IMRN International Mathematics Research Notices
2005, No. 4

Curves in Abelian Varieties over Finite Fields

Fedor Bogomolov and Yuri Tschinkel

1 Introduction

Let k be an algebraic closure of a finite field and let C be a curve over k. Assume that C is embedded into an abelian algebraic group G over k, with the group operation written additively. Let c be a k-rational point of C. In this note, we study the distribution of orbits $\{m\cdot c\}_{m\in\mathbb{N}}$ in the set $G(k)$ of k-rational points of G. One of our main results is the following theorem.

Theorem 1.1. Let C be a smooth projective curve over k of genus $g = g(C) \geq 2$. Let A be an abelian variety containing C. Assume that C generates A, that is, the Jacobian J of C admits a geometrically surjective map onto A. For any $\ell \in \mathbb{N}$,

$$A(k) = \bigcup_{m=1 \bmod \ell} m \cdot C(k), \tag{1.1}$$

that is, for every $a \in A(k)$ and $\ell \in \mathbb{N}$, there exist $m \in \mathbb{N}$ and $c \in C(k)$ such that $a = m \cdot c$ and $m = 1 \bmod \ell$.

Moreover, let $A(k)\{\ell\} \subset A(k)$ be the ℓ-primary part of $A(k)$ and let S be any finite set of primes. Then, there exists an infinite set of primes Π, containing S and of positive density, such that the natural composition

$$C(k) \longrightarrow A(k) \longrightarrow \bigoplus_{\ell\in\Pi} A(k)\{\ell\} \tag{1.2}$$

is surjective. □

Received 13 October 2004.
Communicated by Enrico Bombieri.

2 Curves and their Jacobians

Throughout, C is a smooth irreducible projective curve of genus $g = g(C) \geq 2$ and J is its Jacobian. Assume that C is defined over $\mathbb{F}_q \subset k$ with a point $c_0 \in C(\mathbb{F}_q)$ which we use to identify the degree n Jacobian $J^{(n)}$ with J and to embed C in J. Consider the maps

$$\begin{aligned} C^n &\xrightarrow{\phi_n} \mathrm{Sym}^{(n)}(C) \xrightarrow{\varphi_n} J^{(n)} = J, \\ c = (c_1, \dots, c_n) &\longrightarrow (c_1 + \cdots + c_n) \longrightarrow [c]. \end{aligned} \tag{2.1}$$

Here, $(c_1 + \cdots + c_n)$ denotes the zero-cycle and ϕ_n is a finite cover of degree $n!$. For $n \geq 2g+1$, the map φ_n is a $\mathbb{P}^{n-g}$-bundle and the map $C^n \to J^{(n)}$ is surjective with geometrically irreducible fibers (see, e.g., [3, Corollary 9.1.4]). We need the following.

Lemma 2.1. For every point $x \in J(\mathbb{F}_q)$ and every $n \geq 2g+1$, there exist a finite extension $k'/\mathbb{F}_q$ and a point $y \in \mathbb{P}_x(k') = \varphi_n^{-1}(x)(k')$ such that the degree n zero-cycle $c_1 + \cdots + c_n$ on C corresponding to y is k'-irreducible. □

Proof. This follows from a version of an equidistribution theorem of Deligne as in [3, Theorem 9.4.4]. ■

Proof of Theorem 1.1. We may assume that $A = J$. Let $a \in A(k)$ be a point. It is defined over some finite field $\mathbb{F}_q$ (with $c_0 \in C(\mathbb{F}_q)$). Fix a finite extension $k'/\mathbb{F}_q$ as in Lemma 2.1 and let N be the order of $A(k')$.

Choose a finite extension k''/k', of degree $n \geq 2g+1$, such that n and the order of the group $A(k'')/A(k')$ are coprime to $N\ell$. By Lemma 2.1, there exists a k'-irreducible cycle $c_1 + \cdots + c_n$ mapped to a. The orders of $c_1 - c_j$, for $j = 1, \dots, n$, are all equal and are coprime to $N\ell$ (note that all c_j have the same order and the same image under the projection $A(k'') \to A(k')$). Then, there is an $m \in \mathbb{N}$, $m = 1 \bmod N\ell$, such that

$$0 = m\left(nc_1 - \sum_{j=1}^{n} c_j\right) = mnc_1 - ma = mnc_1 - a. \tag{2.2}$$

We turn to the second claim. Fix a prime p such that $p > (2g)!$ and $p \nmid |\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|$ for all $\ell \in \Pi$. Let Π be the set of *all* primes ℓ such that $p \nmid |\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|$. We have $\ell \in \Pi$ if $\ell^i \neq 1 \bmod p$ for all $i = 1, \dots, 2g$. In particular, Π has positive density.

