Glasgow Math. J. **47** (2005) 115–122. © 2005 Glasgow Mathematical Journal Trust.
DOI: 10.1017/S0017089504002113. Printed in the United Kingdom

PRIME DIVISORS OF SEQUENCES ASSOCIATED TO ELLIPTIC CURVES

GRAHAM EVEREST
School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK
e-mail: g.everest@uea.ac.uk

and IGOR E. SHPARLINSKI
Department of Computing, Macquarie University, NSW 2109, Australia
e-mail: igor@comp.mq.edu.au

(Received 10 February, 2004; accepted 22 June, 2004)

Abstract. We consider the primes which divide the denominator of the x-coordinate of a sequence of rational points on an elliptic curve. It is expected that for every sufficiently large value of the index, each term should be divisible by a primitive prime divisor, one that has not appeared in any earlier term. Proofs of this are known in only a few cases. Weaker results in the general direction are given, using a strong form of Siegel's Theorem and some congruence arguments. Our main result is applied to the study of prime divisors of Somos sequences.

2000 *Mathematics Subject Classification.* 11A41, 11G05.

1. Introduction. Let $\mathbf{E}$ denote the elliptic curve in generalized Weierstrass form,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

defined over $\mathbb{Q}$, the rational numbers. We assume that the coefficients are chosen to lie in $\mathbb{Z}$ and equation (1) defines a minimal model. For background, definitions and all properties of elliptic curves used in this paper, consult [**19**], [**22**] and [**21**]. Let $\mathbb{K}$ denote an algebraic number field of degree $d = [\mathbb{K}:\mathbb{Q}]$ over $\mathbb{Q}$. Throughout the paper, $\mathbf{E}(\mathbb{K})$ denotes the group of $\mathbb{K}$-rational points of $\mathbf{E}$ and O denotes the point at infinity, the identity for the group of $\mathbb{K}$-rational points. Suppose P and Q denote $\mathbb{K}$-rational points, $P, Q \in \mathbf{E}(\mathbb{K})$, with P non-torsion. Assume that $nP + Q \neq O$ for all positive integers n and write $nP + Q = (x_n, y_n)$. The assumptions on $\mathbf{E}$ allow the factorization

$$(x_n) = (x(nP + Q)) = \alpha_n/\beta_n, \tag{2}$$

of the principal ideal $(x(nP + Q))$ into relatively prime integral ideals α_n and β_n.

In the rational case, we may take β_n to be a positive integer. Silverman [**20**] proved that when P is a rational point and $Q = O$ the point at infinity, for all sufficiently large n, β_n has a *primitive divisor*, that is, a divisor of β_n which is coprime to β_m for all positive integers $m < n$. In general, the expression *primitive ideal divisor* of a term β_n is used to describe an ideal $\mathcal{I}$ which divides β_n and is coprime to β_m with $m < n$. Cheon and Hahn [**2**] have extended Silverman's result in [**20**] to the algebraic case, showing that for all sufficiently large n, β_n has a primitive ideal divisor. The same conclusions are drawn in [**5**] under the assumption that Q is an arbitrary torsion point. Under the assumption

that $Q = O$ and P is the image of a $\mathbb{K}$-rational point under a non-trivial isogeny, it is shown in [**5**] that for all sufficiently large n, β_n has a composite primitive ideal divisor. Pheidas [**11**] has raised the exciting possibility that results of this kind could be related to Hilbert's Tenth Problem over the rationals, which has still not been settled.

