New York Journal of Mathematics

New York J. Math. **22** (2016) 95–114.

# The perfect power problem for elliptic curves over function fields

**Gunther Cornelissen and Jonathan Reynolds**

Abstract. We generalise the Siegel–Voloch theorem about $S$-integral points on elliptic curves as follows: let $K/\mathbf{F}$ denote a global function field over a finite field $\mathbf{F}$ of characteristic $p \geq 5$, let $S$ denote a finite set of places of $K$ and let $E/K$ denote an elliptic curve over $K$ with $j$-invariant $j_E \notin K^p$. Fix a function $f \in K(E)$ with a pole of order $N > 0$ at the zero of $E$. We prove that there are only finitely many rational points $P \in E(K)$ such that for any valuation outside $S$ for which $f(P)$ is negative, that valuation of $f(P)$ is divisible by some integer not dividing $N$. We also present some effective bounds for certain elliptic curves over rational function fields.

Contents



## 1. Introduction

To put our work in context, we cite a few results from the literature on perfect powers and $S$-integral points in linear recurrent sequences and on elliptic curves (the analogy arising from the fact that denominators of rational points on elliptic curves give rise to higher order recurrence sequences called "elliptic divisibility" sequences).

Received April 17, 2015.

2010 *Mathematics Subject Classification.* 11G05, 11D41.

*Key words and phrases.* Elliptic divisibility sequences, Siegel's theorem, perfect powers.

This work was completed whilst the authors enjoyed the hospitality of the University of Warwick (special thanks to Richard Sharp for making it possible) and during a visit of the first author to the Hausdorff Institute in Bonn.

ISSN 1076-9803/2016

- Pethő [12], and Shorey and Stewart have proven that a large class of linear recurrent sequences over the integers contain only finitely many pure powers $> 2$ up to factors from a given finite set of primes (see, e.g., Corollary 2 in [15]).
- Bugeaud, Mignotte and Siksek have applied the modular method to explicitly list all perfect powers in the classical Fibonacci sequence (see, e.g., [4]).
- Lang and Mahler have shown that Siegel's theorem on integral points generalises to the statement that the set of $S$-integral points on curves of genus $\geq 1$ over a number field is finite, for every finite set $S$ of valuations ([16], [9], [10]).
- In [6], it is proven that the set of denominators of points on an elliptic curve over $\mathbf{Q}$ contains only finitely many $\ell$-th powers for *fixed* $\ell > 2$ (cf. also [13] for a general number field).

In this paper, we consider such questions over global function fields $K$ over a finite field $\mathbf{F}$ of characteristic $p \geq 5$ (where we say that $x \in K$ is a perfect $\ell$-th power if all its valuations are divisible by $\ell$). For a study of recurrent sequences in this setting, see, e.g., [8] and references therein. The analogue of Siegel's theorem was proven by Voloch ([23]; under the necessary assumption that the elliptic curve is not isotrivial). We are interested in strenghtening this by considering perfect powers $> 2$ up to a finite set $S$ of valuations in denominators of points on elliptic curves over $K$ (here, "denominators" refers to negative valuations of the coordinates of the point). Our main result generalizes the Siegel–Voloch theorem and at the same time gives a finiteness result that is uniform in the powers that can occur:

**Theorem 1.1.** *Let $K$ be a global function field over a finite field $\mathbf{F}$ of characteristic $p \geq 5$ and $S$ a finite set of places of $K$. Suppose that $E$ is an elliptic curve over $K$ with $j$-invariant $j_E \notin K^p$. Let $f$ denote a function in $K(E)$ with a pole of order $-\operatorname{ord}_O(f) > 0$ at the zero point $O = O_E$ of $E$. Define the set*

$$\mathscr{P}(E,K,S,f)_n := \{P \in E(K) : n \mid \nu(f(P)),\ \text{for all } \nu \notin S \text{ with } \nu(f(P)) < 0\}, \tag{1}$$

*consisting of points $P$ for which the "denominator" of $f(P)$ is an $n$-th power up-to-$S$. Then*

$$\mathscr{P}(E,K,S,f) := \bigcup_{n \nmid \operatorname{ord}_O(f)} \mathscr{P}(E,K,S,f)_n \tag{2}$$

*is finite.*

**Remark 1.2.** The result implies *Voloch's analogue of Siegel's theorem* ([23], 5.3) for curves with $j_E \notin K^p$, which states that the set of $S$-integer values of $f$ on $E$, defined as

$$\mathscr{Q}(E,K,S,f) := \{P \in E(K) \colon \nu(f(P)) \geq 0 \text{ for all } \nu \notin S\}$$

is finite. This is implied by the above theorem by combining it with the equality

$$\mathscr{Q}(E,K,S,f) = \bigcap_{n\geq 1} \mathscr{P}(E,K,S,f)_n.$$

**Remark 1.3.** There is a corresponding statement for smooth curves of genus one (not necessarily with a $K$-rational point), that follows immediately from the theorem: if $C$ is a curve of genus one over a global function field $k$ over $\mathbf{F}$ and $f \in k(C) - k$ is a nonconstant function, then let $O \in C(K)$ denote a pole of $f$ in some finite extension $K/k$. Then if the $j$-invariant of the Jacobian of $C$ is not a $p$-th power in $K$, the set $\mathscr{P}(C,k,S,f)$ (defined as in (1) and (2)) is finite.

Also, replacing $f$ by $f^{-1}$, there is a corresponding result for functions which have a zero at $O$ (but then concerning $P$ for which $\nu(f(P)) > 0$ implies $n \mid \nu(f(P))$).

**Remark 1.4.** To make the *analogy with linear recurrent sequences*, one can apply the theorem to multiples of a fixed (infinite order) point $P$ in $E(K)$ and the coordinate function $x$ on a Weierstrass equation for $E$, for which $\mathrm{ord}_O(x) = -2$, then it says something about perfect powers in the associated elliptic divisibility sequence: assume that $j_E \notin K^p$, and fix a place $\infty$ of $K$ such that the ring of functions $\mathscr{O}$ regular outside $\infty$ is a PID. Factor $x(P) = A_P/B_P^2$ with $A_P$ and $B_P$ coprime in $\mathscr{O}$. Then $\{B_{nP}\}$ is a divisibility sequence in the UFD $\mathscr{O}$ in the conventional sense, and the theorem (with $S = \{\infty\}$) says that it contains only finitely many perfect powers, in the usual meaning of the word.

As was observed in [8] (Lemma 22), if $K$ is a function field, the structure of the formal group associated to $E(K_v)$ implies that if $\nu(x(nP)) < 0$, then $\nu(x(mnP)) = \nu(nP)$ for all integers $m$ coprime to the characteristic of $K$, in stark contrast with the number field case, where $\{\nu(x(mnP))\}_{m\geq 1}$ in unbounded. This does not imply anything about large perfect powers, since it might be that the smallest $n$ for which $\nu(x(nP))$ is negative has very large $-\nu(x(nP))$; see the next remark.

**Remark 1.5.** There is *no absolute (i.e., not depending on the elliptic curve $E$) bound on the power* that can occur in denominators of elliptic curves over function fields. For example, consider the curve

$$E\colon y^2 + xy = x^3 - t^{2d}$$

over the rational function field $K = \mathbf{F}_p(t)$ with $p = 1 \bmod 4$, and let $\{B_m\}$ be the elliptic divisibility sequence over $\mathscr{O} = \mathbf{F}_p[t]$ generated by $P = (0, at^d) \in E(K)$ where $a$ is chosen so that $a^2 = -1 \bmod p$. Then

$$B_1 = B_2 = B_3 = 1 \quad \text{and} \quad B_4 = t^d.$$

(This curve is taken from Theorem 1.5 in [21].)

