The distribution of integral multiples of real points on an elliptic curve.

Alex Cowan
cowan@math.columbia.edu

1 Introduction

Let \( E : y^2 = 4x^3 - g_2x - g_3 \) be an elliptic curve with \( g_2, g_3 \in \mathbb{R} \), and suppose that \( P \in E(\mathbb{R}) \). In this paper we investigate the statistics of the coordinates \( x(nP), y(nP) \in \mathbb{R} \) of \( nP \) for \( n \in \mathbb{Z} \). The set of points \( (x, y) \in \mathbb{R}^2 \) which satisfy the equation for \( E \) form either one or two connected subsets of \( \mathbb{R}^2 \), depending on whether the polynomial \( 4x^3 - g_2x - g_3 \) has one or three real roots. In the case where \( 4x^3 - g_2x - g_3 \) has three real roots, the coordinates of points making up one of the connected subsets are bounded, while in the other the coordinates are unbounded. In this case we will say that \( E(\mathbb{R}) \) has two connected components, and we will refer to them as the “bounded component” and “unbounded component”. If instead \( 4x^3 - g_2x - g_3 \) has only one real root, then we will say that \( E(\mathbb{R}) \) has only one component, we will refer to it as the “unbounded component”.

In section 3, we prove theorems which explain how large the coordinates of \( nP \) get as a function of \( n \):

**Theorem 1.1.** Suppose that \( E/\mathbb{C} \) has periods \( \omega_1 \) and \( \omega_2 \), chosen such that \( \omega_1 \in \mathbb{R}_{>0} \) and \( \text{Im}(\omega_2) > 0 \). Then for every point \( P \) of infinite order in the unbounded component of \( E(\mathbb{R}) \), there exist infinitely many \( n \) such that

\[
x(nP) > \frac{5}{\omega_1^2} n^2 + O(n^{-2}) \quad \text{and} \quad y(nP) > \frac{2 \cdot 5^2}{\omega_1^3} n^3 + O(n^{-1}).
\]

If \( P \) is instead a point of infinite order on the bounded component of \( E(\mathbb{R}) \) (in the case where \( E(\mathbb{R}) \) has two connected components), then there exist infinitely many \( n \) such that

\[
x(nP) > \frac{5}{4\omega_1^2} n^2 + O(n^{-2}) \quad \text{and} \quad y(nP) > \frac{5^2}{4\omega_1^3} n^3 + O(n^{-1}).
\]

The implied constants depend only on \( E \).

**Theorem 1.2.** Let \( f \) be a function from \( \mathbb{N} \) to \( \mathbb{R}_{>0} \). If \( \sum_{n=1}^{\infty} f(n)^{-1} \) diverges, then for all points \( P \) in \( E(\mathbb{R}) \) except for a set of points of Lebesque measure zero, there exist infinitely many positive integers \( n \) such that

\[
x(nP) > f(n)^2 \quad \text{and} \quad y(nP) > f(n)^3,
\]

while if \( \sum_{n=1}^{\infty} f(n)^{-1} \) converges, then the set of points \( P \) in \( E(\mathbb{R}) \) for which there exist infinitely many such \( n \) has measure zero.

**Theorem 1.3.** For any \( E \) and any function \( f : \mathbb{N} \to \mathbb{R}_{>0} \), there exists a point \( P \) in \( E(\mathbb{R}) \) such that, for infinitely many positive integers \( n \),

\[
x(nP) > f(n)^2 \quad \text{and} \quad y(nP) > f(n)^3.
\]
Variants of these theorems can be given for general $P \in E(\mathbb{C})$, and not just for $P \in E(\mathbb{R})$. For example,

**Theorem 1.4.** Let $P$ be a point in $E(\mathbb{C})$ of infinite order. Then

$$|x(nP)| \gg n \quad \text{and} \quad |y(nP)| \gg n^2,$$

where the implied constants depend only on $P$.

