PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 10, Pages 2851–2856
S 0002-9939(99)05125-4
Article electronically published on June 17, 1999

KAMIENNY'S CRITERION AND THE METHOD OF COLEMAN AND CHABAUTY

MATTHEW H. BAKER

(Communicated by David E. Rohrlich)

Abstract. This paper gives a new proof of Kamienny's Criterion using the method of Coleman and Chabauty.

1. Introduction

The strong uniform boundedness conjecture for the torsion on elliptic curves (proven by L. Merel) is the following assertion: given a positive integer d, there is a constant B_d depending only on d such that for any number field K of degree d over $\mathbb{Q}$, and any elliptic curve E/K with a point $P \in E(K)$ of order n, we have $n \leq B_d$. It was known prior to Merel's work that it is sufficient to prove this statement with $n = N$ a *prime*; see [3]. Using the existence of a quotient of $J_0(N)$ with finite Mordell-Weil group (Mazur's Eisenstein quotient or Merel's winding quotient), this conjecture can be reduced to a question of showing that certain Hecke operators are linearly independent mod p for some auxiliary prime p when N is sufficiently large (with respect to d). This reduction step is known as Kamienny's criterion, and will be explained in more detail shortly.

The *winding quotient* J_e of $J_0(N)$ is, philosophically speaking, the largest quotient of $J_0(N)$ with finite Mordell-Weil group. It is defined as $J_e := J_0(N)/I_e J_0(N)$, where I_e is the ideal $\mathrm{Ann}_{\mathbf{T}} e$ in the Hecke algebra $\mathbf{T}$, e is the "winding element" in $\mathrm{H}_1(X_0(N); \mathbb{Q})$ (see [8, §1]), and $I_e J_0(N)$ is the abelian subvariety of $J_0(N)$ generated by I_e. The finiteness of the Mordell-Weil group of J_e follows from deep algebraic and analytic results of Kolyvagin-Logachev, Gross-Zagier, Bump-Friedberg-Hoffstein, and others. (See [8, Prop. 1].)

Let I now be any ideal in $\mathbf{T}$ such that $J := J_0(N)/IJ_0(N)$ has finite Mordell-Weil group. Kamienny's criterion, which first appeared in [5], can be stated as follows:

Theorem 1 (Kamienny's Criterion)**.** *The strong uniform boundedness conjecture is implied by the following hypothesis:*

Given $d > 0$, there exists a constant B_d such that for all primes $N > B_d$ there exists a prime number $p \neq 2$ or N such that the Hecke operators $T_1, \ldots, T_d$ are linearly independent in $\mathbf{T}/(p, I)$.

Received by the editors January 7, 1998.
1991 *Mathematics Subject Classification.* Primary 14G25, 11G05; Secondary 11G30.
Key words and phrases. Arithmetic geometry, modular curves, p-adic analysis, elliptic curves.
Special thanks to Loic Merel for his assistance with this work. The author of this work was supported by an NDSEG Fellowship.

Remark. The above hypothesis implies that $\dim(J) \geq d$.

Merel established the strong uniform boundedness conjecture by proving, using modular symbols, that the hypothesis in Kamienny's Criterion is satisfied when $J = J_e$, the winding quotient of $J_0(N)$.

The standard argument for proving Kamienny's criterion uses ideas of Mazur and Kamienny on formal immersions. I will give another argument using the ideas of Coleman and Chabauty, translating the condition that certain Hecke operators are linearly independent into a statement that certain p-adic integrals have few common zeros.

Remark. In what follows, we use very little of the actual machinery behind Coleman's general theory of p-adic integration; the theory of formal Lie groups is probably sufficient. But since my goal in this work was to understand the Coleman-Chabauty method in the context of determining rational points on symmetric powers of curves, we will freely adopt the notation of [1] and [2].

2. The method of Coleman and Chabauty

We give only a brief sketch of the needed results.

Let p be a prime number.

Let $\mathfrak{C}$ be the category of complete varieties Y over $\mathbb{Q}$ having smooth proper models $\mathcal{Y}$ over $\mathbb{Z}_p$, together with a base point $y_0 \in Y(\mathbb{Q})$. The morphisms must preserve base-points and be defined over $\mathbb{Q}$.