Results about primitive divisors have a long and fine tradition for certain sequences which satisfy a linear recurrence relation, see [**6**]. Consider the sequence $u_n = a^n - b^n$, where $a > b$ are positive coprime integers. Zsigmondy's theorem [**28**] says that u_n always has a primitive divisor unless (i) $a = 2$, $b = 1$ and $n = 6$ or (ii) $a + b = 2^k$ and $n = 2$. In [**15**], Schinzel extended this result in a number of directions. He established a large class of indices for which u_n has a composite primitive divisor. As an example of his results, when u is the Mersenne sequence ($a = 2$ and $b = 1$), he proved u_{4k} has a composite primitive divisor for all odd $k > 5$. He also proved an algebraic version for primitive ideal divisors of sequences of the form $u_n = \alpha^n - \beta^n$, where α and β are algebraic numbers with α/β not a root of unity (see [**16**] and [**17**]). If the sequence is changed slightly to $u_n = \gamma\alpha^n - \beta^n$, then a Zsigmondy-type theorem is proved in [**16**] under the assumption that γ is a root of unity. The Zsigmondy theorem extends to all Lucas and Lehmer sequences and has recently been cast in a very strong uniform manner. Bilu, Hanrot and Voutier proved in [**1**] that for any $n > 30$, the n-th term of any Lucas or Lehmer sequence has a primitive divisor.

For an integral ideal $\mathcal{I}$ of $\mathbb{K}$, let $\omega_{\mathbb{K}}(\mathcal{I})$ denote the number of prime ideal divisors of $\mathcal{I}$. Assuming P is non-torsion guarantees that all of the terms in the sequence $\beta = (\beta_n)$ are non-zero. Obviously, for any sequence of integral ideals $v = (v_n)$ which satisfies a Zsigmondy-type theorem, the following lower bound holds:

$$\omega_{\mathbb{K}}\left(\prod_{n=M+1}^{M+N} v_n\right) \geq N, \tag{3}$$

for all sufficiently large M. In the absence of a full Zsigmondy theorem for elliptic sequences, we still prove a similar lower bound.

Recall that $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$. Throughout the paper, the implied constants may dependent on $\mathbf{E}$ and the points P and Q.

THEOREM 1.1. *Let P and Q denote algebraic points on an elliptic curve, with P non-torsion. With β_n defined by* (2)*, for all sufficiently large M,*

$$\omega_{\mathbb{K}}\left(\prod_{n=M+1}^{M+N} \beta_n\right) \gg N. \tag{4}$$

Very few results about the existence of primitive (rational) divisors are known for the Lehmer-Pierce sequence $\mathrm{Nm}(\alpha^n - \beta^n)$ (see [**9**, **12**]), where $\mathrm{Nm}(z)$ denotes the usual field norm of $z \in \mathbb{K}$. In [**4**], some easy counter-examples are given but the general problem remains very much open. In the elliptic case, the same problem is studied in [**5**], with greater success, although a fully general understanding lies some way off. Write b_n for the ideal norm

$$b_n = \mathrm{Nm}(\beta_n). \tag{5}$$

An immediate corollary of Theorem 1.1 follows. When $\mathbb{K} = \mathbb{Q}$, write $\omega_{\mathbb{K}} = \omega_{\mathbb{Q}} = \omega$ in the usual way.

https://doi.org/10.1017/S0017089504002113 Published online by Cambridge University Press

COROLLARY 1.2. *With b_n defined by* (5)*, for all sufficiently large M,*

$$\omega\left(\prod_{n=M+1}^{M+N} b_n\right) \gg N.$$

The proof of the Corollary is immediate because $\omega_{\mathbb{K}}(\beta) \leq d\omega(\mathrm{Nm}(\beta))$ for any ideal β from $\mathbb{K}$.

Finally, we include some discussion to indicate what the true picture might be for divisors of sequences $\beta = (\beta_n)$ as in (2). Calculations support our belief that for any given w, for all sufficiently large n, β_n has a primitive ideal divisor with at least w distinct prime ideal factors. For the moment, the best result we can obtain in that direction is the following.

THEOREM 1.3. *With the hypotheses of Theorem 1.1, suppose $Q = O$. Given any $w > 0$, there is an integer $q \geq 1$ such that*

$$\omega_{\mathbb{K}}\left(\prod_{n=M+1}^{M+N} \beta_{qn}\right) \geq wN.$$

In the next two sections, we gather some tools then prove Theorem 1.1. In the following section, the proof of Theorem 1.3 is given. Finally, we give an application of Theorem 1.1 to the study of divisors of Somos sequences.

