SPHERE PACKING DENSITIES OF SUBLATTICES OF THE MORDELL-WEIL LATTICES OF TWO FAMILIES OF ELLIPTIC CURVES

ARJUN NIGAM

Abstract. In this paper, we examine certain maximal rank sublattices of the Mordell-Weil lattices of two families of elliptic curves over fields of characteristic $p > 0$. We compute explicit lower bounds on the densest sphere packings of these sublattices by finding lower bounds on the minimal norms of the sublattices and explicitly computing the volumes of their fundamental domains.

1. Preliminaries

A sphere packing in $\mathbb{R}^n$ is an arrangement of non-overlapping spheres of the same radius. The densest sphere packing in $n$ dimensions is a sphere packing in $\mathbb{R}^n$ such that the fraction of the volume occupied by the spheres is maximal. Lagrange proved in 1773 that the densest sphere packing in two dimensions is the hexagonal packing. More than 200 years later, Thomas Hales proved that the cubic close packing and hexagonal close packing arrangements achieve the densest sphere packing in three dimensions. In 2016, Henry Cohn, Abhinav Kumar, Stephen D. Miller, Danylo Radchenko, and Maryna Viazovska resolved the problem of finding the densest sphere packing for dimensions 8 and 24.

Definition 1.1. Let $\Lambda$ be a free $\mathbb{Z}$-module in $\mathbb{R}^n$ of maximal rank. A sphere packing on $\Lambda$ is a non-overlapping arrangement of spheres of the same radius in $\mathbb{R}^n$ such that each sphere is centered at a point of $\Lambda$. The densest sphere packing of $\Lambda$ is a sphere packing on $\Lambda$ of maximal density.

Definition 1.2. Let $\Lambda$ be a free $\mathbb{Z}$-module in $\mathbb{R}^n$ of maximal rank. The packing radius of $\Lambda$ is the radius of the largest open ball in $\mathbb{R}^n$ whose translates by elements of $\Lambda$ do not overlap.

Definition 1.3. Let $k$ and let $E$ be a $k$-scheme. Then a point $P$ of $E$ is called a $k$-rational point if it is a section of the morphism $E \rightarrow \text{Spec}(k)$. When $E$ is a projective variety, this translates to each coordinate of $P$ being an element of $k$. The set of rational points of $E$ over $k$ is denoted as $E(k)$.

Definition 1.4. An elliptic curve over a field $k$ is a smooth, projective, one-dimensional algebraic $k$-variety $E$ of genus 1 with a specified $k$-rational point.

It is a well-known fact that there is a binary operation on $E(k)$ which makes it into an abelian group. Moreover, if $k$ is a number field or a function field over a finite field, then $E(k)$ is a finitely generated abelian group. Thus, we get that $E(k)_{\text{free}} := E(k)/E(k)_{\text{torsion}}$ is a free abelian group of finite rank. There is also a positive-definite quadratic form $\hat{h} : E(k)_{\text{free}} \rightarrow \mathbb{R}$ called the Néron–Tate height. The Néron–Tate height has an associated positive-definite symmetric bilinear form $< - , - > : E(k)_{\text{free}} \times E(k)_{\text{free}} \rightarrow \mathbb{R}$ given by

$$< P, Q > = \frac{1}{2} (\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q))$$

Definition 1.5. A lattice is a finitely generated free abelian group equipped with a positive-definite symmetric bilinear form. The Mordell-Weil lattice of $k$-rational points of an elliptic curve $E$ is the group $E(k)_{\text{free}}$ equipped with the bilinear form described above.