**Remark 1.6.** The *requirement* $p \geq 5$ arises from our method of proof because we apply the abc-conjecture to a ternary equation associated to the 2-division polynomial on a short Weierstrass form and we take field extensions of degree 2 and 3 in the proof (which could introduce inseparability if $p \leq 3$).

**Remark 1.7.** The following two examples show what can go wrong if $j_E \in K^p$. First, suppose

$$E' \colon y^2 = x^3 + ax + b$$

is an elliptic curve of nonzero rank over $K$ (so $j_{E'} \notin \mathbf{F}$) and let $E$ be given by

$$E \colon y^2 = x^3 + a^p x + b^p$$

for some $a, b \in K$. Then $E(K)$ contains infinitely many $p$-th powers $(\widetilde{x}^p, \widetilde{y}^p)$ for $(\widetilde{x}, \widetilde{y})$ running through the infinite set $E'(K)$. In this example, $j_E \in K^p - \mathbf{F}$.

Secondly, if $y^2 = x^3 + ax + b$ is a curve with $a, b \in \mathbf{F}$ and

$$K \supseteq \mathbf{F}(t, \sqrt{1 + at^4 + bt^6})$$

then $E(K)$ contains the points

$$\left( \frac{1}{t^{2p^m}}, \frac{\sqrt{1 + at^4 + bt^6}}{t^{3p^m}} \right)$$

for all $m$, on which the $x$-coordinate has unbouded negative $t$-valuation. Here, $j \in \mathbf{F}$ is in the ground field, so $j \in K^{p^s}$ for all $s$.

Here is an outline of the proof of the theorem. Throughout the proof we can enlarge the field $K$ to a separable extension and the set $S$ to a larger set of valuations. We use a standard reduction from a general function $f$ to a coordinate function $x$ on a short Weierstrass equation. We use the method of "Klein forms" to show that the existence of a point in $\mathscr{P}(E, K, S, f)_n$ implies the existence of a solution to a ternary equation of the form $X^2 + Y^3 = Z^{4n}$ in $S$-integers. We then use Mason's theorem (the "abc-conjecture in function fields") to bound $n$ unless it is divisible by $p$. We can conclude that the union in (2) needs to be taken over only finitely many $n$. Finally, we use the Siegel identities to prove that each individual $\mathscr{P}(E, K, S, f)_n$ is finite, or $j_E \in K^p$.

In principle, the method is *effective*, in that all occurring constants can be bounded above in terms of $E, K$ and $S$, but doing this abstractly in practice is rather painful, given that the proof involves recurrent enlargement of $K$ and $S$.

As an example of making the results explicit, we prove the following in Section 5.2, which shows what kind of bounds one can expect (i.e., linear in the degree of the discriminant of the curve):

**Proposition 1.8.** *Assume that $E$ is an elliptic curve over a rational function field $K = \mathbf{F}_q(t)$ with coefficients from $\mathbf{F}_q[t]$ such that all 2-torsion points on $E$ are $K$-rational and $j_E \notin K^p$. Assume that $P = 2Q \in 2E(K)$ has associated elliptic divisibility sequence $\{B_n\}$. If $B_n \notin \mathbf{F}$ is a perfect $\ell$-th power of a polynomial in $t$, then we have the following bounds:*

$$\ell \leq 3 \deg \Delta_E + 1; \quad \deg B_n \leq \frac{49}{2} \deg \Delta_E; \quad n \leq \sqrt{\frac{588 \deg \Delta_E}{12h(x(P)) - h(j_E)}},$$

*where $h(x) = \max\{\deg(A), \deg(B)\}$ if $x = A/B$ with $A$ and $B$ coprime in $\mathbf{F}_q[t]$.*

We apply this to an explicit curve in Example 5.3.

In the final section, we briefly discuss what can be proven if the $j$-invariant is a $p$-th power and $j \notin \mathbf{F}$, using Frobenius twists.

## 2. First reductions

**2.1.** Let $K$ denote a global function field of genus $g$ over a finite field $\mathbf{F}$ of characteristic $p \geq 5$, let $M_K$ denote the set of all normalized valuations of $K$, normalized so the product formula holds. Let $S$ denote a nonempty finite set $S \subset M_K$. Let $\mathscr{O}_{K,S}$ denote the ring of $S$-integers

$$\mathscr{O}_{K,S} = \{x \in K : \nu(x) \geq 0 \text{ for all } \nu \notin S\},$$

and

$$\mathscr{O}^*_{K,S} = \{x \in K : \nu(x) = 0 \text{ for all } \nu \notin S\}$$

the ring of $S$-units. We call two elements $a, b \in \mathscr{O}_{K,S}$ *coprime $S$-integers* if for all $\nu \notin S$, either $\nu(a) = 0$ or $\nu(b) = 0$. Since the ground field $\mathbf{F}$ is finite, the class number $h_{K,S}$ of $\mathscr{O}_{K,S}$ is also finite ([14], Prop. 14.2), and this implies:

**Lemma 2.2.** *There exists a set $S'$ consisting of at most $h_{K,S} - 1$ valuations such that $\mathscr{O}_{K,S\cup S'}$ is a PID.*

**2.3.** Let $E$ denote an elliptic curve over $K$, with $j$-invariant $j_E \notin \mathbf{F}$. Fix a short Weierstrass equation $y^2 = x^3 + ax + b$ for $E/K$, which is possible since $p \geq 5$. Let $O = O_E$ denote the zero point of the group $E$. If $P \in E(K)$ is a rational point with $P \neq O$, write it in affine form as $P = (x(P), y(P))$.

**Lemma 2.4.** *Theorem* 1.1 *holds for a field $K$ and a set of valuations $S$ if it holds for a separable field extension $K'/K$ and a set $S'$ of $K'$-valuations that contains the extension of all $S$-valuations to $K'$.*

**Proof.** Under the given conditions, $\mathscr{P}(E, K, S, f)_n \subseteq \mathscr{P}(E, K', S', f)_n$ for all $n$, and separability of $K'/K$ implies that $j_E \notin (K')^p$. □

**Proposition 2.5.** *Theorem* 1.1 *holds true for all nonconstant functions $f$ if it holds true for the coordinate function $x$ on a short Weierstrass model for the curve $E$.*

**Proof.** We claim that if $P \in \mathscr{P}(E,K,S,f)_n$ for some $n$ coprime to $\operatorname{ord}_O f$, then we also have that $P \in \mathscr{P}(E,K,S',x)_{n'}$ for some $n' > 2 = -\operatorname{ord}_O x$ and and extension $S' \supseteq S$, where $x$ is the $x$-coordinate of a Weierstrass model $y^2 = x^3 + ax + b$. The method of proof is taken from [13], 5.2.3 (cf. [18] IX.3.2.2 for a similar reduction in case of Siegel's theorem).

Write $f = (\varphi(x) + y\psi(x))/\eta(x)$ for polynomials $\varphi, \psi, \eta \in K[x]$ of respective degrees $d_1, d_2$ and $d_3$.

