PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 132, Number 4, Pages 955–963
S 0002-9939(03)07311-8
Article electronically published on November 7, 2003

PRIMES GENERATED BY ELLIPTIC CURVES

GRAHAM EVEREST, VICTOR MILLER, AND NELSON STEPHENS

(Communicated by David E. Rohrlich)

ABSTRACT. For a rational elliptic curve in Weierstrass form, Chudnovsky and Chudnovsky considered the likelihood that the denominators of the x-coordinates of the multiples of a rational point are squares of primes. Assuming the point is the image of a rational point under an isogeny, we use Siegel's Theorem to prove that only finitely many primes will arise. The same question is considered for elliptic curves in homogeneous form, prompting a visit to Ramanujan's famous taxi-cab equation. Finiteness is provable for these curves with no extra assumptions. Finally, consideration is given to the possibilities for prime generation in higher rank.

1. INTRODUCTION

Suppose E denotes an elliptic curve in Weierstrass form which is defined over $\mathbb{Q}$. The standard reference for elliptic curves is [10]. The curve E is given by an equation

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

with $a_1, \ldots, a_4, a_6 \in \mathbb{Z}$. Suppose E has a non-torsion point $P \in E(\mathbb{Q})$. Write

$$x(nP) = \frac{A_n}{B_n^2}, \tag{1.2}$$

in lowest terms, with A_n and B_n in $\mathbb{Z}$. In [3], Chudnovsky and Chudnovsky considered the likelihood that B_n might be a source of "large" primes. The following examples are taken from their paper; in both, the index n was allowed to run out to $n = 100$.

Example 1.1.

$$E: \quad y^2 = x^3 + 26, \quad P = [-1, 5].$$

The term B_{29} is a prime with 286 decimal digits.

$$E: \quad y^2 = x^3 + 15, \quad P = [1, 4].$$

The term B_{41} is a prime with 510 decimal digits.

In some respects, this method for producing primes mirrors the genus-zero situation with sequences such as the Mersenne and Fibonacci sequences. Genus-zero sequences are expected to produce large primes; for many years, the largest known

Received by the editors November 22, 2002.
2000 *Mathematics Subject Classification.* Primary 11G05, 11A41.
Thanks go to John Cremona, Joe Silverman and Felipe Voloch for helpful comments.

primes have come from the Mersenne sequence. However, in [5], further numerical work suggested that for fixed E and P, the sequence B_n should only contain finitely many primes. A heuristic argument suggested that the number of prime terms should be bounded. The elliptic Lehmer problem asks whether the global height of a non-torsion rational point is bounded below by a uniform constant. Under an affirmative answer, the methods in [5] predict a uniform upper bound for the number of prime terms B_n.

The sequence B_n is a divisibility sequence, meaning that $B_m|B_n$ whenever $m|n$. This follows from the p-adic analysis of elliptic curves as in [10]. Therefore, using Lemma (2.2) below, there can only be finitely many primes in the sequence B_n if P is a nontrivial multiple of another point or if P is a non-integral point or the index n is not itself prime. We call a point a *generator* if it is not a nontrivial multiple of another point. Any generator can be taken as one of the basis elements for $E(\mathbb{Q})$. However, note that a generator cannot necessarily be included in a basis for $E(\mathbb{Q})$ modulo torsion.

Let E and E' be two elliptic curves, defined over $\mathbb{Q}$. An *isogeny* is a nonzero homomorphism

$$\phi : E \to E'$$

taking the zero of E to the zero of E'. The isogeny has an integral degree $m \geq 1$ (see section 2). The curves E and E' are said to be *m-isogenous* if there is an isogeny of degree m between them. The key definition of this paper now follows:

Definition 1.2. Writing $\phi(P) = P'$, we say that the point $P' \in E'(\mathbb{Q})$ is *magnified*.

For the magnified point P' write $x(nP') = A'_n/B'^2_n$.

