New York Journal of Mathematics

New York J. Math. **25** (2019) 642–650.

On second-order linear recurrence sequences in Mordell-Weil groups

Stefan Barańczuk

ABSTRACT. In this paper we determine second-order linear recurrence sequences in Mordell-Weil groups of elliptic curves over number fields without complex multiplication having almost all primes as divisors. We also consider more general groups of Mordell-Weil type.

CONTENTS

Results

Linear integral recurring sequences of order two are recurrences defined by the recursion relation

$$x_{n+2} = ax_{n+1} + bx_n$$

where the parameters a, b and the initial terms x_0, x_1 are integers. We say that a positive integer d is a *divisor of a sequence* if it divides some term of the sequence. L. Somer ([Som]) using a result by A. Schinzel ([Sch2]) determined those linear integral recurring sequences of order two that have almost all prime numbers as divisors. Essentially, they are multiples of translations of recurrences with initial terms $0, 1$. Note also that M. Ward ([W], Theorem 1.) proved that a linear integral recurring sequence of order two which is not non-trivially degenerate has an infinite number of distinct prime divisors.

In the present paper we address analogous problem for sequences in Mordell-Weil groups of elliptic curves. Let K be a number field and E/K an

Received November 15, 2018.
2010 *Mathematics Subject Classification.* 11G05, 11B50.
Key words and phrases. Mordell-Weil groups, algebraic K-theory groups, recurrence sequences, reduction maps.

ISSN 1076-9803/2019

elliptic curve without complex multiplication. For $P, Q \in E(K)$ and rational integers a, b we define the following sequence

$$\begin{cases} S_0 = P, \\ S_1 = Q, \\ S_{n+2} = aS_{n+1} + bS_n \quad \text{for } n \geq 0 \end{cases}$$

and ask for its divisors, where in this setting a divisor of a sequence is a prime v of good reduction such that for some n we have $S_n = 0 \bmod v$.

We have the following simple analogue of Ward's result:

Proposition 1. *Suppose that the set of distinct terms of $\{S_n\}$ is infinite or one of the terms equals 0. Then $\{S_n\}$ has an infinite number of distinct prime divisors.*

Proof. Let E be given by a Weierstrass equation with all coefficients in the ring of integers of K. For every point $P \in E(K)$ and every prime v of good reduction we have $P = 0 \bmod v$ if and only if the denominator of the x-coordinate of P is divisible by v. Thus by Siegel's theorem on S-integral points, for any finite set of primes there are only finitely many points in $E(K)$ having no prime divisor outside the set. □

The aim of the paper is to prove the following analogue of Somer's result:

Theorem 2. *The following are equivalent:*

- *For all but finitely many primes v there exists a natural number n such that*
$$S_n = 0 \bmod v. \tag{1}$$
- *There is a point $R \in E(K)$ and a natural number N such that for every $n \geq 0$ we have*
$$S_{n+N} = s_n R$$
where $\{s_n\}$ is a linear integral recurring sequence of order two having all positive integers as divisors. In particular, when the group $E(K)_{\text{tors}}$ is trivial then the whole sequence $\{S_n\}$ is of the given form.

Remark 1. For a rational integer n let F_n denote the n-th Fibonacci number. Recall that every positive integer divides infinitely many terms of the sequence $\{F_n\}_{n\geq 0}$. Fix a natural number N and a prime number p. Let E/K be an elliptic curve over a number field K such that the group $E(K)$ has a nontorsion point P and a torsion point T of order p^{N+1}. Consider the sequence

$$S_n = p^n(F_{n-N}P + F_{n-N-1}T) \text{ for } n \geq 0.$$

This sequence is recursive with recursive rule

$$S_{n+2} = pS_{n+1} + p^2 S_n \text{ for } n \geq 0.$$

We have

$$S_n = p^n F_{n-N} P \text{ for } n \geq N+1$$

but

$$S_N = p^N(F_0 P + F_{-1} T) = p^N T \neq 0,$$
$$S_{N+1} = p^{N+1}(F_1 P + F_0 T) = p^{N+1} P$$

so S_N and S_{N+1} cannot be multiples of the same point in $E(K)$. This example shows that in general the number N in the formulation of Theorem 2 cannot be uniformly bounded.