2. Congruences and the growth of b_n. The first lemma is a very strong form of Siegel's Theorem.

LEMMA 2.1. *Suppose P denotes a non-torsion $\mathbb{K}$-rational point of $\mathbf{E}$. For all sufficiently large n*

$$\log b_n = dhn^2 + O(n),$$

where the constant $h = \widehat{h}(P)$ is the global canonical height of the underlying point P.

Proof of Lemma 2.1. Writing $H(R)$ for the naive height of an algebraic point, then

$$H(R) = \prod_v \max\{1, |x(R)|_v\}^{\frac{1}{d}},$$

where the product is taken over all valuations v of $\mathbb{K}$, including the archimedean or infinite valuations, which correspond to the embeddings of $\mathbb{K}$ into $\mathbb{C}$. In our set-up, we can interpret this as

$$\log H(nP + Q) = \frac{1}{d}\sum_{v|\infty} \log \max\{1, |x_n|_v\} + \frac{1}{d}\log b_n.$$

The theory of heights gives an estimate for

$$\log H(nP + Q) = \widehat{h}(nP + Q) + O(1),$$

https://doi.org/10.1017/S0017089504002113 Published online by Cambridge University Press

where $\widehat{h}(nP+Q)$ denotes the canonical height of $nP+Q$. Since this is a positive definite quadratic form, the bound in (6) follows:

$$\sum_{v|\infty} \log \max\{1, |x_n|_v\} + \log b_n = dhn^2 + O(n). \tag{6}$$

The estimate in Lemma 2.1 follows from an upper bound for $|x_n|_v$ for each archimedean valuation v. When this quantity is large it means $nP+Q$ is close to the point at infinity in that valuation. On the complex torus, this means the elliptic logarithm is close to zero. Thus bounds from elliptic transcendence theory are applicable. We use Théorème 2.1 in [**3**] but see also [**24**] where an explicit version of David's Theorem appears on page 20. The nature of the bound is

$$\log |x_n|_v \ll \log n \log\log n, \tag{7}$$

where the implied constant depends upon v, $\mathbf{E}$ and the points P and Q. Combining the estimates in (6) and (7) gives Lemma 2.1. □

For integers $M \geq 0$, $N \geq 1$, and $\mathcal{I}$ an integral ideal, denote by $T(M, N, \mathcal{I})$ the number of solutions of the congruence

$$\beta_n \equiv 0 \pmod{\mathcal{I}}, \qquad M+1 \leq n \leq M+N.$$

LEMMA 2.2. *If P is not a torsion point and $\mathcal{I}$ is an integral ideal then for any integers $M \geq 0$, $N \geq 1$,*

$$T(M, N, \mathcal{I}) \ll \frac{N}{(\log \mathrm{Nm}(\mathcal{I}))^{1/2}} + 1.$$

Proof. In this proof we are going to use the arithmetic of the curve $\mathbf{E}$ modulo $\mathcal{I}$ so some care is needed. For any ideal $\wp^r$, where $\wp$ denotes a prime ideal of $\mathbb{K}$, the set of rational points with denominator divisible by $\wp^r$, together with O, forms a group. For a detailed proof of this statement in the rational case, consult [**22**, Chapter 2, Section 4]. The set of points with denominators divisible by $\mathcal{I}$ is the intersection of those groups for all powers of prime ideals dividing $\mathcal{I}$; hence it too is a group and is closed under subtraction between two points.

Suppose that there are two integers n and k with $1 \leq n < n+k \leq N$ and $k \leq N/(T(M, N, \mathcal{I}) - 1)$ for which

$$\beta_n \equiv \beta_{n+k} \equiv 0 \pmod{\mathcal{I}}.$$

By the opening remark, subtracting gives again a point with denominator divisible by $\mathcal{I}$, $kP \equiv O \pmod{\mathcal{I}}$. Because P is not a torsion point we conclude that $b_k \neq 0$ and thus $b_k \geq \mathrm{Nm}(\mathcal{I})$. Lemma 2.1 now implies the desired bound. □