Theorem 1.3. *Given an isogeny $\phi : E \to E'$ of degree > 1 and a magnified point $P' \in E'(\mathbb{Q})$, the terms B'_n are prime for only finitely many n.*

Example 1.4. Here and elsewhere, we use the notation on Cremona's web site [2].

(1) The curve of conductor 136A1,

$$E: \quad y^2 = x^3 + x^2 - 4x,$$

is 2-isogenous to the curve in minimal Weierstrass form,

$$E': \quad y^2 = x^3 + x^2 + 16x + 16.$$

The generator $P = [-2, 2]$ on E maps to the generator $P' = [0, 4]$ on E'. Thus the sequence of denominators for P' on E' contains only a finite number of primes.

(2) The curve of conductor 324A1,

$$E: \quad y^2 = x^3 - 9x + 9,$$

is 3-isogenous to the curve in minimal Weierstrass form,

$$E': \quad y^2 = x^3 - 189x - 999.$$

The generator $P = [1, 1]$ on E maps to the generator $P' = [-8, 1]$ on E'. Thus the sequence of denominators for P' on E' contains only a finite number of primes.

The proof of Theorem 1.3 follows in the next section after some preliminaries on isogenies and heights. Comments are also given about what is needed to obtain effective and uniformity statements. A short section is then included with a more explicit proof; this is justified since it does actually yield a stronger statement. It

will be proved that only finitely many prime powers can occur among the denominators; see Theorem 3.1. After that, the question of prime (power) appearance is answered, without any hypotheses, for a curve in homogeneous form. Finally, these methods will be used to comment on the higher-rank situation and the possibility that two independent points can be used to produce infinitely many primes. This opening section concludes with some notes.

Notes

1. We felt it incumbent upon us to comment on the scarcity, or not, of generators for rank-1 curves which are magnified points. The following table, drawn from [2], provides statistics for all curves of conductor less than or equal to 200. It gives the number of isogeny classes of curves with a point of infinite order (all such curves within the tables have rank 1), together with the number of such classes having more than one curve in the class.

Range of conductor	Classes with rank 1	Classes with isogeny
11-50	2	0
51-100	15	4
101-150	25	11
151-200	33	18
Total	75	33

It is difficult to draw general conclusions from the table. It is not known whether the abundance of isogenies for small conductors is typical.

When the class contains more than one curve, there might be more than one curve that satisfies the criterion of the theorem. For example, there are three curves in the isogeny class 91B. The curve 91B2 is 3-isogenous to 91B1 and, under the isogeny, the image of the generator of 91B2 is a generator of 91B1. The curve 91B2 is also 3-isogenous to 91B3 and, under this isogeny, the image of the generator of 91B3 is a generator of 91B2. Thus both 91B1 and 91B2 have generators for which the sequence of denominators contains only a finite number of primes.

2. It was suggested in [5] that if S denotes any fixed, finite set of primes, then the S-free part of B_n can only be prime finitely often. The proof that follows demonstrates this stronger property.

3. Under the assumption that a generator has everywhere good reduction, the denominator sequence forms an *elliptic divisibility sequence* (EDS). For example, the generator P' in Example 1.4 (2) has everywhere good reduction. See Shipsey's thesis [9] or [14] for background on these sequences. The statement in Theorem 1.3 holds for EDSs also. This is because the sequence of denominators always divides the corresponding EDS.

2. Proof of Theorem 1.3

Firstly, recall some basic properties of isogenies. There is a dual homomorphism $\phi' : E' \to E$, and the composite homomorphisms $\phi'\phi$ and $\phi\phi'$ are multiplication by m on E and E', respectively, for some integer m, which is said to be the *degree* of the isogeny. If E and E' are m-isogenous and m is prime, then for precisely one of these curves a generator is mapped into a generator of the other. For the other curve, a generator is mapped to m times a generator. Thus the theorem proves that, within any isogeny class of curves containing more than one curve and having

a point of infinite order, there exists at least one generator on at least one of the curves for which the sequence of denominators contains only a finite number of primes.