Remark 2. Classic linear recurring sequences of order two can be rewritten as

$$\alpha^n A - \beta^n B$$

or

$$\alpha^n (A + nB),$$

however in our setting there is no such equivalence, thus the sequences of the above forms have to be discussed separately; we have investigated them in [Bar2].

Remark 3. Let P, Q be points in the Mordell-Weil group of an elliptic curve. K. Stange ([Sta]) initiated a study of what she called *elliptic nets*, i.e., two-parameter sequences $\{nP + mQ\}$. The sequences we investigate are particular subsequences of Stange's nets.

In the remainder of this paper we will use the following notation:

ord T	the order of a torsion point $T \in E(K)$
$\mathrm{ord}_v P$	the order of a point P mod v where v is a prime of good reduction
$l^k \parallel n$	means that l^k exactly divides n, i.e. $l^k \mid n$ and $l^{k+1} \nmid n$ where l is a prime number, k a positive integer and n a natural number.

Before we present the proof of Theorem 2 we encapsulate the used properties of Mordell-Weil groups and of recurrence sequences in the following three Propositions.

Proposition 3.

(a) *For all but finitely many primes v the induced reduction map is injective when restricted to the torsion part of the Mordell-Weil group.*

(b) *Let l be a prime number and $(k_1, \ldots, k_m)$ a sequence of nonnegative integers. If $P_1, \ldots, P_m \in E(K)$ are points linearly independent over $\mathrm{End}_{\bar{K}}(E)$ then there is an infinite family of primes v such that $l^{k_i} \parallel \mathrm{ord}_v P_i$ if $k_i > 0$ and $l \nmid \mathrm{ord}_v P_i$ if $k_i = 0$.*

(c) *For every nontorsion point $P \in E(K)$ there exists a natural number M such that for every $m > M$ there is a prime v such that $\mathrm{ord}_v P = m$.*

Proof.
(a) Well known (see [SilAEC], Proposition 3.1).
(b) See [Bar1], Theorem 5.1.
(c) See [Sil], Proposition 10 for elliptic curves over $\mathbb{Q}$ and [CH] for elliptic curves over arbitrary number fields. □

Proposition 4. *Let the sequence $\{x_n\}$ be defined as follows:*

$$\begin{cases} x_0 = 0, \\ x_1 = 1, \\ x_{n+2} = ax_{n+1} + bx_n \quad \textit{for } n \geq 0 \end{cases}$$

with a, b being nonzero integers. One of the following holds:

- *There exists a prime number p such that either the sequence*
$$\{x_{n+1} + bx_n\}_{n \geq 0}$$
or the sequence
$$\{x_{n+1} - bx_n\}_{n \geq 0}$$
has the property that none of its terms is divisible by p.
- *No term of $\{x_n\}_{n>0}$ is exactly divisible by 2^2 and no two consecutive terms are both even.*

Proof. If there is a prime number p dividing $a + b - 1$ then for every $n \geq 0$

$$x_{n+2} + bx_{n+1} = x_{n+1} + bx_n \bmod p$$

thus by induction every term of the sequence $\{x_{n+1} + bx_n\}_{n \geq 0}$ is congruent to 1 modulo p.

If there is a prime number p dividing $a - b + 1$ then for every $n \geq 0$

$$x_{n+2} - bx_{n+1} = -(x_{n+1} - bx_n) \bmod p$$

thus by induction every term of the sequence $\{x_{n+1} - bx_n\}_{n \geq 0}$ is congruent to ± 1 modulo p.