The proofs of these theorems rely on the work of Hurwitz [5], Khinchin [6] [7], and Dirichlet (see [4], theorem 200) in the field of Diophantine approximation. The correspondence between results in Diophantine approximation and asymptotics for the size of the coordinates of $nP$ can be extended further.

In section 4, we investigate the full distribution of the $x$ and $y$ coordinates of $nP$. Let $\omega_1$ and $\omega_2$ be the periods of $E/\mathbb{C}$, chosen such that $\omega_1 \in \mathbb{R}_{>0}$ and $\text{Im}(\omega_2) > 0$. Let $\Lambda$ be the $\mathbb{C}$-lattice with basis $\langle \omega_1, \omega_2 \rangle$. Then $E/\mathbb{C}$ is parameterized by elements $z$ of $\mathbb{C}/\Lambda$ via $z \mapsto (\varphi(z), \varphi'(z))$, where

$$\varphi(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda, \lambda \neq 0} \left( \frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right).$$

We prove the following regarding the distribution of integer multiples of a fixed $P \in E(\mathbb{R})$ in section 4:

**Theorem 1.5.** Let $P$ be a point of infinite order in $E(\mathbb{R})$, and let $c_P$ be the preimage of $P$ under the parameterization $z \mapsto (\varphi(z), \varphi'(z))$. Let $\omega_1$ and $\omega_2$ be the periods of $E/\mathbb{C}$, chosen such that $\omega_1 \in \mathbb{R}_{>0}$ and $\text{Im}(\omega_2) > 0$. Let $\Lambda$ be the $\mathbb{C}$-lattice with basis $\langle \omega_1, \omega_2 \rangle$. Define $I_P \subset \mathbb{C}/\Lambda$ as follows:

$$I_P := \left\{ [0, \omega_1], \begin{array}{cl} [0, \omega_1] \cup ([0, \omega_1] + \frac{\omega_2}{2}), & \text{Im}(z_P) = 0 \text{ mod } \Lambda, \\
[0, \omega_1] \cup ([0, \omega_1] + \frac{\omega_2}{2}), & \text{Im}(z_P) = \text{Im}(\frac{\omega_2}{2}) \text{ mod } \Lambda, \\
\end{array} \right\}$$

where $[0, \omega_1]$ denotes the interval of real numbers. Then, for any $U \subseteq \mathbb{R}^2$, we have

$$\lim_{n \to \infty} \frac{1}{2n} \# \{ |k| < n : (x(kP), y(kP)) \in U \} = \frac{\mu(\{ z \in I_P : (\varphi(z), \varphi'(z)) \in U \})}{\mu(I_P)},$$

where $\mu$ is the Lebesgue measure.

From this we can deduce the following corollary, which illustrates the distribution of $nP$ more clearly:

**Corollary 1.6.** Fix $P_0 = (x_0, y_0) \in E(\mathbb{R})$ and $\varepsilon > 0$. For all $P \in E(\mathbb{R})$ of infinite order, the natural density of integers $n$ for which $(x(nP) - x_0)^2 + (y(nP) - y_0)^2 < \varepsilon^2$ is

$$\frac{2\eta(\varepsilon + O(\varepsilon^2))}{\omega_1 \sqrt{b_0^2 + (6x_0^2 - \frac{a_3}{2})^2}},$$

where $\eta = 1$ if both $P$ and $P_0$ are on the unbounded component of $E(\mathbb{R})$, $\eta = \frac{1}{2}$ if $P$ is on the bounded component of $E(\mathbb{R})$, and $\eta = 0$ if $P_0$ is on the bounded component of $E(\mathbb{R})$ but $P$ is not. The implied constant depends on both $E$ and $P_0$.