Secondly, recall Siegel's Theorem and the behaviour of the height under isogeny. Let

$$h = \hat{h}(P) \quad \text{and} \quad h' = \hat{h}(P')$$

denote the canonical heights of P and P'. The first two statements in the Lemma are variants of Siegel's Theorem; see [10].

Lemma 2.1. *For any finite set of primes S, only finitely many terms B_n are S-units. A strong form of Siegel's Theorem gives*

$$\frac{\log |A_n|}{\log |B_n^2|} \to 1, \tag{2.1}$$

as $n \to \infty$. With the definitions above,

$$h' = mh. \tag{2.2}$$

Proof of Theorem 1.3. Suppose P denotes a generator on a curve E and there is an isogeny $\phi : E \to E'$ that takes P to a generator P'. Let S denote the set of primes for which E, E' and the isogeny cannot be reduced modulo p to give an isogeny on elliptic curves modulo p. Then S is a finite set. For all sufficiently large n, there is a prime divisor q of B_n not in S, by Siegel's Theorem. Reducing the curves and the isogeny modulo q we see at once that q divides B'_n. Using (2.1) and (2.2) we see that if n is large enough, q is a proper divisor. □

Notice that the proof also shows that the S-free part of the denominator can be prime only finitely often, where S denotes any fixed finite set of primes. The proof given is a fairly simple verification of Theorem 1.3. It seems worth investigating how it could be stengthened. Firstly, we consider making the result effective. Then we ask what might be required in order to prove the uniformity statement.

The effectiveness question can be settled using deep methods from elliptic transcendence theory. For any finite set of primes S, write $|k|_S$ for the S-free part of the integer k, with $|k|_S = k$ if S is the empty set.

Lemma 2.2. *There is a constant $K > 0$ such that*

$$\log |B_n^2|_S = 2hn^2 + O((\log n)^K). \tag{2.3}$$

The constants K and the one implied by the big O-notation are effective.

Proof. Recall the following effective result about the difference between the Weil height and the canonical height (see [10]):

$$\max\{\log(A_n), \log(B_n^2)\} = 2hn^2 + O(1). \tag{2.4}$$

When S is empty, elliptic transcendence theory (see [4]) gives (2.3) with $K = 1$. For each $p \in S$, p-adic elliptic transcendence theory (see [4] again) shows there is an effective constant $K_p > 0$ depending on E and p only, such that

$$\log |B_n^2|_p = O((\log n)^{K_p}).$$

Putting these together with (2.4) gives (2.3). □

Using Lemma 2.2 in the proof of Theorem 1.3 allows an effective version to be proved, although in practice, the constants might be too unwieldy to use.

In order to obtain a uniform bound, a stronger version of Lemma 2.2 is required. Let S consist of the primes for which E does not reduce to a nonsingular curve. Suppose (2.3) could be strengthened to

$$\log |B_n^2|_S = 2hn^2 + O(\log(\Delta_E)), \tag{2.5}$$

with a uniform error term, where Δ_E denotes the discriminant of E. Then Lang's Conjecture, which says that $\log(\Delta_E)/h$ is uniformly bounded, would enable the uniformity statement to be proved. In the function field case, Lang's Conjecture is proved. However, we are unaware of anything in the literature as good as (2.5) for the function field case (see [7], [12] and [13]).

Finally, note that Lang's Conjecture implies an affirmative answer to the elliptic Lehmer problem. Thus, our remarks above give a kind of post hoc credence to the heuristic argument in [5].

