COLLOQUIUM MATHEMATICUM

VOL. 137 2014 NO. 2

A REMARK ON CERTAIN SIMULTANEOUS DIVISIBILITY SEQUENCES

BY

STEFAN BARAŃCZUK and PIOTR RZONSOWSKI (Poznań)

Abstract. We investigate possible orders of reductions of a point in the Mordell–Weil groups of certain abelian varieties and in direct products of the multiplicative group of a number field. We express the result obtained in terms of divisibility sequences.

Let B be an abelian group with finite torsion subgroup and $r_v\colon B \to B_v$ be an infinite family of group homomorphisms whose targets B_v are finite abelian groups. We will use the following notation:

$P \bmod v$	$r_v(P)$ for $P \in B$
$P = Q \bmod v$	$r_v(P) = r_v(Q)$ for $P, Q \in B$
B_{tors}	the torsion subgroup of B
e	the exponent of B_{tors}
$\operatorname{ord} T$	the order of a torsion point $T \in B$
$\operatorname{ord}_v P$	the order of a point $P \bmod v$.

We impose the following assumption on the family $r_v\colon B \to B_v$:

- For every point $P \in B$ of infinite order and for almost every natural number n there exists v such that $\operatorname{ord}_v P = n$.

Theorem. *If $(P_1, \ldots, P_k) \in B \oplus \cdots \oplus B$ is a point of infinite order such that the points $P_1, \ldots, P_k$ are pairwise linearly dependent over $\mathbb{Z}$ then for every sufficiently large integer n there exists v such that* $\operatorname{ord}_v(P_1, \ldots, P_k) = en$.

Let B be the Mordell–Weil group of an elliptic curve E over a number field K. If v is a prime ideal in $\mathcal{O}_K$ of good reduction then $r_v\colon B \to B_v$ is the reduction map $E(K) \to E_v(k_v)$. In this case the assumption we have imposed holds; moreover, for all but finitely many P there exists such a prime v for each $n > 0$. This was proved by J. Silverman [3] for $K = \mathbb{Q}$ and then by J. Cheon and S. Hahn [1] for arbitrary number fields K. Thus for an abelian variety $A = E \times \cdots \times E$ we can specialize the Theorem to

2010 *Mathematics Subject Classification*: Primary 11G35; Secondary 11G05, 11G10, 14H52.

Key words and phrases: elliptic curves, reductions, divisibility sequences.

DOI: 10.4064/cm137-2-5

Corollary. *Let E be an elliptic curve over a number field K and $(P_1,\dots,P_k) \in A(E) = E(K) \times \cdots \times E(K)$ be a point of infinite order such that the points $P_1,\dots,P_k$ are pairwise linearly dependent over $\mathbb{Z}$. Denote by e the exponent of the torsion subgroup of $E(K)$. Then for every sufficiently large integer n there exists a prime v of good reduction such that* $\mathrm{ord}_v(P_1,\dots,P_k) = en$.

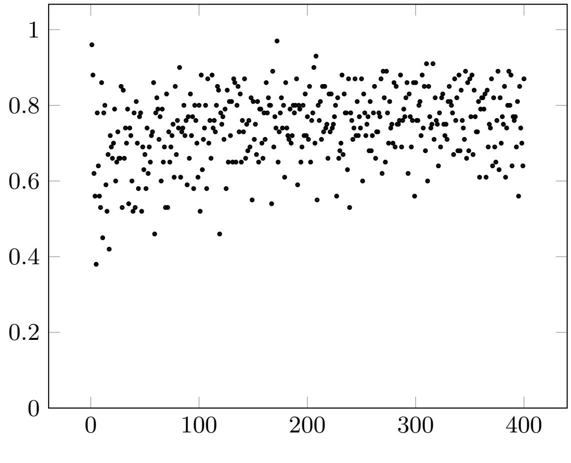
In particular, if $E(K)$ is of rank 1 and with trivial torsion subgroup then $A = E \times \cdots \times E$ is an example of an abelian variety to whose Mordell–Weil group $A(K)$ we generalize the result of Silverman and Cheon and Hahn.

Note that the factor e coming from the torsion subgroup of $E(K)$ cannot be omitted. Indeed, let E/K be a curve such that there exists a point P of infinite order and a torsion point T. Since the mod v reduction map is injective on the torsion subgroups of $E(K)$ for almost all v, the order of $(P,T) \in E \times E$ mod v is divisible by the order of T for almost all v.