**Figure 1.7.** $\{nP : 1 < n < 3000\}$ for $P$ a generator of E37a: $y^2 = x^3 - 16x + 16$ [2], with contour lines of the limiting density. The top 16% and bottom 16% of points are not shown.
As an application of these growth and distribution results, we explain certain numerical observations of Brenner and Macleod made in [1]. There, Brenner and Macleod find the positive integer solutions \( a, b, c \) to the equation

\[
\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = N. \tag{1}
\]

Solutions to (1) are given by certain rational points on certain elliptic curves \( E_N \). If \( E_N \) has rank 1 and \( P \) is a generator for \( E_N \), then Brenner and Macleod make numerical observations regarding the set of \( n \in \mathbb{Z} \) for which \( nP \) yields a solution to equation (1). In particular, they investigate what the least \( n \) that yields a solution is, as well as what proportion of integers \( n \) yield solutions. Using theorems 1.1 and 1.5 we can explain their observations.

2 Background

Let \( E : y^2 = 4x^3 - g_2x - g_3 \) be an elliptic curve with \( g_2, g_3 \in \mathbb{R} \), and periods \( \omega_1 \) and \( \omega_2 \), chosen such that \( \omega_1 \in \mathbb{R}_{>0} \) and \( \text{Im}(\omega_2) > 0 \). Let \( \Lambda \) be the \( \mathbb{C} \)-lattice with basis \( \langle 1, \frac{\omega_2}{\omega_1} \rangle \). Then \( E/\mathbb{C} \) is parameterized by elements \( z \) of \( \mathbb{C}/\Lambda \) via \( z \mapsto \left( \omega_1^{-2} \varphi \left( \frac{z}{\omega_1} \right), \omega_1^{-3} \varphi' \left( \frac{z}{\omega_1} \right) \right) \), where

\[
\varphi(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda, \lambda \neq 0} \left( \frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right).
\]

This map is an isomorphism of groups and complex analytic varieties between \( \mathbb{C}/\Lambda \) and \( E/\mathbb{C} \). This is a different normalization of the parameterization \( \mathbb{C}/\Lambda \to E(\mathbb{C}) \) given in the introduction.

The function \( \varphi \) is called the Weierstrass-\( \wp \) function, and is discussed at length in [8] and [3]. This function is meromorphic and periodic modulo \( \Lambda \), so \( \varphi(z) \) can only be real when \( z \) either has imaginary part \( 0 \) or \( \frac{1}{2} \text{Im}(\omega_2/\omega_1) \) modulo \( \Lambda \). Furthermore, if \( z \) has imaginary part \( \frac{1}{2} \text{Im}(\omega_2/\omega_1) \), then \( \varphi(z) \) will be real if and only if choosing \( \omega_1 \) to be real forces \( \omega_2 \) to be pure imaginary, in which case \( \Lambda \) is said to be “rectangular”.

The function \( \varphi(z) \) has a pole of order 2 when \( z \in \Lambda \) and has no other poles. From this it follows that the set of \( z \in \mathbb{C}/\Lambda \) which have imaginary part \( 0 \) modulo \( \Lambda \) maps to the unbounded component of \( E(\mathbb{R}) \), and, if \( \Lambda \) is rectangular, the set of \( z \in \mathbb{C}/\Lambda \) which have imaginary part \( \frac{1}{2} \text{Im}(\omega_2/\omega_1) \) modulo \( \Lambda \) maps to the bounded component of \( E(\mathbb{R}) \). If \( z_P \) has imaginary part \( \frac{1}{2} \text{Im}(\omega_2/\omega_1) \), then \( nz_P \) will as well exactly when \( n \) is odd, and thus the \( x \) and \( y \) coordinates of \( nP \) will be on the bounded component of \( E(\mathbb{R}) \) exactly when \( n \) is odd.