3. Explicit isogenies

Theorem 3.1. *Given an isogeny $\phi : E \to E'$ of degree > 1 and a magnified point $P' \in E'(\mathbb{Q})$, the terms B'_n are prime powers for only finitely many n.*

Proof. We give an explicit proof of Theorem 3.1 using Vélu's formulae in [11]. This proof exhibits a kind of generic factorizability of the denominators of the multiples of P'. Isogenies of composite degree are composed of isogenies of prime degree; it is only necessary to prove the theorem for these. The formulae that follow, for isogenies of prime degree, are taken from [11]. They make use of the coordinates of a point $S = (x_1, y_1)$ of order m on the curve and its multiples $kS = (x_k, y_k)$, for $1 < k < m$. The point S may or may not have coordinates in the base field $\mathbb{Q}$. However the formulae, when applied to a point P on a curve E over $\mathbb{Q}$, yield an isogenous curve E' and a $\mathbb{Q}$-rational point P' whenever the isogeny exists. It is necessary to consider the cases $m = 2$ and m odd separately.

For $m = 2$, the curve E must have a 2-torsion point $S = (x_1, y_1)$ over $\mathbb{Q}$. Let

$$t = 3x_1^2 + 2a_2x_1 + a_4 - a_1y_1,$$
$$u = 4x_1^3 + b_2x_1^2 + 2b_4x_1 + b_6,$$

and

$$w = u + x_1t.$$

Then the isogenous curve E' has

$$[a'_1, a'_2, a'_3, a'_4, a'_6] = [a_1, a_2, a_3, a_4 - 5t, a_6 - b_2t - 7w]. \tag{3.1}$$

Also $P' = (x', y')$, the image of $P = (x, y)$, has x' given by

$$x' = x + t/(x - x_1) + u/(x - x_1)^2. \tag{3.2}$$

It is possible that x_1 and y_1 are not in $\mathbb{Z}$ and, subsequently, the coefficients given for E' are also not in $\mathbb{Z}$. It is possible, even if the coefficients of E' are in $\mathbb{Z}$, that the curve E' is not in minimal Weierstrass form. If this happens, a transformation to take E' to E_0 which is minimal will take x to $v^2x_0 + r$ for some $v, r \in \mathbb{Z}$. The denominator of x_0 will thus be divisible by the denominator of x, and this will not affect the primality statement. We shall assume this transformation has been made

and retain the same notation. Note that the value for u in the formulae above is zero because the roots of the expression on the right are the x-coordinates of the two division points on the curve. The expressions above were given to unify the presentation.

Suppose P denotes a generator on a curve E with coordinates in $\mathbb{Z}$ and there is an isogeny $\phi : E \to E'$ that takes P to a generator P'. Write $Q = (X/Z^2, Y/Z^3)$ for an arbitrary multiple of P. The isogeny maps this point to $Q' = (X'/Z'^2, Y'/Z'^3)$, the same multiple of P'. Using (3.2), and inserting $u = 0$, gives

$$\frac{X'}{Z'^2} = \frac{X}{Z^2} + \frac{tZ^2}{X - x_1 Z^2}.$$

For all sufficiently large multiples of P, we have $Z' > Z > 1$ by (2.3) and (2.2). Clearly $(X, Z) = (Z, X - x_1 Z^2) = 1$. Hence Z' will be a product of Z and a factor of $X - x_1 Z^2$, coprime and both greater than 1. Hence the denominator cannot be a prime power for all sufficiently large multiples of P'.

For odd m, the formulae for t, u, w are given as follows. Define, for each k with $1 \le k \le (m-1)/2$,

$$t_k = 6x_k^2 + b_2 x_k + b_4,$$
$$u_k = 4x_k^3 + b_2 x_k^2 + 2b_4 x_k + b_6,$$

and

$$w_k = u_k + x_k t_k.$$

Then with

$$t = \sum t_k, \qquad u = \sum u_k, \qquad \text{and} \qquad w = \sum w_k,$$

the formula for E' is exactly as in (3.1). However, $x(P')$ is given by

$$x' = x + \sum_{k=1}^{(m-1)/2} \left\{ \frac{t_k}{(x - x_k)} + \frac{u_k}{(x - x_k)^2} \right\}. \tag{3.3}$$

