MATHEMATICS OF COMPUTATION
Volume 88, Number 315, January 2019, Pages 453–465
http://dx.doi.org/10.1090/mcom/3342
Article electronically published on May 4, 2018

ELLIPTIC CURVES MAXIMAL OVER EXTENSIONS OF FINITE BASE FIELDS

A. S. I. ANEMA

ABSTRACT. Given an elliptic curve E over a finite field $\mathbb{F}_q$ we study the finite extensions $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ such that the number of $\mathbb{F}_{q^n}$-rational points on E attains the Hasse upper bound. We obtain an upper bound on the degree n for E ordinary using an estimate for linear forms in logarithms, which allows us to compute the pairs of isogeny classes of such curves and degree n for small q. Using a consequence of Schmidt's Subspace Theorem, we improve the upper bound to $n \leq 11$ for sufficiently large q. We also show that there are infinitely many isogeny classes of ordinary elliptic curves with $n = 3$.

1. Introduction

Let E be an elliptic curve over $\mathbb{F}_q$. Recall the well-known Hasse bound on the number of points on an elliptic curve

$$||E(\mathbb{F}_{q^n})| - q^n - 1| \leq \left\lfloor 2\sqrt{q}^n \right\rfloor;$$

see for example [9, Theorem V.1.1] or [10, Theorem 5.1.1]. If E attains the Hasse upper bound over some finite extension, that is,

$$|E(\mathbb{F}_{q^n})| = q^n + 1 + \left\lfloor 2\sqrt{q}^n \right\rfloor$$

for some n, then we say E is *maximal* over $\mathbb{F}_{q^n}$. We are interested in the following.

Question. Let E be an elliptic curve over $\mathbb{F}_q$. Is E maximal over some finite extension of $\mathbb{F}_q$?

This question is studied and partially answered by Doetjes in [3]. He shows that every elliptic curve over $\mathbb{F}_2$ is maximal over some extension, that elliptic curves over $\mathbb{F}_3$ in five isogeny classes are maximal over some extension, that elliptic curves over $\mathbb{F}_3$ in the remaining two isogeny classes are not maximal over extensions of low degree, and that elliptic curves over $\mathbb{F}_q$ with q a square are maximal over some extension in precisely three cases. A similar question is studied by Heuberger and Mazzoli in [6].

Our first result is summarized below.

Received by the editor September 5, 2017, and, in revised form, November 22, 2017.
2010 *Mathematics Subject Classification.* Primary 11G20; Secondary 11J86, 11J87, 11N36.
This research was performed by the author at the University of Groningen for his Ph.D. thesis and was financially supported by Discrete, Interactive and Algorithmic Mathematics, Algebra and Number Theory (DIAMANT), a mathematics cluster funded by the Netherlands Organisation for Scientific Research (NWO).

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{F}_q$ and $a_1 = q + 1 - |E(\mathbb{F}_q)|$.*

(1) *If E is supersingular, that is, $a_1 \in \{0, \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, \pm 2\sqrt{q}\}$, then E is maximal over infinitely many extensions of $\mathbb{F}_q$ except when $a_1 \in \{-\sqrt{q}, 2\sqrt{q}\}$. In these exceptional cases extensions over which E is maximal do not exist.*
(2) *If E is ordinary, that is, $\gcd(a_1, q) = 1$, then there are at most finitely many extensions of $\mathbb{F}_q$ over which E is maximal. Furthermore, if q is a square, then such extensions do not exist.*

We prove the first part of the theorem in Section 2. The second part we treat in Section 3. There we also give an explicit bound on the degree of the extension and list the pairs q, a_1 with $q < 1000$ corresponding to ordinary elliptic curves over $\mathbb{F}_q$ maximal over some finite extension. In Subsection 3.3 we show that the degree of the extension is at most 11 for sufficiently large q.

Our second result follows.

Theorem 1.2. *For infinitely many primes p there exists an elliptic curve E over $\mathbb{F}_p$ such that E is maximal over $\mathbb{F}_{p^3}$.*

This confirms an observation made by Soomro in [10, Section 2.7] as well as our computations in Subsection 3.2. We prove the theorem in Section 4.

Notice that the property of E to be maximal over $\mathbb{F}_{q^n}$ depends only on the isogeny class of E, because isogenous elliptic curves over a finite field have the same number of points; see [2, Lemma 15.1]. The isogeny classes of elliptic curves over $\mathbb{F}_q$ correspond to integers a_1 such that $|a_1| \leq 2\sqrt{q}$ and some additional conditions; see [11, Theorem 4.1]. Define the integers a_n as

$$a_n = q^n + 1 - |E(\mathbb{F}_{q^n})|.$$

If α is an eigenvalue of Frobenius, that is, a root of the polynomial $X^2 - a_1 X + q$, then $a_n = \alpha^n + \bar{\alpha}^n$ with $\bar{\alpha}$ the conjugate of α; see [9, Section V.2]. So, the a_n's satisfy the recurrence relation

$$a_{n+1} = a_1 a_n - q a_{n-1}$$

for n a positive integer and $a_0 = 2$. Hence we reduced our question to:

Question. Let q be a prime power and a_1 an integer such that $|a_1| \leq 2\sqrt{q}$. Is there a positive integer n such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$?

In this article q, a_1 are integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$, α is a root of $X^2 - a_1 X + q$ and $\beta = \frac{\alpha}{\sqrt{q}}$. Fix an embedding $\mathbb{Q}(\sqrt{q}, \alpha) \to \mathbb{C}$ such that $\sqrt{q} > 0$ and α lies in the upper half-plane, that is, $\arg(\alpha) \in [0, \pi]$.

If β is a root of unity, then the pair q, a_1 is called *supersingular*, otherwise the pair is called *ordinary*. This definition agrees with the one for elliptic curves whenever the pair q, a_1 corresponds to an isogeny class of elliptic curves; see again [11, Theorem 4.1].