The Galois group $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) = \widehat{\mathbb{Z}}$ contains $\mathbb{Z}_p$ as a closed subgroup. Put $k' := \bar{\mathbb{F}}_q^{\mathbb{Z}_p}$. For $\ell \in \Pi$, there exist no nontrivial continuous homomorphisms of $\mathbb{Z}_p$ into $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$; and the Galois action of $\mathbb{Z}_p$ on $A(k)\{\ell\}$ is trivial. In particular,

$$A(k') \supset \prod_{\ell \in \Pi} A(k)\{\ell\}. \tag{2.3}$$

Now we apply the above argument. Given a point $a \in \prod_{\ell\in\Pi} A(k)\{\ell\}$, we find points $c_1, \dots, c_{p^r} \in C(k)$, defined over an extension of k' of degree p^r, and such that the cycle $c_1 + \dots + c_{p^r}$ is k'-irreducible and equal to a. By construction, p and the orders of $c_i - c_j$ are coprime to every $\ell \in \Pi$ for all $i \neq j$. We conclude that the natural map

$$C(k) \longrightarrow \prod_{\ell\in\Pi} A(k)\{\ell\} \tag{2.4}$$

is surjective. ■

Remark 2.2. This shows that, over finite fields, all algebraic points on A are obtained from a 1-dimensional object by multiplication by a scalar.

Remark 2.3. The fact that

$$C(k) \longrightarrow \bigoplus\nolimits_{\ell\in\Pi} A(k)\{\ell\} \tag{2.5}$$

is surjective was established for Π consisting of one prime in [1]; for a generalization to finite Π, see [6].

3 Semi-abelian varieties

Let C be an irreducible curve over k and $C_\circ \subset C$ a Zariski open subset embedded into a semi-abelian group T, a torus fibration over the Jacobian $J = J_C$. Assume that $C_\circ$ generates T, that is, every point in $T(k)$ can be written as a product of points in $C_\circ(k)$.

Theorem 3.1. For every $t \in T(k)$, there exist a point $c \in C_\circ(k)$ and an $m \in \mathbb{N}$ such that $t = c^m$. □

Proof. We follow the arguments of Section 2. For $n \gg 0$, the map

$$\begin{aligned} C_\circ^n &\longrightarrow J_{C_\circ}, \\ (c_1, \dots, c_n) &\longmapsto \prod_{j=1}^{n} c_j \end{aligned} \tag{3.1}$$

to the generalised Jacobian has geometrically irreducible fibers. In our case, $C_\circ$ is a complement to a finite number of points in C and the generalised Jacobian $J_{C_\circ}$ is a semi-abelian variety fibered over the Jacobian $J = J_C$ with a torus T_0 as a fiber.

In particular, if $\mathbb{F}_q \subset k$ is sufficiently large (with $C_\circ(\mathbb{F}_q) \neq \varnothing$), then, for some finite extension $k'/\mathbb{F}_q$ and $t \in J_{C_\circ}(\mathbb{F}_q)$, there exist $c_1, \dots, c_n \in C_\circ(k'')$, where k''/k' is the unique extension of k' of degree n, such that the Galois group $\mathrm{Gal}(k''/k')$ acts transitively on the set $\{c_1, \dots, c_n\}$ and $t = \prod_{j=1}^{n} c_j$. The Galois group $\mathrm{Gal}(k''/k')$ is generated by the Frobenius element Fr so that

$$t = \prod_{j=0}^{n-1} \mathrm{Fr}^j(c), \tag{3.2}$$

where $c := c_1$.

Every k-point in $J_{C_\circ}$ is torsion. Let $x \in J_{C_\circ}[N]$ and assume that x is defined over a finite field k'. Consider the extension k''/k', of degree $n > 2g(C_\circ) + 1$, coprime to $N\ell$, and such that the order of $J_{C_\circ}(k'')/J_{C_\circ}(k')$ is coprime to $N\ell$. It suffices to take k'' to be disjoint from the field defined by the points of the $N\ell$-primary subgroup of $J_{C_\circ}$. Then, the result for $J_{C_\circ}$ follows as in Theorem 1.1. Since $J_{C_\circ}$ surjects onto T, the result holds for T. ■

Remark 3.2. Note that the action of the Frobenius Fr on $\mathbb{G}_m^d(k)$ is given by the scalar endomorphism $z \mapsto z^q$, where $q = \#k'$. It follows that if $T = \mathbb{G}_m^d$ is generated by $C_\circ$, then every $t \in T(k)$ can be represented as

$$t = \prod_{j=0}^{n-1} c^{q^j} = c^{(q^n-1)/(q-1)} \tag{3.3}$$

for some $c \in C_\circ(k)$.

