G. Leterrier *Res. Number Theory (2022)8:23*
https://doi.org/10.1007/s40993-022-00321-0

Research in Number Theory

RESEARCH

On the Mordell–Weil lattice of $y^2 = x^3 + bx + t^{3^n+1}$ in characteristic 3

Gauthier Leterrier

*Correspondence:
gauthier.leterrier@epfl.ch
Department of Mathematics, École Polytechnique Fédérale de Lausanne, Station 8, 1015 Lausanne, Switzerland

Abstract

We study the elliptic curves given by $y^2 = x^3 + bx + t^{3^n+1}$ over global function fields of characteristic 3 ; in particular we perform an explicit computation of the L-function by relating it to the zeta function of a certain superelliptic curve $u^3 + bu = v^{3^n+1}$. In this way, using the Néron–Tate height on the Mordell–Weil group, we obtain lattices in dimension $2 \cdot 3^n$ for every $n \geq 1$, which improve on the currently best known sphere packing densities in dimensions 162 (case $n = 4$) and 486 (case $n = 5$). For $n = 3$, the construction has the same packing density as the best currently known sphere packing in dimension 54, and for $n = 1$ it has the same density as the lattice E_6 in dimension 6.

Keywords: Elliptic curves, Function fields, L-functions, Mordell–Weil group, Sphere packings

Mathematics Subject Classification: 11G05, 11M38, 11T24, 11H31

1 Introduction and main results

Following ideas of Elkies [7–9] and Shioda [18] (from the 1990's), one can use elliptic curves over global function fields to get interesting lattice sphere packings of arbitrarily large rank. This is an opportunity to study their arithmetic, and in particular their L-function. Interestingly, for our family of elliptic curves, we can compute the L-function very explicitly and deduce the main arithmetic invariants of our curves.

For a given positive integer $n \geq 1$ and for an element $b \in \mathbb{F}_{3^n}^\times$, we consider the elliptic curves given by the (affine) Weierstrass equation:

$$E_{n,b} \ : \ y^2 = x^3 + bx + t^{3^n+1} \tag{1.1}$$

over $\mathbb{F}_{3^n}(t)$. One of our main results here is the explicit computation of the L-function of $E_{n,b}$ over $\mathbb{F}_{3^{2n}}(t)$ for some choice of the parameter b. In particular, we can determine the exact value of the (analytic) rank of those elliptic curves.

Theorem 1.1 *Let $n \geq 1$ be an integer and set $q = 3^n$. Let $b \in \mathbb{F}_q^\times$ be any element such that $b^{\frac{q-1}{2}} = (-1)^{n+1}$.*

Then the L-function (as defined in Eq. 2.2) of the elliptic curve $E_{n,b}$ over $\mathbb{F}_{q^2}(t)$ given by (1.1) is equal to

$$L\left(E_{n,b}/\mathbb{F}_{q^2}(t),\ T\right) = (1-q^2T)^{2\cdot 3^n}. \tag{1.2}$$

In particular, the analytic rank of $E_{n,b}$ over $\mathbb{F}_{q^2}(t)$ is equal to $2\cdot 3^n$.

Let us explain how to construct a lattice from those curves. In general, if E is an elliptic curve over a global function field $K = k(X)$, where X is a smooth projective algebraic curve over a finite field k (we will mostly focus on the case $X = \mathbb{P}^1$), then $E(K)$ is a finitely generated abelian group, by Mordell–Weil theorem (generalized by Lang and Néron ; see [19, Theorem III.6.1]). We denote the identity element by O_E.

Given a Weierstrass equation for E over $k(X)$, we have a degree-2 cover $x : E \to \mathbb{P}^1$ given by the x-coordinate. For every $P \in E(k(X)) \smallsetminus \{O_E\}$, we can see $x(P) \in k(X)$ as a rational map $X \dashrightarrow \mathbb{P}^1$. We can therefore define the naive height as

$$\begin{aligned} h : E(K) &\longrightarrow \mathbb{Z}_{\geq 0} \\ P &\longmapsto \begin{cases} \deg(x(P)) & \text{if } P \neq O_E \\ 0 & \text{else} \end{cases} \end{aligned}$$

(if $x(P) \in k$ is constant, its degree is set to be 0). We define the (canonical) Néron–Tate height as

$$\hat{h}(P) := \lim_{n\to+\infty} 4^{-n} h(2^n P) \in \mathbb{R} \tag{1.3}$$

for every $P \in E(K)$. It is a quadratic form, which is positive-definite on $E(K)/E(K)_{\text{tors}}$ ([19, Theorem III.4.3]), where $E(K)_{\text{tors}}$ denotes the torsion subgroup of $E(K)$. Therefore, we obtain a lattice, called the Mordell–Weil lattice of E over K. We introduce a convenient sublattice, namely:

Definition 1.2 The narrow Mordell–Weil lattice of E over K consists of all the points $P \in E(K)$ such that for every place v of K, the reduction $\overline{P}$ is a non-singular point on the reduction $\overline{E_v}$ of a minimal integral Weierstrass model E_v of E at v. It is denoted by $E(K)^0 \subset E(K)$.

Now, given a lattice $L \hookrightarrow \mathbb{R}^d$, let

$$\lambda_1(L) := \min\{\|v\| \ :\ v \in L \smallsetminus \{0\}\} \tag{1.4}$$

be the length of one of its shortest non-zero vectors. Then the translates $B + L$ of the euclidean ball $B = B\left(0, \frac{\lambda_1(L)}{2}\right) \subset \mathbb{R}^d$ by points of L defines a lattice packing of balls. Its density is defined as the proportion of the space covered by $B + L$, i.e.,

$$D(L) := \limsup_{r\to+\infty} \frac{\text{vol}((B+L)\cap B(0,r))}{\text{vol}(B(0,r))} \in [0,1]. \tag{1.5}$$

In the case of such a lattice packing, we can simplify the expression into $D(L) = \frac{(\lambda_1(L)/2)^d \cdot \text{vol}(B(0,1))}{\text{vol}(\mathbb{R}^d/L)}$. This motivates us to consider the following normalization:

Definition 1.3 The center density of a packing of balls given by a lattice $L \hookrightarrow \mathbb{R}^d$ as

$$\delta(L) := \frac{(\lambda_1(L)/2)^d}{\mathrm{vol}(\mathbb{R}^d/L)}.$$

The maximal sphere packing density $P_d := \sup_{L \subset \mathbb{R}^d \text{ lattice}} D(L)$, in a given dimension d, is known exactly only if $d \leq 8$ or if $d = 24$. Minkowski used a non-constructive argument to show that $P_d \geq 2 \cdot 2^{-d}$ (we refer to [6] for more details). Very little seems to be known about explicit lattice constructions that reach this lower bound, let alone exceed it, if the dimension is large enough.

It turns out that as a corollary of Theorem 1.1 and of results of Shioda, we get a lower bound on the sphere packing density of the narrow Mordell–Weil lattice of the elliptic curves $E_{n,b}$.

Corollary 1.4 *Let $n \geq 1$ be an integer, fix $b \in \mathbb{F}_{3^n}^{\times}$ as in Theorem 1.1, and set $q = 3^n$.*

Let $L_n := E_{n,b}\left(\mathbb{F}_{q^2}(t)\right)^0$ be the narrow Mordell–Weil lattice of the elliptic curve $E_{n,b}$ over $\mathbb{F}_{q^2}(t)$, as defined in Definition 1.2.

Then the rank of L_n is $2 \cdot 3^n$ and its center density satisfies the lower bound

$$\delta(L_n) \geq \left(\frac{3^{n-1}+1}{4}\right)^{3^n} \cdot 3^{-n\left(\frac{3^{n-1}-1}{2}\right)-\frac{1}{2}} \tag{1.6}$$

In particular, for $n \in \{1, ..., 7\}$, we get the following values, gathered in the table below.

n	Rank of L_n	$\log_2(\delta(L_n)) \geq$	Best *lattice* packing density known so far
1	6	$\log_2\left(\sqrt{3}/24\right) \simeq -3.79248$	$\delta(E_6) = \frac{\sqrt{3}}{24}$ ([6], p. xix)
2	18	$\log_2\left(\frac{\sqrt{3}}{27}\right) \simeq -3.962406$	-3.79248 [6], p. xix
3	54	$\log_2\left(\frac{\sqrt{3}\cdot 5^{27}}{2^{27}\cdot 3^{13}}\right) \simeq 15.88002$	15.88 (Elkies [6], p. xviii)
4	162	144.1852	130.679 [10]
5	486	741.1001	703.05 [2]
6	1458	3172.032	3236.6 [2]

We see that in dimensions 6 and 54, we get the same density as the previous densest known lattice packings of balls (in fact no construction is provided for the 54-dimensional lattice MW_{54} listed in [6], p. xx). Moreover, in dimensions 162 and 486, we improve the current records. But in dimension 18, another construction achieves a higher packing density, and in dimensions above 1458, non-constructive lower bounds are the best known so far.

1.1 Outline of the proofs

Theorem 1.1 is proved in Sect. 2 by performing an explicit computation of the L-function. This requires counting the number of points on the reduction of $E_{n,b}$ modulo all the places of $\mathbb{F}_{q^2}(t)$, which involves sums of Legendre symbols, introduced in subsection 2.2.

Those sums can be determined thanks to an auxiliary superelliptic curve over $\mathbb{F}_q$ (see subsection 2.3), and using the fact that $x \mapsto x^3 + bx$ is an additive map in characteristic 3 (see Lemmas 2.4, 2.6). Finally, the number of points over $\mathbb{F}_{q^2}$ of this auxiliary superelliptic curve can be computed essentially because its jacobian is isogenous to a power of a *supersingular* elliptic curve.