For a real number \( r \), let \( \{r\} \) denote the distance from \( r \) to the nearest integer. If \( x(nP) \) and \( y(nP) \) denote the \( x \) and \( y \) coordinates of \( nP \) respectively, then, because \( \varphi(z) \) has a pole of order 2 when \( z \in \Lambda \), we have

\[
x(nP) \approx \omega_1^{-2} \left\{ \frac{z_P}{\omega_1} \right\}^{-2} \quad \text{and} \quad y(nP) \approx -2\omega_1^{-3} \left\{ \frac{z_P}{\omega_1} \right\}^{-3}
\]

when \( z_P \) is real modulo \( \Lambda \) and \( \left\{ \frac{z_P}{\omega_1} \right\} \) is small.

The following lemmas will be useful for studying \( \left\{ \frac{z_P}{\omega_1} \right\} \):

**Lemma 2.1. (Hurwitz)** For all irrational \( \alpha \) there exist infinitely many pairs of integers \( (m,n) \) such that

\[
|\alpha - \frac{m}{n}| < \frac{1}{\sqrt{5}n^2}.
\]

**Proof.** See [5].
Lemma 2.2. (Dirichlet) Let \( \alpha_1, \ldots, \alpha_k \) be irrational numbers. For any natural number \( N \) there exists an \( n < N \) such that

\[
\{n\alpha_j\} < \frac{1}{N^{\frac{1}{k}}}
\]

for all \( j \in \{1, 2, \ldots, k\} \).

Proof. See [4], theorem 200.

Lemma 2.3. (Khinchin) Let \( f \) be a function from \( \mathbb{N} \) to \( \mathbb{R}_{>0} \). If \( \sum_{n=1}^{\infty} f(n)^{-1} \) diverges, then for all real numbers \( \alpha \) except for a set of Lebesgue measure zero, there exist infinitely many pairs of integers \( (m,n) \) such that

\[
|\alpha - \frac{m}{n}| < \frac{1}{nf(n)}.
\]

while if \( \sum_{n=1}^{\infty} f(n)^{-1} \) converges, then the set of real numbers \( \alpha \) for which there exist infinitely many pairs of integers \( (m,n) \) such that

\[
|\alpha - \frac{m}{n}| < \frac{1}{nf(n)}
\]

has Lebesgue measure zero.

Proof. See [7].

In the opposite direction, we have the following:

Lemma 2.4. For any function \( f(n) : \mathbb{N} \to \mathbb{R}_{>0} \), there exists a real number \( \alpha \) such that the inequality

\[
|\alpha - \frac{m}{n}| < \frac{1}{nf(n)}
\]

is satisfied for infinitely many pairs of integers \( (m,n) \).

Proof. See [6].

3 Growth Rates

Using lemmas 2.1, 2.2, 2.3, and 2.4 we can now prove theorems 1.1, 1.4, 1.2, and 1.3.

Proof of theorem 1.1. First suppose that \( P \) is a point of infinite order on the unbounded component of \( E(\mathbb{R}) \), and let \( z_P \) be the preimage of \( P \) under the parameterization \( \mathbb{C}/\Lambda \rightarrow E(\mathbb{C}) \) defined by \( z \mapsto \left( \omega_1^{-2} \varphi\left( \frac{z}{\omega_1} \right), \omega_1^{-3} \varphi'\left( \frac{z}{\omega_1} \right) \right) \), where \( \Lambda \) is the \( \mathbb{C} \) lattice with basis \( (1, \frac{\omega_2}{\omega_1}) \). Then \( z_P \) is real modulo \( \Lambda \). When \( \left\{ \frac{z_P}{\omega_1} \right\} \) is small we have

\[
\varphi\left( \frac{n z_P}{\omega_1} \right) = \left\{ \frac{n z_P}{\omega_1} \right\}^{-2} + \mathcal{O}\left( \left\{ \frac{n z_P}{\omega_1} \right\}^2 \right) \quad \text{and} \quad \varphi'\left( \frac{n z_P}{\omega_1} \right) = -2 \left\{ \frac{n z_P}{\omega_1} \right\}^{-3} + \mathcal{O}\left( \left\{ \frac{n z_P}{\omega_1} \right\} \right),
\]

where the implied constant depends only on \( E \). Lemma 2.1 implies that the inequality \( \left\{ \frac{z_P}{\omega_1} \right\} < \frac{1}{\sqrt{5n}} \) holds for infinitely many \( n \), so for these \( n \) we have

\[
\varphi\left( \frac{n z_P}{\omega_1} \right) > 5n^2 + \mathcal{O}(n^{-2}),
\]

and

\[
\varphi'\left( \frac{n z_P}{\omega_1} \right) > 2 \cdot 5^2 n^3 + \mathcal{O}(n^{-1}).
\]