Again, the coordinates of the isogenous curve and the image of the point will have values in $\mathbb{Q}$ but not necessarily in $\mathbb{Z}$. Consider first the case where the x_k and hence t, u, w are integers. Write $Q = (X/Z^2, Y/Z^3)$ for an arbitrary multiple of P. The isogeny maps this point to $Q' = (X'/Z'^2, Y'/Z'^3)$, the same multiple of P'. Using (3.3) gives

$$\frac{X'}{Z'^2} = \frac{X}{Z^2} + \sum_{k=1}^{(m-1)/2} \left\{ \frac{t_k Z^2}{X - x_k Z^2} + \frac{u_k Z^4}{(X - x_k Z^2)^2} \right\}.$$

Now $(X, Z) = (Z, X - x_k Z^2) = 1$, in $\mathbb{Q}(x_k)$. Just as before, for sufficiently large multiples of P, we have $Z' > Z > 1$. Hence, for almost all multiples of P, Z' will be a product of Z and a nontrivial factor of $\prod(X - x_k Z^2)$. This latter factor is coprime with Z and both are greater than 1. As before, the denominator cannot be a prime power for all sufficiently large multiples of P'.

Finally, consider the case when the x_k are not integers. The equation for the x-coordinate of the m division points is a polynomial of degree 3 ($m = 2$) and degree $(m^2 - 1)/2$ (m odd) with leading coefficient r, where $r \mid m^2$. If the x_k are not integers, then the values of rx_k are. It follows that in the latter case,

r^2t, r^3u, r^4w are in $\mathbb{Z}$. Hence $E_0 = [ra'_1, r^2a'_2, r^3a'_3, r^4a'_4, r^6a'_6]$ and $P_0 = (r^2x', r^3y')$ have coordinates in $\mathbb{Z}$. The proof is now similar to the first case. □

4. The curve $u^3 + v^3 = D$

This section shows that the primality question can be answered in full generality for elliptic curves in homogeneous form.

Theorem 4.1. *Suppose E denotes an elliptic curve defined by an equation*

$$u^3 + v^3 = D, \tag{4.1}$$

for some nonzero $D \in \mathbb{Q}$. Let P denote a non-torsion $\mathbb{Q}$-rational point. Write, in lowest terms,

$$P = \left(\frac{A_P}{B_P}, \frac{C_P}{B_P}\right).$$

The integers B_P are prime powers for only finitely many $\mathbb{Q}$-points P.

Example. As Ramanujan famously pointed out, the taxi-cab equation

$$x^3 + y^3 = 1729, \tag{4.2}$$

has two distinct integral solutions. These give rise to points $P = [1, 12]$ and $Q = [9, 10]$ on the elliptic curve (4.2). The only rational points on (4.2) which seem to yield prime power denominators are $2Q$ and $P + Q$ (and their inverses).

Proof of Theorem 4.1. It is well known that there is a birational transformation between the homogenous model (4.1) and the Weierstrass model

$$y^2 = x^3 - 2^4 3^3 D^2.$$

The transformations are given by

$$\begin{aligned} x &= \frac{2^2 3D}{u+v}, \qquad y = \frac{2^2 3^2 D(u-v)}{u+v}, \\ u &= \frac{2^2 3^2 D + y}{6x}, \qquad v = \frac{2^2 3^2 D - y}{6x}. \end{aligned}$$

Writing $x = X/Z^2$ and $y = Y/Z^3$ where $(X, Z) = (Y, Z) = 1$, it follows that

$$u = \frac{2^2 3^2 DZ^3 + Y}{6XZ}.$$

If X divides the numerator of u, then X divides $2^6 3^3 D^2$. By Siegel's Theorem, this can only happen finitely often. Since Z is co-prime to the numerator, (2.1) shows that, apart from a finite number of points, the denominator of u always has two nontrivial coprime factors. □

5. Higher-rank considerations

Joe Silverman asked the first author what other possibilities there might be if the elliptic curve has rank greater than 1. There exists a straightforward generalization possible of the finiteness result, but a real surprise also lies in store.