The answer to the question is divided into two cases, namely the supersingular case and the ordinary case.

2. Supersingular case

The first part of Theorem 1.1 follows directly from Proposition 2.1.

Proposition 2.1. *Let q, a_1 be integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$. If the pair q, a_1 is supersingular, then $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some positive integer n if and only if*

$$a_1 \in \left\{0, \sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, -2\sqrt{q}\right\}.$$

Moreover, if such an integer n exists, then there exist infinitely many.

The proposition above extends the result for $\mathbb{F}_q$ with q a square presented in [3, Chapter 5] to arbitrary $q \geq 2$. The new proof uses the following results.

Lemma 2.2. *If β is a root of the polynomial $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ with q, a_1 integers and q non-zero, then β is a root of unity if and only if*

$$a_1 \in \left\{0, \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, \pm 2\sqrt{q}\right\}.$$

Proof. Suppose that β is a primitive root of unity of order n. Let φ denote Euler's function, then $[\mathbb{Q}(\beta) : \mathbb{Q}] = \varphi(n)$. Since $\left[\mathbb{Q}\left(\sqrt{q}, \beta\right) : \mathbb{Q}\right] \in \{1, 2, 4\}$, the same is true for $[\mathbb{Q}(\beta) : \mathbb{Q}]$. The cyclotomic polynomials of degree dividing 4 are listed in Table 1. Evaluate $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ in a primitive root of unity ζ_n of order n for $n = 1, 2, 3, 4, 6$ to obtain $a_1 = 2\sqrt{q}, -2\sqrt{q}, -\sqrt{q}, 0, \sqrt{q}$, respectively. Notice that β is also a root of $X^4 + \left(2 - \frac{a_1^2}{q}\right)X^2 + 1$, and this polynomial and the cyclotomic polynomial both have degree 4 for $n = 5, 8, 10, 12$. This implies that $a_1 = \pm\sqrt{2q}, \pm\sqrt{3q}$ for $n = 8, 12$, respectively, and that the cases $n = 5, 10$ are impossible. Hence a_1 is as desired.

Assume that

$$a_1 \in \left\{0, \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, \pm 2\sqrt{q}\right\}.$$

If $a_1 = \pm 2\sqrt{q}$, then $X^2 - \frac{a_1}{\sqrt{q}}X + 1 = (X \mp 1)^2$, that is, β is a root of unity. Since β is a root of $X^2 - \frac{a_1}{\sqrt{q}}X + 1$, β is also a root of $X^4 + \left(2 - \frac{a_1^2}{q}\right)X^2 + 1$. If $a_1 \neq \pm 2\sqrt{q}$, then one of both polynomials is listed in Table 1, that is, β is a root of unity. Hence in either case β is a root of unity. $\square$

Lemma 2.3. *Let q, a_1 be integers with q positive and $|a_1| \leq 2\sqrt{q}$. If n is a positive integer, then*

$$-a_n = \lfloor 2\sqrt{q}^n \rfloor \quad \Longleftrightarrow \quad |\beta^n + 1| < \frac{1}{\sqrt[4]{q}^n}.$$

Proof. Notice that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ is equivalent to $-a_n \leq 2\sqrt{q}^n < -a_n + 1$, which is the same as $0 \leq a_n + 2\sqrt{q}^n < 1$. Since $|a_n| \leq 2\sqrt{q}^n$ implies $0 \leq a_n + 2\sqrt{q}^n$, in fact $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ if and only if $\left|a_n + 2\sqrt{q}^n\right| < 1$.

Recall that $a_n = \alpha^n + \bar{\alpha}^n$ and $|\alpha| = \sqrt{q}$ and $\beta = \frac{\alpha}{|\alpha|}$. Observe that

$$a_n + 2\sqrt{q}^n = \alpha^n + \bar{\alpha}^n + 2\sqrt{q}^n = \bar{\alpha}^n\left(\beta^{2n} + 1 + 2\beta^n\right) = \bar{\alpha}^n(\beta^n + 1)^2.$$

Substitute this relation in the last inequality to complete the proof. $\square$

TABLE 1. The list of all cyclotomic polynomials Φ_n of degree d dividing 4. Recall that $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = d$.

d	n	Φ_n
1	1	$X - 1$
	2	$X + 1$
2	3	$X^2 + X + 1$
	4	$X^2 + 1$
	6	$X^2 - X + 1$
4	5	$X^4 + X^3 + X^2 + X + 1$
	8	$X^4 + 1$
	10	$X^4 - X^3 + X^2 - X + 1$
	12	$X^4 - X^2 + 1$

Proof of Proposition 2.1. Suppose that $|\beta^n + 1| < \frac{1}{\sqrt[4]{q^n}}$ for some positive integer n and $\beta^m + 1 \neq 0$ for all integers m. Recall that β is a root of $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ and by assumption β is also a root of unity. Thus the order of β is odd. According to Lemma 2.2 and its proof β has order 1 or 3. If the order is 1, then $|\beta^m + 1| = 2$ for all integers m. If the order is 3, then $|\beta^m + 1| \geq 1$ for all integers m. In either case this contradicts $|\beta^n + 1| < \frac{1}{\sqrt[4]{q^n}}$. Hence for n a positive integer

$$|\beta^n + 1| < \frac{1}{\sqrt[4]{q}^n} \quad \Longleftrightarrow \quad \beta^n + 1 = 0.$$

Lemma 2.2 implies that $\beta^n + 1 = 0$ for some positive integer n if and only if the order of β is even if and only if $a_1 \in \{0, \sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, -2\sqrt{q}\}$.

The proposition follows from Lemma 2.3. $\square$

3. Ordinary case

The first result restricting the possible values of q and n in this case follows.