Date: June 15, 2022.
If \((\Lambda, <-, ->)\) is a lattice where \(\Lambda\) is of rank \(n\), then we can find a group homomorphism \(\Phi: \Lambda \rightarrow \mathbb{R}^n\) such that \((\Phi(P)) \cdot (\Phi(Q)) = < P, Q >\) for all \(P\) and \(Q\) in \(\Lambda\). \(\Phi\) can be constructed using the Gram-Schmidt process. Thus, instead of studying the lattice \((\Lambda, <-, ->)\), we can study its image in \(\mathbb{R}^n\) equipped with the usual dot product. Note that \(\Phi\) is not unique. In fact, the images of \(\Lambda\) under different \(\Phi\) may be different. However, they will be isomorphic as lattices. Thus, we can define the \(k\)-density of the densest sphere packing associated to an elliptic curve \(E\) as the density of the densest sphere packing of an embedding of the lattice \(E(k)_{\text{free}}\) into \(\mathbb{R}^n\).

2. General Results

Proposition 2.1. Let \(\rho\) be packing radius of a maximal rank abelian subgroup \(\Lambda \subseteq \mathbb{R}^n\) and let \(V(\Lambda)\) be the volume of the fundamental domain of \(\Lambda\). Then the density of the densest sphere packing of \(\Lambda\) is given by

\[
\frac{\pi^{n/2}}{V(\Lambda) \cdot \Gamma(n/2 + 1)} \rho^n.
\]

Proof. This follows from the formula for the volume of the \(n\)-ball of radius \(\rho\) and the observation that the volume of the fundamental domain occupied by the spheres to achieve the densest packing is exactly the volume of an \(n\)-sphere of radius \(\rho\). \(\square\)

Definition 2.2. Let \(\Lambda\) be a maximal rank free subgroup of \(\mathbb{R}^n\). Then the normalized center density \(\delta_\Lambda\) is given by

\[
\frac{\rho^n}{V(\Lambda)}
\]

where \(\rho\) is the packing radius of \(\Lambda\) and \(V(\Lambda)\) is the volume of the fundamental domain of \(\Lambda\).

It is easy to see that for a fixed \(n\), the ratio of the normalized sphere density and the sphere density is constant for all lattices in \(\mathbb{R}^n\). Thus, having a large lower bound on the normalized sphere packing density gives us a large lower bound on the sphere packing density.

Proposition 2.3. \([\text{Elk94}]\) Let \(E\) be an elliptic curve over \(K\) where \(K\) is a number field or function field over a finite field. For any subfield \(k\) of \(K\), the normalized center density of \(E(k)\) is given by

\[
\Delta^{-1/2} \left( \frac{N_{\text{min}}}{4} \right)^{n/2}
\]

where \(n\) is the rank of \(E(k)\), \(N_{\text{min}}\) is the minimal non-zero value of the Néron–Tate height function, and \(\Delta\) is the absolute value of the determinant of the pairing matrix of the generators of \(E(k)_{\text{free}}\).

Proof. Note that the volume of the fundamental domain of a lattice is the square root of the absolute value of the determinant matrix of a set of generators of the lattice. To avoid overlaps in the Mordell-Weil lattice, the packing radius \(\rho\) must be half the minimal distance between any two distinct points of the lattice. This minimal distance is given by \(\sqrt{N_{\text{min}}}\). \(\square\)

3. The Curve \(E: y^2 = x^3 + t^q - t\)

Let \(p > 3\) be a prime such that \(p \equiv -1\) mod 6, \(q\) an odd power of \(p\), and \(r\) a sufficiently large power of \(p\) (the notion of “sufficiently large" is made precise below). In this section, we consider the curve given by \(y^2 = x^3 + t^q - t\) over the field \(k := \mathbb{F}_r(t)\).

Definition 3.1. Fix an odd \(p\)-power \(q = p^s\). We say that \(r := p^s\) is sufficiently large if \(s\) is a multiple of \(c\), \(8\) divides \((p + 1)s\), and \(3(p^s - 1)\) divides \(p^s - 1\). In particular, \(\mathbb{F}_q \subseteq \mathbb{F}_r\). If \(r\) is sufficiently large, then so are all powers of \(r\).
Definition 3.2. The naive height $h$ of a $\mathbb{F}_r(t)$-rational point $P = (x, y)$ on an elliptic curve is $\deg(x) := \max(\deg(f), \deg(g))$ where $x = \frac{f(t)}{g(t)}$ for $f$ and $g$ coprime polynomials. If $P = [0 : 1 : 0]$, then we define $h(P) = 0$.