4 Applications

In this section, we discuss applications of Theorem 1.1.

Corollary 4.1. Let A be the Jacobian of a hyperelliptic curve C of genus $g \geq 2$ over k, embedded so that the standard involution ι of A induces the hyperelliptic involution of C. Let $Y = A/\iota$ and $Y^\circ \subset Y$ be the smooth locus of Y. Then, every point $y \in Y^\circ(k)$ lies on a rational curve. □

Proof. Let $a \in A(k)$ be a point in the preimage of $y \in Y^\circ(k)$. By Theorem 1.1, there exists an $m \in \mathbb{N}$ such that $mc = a$. The endomorphism "multiplication by m" commutes with ι. Since $a \in m \cdot C(k)$, we have $s \in R(k)$, where $R = m \cdot C/\iota \subset Y$ is a rational curve. ■

Remark 4.2. This corollary was proved in [2] using more complicated endomorphisms of A. It leads to the question whether or not *every* abelian variety over $k = \bar{\mathbb{F}}_p$ is generated by a hyperelliptic curve. This property fails over large fields [4, 5].

Corollary 4.3. Let C be a curve of genus $g \geq 2$ over a number field K. Assume that $C(K) \neq \varnothing$ and choose a point $c_0 \in C(K)$ to embed C into its Jacobian A. Choose a model of A over the integers $\mathcal{O}_K$ and let $S \subset \mathrm{Spec}(\mathcal{O}_K)$ be a finite set of non-Archimedean places of good or semi-abelian reduction for A. Assume that C has irreducible reduction C_ν, $\nu \in S$ (in particular, C_ν, $\nu \in S$, generates the reduction A_ν). Let k_ν be the residue fields and fix $a_\nu \in A(k_\nu)$, $\nu \in S$. Then, there exist a finite extension L/K, a point $c \in C(L)$, and an integer $m \in \mathbb{N}$ such that for all $\nu \in S$ and all places $w \mid \nu$, the reduction $(m \cdot c)_w = a_\nu \in A(k_\nu) \subset A(l_w)$, where l_w is the residue field at w. □

Proof. We follow the argument in the proof of Theorem 1.1. Denote by n_ν the orders of a_ν, for $\nu \in S$ and let n be the least common multiple of n_ν. Replacing K by a finite extension and S by the set of all places lying over it, we may assume that the n-torsion of A is defined over K. There exist extensions $k_{\nu'}/k_\nu$ for all $\nu \in S$, points $c_{\nu'} \in C(k_{\nu'}) \subset A(k_{\nu'})$, and $m_{\nu'} = 1 \bmod n$, such that $m_{\nu'} c_{\nu'} = a_\nu$. Thus, there is an $m \in \mathbb{N}$ such that

$$m c_{\nu'} = a_\nu. \tag{4.1}$$

There exist an extension L/K and a point $c \in C(L)$ such that for all $\nu \in S$ and all w over ν, the corresponding residue field l_w contains $k_{\nu'}$ and the reduction of c modulo w coincides with $c_{\nu'}$. Using the Galois action on (4.1), we find that mc reduces to a_ν for all w. ■

Over $\bar{\mathbb{Q}}$, it is not true that $A(\bar{\mathbb{Q}}) = \bigcup_{r \in \mathbb{Q}} r \cdot C(\bar{\mathbb{Q}})$. Indeed, by the results of Faltings and Raynaud, the intersection of $C(\bar{\mathbb{Q}})$ with every finitely generated $\mathbb{Q}$-subspace in $A(\bar{\mathbb{Q}})$ is finite.

Consider the map

$$C(\bar{\mathbb{Q}}) \longrightarrow \mathbb{P}\big(A(\bar{\mathbb{Q}})/A(\bar{\mathbb{Q}})_{\mathrm{tors}} \otimes \mathbb{R}\big) \tag{4.2}$$

(defined modulo translation by a point). It would be interesting to analyze the discreteness and the metric characteristics of the image of $C(\bar{\mathbb{Q}})$, combining the classical theorem of Mumford with the results of [7].