The idea behind this approach was inspired by the work of Elkies [7], where a counting argument about hyperelliptic curves has been used. In our case, this will get replaced by a *superelliptic* curve (see subsection 2.3).

In both works, the elliptic curves (over function fields of characteristic 2 and 3 respectively) are isotrivial—we also say equivalently"potentially constant". But in our case $E_{n,b}$ is a *cubic* twist of a constant curve (i.e., defined over $\mathbb{F}_q$; see Proposition 3.5), while the elliptic curves studied by Elkies were *quadratic* twists, which is what allowed to compute of the rank and the L-function.

Finally, Corollary 1.4, proved in Sect. 3, follows from the use of Birch–Swinnerton-Dyer formula (known in this case, because $E_{n,b}$ is *isotrivial*, see Theorem 3.4 and Proposition 3.5), as well as a result of Shioda on the lower bound of the height of points in the narrow Mordell–Weil lattice theorem(3.6). In subsection 3.3, we discuss the sharpness of inequality (1.6).

For the convenience of the reader, some frequently used notations are gathered in a list of symbols at the end of this document.

Remark 1.5 Before continuing, we mention that Shioda's results in [17] (especially remark 10 therein) tell us that if m is an even integer and $3^e \equiv -1 \pmod{2m}$ for some integer $e \geq 1$, taken to be minimal, then the rank of $\mathrm{E}_m(\overline{\mathbb{F}_3}(t))$ is $f(\mathrm{E}_m) - 4$, where $f(\mathrm{E}_m)$ denotes the conductor of the elliptic curve $\mathrm{E}_m : y^2 = x^3 + x + t^m$ over $\mathbb{F}_3(t)$.

We are going to investigate the situation where $m = 3^n + 1$ for some integer $n \geq 1$, which is *not* directly covered by the above result. Even if it did apply (e.g., via theorem 1, *ibid.*), we would need to know over what finite field of constants the rank is achieved, so anyway we need to use another technique to determine the rank.

It is also possible to express the L-function of $\mathrm{E_m}$ over $\mathbb{F}_p(t)$ for any odd prime p explicitly in terms of Jacobi sums, which allows to get another proof of theorem 1.1. See also remark 2.8 below.

2 Proof of Theorem 1.1

2.1 Definition of the *L*-function

In this paragraph, we consider a finite field $k = \mathbb{F}_{|k|}$, and we set $K = k(t)$. Recall that the set of places v of K (i.e., an equivalence class of absolute values on K, which are necessarily trivial on k and are non-archimedean) is in bijection with the set of closed points of $\mathbb{P}^1_k$, which is itself in bijection with the set of Galois orbits of $\bar{k}$-rational points in $\mathbb{P}^1(\bar{k})$.

We denote by ∞ the place of K associated to the point $[1 : 0] \in \mathbb{P}^1_k$ (it is given by $-\deg$).

Let E be an elliptic curve over K. For any place v of K, we let E_v be a minimal *integral* Weierstrass model at v. We let $\overline{E_v}$ be its reduction modulo an uniformizer π_v of the ring

of integers $\mathcal{O}_v \subset K_v$ of the completion K_v of K at v, that is: $\overline{E_v} := E_v \times_{\mathcal{O}_v} \mathcal{O}_v/(\pi_v)$. This is a projective plane cubic curve (possibly singular) over the finite field $\mathbb{F}_v := \mathcal{O}_v/(\pi_v)$, and its isomorphism class does not depend on the choice of a minimal integral Weierstrass model E_v (this follows from Proposition VII.1.3 (b) in [20]).

We now define the integers

$$\begin{aligned} A_E(v,j) &:= |k|^j + 1 - \left|\overline{E_v}(\mathbb{F}_{|k|^j})\right|, \\ a_v(E) &:= A_E(v, \deg(v)) = |\mathbb{F}_v| + 1 - \left|\overline{E_v}(\mathbb{F}_v)\right|, \end{aligned} \tag{2.1}$$

where $j \geq 1$ is any integer multiple of $\deg(v) := [\mathbb{F}_v : k]$ (so in particular $\mathbb{F}_{|k|^j}$ is an extension of $\mathbb{F}_v$). Notice that $a_v(E)$ is equal 0 if E has additive reduction at v, and ± 1 if E has multiplicative reduction at v (this follows from Proposition III.2.5 in [20], see also section 2.10 in [26]).

We define the *local factor* at v as

$$L_v(E/K, T) := \begin{cases} 1 - a_v(E)T^{\deg(v)} + |k|^{\deg(v)}T^{2\deg(v)} & \text{if } E \text{ has good reduction at } v \\ 1 - a_v(E)T^{\deg(v)} & \text{else.} \end{cases}$$

The L-function is defined as

$$L(E/K, T) := \prod_{\substack{v \text{ place} \\ \text{of } K}} L_v(E/K, T)^{-1} \in \mathbb{Z}[[T]]. \tag{2.2}$$

One can re-write the L-function as follows (this is Lemme 1.3.15 in [12]), by an elementary computation, where $[w]$ is the place corresponding to w :

$$\log L(E/K, T) = \sum_{j \geq 1} \left(\sum_{w \in \mathbb{P}^1(\mathbb{F}_{|k|^j})} A_E([w], j) \right) \frac{T^j}{j}. \tag{2.3}$$

2.2 Definition of the relevant Legendre sums

We first analyze the reduction types of the elliptic curve $E_{n,b}$ over $\mathbb{F}_{q^2}(t)$, which we state as a proposition for later use. To this end, we recall some standard notations.

Definition 2.1 Let k be a finite field, and let X be a smooth projective geometrically irreducible algebraic curve over k. Denote by g_X its genus. Set $K = k(X)$ and let E be an elliptic curve over K.

(1) We denote by $\Delta_{\min}(E/K)$ the minimal discriminant of E/K (as in [19, Exercise 3.35]). It is a divisor on the curve X.
(2) We denote by $f(E/K)$ the degree of the conductor divisor of E/K (see [19, Exercise 3.36]).
(3) For each place v of K, we denote by $c_v(E/K)$ the local Tamagawa factor of E/K at v, i.e., the number of irreducible components of the special fiber of the Néron model of E at v that have multiplicity 1 and are defined over the residue field $\mathbb{F}_v$ at v. We also set $c(E/K) := \prod_{v \in |X|} c_v(E/K)$.

Proposition 2.2 *Let $E_{n,b}$ be the elliptic curve $y^2 = x^3 + bx + t^{3^n+1}$ over $K_n := \mathbb{F}_{3^{2n}}(t)$ (where $b \in \mathbb{F}_{3^n}^\times$ and $n \geq 1$ are fixed).*

Then $E_{n,b}$ has good reduction at all places $v \neq \infty$ and has bad additive reduction of type IV at $v = \infty$, with the following invariants:

$$\begin{aligned} \deg\left(\Delta_{\min}(E_{n,b}/K_n)\right) &= 12\lceil(3^n+1)/6\rceil = 2\cdot(3^n+3), \\ f(E_{n,b}/K_n) &= \deg\left(\Delta_{\min}(E_{n,b}/K_n)\right) - 2, \\ c(E_{n,b}/K_n) &= c_\infty(E_{n,b}/K_n) = 3. \end{aligned}$$

Proof Its Weierstrass discriminant is $-b^3 \in \mathbb{F}_{3^n}^\times$ according to proposition A.1.1.(b) in [20]. In particular, $E_{n,b}$ had good reduction at all places $v \neq \infty$ and $y^2 = x^3 + bx + t^{3^n+1}$ is a minimal integral Weierstrass model at all $v \neq \infty$.

We follow Tate's algorithm as written down in [19], IV.9, p. 366. Let $m := 3^n + 1$ and $\mu := \lceil \frac{m}{6} \rceil \geq 1$. It is easy to see that $m \equiv 4 \pmod 6$ (e.g., by induction on n), so $6\mu - m = 2$.

The affine equation $E_\infty : y^2 = x^3 + bxt^{-4\mu} + t^{m-6\mu}$ is a minimal integral Weierstrass model at $v = \infty$, where we take $\pi_v := t^{-1}$ as uniformizer.

We have the following coefficients, as defined in [19], IV.9, p. 364 :

$$b_2 = 0, \qquad b_4 = 2bt^{-4\mu}, \qquad b_6 = 4t^{m-6\mu}, \qquad b_8 = -\frac{1}{4}\cdot(2bt^{-4\mu})^2.$$

The singular point on the reduction of E_∞ modulo π is $(\overline{0}, \overline{0})$, which means that the condition in *Step 2* of Tate's algorithm (as in [19], IV.9, p. 366) is satisfied.

Since $6\mu - m = 2$, the constant coefficient $a_6 := t^{m-6\mu}$ is equal to (hence divisible by) π^2. Moreover, b_8 is divisible by π^3, but b_6 is not divisible by π^3. Therefore, Tate's algorithm stops at *Step 5*, which states that E has bad additive reduction of Kodaira–Néron type IV.

From there, we know that the Tamagawa number at $v = \infty$ is $c_\infty(E) = 3$, and that the local conductor is $f_v = v(\Delta) - 2$ and $v_\pi(\Delta) = 12\mu = 12\lceil m/6 \rceil$, since the Weierstrass discriminant is $\Delta = -8b_4^3 - 27b_6^2 = -8\cdot 8b^3\pi^{12\mu}$. □

When k is a finite field of odd cardinality, let $\lambda_k : k^\times \to \{\pm 1\} \hookrightarrow \mathbb{C}^\times$ be the Legendre symbol (i.e., the unique character of order 2, given explicitly by $x \mapsto x^{\frac{|k|-1}{2}}$).