If $(a, b) \in \{(1, 1), (-1, 1)\}$ then the sequence $\{x_n \bmod 8\}_{n \geq 0}$ equals

$$0, 1, \pm 1, 2, \pm 3, 5, 0, 5, \pm 5, 2, \pm 7, 1, 0, 1 \ldots$$

so no term is exactly divisible by 2^2 and no two consecutive terms are both even. □

Proposition 5. *Let $\{x_n\}_{n \geq 0}$ be a linear integral recurring sequence of order two with nonzero parameters a, b.*

(a) *Let p be a prime number dividing b and e a positive integer such that $p^e \mid x_n$ for infinitely many indices n. Then there exists a natural number N such that $p^e \mid x_n$ for every $n \geq N$.*
(b) *If $\gcd(x_0, x_1) = 1$ then for every $n \geq 0$ the number $\gcd(x_n, x_{n+1})$ has no prime divisors other than those dividing b.*

Proof.
(a) There is $n_1 > 0$ such that $p \mid x_{n_1}$ hence by induction on n we have $p \mid x_n$ for every $n \geq n_1$. Now we proceed by induction on the exponent. Suppose that for a positive integer $i < e$ there is n_i such that $p^i \mid x_n$ for every $n \geq n_i$. Let $n_{i+1} > n_i$ be such that $p^{i+1} \mid x_{n_{i+1}}$. Then by induction on n we have $p^{i+1} \mid x_n$ for every $n \geq n_{i+1}$.
(b) For $n \geq 0$ we have

$$\gcd(x_{n+1}, x_{n+2}) = \gcd(x_{n+1}, ax_{n+1} + bx_n) = \gcd(x_{n+1}, bx_n)$$

so we are done by induction. □

Proof of Theorem 2. ($\Rightarrow$) For $n \geq 0$ we have

$$S_{n+2} = x_{n+2}Q + bx_{n+1}P \tag{2}$$

where the sequence $\{x_n\}$ is defined as follows:

$$\begin{cases} x_0 = 0, \\ x_1 = 1, \\ x_{n+2} = ax_{n+1} + bx_n \quad \text{for } n \geq 0. \end{cases}$$

If some term of $\{S_n\}$ equals 0 we are done. So assume that this is not the case. In particular, this means that no S_n is divisible by infinitely many primes.

First we suppose that P, Q are nontorsion and a, b are nonzero. We will show that P, Q are linearly dependent. By Proposition 4 there are two cases to be considered.

Let us consider the case when there exists a prime number p such that no term of $\{x_{n+1} + bx_n\}_{n \geq 0}$ (resp. of $\{x_{n+1} - bx_n\}_{n \geq 0}$) is divisible by p. Rewrite (2) as

$$\begin{gathered} S_{n+2} = (x_{n+2} + bx_{n+1})Q + x_{n+1}(bP - bQ) \\ (\text{resp. } S_{n+2} = (x_{n+2} - bx_{n+1})Q + x_{n+1}(bP + bQ)). \end{gathered} \tag{3}$$

Suppose that P, Q are linearly independent. Then $bP - bQ, Q$ (resp. $bP + bQ, Q$) are also linearly independent and by Proposition 3 *(b)* there is an infinite family of primes v such that $p \nmid \operatorname{ord}_v(bP - bQ)$ (resp. $p \nmid \operatorname{ord}_v(bP + bQ)$) and $p \mid \operatorname{ord}_v Q$. By (1) and (3) we have that for some n

$$(x_{n+2} + bx_{n+1})Q + x_{n+1}(bP - bQ) = 0 \bmod v$$

$$(\text{resp. } (x_{n+2} - bx_{n+1})Q + x_{n+1}(bP + bQ) = 0 \bmod v)$$

and by the choice of the orders of $bP - bQ$, Q (resp. of $bP + bQ$, Q) the coefficient $(x_{n+2} + bx_{n+1})$ (resp. $(x_{n+2} - bx_{n+1})$) has to be divisible by p.

By the contradiction P, Q are linearly dependent.

Now we consider the case when no term of the sequence $\{x_n\}$ is exactly divisible by 2^2 and no two consecutive terms are both even. Suppose that P, Q are linearly independent. By Proposition 3 *(b)* there is an infinite family of primes v such that $2^3 \parallel \mathrm{ord}_v Q$ and $2 \parallel \mathrm{ord}_v bP$.

If $2 \nmid x_{n+2}$ then $2^3 \mid \mathrm{ord}_v(x_{n+2}Q)$ but $2^3 \nmid \mathrm{ord}_v(bx_{n+1}P)$.