First we compute the order of the pole of $f$ at $O$: since $x$ is of order $-2$ and $y$ of order $-3$, we find

$$\begin{aligned} \operatorname{ord}_O(f) &= \operatorname{ord}_O(\varphi(x) + y\psi(x)) - \operatorname{ord}_O(\eta) \\ &= -\max\{2(d_1 - d_3), 2(d_2 - d_3) + 3\}. \end{aligned} \tag{3}$$

Enlarge $S$ so that $a, b$ and all coefficients of these three polynomials are $S'$-integers and their leading coefficients are $S'$-units, keeping $\mathscr{O}_{K,S'}$ a PID. If we write $x(P) = (A/B^2, C/B^3)$ in $S$-integers $A, B, C$ with $B$ coprime to $AC$, then we have the following two expressions for $f(P)$:

$$f(P) = \frac{1}{B^{3+2(d_2-d_3)}} \cdot \frac{B^{3+2(d_2-d_1)}\left(B^{2d_1}\varphi(A/B^2)\right) + C\left(B^{2d_2}\psi(A/B^2)\right)}{B^{2d_3}\eta(A/B^2)} \tag{4}$$

$$= \frac{1}{B^{2(d_1-d_3)}} \cdot \frac{B^{2(d_1-d_2)-3}\left(CB^{2d_2}\psi(A/B^2)\right) + \left(B^{2d_1}\varphi(A/B^2)\right)}{B^{2d_3}\eta(A/B^2)}. \tag{5}$$

First, suppose that in (3), $-\operatorname{ord}_O(f) = 2(d_2 - d_3) + 3 > 0$, or, equivalently, $3 + 2(d_2 - d_1) > 0$. Then in the first representation of $f(P)$ in (4) we find that $B$ is coprime to the numerator and denominator of the second factor. Assume that $v \notin S'$ with $v(x(P)) < 0$, i.e., $v(B) > 0$. Then

$$v(f(P)) = -(3 + 2(d_2 - d_3))v(B) < 0,$$

and from $P \in \mathscr{P}(E,K,S,f)_n$ we conclude that $n \mid v(f(P))$, i.e.,

$$n \mid v(B) \cdot (3 + 2(d_2 - d_3)).$$

The hypothesis $n \nmid \operatorname{ord}_O(f)$ implies that $m \mid v(B)$ for some divisor $m > 1$ of $n$, i.e., $P \in \mathscr{P}(E',K,S',x)_{2m}$ with $m > 1$ (i.e., $2m \nmid \operatorname{ord}_O(x) = -2$).

Secondly, suppose that in (3), $-\operatorname{ord}_O(f) = 2(d_1 - d_3) > 0$, or, equivalently, $2(d_1 - d_2) - 3 > 0$, then in the second representation of $f(P)$ in (5) we find that $B$ is coprime to the numerator and denominator of the second factor. Assume that $v \notin S'$ with $v(x(P)) < 0$, i.e., $v(B) > 0$. Then

$$v(f(P)) = -2(d_1 - d_3))v(B) < 0,$$

and from $P \in \mathscr{P}(E,K,S,f)_n$ we conclude that $n \mid v(f(P))$, i.e.,

$$n \mid v(B) \cdot 2(d_1 - d_3).$$

The hypothesis $n \nmid \operatorname{ord}_O(f)$ implies that $m \mid v(B)$ for some divisor $m > 1$ of $n$, i.e., $P \in \mathscr{P}(E',K,S',x)_{2m}$ with $m > 1$ (i.e., $2m \nmid \operatorname{ord}_O(x) = -2$). $\square$

## 3. Bounding the exponent

Without loss of generality, we assume that $E$ is given by a Weierstrass equation in short form $y^2 = x^3 + ax + b$, with $j_E \notin K^p$ and $f = x$. For the next reduction, we take our inspiration from Bennett and Dahmen ([2], Section 2) in using a classical syzygy for binary cubic forms, applied to the 2-division polynomial.

**Proposition 3.1.** *Given $E$, up to replacing $K$ by a sufficiently large separable extension and enlarging $S$ so that $\mathscr{O}_{K,S}$ is a PID, we have the following: if there exists $P \in \mathscr{P}(E, K, S, x)_n \neq \emptyset$, then there exists a solution to*

$$X^3 + Y^2 = Z^{4\ell} \text{ where } \ell = \begin{cases} n \text{ if } n \text{ is odd;} \\ n/2 \text{ if } n \text{ is even,} \end{cases}$$

*with $X, Y, Z \in \mathscr{O}_{K,S}$ pairwise coprime and $\nu(Z) = 0$ for all $\nu \in S$, and with $B_P = Z^\ell v$ for some $S$-unit $v$, where $x(P) = A_P/B_P^2$ is a representation in coprime $S$-integers.*

**Proof.** There exists a finite separable extension $K'$ of $K$ such that $E(K) \subseteq 2E(K')$: it suffices to let $K'$ contain the coordinates of the solutions $D$ to the equations $C = 2D$ for $C$ running through a finite set of generators for $E(K)$ (this can also be done without halving generators, see Remark 3.3 below). Separability of $K'/K$ follows from the fact that the degree of $K'/K$ is only divisible by powers of 2 and 3, and we assume $p \geq 5$.

Replace $K$ by $K'$. Without loss of generality, enlarge $S$ so that it contains all divisors of the discriminant $\Delta_E$ of $E$, and such that the coefficients of the Weierstrass model of $E$ are in $\mathscr{O}_{K,S}$ and $\mathscr{O}_{K,S}$ is a principal ideal domain. Suppose that $P \in \mathscr{P}(E, K, S, x)$, and write $2Q = P$ with $Q \in E(K)$, where $x(Q) = A_Q/B_Q^2$ with $A_Q, B_Q$ coprime in $\mathscr{O}_{K,S}$. Then

$$\frac{A_P}{B_P^2} = \frac{B_Q^8 \vartheta_2(A_Q/B_Q^2)}{B_Q^2 \psi_2^2(A_Q/B_Q^2) B_Q^6}.$$

where

$$\vartheta_2(x) = x^4 - 2ax^2 - 8bx + a^2 \text{ and } \psi_2^2(x) = 4(x^3 + ax + b)$$

are classical division polynomials. This gives a representation of $x(Q)$ in which numerator and denominator are in $\mathscr{O}_{K,S}$, and (cf., e.g., Ayad [1]) the greatest common divisors of numerator and denominator divides the discriminant $\Delta_E$ of $E$. Furthermore, the factors $B_Q^2$ and $\psi_2^2(A_Q/B_Q^2)B_Q^6$ are coprime.

Consider the binary cubic form

$$K_2(X, Y) = 4(X^3 + aXY^2 + bY^3).$$

A classical result, a "syzygy for the covariants", apparently first discovered by Eisenstein [5] (cf. [7]), says the following:

**Lemma 3.2.** *If $F$ is a binary cubic form with discriminant $\Delta_F$, set*

$$H(x,y) = \frac{1}{4}\det\begin{pmatrix} \frac{\partial^2 F}{\partial x\partial x} & \frac{\partial^2 F}{\partial x\partial y} \\ \frac{\partial^2 F}{\partial x\partial y} & \frac{\partial^2 F}{\partial y\partial y}\end{pmatrix} \quad \textit{and} \quad G(x,y) = \det\begin{pmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} \\ \frac{\partial H}{\partial x} & \frac{\partial H}{\partial y}\end{pmatrix}.$$

*Then*

$$G^2 + 4H^3 = -27\Delta_F F^2. \tag{6}$$

We return to the proof of Proposition 3.1. If $P \in \mathscr{P}(E,K,S,x)_n$ for some $n > 2$, then $B_P = uC^\ell$ where $\nu(u) = 0$ for $\nu \notin S$, and $\ell = n$ if $n$ is odd and $\ell = n/2$ if $n$ is even. We see that

$$K_2(A_Q, B_Q^2) = \psi_2^2(A_Q/B_Q^2)B_Q^6 = u^2C^{2\ell}/\delta,$$

with $\nu(\delta) \neq 0$ only for the finitely many valuations $\nu$ for which $\nu(\Delta_E) \neq 0$, which are included in $S$.

