CURVES IN ABELIAN VARIETIES OVER FINITE FIELDS

by

Fedor Bogomolov and Yuri Tschinkel

Abstract. — We study the distribution of algebraic points on curves in abelian varieties over finite fields.

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:

**Theorem 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 \( A \), i.e., the Jacobian \( J \) of \( C \) admits a geometrically surjective map onto \( A \). For any \( \ell \in \mathbb{N} \) we have

\[
A(k) = \bigcup_{m=1 \mod \ell} m \cdot C(k),
\]

i.e., 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 \( m = 1 \mod \ell \).

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

\[
C(k) \to A(k) \to \bigoplus_{\ell \in \Pi} A(k) \{\ell\}.
\]

is surjective.
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.

2. Curves and their Jacobians

Throughout, \( C \) is a smooth irreducible projective curve of genus \( g = g(C) \geq 2 \) and \( J \) 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

\[
\begin{align*}
C^n & \xrightarrow{\phi_n} \text{Sym}^{(n)}(C) \xrightarrow{\varphi_n} J^{(n)} = J, \\
(c_1, \ldots, c_n) & \mapsto (c_1 + \cdots + c_n) \mapsto [c],
\end{align*}
\]

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

**Lemma 2.** — 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 7.** — 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 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 there exists a \( k' \)-irreducible cycle \( c_1 + \cdots + c_n \) mapped to \( a \). The orders of \( c_1 - c_j \), for \( j = 1, \ldots, n \), 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.
Then there is an \( m \in \mathbb{N} \), \( m = 1 \mod N\ell \), such that
\[
0 = m(nc_1 - \sum_{j=1}^{n} c_j) = mnc_1 - ma = mnc_1 - a.
\]

We turn to the second claim. Fix a prime \( p > (2g)! \) and so that \( p \nmid |\text{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})| \), for all \( \ell \in S \). Let \( \Pi \) be the set of all primes \( \ell \) such that \( p \nmid |\text{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})| \). We have \( \ell \in \Pi \) if \( \ell^i \neq 1 \mod p \), for all \( i = 1, \ldots, 2g \).

In particular, \( \Pi \) has positive density.

The Galois group \( \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \hat{\mathbb{Z}} \) contains \( \mathbb{Z}_p \) as a closed subgroup.

Put \( k' := \mathbb{F}_q^{\mathbb{Z}_p} \). For \( \ell \in \Pi \), there exist no non-trivial continuous homomorphisms of \( \mathbb{Z}_p \) into \( \text{GL}_{2g}(\mathbb{Z}_\ell) \); and the Galois-action of \( \mathbb{Z}_p \) on \( A(k') \) is trivial. In particular,
\[
A(k') \supset \prod_{\ell \in \Pi} A(k)\{\ell\}.
\]

Now we apply the argument above: given a point \( a \in \prod_{\ell \in \Pi} A(k)\{\ell\} \) we find points \( c_1, \ldots, c_{p^r} \in C(k) \), defined over an extension of \( k' \) of degree \( p^r \), and such that the cycle \( c_1 + \cdots + c_{p^r} \) 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
\[
C(k) \to \prod_{\ell \in \Pi} A(k)\{\ell\}
\]
is surjective.

**Remark 3.** — This shows that, over finite fields, all algebraic points on \( A \) are obtained from a 1-dimensional object by multiplication by a scalar.

**Remark 4.** — The fact that
\[
C(k) \to \bigoplus_{\ell \in \Pi} A(k)\{\ell\}
\]
is surjective was established for \( \Pi \) consisting of one prime in [1]; for a generalization to finite \( \Pi \) see [6].
3. Semi-abelian varieties

Let \( C \) be an irreducible curve over \( k \) and \( C_0 \subset C \) a Zariski open subset embedded into a semi-abelian group \( T \), a torus fibration over the Jacobian \( J = J_C \). Assume that \( C_0 \) generates \( T \), i.e., every point in \( T(k) \) can be written as a product of points in \( C_0(k) \).

**Theorem 5.** — For every \( t \in T(k) \) there exist a point \( c \in C_0(k) \) 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
\[
C^n_n \rightarrow J_{C_0}
\]
\[
(c_1, \ldots, c_n) \mapsto \prod_{j=1}^n c_j
\]
to the generalised Jacobian has geometrically irreducible fibers. In our case \( C_0 \) is a complement to a finite number of points in \( C \) and the generalised Jacobian \( J_{C_0} \) 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 \( C_0(\mathbb{F}_q) \neq \emptyset \)) then, for some finite extension \( k'/\mathbb{F}_q \) and \( t \in J_{C_0}(\mathbb{F}_q) \) there exist \( c_1, \ldots, c_n \in C_0(k'^n) \), where \( k'^n/k' \) is the unique extension of \( k' \) of degree \( n \), such that the Galois group \( \text{Gal}(k'^n/k') \) acts transitively on the set \( \{ c_1, \ldots, c_n \} \) and \( t = \prod_{j=1}^n c_j \). The Galois group \( \text{Gal}(k'^n/k') \) is generated by the Frobenius element \( \text{Fr} \) so that
\[
t = \prod_{j=0}^{n-1} \text{Fr}^j(c),
\]
where \( c := c_1 \).