Remark 2.3 It is important to be careful about the subscript k in λ_k, because when q' is a power of some odd prime power q, the restriction of $\lambda_{\mathbb{F}_{q'}}$ to the subfield $\mathbb{F}_q$ is *not* equal to $\lambda_{\mathbb{F}_q}$ (e.g., $\lambda_{\mathbb{F}_{q^2}}(x) = 1$ for every $x \in \mathbb{F}_q$).

According to Eq. 2.3, computing the L-function of $E_{n,b}$ amounts to determining the sums

$$S_b(n,j) := \sum_{w \in \mathbb{P}^1(\mathbb{F}_{(q^2)^j})} A_{E_{n,b}}(w,j), \tag{2.4}$$

where $q = 3^n$, as we have $\log L(E_{n,b}/\mathbb{F}_{q^2}(t), T) = \sum_{j\geq 1} S_b(n,j)\frac{T^j}{j}$. From the Definition (2.1) of $A_E(w,j)$ and of $E_{n,b}$, we see that the above sum is equal to

$$S_b(n,j) = -\sum_{w,x \in \mathbb{F}_{(q^2)^j}} \lambda_{\mathbb{F}_{(q^2)^j}}\left(x^3 + bx + w^{3^n+1}\right). \tag{2.5}$$

Notice that we can discard the terms with $w = [1:0]$ since we have $A_{E_{n,b}}(\infty, j) = 0$ for every $j \geq 1$ by Proposition 2.2.

The strategy to evalute those sums $S_b(n,j)$ consists of two steps :

(1) First, we will compute the number of points on a certain superelliptic curve $C_{n,b}$, given by $v^{3^n+1} = u^3 + bu$ over $\mathbb{F}_{3^{2nj}}$ for every $j \geq 1$, where $b \in \mathbb{F}_{3^n}^\times$ is chosen as in Theorem 1.1.
(2) Secondly, we study the sums

$$\sigma_b(j,t) := \sum_{x \in \mathbb{F}_{3^{2nj}}} \lambda_{\mathbb{F}_{3^{2nj}}}(x^3 + bx + t), \tag{2.6}$$

where $t \in \mathbb{F}_{3^{2nj}}$ and $j \geq 1$ is any integer.

2.3 Number of points on the superelliptic curve $C_{n,b}$

For any $n \geq 1$, let $C_{n,b}^{\mathrm{aff}}$ be the affine curve $v^{3^n+1} = u^3 + bu$, defined over $\mathbb{F}_{3^n}$, where $b \in \mathbb{F}_{3^n}^\times$ satisfies $b^{(3^n-1)/2} = (-1)^{n+1}$ as in the statement of Theorem 1.1. Note that $C_{n,b}^{\mathrm{aff}}$ is smooth.

There is a smooth projective irreducible curve $C_{n,b}$ over $\mathbb{F}_{3^n}$ (unique up to isomorphism) such that its function field is the same as the one of $C_{n,b}^{\mathrm{aff}}$. We say that $C_{n,b}$ is a *superelliptic curve*.

It turns out that $C_{n,b}$ has a unique point at infinity, defined over $\mathbb{F}_{3^n}$ (see Proposition 2 in [11]), so that $|C_{n,b}(k)| = \left|C_{n,b}^{\mathrm{aff}}(k)\right| + 1$ for every finite extension k of $\mathbb{F}_{3^n}$.

The key point is that we will be able to deduce the number of points $|C_{n,b}(\mathbb{F}_{3^{2nj}})|$, for all $j \geq 1$, just from the computation of $|C_{n,b}(\mathbb{F}_{3^{2n}})|$. Now, we can compute $|C_{n,b}(\mathbb{F}_{3^{2n}})|$ because the norm map

$$\mathbb{F}_{3^{2n}}^\times \longrightarrow \mathbb{F}_{3^n}^\times, \qquad v \longmapsto v^{3^n} \cdot v = v^{3^n+1} =: w$$

is a surjective morphism, with kernel of size $\dfrac{3^{2n}-1}{3^n-1} = 3^n + 1$.

Therefore, we get

$$|C_{n,b}(\mathbb{F}_{3^{2n}})| = 1 + 3 + (3^n+1) \sum_{w \in \mathbb{F}_{3^n}^\times} \#\{u \in \mathbb{F}_{3^{2n}} \ : \ u^3 + bu = w\} \tag{2.7}$$

We determine each term in the latter sum in the following lemma (applied to the case where $p := 3$).

Lemma 2.4 *Let p be an odd prime, $n \geq 1$ be an integer, set $q = p^n$ and let $b \in \mathbb{F}_{p^n}^\times$ be any element such that*

$$\mathrm{Nr}_{\mathbb{F}_q/\mathbb{F}_p}(b) \ = \ b^{\frac{p^n-1}{p-1}} = (-1)^{n+1}. \tag{2.8}$$

Then we have

$$\#\{x \in \mathbb{F}_{q^2} \ : \ x^p + bx \in \mathbb{F}_q\} = p^{n+1} = p \cdot q.$$

Proof Consider the maps $f, g_b : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ defined by $f : x \mapsto x^q - x$ and $g_b : x \mapsto x^p + bx$. The key point is that these maps are endomorphisms of the additive group $(\mathbb{F}_{q^2}, +)$ seen as vector space over $\mathbb{F}_p$, and we can describe the set $\{x \in \mathbb{F}_{q^2} \ : \ x^p + bx \in \mathbb{F}_q\}$ as the kernel of $f \circ g_b$. Thereby, the proof essentially boils down to a basic argument of linear algebra. A direct computation shows that $f \circ g_b = g_b \circ f$ (using the fact that $b \in \mathbb{F}_q^\times$).

The rank-nullity theorem yields

$$\dim(\ker(g_b \circ f)) = \dim(\ker(f)) + \dim(\ker(g_b) \cap \mathrm{Im}(f)), \tag{2.9}$$

where the dimensions are taken over $\mathbb{F}_p$.

It is clear that $\dim(\ker(f)) = n$, since $q = p^n$, and that $\ker(g_b)$ has dimension 1 since it consists of roots in $\overline{\mathbb{F}_p}$ of the separable polynomial $X^p + bX$ which has degree p, and all those roots actually lie in $\mathbb{F}_{q^2}$. Indeed, if $x^p = -bx$ then

$$\begin{aligned} x^{p^n} &= (-b)^{1+p+\cdots+p^{n-1}} \cdot x = (-b)^{\frac{p^n-1}{p-1}} \cdot x \overset{(2.8)}{=} (-1)^{\frac{p^n-1}{p-1}} \cdot (-1)^{n+1} x \\ &\overset{p \text{ odd}}{=} (-1)^n \cdot (-1)^{n+1} x = -x, \end{aligned} \tag{2.10}$$

which implies that $x^{q^2} = (x^q)^q = (-x)^q = x$, i.e., $x \in \mathbb{F}_{q^2}$ as claimed.

The above computation (2.10) also shows that any element $x \in \ker(g_b)$ satisfies $x^{p^n} = -x$, so that $f(x) = -2x$, which shows that $x \in \mathrm{Im}(f)$ (recall that p is odd, so $-2 \in \mathbb{F}_p^\times$ is invertible). In other words, we have $\ker(g_b) \cap \mathrm{Im}(f) = \ker(g_b)$. Finally we get $\dim(\ker(f \circ g_b)) = \dim(\ker(g_b \circ f)) = n + 1$ from equation 2.9, which yields

$$\#\{x \in \mathbb{F}_{q^2} \ : \ x^p + bx \in \mathbb{F}_q\} = |\ker(f \circ g_b)| = p^{n+1},$$

which is what we wanted to prove. □

Therefore, from Eq. 2.7 and the above Lemma 2.4 (applied to $p = 3$), we get

$$\begin{aligned} |C_{n,b}(\mathbb{F}_{3^{2n}})| &= 1 + 3 + (3^n + 1)\left(\#\{u \in \mathbb{F}_{3^{2n}} \ : \ u^3 + bu \in \mathbb{F}_{3^n}\} - 3\right) \\ &= 1 + 3^n \cdot 3^{n+1} \end{aligned}$$

We now consider $C_{n,b}$ as a curve over $\mathbb{F}_{3^{2n}}$ (instead of a curve over $\mathbb{F}_{3^n}$). Let us write ω_k for the eigenvalues of the Frobenius endomorphism of $x \mapsto x^{3^{2n}}$ acting on $H^1_{\acute{e}t}(C_{n,b} \times \overline{\mathbb{F}_3}, \mathbb{Q}_\ell)$, where $1 \le k \le 2 \cdot g(C_{n,b})$ and $g(C_{n,b})$ denotes the genus of $C_{n,b}$ and $\ell \neq 3$ is a prime. It is known from the Weil conjectures that the ω_k are the reciprocal of the roots of the numerator (in $\mathbb{Z}[T]$) of zeta function $Z(C_{n,b}/\mathbb{F}_{3^{2n}}, T)$; in particular, they can be seen as complex numbers and their modulus is known to be equal to $|\omega_k| = \sqrt{3^{2n}} = 3^n$. Thereby, Lefschetz trace formula tells us that

$$|C_{n,b}(\mathbb{F}_{3^{2n}})| = 3^{2n} + 1 - \sum_{k=1}^{2g(C_{n,b})} \omega_k.$$

