New York Journal of Mathematics

New York J. Math. **23** (2017) 41–47.

On certain sequences in Mordell–Weil type groups

Stefan Barańczuk

Abstract. In this paper we investigate divisibility properties of two families of sequences in the Mordell–Weil group of elliptic curves over number fields without complex multiplication. We also consider more general groups of Mordell–Weil type.

M. Ward ([W], Theorem 1.) proved that a linear integral recurring sequence of order two which is not nontrivially degenerate has an infinite number of distinct prime divisors, where by a divisor of a sequence we mean a positive integer dividing some term of the sequence. Then L. Somer ([Som]) using a result by A. Schinzel ([Schi2]) determined those recurrences that have almost all primes as divisors.

The general terms of nondegenerate linear recurring sequences of order two are of the form

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

and the general terms of trivially degenerate linear recurring sequences of order two are of the form

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

In the present paper we investigate analogues of such sequences in Mordell–Weil group of elliptic curves:

Let F be a number field, E/F an elliptic curve without complex multiplication, $P, Q \in E(F)$ and ϕ, ψ be isogenies (since we deal with curves without CM the isogenies are simply endomorphisms defined by the multiplication by rational integers; see Remark 5). We investigate sequences:

$$W_n = \phi^n P - \psi^n Q \tag{1}$$

and

$$W_n = \phi^n (P + nQ). \tag{2}$$

In this setting a divisor of a sequence is a prime ideal v of good reduction such that for some term W_n in the sequence we have $W_n = 0 \mod v$; see Remark 4.

Received September 27, 2016.

2010 *Mathematics Subject Classification.* 11R70, 14K15.

Key words and phrases. Mordell–Weil groups, algebraic K-theory groups, sequences, reduction maps.

ISSN 1076-9803/2017

In the paper, "almost all primes" means "all but finitely many primes"; see Remark 6.

For us a sequence of either type is degenerate when the set of its terms is finite.

Let us first state our analogue of Ward's result:

Proposition 1. *Let (W_n) be nondegenerate or one of its terms be equal to 0. Then (W_n) has an infinite number of distinct prime divisors.*

Proof. If one of the terms equals 0 then there is nothing to prove. So assume that the set of the terms of the sequence is infinite. The assertion is an immediate corollary of Siegel's theorem on S-integer points. Indeed, if the set S of distinct prime divisors of (W_n) were finite, then (W_n) would be finite, since for a prime v of good reduction $W_n = 0 \mod v$ if and only if the denominator of the x-coordinate of W_n is divisible by v. □

Now we turn to our analogues of Somer's results. In their proofs we use several times the following proposition:

Proposition 2.

(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) *If $P \in E(F)$ is nontorsion then for every prime number l there exist infinitely many primes v such that the order of $P \mod v$ is divisible by l and infinitely many primes v such that the order of $P \mod v$ is not divisible by l .*

Proof. (a) Well known for elliptic curves (see [SilAEC], Proposition 3.1). For general Mordell–Weil type groups (cf. Remark 3) see Lemma 3.11 of [BanGK].

(b) For the proof of this statement for Mordell–Weil type groups see [Bar1], Theorem 5.1. If the reader is focused on elliptic curves, better reference is [Sil], Proposition 10 (for elliptic curves over $\mathbb{Q}$) and [CH] (for elliptic curves over arbitrary number fields). For abelian varieties this result is proved in [Pink], Corollary 4.3. □

Theorem 3. *Let $P, Q \in E(F)$ and ϕ, ψ be rational integers. Define*

$$W_n = \phi^n P - \psi^n Q.$$

The following are equivalent:

- *For almost every v there exists a natural number n_v such that*

$$W_{n_v} = 0 \mod v. \tag{3}$$

- *There exists a natural number n such that*

$$W_n = 0$$

or we have the following particular case: P, Q are nontorsion, ϕ, ψ are nonzero, $\phi \neq \pm\psi$, the set of prime divisors of ϕ equals the set

of prime divisors of ψ and there exists a natural number n such that W_n is a torsion point killed by some power of $\gcd(\phi, \psi)$.