Some numerical computations we performed using SAGE suggest that the assumption of the Theorem that the points $P_1,\dots,P_k$ are pairwise linearly dependent over $\mathbb{Z}$ cannot be omitted. Namely let $\mathbb{E}$ be the set of all elliptic curves $E/\mathbb{Q}$ from Cremona's list such that conductor of E is in $\{1,\dots,2031\}$, $E(\mathbb{Q})$ is torsion free and $\operatorname{rank} E/\mathbb{Q} = 2$ (note that $\#\mathbb{E} = 100$). For every $E \in \mathbb{E}$ we denote the generators of the Mordell-Weil group $E(\mathbb{Q})$ by P_E, Q_E. We investigate the function $f\colon \{2,\dots,400\} \to [0,1]$ defined by

$$f(n) = \frac{\#\{(P_E,Q_E) : \mathrm{ord}_p(P_E,Q_E) \neq n \text{ for every prime } p \text{ of good reduction}\}}{\#\mathbb{E}}$$

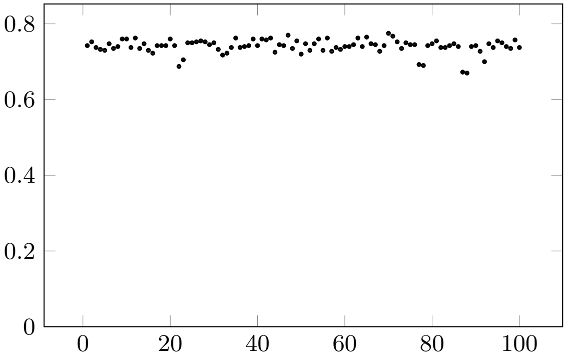
measuring for given n for how many of all the points (P_E,Q_E) the order n cannot be obtained. The arithmetic mean of f equals circa 74/100, the maximal value is 97/100 for $n = 173$, the minimal value is 38/100 for $n = 6$ and the standard deviation is slightly above 9/100.



Now let us consider the function $g\colon \mathbb{E} \to [0,1]$ given by

$$g(E) = \frac{\#\{n : \operatorname{ord}_p(P_E, Q_E) \neq n \text{ for every prime } p \text{ of good reduction}\}}{400},$$

measuring for a given point (P_E, Q_E) the percentage of orders from 2 to 401 that cannot be obtained. Here the arithmetic mean equals of course the one computed above, the maximal value is $310/400 \approx 77/100$, the minimal value is $268/400 \approx 67/100$ and the standard deviation is slightly below $2/100$.



Now notice that the second statement of the Theorem in [1] (i.e. for almost all points P for every $n > 0$ there exists a prime v such that $\operatorname{ord}_v P = n$) does not hold for abelian varieties we investigate. Indeed, let us consider a curve E/K and a nontorsion point $P \in E(K)$ such that for some prime number p and any prime v of good reduction, $\operatorname{ord}_v P \neq 1, p$ (for example, if $E/\mathbb{Q}\colon y^2 + y = x^3 + x^2 - 2x$ and $P = (0,0)$ then $2P = (3,5)$, hence for every v we have $2P \neq 0 \bmod v$). Now for every natural number a and every prime v of good reduction the order of the image of the point $(aP, P) \in E(K) \times E(K)$ under reduction modulo v is not p. Indeed, $\operatorname{ord}_v(aP, P) = \operatorname{lcm}(\operatorname{ord}_v aP, \operatorname{ord}_v P)$ but $\operatorname{ord}_v P \neq 1, p$ so $\operatorname{ord}_v(aP, P) \neq p$. However if a point P has the above-mentioned property of the second statement of the Theorem in [1] and $e = 1$ then so does any nonzero point of the form $(b_1 P, \ldots, b_k P)$ (substitute $N = 1$ in the proof).

Note that elliptic curves are examples of simple abelian varieties, and the counterexamples we provide in this paper are only valid for nonsimple abelian varieties, hence the generalization of the result of Silverman, Cheon and Hahn to simple abelian varieties could still hold. However the proof would certainly require methods different form those we use in this article.