Proposition 3.1. *Let q, a_1 be integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$. If the pair q, a_1 is ordinary and $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some positive integer n, then q is not a square and n is odd.*

Proof. Assume that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some positive integer n. Recall that $\beta = \frac{\alpha}{|\alpha|}$. If q is a square or n is even, then $\lfloor 2\sqrt{q}^n \rfloor = 2\sqrt{q}^n$, that is, $\beta^n + 1 = 0$ (see Lemma 2.3). However, by assumption β is not a root of unity. $\square$

3.1. **Upper bound on the degree.** Given an ordinary pair q, a_1 we derive an upper bound on the n's such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ using an estimate for linear forms in two logarithms from [7].

Proposition 3.2. *For every integer $q \geq 2$ let N_q be the unique zero of*

$$n \longmapsto \frac{n}{4}\log(q) - 8.87\left(10.98\pi + \frac{1}{2}\log(q)\right)(2\log(n) + 3.27)^2 - \log\left(\frac{\pi}{3}\right)$$

larger than 8007.

(1) *The sequence $\{N_q\}_{q\geq 2}$ decreases monotonically.*
(2) *If the pair of integers q, a_1 with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$ is ordinary and $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some n, then $n < N_q$.*

Table 2. The value of $\lfloor N_q \rfloor$ for various q.

q	$\lfloor N_q \rfloor$	q	$\lfloor N_q \rfloor$
2	1840001	10^3	142072
3	1093182	10^4	104910
10	475174	10^5	83424
10^2	220290	10^6	69510

We computed the value of N_q for several q and list them in Table 2. In the case $q = 3$ Doetjes mentioned [3, p. 25] that for $a_1 = -2$ and $a_1 = 1$ there are no $n < 10^6$ such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$, and he expected that such n do not exist at all. Since his argument extends to $n < 2998887$, our upper bound on n shows that his observation is correct.

We denote the principal value of the argument and the complex logarithm by arg and log, respectively.

Lemma 3.3. *Let q, a_1 be integers with q positive and $|a_1| \leq 2\sqrt{q}$. If n is a positive integer such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$, then*

$$|m\pi + n \arg(\beta)| = |\arg(-\beta^n)| < \frac{\pi}{3} \frac{1}{\sqrt[4]{q}^n}$$

for some odd integer m such that $|m| \leq n$.

Proof. Assume that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some positive integer n. Since $|\beta| = 1$ by construction and $|\beta^n + 1| < \frac{1}{\sqrt[4]{q}^n} < 1$ by Lemma 2.3, $|\arg(-\beta^n)| < \frac{\pi}{3}$. Use $|\sin(\phi)| \geq \frac{3}{\pi}|\phi|$ for $|\phi| \leq \frac{\pi}{6}$ and $\frac{1}{2}|z - 1| = \left|\sin\left(\frac{1}{2}\arg(z)\right)\right|$ for $|z| = 1$ to obtain

$$|\arg(-\beta^n)| < \frac{\pi}{3} \frac{1}{\sqrt[4]{q}^n}.$$

Notice that

$$\arg(-\beta^n) = \arg(-1) + n\arg(\beta) + 2\pi k = (2k+1)\pi + n\arg(\beta)$$

for some integer k. Define $m = 2k + 1$. Since $|\arg(\beta)| \leq \pi$ and $|\arg(-\beta^n)| < \frac{\pi}{3}$,

$$|m|\pi = |\arg(-\beta^n) - n\arg(\beta)| \leq |\arg(-\beta^n)| + n|\arg(\beta)| < \left(n + \frac{1}{3}\right)\pi,$$

that is, $|m| \leq n$ as m, n are integers. □

The *logarithmic height* of an algebraic number β is defined as

$$\frac{1}{n}\left(\log|b| + \sum_{i=1}^{n} \log\max\{1, |\beta_i|\}\right)$$

with $b\prod_{i=1}^{n}(X - \beta_i)$ the minimal polynomial of β over $\mathbb{Z}$.

Lemma 3.4. *Let β be an algebraic number of absolute value one. If n is a positive integer, m is a non-zero integer such that $|m| \leq n$ and β is not a root of unity, then* $\log|m\pi + n\arg(\beta)|$ *is at least*

$$-8.87(10.98\pi + dl)\max\left\{17, \frac{\sqrt{d}}{10}, d\log(n) - 0.88d + 5.03\right\}^2,$$

where l is an upper bound on the logarithmic height of β and $d = \frac{1}{2}[\mathbb{Q}(\beta) : \mathbb{Q}]$.

Proof. Since the logarithmic heights of β and $\bar{\beta}$ are equal and $\arg\left(\bar{\beta}\right) = -\arg(\beta)$, replace β by $\bar{\beta}$ and m by $-m$ as necessary to reduce to the case of negative m.

Let a and H be as in [7, Théorème 3]. Observe that

$$20 \leq a \leq 10.98\pi + dl$$

and using $20 \leq a$ and $|m| \leq n$ that

$$H \leq \max\left\{17, \frac{\sqrt{d}}{10}, d\log(n) - 0.88d + 5.03\right\}.$$

Since $|\beta| = 1$ and β is not a root of unity, apply [7, Théorème 3] to $|m|\pi i - n\log(\beta)$ and use $\log(\beta) = \arg(\beta)i$ to obtain the desired lower bound. □

Lemma 3.5. *Let q, a_1 be integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$. If the pair q, a_1 is ordinary and q is not a square, then the minimal polynomial of β over $\mathbb{Q}$ is*

$$X^4 + \left(2 - \frac{a_1^2}{q}\right)X^2 + 1.$$

Proof. Since β is a root of $X^2 - \frac{a_1}{\sqrt{q}}X + 1$, it is also a root of the polynomial above. Proposition 2.1 gives $a_1 \neq 0, \pm 2\sqrt{q}$, because β is not a root of unity. Thus $\sqrt{q} \in \mathbb{Q}(\beta)$ and $\mathbb{R}(\beta) = \mathbb{C}$. Hence $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$, that is, the degree 4 polynomial is irreducible. □

