C. R. Acad. Sci. Paris, Ser. I 351 (2013) 1–3

Contents lists available at SciVerse ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number Theory

On the prime divisors of the number of points on an elliptic curve

Autour des diviseurs premiers du nombre des points sur une courbe elliptique

Chris Hall [a], Antonella Perucca [b]

[a] *University of Wyoming, United States*
[b] *University of Regensburg, Germany*

A R T I C L E I N F O

Article history:
Received 9 November 2012
Accepted after revision 9 January 2013
Available online 29 January 2013

Presented by Jean-Pierre Serre

A B S T R A C T

Let E be an elliptic curve defined over a number field K and let S be a density-one set of primes of K of good reduction for E. Faltings proved in 1983 that the K-isogeny class of E is characterized by the function $\mathfrak{p} \mapsto \#E(k_{\mathfrak{p}})$, which maps a prime $\mathfrak{p} \in S$ to the order of the group of points of E over the corresponding field $k_{\mathfrak{p}}$. We show that, in this statement, the integer $\#E(k_{\mathfrak{p}})$ can be replaced by its radical.

R É S U M É

Soit E une courbe elliptique définie sur un corps de nombres K, et soit S un ensemble de densité 1 de places de K en lesquelles E a bonne réduction. Faltings a montré en 1983 que la classe de K-isogénie de E est caracterisée par la fonction $\mathfrak{p} \mapsto \#E(k_{\mathfrak{p}})$, qui envoie chaque place $\mathfrak{p} \in S$ sur l'ordre du groupe des points de E sur le corps résiduel correspondant. On montre qu'il suffit de considérer les nombres premiers divisant cet ordre.

Let E, E' be elliptic curves defined over a number field K. Let S be a density-one set of primes of K of good reduction for E and E'. For every $\mathfrak{p} \in S$ write $k_{\mathfrak{p}}$ for the residue field. Faltings proved in 1983 that the curves E, E' are K-isogenous if and only if for every prime $\mathfrak{p} \in S$ they have the same number of points over the residue field: $\#E(k_{\mathfrak{p}}) = \#E'(k_{\mathfrak{p}})$ (cf. [1, Cor. 2]). A weaker condition that one could ask for is that these two integers have the same radical, that is, $\ell \mid \#E(k_{\mathfrak{p}})$ if and only if $\ell \mid \#E'(k_{\mathfrak{p}})$, for every prime number ℓ. We show that this is indeed enough. More precisely:

Theorem. *Suppose E, E' are elliptic curves over a number field K, and let S be a density-one set of primes of K over which E, E' have good reduction. If $\Lambda \subseteq \mathbb{N}$ is an infinite set of primes, then the following are equivalent*:

1. *E, E' are K-isogenous*;
2. *$\ell \mid \#E(k_{\mathfrak{p}})$ if and only if $\ell \mid \#E'(k_{\mathfrak{p}})$, for every $\ell \in \Lambda$ and for every $\mathfrak{p} \in S$.*

The natural generalization of this result to higher dimensional Abelian varieties ('faithfully of type GSp', cf. [4]) has recently been proven by N. Ratazzi in [6], relying on the method that we used in a preceding version of this paper [3]. We thank F. Pellarin for helping us simplify Step 3 of the proof.

E-mail addresses: chall14@uwyo.edu (C. Hall), antonella.perucca@mathematik.uni-regensburg.de (A. Perucca).

1631-073X/$ – see front matter
http://dx.doi.org/10.1016/j.crma.2013.01.003

1. Preliminaries

Let K be a number field, and after fixing a Galois closure $\bar{K}$ of K let G_K be the absolute Galois group. Let ℓ be a prime number, and write μ_ℓ for the set of ℓ-th roots of unity in $\bar{K}$. Let E be an elliptic curve defined over K. We write $K_\ell := K(E[\ell])$ for the smallest extension of K over which the ℓ-th torsion points of $E(\bar{K})$ are defined. We call G_ℓ the Galois group of K_ℓ/K, which we consider embedded in $\mathrm{GL}_2(\mathbb{F}_\ell)$ after choosing a basis for $E[\ell]$. Let $H_\ell \subseteq G_\ell$ be the Galois group of $K_\ell/K(\mu_\ell)$. Well-known properties of the Weil pairing imply that $H_\ell = G_\ell \cap \mathrm{SL}_2(\mathbb{F}_\ell)$. Finally, let $\mathcal{E} := \mathrm{End}_{\bar{K}}(E) \otimes \mathbb{Q}$, which we identify to a subfield of $\bar{K}$ in one of the two possible ways. We will use the following independence result:

Proposition 1. *If L/K is a finite extension then for all but finitely many primes ℓ we have $L \cap K_\ell \subseteq K\mathcal{E}$.*

Proof. It suffices to show $L\mathcal{E} \cap K_\ell\mathcal{E} \subseteq K\mathcal{E}$ hence we may suppose $\mathcal{E} \subseteq K$. Note, there are only finitely many possibilities for $L \cap K_\ell$ and we may neglect the subextensions occurring only for finitely many ℓ. Suppose that $F \subseteq L$ satisfies $F = L \cap K_\ell$ for infinitely many ℓ. We are left to show that $F = K$. By [7, Th. 3 and §4.5, Cor.] we know $K_{\ell_1} \cap K_{\ell_2} = K$ for every sufficiently large prime numbers $\ell_1 \neq \ell_2$. Then the only possibility is $F = K$. □

Let S be a density-one set of primes of K of good reduction for E. If v_ℓ denotes the ℓ-adic valuation, we define ρ_ℓ to be the following map:

$$\rho_\ell : S \to \{0, 1\} \quad \mathfrak{p} \mapsto \min\{1, v_\ell(\#E(k_\mathfrak{p}))\}.$$

There is a Galois–theoretic way to analyze ρ_ℓ:

Lemma 2. *Suppose $\mathfrak{p} \in S$ is not over ℓ and does not ramify in K_ℓ and $\mathfrak{q}$ is a prime of K_ℓ over $\mathfrak{p}$. If $\phi_\mathfrak{q} \in G_\ell$ is the Frobenius of $\mathfrak{q}$, then $\rho_\ell(\mathfrak{p}) = 1$ if and only if $\det(\phi_\mathfrak{q} - 1) = 0$.*

Proof. The embedding $E(k_\mathfrak{p}) \to E(k_\mathfrak{q})$ identifies $E(k_\mathfrak{p})[\ell]$ with $\ker(\phi_q - 1) \subseteq E[\ell]$, hence $\ell \mid \#E(k_\mathfrak{p})$ if and only if 1 is an eigenvalue of $\phi_\mathfrak{q}$. □

Let E' be another elliptic curve over K and suppose that the primes in S are also of good reduction for E'. Define analogously K'_ℓ, G'_ℓ, H'_ℓ, $\mathcal{E}'$ and ρ'_ℓ for E'. We use the notation $\Gamma_\ell \subseteq G_\ell \times G'_\ell$ for the Galois group of the compositum $K_\ell K'_\ell/K$.

Lemma 3. *If $\rho_\ell = \rho'_\ell$, then $\det(\gamma - 1), \det(\gamma' - 1)$ are both zero or both non-zero for every $(\gamma, \gamma') \in \Gamma_\ell$.*

Proof. By the Cebotarev Density Theorem there is some prime $\mathfrak{p} \in S$ not over ℓ, unramified in $K_\ell K'_\ell$ and whose Frobenius conjugacy class in Γ_ℓ contains (γ, γ'). Lemma 2 implies the values $\rho_\ell(\mathfrak{p})$, $\rho'_\ell(\mathfrak{p})$ respectively identify whether or not $\det(\gamma - 1), \det(\gamma' - 1)$ are non-zero, and thus the hypothesis $\rho_\ell(\mathfrak{p}) = \rho'_\ell(\mathfrak{p})$ implies the determinants are both zero or both non-zero. □

2. Proof of the theorem

The implication $1 \Rightarrow 2$ is trivial, so we prove $2 \Rightarrow 1$. Our assumption is that $\rho_\ell = \rho'_\ell$ for every $\ell \in \Lambda$.