We wish to find a lower bound on $N_{\min}$ for our elliptic curve. This is the same as finding the minimum value of $\hat{h}$ on non-torsion points. Since $\hat{h}$ has a bounded difference with the naive height, it is perhaps useful to find a lower bound on the naive height.

Proposition 3.3. The naive height on $E$ is bounded below by $\frac{q+1}{3}$.

Proof. Let $\text{ord}_{\infty}$ denote the valuation at $\infty$. Let $P = (x, y)$ be a point on $E$ that is not the identity. Then we can apply $\text{ord}_{\infty}$ to both sides of $y^2 = x^3 + t^q - t$ to get

$$2\text{ord}_{\infty}(y) = \text{ord}_{\infty}(x^3 + t^q - t).$$

Note that $\text{ord}_{\infty}(t) = -1 \neq -q = \text{ord}_{\infty}(t^q)$. Thus, we may use the strict triangle inequality to get that $\text{ord}_{\infty}(t^q - t) = -q$. However, $q$ is not a multiple of 3, whereas $\text{ord}_{\infty}(x^3) = 3\text{ord}_{\infty}(x)$ is, so we must have, using the strict triangle inequality again, that

$$\text{ord}_{\infty}(x^3 + t^q - t) = \min(3\text{ord}_{\infty}(x) - q).$$

We also know that $2\text{ord}_{\infty}(y) = \text{ord}_{\infty}(y^2) = \min(3\text{ord}_{\infty}(x) - q)$. Since $2$ does not divide $q$, we must have that $3\text{ord}_{\infty}(x) < -q$. Thus, we get

$$\text{ord}_{\infty}(x) \leq -\left(\frac{q+1}{3}\right).$$

This shows that $x$ has a pole of order at least $\frac{q+1}{3}$ at $\infty$, so we must have $h(P) = \deg(x) \geq \frac{q+1}{3}$. □

Using this proposition, we can now prove that the naive height and the Néron–Tate height are the same for our curve.

Proposition 3.4. The Néron–Tate height and the naive height agree on $E$.

Proof. Since the Neron-Tate height $\hat{h}$ is uniquely characterized by the fact that its difference with the naive height $h$ is bounded and $\hat{h}(2P) = 4\hat{P}$ for all $\mathbb{F}_r(t)$-rational point on the curve, it suffices to show that the naive height on $E$ satisfies

$$h(2P) = 4h(P)$$

for all rational points points $P$ on the curve $E$. Clearly, this holds for when $P$ is the identity. Let $P = (x, y)$ be a non-identity $\mathbb{F}_r(t)$-rational point on the curve where $x = \frac{f(t)}{g(t)}$ where $f$ and $g$ are coprime polynomials. By the proof of Proposition 3.3, we have

$$\deg(g) - \deg(f) = \text{ord}_{\infty}(x) \leq -\left(\frac{q+1}{3}\right).$$

This implies that $\deg(f) \geq \deg(g) + \frac{q+1}{3}$, so we conclude that $\deg(x) = \deg(f)$ for all points $P = (x, y)$ with $x = \frac{f}{g}$ where $f$ and $g$ are coprime polynomials.

Now, we compute $2P$ explicitly. Using basic arithmetic of elliptic curves, we see that the first coordinate of the point $2P$ is

$$\frac{f^4 - 8fg^3 \cdot (t^q - t)}{4(gf^3 + g^4 \cdot (t^q - t))}.$$

By our earlier observation on the height of $\mathbb{F}_r(t)$-rational points of $E$, if there is no cancellation between the numerator and the denominator, the naive height of $2P$ is $\deg(f^4 - 8fg^3 \cdot (t^q - t))$. However, using Proposition 3.3, we get

$$\deg(f^4) = 4\deg(f) \geq \deg(f) + 3\deg(g) + q + 1 > \deg(8fg^3 \cdot (t^q - t)).$$
Thus, we get \( \deg(f^4 - 8fg^3 \cdot (t^q - t)) = \deg(f^4) = 4\deg(f) = 4h(P) \).