If $2 \parallel x_{n+2}$ then $2^2 \mid \mathrm{ord}_v(x_{n+2}Q)$ but $2^2 \nmid \mathrm{ord}_v(bx_{n+1}P)$.

If $2^3 \mid x_{n+2}$ then $2 \nmid \mathrm{ord}_v(x_{n+2}Q)$ but $2 \mid \mathrm{ord}_v(bx_{n+1}P)$ since no two consecutive terms of $\{x_n\}$ are both even.

All imply by (2) that no term of $\{S_n\}$ equals 0 modulo v. Hence P, Q must be linearly dependent.

Linear dependence of P, Q means that there exist nonzero integers t, u, a nontorsion point $R \in E(K)$ and torsion points $T_0, T_1 \in E(K)$ such that $P = tR + T_0$ and $Q = uR + T_1$. If $\gcd(t, u) > 1$ we replace t, u, R by $t/\gcd(t, u), u/\gcd(t, u), \gcd(t, u)R$ resp., so we can assume that $\gcd(t, u) = 1$. Now (2) takes the form

$$S_{n+2} = (ux_{n+2} + tbx_{n+1})R + x_{n+2}T_1 + x_{n+1}bT_0. \tag{4}$$

Define the sequence $\{y_n\}$ as follows:

$$\begin{cases} y_0 = t, \\ y_1 = u, \\ y_{n+2} = ux_{n+2} + tbx_{n+1} \quad \text{for } n \geq 0. \end{cases}$$

and rewrite (4) as

$$S_{n+2} = y_{n+2}R + x_{n+2}T_1 + x_{n+1}bT_0. \tag{5}$$

Notice that the sequence $\{y_n\}$ has the parameters a and b.

If $E(K)_{\mathrm{tors}}$ is trivial we are done by Proposition 3 *(c)*. So suppose that $E(K)_{\mathrm{tors}}$ is nontrivial. By Proposition 3 *(c)* for all but finitely many natural numbers m there is a prime v such that the product of m and the order of $E(K)_{\mathrm{tors}}$ divides $\mathrm{ord}_v R$. Thus by (1) and (5) for every large enough natural number m some term of the sequence $\{y_n\}$ is divisible by m hence the sequence is divisible by all positive integers.

By Proposition 3 *(c)* the set of primes v such that $\mathrm{ord}_v R$ is coprime to the order of $E(K)_{\mathrm{tors}}$ is infinite thus by (1), (5) and Proposition 3 *(a)* there is n_0 such that S_{n_0} is a multiple of R. The terms preceding S_{n_0} are divisible by finitely many primes only hence we can ignore them. So we assume without the loss of generality that $T_0 = 0$ and rewrite (5) as

$$S_{n+2} = y_{n+2}R + x_{n+2}T_1. \tag{6}$$

If $T_1 = 0$ we are done. So suppose that this is not the case. Denote $\pi = \operatorname{ord} T_1$. Consider a finite field extension K'/K for which there exists a torsion point $T_2 \in E(K')$ such that the subgroup generated by T_1 and T_2 is isomorphic to $(\mathbb{Z}/\pi\mathbb{Z})^2$. By Proposition 3 *(c)* for almost every m coprime to π there exists a prime v' in K' such that $\operatorname{ord}_{v'}(R - T_2) = m$. Let v be a prime in K below v'. If $S_{n+2} = 0 \bmod v$ then $S_{n+2} = 0 \bmod v'$ so by (6) the corresponding x_{n+2}, y_{n+2} are both divisible by π provided v is not exceptional in view of Proposition 3 *(a)*. Hence for infinitely many indices n the terms x_n, y_n are both divisible by π.

Factorize $\pi = \pi_1\pi_2$ where π_1 is a natural number having no prime divisors other then prime divisors of b and π_2 is a natural number coprime to b.

Applying Proposition 5 *(a)* to every prime divisor of π_1 we get that $\pi_1 \mid x_n$ and $\pi_1 \mid y_n$ for every sufficiently large n.