3. Proof of Theorem 1.1. For a prime ideal $\wp$ and an integer $k \geq 1$ we denote by $v_\wp(k)$ the $\wp$-adic order of k. Let

$$W = \prod_{n=M+1}^{M+N} \beta_n.$$

https://doi.org/10.1017/S0017089504002113 Published online by Cambridge University Press

For a prime ideal $\wp$, we denote by $r_\wp$ the $\wp$-adic order of W and by $s_\wp$ the largest $\wp$-adic order of the terms β_n, $n = M+1, \ldots, M+N$. Then

$$r_\wp \le \sum_{s=1}^{s_\wp} T(M, N, \wp^s).$$

By Lemma 2.2 we have

$$r_\wp \ll \sum_{s=1}^{s_\wp} \left(\frac{N}{(s \log \mathrm{Nm}(\wp))^{1/2}} + 1 \right) \ll \frac{N s_\wp^{1/2}}{(\log \mathrm{Nm}(\wp))^{1/2}} + s_\wp.$$

By Lemma 2.1 we see that $s_\wp \ll (N+M)^2 / \log \mathrm{Nm}(\wp)$. Therefore

$$r_\wp \ll \frac{(N+M)^2}{\log \mathrm{Nm}(\wp)}.$$

Thus

$$\begin{aligned} \log \mathrm{Nm}(W) &= \sum_{r_\wp > 0} r_\wp \log \mathrm{Nm}(\wp) \ll (N+M)^2 \sum_{r_\wp > 0} 1 \\ &= (N+M)^2 \omega_{\mathbb{K}} \left(\prod_{n=M+1}^{M+N} \beta_n \right). \end{aligned}$$

Lemma 2.1 implies that $N(N+M)^2 \ll \log \mathrm{Nm}(W)$ which finishes the proof. □

4. Proof of Theorem 1.3.

LEMMA 4.1. *If $Q = O$, then the sequence β_n is a divisibility sequence, meaning that $\beta_m | \beta_n$ as ideals, whenever $m|n$.*

Proof. The proof of this follows from the standard local theory of elliptic curves; see [**19**, Chapters 4 and 7]. For every prime ideal $\wp$, write $\mathbb{K}_\wp$ for the completion of $\mathbb{K}$ with respect to the valuation corresponding to $\wp$. There is a subgroup of the group of $\mathbb{K}_\wp$-rational points:

$$\mathbf{H}(\mathbb{K}_\wp) = \{O\} \cup \{R \in \mathbf{E}(\mathbb{K}_\wp) : \mathrm{ord}_\wp(x(R)) \le -2\}.$$

From [**19**, Theorem 6.4], for all $R \in \mathbf{H}(\mathbb{K}_\wp)$, we have

$$\mathrm{ord}_\wp(x(nR)) = \mathrm{ord}_\wp(x(R)) - 2\mathrm{ord}_\wp(n)$$

and the divisibility statement follows at once from this. □

Proof of Theorem 1.3. Suppose $r \ge 3w$ is an integer and $r < p_1 < \ldots < p_r$ denote r distinct primes. Put $q = p_1 \ldots p_r$. Recalling the notation of (2), let $R = qP$ and write $(x(nR)) = \gamma_n / \delta_n$ for the factorisation into integral ideals. Similarly, for each $i = 1, \ldots, r$, write $R_i = p_i P$ with $(x(nR_i)) = \gamma_{in} / \delta_{in}$ for the factorisation into integral ideals. We claim that if n is coprime to q, then δ_n has at least r distinct primitive prime ideal divisors.

https://doi.org/10.1017/S0017089504002113 Published online by Cambridge University Press