The genus of $C_{n,b}$ is equal to $g(C_{n,b}) = 3^n$ (see Proposition 2 in [11]). Hence we get

$$|C_{n,b}(\mathbb{F}_{3^{2n}})| = 1 + 3^{2n+1} = 3 \cdot 3^{2n} + 1 = 3^{2n} + 1 - \sum_{k=1}^{2 \cdot 3^n} \omega_k,$$

which implies $-2 \cdot 3^{2n} = \sum_{k=1}^{2 \cdot 3^n} \omega_k$. Because the $\omega_k \in \mathbb{C}$ satisfy $|\omega_k| = \sqrt{3^{2n}} = 3^n$, this forces $\omega_k = -3^n$ for every k (e.g., by taking the real part of the latter sum). We conclude that for every $n \ge 1$ and every $j \ge 1$:

$$|C_{n,b}(\mathbb{F}_{3^{2nj}})| = 3^{2nj} + 1 - 2 \cdot 3^n \cdot (-3^n)^j.$$

This completes the step (1) announced above. We can sum up what we have obtained above in terms of the zeta function of $C_{n,b}$:

Proposition 2.5 *Let $n \geq 1$ be an integer and let $b \in \mathbb{F}_{3^n}^{\times}$ be as in Theorem 1.1. The zeta function of the superelliptic curve $C_{n,b}$ over $\mathbb{F}_{3^{2n}}$ is given by*

$$Z\big(C_{n,b}/\mathbb{F}_{3^{2n}},\ T\big) \ = \ \frac{(1+3^nT)^{2\cdot 3^n}}{(1-T)(1-3T)}.$$

In particular, for every $j \geq 1$, we have

$$|C_{n,b}(\mathbb{F}_{3^{2nj}})| = 3^{2nj} + 1 - 2\cdot 3^n \cdot (-3^n)^j.$$

2.4 Evaluating the sums $\sigma_b(j,t)$

This paragraph is devoted to the explicit computation of the sums $\sigma_b(j,t)$ defined in Eq. 2.6. Then we will conclude the proof of theorem 1.1.

Lemma 2.6 *Let $n \geq 1$ be an integer, set $q = 3^n$ and fix $b \in \mathbb{F}_{3^n}$ such that $\lambda_{\mathbb{F}_{3^n}}(b) = (-1)^{n+1}$. Let $j \geq 1$ be any integer. Consider the map $g_{b,j} : \mathbb{F}_{q^{2j}} \to \mathbb{F}_{q^{2j}}$ defined by $g_{b,j} : x \mapsto x^3 + bx$.*

Then for every $t \in \mathbb{F}_{q^{2j}}$ we have :

$$\sigma_b(j,t) = \begin{cases} -2\cdot(-3^n)^j & \text{if } t \in \mathrm{Im}(g_{b,j}) \\ (-3^n)^j & \text{otherwise.} \end{cases}$$

Proof

Step 1 The first key point here is to use again the fact that the map $g_{b,j}$ is additive, in order to deduce that $\sigma_b(j,t)$ takes only two values (for fixed j, b and variable t).
Indeed, if we pick any $x_0 \in \mathbb{F}_{q^{2j}}$, then

$$\begin{aligned}\sigma_b(j,t) &\overset{(2.6)}{=} \sum_{x\in\mathbb{F}_{q^{2j}}} \lambda_{\mathbb{F}_{q^{2j}}}\big(g_{b,j}(x)+t\big) = \sum_{x'\in\mathbb{F}_{q^{2j}}} \lambda_{\mathbb{F}_{q^{2j}}}\big(g_{b,j}(x'+x_0)+t\big) \\ &= \sum_{x'\in\mathbb{F}_{q^{2j}}} \lambda_{\mathbb{F}_{q^{2j}}}\big(g_{b,j}(x') \ + \ g_{b,j}(x_0)+t\big) = \sigma_b(j,t+g_{b,j}(x_0)).\end{aligned}$$

In other words, $\sigma_b(j,t)$ only depends on the class of t in the quotient additive group $\mathbb{F}_{q^{2j}} \big/ \mathrm{Im}(g_{b,j})$. Moreover, notice that

$$\begin{aligned}\sigma_b(j,t) &= \sum_{x'\in\mathbb{F}_{q^{2j}}} \lambda_{\mathbb{F}_{q^{2j}}}\big(g_{b,j}(-x')+t\big) = \sum_{x'\in\mathbb{F}_{q^{2j}}} \lambda_{\mathbb{F}_{q^{2j}}}\big(-g_{b,j}(x')+t\big) \\ &= \lambda_{\mathbb{F}_{q^{2j}}}(-1)\cdot\sigma_b(j,-t) = \sigma_b(j,-t),\end{aligned}$$

where the last equality holds because -1 is a square in $\mathbb{F}_{3^2}$ and hence in $\mathbb{F}_{3^{2nj}}$.
Since $[\mathbb{F}_{q^{2j}} : \mathrm{Im}(g_{b,j})] = |\ker(g_{b,j})| = 3$ (because $-b \in \mathbb{F}_q$ is a square in $\mathbb{F}_{q^2} \hookrightarrow \mathbb{F}_{q^{2j}}$), we deduce that $\sigma_b(j,t)$ only takes two values (for fixed j, b and variable t). The first value occurs when $t \in \mathrm{Im}(g_{b,j})$ in which case $\sigma_b(j,t) = \sigma_b(j,0)$. Let us denote

by σ^* the other value of $\sigma_b(j,t)$, which occurs when $t \notin \mathrm{Im}(g_{b,j})$. Observe that the value of σ^* can be deduced from the sum

$$\sum_{t\in\mathbb{F}_{3^{2nj}}} \sigma_b(j,t) = |\mathrm{Im}(g_{b,j})| \cdot \sigma_b(j,0) \ + \ \left(3^{2nj} - |\mathrm{Im}(g_{b,j})|\right) \cdot \sigma^*$$
$$= 3^{2nj}\left(\frac{1}{3}\sigma_b(j,0) \ + \ \frac{2}{3}\sigma^*\right)$$

because the left-hand side sum vanishes :

$$\sum_{t\in\mathbb{F}_{3^{2nj}}} \sigma_b(j,t) \ = \ \sum_{x\in\mathbb{F}_{3^{2nj}}} \sum_{t\in\mathbb{F}_{3^{2nj}}} \lambda_{\mathbb{F}_{3^{2nj}}}(x^3+bx+t) = 0,$$

since all the inner sums are 0 (they are sums of a non-trivial multiplicative character over the whole group—recall also that $\lambda_{\mathbb{F}_{3^{2nj}}}(0) = 0$). Therefore $\sigma^* = -\frac{1}{2}\sigma_b(j,0)$, so it is enough to determine the value of $\sigma_b(j,0)$.

Step 2 Now we compute the sum $\sigma_b(j,0) = \sum_{x\in\mathbb{F}_{q^{2j}}} \lambda_{\mathbb{F}_{q^{2j}}}(x^3+bx)$.

The most conceptual (and easiest, or shortest) proof relies on the fact that if $\pi : Y \to X$ is a surjective morphism between two smooth irreducible projective algebraic curves (or even varieties) defined over a finite field, then the numerator of the zeta function of X divides the one of Y in $\mathbb{Z}[T]$. This can be argued using the Tate modules of the jacobians of these curves, see for instance Proposition 5 in [1].

In our case, we have the morphism

$$\pi : C_{n,b} \to \mathcal{E}_b \qquad (u,v) \mapsto \left(u, v^{\frac{3^n+1}{2}}\right)$$

where $\mathcal{E}_b$ is the elliptic curve given by $y^2 = x^3 + bx$ over $\mathbb{F}_{3^n}$ (we defined the morphism on the affine charts, but it extends uniquely to a morphism between the smooth projective curves $C_{n,b} \to \mathcal{E}_b$). Being a non-constant morphism between irreducible curves, π must be surjective.

The numerator of $Z(C_{n,b}/\mathbb{F}_{3^{2n}}, T)$ is $(1+3^nT)^{2\cdot 3^n}$ by Proposition 2.5. Therefore, the numerator of $Z(\mathcal{E}_b/\mathbb{F}_{3^{2n}}, T)$ is $(1+3^nT)^2$ (which implies that $\mathcal{E}^b$ is supersingular). Thus we deduce from standard arguments (see [20], application V.1.3 and theorem V.2.3.1) that

$$1 + 3^{2nj} + \sigma_b(j,0) \ = \ |\mathcal{E}_b(\mathbb{F}_{3^{2nj}})| \ = \ 1 + 3^{2nj} - 2(-3^n)^j,$$

which gives the claimed value for $\sigma_b(j,0)$. Therefore, from step 1 we get the value $\sigma^* = (-3^n)^j$ and this finishes the proof.

□

Remark 2.7 It is possible to give more concrete and elementary (but computationally longer) proofs of the identity $\sigma_b(j,0) = -2\cdot(-3^n)^j$ from Lemma 2.6, via quartic Jacobi sums.

Moreover, when n is odd, one can also give a direct proof of the step 2 above, because the change of variables $x \mapsto -x$ allows to determine the number of points of the elliptic curve $\mathcal{E}_b : y^2 = x^3 + bx$ over $\mathbb{F}_{3^n}$ (because -1 is not a square in $\mathbb{F}_{3^n}$) and hence over any field extension thereof.

We are now in position to prove our main result.

Proof of theorem 1.1 By the identity just below Eq. 2.4, we recall that

$$\log L(E_{n,b}/\mathbb{F}_{q^2}(t),\, T) = \sum_{j\geq 1} S_b(n,j)\frac{T^j}{j}.$$

From Eqs. 2.5 2.6, one can write

$$-S_b(n,j) = \sum_{w\in\mathbb{F}_{3^{2nj}}} \sigma_b(j, w^{3^n+1})$$

(be careful of the minus sign). Define the set

$$\Gamma_b(n,j) := \left\{ w \in \mathbb{F}_{3^{2nj}} \;:\; w^{3^n+1} \in \mathrm{Im}(g_{b,j}) \right\},$$

where $g_{b,j} : \mathbb{F}_{3^{2nj}} \to \mathbb{F}_{3^{2nj}}$ denotes the map $x \mapsto x^3 + bx$ as in Lemma 2.6.