Thus there is N such that π_1 divides both x_n, y_n for every $n \geq N$ and π divides both x_N, y_N. By Proposition 5 *(b)* both x_{N+1}, y_{N+1} are coprime to π_2 thus there is an integer α such that $\alpha y_{N+1} = x_{N+1} \bmod \pi_2$. Since $y_N = x_N = 0 \bmod \pi_2$ we have $\alpha y_N = x_N \bmod \pi_2$ so we get by induction that $\alpha y_n = x_n \bmod \pi_2$ for every $n \geq N$. We also have $\alpha y_n = x_n \bmod \pi_1$ for every $n \geq N$. Thus

$$\alpha y_n = x_n \bmod \pi \tag{7}$$

for every $n \geq N$ since π_1, π_2 are coprime. Define the point $\tilde{R} = \pi_1 R + \alpha\pi_1 T_1$ and the sequence $\{\tilde{y}_n\}_{n=N}^{n=\infty}$ by $\tilde{y}_n = y_n/\pi_1$ for every $n \geq N$.

The proof is complete since for every $n \geq N$ we have by (7) that

$$\tilde{y}_n \tilde{R} = y_n R + x_n T_1.$$

Now it remains to discuss the cases when one of the points P, Q is torsion or one of the numbers a, b is 0.

If one of the points is torsion and nonzero and the other is nontorsion and both a, b do not equal 0 then we eventually arrive at the solved case.

If both P, Q are torsion then the assertion of Theorem 2 follows immediately from Proposition 3 *(a)*.

If both a, b equal 0 then $S_2 = 0$.

If exactly one of the numbers a, b equals 0 then we have either of the sequences

$$\begin{array}{l} P, Q, bP, bQ, b^2P, b^2Q, \dots \\ P, Q, aQ, a^2Q, a^3Q, \dots \end{array}.$$

By Proposition 3 *(b)* and Proposition 3 *(a)* there is an infinite set of primes that are not divisors of either of them unless there is a zero term, i.e. P or

Q is torsion with the order dividing a power of b when $a = 0$ or Q is torsion with the order dividing a power of a when $b = 0$.

($\Leftarrow$) If $\{s_n\}$ is a linear integral recurring sequence of order two having all positive integers as divisors then for any prime v of good reduction we can find a term s_n divisible by $\mathrm{ord}_v R$.

$\square$

Remark 4. Consider the following groups:

(1) $R^{\times}_{F,S}$, S-units groups, where F is a number field and S is a finite set of ideals in the ring of integers R_F,
(2) $A(F)$, Mordell-Weil groups of abelian varieties over number fields F with $\mathrm{End}_{\bar{F}}(A) = \mathbb{Z}$,
(3) $K_{2n+1}(F)$, $n > 0$, odd algebraic K-theory groups.

Like Mordell-Weil groups of elliptic curves they are equipped with reduction maps modulo prime ideals so we can ask the question of the paper in their context too (cf. Remark 3 of [Bar2]).

In the S-units groups case we obtain the same result as in Theorem 2 (notice that we have to change the additive notation to multiplicative) since they share appropriate properties of Mordell-Weil groups; in particular, the analogue of Proposition 3 *(c)* is the main result of [Sch1].

In the remaining groups cases we lack analogues of Proposition 3 *(c)* so we obtain slightly weaker results. Let G be an arbitrary group as above. The direct analogue of Theorem 2 holds for G provided that the torsion part of G is trivial. Indeed, if a or b equals 0 then proof is again immediate. So suppose that a and b are nonzero. Repeating the first lines of the proof of Theorem 2 we get that P and Q are dependent. This means that there is a point $R \in G$ such that for every $n \geq 0$ we have

$$S_n = s_n R$$

where $\{s_n\}$ is a linear integral recurring sequence of order two that by Theorem 5.1 in [Bar1] is divisible by every power of every prime number. If some s_n equals 0 we are done. So suppose that this is not the case. By Theorems 1 and 3 of [Som] we get that $\{s_n\}$ is either a multiple of a translation of a sequence with zero term or a sequence of the form $gh^{n-1}(i + jn)$ with coprime i, j.