From Cheon and Hahn's Theorem [**2**], for all sufficiently large n, δ_{in} has a primitive prime ideal divisor. We claim each of these is a primitive prime ideal divisor of δ_n when n is coprime to q. By Lemma 4.1, $\beta = (\beta_n)$ is a divisibility sequence, thus any divisor of δ_{in} is a divisor of δ_n. Suppose $\wp$ is a primitive prime ideal divisor of δ_{in} and $\wp$ divides δ_m for some m. Then $mR = mqP \equiv O \bmod \wp$. In other words, $(mq/p_i)(p_iP) \equiv O \bmod \wp$. Now $\wp$ is a primitive divisor of δ_{in} and this forces n to divide mq/p_i. Since n is coprime to q, this forces n to divide m and shows that every primitive ideal divisor of δ_{in} is a primitive ideal divisor of δ_n. Each of these primitive ideal divisors is distinct thus we conclude that δ_n has at least r distinct primitive prime ideal divisors. It follows that for M sufficiently large,

$$\omega_{\mathbb{K}}\left(\prod_{n=M+1}^{M+N}\beta_{qn}\right) \geq \omega_K\left(\prod_{n=M+1,(n,q)=1}^{M+N}\delta_n\right) \geq rN\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$
$$\geq rN\left(1-\frac{1}{r}\right)^r \geq re^{-1}N \geq wN,$$

which completes the proof of Theorem 1.3. □

5. Somos sequences. Sequences such as $u_n = a^n - b^n$ are known to satisfy a binary linear recurrence relation with integer coefficients. Recently, Swart [**25**], building on some unpublished identities of Nelson Stephens, has related elliptic curves to *Somos sequences*. These sequences, named after Michael Somos [**23**], satisfy a bilinear recurrence relation of the form

$$s_{n+2}s_{n-2} = As_{n+1}s_{n-1} + Bs_n^2, \tag{8}$$

where A and B are rational numbers, not both zero. A special case is the sequence $s = (s_n)$ with $A = B = 1$, which begins $1, 1, 1, 1, \ldots$ with subsequent terms defined by the recurrence relation (8). This is known as the *Somos-4 sequence*. Although a division is needed in the definition of the later terms, they do all turn out to be integral. For an introduction to Somos sequences, as well as links to other areas of mathematics, consult [**6**], [**7**], [**8**], [**10**], [**13**], [**14**].

If $P = (x, y)$ and Q are rational points with $Q + nP$ never the point at infinity, continue to write $Q + nP = (x_n, y_n)$. Then a sequence s satisfying (8) can be obtained as follows (see [**25**]): let s_{-1} and s_0 be arbitrary non-zero rational numbers and

$$s_{n+1} = -\frac{(x_n - x)s_n^2}{s_{n-1}} \text{ for } n \geq 0. \tag{9}$$

Clearly the sequence $s = (s_n)$ could turn out to have rational terms. In fact Swart [**25**] shows that the denominators are easy to understand in terms of the starting data. In a sense that can be made precise, each rational sequence is equivalent to an integral sequence. Moreover, she shows that beginning with a rational sequence s satisfying (8) it is possible to reverse the process and recover an elliptic curve together with the two rational points P and Q which yields the sequence s according to the formula in (9).

EXAMPLE 5.1. If s is the Somos-4 sequence, the corresponding elliptic curve is

$$y^2 + y = x^3 - x,$$

https://doi.org/10.1017/S0017089504002113 Published online by Cambridge University Press

with $Q=(0,0)$ and $P=(1,0)=2Q$ and $s_{-1}=s_0=1$. Thus the terms of the Somos-4 sequence correspond to the denominators of the odd multiples of the point $Q=(0,0)$.

Any *elliptic divisibility sequence* (see [**18**, **26**, **27**] for background and basic properties) arises when Q is the point at infinity, and satisfies a relation (8) with $A=1$ and $B=-1$. Thus Somos sequences are a generalisation of elliptic divisibility sequences. We are able to record a weaker version of Theorem 1.1 for Somos sequences. This is stated in the rational case because it relies on Swart's thesis, which deals with rational sequences only (although her methods will surely generalise to algebraic sequences). The definition of ω extends to all non-zero rational numbers, if $q=a/b$ with a and b denoting coprime integers then $\omega(q)=\omega(a)$.