Proof of Proposition 3.2. Define the function $f : \mathbb{R}_{\geq 1} \times \mathbb{R}_{\geq 1} \to \mathbb{R}$ as

$$(q, n) \longmapsto \frac{n}{4}\log(q) - 8.87\left(10.98\pi + \frac{1}{2}\log(q)\right)(2\log(n) + 3.27)^2 - \log\left(\frac{\pi}{3}\right).$$

Observe that $f(1, n) < 0$ for all $n \geq 1$. The function $\mathbb{R}_{\geq 1} \to \mathbb{R}$

$$n \longmapsto q \cdot \frac{\partial f}{\partial q}(q, n) = \frac{n}{4} - \frac{8.87}{2}(2\log(n) + 3.27)^2$$

is independent of q, strictly convex, has a unique minimum $1243 < n_1 < 1244$ and has a unique zero $8007 < n_2 < 8008$ such that $n_2 > n_1$. Therefore $\frac{\partial f}{\partial q}(q, \lfloor n_2 \rfloor) < 0$ for all $q \geq 1$, and as a result $f(q, \lfloor n_2 \rfloor) < 0$ for all $q \geq 1$. On the other hand, $n \mapsto f(q, n)$ is also strictly convex, because (for $q, n \geq 1$)

$$\frac{\partial^2 f}{\partial n^2}(q, n) = 35.48\left(10.98\pi + \frac{1}{2}\log(q)\right)\frac{2\log(n) + 1.27}{n^2} > 0.$$

Moreover, if $q > 1$, then $f(q, n) > 0$ for sufficiently large n. Combined with $f(q, \lfloor n_2 \rfloor) < 0$ this shows that for all $q > 1$ there exists a unique $N_q > \lfloor n_2 \rfloor$ such that $f(q, N_q) = 0$.

Since $q \cdot \frac{\partial f}{\partial q}(q, n) = c_n > 0$ for all $n > \lfloor n_2 \rfloor$, $f(q', N_q) > f(q, N_q) = 0$ for all $q' > q$, which implies that $N_{q'} < N_q$ for all $q' > q$. Hence the first part of the proposition follows.

Assume that the pair q, a_1 is ordinary and $-a_n = \left\lfloor 2\sqrt{q}^n \right\rfloor$ for some integer n. Lemma 3.3 gives

$$|m\pi + n\arg(\beta)| < \frac{\pi}{3}\frac{1}{\sqrt[4]{q}^n}$$

for some odd integer m such that $|m| \leq n$. The integer q is not a square by Proposition 3.1 and the minimal polynomial of β over $\mathbb{Z}$ has degree 4 and divides

$$qX^4 + \left(2q - a_1^2\right)X^2 + q$$

by Lemma 3.5, so that $[\mathbb{Q}(\beta):\mathbb{Q}] = 4$. Since $|\beta| = 1$ and β is not a root of unity, β, $\bar{\beta}$, $-\beta$ and $-\bar{\beta}$ are the distinct roots of this polynomial so that the logarithmic height of β is at most $\frac{1}{4}\log(q)$. Lemma 3.4 says

$$\log|m\pi + n\arg(\beta)| \geq -8.87\left(10.98\pi + \frac{1}{2}\log(q)\right)\max\{17, 2\log(n) + 3.27\}^2.$$

Let n_0 be such that $17 = 2\log(n_0) + 3.27$, that is, $n_0 = e^{6.865} \approx 958.1$. If $n \geq N_q$, then $n > \lfloor n_2 \rfloor > n_0$ and so $f(q,n) < 0$ by the upper and lower bounds on $|m\pi + n\arg(\beta)|$, which contradicts $f(q,n) \geq 0$ for all $n \geq N_q$. This proves the second part of the proposition. □

3.2. **Computing maximal triples.** Given an ordinary pair q, a_1 the upper bound in Proposition 3.2 reduces the problem of determining the $n > 1$ such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ to a finite computation. An efficient method to compute such n is described in [3, Section 6.1]: n is essentially the denominator of a convergent of $\frac{\arg(\beta)}{\pi}$. We extend [3, Stelling 6.8] in order to take into account numerical errors.

Proposition 3.6. *Let q, a_1 be integers with $q \geq 2$ and $a_1 = 2\sqrt{q}\cos(\theta)$ for some $\theta \in [0,\pi]$ and $x \in \mathbb{R}$ such that for some positive integer N,*

$$\left|x - \frac{\theta}{\pi}\right| \leq \frac{1}{2N^2} \cdot \begin{cases} 1 - \frac{2}{3}\frac{13}{\sqrt[4]{2}^{13}} & \text{if } q = 2, \\ 1 - \frac{2}{3}\frac{3}{\sqrt[4]{q}^{3}} & \text{if } q \geq 3. \end{cases}$$

If $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some odd integer $3 \leq n \leq N$ and either $q \geq 3$ or $n \geq 13$, then $\frac{m}{n}$ is a convergent of x for some odd m.

Propositions 3.1 and 3.6 together with $x = \frac{\theta}{\pi}$ imply [3, Stelling 6.8].

Proof. Assume that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some n. Since $\arg(\beta) = \theta$ by the choice of β, Lemma 3.3 implies that

$$\left|\frac{m}{n} - \frac{\theta}{\pi}\right| < \frac{1}{3}\frac{1}{n\sqrt[4]{q}^n}$$

for some odd integer m such that $|m| \leq n$. If $x \in \mathbb{R}$ such that

$$\left|x - \frac{\theta}{\pi}\right| \leq \frac{1}{2n^2} - \frac{1}{3}\frac{1}{n\sqrt[4]{q}^n},$$

then $\left|x - \frac{m}{n}\right| < \frac{1}{2n^2}$ so that $\frac{m}{n}$ is a convergent of x by [4, Theorem 184].