Every \( k \)-point in \( J_{C_0} \) is torsion. Let \( x \in J_{C_0}[N] \) and assume that \( x \) is defined over a finite field \( k' \). Consider the extension \( k''/k' \), of degree \( n > 2g(C_0)+1 \), coprime to \( N \ell \), and such that the order of \( J_{C_0}(k'')/J_{C_0}(k') \) 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 \( J_{C_0} \). Then the result for \( J_{C_0} \) follows as in Theorem 1. Since \( J_{C_0} \) surjects onto \( T \), the result holds for \( T \).

**Remark 6.** — Note that the action of the Frobenius \( \text{Fr} \) on \( \mathbb{G}_{m, k}^d(k) \) is given by the scalar endomorphism \( z \mapsto z^q \), where \( q = \#k' \). It follows...
that if \( T = G_m^d \) is generated by \( C_0 \) then every \( t \in T(k) \) can be represented as
\[
t = \prod_{j=0}^{n-1} c q^j = c^{(q^n-1)/(q-1)}.
\]
for some \( c \in C_0(k) \).

4. Applications

In this section we discuss applications of Theorem 1.

**Corollary 7.** — Let \( A \) be the Jacobian of a hyperelliptic curve \( C \) of genus \( g \geq 2 \) over \( k \), embedded so that the standard involution \( \iota \) of \( A \) induces the hyperelliptic involution of \( C \). Let \( Y = A/\iota \) and \( Y^o \subset Y \) be the smooth locus of \( Y \). Then every point \( y \in Y^o(k) \) lies on a rational curve.

**Proof.** — Let \( a \in A(k) \) be a point in the preimage of \( y \in Y^o(k) \). By Theorem 1, there exists an \( m \in \mathbb{N} \) such that \( mc = a \). The endomorphism “multiplication by \( m \)” commutes with \( \iota \). Since \( a \in m \cdot C(k) \) we have \( y \in R(k), \) where \( R = m \cdot C/\iota \subset Y \) is a rational curve. \( \square \)

**Remark 8.** — This corollary was proved in \([2]\) using more complicated endomorphisms of \( A \). It leads to the question whether or not every abelian variety over \( k = \overline{\mathbb{F}}_p \) is generated by a hyperelliptic curve. This property fails over large fields \([4], [5]\).

**Corollary 9.** — Let \( C \) be a curve of genus \( g \geq 2 \) over a number field \( K \). Assume that \( C(K) \neq \emptyset \) 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 \( S \subset \text{Spec}(\mathcal{O}_K) \) be a finite set of nonarchimedean places of good or semi-abelian reduction for \( A \). Assume that \( C \) has irreducible reduction \( C_v, v \in S \) (in particular \( C_v, v \in S \), generates the reduction \( A_v \)). Let \( k_v \) be the residue fields and fix \( a_v \in A(k_v), v \in S \). 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 \( v \in S \) and all all places \( w | v \), the reduction \( (m \cdot c)_w = a_v \in A(k_v) \subset A(l_w) \), where \( l_w \) is the residue field at \( w \).
Proof. — We follow the argument in the proof of Theorem 1. Denote by $n_v$ the orders of $a_v$, for $v \in S$ and let $n$ be the least common multiple of $n_v$. Replacing $K$ be 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 $k_v'/k_v$, for all $v \in S$, points $c_v' \in C(k_v') \subset A(k_v')$ and $m_v' = 1 \mod n$, such that $m_v'c_v' = a_v$. Thus there is an $m \in \mathbb{N}$ such that

$$m v' = a_v.$$  

(4.1)

There exist an extension $L/K$ and a point $c \in C(L)$ such that for all $v \in S$ and all $w$ over $v$, the corresponding residue field $l_w$ contains $k_v'$ and the reduction of $c$ modulo $w$ coincides with $c_v'$. Using the Galois action on Equation (4.1), we find that $mc$ reduces to $a_v$, for all $w$.

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

Consider the map

$$C(\overline{\mathbb{Q}}) \to \mathbb{P}(A(\overline{\mathbb{Q}})/A(\overline{\mathbb{Q}})_{\text{tors}} \otimes \mathbb{R})$$

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

References

[1] G. W. Anderson and R. Indik – “On primes of degree one in function fields”, Proc. Amer. Math. Soc. 94 (1985), no. 1, p. 31–32.
[2] F. Bogomolov and Y. Tschinkel – “Rational curves and points on K3 surfaces”, math.AG/0310254.
[3] N. M. Katz – Twisted $L$-functions and monodromy, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, NJ, 2002.
[4] F. Oort and J. de Jong – “Hyperelliptic curves in abelian varieties”, J. Math. Sci. 82 (1996), no. 1, p. 3211–3219, Algebraic geometry, 5.
[5] G. P. Pirola – “Curves on generic Kummer varieties”, Duke Math. J. 59 (1989), no. 3, p. 701–708.
F. Pop and M. Saidi – “On the specialization homomorphism of fundamental groups of curves in positive characteristic”, Galois groups and fundamental groups (L. Schneps, ed.), MSRI Publications, vol. 41, Cambridge Univ. Press, 2003, p. 107–118.

L. Szpiro, E. Ullmo and S. Zhang – “Équirépartition des petits points”, Invent. Math. 127 (1997), no. 2, p. 337–347.