Theorem 5.1. *Let E denote an elliptic curve in Weierstrass form* (1.1)*. Suppose that P and Q denote independent points both magnified under the same isogeny. Write*

$$x(nP + mQ) = \frac{A_{nm}}{B_{nm}^2}. \tag{5.1}$$

Then there are only finitely many pairs (m, n) for which B_{nm} is prime.

Example. The elliptic curve

$$y^2 + xy = x^3 + x^2 - 156x + 2070$$

has independent generators $P = [3, 39]$ and $Q = [13, 43]$ which are magnified under the same 2-isogeny. This is because $T = [-69/4, 69]$ is a 2-torsion point for which $x(P) - x(T)$ and $x(Q) - x(T)$ are both rational squares. We can therefore appeal to Cassels' treatment of explicit 2-isogenies in [1] (see Lemma 1 on p. 60).

In [6] and [8], a heuristic argument together with results from some numerical experiments indicate that for certain curves in Weierstrass form (1.1), if P and Q denote independent non-torsion rational points, then the denominators of $nP+mQ$ can be the squares of primes infinitely often. Indeed, there seem to be asymptotically $c \log X$ such primes with $|m|, |n| < X$. Of course, none of the numerical examples that are considered in [6] and [8] use magnified points.

The proof of Theorem 5.1 involves little that goes beyond our earlier method; so no details are given.

References

1. J. W. S. Cassels, *Lectures on Elliptic Curves*, London Mathematical Society Student Texts 24, Cambridge University Press, Cambridge, 1991. MR **92k:**11058
2. J. E. Cremona, *Elliptic Curve Data*, up-dated 14-1-02, http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html
3. D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. in Appl. Math. 7 (1986), 385–434. MR **88h:**11094
4. David Sinnou, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France (N.S.) (1995), no. 62, iv+143. MR **98f:**11078
5. Manfred Einsiedler, Graham Everest and Thomas Ward, *Primes in elliptic divisibility sequences*, LMS J. Comput. Math. 4 (2001), 1–13. MR **2002e:**11181
6. Graham Everest, Peter Rogers and Thomas Ward, *A higher rank Mersenne problem*, ANTS V Proceedings, Springer Lecture Notes in Computer Science, 2369 (2002), 95-107.
7. Marc Hindry and Joseph H. Silverman, *Diophantine Geometry*, Graduate Texts in Mathematics, Volume 201, Springer-Verlag, New York, 2000. MR **2001e:**11058
8. Peter Rogers, *Topics in Elliptic Divisibility Sequences*, MPhil thesis, University of East Anglia, 2003.
9. Rachel Shipsey, *Elliptic divisibility sequences*, Ph.D. thesis, Univ. of London, 2000.
10. Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, No. 106, Springer-Verlag, New York, 1986. MR **87g:**11070
11. J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris 273 (1971), 238-241. MR **45:**3414
12. J. F. Voloch, *Siegel's theorem for complex function fields*, Proc. Amer. Math. Soc. 121 (1994), 1307-1308. MR **94j:**11052
13. J. F. Voloch, *Diophantine approximation on abelian varieties in characteristic p*, Amer. J. of Math. 117 (1995), 1089-1095. MR **96i:**11061

14. Morgan Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. 70 (1948), 31–74. MR **9:**332j

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom
E-mail address: g.everest@uea.ac.uk

Center for Communications Research, Princeton, New Jersey 08540
E-mail address: victor@idaccr.org

Department of Mathematical and Computer Sciences, Goldsmiths College, London SE14 6NW, United Kingdom
E-mail address: nelson@gold.ac.uk