Define the function $f : \mathbb{R} \to \mathbb{R}$ as

$$f(n) = 1 - \frac{2}{3}\frac{n}{\sqrt[4]{q}^n}.$$

It has a global minimum at $n_0 = \frac{4}{\log(q)}$. Observe that $f(n_0)$ is positive except for $q = 2$. Consider the following cases:

- If $q = 2$, then $n = 13$ is the first integer for which $f(n)$ is positive.
- If $q = 3$, then $3 < n_0 < 4$ and $f(3) < f(5)$.
- If $q \geq 4$, then $n_0 < 3$.

Since $3 \leq n \leq N$ is odd and either $q \geq 3$ or $n \geq 13$,

$$\frac{f(n)}{2n^2} \geq \frac{f(n)}{2N^2} \geq \frac{1}{2N^2}\begin{cases} f(13) & \text{if } q = 2, \\ f(3) & \text{if } q \geq 3. \end{cases} \geq \left|x - \frac{\theta}{\pi}\right|.$$

Hence $\frac{m}{n}$ is a convergent of x. □

Beware of applying the above proposition. If $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some n, then $\frac{m}{n}$ is equal to a convergent of $\frac{\theta}{\pi}$ according to the proposition, but m and n need not be relatively prime. However, let $d = \gcd(m, n)$ and $\tilde{n} = \frac{n}{d}$. In this case

$$\frac{1}{d} \arg(-\beta^n) = \frac{m}{d}\pi + \frac{n}{d} \arg(\beta) = \left(\frac{m}{d} - \tilde{m}\right)\pi + \arg\left(-\beta^{\tilde{n}}\right)$$

using that $\arg\left(-\beta^{\tilde{n}}\right) = \tilde{m}\pi + \tilde{n}\arg(\beta)$ for some odd integer $\tilde{m}$. Moreover, $\frac{m}{d} = \tilde{m}$, because $\arg(-\beta^n), \arg\left(-\beta^{\tilde{n}}\right) \in (-\pi, \pi]$ and $m, \tilde{m}$ are odd. Thus

$$\frac{1}{2}\left|\beta^{\tilde{n}} + 1\right| = \left|\sin\left(\frac{1}{2}\arg\left(-\beta^{\tilde{n}}\right)\right)\right| \leq \left|\sin\left(\frac{1}{2}\arg(-\beta^n)\right)\right| = \frac{1}{2}|\beta^n + 1|,$$

so that $-a_{\tilde{n}} = \left\lfloor 2\sqrt{q}^{\tilde{n}} \right\rfloor$ by Lemma 2.3 for n and $\tilde{n}$.

Algorithm 1. The procedure MaximalCurves takes as input integers q, a_1 with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$ such that the pair is ordinary and outputs the n's with $n > 1$ such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$. The function MaximalDegree(q) returns the upper bound on n from Proposition 3.2, the function Convergents(x, N) computes the convergents of x with denominator at most N and the function IsSolution(q, a_1, n) checks $-a_n = \lfloor 2\sqrt{q}^n \rfloor$.

```
procedure MaximalCurves(q, a_1)
    if q not square then
        θ ← ArcCos(a_1 / (2√q))
        N ← MaximalDegree(q)
        C ← Convergents(θ/π, N)
        if q = 2 then
            for all n ∈ {3, 5, 7, 9, 11} do
                if IsSolution(q, a_1, n) then
                    print n
                end if
            end for
        end if
        for all m/n ∈ C : m odd, n odd do
            ConvergentsToSolutions(q, a_1, N, n)
        end for
    end if
end procedure

procedure ConvergentsToSolutions(q, a_1, N, n)
    if IsSolution(q, a_1, n) then
        if n > 1 then
            print n
        end if
        for all p ∈ {3, ..., ⌊N/n⌋} : p prime do
            ConvergentsToSolutions(q, a_1, N, pn)
        end for
    end if
end procedure
```

TABLE 3. The list of all pairs q, a_1 with $q < 10^3$ a prime power, $|a_1| \leq 2\sqrt{q}$ and $\gcd(q, a_1) = 1$ such that $-a_3 = \lfloor 2\sqrt{q}^3 \rfloor$.

q	a_1	q	a_1	q	a_1	q	a_1	q	a_1	q	a_1
2	1	37	6	103	10	229	15	479	22	787	28
3	2	47	7	167	13	257	16	487	22	839	29
5	2	61	8	173	13	293	17	571	24	967	31
8	3	67	8	193	14	359	19	577	24		
11	3	79	9	197	14	397	20	673	26		
17	4	83	9	199	14	401	20	677	26		
23	5	97	10	223	15	439	21	727	27		
27	5	101	10	227	15	443	21	733	27		

TABLE 4. The list of all pairs q, a_1 with $q < 10^6$ a prime power, $|a_1| \leq 2\sqrt{q}$ and $\gcd(q, a_1) = 1$ such that $-a_5 = \lfloor 2\sqrt{q}^5 \rfloor$.

q	a_1	q	a_1	q	a_1
2	-1	128	-7	10399	165
3	-1	317	-11	22159	-92
11	-2	2851	-33	122147	-216
23	-3	8807	-58	192271	-271
31	9	10391	-63	842321	1485

We implemented Algorithm 1 in PARI/GP [8] for pairs q, a_1 corresponding to isogeny classes of ordinary elliptic curves, that is, q is a prime power, $|a_1| \leq 2\sqrt{q}$ and $\gcd(q, a_1) = 1$. The upper bounds on the degree n in Table 2 combined with Proposition 3.6 show that approximating $\frac{\theta}{\pi}$ up to an error of at most 10^{-15} is sufficient to compute the relevant convergents of $\frac{\theta}{\pi}$. The execution time of the function IsSOLUTION is reduced by verifying the necessary condition in Lemma 3.3 before computing a_n.