Proof. ($\Rightarrow$) First consider simple cases. If both ϕ, ψ equal 0 the assertion is obvious. If both P, Q are torsion points, then the assertion follows immediately from Proposition 2(a). Similarly we deal when $\phi = 0$ and Q is torsion or $\psi = 0$ and P is torsion. So suppose that $\phi \neq 0$ and P is nontorsion. If $\psi = 0$ or Q is torsion, then fix a prime number l, coprime to ϕ if $\psi = 0$ or coprime to both the order of Q and to ϕ if Q is torsion. By Proposition 2(b) there exist infinitely many v's such that l divides the order of $P \mod v$, thus the condition (3) is not met. Summarizing, we are reduced to proving the Theorem when P, Q are nontorsion and $\phi, \psi \neq 0$.

By (3) and the Theorem in [Bar2] there exist natural numbers k, l and nonzero integers a, b such that

$$\phi^k P = aQ \quad \text{and} \quad \psi^l Q = bP, \tag{4}$$

and without loss of generality we can assume that $l = k$. Indeed, suppose that $k > l$. Then multiplying $\psi^l Q = bP$ by ψ^{k-l} we get $\psi^k Q = \psi^{k-l} bP$ and $\psi^{k-l} b$ is our new b.

Now (4) immediately implies that $abQ = \phi^k \psi^k Q$ thus

$$ab = \phi^k \psi^k \tag{5}$$

since Q is nontorsion.

Let l by any prime number. By Proposition 2(b) there exist infinitely many v's such that l divides the order of $Q \mod v$. But multiplying (3) by ϕ^k and using (4) we get

$$(\phi^{n_v} a - \psi^{n_v} \phi^k) Q = 0 \mod v$$

for some natural n_v. It means that l divides $\phi^{n_v} a - \psi^{n_v} \phi^k$. Since l was arbitrary we get by [Schi1] that there exists a natural number s such that

$$\phi^s a - \psi^s \phi^k = 0 \tag{6}$$

and analogously we have

$$\psi^t b - \phi^t \psi^k = 0, \tag{7}$$

for some natural number t, which together with (5) gives

$$\phi^{t-s} = \psi^{t-s}.$$

Hence we have three possibilities: $\phi = \psi$ or $\phi = -\psi$ and $t - s$ is even or $t - s = 0$; the first two imply the assertion of the theorem immediately. Indeed, if $\phi = \psi$ then by (6) we have $a = \phi^k$, thus $\phi^k P - \psi^k Q = 0$ by (4). If $\phi = -\psi$ then again by (6) and (4) we get either $\phi^k P - \psi^k Q = 0$ or $\phi^{k+1} P - \psi^{k+1} Q = 0$, depending on the parity of the numbers s, k.

So suppose that $\phi \neq \pm\psi$ and $t - s = 0$. Since $a = \psi^s \phi^{k-s}$ and $b = \phi^s \psi^{k-s}$ by (6) and (7), thus by (4) $\phi^k P = \psi^s \phi^{k-s} Q$ and $\psi^k Q = \phi^s \psi^{k-s} P$

so $\phi^k(\phi^s P - \psi^s Q) = 0$ and $\psi^k(\phi^s P - \psi^s Q) = 0$ hence by the Euclidean algorithm $\gcd(\phi^k, \psi^k)(\phi^s P - \psi^s Q) = 0$.

The exponent s is unique. Indeed, suppose that there are two numbers $s'' > s'$ such that both $\phi^{s'} P - \psi^{s'} Q$, $\phi^{s''} P - \psi^{s''} Q$ are torsion. Then $(\psi^{s''} - \phi^{s''-s'}\psi^{s'})Q = \phi^{s''-s'}(\phi^{s'} P - \psi^{s'} Q) - (\phi^{s''} P - \psi^{s''} Q)$ is torsion as a linear combination of two torsion points. But $\psi^{s''} - \phi^{s''-s'}\psi^{s'} \neq 0$, a contradiction.

Let us denote $T = \phi^s P - \psi^s Q$, $\eta = \gcd(\phi, \psi)$. We have shown above that $\eta^k T = 0$.

Now let us consider the case when the set of prime divisors of ϕ does not equal the set of prime divisors of ψ. Without loss of generality we can assume that a prime number l divides ϕ and does not divide ψ. By Proposition 2(b) there are infinitely many primes v such that l divides the order of $Q \mod v$.

Suppose that the assertion of the theorem does not hold, i.e., $W_n \neq 0$ for every natural n, thus for each W_n there might exist only finitely many primes v such that $W_n = 0 \mod v$. Hence the numbers n_v are greater then $\max(s, k)$ for almost all v's chosen above.