So let $(Y, \mathcal{Y}, y_0) \in \mathfrak{C}$. To each $\omega \in H^0(\mathcal{Y}, \Omega_{\mathcal{Y}/\mathbb{Z}_p})$ we can associate its "definite" Coleman integral

$$\begin{aligned} \lambda_\omega : \quad & Y(\mathbb{C}_p) \to \mathbb{C}_p, \\ & P \mapsto \textstyle\int_{y_0}^{P} \omega. \end{aligned}$$

If we consider Y as a rigid space over $\mathbb{C}_p$, then λ_ω is analytic on each residue class. It also is constructed in such a way as to have nice global properties, according to Dwork's principle of "analytic continuation along Frobenius".

We can think of this p-adic integral as giving us a pairing $\langle P, \omega \rangle = \lambda_\omega(P)$.

Some functorial properties of p-adic integration are:

(i) If $\phi : (X, \mathcal{X}, x_0) \to (Y, \mathcal{Y}, y_0)$ is a morphism in $\mathfrak{C}$ and $\omega \in H^0(\mathcal{Y}, \Omega_{\mathcal{Y}/\mathbb{Z}_p})$, then $\langle P, \phi^* \omega \rangle = \langle \phi(P), \omega \rangle$.

(ii) If σ is a continuous automorphism of $\mathbb{C}_p$, then $\langle P, \omega \rangle^\sigma = \langle P^\sigma, \omega \rangle$.

(iii) On an abelian variety, each λ_ω is a homomorphism. In particular, as $\mathbb{C}_p$ is torsion-free, $\lambda_\omega(T) = 0$ for all torsion points $T \in Y(\mathbb{C}_p)$.

Let $\phi : (X, \mathcal{X}, x_0) \to (A, \mathcal{A}, 0)$ be a morphism in $\mathfrak{C}$, where A is an abelian variety over $\mathbb{Q}$ with smooth proper Neron model $\mathcal{A}/\mathbb{Z}_p$, i.e., A has good reduction at p. Then $H^0(\mathcal{A}, \Omega_{\mathbb{A}/\mathbb{Z}_p})$ is free of rank g as a $\mathbb{Z}_p$-module. Also, $A(\mathbb{Q}_p)/A(\mathbb{Q}_p)^{\mathbf{tor}}$ is a free $\mathbb{Z}_p$-module of rank g.

The Coleman integrals give us a perfect pairing of $\mathbb{Q}_p$-vector spaces

$$A(\mathbb{Q}_p) \otimes \mathbb{Q}_p \times H^0(\mathcal{A}, \Omega_{\mathbb{A}/\mathbb{Z}_p}) \otimes \mathbb{Q}_p \to \mathbb{Q}_p.$$

Suppose that $\operatorname{rank} A(\mathbb{Q}) = r < g$, and let $\bar{A}(\mathbb{Q})$ be the smallest linear subspace of $A(\mathbb{Q}_p) \otimes \mathbb{Q}_p$ containing $A(\mathbb{Q})$. Clearly we have $\dim \bar{A}(\mathbb{Q}) \leq r$.

As $r < g$, the annihilator of $\bar{A}(\mathbb{Q})$ with respect to the pairing $\langle \cdot, \cdot \rangle$ is nontrivial; call it W. We see in particular that $\langle A(\mathbb{Q}), W \rangle = 0 \Rightarrow \langle X(\mathbb{Q}), \phi^* W \rangle = 0$.

In this context, the idea of Coleman-Chabauty is that we can bound the number of points in $X(\mathbb{Q})$ by bounding the number of common zeros over $\mathbb{Q}_p$ of the integrals associated to differentials in $\phi^* W$. For an application of this idea to Fermat's Last Theorem, see [7].

3. Kamienny's Criterion

The purpose of this section is to give our proof of Theorem 1. We use the notations of that theorem, so we fix a prime number N and an arbitrary auxiliary prime $p \neq 2, N$. We let $J := J_0(N)/IJ_0(N)$, where I is an ideal in $\mathbf{T}$ such that $J \neq 0$ and the Mordell-Weil group of J is finite. Since $J_0(N)$ has good reduction at p, so does J, and we denote by $\mathcal{J}$ the Neron model of J, which is an abelian scheme over $\mathbb{Z}_p$. We also denote by $\mathcal{J}_0(N)$ the Neron model for $J_0(N)$, and by $\mathcal{X}_0(N)$ a smooth proper model over $\mathbb{Z}_p$ for $X_0(N)$.

We will assume:

Assumption. *For $N >> 0$ (with respect to d), $T_1, \ldots, T_d$ are linearly independent in $\mathbf{T}/(p, I)$.*

As already remarked, this implies that $s := \dim(J)$ is $\geq d$.