Using our program we computed the triples (q, a_1, n) with $q < 10^6$ a prime power, $|a_1| \leq 2\sqrt{q}$, $\gcd(q, a_1) = 1$ and $n > 1$ such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$. All triples have $n = 3$ or $n = 5$, except for $(2, 1, 13)$ and $(5, 1, 7)$. The triples with $n = 3$ and $q < 10^3$ are listed in Table 3 and the triples with $n = 5$ and $q < 10^6$ are listed in Table 4. Based on these results we expect that the cases $n = 3$ and $n = 5$ occur infinitely often, whereas the cases $n \geq 7$ happen at most finitely many times.

3.3. **Upper bound on the cardinality.** In this subsection we determine an upper bound on q and conclude the following.

Theorem 3.7. *There exist only finitely many ordinary pairs q, a_1 such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some $n \geq 13$.*

Since Proposition 3.2 also gives an upper bound on the degree n independent of q, the theorem is an immediate consequence of the next proposition.

Proposition 3.8. *Let $n \geq 13$ be an integer. There exists a constant q_n such that if $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some integers q, a_1 with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$, then $q \leq q_n$ or the pair q, a_1 is supersingular.*

The *height* of an algebraic number β is defined as the maximum of the absolute value of the coefficients of the minimal polynomial of β over $\mathbb{Z}$.

Proof. Assume that q, a_1 are integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$ such that $-a_n = \lfloor 2\sqrt{q^n} \rfloor$ for some n, then $|\beta^n + 1| < \frac{1}{\sqrt[4]{q^n}}$ by Lemma 2.3. Moreover, assume that the pair q, a_1 is ordinary, that is, β is not a root of unity.

Observe that $\beta^n + 1 = \prod_{i=1}^n \left(\beta - \zeta_{2n}^{2i+1}\right)$. Let i_0 be an integer such that

$$\left|\beta - \zeta_{2n}^{2i_0+1}\right| = \min_i \left|\beta - \zeta_{2n}^{2i+1}\right|,$$

which determines i_0 uniquely modulo n because β is not a root of unity. Since

$$\left|\beta - \zeta_{2n}^{2i+1}\right| \geq \min\left\{\left|\zeta_{2n}^{2i_0} - \zeta_{2n}^{2i+1}\right|, \left|\zeta_{2n}^{2i_0+2} - \zeta_{2n}^{2i+1}\right|\right\} > 0,$$

for all $i \not\equiv i_0 \bmod n$, there exists a positive constant c_n such that

$$|\beta^n + 1| \geq c_n|\beta - \zeta_{2n}^m| \geq c_n\left|\frac{a_1}{2\sqrt{q}} - \cos\left(\frac{m\pi}{n}\right)\right|$$

with $m = 2i_0 + 1$. Let $\varepsilon > 0$. According to [1, Theorem 2.7] there exists an ineffective constant c_0' depending on $\cos\left(\frac{m\pi}{n}\right)$ and ε such that

$$\left|\frac{a_1}{2\sqrt{q}} - \cos\left(\frac{m\pi}{n}\right)\right| \geq \frac{c_0'}{h^{3+\varepsilon}}$$

with h the height of $\frac{a_1}{2\sqrt{q}}$. Since there are n possible values of m, the above inequality is also true for some constant c_0 depending only on n and ε. The height of $\frac{a_1}{2\sqrt{q}}$ is at most $4q$. Therefore

$$|\beta^n + 1| \geq \frac{c_0 c_n}{(4q)^{3+\varepsilon}} = \frac{c}{q^{3+\varepsilon}}$$

for some positive constant c depending only on n and ε.

Choose $\varepsilon = \frac{1}{8}$ and $n \geq 13$. The upper and lower bounds on $|\beta^n + 1|$ imply $c < q^{3+\varepsilon-\frac{n}{4}}$. The right-hand side converges to zero for $q \to \infty$, but $c > 0$. Hence $q \leq q_n$ for some constant q_n independent of β. $\square$

In some sense this proposition is the best possible in terms of n, because for $n = 7, 9, 11$ and m relatively prime to n we deduce from [1, Theorem 2.8] that there exists a constant $\tilde{c}$ and infinitely many algebraic numbers γ of degree 1 or 2 such that $\left|\gamma - \cos\left(\frac{m\pi}{n}\right)\right| < \frac{\tilde{c}}{h_\gamma^{3-\varepsilon}}$, where h_γ is the height of γ. If $h_\gamma \sim q$, then this upper bound is eventually smaller than $\frac{1}{\sqrt[4]{q^n}}$.

4. Maximal over cubic extensions

In this section we prove Theorem 1.2. For the sake of completeness we also discuss some properties of the case $n = 3$. The discussion is closely related to [10, Section 2.7].

Given a supersingular pair q, a_1 such that $|a_1| \leq 2\sqrt{q}$ and $-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor$, then $a_1 = -2\sqrt{q}$ or $a_1 = \sqrt{q}$ by Proposition 2.1. In this case q must be a square. Since q is a prime in Theorem 1.2, we only consider ordinary pairs.