Let $\{s_n\}$ be a multiple of a translation of a linear integral recurring sequence of order two $\{t_n\}$ with $t_0 = 0$. For such sequences we have that if $m_1 \mid t_{n_1}$ and $m_2 \mid t_{n_2}$ with $n_1, n_2 \geq 1$ then m_1 and m_2 both divide t_n for every n divisible by $n_1 n_2$. Thus for every natural number N the sequence $\{t_n\}_{n \geq N}$ is divisible by all positive integers and so is $\{s_n\}$.

Now let $s_n = gh^{n-1}(i + jn)$ with coprime i, j. If $j = 0$ then $\{s_n\}$ cannot be divisible by every power of every prime number unless its terms are all 0. So $j \neq 0$. Suppose there is a prime number p such that $p \mid j$ and $p \nmid h$. Then there is a power of p not dividing $\{s_n\}$. So all primes dividing j divide

h. Let m be an arbitrary positive integer. Factorize $m = m_1 m_2$ where m_1 is a natural number having no prime divisors other then prime divisors of j and m_2 is a natural number coprime to j. Since m_2 is coprime to j there are infinitely many n such that $m_2 \mid (i + jn)$. In particular, if those n's are large enough we have $m_1 \mid h^{n-1}$ thus $m \mid s_n$.

Acknowledgments

We drew inspiration form Prof. Schinzel's lecture on recursive sequences and congruences he gave in Poznań in 2016 at the *Arithmetic Algebraic Geometry Seminar* organized by G. Banaszak and P. Krasoń.

References

[Bar1] Barańczuk, Stefan. On reduction maps and support problem in K-theory and abelian varieties. *J. Number Theory* **119** (2006), no. 1, 1–17. MR2228946, Zbl 1107.14033, arXiv:math/0504215, doi: 10.1016/j.jnt.2005.10.011. 645, 649

[Bar2] Barańczuk, Stefan. On certain sequences in Mordell–Weil type groups. *New York J. Math.* **23** (2017), 41–47. MR3611072, Zbl 06684171. 644, 649

[CH] Cheon, Jung Hee; Hahn, Sang Geun. The orders of the reductions of a point in the Mordell–Weil group of an elliptic curve. *Acta Arith.* **88** (1999), no. 3, 219–222. MR1683630, Zbl 0933.11029, doi: 10.4064/aa-88-3-219-111. 645

[Sch1] Schinzel, Andrzej. Primitive divisors of the expression $A^n - B^n$ in algebraic number fields. *J. Reine Angew. Math.* **268(269)** (1974), 27–33. MR0344221, Zbl 0287.12014, doi: 10.1515/crll.1974.268-269.27. 649

[Sch2] Schinzel, Andrzej. On power residues and exponential congruences. *Acta Arith.* **27** (1975), 397–420. MR0379432, Zbl 0342.12002, doi: 10.4064/aa-27-1-397-420. 642

[Sil] Silverman, Joseph H. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory* **30** (1988), no. 2, 226–237. MR0961918, Zbl 0654.10019, doi: 10.1016/0022-314X(88)90019-4. 645

[SilAEC] 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, Zbl 1194.11005, doi: 10.1007/978-0-387-09494-6. 645

[Som] Somer, Lawrence. Which second-order linear integral recurrences have almost all primes as divisors? *Fibonacci Quart.* **17** (1979), no. 2, 111–116. MR0536958, Zbl 0401.10015. 642, 649

[Sta] Stange, Katherine E. Elliptic nets and elliptic curves. *Algebra Number Theory* **5** (2011), no. 2, 197–229. MR2833790, Zbl 1277.11063, arXiv:0710.1316, doi: 10.2140/ant.2011.5.197. 644

[W] Ward, Morgan. Prime divisors of second order recurring sequences. *Duke Math. J.* **21** (1954), 607–614. MR0064073, Zbl 0058.03701, doi: 10.1215/S0012-7094-54-02163-8. 642

(Stefan Barańczuk) Faculty of Mathematics and Computer Science, Adam Mickiewicz University, ul. Umultowska 87, Poznań, Poland
stefbar@amu.edu.pl

This paper is available via http://nyjm.albany.edu/j/2019/25-30.html.