What we need to prove, then, is

Goal. *Let K be a number field of degree d. For $N >> 0$ (with respect to d), there are no K-rational elliptic curves having K-rational points of order N.*

The way in which we use our assumption that the rank of $J(\mathbb{Q})$ is zero is that it implies $J(\mathbb{Q}) \otimes \mathbb{Q}_p = 0$, and so $W = H^0(\mathcal{J}, \Omega_{\mathcal{J}/\mathbb{Z}_p}) \otimes \mathbb{Q}_p$ annihilates $J(\mathbb{Q})$ with respect to the pairing $\langle \cdot, \cdot \rangle$.

By standard arguments, it is enough to show that $\infty^{(d)}$ is the only $\mathbb{Q}$-rational point of $X_0(N)^{(d)}$ in its residue class U mod p; see [3]. [Here $X_0(N)^{(d)}$ denotes the d-th symmetric power of $X_0(N)$. It has a smooth model $\mathcal{X}_0(N)^{(d)}$ over $\mathbb{Z}_p$]. Briefly, the idea is as follows. Suppose we are given $d \geq 1$, a number field K of degree d, an elliptic curve E/K, and $P \in E(K)$ a point of prime order N. Let $y \in X_0(N)(K)$ correspond to $(E/\langle P \rangle, E[N]/\langle P \rangle)$. Then standard facts about elliptic curves show that the strong uniform boundedness conjecture is true if E has good or additive reduction at some prime $\mathfrak{p}$ of K lying over p (see [5, Lemma 3.2]). So y specializes to $\widetilde{\infty}$ on $\widetilde{\mathcal{X}_0(N)}$ under reduction mod $\mathfrak{p}$ for every such $\mathfrak{p}$. Now let $x := \sum_\sigma \sigma(y) \in X_0(N)^{(d)}(\mathbb{Q})$, where the sum is over the d embeddings $\sigma : K \hookrightarrow \mathbb{C}$. Then x specializes to $\widetilde{\infty^{(d)}}$ in $\widetilde{\mathcal{X}_0(N)^{(d)}}$.

Using the Coleman-Chabauty philosophy, we should try to show, then, that there is only one point (namely $\infty^{(d)}$) in $U(\mathbb{Q}_p)$ annihilated by $\phi^* W$ under the pairing $\langle \cdot, \cdot \rangle$, where ϕ is the natural map

$$\phi : \mathcal{X}_0(N)^{(d)} \to \mathcal{J}_0(N) \to \mathcal{J}$$

sending $\infty^{(d)} \in X_0(N)^{(d)}(\mathbb{Q})$ to 0. To do this, we consider local expansions for differentials on $X_0(N)^{(d)}$.

Let $r : X_0(N)^{(d)}(\mathbb{C}_p) \to \widetilde{\mathcal{X}_0(N)^{(d)}}(\bar{\mathbb{F}}_p)$ be the reduction map. The residue class $U = r^{-1}(\widetilde{\infty^{(d)}})$ has a natural structure as a rigid analytic space over $\mathbb{C}_p$. Since $\widetilde{\infty^{(d)}}$ is a nonsingular point of the reduction, there exists an isomorphism of rigid

spaces

$$\psi : U \xrightarrow{\sim} \mathbb{B}^d_{\mathbb{C}_p}(1)$$

defined over $\mathbb{Q}_p^{\mathrm{unr}}$, where $\mathbb{B}^d_{\mathbb{C}_p}(1)$ is the d-dimensional "open" unit ball in $\mathbb{C}_p$. (See [4, Theorem 4.2].) We may assume that $\psi(\infty^{(d)}) = (0, \dots, 0)$, and we can now expand differentials in terms of the local parameters $\sigma_1, \dots, \sigma_d$ on U afforded by the isomorphism ψ.

As $p \neq 2$, we have

$$\phi^* : H^0(\mathcal{J}, \Omega_{\mathcal{J}/\mathbb{Z}_p}) \hookrightarrow H^0(\mathcal{J}_0(N), \Omega_{\mathcal{J}_0(N)/\mathbb{Z}_p}) \xrightarrow{\sim} H^0(\mathcal{X}_0(N)^{(d)}, \Omega_{\mathcal{X}_0(N)^{(d)}/\mathbb{Z}_p}).$$

(See [6, Cor. 1.1] and [9, Prop. 5.3].) Since

$$H^0(\mathcal{J}_0(N), \Omega_{\mathcal{J}_0(N)/\mathbb{Z}_p}) \cong H^0(\mathcal{X}_0(N), \Omega_{\mathcal{X}_0(N)/\mathbb{Z}_p}) \cong S_2(\Gamma_0(N); \mathbb{Z}_p),$$

we may identify an element $\omega \in H^0(\mathcal{J}, \Omega_{\mathcal{J}/\mathbb{Z}_p})$ by its q-expansion

$$(a_1 q + a_2 q^2 + \dots)\frac{dq}{q},$$

where q is a local parameter around ∞ on $X_0(N)$.