Recall the recurrence relation $a_{n+1} = a_1 a_n - q a_{n-1}$ with $a_0 = 2$ mentioned in the introduction. From this we deduce $a_3 = a_1^3 - 3qa_1$. Therefore

$$-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor \quad \Longleftrightarrow \quad 0 \leq a_1^3 - 3qa_1 + 2\sqrt{q}^3 < 1.$$

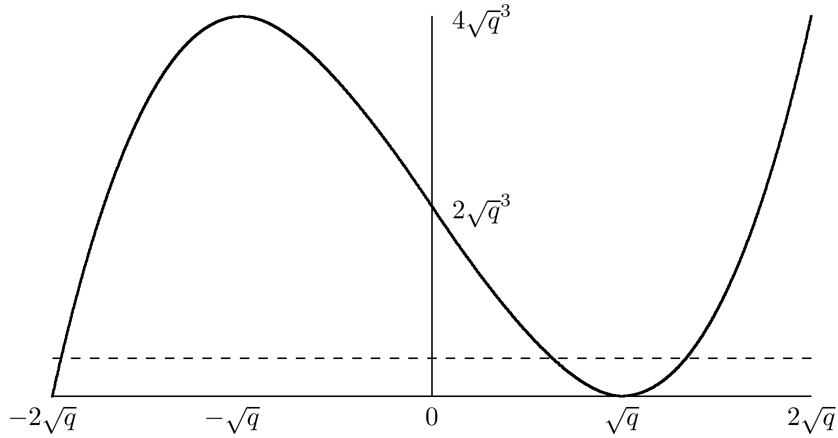

FIGURE 1. The graph of $f_q(a) = a^3 - 3qa + 2\sqrt{q}^3$.

Define the function $f_q : \left[-2\sqrt{q}, 2\sqrt{q}\right] \to \mathbb{R}$ as $x \mapsto x^3 - 3qx + 2\sqrt{q}^3$. The graph of f_q is shown in Figure 1.

Proposition 4.1. *Let q, a_1 be integers such that $q \geq 3$ and $|a_1| \leq 2\sqrt{q}$. If $-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor$, then $a_1 = -\left\lfloor 2\sqrt{q} \right\rfloor$ or $a_1 = \left[\sqrt{q}\right]$.*

Proof. Notice that f_q is maximal at $x = -\sqrt{q}, 2\sqrt{q}$ and that f_q is minimal at $x = -2\sqrt{q}, \sqrt{q}$ and

$$f_q(-2\sqrt{q} + 1) = (3\sqrt{q} - 1)^2 > 1$$

and

$$f_q\left(\sqrt{q} \pm \frac{1}{2}\right) = \frac{3}{4}\sqrt{q} \pm \frac{1}{8} > 1.$$

Hence $-2\sqrt{q} \leq a_1 < -2\sqrt{q} + 1$ or $\sqrt{q} - \frac{1}{2} < a_1 < \sqrt{q} + \frac{1}{2}$, that is, $a_1 = -\left\lfloor 2\sqrt{q} \right\rfloor$ or $a_1 = \left[\sqrt{q}\right]$. □

According to the following proposition the case $a_1 = -\left\lfloor 2\sqrt{q} \right\rfloor$ is possible only if the pair q, a_1 is supersingular.

Proposition 4.2. *Let q be an integer with $q \geq 2$ and $a_1 = -\left\lfloor 2\sqrt{q} \right\rfloor$. If $-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor$, then q is a square.*

Proof. Assume that q is not a square. Let $a = -a_1 = \left\lfloor 2\sqrt{q} \right\rfloor$.

The function f_q is strictly monotonically increasing and strictly concave on the interval $\left(-2\sqrt{q}, -\sqrt{q}\right)$, because $\frac{df_q}{dx} = 3x^2 - 3q$ and $\frac{d^2 f_q}{dx^2} = 6x$ are positive and negative, respectively. Let x_0 be the intersection between the line $y = 1$ and the line through $\left(-2\sqrt{q}, 0\right)$ and $\left(-2\sqrt{q} + 1, f_q\left(-2\sqrt{q} + 1\right)\right)$. Then

$$a_1 + 2\sqrt{q} < x_0 + 2\sqrt{q} = \frac{1}{\left(3\sqrt{q} - 1\right)^2}.$$

Notice that $4q = a^2 + b$ with $1 \le b \le 2a$. Since $\sqrt{1+x} \ge 1 + \left(\sqrt{2}-1\right)x$ for $0 \le x \le 1$,

$$a_1 + 2\sqrt{q} = a\left(-1 + \sqrt{1 + \frac{b}{a^2}}\right) \ge \left(\sqrt{2}-1\right)\frac{b}{a} \ge \frac{\sqrt{2}-1}{a} \ge \frac{\sqrt{2}-1}{\sqrt{q}}.$$

Combining the upper and lower bounds on $-a + 2\sqrt{q}$ yields

$$0 > \left(\sqrt{2}-1\right)\left(3\sqrt{q}-1\right)^2 - \sqrt{q},$$

but the right-hand side is positive by construction. Contradiction. $\square$

We recall a sufficient condition on q such that $-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor$ for $a_1 = \left[\sqrt{q}\right]$. It is [10, Proposition 2.7.1] with a different proof.

Proposition 4.3 (Soomro)**.** *If $q = a_1^2 + b$ with integers a_1, b such that $a_1 \ge 2$ and $|b| \le \sqrt{a_1}$, then $-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor$.*