In the case of $E/\mathbb{Q}$ the problem we consider can be reformulated in terms of primitive divisors in elliptic divisibility sequences (see e.g. [4]). Namely if E is an elliptic curve defined over $\mathbb{Q}$ given by a Weierstrass equation with integer coefficients then for every point $P \in E(\mathbb{Q})$ of infinite order and for every natural number n we have

$$nP = \left(\frac{A_n}{D_n^2}, \frac{C_n}{D_n^3}\right)$$

where A_n, C_n, D_n are integers such that A_n, D_n are co-prime. The sequence $(D_n)_{n\geq 1}$ is called an *elliptic divisibility sequence*, and a prime number p is called a *primitive divisor* of D_n if $p \mid D_n$ and $p \nmid D_i$ for all $1 \leq i < n$. Note that for a prime number p of good reduction, $nP = 0 \bmod p$ if and only if $p \mid D_n$, hence $\operatorname{ord}_p P = n$ if and only if p is a primitive divisor of D_n. Thus we have

Corollary. *Let E be an elliptic curve defined over $\mathbb{Q}$ such that the group $E(\mathbb{Q})$ is torsion-free. Let $P_1, \ldots, P_k \in E(\mathbb{Q})$ be nonzero points pairwise linearly dependent over $\mathbb{Z}$. Let $(D_{i,n})_{n\geq 1}$ be the elliptic divisibility sequence defined by P_i, and set $\delta_n := (D_{1,n}, \ldots, D_{k,n})$ for $n \geq 1$. Then for every sufficiently large integer n there exists a primitive divisor of δ_n, i.e. a prime number p such that p divides $D_{i,n}$ for each i, but for every natural number $m < n$ there exist i such that p does not divide $D_{i,m}$.*

The result of Silverman, Cheon and Hahn has a predecessor for the multiplicative group of a number field, proved by A. Schinzel: Theorem 1 in [2] states that if for a number field K and a finite set S of its primes we let $B = \mathcal{O}_{K,S}$ and if v's are primes outside S then the assumption we imposed on the family $r_v\colon B \to B_v$ is fulfilled. Thus we get the following specialization of the Theorem:

Corollary. *Let K be a number field and $(x_1, \ldots, x_k) \in K^* \times \cdots \times K^*$ be a point such that the numbers $x_1, \ldots, x_k$ are pairwise multiplicatively dependent and the subgroup of K^* generated by them does not contain a nontrivial root of unity. Then for every sufficiently large integer n there exists a prime v of K such that* $\operatorname{ord}_v(x_1, \ldots, x_k) = n$.

Proof of Theorem. Let us consider the subgroup of B generated by $eP_1, \ldots, eP_k$. By the definition of e this subgroup is free abelian and by the assumption on pairwise linear dependence of the points $P_1, \ldots, P_k$ it is of rank 1, hence it has a generator, say P. Write $eP_i = b_iP$ for $i = 1, \ldots, k$. Now

$$\begin{aligned}
\frac{\operatorname{ord}_v(P_1, \ldots, P_k)}{\gcd(e, \operatorname{ord}_v(P_1, \ldots, P_k))} &= \operatorname{ord}_v(eP_1, \ldots, eP_k) \\
&= \operatorname{ord}_v(b_1P, \ldots, b_kP) = \operatorname{lcm}\left(\frac{\operatorname{ord}_v P}{\gcd(b_1, \operatorname{ord}_v P)}, \ldots, \frac{\operatorname{ord}_v P}{\gcd(b_k, \operatorname{ord}_v P)}\right) \\
&= \frac{\operatorname{ord}_v P}{\gcd(\gcd(b_1, \operatorname{ord}_v P), \ldots, \gcd(b_k, \operatorname{ord}_v P))} = \frac{\operatorname{ord}_v P}{\gcd(b_1, \ldots, b_k, \operatorname{ord}_v P)}.
\end{aligned}$$

Substituting $en := \operatorname{ord}_v(P_1, \dots, P_k)$, $m := \gcd(b_1, \dots, b_k)$, $x := \operatorname{ord}_v P$ in the above equation we get the Diophantine equation

$$x = n \gcd(m, x)$$

with given m, n. This equation has a solution greater than or equal to n, e.g. $x = nm$. By [1] there exists a natural number N such that for every $x \geq N$ there exists a prime v such that $\operatorname{ord}_v P = x$. ■

Acknowledgments. The authors are grateful to Grzegorz Banaszak for his careful reading and corrections to preliminary versions of the paper, and to the referee for suggesting the direction of numerical computations as well as for remarks which led to essential clarification of arguments.

REFERENCES

[1] 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

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

[3] J. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory 30 (1988), 226–237.

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

Stefan Barańczuk, Piotr Rzonsowski
Faculty of Mathematics and Computer Science
Adam Mickiewicz University
Umultowska 87
61-614 Poznań, Poland
E-mail: stefbar@amu.edu.pl
rzonsol@amu.edu.pl

Received 13 February 2014;
revised 18 June 2014 (6161)