In terms of the corresponding symmetric parameters $\sigma_1, \dots, \sigma_d$ for $X_0(N)^{(d)}$ around $\infty^{(d)}$, the map ϕ^* sends ω to

$$a_1 d\sigma_1 - a_2 d\sigma_2 + \cdots + (-1)^{d-1} a_d d\sigma_d + \text{higher order terms}$$

by "Newton's Lemma". (See [9, Lemma 5.4] or [3, Lemma 4.2].)

Recalling that $s = \dim J$, let $\omega_1, \dots, \omega_s$ be a basis for $H^0(\mathcal{J}, \Omega_{\mathcal{J}/\mathbb{Z}_p})$, and let $\eta_i = \phi^* \omega_i$ for $1 \leq i \leq s$.

Writing $\omega_i = (\sum_{j=1}^{\infty} a_{ij} q^j)\frac{dq}{q}$, it follows from the construction of Coleman's integrals that a local power series expansion for the λ_{η_i} is given by integrating the expansions of the η_i in the obvious way:

$$\lambda_{\eta_i} = a_{i1}\sigma_1 - \cdots + (-1)^{d-1} a_{id}\sigma_d + g_i(\sigma_1, \dots, \sigma_d),$$

where $g_i \in (\sigma_1, \dots, \sigma_d)^2 \mathbb{Q}_p[[\sigma_1, \dots, \sigma_d]]$ and $dg_i = \sum_j \frac{\partial g_i}{\partial \sigma_j} d\sigma_j$ has coefficients in $\mathbb{Z}_p$. Note that the constant term coming from the integration is zero because $\lambda_{\eta_i}(\infty^{(d)}) = 0$.

If we make the change of variables $p\sigma'_j = \sigma_j$, then to study the zeros of λ_{η_i} in $\mathbb{B}^d_{\mathbb{C}_p}(1)$ it suffices to find the zeros of

$$\lambda'_{\eta_i} = \frac{1}{p}\lambda_{\eta_i} = a_{i1}\sigma'_1 - \cdots + (-1)^{d-1} a_{id}\sigma'_d + p g'_i(\sigma'_1, \dots, \sigma'_d)$$

in $\mathbb{B}^d_{\mathbb{C}_p}[1]$, the "closed" ball of radius 1. One easily checks, using the fact that $p > 2$, that $g'_i \in \mathbb{Z}_p[[\sigma'_1, \dots, \sigma'_d]]$.

Now suppose that $x \neq \infty^{(d)}$ in $U(\mathbb{Q}_p)$ is such that $\langle x, \phi^* W \rangle = 0$. As desired, we will show that this leads to a contradiction.

Let $\psi' = \frac{1}{p} \circ \psi : U \xrightarrow{\sim} \mathbb{B}^d_{\mathbb{C}_p}[1]$, and let R^u be the ring of integers in $\mathbb{Q}_p^{\mathrm{unr}}$. Then $\psi'(x) = (x_1, \dots, x_d)$, with $x_i \in R^u, 1 \leq i \leq d$. Now $x \neq \infty^{(d)}$ implies that not all x_i are 0, so there is an integer $k \geq 0$ such that

$$\psi'(x) = (p^k x'_1, \dots, p^k x'_d),$$

with $x'_i \in R^u$ for all i, and with not all $x_i \equiv 0 \bmod p$.

By assumption, $\lambda_{\eta_i}(x) = 0$ for $i = 1, \ldots, s$, and thus

$$\sum_{j=1}^{d} (-1)^{j-1} a_{ij} p^k x'_j + p \cdot p^{2k} \cdot g'_i(x'_1, \ldots, x'_d) = 0$$

for $i = 1, \ldots, s$. Hence in particular

$$\sum_{j=1}^{d} (-1)^{j-1} a_{ij} x'_j \equiv 0 \mod p$$

for $i = 1, \ldots, s$.