COROLLARY 5.2. *Let* $\mathbf{E}$ *denote a rational elliptic curve having rational points* P *and* Q *with* P *non-torsion and* $Q+nP=(x_n, y_n)$ *not the point at infinity for all* n. *Let* s *denote a rational sequence defined by* (9), *which satisfies* (8) *for some* A *and* B. *Then*

$$\omega\left(\prod_{n=1}^{N} s_n\right) \gg N.$$

Proof. It is shown in [**5**] that for any Somos sequence $s=(s_n)$, any primitive divisor of b_n is a primitive divisor of the sequence of numerators of s_{n-1}. The result now follows from Corollary 1.2 □

It seems likely that the methods in this paper could be used to prove a stronger version of Corollary 5.2, of the kind in Corollary 1.2.

ACKNOWLEDGEMENTS. Our thanks go to Helen King for helping to clarify the proof of Theorem 1.1. Most of this paper was written during a very enjoyable visit by the second author to the University of East Anglia. Thanks especially to Tom Ward, whose hospitality was very much appreciated.

REFERENCES

1. Yu. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.* **539** (2001), 75–122.

2. J. Cheon and S. Hahn, The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve, *Acta. Arith.* **88** (1999), 219–222.

3. S. David, *Minorations de formes linéaires de logarithmes elliptiques*, *Mém. Soc. Math. France (N.S.)* **62** (1995).

4. G. Everest and K. Győry, Primitive prime divisors, Preprint (2003).

5. G. Everest and H. King, Primitive divisors of bilinear recurrence sequences, Preprint (2003).

6. G. Everest, A. J. van der Poorten, I. E. Shparlinski and T. Ward, *Recurrence sequences*, Math. Surveys and Monographs, **104** (Amer. Math. Soc., Providence, RI, 2003).

7. D. Gale, The strange and surprising saga of the Somos sequences, *Math. Intelligencer* **13** (1991), 40–42.

8. D. Gale, Somos sequence update, *Math. Intelligencer* **13** (1991), 49–50.

9. D. H. Lehmer, Factorization of certain cyclotomic functions, *Ann. of Math.* **34** (1933), 461–479.

10. J. L. Malouf, An integer sequence from a rational recursion, *Discrete Math.* **110** (1992), 257–261.

11. T. Pheidas, An effort to prove that the existential theory of $\mathbb{Q}$ is undecidable, *Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent 1999)*, *Contemp. Math.* **207**, (2000), 237–252.

12. T. A. Pierce, Numerical factors of the arithmetical forms $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$, *Ann. of Math.* **18** (1917), 53–64.

13. J. Propp, The Somos sequence site, Available from http://www.math.wisc.edu/~propp/somos.html.

14. R. M. Robinson, Periodicity of Somos sequences, *Proc. Amer. Math. Soc.* **116** (1992), 613–619.

15. A. Schinzel, On primitive prime factors of $a^n - b^n$, *Proc. Camb. Phil. Soc.* **58** (1962), 555–562.

16. A. Schinzel, Primitive divisors of the expression $A^n - B^n$ in algebraic number fields, *J. Reine Angew. Math.* **268/69** (1974), 27–33.

17. A. Schinzel, An extension of the theorem on primitive divisors in algebraic number fields, *Math. Comp.* **61** No. 203 (1993), 441–444.

18. R. Shipsey, *Elliptic divisibility sequences*, PhD Thesis, University of London (2000).

19. J. H. Silverman, *The arithmetic of elliptic curves* (Springer-Verlag, 1986)

20. J. H. Silverman, Weiferich's criterion and the *ABC*-conjecture, *J. Number Theory* **30** (1988), 226–237.

21. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves* (Springer-Verlag, 1994).

22. J. H. Silverman and J. Tate, *Rational points on elliptic curves* (Springer-Verlag, 1992).

23. M. Somos, Problem 1470, *Crux Mathematicorum.* **15** (1989), 208.

24. R. J. Stroeker and N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms, *Acta. Arith.* **67** (1994), 177–196.

25. C. Swart, *Elliptic divisibility sequences*, PhD Thesis, University of London (2003).

26. M. Ward, The law of repetition of primes in an elliptic divisibility sequence, *Duke Math. J.* **15** (1948), 941–946.

27. M. Ward, Memoir on elliptic divisibility sequences, *Amer. J. Math.* **70** (1948), 31–74.

28. K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math.* **3** (1892), 265–284.