Notice that all the fibers of the map

$$C^{\mathrm{aff}}_{n,b}(\mathbb{F}_{3^{2nj}}) \longrightarrow \Gamma_b(n,j), \qquad (u,v) \longmapsto v$$

have size 3 (they have the shape $\{(u,v);(u\pm\beta,v)\}$, where $\beta \in \mathbb{F}_{3^{2n}} \hookrightarrow \mathbb{F}_{3^{2nj}}$ is an element such that $\beta^2 = -b$). Thereby, we deduce from Proposition 2.5 that

$$|\Gamma_b(n,j)| = \frac{1}{3}(|C_{n,b}(\mathbb{F}_{3^{2nj}})| - 1) = \frac{1}{3}(3^{2nj} - 2\cdot 3^n\cdot(-3^n)^j) \tag{2.11}$$

Therefore, using Lemma 2.6 and the above expression of $S_b(n,j)$, we get

$$\begin{aligned} -S_b(n,j) &= -2\cdot(-3^n)^j\cdot|\Gamma_b(n,j)| \quad + \quad (-3^n)^j\cdot\left(3^{2nj} - |\Gamma_b(n,j)|\right) \\ &= (-3^n)^j\cdot\left(3^{2nj} - 3\cdot|\Gamma_b(n,j)|\right) \\ &\overset{(2.11)}{=} (-3^n)^j\cdot 2\cdot 3^n\cdot(-3^n)^j \\ &= 2\cdot 3^{n(1+2j)} = 2q^{1+2j}, \end{aligned}$$

Finally, we conclude that

$$\begin{aligned} \log L(E_{n,b}/\mathbb{F}_{q^2}(t),\, T) &= \sum_{j\geq 1} S_b(n,j)\frac{T^j}{j} \\ &= -2q\sum_{j\geq 1}\frac{(q^2T)^j}{j} \\ &= 2q\cdot\log(1-q^2T), \end{aligned}$$

which precisely means that

$$L\left(E_{n,b}/\mathbb{F}_{q^2}(t),\;T\right) = (1-q^2T)^{2\cdot 3^n},$$

as desired. This finishes the proof. □

Remark 2.8 We explain why the case of characteristic 3 is very special. For an odd prime p, the elliptic surface (of Delsarte type in Shioda's terminology from [17]) associated to $E : y^2 = x^3 + x + t^m$ over $\mathbb{F}_p$ is birationally equivalent to a quotient of the Fermat surface $\mathcal{F}_d$ of degree d, where $d := \frac{4m}{\gcd(2,m)}$. So one can follow the approach taken in [13] to express the L-function of E in terms of Jacobi sums, like $j(\theta, \theta^2) = \sum_{x \in k} \theta(x)\theta^2(1-x)$ for some suitable multiplicative characters θ (of order dividing d) on finite extensions k of $\mathbb{F}_p$.

If $p^e \equiv -1 \pmod{d}$ for some integer $e \geq 1$, then one can apply [24, Proposition 8.1] to compute explicitly those Jacobi sums. However, in our case where $m = p^n + 1$, this condition is not fulfilled so in general this does not allow to compute $j(\theta, \theta^2)$ directly. But in characteristic $p = 3$, we have (when θ^6 is not trivial) $j(\theta, \theta^2) = \dfrac{g(\theta)g(\theta^2)}{g(\theta^3)} = g(\theta^2)$, where $g(\chi) := \displaystyle\sum_{x \in k} \chi(x) \exp\left(\frac{2\pi i}{p} \mathrm{tr}_{k/\mathbb{F}_p}(x)\right)$ is the Gauss sum corresponding to a multiplicative character χ on k. We can then apply Tate–Shafarevitch's lemma [24, Lemma 8.3] to compute $g(\theta^2)$ explicitly in the case $m = 3^n + 1$.

3 Proof of corollary 1.4

We now turn to the proof of the corollary concerning the narrow Mordell–Weil lattice attached to the elliptic curves $E_{n,b}$ (see Definition 1.2), and the lower bound on its sphere packing density (see Definition 1.3).

Estimating the sphere packing density of a lattice L requires three steps :

(1) Determine the rank of L. In the case of the Mordell–Weil lattice of $E_{n,b}$, this is essentially done in Theorem 1.1.
(2) Get an upper bound on the covolume of L. In our case, this is achieved by using the so-called Birch–Swinnerton-Dyer formula which we discuss below.
(3) Finally, get a lower bound on the minimal non-zero norm in L. In the context of the narrow Mordell–Weil lattices, we use a result of Shioda (see Theorem 3.6 below).

3.1 Birch–Swinnerton-Dyer conjecture and formula

We briefly recall what the Birch–Swinnerton-Dyer (BSD) conjecture is, and what is known about it. Originally, it was stated for elliptic curves over $\mathbb{Q}$, but it was then generalized to abelian varieties over any global field. However, for the sake of simplicity, we will stick to the case of elliptic curves over function fields, as given in [14, Conjecture 2.10].

Theorem 2.6 *ibid.* states that the L-function $L(E/K, T)$ of any non-constant elliptic curve over a global function field is a polynomial in T with integral coefficients. In the case of the curves $E_{n,b}$ defined above, Theorem 1.1 provides a proof of the fact $L(E/K, T) \in \mathbb{Z}[T]$. In particular, this allows us to speak of the order of vanishing of the L-function at any given value of T in $\mathbb{C}$. Before stating the conjecture, we introduce some (standard) notations :

Definition 3.1 Let k be a finite field, and let X be a smooth projective geometrically irreducible algebraic curve over k. Denote by g_X its genus. Set $K = k(X)$ and let E be an elliptic curve over K.

(1) Given the Néron–Tate height $\hat{h} : E(K) \to \mathbb{R}_{\geq 0}$ as in Eq. 1.3, we define the pairing

$$\langle -, - \rangle : E(K) \to \mathbb{R}, \quad (P, Q) \mapsto \frac{1}{2} \cdot \left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right).$$

Then the *regulator* of E/K is the discriminant of this pairing, and we denote it by $\mathrm{Reg}(E/K) := \det\Big((\langle P_i, P_j\rangle)_{1\le i,j\le r}\Big)$, where $\{P_1, ..., P_r\}$ is any $\mathbb{Z}$-basis of the free abelian group $E(K)/E(K)_{\mathrm{tors}}$ (we set $\mathrm{Reg}(E/K) = 1$ by convention if the rank is $r = 0$).

(2) We further set the *special value* of the L-function of E/K to be

$$L^*(E/K) \;:=\; \frac{1}{\rho!}L^{(\rho)}(E/K, T)\Big|_{T=|k|^{-1}}$$

where $\rho = \rho(E/K) := \mathrm{ord}_{T=|k|^{-1}} L(E/K, T)$ denotes the *analytic rank*.

(3) The Tate–Shafarevitch group is defined as

$$Ш(E/K) := \ker\Big(H^1(G_K, E(K^{\mathrm{sep}})) \xrightarrow{\mathrm{res}} \prod_{v \text{ places of } K} H^1(G_{K_v}, E(K_v^{\mathrm{sep}}))\Big).$$

where $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ denotes the absolute Galois group (and same for each K_v), and the map is induced by the restriction of cocycles from G_K to G_{K_v} (using embeddings $K^{\mathrm{sep}} \hookrightarrow K_v^{\mathrm{sep}}$).

(4) Finally, we define the *height* of E/K as $H(E/K) := |k|^{\frac{\deg(\Delta_{\min}(E/K))}{12}}$.

Remark 3.2 Because the L-function is a rational function in $\mathbb{Q}(T)$, we also have $L^*(E/K) = \dfrac{L(E/K, T)}{(1-|k|T)^{\rho}}\Big|_{T=|k|^{-1}}$ and this is a non-zero rational number.

There is another normalization of the Néron–Tate height, which is $\hat{h}' := \log(|k|)\cdot\hat{h}$, as in [14] (lecture 3, §2). In that case, for the BSD formula to be true, one has to take the special value of the *complex* L-function, namely the value $\mathcal{L}^*(E/K)$ such that

$$\mathcal{L}(E/K, s) := L\left(E/K, \left|k\right|^{-s}\right) \sim L^*(E/K)\cdot(s-1)^{\rho}, \quad \text{as } s \to 1$$

The two normalizations are consistent. Indeed, on the one hand, if one defines $\mathrm{Reg}'(E/K)$ as the discriminant with respect to the pairing associated to $\hat{h}'$ (as in Definition 3.1), then one has $\mathrm{Reg}'(E/K) = \log(|k|)^r\ \mathrm{Reg}(E/K)$. On the other hand, since $1 - |k|^{1-s} \sim \log(|k|)(s-1)$ as $s \to 1$, we have $\mathcal{L}^*(E/K) = \log(|k|)^r\, L^*(E/K)$.

We make the choice of using $\hat{h}$ and not $\hat{h}'$ because then the narrow Mordell–Weil group $E(K)^0$ (Definition 1.2) becomes an *integral* lattice (see Theorem 3.6).