Claim. For $N >> 0$ (in terms of d), we can pick $\omega_1, \ldots, \omega_d \in H^0(\mathcal{J}, \Omega_{\mathcal{J}/\mathbb{Z}_p})$ in such a way that $(\widetilde{a_{ij}}), 1 \leq i, j \leq d$, is congruent to the $d \times d$ *identity matrix* over $\mathbb{F}_p$. [In fact, we only need $(\widetilde{a_{ij}})$ to be invertible.]

Given the claim, we then use this choice of $\omega_1, \ldots, \omega_d$ and find that

$$\sum_{j=1}^{d} (-1)^{j-1} \delta_{ij} x'_j \equiv 0 \mod p$$

for $i = 1, \ldots, s$, hence $x'_i \equiv 0 \bmod p$ for $i = 1, \ldots, d$, a contradiction. [Recall that $s \geq d$.] So we find that $U(\mathbb{Q}) = \{\infty^{(d)}\}$, from which Kamienny's criterion follows.

Proof of Claim. We note that there is a perfect pairing of $\mathbb{F}_p$-vector spaces

$$\mathbf{T}/p \times S_2(\Gamma_0(N); \mathbb{F}_p) \to \mathbb{F}_p$$

given by $\langle\langle T, f \rangle\rangle = a_1(f|T)$.

This induces a perfect pairing

$$\langle\langle \cdot, \cdot \rangle\rangle' : \mathbf{T}/(p, I) \times S_2(\Gamma_0(N); \mathbb{F}_p)[I] \to \mathbb{F}_p,$$

and since $p \neq 2$, we may identify $S_2(\Gamma_0(N); \mathbb{F}_p)[I]$ with $H^0(\tilde{\mathcal{J}}, \Omega_{\tilde{\mathcal{J}}/\mathbb{F}_p})$. (See [3, Proof of theorem 4.3].)

We now use our main assumption, which tells us that $T_1, \ldots, T_d$ are linearly independent in the $\mathbb{F}_p$-vector space $\mathbf{T}/(p, I)$. Now let $f_1, \ldots, f_d$ be the dual basis to $T_1, \ldots, T_d$ with respect to the pairing $\langle\langle \cdot, \cdot \rangle\rangle'$. Then if we write $\omega_i = (\sum_{j=1}^{\infty} a_{ij} q^j) \frac{dq}{q}$ for some choice of elements of $H^0(\mathcal{J}, \Omega_{\mathcal{J}/\mathbb{Z}_p})$ which lift (mod p) the differentials corresponding to the f_i, we find that

$$\widetilde{a_{ij}} = a_i(f_j) = a_1(f_j|T_i) = \langle\langle T_i, f_j \rangle\rangle' = \delta_{ij} \in \mathbb{F}_p,$$

as claimed. □

References

[1] R. Coleman: Torsion Points on Curves and p-adic Abelian Integrals. Annals of Mathematics. **121**, 111-168 (1985) MR **86j:**14014

[2] R. Coleman: Effective Chabauty. Duke Math. J. **52**, 765-770 (1985) MR **87f:**11043

[3] B. Edixhoven: Rational Torsion Points on Elliptic Curves Over Number Fields [after Kamienny and Mazur]. Séminaire Bourbaki 46ème année, 1993-94, n. 782. MR **96c:**11056

[4] L. Gerritzen and M. van der Put: *Schottky Groups and Mumford Curves*, Lecture Notes in Mathematics 817, Springer-Verlag, 1980. MR **82j:**10053

[5] S. Kamienny: Torsion Points on Elliptic Curves over Fields of Higher Degree. International Mathematics Research Notices. 6, 129-133 (1992) MR **93e:**11072

[6] B. Mazur: Rational Isogenies of Prime Degree. Inventiones math. **44**, 129-162 (1978) MR **80h:**14022

[7] W. McCallum: On the Method of Coleman and Chabauty. Mathematische Annalen. **299**, 565-596 (1994) MR **95c:**11079
[8] L. Merel: Bornes Pour la Torsion des Courbes Elliptiques sur les Corps de Nombres. Inventiones math. **124**, 437-449 (1996) MR **96i:**11057
[9] J.S. Milne: "Abelian Varieties" in *Arithmetic Geometry* (ed. Cornell, Silverman), Springer-Verlag, 1986. MR **89b:**14029

Department of Mathematics, University of California, Berkeley, California 94720-3840
E-mail address: baker@math.berkeley.edu