The syzygy (6) for $F = K_2$ (with $\Delta_F = \Delta_E$) gives an equation of the form

$$aX^3 + bY^2 = Z^{4\ell},$$

where $X, Y, Z \in \mathscr{O}_{K,S}$ are nonzero and $a, b$ are $S$-units with

$$a = -\frac{\delta}{27u^4\Delta_E}, \qquad b = -\frac{4\delta}{27u^4\Delta_E},$$
$$X = G(A_Q, B_Q^2), \qquad Y = H(A_Q, B_Q^2), \qquad Z = C.$$

Since the resultant of any pair of $F, G$ and $H$ is a divisor of $\Delta_E^3$ (as can be seen by direct computation, or as in Prop. 2.1 in [2]), we find that the only common divisors of any pair of $X, Y$ and $Z$ belongs to $S$, i.e., $X, Y$ and $Z$ are pairwise coprime $S$-integers. Furthermore, if $\nu(Z) \neq 0$ for some $\nu \in S$, fix a uniformizer $\pi_\nu \in \mathscr{O}_{K,S}$ for $\nu$ (this is possible since we assume $\mathscr{O}_{K,S}$ is a PID), and replace the equation by

$$a'X^3 + b'Y^2 = (Z')^{4\ell}$$

with

$$a' = \pi_\nu^{-4\ell\nu(Z)}a, \quad b' = \pi_\nu^{-4\ell\nu(Z)}b \quad \text{and} \quad Z' = \pi_\nu^{-\nu(Z)}Z;$$

then the new equation has has $\nu(Z') = 0$. Doing this for all such (finitely many) valuations, we may assume $\nu(Z) = 0$ for $\nu \in S$. Note that $B_P = Z^\ell v$ for an $S$-unit $v$.

Dirichlet's $S$-unit theorem for function fields (due to F. K. Schmidt, cf., e.g., [14], 14.2) shows that there are only finitely many values of $a$ and $b$ up to sixth powers, so we can enlarge $K$ to contain the relevant sixth roots (separable since $p \geq 5$) to find a solution in $K$ to $X^3 + Y^2 = Z^{4\ell}$ with $X, Y, Z$ coprime $S$-integers and $\nu(Z) = 0$ for all $\nu \in S$. □

**Remark 3.3.** In explicit bounds, the following observation might be useful. The extension $K'/K$ such that $E(K) \subseteq 2E(K')$ that is needed at the start of the proof can be constructed independently of choosing generators for $E(K)$: if $P = (x(P), y(P))$ satisfies the Weierstrass equation, we find that

$$\prod_{T \in E[2]-O} (x(P) - x(T)) = y(P)^2$$

is a square. Extend $S$ so that $\mathscr{O}_{K,S}$ is a PID. Now the common divisors of the factors on the left hand side divide $\Delta_E$. Therefore, if we extend $K$ to $K'$ so that all prime divisors of $\Delta_E$ and all elements of $\mathscr{O}_{K,S}^*$ (in which squares have finite index by the function field analogue of Dirichlet's unit theorem) become squares in $K'$, then all $x(P) - x(T)$ are squares in $K'$. Now the explicit formula for the 2-isogeny $[2]\colon E \mapsto E$ implies that $E(K) \subseteq 2E(K')$.

**3.4.** The (logarithmic) height of $x \in K$ is defined by

$$h(x) = -\sum_{\substack{\nu \in M_K \\ \nu(x) < 0}} \nu(x).$$

Note that $h(x) \geq 0$ and $h(x) \in \mathbf{Z}$ for all $x \in K$. Let

$$h(x)_0 = \sum_{\substack{\nu \in M_K \\ \nu(x) > 0}} \nu(x).$$

Note that $\nu(1/x) = -\nu(x)$, so $\nu(x) > 0$ if and only if $\nu(1/x) < 0$. Thus, by the product formula:

**Lemma 3.5.** *For all $x \in K^*$, $h(1/x) = h(x)_0 = h(x)$.*

We will apply the following theorem of Mason's (the "abc-conjecture for function fields"):

**Theorem 3.6** (Mason [11] Lemma 10, p. 97)**.** *Suppose that $\gamma_1, \gamma_2$ and $\gamma_3$ are nonzero elements of $K$ with*

$$\gamma_1 + \gamma_2 + \gamma_3 = 0 \quad \textit{and} \quad \nu(\gamma_1) = \nu(\gamma_2) = \nu(\gamma_3)$$

*for each valuation $\nu$ not in a finite set $T$. Then either*

$$\gamma_1/\gamma_2 \in K^p \quad \textit{or} \quad h(\gamma_1/\gamma_2) \leq |T| + 2g_K - 2.$$

**Remark 3.7.** It seems that for $g_K = 0$ and $|T| \leq 1$, the right hand side could be negative. However, if $T = \emptyset$, then $\gamma_i$ have the same valuation for all $v$, and hence their quotients $\gamma_i/\gamma_j$ are in the constant field $\mathbf{F}$; in particular, since $\mathbf{F}$ is finite, they are in $K^p$. If $|T| = 1$, then $\gamma_i$ have the same valuation at all but one $v$; but then, by the product formula, they have the same valuation everywhere, and the previous argument applies.

**Remark 3.8.** If $\gamma_1+\gamma_2+\gamma_3=0$, then $\gamma_1/\gamma_2 \in K^p$ is equivalent to $\gamma_3/\gamma_2 \in K^p$ (since $\gamma_3/\gamma_2 = -1-\gamma_1/\gamma_2$)), which is equivalent to $\gamma_1/\gamma_3 \in K^p$ (since $\gamma_1/\gamma_3 = \gamma_1/\gamma_2 \cdot \gamma_2/\gamma_3$). In the future, we will only list one of these conditions, but freely apply the other (equivalent) ones.

**Proposition 3.9.** *If $X, Y, Z \in \mathscr{O}_{K,S}$ are pairwise coprime $S$-integers with $\nu(Z)=0$ for all $\nu \in S$, $Z \notin \mathbf{F}$ and $X^3/Z^N \notin K^p$, that satisfy an equation of the form*

$$X^3+Y^2=Z^N$$

*for $N \geq 1$, then $N \leq C'$ for some constant $C'$ that depends on $K$ and $S$ only.*

**Proof.** Mason's Theorem 3.6 applied to

$$\{\gamma_1,\gamma_2,\gamma_3\} = \{X^3/Z^N, Y^2/Z^N, -1\}$$

in all combinations, with

$$T = S \cup \{\nu\colon \nu(X)>0 \text{ or } \nu(Y)>0 \text{ or } \nu(Z)>0\}$$

implies: if $X^3/Y^2 \notin K^p$, then

$$\max\{h(X^3/Z^N), h(Y^2/Z^N), h(X^3/Y^2)\} \leq 2g_K - 2 + |S| + h(XYZ), \tag{7}$$

Using Lemma 3.5 and the fact that we are assuming $\nu(Z)=0$ for all $\nu \in S$, we find

$$\begin{aligned} h(X^3/Z^N) &= - \sum_{\substack{\nu \in S \\ \nu(X^3/Z^N)<0}} \nu(X^3/Z^N) + N \sum_{\substack{\nu \notin S \\ \nu(Z)>0}} \nu(Z) \\ &= - \sum_{\substack{\nu \in S \\ \nu(X^3)<0}} \nu(X^3) + Nh(Z) \end{aligned}$$

and also

$$\begin{aligned} h(X^3/Z^N) &= h(Z^N/X^3) \\ &= - \sum_{\substack{\nu \in S \\ \nu(Z^N/X^3)<0}} \nu(Z^N/X^3) + 3 \sum_{\substack{\nu \notin S \\ \nu(X)>0}} \nu(X) \\ &= 3 \sum_{\substack{\nu \in S \\ \nu(X)>0}} \nu(X) + 3 \sum_{\substack{\nu \notin S \\ \nu(X)>0}} \nu(X) \\ &= 3h(X). \end{aligned}$$

Thus,

$$h(X^3/Z^N) = 3h(X) \geq Nh(Z).$$

Similarly, we find

$$h(Y^2/Z^N) = 2h(Y) \geq Nh(Z).$$

We also have

$$h(X^3/Y^2) \geq \max\{2h(Y), 3h(X)\}.$$

Combining this with the estimate (7) from Mason's Theorem yields

$$\max\{3h(X), 2h(Y), Nh(Z)\} \leq 2g_K - 2 + |S| + h(X) + h(Y) + h(Z). \tag{8}$$

Let

$$\Sigma = \Sigma_{X,Y,Z} = h(X) + h(Y) + h(Z)$$

and

$$C = C_{K,S} = 2g_K - 2 + |S|.$$

From (8), we find inequalities

$$h(X) \leq \frac{1}{3}(\Sigma + C) \text{ and } h(Y) \leq \frac{1}{2}(\Sigma + C) \text{ and } h(Z) \leq \frac{1}{N}(\Sigma + C),$$

which add up to

$$\Sigma \leq \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{N}\right)(\Sigma + C),$$

or

$$\frac{1}{N} \geq \frac{1}{1 + \frac{C}{\Sigma}} - \frac{5}{6}. \tag{9}$$

Now there are two possibilities:

*Case* 1. $\Sigma > 11C$. From (9) it follows that $N < 12$.