Proof. Let $0 < \epsilon \le \frac{1}{3}$. Consider the function

$$g_\epsilon(x) = 1 + \frac{3}{2}x + \frac{3}{8}(1+\epsilon)x^2 - \sqrt{1+x}^3$$

and compute $\frac{dg_\epsilon}{dx} = \frac{3}{2} + \frac{3}{4}(1+\epsilon)x - \frac{3}{2}\sqrt{1+x}$ and $\frac{d^2 g_\epsilon}{dx^2} = \frac{3}{4}(1+\epsilon) - \frac{3}{4}\sqrt{1+x}^{-1}$. The function g_ϵ has extrema in $x = -\frac{4\epsilon}{(1+\epsilon)^2}$ and $x = 0$. The former is a maximum and the latter is a minimum. Let x_ϵ the unique zero of g_ϵ such that $-1 \le x_\epsilon < -\frac{4\epsilon}{(1+\epsilon)^2}$. Hence for all $x > x_\epsilon$ and $x \ne 0$,

$$\sqrt{1+x}^3 < 1 + \frac{3}{2}x + \frac{3}{8}(1+\epsilon)x^2.$$

Define $x = \frac{b}{a_1^2}$. Notice that

$$f_q(a_1) = -2{a_1}^3 - 3ba_1 + 2\sqrt{a_1^2 + b}^3 = 2a_1^3\left(-1 - \frac{3}{2}x + \sqrt{1+x}^3\right)$$

is minimal on (x_ϵ, ∞) for $x = 0$. If $x > x_\epsilon$ and $x \ne 0$, then

$$0 \le f_q(a_1) = 2a_1^3\left(-1 - \frac{3}{2}x + \sqrt{1+x}^3\right) < \frac{3}{4}(1+\epsilon)\frac{b^2}{a_1}.$$

Observe that if $b = 0$ (or $x = 0$), then $f_q(a_1) = 0$.

Assume that $\epsilon = \frac{1}{3}$ and $|b| \le \sqrt{a_1}$, then $x \ge -\sqrt{a_1}^{-3} > -1 = x_\epsilon$ and $0 \le f_q(a_1) < \frac{3}{4}(1+\epsilon) = 1$. Hence $-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor$. $\square$

A closer look at the proof tells us that in the proposition above the constraint $b^2 \le a_1$ can be replaced by $b^2 \le \frac{4}{3}\frac{1}{1+\epsilon}a_1$ at the expense of introducing a lower bound on a_1 in terms of ϵ.

Before proving Theorem 1.2, let us explain that it is a non-trivial statement. Let q, a_1 be a pair such that q is an odd prime and $|a_1| \le 2\sqrt{q}$. Then $a_1 = \left[\sqrt{q}\right]$ and the proposition above suggests that $q = a_1^2 + b$ with $b^2 \le ca_1$ for some positive constant c. However, the primes of this form have Dirichlet density zero; see [10, Remark 2.7.2]. Hence it is unlikely to find such primes.

The idea of the proof is to reduce the problem to a question on Gaussian primes in a small sector of the plane and apply [5, Theorem 1].

Proof of Theorem 1.2. Consider the set

$$S_1 = \left\{(a,b) \in \mathbb{Z}^2 : p = a^2 + b \text{ prime}, 0 < a, |b| \leq \sqrt{a}\right\}$$

and the subset $S_2 = \{(a,b) \in S_1 : b \text{ square}\}$. The set S_2 corresponds to

$$S_3 = \left\{(a,c) \in \mathbb{Z}^2 : p = a^2 + c^2 \text{ prime}, 0 < a, 0 \leq c \leq \sqrt[4]{a}\right\}.$$

Define for $\theta > 0$

$$S_4(\theta) = \left\{(a,c) \in \mathbb{Z}^2 : p = a^2 + c^2 \text{ prime}, 0 < a, 0 \leq c < p^{\theta}\right\}$$

and write $S_4(\theta) = S_5(\theta) \cup S_6(\theta)$ with $S_5(\theta) = \left\{(a,c) \in S_4(\theta) : a \geq p^{4\theta}\right\}$ and $S_6(\theta) = \left\{(a,c) \in S_4(\theta) : a < p^{4\theta}\right\}$. Observe that $S_5(\theta) \subset S_3$. If $\theta < \frac{1}{8}$, then the set $S_6(\theta)$ is finite, because $p = a^2 + c^2 < p^{8\theta} + p^{2\theta}$ and

$$\lim_{p \to \infty} \left(p^{8\theta - 1} + p^{2\theta - 1}\right) = 0.$$

The set $S_4(0.119)$ is infinite by [5, Theorem 1] and $0.119 < \frac{1}{8}$. Hence the sets $S_5(0.119) \subset S_3$ and $S_2 \subset S_1$ are also infinite. If $p = a_1^2 + b \in S_1$, then $|a_1| \leq 2\sqrt{q}$ and $-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor$ by Proposition 4.3. □

References

[1] Y. Bugeaud, *Approximation by Algebraic Numbers*, Cambridge Tracts in Mathematics, vol. 160, Cambridge University Press, Cambridge, 2004. MR2136100

[2] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291. MR0199150

[3] P. Doetjes, *Maximale elliptische krommen over eindige lichamen*, Bachelor's thesis, Rijksuniversiteit Groningen, 2009, `http://irs.ub.rug.nl/dbi/4a9d2d8a403dc`.

[4] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford University Press, 1975.

[5] G. Harman and P. Lewis, *Gaussian primes in narrow sectors*, Mathematika **48** (2001), no. 1-2, 119–135 (2003). MR1996365

[6] C. Heuberger and M. Mazzoli, *Elliptic curves with isomorphic groups of points over finite field extensions*, J. Number Theory **181** (2017), 89–98. MR3689671

[7] M. Laurent, M. Mignotte, and Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory **55** (1995), no. 2, 285–321. MR1366574

[8] The PARI Group, *PARI/GP version 2.9.3*, 2017, `http://pari.math.u-bordeaux.fr/`.

[9] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210

[10] M. A. Soomro, *Algebraic curves over finite fields*, Ph.D. thesis, Rijksuniversiteit Groningen, 2013, `http://irs.ub.rug.nl/ppn/35797039X`.

[11] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR0265369

Johann Bernoulli Institute for Mathematics and Computer Science, University of Groningen, P.O. Box 407, 9700 AK Groningen, The Netherlands

Email address: `a.s.i.anema@22gd7.nl`