All we need to show now is that

\[
\frac{f^4 - 8fg^3 \cdot (t^q - t)}{4(gf^3 + g^4 \cdot (t^q - t))}
\]

has no cancellation. Assume that \( \tau \) is an irreducible (in \( \mathbb{F}_r[t] \)) that divides both the numerator and denominator. Then \( \tau \) must also divide

\[
g(f^4 - 8fg^3 \cdot (t^q - t)) - \frac{f}{4}(4(gf^3 + g^4 \cdot (t^q - t))) = -9g^4f \cdot (t^q - t).
\]

Since \( \tau \) is irreducible and \( \theta \neq 0 \), we must then have that \( \tau \) either divides \( g, f \), or \( t^q - t \).

**Case 1:** \( \tau \) divides \( g \)

Since \( \tau \) divides both \( f^4 - 8fg^3 \cdot (t^q - t) \) and \( g \), we must have that it divides \( f \) as well. This is a contradiction as \( f \) and \( g \) were assumed to be coprime polynomials.

**Case 2:** \( \tau \) divides \( f \)

Since \( \tau \) divides both \( gf^3 + g^4 \cdot (t^q - t) \) and \( f \), we must have that it divides either \( g \) or \( t^q - t \). Since \( g \) and \( f \) are coprime polynomials, this can only happen if \( \tau \) divides \( t^q - t \). However, \( \mathbb{F}_q \subseteq \mathbb{F}_r \) and the roots of \( t^q - t \) are precisely the elements of \( \mathbb{F}_r \). Thus, the irreducible \( \tau \) must be of the form \( t - \alpha \) for some \( \alpha \in \mathbb{F}_q \). Since \( \tau \) divides \( f \), we must have that \( f \) has a root at \( \alpha \). Since \( x = \frac{f(t)}{g(t)} \) where \( f \) and \( g \) are coprime polynomials, we also get that \( x \) has a root at \( \alpha \). Since \( t^q - t \) has a root at \( \alpha \) of multiplicity one, we can use the strict triangle inequality to get

\[
2\ord_\alpha(y) = \ord_\alpha(y^2) = \ord_\alpha(x^3 + t^q - t) = \min(\ord_\alpha(x^3), \ord_\alpha(t^q - t)) = 1,
\]

which is a contradiction as \( 2 \) does not divide \( 1 \).

**Case 3:** \( \tau \) divides \( t^q - t \)

Since \( \tau \) divides both \( f^4 - 8fg^3 \cdot (t^q - t) \) and \( t^q - t \), we must have that it divides \( f \) as well. This then leads to the same contradiction as in Case 2.

This shows that there is no cancellation in \( \frac{f^4 - 8fg^3 \cdot (t^q - t)}{4(gf^3 + g^4 \cdot (t^q - t))} \), so the naive height satisfies \( h(2P) = 4h(P) \). \( \square \)

Remark: Using Proposition 3.4, we can give an elementary argument to show that \( E(\mathbb{F}_r(t)) \) is torsion-free for \( r \) sufficiently large. Let \( P = (x, y) \) be a non-trivial \( \mathbb{F}_r(t) \)-rational point on \( E \) that is torsion. By Proposition 3.4, we know that \( 0 = h(2P) = \deg(x) \). This is only possible if \( x = c \) for some \( c \in \mathbb{F}_r \). This would imply that \( y^2 = t^q - t + c^3 \). This means that \( y \) is a polynomial in \( t \). Since \( q \) is an odd integer, \( t^q - t + c^3 \) cannot be the square of a polynomial. This is a contradiction.

