Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 346 (2008) 599–602
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Number Theory

Integral j-invariants and Cartan structures for elliptic curves

Yu. Bilu, Pierre Parent

Institut de mathématiques de Bordeaux, 351, cours de la Libération, 33405 Talence cedex, France

Received 23 November 2007; accepted after revision 14 April 2008

Available online 29 April 2008

Presented by Jean-Pierre Serre

Abstract

We bound the j-invariant of integral points on a modular curve in terms of the congruence group defining the curve. We apply this to prove that, under the GRH, the modular curve $X_{\mathrm{split}}(p^5)$ has no non-trivial rational point if p is a sufficiently large prime number. ***To cite this article: Yu. Bilu, P. Parent, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Résumé

Invariants j entiers et structures de Cartan de courbes elliptiques. On borne l'invariant j des points entiers des courbes modulaires, en fonction du groupe de congruence définissant la courbe. Sous l'hypothèse de Riemann généralisée, on en déduit que, si p est un nombre premier suffisamment grand, la courbe modulaire $X_{\mathrm{split}}(p^5)$ n'a pas de point rationnel non trivial. ***Pour citer cet article : Yu. Bilu, P. Parent, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

1. Introduction

Let $N \geqslant 3$ be an integer and $\bar{\Gamma}$ a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\det(\bar{\Gamma}) = (\mathbb{Z}/N\mathbb{Z})^*$. We set $\Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$ to be the pull-back of $\bar{\Gamma}$ and X_Γ the corresponding proper modular curve over $\mathbb{Q}$, as defined in [10]. We consider the set of integral points $Y_\Gamma(\mathbb{Z})$, consisting of those $P \in X_\Gamma(\mathbb{Q})$ for which $j(P) \in \mathbb{Z}$, where j is, as usual, the modular invariant. We denote by $\mathcal{C}$ the set of cusps of $X_\Gamma(\bar{\mathbb{Q}})$.

Theorem 1.1. *Assume that* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *does not act transitively on* $\mathcal{C}$. *Then for* $P \in Y_\Gamma(\mathbb{Z})$ *we have* $\log|j(P)| \leqslant 21N^2|\bar{\Gamma}| + 90N$.

We remark that this estimate is certainly not best possible for the method. Besides refining the constants, one can probably obtain an estimate of shape $\log|j(P)| = O(p^{-1}N^2|\bar{\Gamma}|\log p)$, where p is the smallest prime divisor of N. This would allow us to replace p^5 by p^4 in Theorem 1.2.

We then apply this result to the curve $X_{\mathrm{split}}(p)(\mathbb{Q})$, for a prime p, where for $n \geqslant 0$ the curve $X_{\mathrm{split}}(p^n)$ corresponds to a group $\overline{\Gamma}$ which is the normalizer of a split Cartan subgroup mod p^n, i.e. a group conjugate to that of diagonal and

E-mail addresses: Yuri.Bilu@math.u-bordeaux1.fr (Yu. Bilu), Pierre.Parent@math.u-bordeaux1.fr (P. Parent).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2008.04.002

antidiagonal matrices mod p^n. We are motivated by a question of Serre [8]: does there exist an absolute constant C such that for any non-CM elliptic curve E over $\mathbb{Q}$ and any prime $p > C$ the natural Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$ is surjective? One knows that it suffices for a positive answer to bound the primes p such that a non-CM curve has a Galois structure included in the normalizer of a (split or non-split) Cartan subgroup of $\mathrm{GL}(E[p])$. Equivalently, one would like to prove that, for large p, the only rational points of $X_{\mathrm{split}}(p)$ and $X_{\mathrm{nonsplit}}(p)$ are the cusps and CM points. In the present Note we prove the following:

Theorem 1.2. *Assume the Generalized Riemann Hypothesis for zeta functions of number fields* (*GRH in the sequel*). *Then for large enough prime p, every point in $X_{\mathrm{split}}(p^5)(\mathbb{Q})$ is either CM or a cusp.*

More general results (with more detailed proofs) will appear in [1]. After this note was submitted we noticed that, at the expense of replacing p^5 by a higher power (probably p^9), the GRH-assumption in Theorem 1.2 can be suppressed, using the isogeny estimate of Masser and Wüstholz [5] (which, as the referee indicated to us, has been made explicit by Pellarin [7]). This will also be addressed in [1].