Now if instead \( P \) is on the bounded component of \( E(\mathbb{R}) \), then \( 2z_P \) is real modulo \( \Lambda \), so the argument above can be applied to \( 2P \).
The most important benefit of corollary 1.6 is that it gives a description of the distribution of $\|z\|_E$ where the implied constant depends only on $\alpha_1$ and $\alpha_2$. One simple application of theorem 1.5 comes from taking $n = 1$. Theorem 1.5 is an immediate consequence of this fact. This lemma implies that, for any irrational $\alpha$, the sequence $a_n = \{na\}$ is equidistributed modulo 1 ([9], Satz 2). Theorem 1.5 is an immediate consequence of this fact.

4 Distributions

Next we turn our attention to results about the full distribution of $x(nP)$ and $y(nP)$ as $n$ varies. Let $X$ be a topological space with a measure $\mu$. We say that a sequence $(a_n)$ of elements of $X$ is equidistributed with respect to $\mu$ if and only if, for every function $f : X \to \mathbb{C}$, we have

$$\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} f(a_k) = \int_X f(x) \, d\mu.$$  

Sometimes we will say that a sequence is equidistributed in a space if it’s clear what the associated measure is.

The following result, due Weyl [9], is an important tool for proving that certain sequences are equidistributed modulo 1:

**Lemma 4.1. (Weyl’s criterion)** A sequence $(a_n)$ of real numbers is equidistributed modulo 1 if and only if for every nonzero integer $\ell$ we have

$$\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \exp(2\pi i\ell a_k) = 0.$$  

This lemma implies that, for any irrational $\alpha$, the sequence $a_n = \{na\}$ is equidistributed modulo 1 ([9], Satz 2). Theorem 1.5 is an immediate consequence of this fact.

One simple application of theorem 1.5 comes from taking $U = [X, \infty] \times \mathbb{R}$ for large $X$ or $U = \mathbb{R} \times [Y, \infty]$ for large $Y$. Then, if $P$ is on the unbounded component of $E(\mathbb{R})$, we have

$$\lim_{n \to \infty} \frac{1}{2n} \# \{|k| < n : x(kP) > X\} = \frac{2}{\omega_1} X^{-\frac{1}{2}} + O(X^{-\frac{2}{5}})$$

and

$$\lim_{n \to \infty} \frac{1}{2n} \# \{|k| < n : y(kP) > Y\} = \frac{2}{\omega_1} Y^{-\frac{4}{5}} + O(Y^{-\frac{2}{5}}),$$

where the implied constant depends only on $E$.

The most important benefit of corollary 1.6 is that it gives a description of the distribution of $nP$ in a way which does not depend on knowledge of the function $\phi$.

**Proof of corollary 1.6.** Let $z_0$ be the preimage of $P_0$ under the map $z \mapsto (\phi(z), \phi'(z))$, and let $\Delta u$ be a real number. Then

\[
(\phi(z_0 + \Delta u), \phi'(z_0 + \Delta u)) = \left(\phi(z_0), \phi'(z_0)\Delta u + \mathcal{O}(\Delta u^2), \phi'(z_0) + \phi''(z_0)\Delta u + \mathcal{O}(\Delta u^2)\right).
\]