**Proposition 3.5.** For \( r \) sufficiently large, \( \text{rank}(E(\mathbb{F}_r(t))) = 2(q - 1) \).

*Proof.* This is Proposition 8.4.1(3) in [UG20]. \( \square \)

**Proposition 3.6.** \( \Delta \) is bounded above by \( r(\mathbb{F}_r(t)) \) for \( r \) sufficiently large.

*Proof.* This follows from Corollary 9.2(3) in [UG20] and the trivial bound \( \text{III}(E) \geq 1 \). \( \square \)

**Proposition 3.7.** For \( r \) sufficiently large, the normalized center density \( \delta_{E(\mathbb{F}_r(t))} \) is bounded below by

\[
\frac{1}{r(\mathbb{F}_r(t))^{1/2}} \cdot \left( \frac{q + 1}{12} \right)^{q - 1}.
\]

*Proof.* This follows by combining the results of Proposition 2.3, Proposition 3.3, Proposition 3.4, Proposition 3.5, and Proposition 3.6. \( \square \)
Let Λ be a maximal rank sublattice of the Mordell-Weil lattice of E. We may then replace Δ by V(Λ) in the formula in Proposition 2.3 to find a lower bound on the normalized packing density of E. With this as the motivation, we list some explicit rational points on the curve and consider the sublattice they generate.

**Proposition 3.8.** Let σ be a solution to \( σ^{6(q-1)} = -1 \) and \( β \) a solution to \( β^d + β = 1 \) in \( \mathbb{F}_r \) for \( r \) sufficiently large. Then \( P = (σ^2(t - (β/σ^6))^{3/2}, σ^2(t - (β/σ^6))^3 + 1) \) is a point in \( E(K) \). Thus, we get \( 6q(q-1) \) \( \mathbb{F}_r(t) \)-rational points on \( E \).

**Proof.** This can be verified by plugging in the point \( P \) into the defining equation of our elliptic curve and using the relations on \( σ \) and \( β \). Alternatively, these points can be deduced by considering the map \( C_{6,q} \rightarrow E_0 \) which we get by presenting \( C_{6,q} \) and \( E_0 : y^2 = x^3 + 1 \) as quotients of the Fermat curve of degree \( q+1 \). \( \Box \)

Using MAGMA, we now compute explicit lower bounds on \( E \) for various values of \( p, q, \) and \( r \).

| \( q \) | \( r \) | Lower Bound on Normalized Density (Using MAGMA) | Lower Bound on Normalized Density (Using Proposition 3.7) | Dimension | Best Known (Normalized) Sphere Packing Density (If Known) |
|------|------|-----------------------------------------------|------------------------------------------------------|-----------|--------------------------------------------------|
| 5    | 5^4  | 0.0625                                        | 0.0625                                               | 8         | 0.0625                                           |
| 5    | 5^8  | 0.0625                                        | 0.0625                                               | 8         | 0.0625                                           |
| 5    | 5^{12}| 0.0625                                        | 0.0625                                               | 8         | 0.0625                                           |
| 5^4  | 5^{16}| \sim 265329770514442013394                   | \sim 619829712395103                                 | 248       |                                                  |
| 11   | 11^2 | \sim 0.0909                                    | \sim 0.0909                                          | 20        | \sim 0.1315                                      |
| 11   | 11^6 | \sim 0.0909                                    | \sim 0.00075                                         | 20        | \sim 0.1315                                      |
| 17   | 17^4 | \sim 2.272                                     | \sim 0.0078                                         | 32        | \sim 2.565                                       |

From this table, we see that there is repetition in the lower bound of the normalized density (computed using MAGMA) when \( q \) is fixed and \( r \) varies. This is to be expected as the explicit points in Proposition 3.8 and the explicit formulation of the Néron–Tate height do not depend on \( r \) (assuming that \( r \) is sufficiently large). Thus, they generate the same lattice. The same repetition is not observed in the lower bound obtained using Proposition 3.7. This is likely due to the fact that we used the trivial bound on \( |\Pi(E(\mathbb{F}_r(t)))| \) when computing it and \( \Pi(E(\mathbb{F}_r(t))) \) may depend on \( r \).

