

Rank of Elliptic Curves over Almost Separably Closed Fields

by

MICHAEL LARSEN*

Department of Mathematics, Indiana University

Bloomington, IN 47405, USA

`larsen@math.indiana.edu`

Abstract. Let E be an elliptic curve over a finitely generated infinite field K . Let K^s denote a separable closure of K , σ an element of the Galois group $G_K = \text{Gal}(K^s/K)$, and $K^s(\sigma)$ the invariant subfield of K^s . We prove that if the characteristic of K is not 2 and σ belongs to a suitable open subgroup of G_K , then $E(K^s(\sigma))$ has infinite rank.

In [2], G. Frey and M. Jarden considered the rank of abelian varieties over fields which are almost separably closed. Specifically, let K denote a field of finite type, K^s a separable closure of K , and $G_K = \text{Gal}(K^s/K)$. For $\sigma_1, \dots, \sigma_n$ a sequence of elements of G_K , let $K^s(\sigma_1, \dots, \sigma_n)$ denote the fixed field of the σ_i . According to [2], if A is an abelian variety over K , there is a subset of G_K^n of measure 1 such that for every n -tuple belonging to the subset, $A(K^s(\sigma_1, \dots, \sigma_n))$ has infinite rank.

QUESTION 1: *Is it true that for every choice of K , A , n , and σ_i ,*

$$\dim A(K^s(\sigma_1, \dots, \sigma_n)) \otimes \mathbb{Q} = \infty?$$

This paper is intended to provide some evidence for the author's suspicion that the answer to the above question is positive, at least when A is an elliptic curve. We mainly discuss the simplest case, $\dim A = n = 1$. It should, perhaps, be remarked that it is known [3] that the torsion of $A(K^s(\sigma_1, \dots, \sigma_n))$ need not be infinite. Of course, this is a rather different kind of problem in that the Galois module $A(K^s)_{\text{tor}}$ is finite dimensional, whereas $A(K^s) \otimes \mathbb{Q}$ is infinite dimensional.

* Partially supported by the Sloan Foundation and by NSF Grant DMS 97-27553.
AMS Classification 11G05

LEMMA 2: *Every elliptic curve E over a field K of characteristic not equal to 2 has an affine open subvariety of the form $y^2 = x^3 + a_2x^2 + a_4x + a_6$. If $\lambda_1, \lambda_2, \lambda_3$ are the roots of the cubic on the right hand side, two elliptic curves are K^s -isomorphic whenever the cross ratios of $\lambda_1, \lambda_2, \lambda_3, \infty$, taken in suitable order, coincide.*

Proof: For the first claim, see [1] (3.1). For the second, note that E is the unique double cover of \mathbb{P}^1 ramified over the points λ_i and ∞ and not elsewhere. Thus E is determined up to isomorphism by the set $\{\lambda_1, \lambda_2, \lambda_3, \infty\}$. The K^s -automorphism group of \mathbb{P}^1 acts transitively on ordered quadruples $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ with fixed cross ratio

$$\frac{(\lambda_3 - \lambda_1)(\lambda_4 - \lambda_2)}{(\lambda_4 - \lambda_1)(\lambda_3 - \lambda_2)}.$$

□

PROPOSITION 3: *If K is a field of characteristic not equal to 2 and E is an elliptic curve over K , there exist elements $a, b, c, d, e, f \in K^s$ such that the three curves*

$$\begin{aligned} (*) \quad & y^2 = (x - a)(x - b)(x - c)(x - d), \\ & y^2 = (x - c)(x - d)(x - e)(x - f), \\ & y^2 = (x - e)(x - f)(x - a)(x - b) \end{aligned}$$

are all K^s -isomorphic to affine open subvarieties of E .

Proof: If the characteristic of K is not 3, we define ω to be a non-trivial cube root of 1. For parameters p and q to be determined, we set

$$a = p, b = q, c = \omega p, d = \omega q, e = \omega^2 p, f = \omega^2 q.$$

It is clear that the cross ratios of the ordered quadruples (a, b, c, d) , (c, d, e, f) , and (e, f, a, b) are the same. It remains to show that any given value λ can be achieved as the common cross ratio for appropriate values of p and q . For fixed $p \neq 0$, the cross ratio is a rational function with linear numerator and quadratic denominator. Such a function maps $K^s \cup \{\infty\}$ onto itself.