2. Proof of Theorem 1.1

Put $A_N = (N^{-1}\mathbb{Z}/\mathbb{Z})^2 \setminus \{\mathbf{0}\}$. Fix $\mathbf{a} = (a_1, a_2) \in A_N$ and let $g_{\mathbf{a}} : \mathcal{H} \to \mathbb{C}$ be the corresponding *Siegel function* [4, Section 2.1]. Then $g_{\mathbf{a}}^{12N}$ defines a $\mathbb{Q}(\zeta_N)$-rational function on the curve $X(N)$, having all its zeros and poles at the cusps (a *modular unit*). Further, since $\det(\bar{\Gamma}) = (\mathbb{Z}/N\mathbb{Z})^*$, the expression $u_{\mathbf{a}} = \prod_{\gamma\in\bar{\Gamma}} g_{\mathbf{a}\gamma}^{12N}$ defines a $\mathbb{Q}$-rational modular unit on X_Γ.

Theorem 1.1 is proved by a variation of Runge's method (see [2] for a general discussion), adapted to modular curves. It is a direct consequence of the following two statements:

Proposition 2.1 *(an analytic estimate). Assume that* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *does not act transitively on $\mathcal{C}$. Then for any $P \in Y_\Gamma(\mathbb{C})$ either $|j(P)| \leqslant 10^{N+2}$ or there exists $\mathbf{a} \in A_N$ such that*

$$\bigl|\log\bigl|u_{\mathbf{a}}(P)\bigr|\bigr| \geqslant N^{-1}\log\bigl|j(P)\bigr| - \bigl(12N|\bar{\Gamma}| + 90\bigr).$$

Proposition 2.2 *(an arithmetic estimate). For every $P \in Y_\Gamma(\mathbb{Z})$ and every $\mathbf{a} \in A_N$ we have $1 \leqslant |u_{\mathbf{a}}(P)| \leqslant 2^{12|\bar{\Gamma}|N}$.*

The proofs of these propositions use the three lemmas below. Let $\mathcal{H}$ be the Poincaré upper half-plane. Recall that $X_\Gamma(\mathbb{C})$ is analytically isomorphic to $\bar{\mathcal{H}}/\Gamma$, where $\bar{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{\mathrm{i}\infty\}$. For $\tau \in \mathcal{H}$ put, as usual, $q_\tau = \exp(2\pi\mathrm{i}\tau)$. By abuse of notation, we denote by j also the modular j-invariant on $\mathcal{H}$. Let D be the familiar fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$ (the hyperbolic triangle with vertices $\mathrm{e}^{\pi i/3}$, $\mathrm{e}^{2\pi i/3}$ and $\mathrm{i}\infty$, together with the geodesic segments $[\mathrm{i}, \mathrm{e}^{2\pi\mathrm{i}/3}]$ and $[\mathrm{e}^{2\pi\mathrm{i}/3}, \mathrm{i}\infty]$).

Lemma 2.3. *For any $\tau \in D$ we have either $|j(\tau)| \leqslant 14\,000$ or $|q_\tau| \leqslant 0.001$. If $|q_\tau| \leqslant 0.001$, then $|\log|j(\tau)q_\tau|| \leqslant 900|q_\tau|$.*

The proof is by straightforward estimates using the standard q-expansions for the modular invariant. See [1] for the details.

Let $\ell_{\mathbf{a}}$ be the order of vanishing of $g_{\mathbf{a}}$ at $\mathrm{i}\infty$; that is, the only rational number such that the limit $\lim_{\tau\to\mathrm{i}\infty} q_\tau^{-\ell_{\mathbf{a}}} g_{\mathbf{a}}(\tau)$ exists and is non-zero.

Lemma 2.4.