2.1. Step 1: Reduction to the case $\mathcal{E}, \mathcal{E}' \subseteq K$

Consider the field $L := K\mathcal{E}\mathcal{E}'$. For a density-one set of primes $\mathfrak{q}$ of L we have: $\mathfrak{q}$ is of good reduction for E and E'; the prime $\mathfrak{p} := \mathfrak{q} \cap K$ is in S; the prime $\mathfrak{q}$ has degree one hence $k_\mathfrak{q} = k_\mathfrak{p}$. We deduce that the assumptions of the theorem hold for L if they hold for K. The following general lemma completes this first step of the proof:

Lemma 4. *If two elliptic curves E, E' defined over K are $K\mathcal{E}\mathcal{E}'$-isogenous, then they are K-isogenous.*

Proof. Let $L := K\mathcal{E}\mathcal{E}'$. Since E, E' are isogenous then $\mathcal{E} = \mathcal{E}'$ and so $L = K\mathcal{E} = K\mathcal{E}'$. Let S_1 be the density-one subset of primes $\mathfrak{p}$ of K which have degree one, which neither ramify in L nor lie over 2 or 3 and which are of good reduction for E and E'. Let $a_\mathfrak{p}$ (respectively $a'_\mathfrak{p}$) denote the trace of the Frobenius at $\mathfrak{p}$ for E (respectively E').

If $\mathfrak{q}$ is a prime of L lying over $\mathfrak{p}$, then $a_\mathfrak{q} = a'_\mathfrak{q}$ since E, E' are L-isogenous. If $\mathfrak{p}$ splits in L, then we have $a_\mathfrak{p} = a_\mathfrak{q}$ and $a'_\mathfrak{q} = a'_\mathfrak{p}$ since $k_\mathfrak{q} = k_\mathfrak{p}$, thus $a_\mathfrak{p} = a'_\mathfrak{p}$. Otherwise, $\mathfrak{p} \in S_1$ is inert, thus [5, Ch. 10, §4, Th. 10] implies E, E' have supersingular reduction over $\mathfrak{p}$. Moreover, since $\#k_\mathfrak{p}$ is prime and thus not a square, proposition [8, Th. 4.1] implies $a_\mathfrak{p} = a'_\mathfrak{p} = 0$. Therefore $a_\mathfrak{p} = a'_\mathfrak{p}$ for every $\mathfrak{p} \in S_1$ as claimed. We conclude by [1, Cor. 2] that E and E' are K-isogenous. □

2.2. Step 2: The curves E, E' are $\bar{K}$-isogenous

By [2, Th. A] (which is a refinement of [7, Lem. 9 and Th. 7]) it suffices to show that there are infinitely many prime numbers ℓ such that $K_\ell = K'_\ell$.

Lemma 5. *For all but finitely many $\ell \in \Lambda$ we have $K_\ell = K'_\ell$.*

Proof. Let $\ell \in \Lambda$, and without loss of generality suppose $K_\ell \nsubseteq K'_\ell$. This means that the kernel of the projection $\Gamma_\ell \to G'_\ell$ is non-trivial. This kernel projects to a non-trivial normal subgroup of G_ℓ, which is contained in H_ℓ because its elements fix $K(\mu_\ell) \subseteq K'_\ell$. Since $\mathcal{E} \subseteq K$ by the first step, for all but finitely many ℓ either $\mathcal{E} = \mathbb{Q}$ and $G_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)$ or $\mathcal{E} \neq \mathbb{Q}$ and G_ℓ is a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, see [7, Th. 2 and §4.5, Cor.].

In the first case, $\gamma = -1$ lies in every non-trivial normal subgroup of $H_\ell = \mathrm{SL}_2(\mathbb{F}_\ell)$ (cf. [2, Lem. 2.2]). In the second case, every $\gamma \in H_\ell$ is semisimple and we know $\det(\gamma) = 1$, so if $\gamma \neq 1$ we have $\det(\gamma - 1) \neq 0$. Either way, we can find an element $(\gamma, 1) \in \Gamma_\ell$ satisfying $\det(\gamma - 1) \neq 0$. Lemma 3 then implies $\rho_\ell \neq \rho'_\ell$, contradicting $\ell \in \Lambda$. $\square$