*Case* 2. $\Sigma \leq 11C$. Since $h(X), h(Y), h(Z) \in \mathbf{Z}$ are positive and bounded above by the constant $11C$ that depends only on $K$ and $S$, there must be finitely many choices for $X$, $Y$ and $Z$. Since $Z \notin \mathbf{F}$, $h(Z) > 0$. Hence we find a bound on $N$, since

$$N \leq Nh(Z) = h(Z^N) \leq \max\{h(X^3 + Y^2) \colon h(X) + h(Y) \leq 11C\}. \qquad \square$$

**Corollary 3.10.** *Assume $j_E \notin K^p$. There exists a constant $\widetilde{C}$ only depending on $E, K$ and $S$ such that*

$$\mathscr{P}(E, K, S, x) \subseteq \bigcup_{3 \leq n \leq \widetilde{C}} \mathscr{P}(E, K, S, x)_n.$$

**Proof.** The successive enlargement of the original field $K$ and the original set of valuations $S$ only depended on $E, K$ and $S$. We assume we have extended the field and set so that we are in the situation of Proposition 3.1. Let $P \in \mathscr{P}(E, K, S, x)$, so $P \in \mathscr{P}(E, K, S, x)_n$ for some $n \geq 3$. Then in particular, $B_P$ is defined and in the notation of the two previous propositions, $Z^\ell = B_P v$ where $v$ is an $S$-unit and $\ell \in \{n, n/2\}$. Propositions 3.1 and 3.9 with $N = 4\ell$ imply that if $\ell > C'/4$ where $C'$ is the constant implied by Proposition 3.9, then either of the following two cases occurs:

(1) $Z \in \mathbf{F}$; then $B_P$ is an $S$-unit and hence

$$P \in \mathscr{Q}(E, K, S, x) \subseteq \mathscr{P}(E, K, S, x)_p.$$

(2) $X^3/Z^{4\ell} \in K^p$; since $X$ and $Z$ are coprime $S$-integers, $Z^{4\ell}$ is a $p$-th power up to an $S$-unit; hence $B_P^4$ is a $p$-th power up to an $S$-unit, and hence (with $p$ odd) $B_P$ is a $p$-th power up to an $S$-unit, so $P \in \mathscr{P}(E,K,S,x)_p$.

Hence

$$\mathscr{P}(E,K,S,x) \subseteq \bigcup_{3\leq n\leq C'/2} \mathscr{P}(E,K,S,x)_n \cup \mathscr{P}(E,K,S,x)_p,$$

so it suffices to take $\widetilde{C} = \max\{C'/2, p\}$. □

## 4. Bounding the solutions

By Corollary 3.10, to prove the main theorem we are now reduced to showing the following:

**Proposition 4.1.** *If $j_E \notin K^p$, then for fixed $n > 2$, the set $\mathscr{P}(E,K,S,x)_n$ is finite.*

**Proof.** The start of the proof is a function field version of the argument in [13], Theorem 5.2.1, which we then combine with the abc-hypothesis in function fields. This means we have to deal with the exceptional case where a term is a $p$-th power, but we show that this implies that $j_E \in K^p$.

Suppose that $P \in \mathscr{P}(E,K,S,x)_n$ for $n > 2$. Without loss of generality, we assume $E$ is in short Weierstrass form with coefficients from $\mathscr{O}_{K,S}$, and $K$ and $S$ have been extended so that $O_{K,S}$ is a PID, the 2-torsion of $E$ is $K$-rational, and $\Delta_E$ is an $S$-unit. Let $\alpha_1, \alpha_2, \alpha_3$ denote the $x$-coordinates of the points in $E[2]$. Extend $S$ further so that the differences $\alpha_i - \alpha_j$ are $S$-units for $i \neq j$. The necessary field extension is separable, since $p \geq 5$.

Let $P = (A_P/B_P^2, C_P/B_P^3) \in E(K)$ where $A_P C_P$ and $B_P$ are coprime $S$-integers. Plugging the coordinates of $P$ into the Weierstrass equation gives

$$C_P^2 = \prod_{i=1}^{3} (A_P - \alpha_i B_P^2).$$

The factors $A_P - \alpha_i B_P^2$ are coprime $S$-integers. Indeed, if $\nu \notin S$ has

$$\nu(A_P - \alpha_i B_P^2) > 0 \quad \text{and} \quad \nu(A_P - \alpha_j B_P^2) > 0,$$

then $\nu((\alpha_i - \alpha_j)B_P^2) > 0$, so $\nu(B_P) > 0$, and hence from $\nu(A_P - \alpha_i B_P^2) > 0$ it follows that also $\nu(A_P) > 0$, a contradiction. Hence

$$A_P - \alpha_i B_P^2 = z_i^2 \tag{10}$$

for some $z_i \in K$, up to $S$-units. By extending $K$ such that all $S$-units from $K$ become squares (which can be done by a finite extension by the function field analogue of Dirichlet's unit theorem) while keeping all previous conditions satisfied, we absorb the $S$-unit into $z_i$. Since the necessary field extension

is of degree a power of 2, it is separable for $p \geq 5$. Taking the difference of any two of the equations (10) yields

$$(\alpha_j - \alpha_i)B_P^2 = (z_i + z_j)(z_i - z_j). \tag{11}$$

Now $z_i + z_j$ and $z_i - z_j$ are coprime, since if $\nu(z_i + z_j) > 0$ and $\nu(z_i - z_j) > 0$ for $\nu \notin S$, then $\nu(z_i) > 0$. But also $\nu(B_P) > 0$ from (11), and hence $\nu(A_P) > 0$ from (10), a contradiction since $A_P$ and $B_P$ are coprime.

Write $B_P = uB^\ell$ with an $S$-unit $u$ for some $B \in \mathscr{O}_{K,S}$ and $n \in \mathbf{Z}$ with $\ell > 1$ and $n = 2\ell$. Then $z_i + z_j$ and $z_i - z_j$ are $n$-th powers up to $S$-units. For convenient notational purposes, let $\Delta$ denote a fixed choice of a plus or minus symbol, and $\nabla$ the opposite sign. We will use without further mentioning that $-1 \in K^p$. We distinguish the following cases:

(1) *There exists a set of distinct indices $i, j, k$ for which $\frac{z_i \pm z_j}{z_i \Delta z_k} \notin K^p$ for both signs $\pm$.*

We have the following *Siegel's identities*:

$$\frac{z_i \pm z_j}{z_i - z_k} \mp \frac{z_j \pm z_k}{z_i - z_k} = 1 = \frac{z_i \pm z_j}{z_i + z_k} \mp \frac{z_j \mp z_k}{z_i + z_k}. \tag{12}$$

In our situation, they become equations of the form

$$aX^{2\ell} + bY^{2\ell} = 1, \tag{13}$$

$a, b \in \mathscr{O}_{K,S}^*$ are $S$-units. Using the function field version of Dirichlet's unit theorem, there is a finite set $R$ of representatives for such units up to $2\ell$-th powers. So $\frac{z_i \pm z_j}{z_i \Delta z_k}$ takes on values inside

$$\mathscr{S} := \{a_0 X_0^{2\ell} \colon X_0 \in K, a_0 \in R \text{ and } \exists Y_0 \in K, b_0 \in R \colon a_0 X_0^{2\ell} + b_0 Y_0^{2\ell} = 1\}.$$

Mason's theorem implies that for $n > 2$ (i.e., $\ell > 1$), the solution set to any of the finitely many ternary equations that occur in the definition of $\mathscr{S}$ is finite, since $\frac{z_i \pm z_j}{z_i \Delta z_k} = aX_0^{2\ell} \notin K^p$ by assumption.