Conjecture 3.3 *(Birch–Swinnerton-Dyer) Let k be a finite field, and let X be a smooth projective geometrically irreducible curve over k. Denote by g_X its genus. Let E be an elliptic curve over the function field $K := k(X)$.*

Then the following statements hold:

(a) The rank of the finitely generated[1] *abelian group $E(K)$ is equal to the order of vanishing of the L-function of E/K at $T = |k|^{-1}$, i.e.,*

$$\mathrm{rk}_{\mathbb{Z}}\big(E(K)\big) = \mathrm{ord}_{T=|k|^{-1}} L(E/K, T).$$

(b) The Tate–Shafarevitch group $Ш(E/K)$ is finite and we have the following identity, called BSD formula (using notations from Definitions 3.1, 2.1):

$$L^*(E/K) \;=\; \frac{|Ш(E/K)|\cdot\mathrm{Reg}(E/K)\cdot c(E/K)}{|E(K)_{\mathrm{tors}}|^2\cdot|k|^{g_X-1}\cdot H(E/K)}. \tag{3.1}$$

[1] This result of finite generation of $E(K)$ is known as Mordell–Weil theorem, further extended by Néron and Lang.

Theorem 3.4 *(Artin, Tate, Milne) Let E be an elliptic curve over the function field $K := k(X)$, where k is a finite field, as in Definition 3.1.*

(1) The statements (a) and (b) in Conjecture 3.3 are equivalent.
(2) Assume that E is a potentially constant (= isotrivial) elliptic curve, i.e., there is a finite extension K'/K such that the base change $E \times_K K'$ is isomorphic to $E' \times_k K'$ for some (constant) elliptic curve E' defined over k.
Then both statements of Conjecture 3.3 are true.

Proof The first part is proved in [16, Theorem 8.1]. The second claim is stated in Lecture 1, Theorem 12.2 of [25], and is proved in lecture 3, theorem 8.1, *ibid.* □

Proposition 3.5 *The elliptic curve $E_{n,b}$ over $K = \mathbb{F}_{3^{2n}}(t)$ from Theorem 1.1 is isotrivial. More precisely, it is a cubic twist of the constant curve $E' : y'^2 = x'^3 + bx'$ over $\mathbb{F}_{3^n}$.*
Moreover, the Mordell–Weil group $E_{n,b}(K)$ is torsion-free.

Proof The first statement is immediate from the change of variables $y = y', x = x' - u$ where $u \in \overline{\mathbb{F}_3(t)}$ satisfies $u^3 + bu = t^{3^n+1}$ (this exactly defines the superelliptic curve from subsection 2.3). One can also see that the j-invariant of $E_{n,b}$ is 0, so it must be an isotrivial elliptic curve.

We now explain why $E_{n,b}(K)$ is torsion-free. If we consider the cubic extension $K' := K(u)$ of K, with $u \in K$ as above, then we have an isomorphism $E'(K') \xrightarrow{\cong} E_{n,b}(K')$, $(x', y') \mapsto (x' + u, y')$ and $E'(K')_{\text{tors}} = E'(\mathbb{F}_{3^{2n}})$ by [25, Proposition 6.1, Lecture 1]. Since $x' - u \notin K$ whenever $x' \in \mathbb{F}_{3^{2n}}$, this proves that $E_{n,b}(K)$ has to be trivial.

Alternatively, one can prove that $E_{n,b}(K)$ is torsion-free as follows: from Proposition 2.2, we know that the product of the Tamagawa numbers is equal to $c(E_{n,b}/K) = \prod_v c_v = 3$. In particular, this is a square-free integer. But Proposition 6.31 in [22] states that $|E_{n,b}(K)_{\text{tors}}|^2$ divides $\prod_v c_v(E_{n,b}/K)$, so we deduce that $E_{n,b}(K)$ is torsion-free. □

3.2 Lower bound on the minimal norm and on the packing density

We start this subsection in a general framework : we let E be an elliptic curve over a global function field $K = k(X)$ as in Definition 3.1, that is, X is a smooth geometrically irreducible projective curve over a finite field k.

One of the main features of the *narrow* Mordell–Weil lattice $E(K)^0 \subset E(K)$ (Definition 1.2) is that it is an *even integral* lattice, and that we have an explicit lower bound on the minimal height among non-zero vectors.

Theorem 3.6 *(Shioda) Let E be an elliptic curve over a global function field $K = k(X)$. Then for every $P \in E(K)^0 \smallsetminus \{0\}$ we have*

$$\hat{h}(P) \geq \frac{1}{6} \deg\left(\Delta_{\min}(E/K)\right).$$

In particular, $E(K)^0$ is torsion-free. Moreover, $(E(K)^0, \hat{h})$ forms an even integral lattice.
Finally, the index $\left[E(K) : E(K)^0\right]$ divides the product $c(E/K) := \prod_v c_v(E/K)$ of the Tamagawa numbers.

Proof For the lower bound on the minimal non-zero norm and the fact that the lattice $E(K)^0$ is even and integral, see theorem 6.44 in [22], as well as Theorem 5.47 and Corollary 5.50, *ibid*.

We now prove the result on the index $\left[E(K) : E(K)^0\right]$. Let $R \subset |X|$ be the set of bad places of E, where $|X|$ denotes the set of closed points of X. For each $v \in R$, let $G_v := \dfrac{\tilde{\mathcal{E}_v}(\mathbb{F}_v)}{\tilde{\mathcal{E}_v}^0(\mathbb{F}_v)}$ be the component group at v, where $\mathcal{E}_v$ denotes the Néron model of E at v and $\mathbb{F}_v$ is the residue field.

By definition and by [19, Corollary IV.9.2.(c)], $E(K)^0$ is the kernel of the map

$$\theta : E(K) \longrightarrow \prod_{v \in R} G_v$$

defined as follows: for each $v \in R$, there is a unique irreducible component $\Theta_{v,i(v,P)}$ of $\tilde{\mathcal{E}_v}$ that contains the image $\widetilde{P_v}$ of P in $\tilde{\mathcal{E}_v}$. Then $P \longmapsto (\Theta_{v,i(v,P)})_{v \in R}$ induces the above map θ.

The map θ is a group homomorphism (see lemma 6.4 in [21], or just notice that $E(K_v) \cong \mathcal{E}_v(\emptyset_v) \to \tilde{\mathcal{E}_v}(\mathbb{F}_v)$ is a morphism) and therefore, we have an injective morphism

$$E(K)/E(K)^0 \hookrightarrow \prod_{v \in R} G_v,$$

which shows the desired divisibility. □

We can now give a lower bound on the sphere packing density of the narrow Mordell–Weil sublattice $E(K)^0 \subset E(K)$ (see Definition 1.3).

Proposition 3.7 *Let E be an elliptic curve over a global function field $K = k(X)$, where X is a smooth projective curve of genus g_X over a finite field k.*

Assume that the L-function of E/K is of the form $L(E/K, T) = (1 - |k|T)^r$ where r is the rank of $E(K)/E(K)_{\text{tors}}$.

Then the center (sphere packing) density of the narrow Mordell–Weil lattice $E(K)^0 \subset E(K)$ (see Definitions 1.2, 1.3) is bounded below by

$$\delta\left(E(K)^0\right) \geq \frac{\left(\dfrac{\deg\left(\Delta_{\min}(E/K)\right)}{24}\right)^{r/2}}{c(E/K)^{1/2} \cdot |E(K)_{\text{tors}}| \cdot |k|^{g_X/2-1/2} \cdot H(E/K)^{1/2}},$$

where we use the notations from Definitions 3.1, 3.3.

Proof First of all, the hypothesis $L(E/K, T) = (1 - |k|T)^r$ implies that BSD formula is true, by part 1 of theorem 3.4—more precisely we used the implication (a) $\implies$ (b). This hypothesis also forces the special value of the L-function to be $L^*(E/K) = 1$.

Because the cardinality of the finite group Ш(E/K) is at least 1, BSD formula allows us to get an upper bound on the discriminant of $E(K)$:

$$\text{Reg}(E/K) \leq |E(K)_{\text{tors}}|^2 \cdot |k|^{g_X - 1} \cdot H(E/K) \cdot c(E/K)^{-1} \tag{3.2}$$

From Theorem 3.6, we have

$$\lambda_1\left(E(K)^0\right) := \min\left\{\hat{h}(P)^{1/2} \ : \ P \in L_n \setminus \{0\}\right\} \geq \left(\frac{\deg\left(\Delta_{\min}(E/K)\right)}{6}\right)^{1/2}.$$

Now the covolume of $E(K)^0$ is given by

$$\mathrm{covol}\left(E(K)^0\right) = [E(K) : E(K)^0] \cdot \mathrm{covol}(E(K)) = [E(K) : E(K)^0] \cdot \mathrm{Reg}(E/K)^{1/2}.$$

Using the last statement of Theorem 3.6, together with equation Eq. 3.2, we deduce

$$\mathrm{covol}\left(E(K)^0\right) \leq c(E/K)^{1/2} \cdot |E(K)_{\mathrm{tors}}| \cdot |k|^{g_X/2-1/2} \cdot H(E/K)^{1/2}$$

Thereby, combining the above inequalities, we see that the center density of the lattice $L_n = E(K)^0$ is bounded below by

$$\delta\left(E(K)^0\right) \geq \frac{\left(\frac{\deg\left(\Delta_{\min}(E/K)\right)}{24}\right)^{r/2}}{c(E/K)^{1/2} \cdot |E(K)_{\mathrm{tors}}| \cdot |k|^{g_X/2-1/2} \cdot H(E/K)^{1/2}},$$

where r is the rank of lattice $E(K)^0$. Notice that the narrow Mordell–Weil $E(K)^0 \subset E(K)$ is a *full-rank* sublattice (this follows for instance from the last statement of Theorem 3.6 : its index in $E(K)$ is finite), so its rank is the same as the rank of $E(K)$. □

We can now conclude with the proof of our main corollary.

Proof of corollary 1.4 For ease of notation, in what follows, we write $K_n := \mathbb{F}_{3^{2n}}(t)$.