Remark: \( E_8 \) is the unique lattice (up to isometry and rescaling) to have the highest density sphere packing in dimension 8. For \( q = 5 \) and \( r = 5^4 \), we observe that the lower bound obtained equals the sphere packing density of \( E_8 \). This means that the Mordell-Weil lattice must have sphere packing density equal to \( E_8 \) which, by uniqueness, implies that the Mordell-Weil lattice is \( E_8 \). Additionally, we get that the explicit points of Proposition 3.8 generate the entire Mordell-Weil lattice.

### 4. The Legendre Curve

Let \( p \) be an odd prime and \( d = p^f + 1 \) for some positive integer \( f \). Consider the function field \( K_d := \mathbb{F}_p(\mu_d, u) \) where \( \mu_d \) is the set of primitive \( d \)th roots of unity and \( u^d - t = 0 \) for indeterminate \( t \). We study the elliptic curve

\[
E : y^2 = x(x+1)(x+t).
\]

As with the previous curve, we would like to have explicit points on this curve.

**Proposition 4.1.** Let \( E \) and \( K_d \) be as defined. Then for a fixed primitive \( d \)th root of unity \( \zeta \) and \( i \in \{0, 1, \ldots, d-1\} \), the point given by \( P_i := \left( \zeta^i u, \zeta^i u(\zeta^i u + 1)^{d/2} \right) \) is a \( K_d \)-rational point of \( E \).

**Proof.** This can be checked by plugging in each \( P_i \) into the equation defining \( E \) or by observing the action of \( \text{Gal}(K_d/K) \) on the \( K_d \)-rational point \( P := (u, u(u+1)^{d/2}) \). \( \Box \)
Proposition 4.2. The set of explicit rational points in Proposition 4.1 generate a rank \( d - 2 \) subgroup of the Mordell-Weil group. \( E(K_d) \) also has rank \( d - 2 \).

Proof. The first part of this proposition follows from Corollary 4.3 in \([Ulm14]\) and the second part follows from Corollary 5.3 of the same paper. \(\square\)

Thus, we get that the subgroup generated by the \( P^{(d)}_i \) is of finite index in \( E(K_d) \). Just like in the previous section, it is difficult to find a set of generators for the free part of the Mordell-Weil group. However, instead of finding a lower bound on the normalized sphere packing density of \( E \), we can find a lower bound on the normalized sphere packing density of the finite index sublattice generated by the \( P^{(d)}_i \).

Proposition 4.3. The height pairing of the points \( P^{(d)}_i \) is given by

\[
< P^{(d)}_i, P^{(d)}_j > = \begin{cases} 
\frac{(d - 1)(d - 2)}{2d} & \text{if } i = j \\
\frac{1 - d}{d} & \text{if } i \neq j \text{ and } i - j \text{ is even} \\
0 & \text{if } i - j \text{ is odd}
\end{cases}
\]

Proof. This is Theorem 8.2 in \([Ulm14]\) \(\square\)

Proposition 4.4. For any non-torsion point \( Q \) in the subgroup generated by the \( P^{(d)}_i \), we have the inequality

\[
\frac{d - 1}{2d} \leq \hat{h}(Q).
\]

Proof. Let \( Q = \sum_{i=0}^{d-1} a_i P^{(d)}_i \) be a point in the subgroup generated by the \( P^{(d)}_i \). Then we can use bilinearity of the height pairing and the previous proposition to get

\[
\hat{h}(Q) = < \sum_{i=0}^{d-1} a_i P^{(d)}_i, \sum_{i=0}^{d-1} a_i P^{(d)}_i > = \frac{(d - 1)(d - 2)(a_0^2 + \cdots + a_{d-1}^2) + (1 - d)(\sum_{i\neq j} a_i a_j)}{2d}.
\]