This implies that the set of values taken by

$$Z_\Delta = \frac{1}{\alpha_j - \alpha_i} \cdot \frac{z_i - z_j}{z_i \Delta z_k} \cdot \frac{z_i + z_j}{z_i \Delta z_k} \tag{14}$$

is finite. To finish the proof that $P$ takes on only finitely many values in this case, we state the following identity, which can be verified by direct computation, or follows from combining the last four indented formulas in the proof of 5.2.1 in [13]:

$$4x(P) = 2(\alpha_i + \alpha_k) + Z_\Delta^{-1} + (\alpha_i - \alpha_k)^2 Z_\Delta, \tag{15}$$

and observe that to every value of $x(P)$ correspond at most two values of $P$.

(2) *There exists a set of distinct indices $i, j, k$ for which $x_\pm := \frac{z_i \pm z_j}{z_i \Delta z_k} \in K^p$ for both signs $\pm$.*

We claim that if this statement holds for one set of indices (for fixed $\Delta$), it holds for all sets of indices (for the same fixed $\Delta$). It suffices to prove it for the permuted indices $(j, i, k)$ and $(k, j, i)$, since these

permutations generate $S_3$. The second permutation is implemented by replacing $x_\pm$ by $\pm(1-x_\pm)$, which are $p$-th powers if and only if $x_\pm$ are so. The first is given by replacing $x_\pm$ by $-x_\pm/(1-x_\pm)$. This proves the claim.

We then conclude from the equalities

$$\lambda := \frac{\alpha_1-\alpha_2}{\alpha_1-\alpha_3} = \frac{z_1-z_2}{z_1+z_3}\cdot\left(\frac{z_1-z_3}{z_1+z_2}\right)^{-1} = \left(\frac{z_1+z_3}{z_1-z_2}\right)^{-1}\cdot\frac{z_1+z_2}{z_1-z_3}$$

(the first if $\Delta = +$ and the second if $\Delta = -$) that $\lambda$ is a $p$-th power. But now we have

$$j_E = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2},$$

(cf. [18], III.1.7), and we conclude that $j_E \in K^p$, which we have assumed is not the case.

(3) *For all triples of pairwise distinct indices $(i,j,k)$, we have $\frac{z_i\mp z_j}{z_i\Delta z_k} \in K^p$ and $\frac{z_i\pm z_j}{z_i\Delta z_k} \notin K^p$, for some choice of signs $\mp$ and $\pm$ (depending on the indices).*

We use the identity

$$\frac{z_i \pm z_j}{z_i\Delta z_k} = \frac{1-\frac{z_i\mp z_j}{z_i\Delta z_k}}{1-\frac{z_i\nabla z_k}{z_i\pm z_j}}$$

to see that $\frac{z_i\nabla z_k}{z_i\pm z_j} \notin K^p$. But together with the assumption that $\frac{z_i\pm z_j}{z_i\Delta z_k} \notin K^p$ (so also its inverse), this implies that both $\frac{z_i\nabla z_k}{z_i\pm z_j}$ and $\frac{z_i\Delta z_k}{z_i\pm z_j}$ are not $p$-th powers, and the first case applies.

This covers all cases and finishes the proof of the theorem. □

**Remark 4.2.** Since one can in principle use the above method to bound the height of elements in $\mathscr{P}(E,K,S,f)_n$ for fixed $n$, and since the constant $\widetilde{C}$ in Corollary 3.10 is in principle computable, the set $\mathscr{P}(E,K,S,f)$ can be explicitly found.

**Remark 4.3.** It might seem that the above proof simultaneously bounds $\ell$ and the height of a solution, so that there is no need for proving Corollary 3.10 first. However, in general the maximal height of a set of representatives of $S$-units up to $2\ell$-th powers depends on $\ell$, making this reasoning impossible. In some special cases, e.g. when the field extension that is used has a *finite* unit group, one can restrict the "coefficients" $a$ and $b$ to a finite set independent of $\ell$, and then such a simultaneous bound *is* possible, see, e.g. Example 5.2 below.

## 5. Explicit bounds

We now show some examples of explicit bounds.

**5.1.** For this, we first list some crude estimates of heights in a rational function field $\mathbf{F}(u)$ (we write the variable as $u$ to avoid confusion when taking field extensions). (see, e.g., [3] 1.5.14-15, but do the nonarchimedean case):

$$\max\{h(xy), h(x+y)\} \le h(x) + h(y) \text{ if } x, y \in \mathbf{F}(u); \tag{16}$$

so that for any $\alpha, x \in \mathbf{F}(u)$, we have

$$h(x) = h(\alpha x \alpha^{-1}) \le h(\alpha x) + h(\alpha^{-1}) = h(\alpha x) + h(\alpha).$$

Hence

$$h(\alpha x) \ge h(x) - h(\alpha) \text{ for all } \alpha, x \in \mathbf{F}(u). \tag{17}$$

**Example/Proof 5.2.** In this example, we show how, in some cases, the proof of Proposition 4.1 can be changed so it implies a simultaneous bound on the exponent and the height of a perfect power, leading to a proof of Proposition 1.8 from the introduction.

Assume that $E$ is an elliptic curve over a rational function field $K = \mathbf{F}_q(t)$ with with $j_E \notin K^p$ and coefficients from $\mathbf{F}_q[t]$ such that all 2-torsion points on $E$ are $K$-rational, and assume that $P = 2Q \in 2E(K)$ with associated elliptic divisibility sequence $\{B_n\}$. Let $S = \{1/t\}$ denote the set consisting of the one place "$1/t$", corresponding to the valuation $\deg_t$, so $\mathscr{O}_{K,S} = \mathbf{F}_q[t]$. Suppose that $B_n = C^\ell$ for some $C \in \mathbf{F}_q[t]$. Since $P = 2Q$, in the proof of Proposition 4.1, the expressions $A_P - \alpha_i B_P = z_i^2$ are actual squares in $\mathbf{F}_q[t]$, so that $(z_i - z_j)/(z_i \Delta z_k) = aX^{2\ell}$ satisfies $aX^{2\ell} + bY^{2\ell} = 1$ for some $a, b \in \mathbf{F}_q(t)$ whose numerator and denominator divide some of the $\alpha_i - \alpha_j$. In particular, they divide $\Delta_E$, so

$$\max\{h(a), h(b)\} \le \deg \Delta_E.$$

If $x \in K$, let $n_0(x)$ denote the number of valuations $\nu$ for which $\nu(x) \ne q0$. Counting the valuation $\deg_t$, we find an estimate

$$\max\{n_0(a), n_0(b)\} \le n_0(\Delta_E) \le \deg \Delta_E + 1. \tag{18}$$

The abc-hypothesis (Mason's theorem) implies a bound on the height of a possible solution $X$, as follows:

$$\max\{h(aX^{2\ell}), h(bY^{2\ell})\} \le -2 + \#\{\nu \colon \nu(aX^{2\ell}) \ne 0 \text{ or } \nu(bY^{2\ell}) \ne 0\} \tag{19}$$

$$\le -2 + n_0(a) + n_0(b) + h(X) + 2h(Y); \tag{20}$$

where we may write $h(X) + 2h(Y)$ instead of $2h(X) + 2h(Y)$ since the equation satisfied by $X$ and $Y$ implies that if $\nu(a) = \nu(b) = 0$ and $\nu(X) < 0$, then also $\nu(Y) < 0$. Using (17), we find

$$\max\{-h(a)+2\ell h(X), -h(b)+2\ell h(Y)\} \le -2+n_0(a)+n_0(b)+h(X)+2h(Y),$$

which implies, using Equation (18):

$$\begin{aligned}(21)\qquad (\ell-1)h(X) &\le (\ell-1)h(X)+(\ell-2)h(Y)\\ &\le -2+n_0(a)+n_0(b)+\frac{1}{2}(h(a)+h(b))\\ &\le \deg\Delta_E+2(n_0(\Delta_E)-1)\\ &\le 3\deg\Delta_E.\end{aligned}$$