So we restrict our attention to those n_v's. Denote $\alpha = n_v - s$ and compute:

$$\begin{aligned}
\eta^{s+\alpha}\psi^s(\phi^\alpha - \psi^\alpha)Q &= \eta^{s+\alpha}(\phi^\alpha T + \psi^s(\phi^\alpha - \psi^\alpha)Q) \\
&= \eta^{s+\alpha}(\phi^\alpha(\phi^s P - \psi^s Q) + (\phi^\alpha\psi^s - \psi^{s+\alpha})Q) \\
&= \eta^{s+\alpha}(\phi^{s+\alpha} P - \psi^{s+\alpha} Q) \\
&= \eta^{s+\alpha}(\phi^{n_v} P - \psi^{n_v} Q) \\
&= 0.
\end{aligned}$$

But that is a contradiction to the choice of the order of Q, since l does not divide $\eta^{s+\alpha}\psi^s(\phi^\alpha - \psi^\alpha)$.

($\Leftarrow$) We only have to consider the particular case, i.e., when the numbers ϕ, ψ have the same set of prime divisors and

$$\phi^k(\phi^n P - \psi^n Q) = 0. \tag{8}$$

Let us factorise the order of $Q \mod v$ as $m_1 m_2$, where all prime numbers dividing m_1 divide ψ and m_2 is coprime to ψ. Let d be a natural number such that m_1 divides both ϕ^{k+d} and ψ^{k+d} and such that the order of $\frac{\phi}{\psi}$ in the group $(\mathbb{Z}/m_2\mathbb{Z})^\times$ divides $k + d$. Then

$$(\phi^{k+d} - \psi^{k+d})Q = 0 \mod v. \tag{9}$$

Now multiplying (8) by ϕ^d and (9) by ψ^n and summing the results we get

$$\phi^{n+k+d} P - \psi^{n+k+d} Q = 0 \mod v$$

so we put $n_v = n + k + d$. □

Proposition 4. *Let $P, Q \in E(F)$ and ϕ be an integer number such that no power of ϕ kills P (in particular $\phi \neq 0$ and P is nonzero). Define $W_n = \phi^n(P + nQ)$. The following are equivalent:*

- *For almost every v there exists a natural number n_v such that*

$$W_{n_v} = 0 \mod v. \tag{10}$$

- *Either P, Q are torsion and there is a natural number n such that $W_n = 0$ or P, Q are nontorsion and there exist a nonzero integer a and a natural number n such that $\phi^n P = aQ$.*

Proof. ($\Rightarrow$) If both P, Q are torsion then we use Proposition 2(a). If P is torsion and Q nontorsion then fix a prime number l coprime to ϕ and dividing the order of P. By Proposition 2(b) there are infinitely many primes v such that l does not divide the order of $Q \mod v$, thus the condition (10) is not met by Proposition 2(a). Hence we can assume that P is nontorsion. By [Bar2] there exist an integer a and a natural number n such that $\phi^n P = aQ$; in particular it implies that Q is nontorsion and $a \neq 0$.

($\Leftarrow$) We only have to consider the case when P, Q are nontorsion. Suppose that $\phi^n P = aQ$ for a nonzero integer a and a natural number n. Factorise the order of $Q \mod v$ as $m_1 m_2$, where all prime numbers dividing m_1 divide ϕ and m_2 is coprime to ϕ. Since ϕ^n is coprime to m_2 it is invertible in the group $(\mathbb{Z}/m_2\mathbb{Z})^\times$. Choose a natural number $n_v > n$ such that $n_v \equiv -a(\phi^n)^{-1} \mod m_2$ and such that m_1 divides $\phi^{n_v - n}$. Now we have

$$\phi^{n_v}(P + n_v Q) = \phi^{n_v - n}(a + \phi^n n_v)Q = 0 \mod v. \qquad \square$$

Remark 1. The assumption in Proposition 4 that no power of ϕ kills P cannot be dropped. Let P be a nonzero torsion point, $\phi^k P = 0$ for some $\phi \neq 0$ and Q be a nontorsion point. Then for every v the condition (10) is met for n_v equal to the product of k and the order of $Q \mod v$, but the assertion of the Theorem does not hold.