Thus, we may write \( \hat{h}(Q) \) as \( \frac{d - 1}{2d} \cdot m \) where \( m \) is some integer. Since the height function is positive definite, we must have that \( m \geq 1 \). This gives us the required lower bound. \(\square\)

Using these results, we can now compute explicit lower bounds on the normalized sphere packing density of \( E \) for various primes \( p \) and non-negative integers \( f \). We list a few examples below:

| \( p \) | \( f \) | Dimension | Normalized Density (Lower Bound) | Best Known (Normalized) Sphere Packing Density | \[Coh17\] |
|---|---|---|---|---|---|
| 3 | 1 | 2 | \( \sim 0.125 \) | \( \sim 0.288 \) | |
| 3 | 2 | 8 | \( \sim 1.953 \times 10^{-6} \) | \( \sim 0.0625 \) | |
| 3 | 3 | 26 | \( \sim 3.208 \times 10^{-26} \) | \( \sim 0.577 \) | |
| 5 | 1 | 4 | \( \sim 0.005 \) | \( \sim 0.125 \) | |
| 5 | 2 | 24 | \( \sim 8.119 \times 10^{-24} \) | \( \sim 1.003 \) | |
| 7 | 1 | 6 | \( \sim 1.22 \times 10^{-4} \) | \( \sim 0.0721 \) | |

We observe that as \( p \) and \( f \) get larger, the normalized density gets smaller. This is because the Gram matrix obtained from the height pairing has a large determinant for large values of \( p \) and \( f \).
5. MAGMA CODE

5.1. Code for a lower bound on the density of the curve \( y^2 = x^3 + t^q - t \).

```magma
p:=5; /* can be any prime equivalent to -1 mod 6*/
c:=1; /* can be any odd integer */
s:=4; /* must be chosen such that it is a multiple of c, (p+1)s is divisible by 8, and 3(p^c-1) divides p^s-1. Once we find such an s, all multiples of it will also work */
r:=p^s;
q:=p^c;
k<zeta> := GF(r);
K<t>:=FunctionField(k);
R<y>:=PolynomialRing(GF(r));
E:=EllipticCurve([0,t^q-t]);
h:= function(P) return Maximum(Degree(Denominator(P[1])),Degree(Numerator(P[1]))); end function;
bil:= function(Q,R) return (h(Q+R)-h(R)-h(Q))/2; end function;
L:=Roots(y^(6*q-6)+1);
M:=Roots(y^q+y-1);
sumt:=t;
A:=[u[1]: u in L];
B:=[v[1]: v in M];
S:=car<a,b>;
Sol:=[E![x[1]^2*(sumt-(x[2]/x[1]^6))^((q+1) div 3),x[1]^3*(sumt-(x[2]/x[1]^6)^q)^((q+1) div 2)]: x in S]; /* These are the explicit points of proposition 3.8 */
I:=[Sol[1]];
k:=2;
while k lt #S and #I lt 2*(q-1) do /* This loop returns a maximal rank sequence of points of Sol */
x:=Sol[k];
M := ZeroMatrix(IntegerRing(),#I+1);
for i in [1..#I] do
    for j in [1..#I] do
        M[i,j]:=bil(I[i],I[j]);
    end for;
end for;
for s in [1..#I] do
    M[s,#I+1]:=bil(I[s],x);
end for;
for r in [1..#I] do
    M[#I+1,r]:=bil(x,I[r]);
end for;
M[#I+1,#I+1]:=bil(x,x);
if Determinant(M) eq 0 then
    k:=k+1;
else
    Append(~I,x);
k:=k+1;
end if;
end while; /* Our next step is to replace I by a Z-linearly independent sequence of points that generates a subgroup bigger than the subgroup generated by I. This will be done by successive iterations of introducing points from Sol and performing the smith-normal form process */
SNFBAS:=[];
for i in [1..#I] do
    v:=ZeroMatrix(IntegerRing(),#I+1,1);
v[i,1]:=1;
end for;
```
Append("SNFBAS",v);
end for;
Grm:= function(J) /* returns the Gram matrix of a sequence of points */
  Gr:=ZeroMatrix(RationalField(),#J);
  for i in [1..#J] do
    for j in [1..#J] do
      Gr[i,j]:=bil(J[i],J[j]);
    end for;
  end for;
  return Gr;
end function;
lincom:= function(Q,J) /* given a basis J and a point Q, the function returns the rational
coefficients of Q when written as a linear combination of elements of J */
  CfQ:=ZeroMatrix(RationalField(),#J,1);
  for i in [1..#J] do
    CfQ[i,1]:=bil(Q,J[i]);
  end for;
  return (Grm(J)^(-1))*CfQ;
end function;
ewbasis:= function(Q,J) /* given a basis J and a point Q, this function returns a Z-basis for the
subgroup generated by Q and the elements of J*/
  n:=lincom(Q,J);
  U:=[ ];
  for p in [1..#J] do
    Append("U",Denominator(n[p,1]));
  end for;
  d:=LCM(U);
  if d eq 1 then
    return J;
  else
    W := ZeroMatrix(IntegerRing(),#J,#J+1);
    for i in [1..#J] do
      W[i,i]:=d;
    end for;
    for j in [1..#J] do
      W[j,#J+1]:=n[j,1]*d;
    end for;
    _,_,WSF:=SmithForm(W);
    for j in [1..#J] do
      Append("L",WSF*SNFBAS[j]);
    end for;
    newbas:=[ ];
    for i in [1..#J] do
      vp:=E!0;
      den:=[ ];
      for j in [1..#J] do
        vp:=vp+L[i][j,1]*J[j];
      end for;
      vp:=vp+L[i][#J+1,1]*Q;
      Append("newbas",vp);
    end for;
    return newbas;
end if;
end function;
for i in [1..#Sol] do
    I:=newbasis(Sol[i],I);
end for;
In:=I;
DetGH:=Numerator(Determinant(Grm(In)));
k:=0;
while((DetGH mod p^k) eq 0) do
    k:=k+1;
end while;
densitylower:=((p^(k-1))^(-0.5))*(((q+1)/12)^(#In div 2));
densitylower;