For characteristic 3, we set

$$a = p, b = q, c = p + 1, d = q + 1, e = p + 2 = p - 1, f = q + 2 = q - 1.$$

Here the numerator of the cross ratio is a constant and the denominator is quadratic in $p - q$, so again every value in $K^s \cup \{\infty\}$ is achieved. □

LEMMA 4: *Let K be an infinite field of finite type and $P_1(x), P_2(x), \dots, P_k(x)$ a sequence of polynomials in $K[x]$ each of which has a zero of odd multiplicity. If L/K is a finite separable extension of K , then there exists $a \in K$ such that $P_i(a)$ is not a perfect square in L for $i = 1, 2, \dots, k$.*

Proof: As the $P_i(x)$ have roots of odd multiplicity, the two variable polynomials $y^2 - P_i(x)$ are irreducible over L . By [4] Ch. 9 Prop. 3.3, the set of $a \in L$ such that $\sqrt{P_i(a)} \notin L$ for all i contains a Hilbert set of K and is therefore infinite by [4] Ch. 9 Th. 4.2.

□

PROPOSITION 5: *If K is a field of finite type of characteristic not equal to 2 and E is an elliptic curve over K , then the set*

$$\bigcup_{[L:K]=2} E(L)_{\text{tor}}$$

of all torsion points of E defined over quadratic extensions of K is finite.

Proof: Let R denote the subring of K generated over the image of \mathbb{Z} in K by the coefficients of E . If F is the field of fractions of R and F_K is the algebraic closure of F in K , then F_K is a finite extension of F since K is of finite type. By Nagata's theorem ([5] Th. 72), the integral closure R_K of R in K is finitely generated. Let S denote $R_K[\Delta^{-1}]$ where Δ is the usual discriminant ([1] (1.8)). Note that Δ is non-zero since E is an elliptic curve over K . By construction, the curve E is obtained by extension of scalars from a curve E_S/S of genus 1 (in the sense of [1]), and by [loc. cit.] Prop. 5.1, E_S is smooth over S .

Let n be a positive integer not divisible by the characteristic of K . It is well known (see e.g. [6] Th. 8.2) that multiplication by n on E_S is étale over $S[1/n]$. Therefore, the n -torsion of $E_{S[1/n]}$ is the spectrum of a ring of the form $S_1 \oplus \dots \oplus S_k$, where each summand S_i is an integral domain étale over $S[1/n]$. For each n -torsion point of E defined over a quadratic extension L of K , there exists i such that the inclusion $S[1/n] \hookrightarrow L$ factors through S_i . This is possible only for S_i of degree 1 or 2 over $S[1/n]$, since the fraction field F_K is algebraically closed in K and therefore every finite extension of F_K is linearly disjoint from K over F_K .

As S is finitely generated, its maximal ideals have finite residue fields. We fix a maximal ideal with residue field \mathbb{F}_q of characteristic p . If K is of characteristic zero, we can choose p to be any sufficiently large prime, and otherwise, $p = \text{char}(K)$. In any case, $p > 2$. As \mathbb{F}_q is a residue field of $S[1/n]$ for all n not divisible by p , every S_i -point of $E_{S[1/n]}$, where S_i is of degree ≤ 2 , defines a point on $E_S(\mathbb{F}_{q^2})$. There are only finitely many such points, and

distinct components S_i define distinct points. Thus, the prime-to- p torsion of E defined over quadratic fields is finite.

As for p -torsion, by Néron's generalization of the Mordell-Weil theorem ([4] Ch. 6 Th. 1), it is finite. Without loss of generality, we may assume that $E(K)$ contains all p -torsion points of E . Thus, the image of G_K in the automorphism group of the p -adic Tate module of E consists only of p -adic matrices which are congruent to 1 (mod p). It is therefore a pro- p group. Since $p > 2$, the p -parts of $E(K)$ and $E(L)$ are the same for L a quadratic extension of K . \square

We remark that in the case $K = \mathbb{Q}$, much more is known, namely, $E(\mathbb{Q}^{\text{ab}})$ is finite [7].