Here the implied constant depends on both $E$ and $P_0$. From the equation of $E$ we can deduce that $\phi''(z_0) = 6\phi(z_0)^2 - \frac{2}{y_0^2}$. Using this fact and the preceding equation, we see that the point $(\phi(z_0 + \Delta u), \phi'(z_0 + \Delta u))$ will satisfy $(\phi(z_0 + \Delta u) - x_0)^2 + (\phi'(z_0 + \Delta u) - y_0)^2 < \varepsilon^2$ if and only if

$$|\Delta u| < \frac{\varepsilon}{\sqrt{y_0^2 + (6x_0^2 - \frac{2}{y_0^2})^2}} \left(1 - (\phi'(z_0) + \phi''(z_0)\frac{\mathcal{O}(\Delta u^3)}{\varepsilon^2})\right).$$

Then, after using theorem 1.5 and noting that $\mathcal{O}(\Delta u^3)\varepsilon^{-2} = \mathcal{O}(\varepsilon)$, we can conclude the result. \qed
In [1], Bremner and Macleod give positive integer solutions \(a, b, c\) to the equation

\[
\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = N. \quad (1)
\]

This equation is the elliptic curve \(E_N : y^2 = x^3 + (4N^2 + 12N - 3)x^2 + 32(N + 3)x\), and in the paper, the authors show that the positive integer solutions of (1) correspond to rational points on \(E_N\) with \(x\) coordinate satisfying either

\[
\frac{3 - 12N - 4N^2 - (2N + 5)\sqrt{4N^2 + 4N - 15}}{2} < x < -2(N + 3) \left( N + \sqrt{N^2 - 4} \right)
\]

or

\[
-2(N + 3) \left( N - \sqrt{N^2 - 4} \right) < x < -\frac{4N + 3}{N + 2}.
\]

Theorem 1.5 implies that for any \(P \in E_N(\mathbb{Q})\) of infinite order on the bounded connected component of \(E_N(\mathbb{R})\), the point \(nP\) will correspond to a positive integer solution to (1) for a certain specific proportion of integers \(n\) in the sense of natural density. Writing down what this specific proportion is for general \(N\) can be done using corollary 1.6. For brevity, define

\[
\begin{align*}
A &:= 4N^2 + 12N - 3, \\
x_{1,\text{left}} &:= -\frac{A}{6} - 3(2N + 5)\sqrt{4N^2 + 4N - 15}, \\
x_{2,\text{left}} &:= -2(N + 3)(N - \sqrt{N^2 - 4}) + \frac{A}{3}, \\
B &:= 32(N + 3), \\
x_{1,\text{right}} &:= -2(N + 3)(N + \sqrt{N^2 - 4}) + \frac{A}{3}, \\
x_{2,\text{right}} &:= -\frac{4N + 3}{N + 2} + \frac{A}{3}.
\end{align*}
\]

Moreover, set

\[
\rho(x) := \left( 4x^3 + 4 \left( B - \frac{1}{3} A^2 \right) x + \frac{16}{27} A^3 - \frac{4}{3} AB + \left( 6x^2 + 2 \left( B - \frac{1}{3} A^2 \right) \right)^2 \right)^{-\frac{1}{2}}.
\]

Then the natural density of integers \(n\) for which \(nP\) solves (1) is

\[
\left( \int_{x_{2,\text{left}}}^{x_{2,\text{right}}} \rho(x) \, dx \right)^{-1} \left( \int_{x_{1,\text{left}}}^{x_{1,\text{right}}} \rho(x) \, dx + \int_{x_{2,\text{left}}}^{x_{2,\text{right}}} \rho(x) \, dx \right).
\]

For \(N = 4\), for example, the proportion is approximately 0.068, while for \(N = 38\) the proportion is approximately 0.003. Additionally, one can use the ideas of theorem 1.1 to conclude that, for any \(P \in E_N(\mathbb{Q})\) of infinite order on the bounded connected component of \(E(\mathbb{R})\), the set \(\{P, 2P, \ldots, nP\}\) contains a positive integer solution to (1) whenever \(n \gg N^2\).

\begin{flushright}
References
\end{flushright}