(i) *Assume that $a_1 \neq 0$. If $|q_\tau| \leqslant 10^{-N}$ then $|\log|g_{\mathbf{a}}(\tau)| - \ell_{\mathbf{a}}\log|q_\tau|| \leqslant 3|q_\tau|^{1/N}$.*
(ii) *Assume that $a_1 = 0$. If $|q_\tau| \leqslant 0.1$ then $|\log|g_{\mathbf{a}}(\tau)| - \ell_{\mathbf{a}}\log|q_\tau| - \log|1 - \exp(2\pi\mathrm{i}a_2)|| \leqslant 3|q_\tau|$.*

The proof again uses estimates coming out of the q-product expansion for $g_{\mathbf{a}}$, as in [4, page 29]. See [1] for the details.

Lemma 2.5. *Assume that* $\mathbf{a} \in A_N$ *is of exact order* N'. *Then the functions* $g_{\mathbf{a}}$ *and* $(1-\zeta_{N'})g_{\mathbf{a}}^{-1}$ *are integral over* $\mathbb{Z}[j]$.

For the proof see [4, Sections 2.1 and 2.2], especially Lemma 2.1 and Theorem 2.2 therein. Though the statement of this theorem is formally weaker than our statement, what Kubert and Lang actually prove is exactly what we need.

Proof of Proposition 2.1. The statement of Proposition 2.1 is stable if one replaces Γ by the subgroup obtained by conjugating by $\mu \in \mathrm{SL}_2(\mathbb{Z})$, and P by P^μ in the conjugate modular curve. Since there exists μ such that P^μ is the image of an element of D, one can assume that P is the image of an element $\tau \in D$.

By [4, Theorem 2.3.2], when $\mathbf{a}$ runs through A_N, the principal divisors $(u_{\mathbf{a}})$ generate a finite index subgroup of the group of $\mathbb{Q}$-rational divisors of degree 0 supported on $\mathcal{C}$. Since $\mathcal{C}$ has at least two orbits under the action of the Galois group, there exist $\mathbb{Q}$-rational divisors of degree 0 supported on $\mathcal{C}$ and whose support contains the cusp c_∞, the image of $\mathrm{i}\infty$ in X_Γ. Hence there exists $\mathbf{a} \in A_N$ such that $\mathrm{ord}_\infty(u_{\mathbf{a}}) \neq 0$. Fix this $\mathbf{a}$ and estimate $|u_{\mathbf{a}}(P)| = |u_{\mathbf{a}}(\tau)|$ where, with a common abuse of notation, we view $u_{\mathbf{a}}$ as a function on $\mathcal{H}$ as well.

Using Lemma 2.4 (where we may assume that $|q_\tau| \leqslant 10^{-N}$, because otherwise Lemma 2.3 implies $|j(P)| \leqslant 10^{N+2}$), we find $\log|u_{\mathbf{a}}(\tau)| = \mathrm{ord}_{c_\infty}(u_{\mathbf{a}}) \log|q_\tau|^{1/e} + R$, where e is the ramification index of the covering $X_\Gamma \to X_{\mathrm{SL}_2(\mathbb{Z})}$ at c_∞ and $|R| \leqslant 12N|\bar{\Gamma}|(3|q|^{1/N} + \log 2) \leqslant 12N|\bar{\Gamma}|$. Here we bound by $\log 2$ each term of the type $\log|1-\exp(2\pi \mathrm{i} a_2)|$ coming from the second part of Lemma 2.4. Using that $\mathrm{ord}_{c_\infty}(u_{\mathbf{a}}) \neq 0$ and $e \leqslant N$, we obtain $|\log|u_{\mathbf{a}}(\tau)|| \geqslant N^{-1}\log|q|^{-1} - 12N|\bar{\Gamma}|$, and we complete the proof using Lemma 2.3. □

Proof of Proposition 2.2. Since P is not a cusp, we have $u_{\mathbf{a}}(P) \neq 0$. Since $u_{\mathbf{a}} \in \mathbb{Q}(X_\Gamma)$, we have $u_{\mathbf{a}}(P) \in \mathbb{Q}$. Further, Lemma 2.5 implies that $u_{\mathbf{a}}$ is integral over the ring $\mathbb{Z}[j]$, which implies that $u_{\mathbf{a}}(P)$ is integral over $\mathbb{Z}$, whence $u_{\mathbf{a}}(P) \in \mathbb{Z}$. This proves that $|u_{\mathbf{a}}(P)| \geqslant 1$.