First of all, we notice that the rank of the lattice $L_n := E_{n,b}(K_n)^0$ is equal to $r = 2 \cdot 3^n$. Indeed, Theorem 3.4 and Proposition 3.5 imply that the BSD conjecture (item (a)) is fulfilled. In particular, the algebraic rank of $E_{n,b}$ over K_n agrees with the analytic rank, which equals $2 \cdot 3^n$ by Theorem 1.1.

This very theorem also allows us to apply the above Proposition 3.7. Thereby, the values from Proposition 2.2 and the last statement of Proposition 3.5 (namely the fact $|E_{n,b}(K_n)_{\mathrm{tors}}| = 1$) yield

$$\delta(L_n) \geq \frac{\left((3^{n-1}+1)/4\right)^{3^n}}{3^{1/2} \cdot 3^{n/2 \cdot (3^{n-1}-1)}},$$

which is exactly the lower bound stated in Corollary 1.4. This concludes the proof. □

3.3 Discussion of the sharpness of the lower bound on the packing density

In this paragraph, we shorty study sufficient conditions under which the inequality in Corollary 1.4 is actually an equality. In fact, this lower bound is sharp if and only the following conditions are all satisfied :

- The index $[E(K) : E(K)^0]$ is equal to $c(E/K)$ (instead of just dividing it, as in Theorem 3.6).
- The lower bound on the minimal norm form Theorem 3.6 is achieved, that is there is a point $P \in E(K)^0$ such that $\hat{h}(P) = \frac{1}{6}\deg\left(\Delta_{\min}(E/K)\right)$, which is equal to $3^{n-1}+1$ when $E = E_{n,b}$ according to Proposition 2.2.
- The Tate–Shafarevitch group $Ш(E/K)$ is trivial.

As for the index $[E_{n,b}(K) : E_{n,b}(K)^0]$, where $K := \mathbb{F}_{3^{2n}}(t)$, we can prove easily that it is in fact equal to $c(E_{n,b}/K) = 3$. First, we know from the last statement of Theorem 3.6 that

$[E_{n,b}(K) : E_{n,b}(K)^0]$ must divide $c(E_{n,b}/K) = 3$, so it is either 1 or 3. We prove that the index cannot be equal to 1 by noticing that the point

$$Q_n := \left(0, t^{(3^n+1)/2}\right) \in E_{n,b}(\mathbb{F}_3(t)) \hookrightarrow E_{n,b}(K)$$

does not belong to $E_{n,b}(K)^0$.

Indeed, if we set $\mu = \lceil (3^n+1)/6 \rceil$, then the point Q_n gets mapped to the point $(Q_n)_\infty := \left(0, t^{(3^n+1)/2-3\mu}\right)$ on the minimal integral Weierstrass model $(E_{n,b})_\nu : y^2 = x^3 + bxt^{-4\mu} + t^{3^n+1-6\mu}$ of $E_{n,b}$ at $\nu := \infty$ (via the map $(x, y) \mapsto (xt^{-2\mu}, yt^{-3\mu})$), as in Proposition 2.2. Then $(Q_n)_\infty$ modulo t^{-1} is the singular point $(\overline{0}, \overline{0})$ of $\overline{(E_{n,b})_\nu}$. Therefore, $Q_n \notin E_{n,b}(K)^0$, as claimed.

Let us say a few words on the lower bound $\hat{h}(P) \geq \frac{1}{6} \deg\left(\Delta_{\min}(E_{n,b}/K)\right) = 3^{n-1} + 1$ for $P \in E_{n,b}(K)^0 \smallsetminus \{0\}$. We do not know whether it is a sharp bound in general, but for $n \in \{1, 2, 3\}$ we can exhibit points that achieve this bound. We first list those points explicitly, and then briefly explain how to compute their Néron–Tate height.

- When $n = 1$ and $b = 1$, the point

  $$P_1 = (t^2, -t^3 + t) \in E_{1,1}(\mathbb{F}_3(t)) \hookrightarrow E_{1,1}(K)$$

  has Néron–Tate height 2, i.e., $\hat{h}(P_1) = 3^0 + 1$. Notice that P_1 lies in the narrow Mordell–Weil sublattice, because at $\nu = \infty$, the point P_1 gets mapped to $(1, -1+t^{-2})$ on the minimal integral Weierstrass model at ∞, so it reduces to the smooth point $(\overline{1}, \overline{-1})$ modulo t^{-1}.
- If $n = 2$, let us write $\mathbb{F}_{3^2} \cong \mathbb{F}_3[X]/(X^2 - X - 1)$ and let z be the class of X in $\mathbb{F}_{3^2}$. One can take $b := z$ since $z^{(3^n-1)/2} = z^4 = -1$. The point

  $$P_2 := \left(t^4 + (z+1)t^2 - 1\,,\ -t^6 + t^4 - t^2 - z + 1\right) \in E_{2,b}(\mathbb{F}_{3^2}(t)) \hookrightarrow E_{2,b}(\mathbb{F}_{3^{2n}}(t))$$

  has height 4. Again, P_2 lies in the narrow Mordell–Weil sublattice : its reduction modulo t^{-1} is $(\overline{1}, \overline{-1})$ as for the $n = 1$ case.
- If $n = 3$ and $b = 1$, then

  $$P_3 = \left(t^{10} + t^8 + t^2\,,\ -t^{15} + t^{13} - t^{11} - t^7 - t^5 + t\right) \in E_{3,1}(K)$$

  has height 10. Moreover, as before, P_3 lies in the narrow Mordell–Weil sublattice.

Using Theorem 6.24 of [22], one can show that $\hat{h}(P_n) = 3^{n-1} + 1$ for $n \leq 3$ by checking that the intersection product $(P_n) \cdot (O)$ vanishes, that is, the sections (P_n) and (O)—from $\mathbb{P}^1$ to the elliptic surface associated to $E_{n,b}$—do not intersect (we use the notations from Proposition 5.4 and Notation 5.5 in [22]).

One can argue as in the proof of Proposition 5.1 of [18] (even though the exact statement from there does not directly apply in characteristic 3): both coordinates of P_n are polynomials in t, so have no pole on $\mathbb{A}^1$, and hence (P_n) and (O) do not intersect at any point of $\mathbb{A}^1$. At $\nu = \infty \in \mathbb{P}^1$, we let $\mu = \lceil (3^n + 1)/6 \rceil$ and observe that under the map $(x(t), y(t)) \mapsto (x(t)t^{-2\mu}, x(t)t^{-3\mu})$, the points P_n get mapped to points $(P_n)_\infty$ on the minimal integral Weierstrass model of $E_{n,b}$ at $\nu = \infty$ such that both coordinates have non-zero constant term. Hence, we see that both coordinates have no pole at $\nu = \infty$, and we conclude that (P_n) and (O) never intersect.

Finally, for the order of the Tate–Shafarevitch group, we can just point out that it is a 3-group, i.e., it is equal to its 3-primary part $Ш(E_{n,b}/K) = Ш(E_{n,b}/K)[3^\infty]$, where

$K = \mathbb{F}_{3^{2n}}(t)$. This follows from BSD formula: because $L^*(E_{n,b}/K) = 1$, $|E_{n,b}(K)_{\mathrm{tors}}| = 1$ and $c(E_{n,b}/K) = 3$, we have

$$|Ш(E_{n,b}/K)| \cdot \mathrm{Reg}(E_{n,b}/K) = \frac{1}{3} \cdot (3^{2n})^{-1+\frac{1}{12}\deg(\Delta_{\min}(E_{n,b}/K))}.$$

But we have seen above that $[E_{n,b}(K) : E_{n,b}(K)^0] = 3$, and we know from Theorem 3.6 that $E_{n,b}(K)^0$ is an integral lattice, so it follows that $\mathrm{Reg}(E_{n,b}/K) \in \frac{1}{3^2}\mathbb{Z}$.

Computations on MAGMA [3] seem to indicate that $Ш(E_{n,b}/K)$ is trivial when $n = 1$, but in analogy with [18, Proposition 4.3, Corollary 4.6], it is possible that it is non-trivial for n large enough.

Remark 3.8 In fact, when $n = 1$, i.e., when the rank is $r = 2 \cdot 3^1 = 6$, it is known that the E_6 lattice provides the best *lattice* sphere packing in 6 dimensions [4], and since the lower bound on the density of the lattice $E_{1,1}(\mathbb{F}_{3^2}(t))^0$ agrees with the density of E_6, the lower bound from Corollary 1.4 must be sharp when $n = 1$, in particular $Ш(E_{1,1}/K)$ is trivial.

Remark 3.9 (1) We mention here that when $n \to +\infty$, we have the asymptotic lower bound $\log_2(\delta(L_n)) \geq 3^n \cdot n \cdot \log_2(3) - \frac{n \cdot 3^{n-1}}{2}\log_2(3) + o(n \cdot 3^n)$ from Corollary 1.4. Because the rank of L_n is $r = 2 \cdot 3^n$, this reads

$$\log_2(\delta(L_n)) \geq \left(\frac{1}{2} - \frac{1}{12}\right) r \log_2(r) + o(r \log_2(r)),$$

which implies

$$D(L_n) \geq 2^{-\frac{1}{12} r \log_2(r) \cdot (1+o(1))} = r^{-r/12 \cdot (1+o(1))}, \tag{3.3}$$

where $D(L_n) \in [0, 1]$ is the packing density as defined in Eq. 1.5. Although this is far from attaining Minkowski–Hlawka lower bound $\geq 2^{-r}$, we get the same asymptotic density as in [7, theorem 1] and [18, Eq. (1.12)].