5.2. Code for a lower bound on the density of the Legendre Curve.

p:=3; /* can choose any odd prime */
f:=2; /* f can be any positive integer */
d:=p^f+1;
M:=ZeroMatrix(RationalField(),d-2); /* the Gram matrix of P_i*/
for i in [1..d-2] do
    for j in [1..d-2] do
        if i eq j then
            M[i,j]:=((d-1)*(d-2))/(2*d);
        elif (i-j) mod 2 eq 0 then
            M[i,j]:=(1-d)/d;
        end if;
    end for;
end for;
det:=AbsoluteValue(Determinant(M));
N:=(d-1)/(2*d);
lowerdensity:= ((N/4)^((d-2)/2))/(Sqrt(det));
lowerdensity;

6. Acknowledgements

I would like to thank Dr. Douglas Ulmer for suggesting the project and mentoring me with it. Dr. Ulmer’s constant encouragement, wisdom, and patient guidance were invaluable in the writing of this paper.

References

[Coh17] H. Cohn. “A conceptual breakthrough in sphere packing”. In: Notices of the American Mathematical Society 64, 2 (2017).

[Elk94] N. Elkies. “Mordell-Weil Lattices in Characteristic 2: I. Construction and First Properties”. In: International Mathematics Research Notices 1994, Issue 8 (1994).

[UG20] D. Ulmer and R. Griffon. “On the arithmetic of a family of twisted constant elliptic curves”. In: Pacific Journal of Mathematics 305 (2020).

[Ulm14] D. Ulmer. “Explicit points on the Legendre curve”. In: Journal of Number Theory 136 (2014).