Remark 2. Proposition 4 with $\phi = \pm 1$ is an example of results known as *detecting linear dependence* in Mordell–Weil groups of elliptic curves over number fields addressed recently in numerous papers; we do not intend to discuss them here and refer to [Bar2] instead.

Remark 3. The following groups:

(1) $R_{F,S}^\times$, 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,

mimic the properties of Mordell–Weil groups of elliptic curves without CM we used in the proof of Theorem 3 (see, e.g., [Bar2] for details), so we can obtain similar results for them. In particular, we get identical results for S-units groups (changing the additive notation to multiplicative) and for abelian varieties. For the K-theory groups case we can repeat part of the proof and obtain the following slightly weaker:

Let F be a number field and $B(F)$ be an odd algebraic K-theory group $K_{2n+1}(F)$, $n > 0$. Let $P, Q \in B(F)$ and ϕ, ψ be rational integers. Suppose that for almost every prime v there exists a natural number n_v such that

$$\phi^{n_v} P - \psi^{n_v} Q = 0 \mod v.$$

Then there exists a natural number n and a torsion point $T \in B(F)$ of order dividing some power of $\gcd(\phi, \psi)$ such that $\phi^n P - \psi^n Q = T$. In particular if $\gcd(\phi, \psi) = 1$ or more generally if $\gcd(\phi, \psi)$ is coprime to the order of $B(F)_{\mathrm{tors}}$ then

$$\phi^n P - \psi^n Q = 0.$$

As for the proof of Proposition 4, it can be repeated in its entirety for the groups we consider thus we obtain the same result for them.

Remark 4. Consider an elliptic curve E over $\mathbb{Q}$ and denote the positive square root of the denominator of x-coordinate of a point $P \in E(\mathbb{Q})$ by D_P. For a prime number l of good reduction the condition "$P = 0 \mod l$" equals the condition "l divides D_P". Sequences D_{nP} are known under the name of *elliptic divisibility sequences*. K. Stange ([Sta]) initiated a study of *elliptic nets*, i.e., their two-parameter generalizations D_{nP+mQ}. The sequences we investigate are particular one-parameter subsequences of Stange's nets.

Remark 5. The methods we use in our proofs do not seem to work for curves with complex multiplication, even if we restrict ϕ and ψ to be rational integers. Indeed, our proofs depend on the fact that if the ring of endomorphisms equals $\mathbb{Z}$ then knowing the order of a point P we know the order of αP for any endomorphism α.

Remark 6. In the paper, "almost all primes" means "all but finitely many primes" while it could read "all but a set of density 0". However in our proofs we rely on Theorem 5.1 of [Bar1]. This theorem states "there are infinitely many primes" but its proof shows that there is a positive density set of such primes.

Acknowledgments

We drew inspiration from Prof. Schinzel's lecture on recursive sequences and congruences he has recently given in Poznań at the *Arithmetic Algebraic Geometry Seminar* organized by G. Banaszak and P. Krasoń. We would like to thank D. Blinkiewicz and G. Banaszak for their interest and helpful remarks. We are grateful to the referee for pointing out numerous deficiencies of the original manuscript.

References

[BanGK] Banaszak, Grzegorz; Gajda, Wojciech; Krasoń, Piotr. Detecting linear dependence by reduction maps. *J. Number Theory* **115**

(2005), no. 2, 322–342. MR2180505, Zbl 1089.11030, arXiv:math/0407249, doi: 10.1016/j.jnt.2005.01.008.

[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.

[Bar2] Barańczuk, Stefan. On a dynamical local-global principle in Mordell–Weil type groups. Preprint, *Expositiones Mathematicae*, 2016. doi: 10.1016/j.exmath.2016.07.001.

[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.

[Pink] Pink, Richard. On the order of the reduction of a point on an abelian variety. *Math. Ann.* **330** (2004), no. 2, 275–291. MR2089426, Zbl 1077.11046, doi: 10.1007/s00208-004-0548-8.

[Schi1] Schinzel, Andrzej. On the congruence $a^x \equiv b \pmod p$. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **8** (1960), 307–309. MR125070, Zbl 0094.25504.

[Schi2] Schinzel, Andrzej. On power residues and exponential congruences. *Acta Arith.* **27** (1975), 397–420. MR0379432, Zbl 0342.12002.

[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.

[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.

[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.

[Sta] Stange, Katherine. 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.

[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.

(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/2017/23-3.html.