(2) We point out some key properties that are shared by the family of elliptic curves studied here and the ones from [7, 18]. Namely, all these three families $(E_i/\mathbb{F}_{q_i}(t))_{i \geq 1}$ of elliptic curves (ordered by increasing conductor) are such that:

- The Szpiro ratio $\sigma_i := \dfrac{\deg(\Delta_{\min}(E_i))}{f(E_i)} \sim 1$ is asymptotic to 1, as $i \to \infty$.
- Brumer's bound [5, proposition 6.9] is asymptotically sharp: as $i \to \infty$ we have

$$\mathrm{rk}(E_i/\mathbb{F}_{q_i}(t)) \sim \frac{f(E_i)\log(q_i)}{2\log(f(E_i))}$$

In fact, using the upper bound on the Brauer–Siegel ratio stated and proved in [15, Theorem 1.10], one can show that the narrow Mordell–Weil lattices $(L_i)_{i \geq 1}$ attached to any family of non-constant elliptic curves satisfying the BSD conjecture and the two properties above, will satisfy the asymptotic lower bound (3.3), as the conductor goes to infinity.

(3) The densities of the narrow and the full Mordell–Weil lattices compare as follows. Let $Q_n := \left(0, t^{(3^n+1)/2}\right)$ be as above. Using theorem 6.24 and Table 6.1 (p. 127) of [22] and the fact that the reduction of $E_{n,b}$ at $v = \infty$ has type IV (Proposition 2.2), one can show that $\hat{h}(Q_n) = 3^{n-1} + 1 - \frac{2}{3}$, using an argument similar as the one for

the computations of $\hat{h}(P_n)$ above. Then

$$\delta\big(E_{n,b}(\mathbb{F}_{3^{2n}}(t))\big) \leq \frac{\big(\hat{h}(Q_n)^{1/2}/2\big)^{2\cdot 3^n} \cdot [E_{n,b}(\mathbb{F}_{3^{2n}}(t)) : L_n]}{\mathrm{covol}(L_n)}$$

Thus we get, because $[E_{n,b}(\mathbb{F}_{3^{2n}}(t)) : L_n] = 3$ as mentioned previously,

$$\begin{aligned}\frac{\delta\big(E_{n,b}(\mathbb{F}_{3^{2n}}(t))\big)}{\delta(L_n)} &\leq 3 \cdot \left(\frac{\hat{h}(Q_n)}{\lambda_1(L_n)^2}\right)^{3^n} \leq 3 \cdot \left(\frac{3^{n-1}+1-2/3}{3^{n-1}+1}\right)^{3^n} \\ &= 3 \cdot \left(1 - \frac{2}{3^n+3}\right)^{3^n}\end{aligned}$$

Thus the narrow Mordell–Weil lattice L_n is always denser than the full Mordell–Weil lattice, and the ratio of the densities tends to $3e^{-2} \simeq 0.406$ as $n \to +\infty$.

List of symbols	
$A_E(v, j)$	For a multiple j of $\deg(v)$, $A_E(v, j) := \lvert k\rvert^j + 1 - \lvert\overline{E_v}(\mathbb{F}_{\lvert k\rvert^j})\rvert$
$C_{n,b}$	Superelliptic curve with affine model $v^{3^n+1} = u^3 + bu$ over $\mathbb{F}_{3^n}$
$c(E/K)$	Product of the Tamagawa numbers $c_v(E/K)$
$D(L)$	Packing density $D(L) \in [0, 1]$ of a lattice L
$\delta(L)$	Center density of a lattice packing L
$\deg(\Delta_{\min}(E/K))$	Degree of the minimal discriminant of an elliptic curve E/K
$E(K)^0$	Narrow Mordell–Weil lattice
$E_{n,b}$	Elliptic curve $y^2 = x^3 + bx + t^{3^n+1}$ over $\mathbb{F}_{3^n}(t)$
$f(E/K)$	Degree of the conductor of an elliptic curve E/K
$H(E/K)$	Height of E/K, given by $H(E/K) = \lvert k\rvert^{\deg(\Delta_{\min})/12}$
$\hat{h}$	Néron–Tate height $\hat{h} : E(K) \to \mathbb{R}_{\geq 0}$
$L^*(E/K)$	Special value of the L-function of E/K at $s = 1$
L_n	Narrow Mordell–Weil lattice $L_n := E_{n,b}\left(\mathbb{F}_{q^2}(t)\right)^0$
$\lambda_1(L)$	Length of one of the shortest non-zero vectors of a lattice L
λ_k	Legendre symbol $k^\times \to \{\pm 1\}$ of a finite field k
q	$q = 3^n$ where $n \geq 1$
$\mathrm{Reg}(E/K)$	Regulator of an elliptic curve E/K
$S_b(n, j)$	Sum of $A_{E_{n,b}}(w, j)$ over $w \in \mathbb{P}^1(\mathbb{F}_{(q^2)^j})$
$\sigma_b(j, t)$	Sum of $\lambda_{\mathbb{F}_{3^{2nj}}}(x^3 + bx + t)$ over $x \in \mathbb{F}_{3^{2nj}}$

Acknowledgements
I would like to thank my advisor, Prof. Maryna Viazovska, for her support and for having suggested to study this topic. I also thank Vlad Serban, Matthew de Courcy-Ireland and the anonymous referee who gave me helpful comments on an earlier version of this paper. This work was funded by the Swiss National Science Foundation (SNSF), Project funding (Div. I-III),Optimal configurations in multidimensional spaces, http://p3.snf.ch/project-184927 N.184927.

Funding Open access funding provided by EPFL Lausanne.

Received: 26 October 2021 Accepted: 25 February 2022
Published online: 17 March 2022

References

1. Aubry, Y., Perret, M.: Divisibility of zeta functions of curves in a covering. Arch. Math. **82**, 205–213 (2004)
2. Ball, K.: A lower bound for the optimal density of lattice packings. Int. Math. Res. Not. **1992**(10), 217–221 (1992)
3. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I The user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)
4. Blichfeldt, H.F.: The minimum values of positive quadratic forms in six, seven and eight variables. Math. Z. **39**, 1–15 (1935)

5. Brumer, A.: The average rank of elliptic curves I. Invent. Math. **109**(1), 445–472 (1992)
6. Conway, J., Sloane, N.: Sphere Packings, Lattices and Groups, vol. 290, 3rd edn. Springer, Berlin (1998)
7. Elkies, N.D.: Mordell-Weil lattices in characteristic 2: I. Construction and first properties. Int. Math. Res. Not. **8**, 343–361 (1994)
8. Elkies, N.D.: Mordell-Weil lattices in characteristic 2 II: the Leech lattice as a Mordell-Weil lattice. Invent. Math. **128**, 1–8 (1997)
9. Elkies, N.D.: Mordell-Weil Lattices in Characteristic 2, III: A Mordell-Weil Lattice of Rank 128. Exp. Math. **10**(3), 467–473 (2001)
10. Flores, A.L., Interlando, J.C., da Nóbrega Neto, T.P., Dantas Lopes, J.O.: On a refinement of Craig's lattices. J. Pure Appl. Algebra **215**(6), 1440–1442 (2011)
11. Galbraith, S.D., Paulus, S.M., Smart, N.P.: Arithmetic on superelliptic curves. Math. Comput. **71**(237), 393–405 (2002)
12. Griffon, R.: *Analogues du thèoréme de Brauer-Siegel pour quelques familles de courbes elliptiques*. PhD thesis, Université Paris Diderot, France (2016)
13. Griffon, R., Ulmer, D.: On the arithmetic of a family of twisted constant elliptic curves. Pac. J. Math. **305**(2), 597–640 (2020)
14. Gross, B.H.: Lectures on the conjecture of Birch and Swinnerton-Dyer. In: Popescu, C., Rubin, K. (eds.) Arithmetic of *L*-functions, 7th edn., pp. 169–210. American Mathematical Society, Providence (2011)
15. Hindry, M., Pacheco, A.: Analogue of the Brauer-Siegel theorem for abelian varieties in positive characteristic. Moscow Math. J. **16**, 01 (2016)
16. Milne, J.: On a conjecture of Artin and Tate. Ann. Math. **102**(2), 517–533 (1975)
17. Shioda, T.: An explicit algorithm for computing the picard number of certain algebraic surfaces. Am. J. Math. **108**(2), 415–432 (1986)
18. Shioda, T.: Mordell-Weil Lattices and Sphere Packings. Am. J. Math. **113**(5), 931–948 (1991)
19. Silverman, J.H.: Advanced Topics in the Arithmetic of Elliptic Curves, 2nd edn. Springer, Berlin (2008)
20. Silverman, J.H.: The Arithmetic of Elliptic Curves, 2nd edn. Springer, Berlin (2008)
21. Schütt, M., Shioda, T.: Elliptic surfaces. In: Keum, J., Konno, K. (eds.) Algebraic Geometry in East Asia-Seoul 2008, pp. 51–160. Mathematical Society of Japan, Tokyo (2010)
22. Schütt, M., Shioda, T.: Mordell-Weil Lattices, 1st edn. Springer, Berlin (2019)
23. The Sage Developers.: *SageMath, the Sage Mathematics Software System (Version 9.3)* (2021)
24. Ulmer, D.: Elliptic curves with large rank over function fields. Ann. Math. **155**(1), 295–315 (2002)
25. Ulmer, D.: Park City lectures on elliptic curves over function fields. In:*Arithmetic of L-functions*, vol. 18, pp. 213–280. IAS/Park City Mathematics Series (2011)
26. Washington, L.C.: Elliptic Curves, Number Theory and Cryptography, 2nd edn. Chapman and Hall, London (2008)

Publisher's Note