THEOREM 6: *If K is an infinite field of finite type of characteristic not equal to 2 and E is an elliptic curve over K , then there exists a finite extension L of K such that for all $\sigma \in G_L$, the rank of E over $L^s(\sigma)$ is infinite.*

Proof: Replacing K by a finite extension containing a, b, \dots, f , we may assume that there exist $a, b, c, d, e, f \in K$ such that the curves (*) are all K -isomorphic to affine open subvarieties of E . We iteratively construct quadratic extensions K_i of K and points $P_i \in E(K_n)$ as follows: for each n we apply Lemma 4 to find $x_n \in K$ such that

$$K_1 K_2 \cdots K_{n-1} \left(\sqrt{(x_n - a)(x_n - b)(x_n - c)(x_n - d)}, \right. \\ \left. \sqrt{(x_n - c)(x_n - d)(x_n - e)(x_n - f)} \right)$$

is a biquadratic extension of $K_1 \cdots K_{n-1}$. Then define L_n to be the biquadratic extension of K generated by the two square roots above. Any element $\sigma \in G_K$ induces an action on L_n which must fix at least one of the three quadratic K -subfields of L_n . In other words, there exists a quadratic extension $K_n \subset L_n$ of K such that one of the three curves (*) has a rational point P_n over $K_n \subset K^s(\sigma)$ with x -coordinate x_n . By Proposition 5, we may assume P_n is not a torsion point. Note that P_n lies over x_n , so the $\text{Gal}(K^s/K_1 \cdots K_{n-1})$ -orbit of P_n is $\pm P_n$. If $a_1 P_1 + \cdots + a_n P_n = 0$ for integers a_i , by the linear disjointness of K_1, \dots, K_n , we can apply an automorphism of K^s which is trivial on all but one of the fields K_1, \dots, K_n and non-trivial on the remaining K_i to obtain

$$a_1 P_1 + \cdots + a_{i-1} P_{i-1} - a_i P_i + \cdots + a_n P_n;$$

subtracting, one obtains $2a_i P_i = 0$, which implies $a_i = 0$. We conclude that the P_i are linearly independent in $E(K^s) \otimes \mathbb{Q}$. Thus,

$$E(K^s(\sigma)) \otimes \mathbb{Q} \supset E\left(\prod_n K_n\right) \otimes \mathbb{Q}$$

is infinite dimensional. \square

THEOREM 7: *There exists an elliptic curve E over a number field K such that*

$$\dim E(K^s(\sigma_1, \sigma_2)) \otimes \mathbb{Q} = \infty$$

for all $\sigma_1, \sigma_2 \in G_K$.

Proof: Consider the curves

$$E_i : y^2 = (x - \zeta^i)(x - \zeta^{i+1})(x - \zeta^{i+2})(x - \zeta^{i+4}), \quad i = 0, 1, \dots, 6,$$

where ζ is a primitive 7th root of unity. These curves are isomorphic over $\mathbb{Q}(\zeta)$ by Lemma 2, and their function fields are the 7 quadratic subfields of a $(\mathbb{Z}/2\mathbb{Z})^3$ -Galois extension of the function field of the projective line. This holds because $(1, 1, 1, 0, 1, 0, 0)$ and the vectors obtained from it by cyclic permutation constitute all the non-zero vectors in a three dimensional subspace of \mathbb{F}_2^7 . The argument now goes through as before. \square

By passing from the Hamming code to larger cyclic codes one can find for every n a hyperelliptic curve C over a cyclotomic field K such that $\text{Jac}(C)(K^s(\sigma_1, \dots, \sigma_n))$ is of infinite rank for all $\sigma_1, \dots, \sigma_n \in G_K$.

Acknowledgement

The author would like to thank the referee for his careful reading and for several useful comments on the exposition.

References

- [1] P. Deligne: Courbes Elliptiques: Formulaire d'après J. Tate, in *Modular Functions of One Variable IV*, Lecture Notes in Mathematics 476, Springer-Verlag, Berlin, 1972.
- [2] G. Frey, M. Jarden: Approximation theory and the rank of abelian varieties over large algebraic fields, *Proc. London Math. Soc.* **28** (1974), 112–128.
- [3] W.-D. Geyer, M. Jarden: Torsion points of elliptic curves over large algebraic extensions of finitely generated fields, *Israel J. Math.* **31** (1978), 157–197.
- [4] S. Lang: *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.
- [5] H. Matsumura: *Commutative Algebra*, Second edition, Benjamin/Cummings, Reading, Mass., 1980.
- [6] J. Milne: Abelian Varieties, in *Arithmetic Geometry*, Springer-Verlag, New York, 1986.
- [7] K. Ribet: Appendix to N. Katz and S. Lang, Finiteness theorems in geometric classfield theory, *Enseign. Math.* **27** (1981), 285–319.