Acknowledgments

We are grateful to Ching-Li Chai, Nick Katz, and Bjorn Poonen for their interest and useful remarks. The first author was partially supported by the NSF.

References

[1] G. W. Anderson and R. Indik, *On primes of degree one in function fields*, Proc. Amer. Math. Soc. **94** (1985), no. 1, 31–32.

[2] F. Bogomolov and Y. Tschinkel, *Rational curves and points on* K3 *surfaces*, preprint, 2003, http://arXiv.org/abs/math.AG/0310254.

[3] N. M. Katz, *Twisted* L*-Functions and Monodromy*, Annals of Mathematics Studies, vol. 150, Princeton University Press, New Jersey, 2002.

[4] F. Oort and J. de Jong, *Hyperelliptic curves in abelian varieties*, J. Math. Sci. **82** (1997), no. 1, 3211–3219.

[5] G. P. Pirola, *Curves on generic Kummer varieties*, Duke Math. J. **59** (1989), no. 3, 701–708.

[6] F. Pop and M. Saïdi, *On the specialization homomorphism of fundamental groups of curves in positive characteristic*, Galois Groups and Fundamental Groups (L. Schneps, ed.), Math. Sci. Res. Inst. Publ., vol. 41, Cambridge University Press, Cambridge, 2003, pp. 107–118.

[7] L. Szpiro, E. Ullmo, and S. Zhang, *Équirépartition des petits points* [*Uniform distribution of small points*], Invent. Math. **127** (1997), no. 2, 337–347 (French).

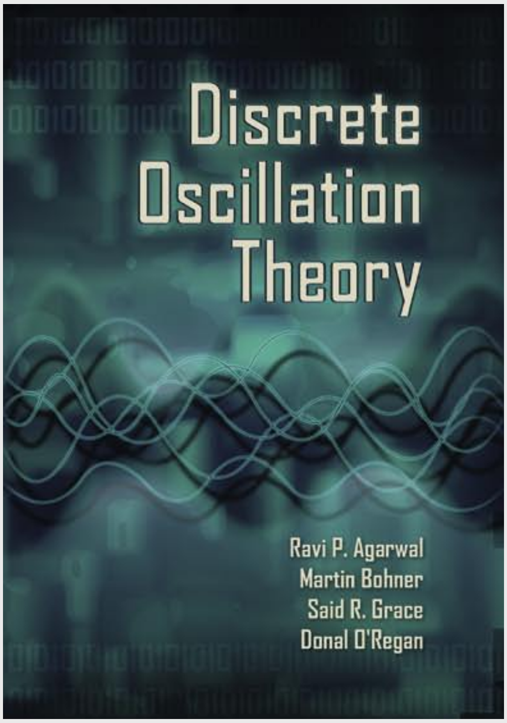
Fedor Bogomolov: Courant Institute of Mathematical Sciences, New York University, 251 Mercer Street, New York, NY 10012, USA
E-mail address: bogomolo@cims.nyu.edu

Yuri Tschinkel: Mathematisches Institut, Georg-August-Universität Göttingen, Bunsenstraße 3-5, 37073 Göttingen, Germany
E-mail address: yuri@uni-math.gwdg.de

CMIA Book Series, Volume 1, ISBN: 977-5945-19-4

DISCRETE OSCILLATION THEORY

Ravi P. Agarwal, Martin Bohner, Said R. Grace, and Donal O'Regan



This book is devoted to a rapidly developing branch of the qualitative theory of difference equations with or without delays. It presents the theory of oscillation of difference equations, exhibiting classical as well as very recent results in that area. While there are several books on difference equations and also on oscillation theory for ordinary differential equations, there is until now no book devoted solely to oscillation theory for difference equations. This book is filling the gap, and it can easily be used as an encyclopedia and reference tool for discrete oscillation theory.

In nine chapters, the book covers a wide range of subjects, including oscillation theory for second-order linear difference equations, systems of difference equations, half-linear difference equations, nonlinear difference equations, neutral difference equations, delay difference equations, and differential equations with piecewise constant arguments. This book summarizes almost 300 recent research papers and hence covers all aspects of discrete oscillation theory that have been discussed in recent journal articles. The presented theory is illustrated with 121 examples throughout the book. Each chapter concludes with a section that is devoted to notes and bibliographical and historical remarks.

The book is addressed to a wide audience of specialists such as mathematicians, engineers, biologists, and physicists. Besides serving as a reference tool for researchers in difference equations, this book can also be easily used as a textbook for undergraduate or graduate classes. It is written at a level easy to understand for college students who have had courses in calculus.