2.3. Step 3: Every $\bar{K}$-isogeny between E, E' is defined over K

We have two elliptic curves E, E' over a number field K that are $\bar{K}$-isogenous and such that $\mathcal{E} = \mathcal{E}' \subseteq K$. Every $\bar{K}$-isogeny between such curves is defined over a finite extension of K with degree at most 6, as the following lemma shows. Let $\mu \subset \mathcal{E}^\times$ be the subgroup of roots of unity and $\mathbb{Z}_\mathcal{E} \subset \mathcal{E}$ be the ring of integers. Let $f : E \to E'$ be a $\bar{K}$-isogeny of degree $d \geqslant 1$, and let $\hat{f} : E' \to E$ be the $\bar{K}$-isogeny satisfying $\hat{f} \circ f = d$. We write ${}^\sigma f$ for the transform of f by $\sigma \in G$ and we define δ to be the following map:

$$\delta : G_K \to \mathcal{E}^\times \quad \sigma \mapsto \frac{1}{d}\big(\hat{f} \circ {}^\sigma f\big).$$

Lemma 6. *The map δ is a group homomorphism with image contained in μ.*

Proof. For every $\sigma_1, \sigma_2 \in G_K$, since ${}^{\sigma_1} f \circ {}^{\sigma_1} \hat{f} = d$ and recalling that the action of G_K on $\mathcal{E} \subseteq K$ is trivial, we have

$$\delta(\sigma_1\sigma_2) = \frac{1}{d}\big(\hat{f} \circ {}^{\sigma_1\sigma_2} f\big) = \frac{1}{d^2}\big(\hat{f} \circ {}^{\sigma_1} f \circ {}^{\sigma_1}\hat{f} \circ {}^{\sigma_1\sigma_2} f\big) = \delta(\sigma_1) \cdot {}^{\sigma_1}\delta(\sigma_2) = \delta(\sigma_1) \cdot \delta(\sigma_2)$$

hence δ is a homomorphism. Since f is defined over a finite extension of K, the image of δ is a finite subgroup of $\mathcal{E}^\times$ so it is contained in μ. $\square$

Suppose that the curves E, E' also satisfy the assumptions of our theorem. We take $\sigma \in G_K$ and show that ${}^\sigma f = f$, or equivalently $\delta(\sigma) = 1$. To do so, we work with one $\ell \in \Lambda$, to be chosen sufficiently large. We take ℓ not dividing d, and such that for every $\zeta \in \mu \setminus \{1\}$ we have $\zeta - 1 \notin \ell\mathbb{Z}_\mathcal{E}$.

Let $L \subseteq \bar{K}$ be the smallest Galois extension of K where f is defined. By Proposition 1 and Lemma 5, up to excluding finitely many ℓ we may suppose that $L \cap K_\ell K'_\ell = K$. Then we may restrict to the case where $\sigma \in G_K$ induces the identity map on K_ℓ and K'_ℓ. This means that $E[\ell]$ is contained in the kernel of ${}^\sigma f - f$, so we have

$$\big(\delta(\sigma) - 1\big) = \hat{f} \circ \big({}^\sigma f - f\big) \in \ell\mathbb{Z}_\mathcal{E}.$$

Since ℓ and d are coprime, we deduce that $\delta(\sigma) - 1$ is in $\ell\mathbb{Z}_\mathcal{E}$, which implies $\delta(\sigma) = 1$.

References

[1] G. Faltings, Finiteness theorems for Abelian varieties over number fields, in: G. Cornell, J.H. Silverman (Eds.), Arithmetic Geometry, Springer-Verlag, New York, 1986, pp. 9–27.
[2] G. Frey, M. Jarden, Horizontal isogeny theorems, Forum Math. 14 (6) (2002) 931–952.
[3] C. Hall, A. Perucca, Radical characterizations of elliptic curves, preprint, arXiv:1109.2440, 2011.
[4] M. Hindry, N. Ratazzi, Points de torsion sur les variétés abéliennes de type GSp, J. Inst. Math. Jussieu 11 (1) (2012) 27–65.
[5] S. Lang, Elliptic Functions, second edition, Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987.
[6] N. Ratazzi, Isogénies horizontales et classes d'isogénies de variétés abéliennes, preprint, arXiv:1211.4387, 2012.
[7] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (4) (1972) 259–331.
[8] W.C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. École Norm. Sup. 4 (2) (1969) 521–560.