\omega} = p\frac{\theta}{\omega} + q$ has no solutions in integers p, q. Then there exist infinitely many pairs of integers (n, m) for which

$$|n| \left| n\frac{\theta}{\omega} + m - \frac{\gamma}{\omega} \right| < \frac{1}{4}.$$

Since $\mathrm{dist}(P, Q)$ differs from $\min_{m\in\mathbb{Z}} |\theta + m\omega - \gamma|$ by a multiplicative constant, we have

$$\mathrm{dist}(P, [n]Q) \asymp |n\theta + m\omega - \gamma| < \frac{|\omega|}{4|n|} = \frac{C}{\sqrt{\hat{h}([n]Q)}}.$$

Proof–Upper Bound

We call a point P *badly approximable* if there exists a constant c (possibly depending on P) for which

$$\text{dist}(P, Q) > c(\hat{h}(Q))^{-1/2}$$

holds for all $Q \in E(\mathbb{Q})$. The upper bound $\nu_E \leq \frac{1}{2}$ will follow if we can show that there exists a point $P \in E(\mathbb{R})^0 \setminus E(\mathbb{Q})$ which is badly approximable.

Translating as before, it suffices to show that the set

$$\left\{\gamma = \exp^{-1}(P) : \ \exists c \text{ st } |n\theta + m\omega - \gamma| > \frac{c}{|n|} \ \forall n, m\right\}$$

is non-empty.

Theorem (Bugeaud-Harrap-Kristensen-Velani)

For every $\theta, \omega \in \mathbb{R}$, the set above has full Hausdorff dimension.

Future Directions

This result naturally suggests some follow-up questions.

1. Establish the conjecture for elliptic curves of arbitrary rank.
2. Extend the result to real number fields.
3. Establish Waldschmidt's conjecture for rank 1 curves. His conjecture can be stated as follows:

Conjecture (Waldschmidt)

For every $\varepsilon > 0$ there exists a constant $h_0 > 0$ such that, for any $h \geq h_0$ and any $P \in E(\mathbb{R})^0$, there exists $Q \in E(\mathbb{Q})$ with $\hat{h}(Q) \leq h$ and

$$\operatorname{dist}(P, Q) \leq h^{-(1/2)+\varepsilon}.$$

This is the strong-type of Dirichlet theorem for this setting.