Now we can assume that $h(X)\neq 0$. Indeed, since we assume that $B_n\notin\mathbf{F}$, there will be a prime $\pi$ dividing $z_i\pm z_j$ for at least one choice of sign. If $\pi\mid z_i+z_k$ (so that $\pi$ cancels out in $(z_i\pm z_j)/(z_i+z_k)$) then use the left hand side of the Siegel identities (12); and if $\pi\mid z_i-z_k$ then choose the right hand side instead. With these choices, we can assume $X\notin\mathbf{F}$.

Hence (21) implies in particular that

$$\ell\le\deg\Delta_E+2n_0(\Delta_E)-1\le 3\deg\Delta_E+1.$$

For symmetry reasons, the estimate (21) also holds with $X$ replaced by $Y$. From (19), we then find (with $\ell\ge 2$) that

$$\begin{aligned}h(aX^{2l}) &\le -2+2n_0(\Delta_E)+3h(X)\\ &\le 3\deg\Delta_E+8(n_0(\Delta_E)-1).\end{aligned}$$

With our previous estimates for height of sums and products, we deduce from this with (14) and (15) that

$$h(Z_\Delta)\le 7\deg\Delta_E+16(n_0(\Delta_E)-1)$$

and finally

$$h(x(nP))\le 17\deg\Delta_E+32(n_0(\Delta_E)-1)\le 49\deg\Delta_E.$$

An estimate for the difference between the height and the canonical height can be deduced from the local (nonarchimedean) counterparts (as in Section 4 of [17]), and gives

$$-\frac{1}{24}h(j_E)\le\hat{h}(R)-\frac{1}{2}h(x(R))\le 0,$$

for all point $R\in E(K)$. So we find

$$n^2=\frac{\hat{h}(nP)}{\hat{h}(P)}\le\frac{h(x(nP))}{2\hat{h}(P)}\le\frac{17\deg\Delta_E+32(n_0(\Delta_E)-1)}{2\hat{h}(P)},$$

from which we can deduce

$$(22)\qquad n\le\sqrt{\frac{49\deg\Delta_E}{2\hat{h}(P)}}\text{ and }n\le\sqrt{\frac{588\deg\Delta_E}{12h(P)-h(j_E)}}.$$

Translated to the corresponding elliptic divisibility sequence, this proves Proposition 1.8. □

**Example 5.3.** Consider the curve

$$E\colon y^2 = x^3 - t(t-2)x^2 + 2t^2(t+1)x \tag{23}$$

over $K = \mathbf{F}_5(t)$ of discriminant and $j$-invariant

$$\Delta_E = 4t^6(t+1)^2(t-1)^2 \text{ and } j_E = -(t^2-2)^3/(t^2-1)^2.$$

The group $E(K)$ is the direct product of the full 2-torsion and a free group of rank one generated by $P = (t, t^2)$, with associated elliptic divisibility sequence

$$1, 1, t^2-1, t^2+1, (t^3+t^2-2t-1)(t^3-t^2-2t+1), \ldots.$$

Now $P = 2Q$ over $K' = \mathbf{F}_5(T)$ with $T = t^2$ (actually, $x(Q) = T^2(T-2)$). In this concrete case one can improve the estimates even further as follows: we observe that the set of differences $\alpha_i - \alpha_j$ belongs to

$$\{2T^2, T^2(T^2+1), T^2(T^2-1)\},$$

so $\max\{n_0(a), n_0(b)\} \le 3$ and $\max\{h(a), h(b)\} \le 4$; going through the estimates using these values, we find

$$(\ell-1)h(X) \le 8; \quad h(aX^{2\ell}) \le 28; \quad h(Z_\Delta) \le 60; \quad h(x(nP)) \le 132,$$

from which we conclude (using $\hat{h}(P) = 1/2$) that $n \le 11$; and it is easy to compute in SAGE [19] that each $B_n$ for $3 \le n \le 11$ has a simple factor. We conclude that the only perfect power denominators occur for $n = 1$ and $n = 2$, which corresponds to $B_1 = B_2 = 1$.

## 6. Nonconstant $j$-invariants

Suppose that $E$ is an elliptic curve with nonconstant $j$-invariant $j \notin \mathbf{F}$. Then there exists an integer $s$ such that $j_E \in K^{p^s} - K^{p^{s+1}}$. Write $j = (j')^{p^s}$ for a uniquely determined $j' \in K$. There exists an elliptic curve $E'$ over $K$ with $j$-invariant $j_{E'} = j'$ such that $E$ is the image of $E'$ under the $p^s$-Frobenius map

$$\mathrm{Fr}_{p^s}\colon (x, y) \mapsto (x^{p^s}, y^{p^s})$$

(see, e.g., [22], Lemma I.2.1).

**Proposition 6.1.** *Let $K$ be a global function field over a finite field $\mathbf{F}$ of characteristic $p \ge 5$ and $S$ a finite set of places of $K$. Suppose that $E$ is an elliptic curve over $K$ with $j$-invariant $j_E \in K^{p^s} - K^{p^{s+1}}$ for some integer $s$. Let $f$ denote a function in $K(E)$ with a pole of order $-\mathrm{ord}_O(f) > 0$ at the zero point $O = O_E$ of $E$. Let $E'$ denote the curve as above, and define*

$$\mathscr{P}(E, K, S, f) := \bigcup_{n \nmid \mathrm{ord}_O(f)\cdot p^s} \mathscr{P}(E, K, S, f)_n$$

*Then*

$$\mathscr{P}(E, K, S, f) \cap \mathrm{Fr}_{p^s}(E'(K)) \tag{24}$$

*is finite.*

**Proof.** A point $P \in \mathscr{P}(E, K, S, f) \cap \mathrm{Fr}_{p^s}(E'(K))$ satisfies that for all $K$-valuations $v \notin S$, if $\nu(f(P)) < 0$ then $n \mid \nu(f(P))$ for some $n$ not dividing $\mathrm{ord}_{O_E} f \cdot p^s$. We have to show that $P$ belongs to a finite set. There exists a (unique) $Q \in E'(K)$ such that $\mathrm{Fr}_{p^s}(Q) = P$. The given function $f \in K(E) - K$ extends to a function

$$f' := f \circ \mathrm{Fr}_{p^s} \in K(E') - K,$$

and for any valuation $\nu \in M_K$, we have

$$\nu(f(P)) = \nu(f(\mathrm{Fr}_{p^s}(Q)) = \nu(f'(Q)).$$

Finally, we have that $\mathrm{ord}_{O_{E'}} f' = p^s \,\mathrm{ord}_{O_E} f$. Now $Q$ satisfies the same conditions as $P$, but for some $n$ not dividing $\mathrm{ord}_{O_E} f \cdot p^s = \mathrm{ord}_{O_{E'}} f'$, so $Q \in \mathscr{P}(E', K, S, f')$. Since we have already proven the proposition for $E'$ over $K$ ($j_{E'} \notin K^p$), this set is finite, so that $P$ also belongs to a finite set. □

One may wonder whether more generally, $\mathscr{P}(E, K, S, f)$ itself (as defined in the above proposition) is finite when $j \notin \mathbf{F}$ (cf. also Remark 1.7). Note that there is an embedding

$$E(K)/\,\mathrm{Fr}_{p^s}(E'(K)) \hookrightarrow \mathrm{Sel}(K, \mathrm{Fr}_{p^s}),$$

where the $p$-Selmer group $\mathrm{Sel}(K, \mathrm{Fr}_{p^s})$ is *finite* $p$-group, as shown by Ulmer [20] (Theorem 3.2 in loc. cit. if $s = 1$ and $E$ has a rational $p$-torsion point; if $s = 1$ in general by the argument at the start of Section 3 of that paper, and for general $s$ by iteration).

## References


[1] Ayad, Mohamed. Points $S$-entiers des courbes elliptiques. *Manuscripta Math.* **76** (1992), no. 3–4, 305–324. MR1185022 (93i:11064), Zbl 0773.14014, doi: 10.1007/BF02567763.

[2] Bennett, Michael A.; Dahmen, Sander R. Klein forms and the generalized superelliptic equation. *Ann. of Math.* (2) **177** (2013), no. 1, 171–239. MR2999040, Zbl 1321.11059.

[3] Bombieri, Enrico; Gubler, Walter. Heights in Diophantine geometry. New Mathematical Monographs, 4. *Cambridge University Press, Cambridge*, 2006. xvi+652 pp. ISBN: 978-0-521-84615-8; 0-521-84615-3. MR2216774 (2007a:11092), Zbl 1115.11034, doi: 10.2277/0511138091.

[4] Bugeaud, Yann; Mignotte, Maurice; Siksek, Samir. Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers. *Ann. of Math.* (2) **163** (2006), no. 3, 969–1018. MR2215137 (2007f:11031), Zbl 1113.11021, arXiv:math/0403046, doi: 10.4007/annals.2006.163.969.

[5] Eisenstein, Gotthold. Untersuchungen über die cubischen Formen mit zwei Variabeln. *J. Reine Angew. Math.* **27** (1844), 89–104. MR1578387, ERAM 027.0785cj, doi: 10.1515/crll.1844.27.89.

[6] Everest, Graham; Reynolds, Jonathan; Stevens, Shaun. On the denominators of rational points on elliptic curves. *Bull. Lond. Math. Soc.* **39** (2007), no. 5, 762–770. MR2365225 (2008g:11098), Zbl 1131.11034, doi: 10.1112/blms/bdm061.

[7] Hoffman, J. William; Morales, Jorge. Arithmetic of binary cubic forms. *Enseign. Math.* (2) **46** (2000), no. 1–2, 61–94. MR1769537 (2001h:11048), Zbl 0999.11021. doi: 10.5169/seals-64795.

[8] Ingram, Patrick; Mahé, Valéry; Silverman, Joseph H.; Stange, Katherine E. ; Streng, Marco. Algebraic divisibility sequences over function fields. *J. Aust. Math. Soc.* **92** (2012), no. 1, 99–126. MR2945679, Zbl 1251.11008, arXiv:1105.5633, doi: 10.1017/S1446788712000092.

[9] Lang, Serge. Integral points on curves. *Inst. Hautes Études Sci. Publ. Math.* **6** (1960), 27–43. MR0130219 (24 #A86), Zbl 0112.13402, doi: 10.1007/BF02698777.

[10] Mahler, Kurt. Über die rationalen Punkte auf Kurven vom Geschlecht Eins. *J. Reine Angew. Math.* **170** (1934), 168–178. MR1581407, Zbl 0008.20002, doi: 10.1515/crll.1934.170.168.

[11] Mason, Richard C. Diophantine equations over function fields. London Mathematical Society Lecture Note Series, 96. *Cambridge University Press, Cambridge*, 1984. x+125 pp. ISBN: 0-521-26983-0. MR0754559 (86b:11026), Zbl 0533.10012, doi: 10.1017/CBO9780511752490.

[12] Pethő, Attila. Perfect powers in second order linear recurrences. *J. Number Theory* **15** (1982), no. 1, 5–13. MR0666345 (84f:10024), Zbl 0488.10009, doi: 10.1016/0022-314X(82)90079-8.

[13] Reynolds, Jonathan. Extending Siegel's theorem for elliptic curves. Ph.D. thesis, University of East Anglia, 2008. `https://archive.uea.ac.uk/~h446483/main.pdf`.

[14] Rosen, Michael. Number theory in function fields. Graduate Texts in Mathematics, 210. *Springer-Verlag, New York*, 2002. xii+358 pp. ISBN: 0-387-95335-3. MR1876657 (2003d:11171), Zbl 1043.11079, doi: 10.1007/978-1-4757-6046-0.

[15] Shorey, Tarlok N.; Stewart, Cameron L. Pure powers in recurrence sequences and some related Diophantine equations. *J. Number Theory* **27** (1987), no. 3, 324–352. MR0915504 (89a:11024), Zbl 0624.10009, doi: 10.1016/0022-314X(87)90071-0.

[16] Siegel, Carl L. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuß. Akad. Wiss., Phys.-Math. Kl.* **1929** (1929), no. 1, 70pp. [Collected Works, pp. 209–266 (*Springer Verlag*, 1966)]. MR3330350, JFM 56.0180.05, doi: 10.1007/978-88-7642-520-2_2.

[17] Silverman, Joseph H. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.* **55** (1990), no. 192, 723–743. MR1035944 (91d:11063), Zbl 0729.14026, doi: 10.2307/2008444.

[18] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. *Springer, Dordrecht*, 2009. xx+513 pp. ISBN: 978-0-387-09493-9. MR2514094 (2010i:11005), Zbl 1194.11005, doi: 10.1007/978-0-387-09494-6.

[19] Stein, William A.; et al. Sage Mathematics Software (Version 5.10.8). The Sage Development Team, 2011. `http://www.sagemath.org`.

[20] Ulmer, Douglas L. $p$-descent in characteristic $p$. *Duke Math. J.* **62** (1991), no. 2, 237–265. MR1104524 (92i:11068), Zbl 0742.14028, doi: 10.1215/S0012-7094-91-06210-1.

[21] Ulmer, Douglas L. Elliptic curves with large rank over function fields. *Ann. of Math.* (2) **155** (2002), no. 1, 295–315. MR1888802 (2003b:11059), Zbl 1109.11314, arXiv:math/0109163, doi: 10.2307/3062158.

[22] Ulmer, Douglas L. Elliptic curves over function fields. *Arithmetic of L-functions*, 211–280, IAS/Park City Math. Ser., 18. *Amer. Math. Soc., Providence, RI*, 2011. pp. 211–280. MR2882692, Zbl 1323.11037. arXiv:1101.1939.

[23] Voloch, José F. Explicit $p$-descent for elliptic curves in characteristic $p$. *Compositio Math.* **74** (1990), no. 3, 247–258. MR1055695 (91f:11042), Zbl 0715.14027. `http://eudml.org/doc/90020`.

(Gunther Cornelissen) Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 TA Utrecht, Nederland
g.cornelissen@uu.nl

(Jonathan Reynolds) INTO University of East Anglia, Norwich Research Park, Norwich, Norfolk, NR4 7TJ, United Kingdom
jonathan.reynolds@uea.ac.uk

This paper is available via http://nyjm.albany.edu/j/2016/22-5.html.