Applying Lemma 2.5 again, we find in the similar fashion that $\Delta u_{\mathbf{a}}(P)^{-1} \in \mathbb{Z}[\zeta_N]$, where Δ is a product of at most $|\bar{\Gamma}|$ factors of the type $(1-\zeta_{N'})^{12N}$, with $N'|N$. Taking the norm, we find $u_{\mathbf{a}}(P)^{\varphi(N)}$ divides $\mathcal{N}_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(\Delta)$, which is a product of at most $|\bar{\Gamma}|$ factors of the type $\mathcal{N}_{\mathbb{Q}(\zeta_{\mathcal{N}})/\mathbb{Q}}(\infty - \zeta_{\mathcal{N}'})^{\infty \in \mathcal{N}}$. Every such factor divides $(N')^{12N\varphi(N)/\varphi(N')}$. Since $(N')^{1/\varphi(N')} \leqslant 2$, the result follows. □

3. Proof of Theorem 1.2

In this section p is a prime number, $n \geqslant 1$ is an integer, and E is a non-CM elliptic curve over $\mathbb{Q}$ such that the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{GL}(E[p^n]) \simeq \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ is the normalizer of a split Cartan subgroup mod p^n as defined in the introduction. We denote by N_E the conductor of E. Note that if E' is any (quadratic) twist of E, then the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{GL}(E'[p^n])$ is again the normalizer of a split Cartan subgroup.

Proposition 3.1. *Assume GRH. For any* $\varepsilon > 0$ *there exists an absolute effective constant* γ_ε *such that, when* $p > \gamma_\varepsilon$, *we have* $p^n \leqslant (\log N_E)^{1+\varepsilon}$.

Proof. This is a straightforward generalization of an argument of Halberstadt and Kraus [3], which makes use of Serre's explicit version of Chebotarev's theorem [9]. It follows from Mazur's celebrated theorem on rational isogenies that the image of $G_{\mathbb{Q}}$ in $\mathrm{GL}(E[p^n](\overline{\mathbb{Q}}))$, which is in the normalizer $\mathfrak{N}$ of a Cartan subgroup $\mathfrak{C}$ by assumption, is not included in $\mathfrak{C}$ itself. Let χ be the quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ defined by $\mathfrak{N}/\mathfrak{C}$. Let E' by the twist of E by χ. The conductors of E' and E are equal by [3, Théorème 1].

For any prime number ℓ not dividing pN_E, the traces $a_\ell(E)$ and $a_\ell(E')$ of a Frobenius substitution Frob_ℓ at the place ℓ acting on the p-adic Tate modules of E and E' satisfy $a_\ell(E) = a_\ell(E')\chi(\ell)$. Since E has no CM, the curves E and E' are not isogeneous. Let ℓ be the smallest prime number not dividing N_E such that $a_\ell(E) \neq a_\ell(E')$. Assuming GRH, it satisfies $\ell \leqslant c(\log N_E)^2(\log\log 2N_E)^{12}$, where c is an absolute constant, by Théorème 21 of [9]. Moreover one has $a_\ell(E) \neq 0$ and $\chi(\ell) = -1$, i.e. $\mathrm{Frob}_\ell \in \mathfrak{N} \setminus \mathfrak{C}$, which implies that $a_\ell(E) \equiv 0 \bmod p^n$. Now Hasse's bounds imply that $p^n \leqslant 2\sqrt{\ell}$, which yields the conclusion of the proposition. □

Proof of Theorem 1.2. Let P be a non-CM non-cuspidal point in $X_{\mathrm{split}}(p^n)(\mathbb{Q})$, giving rise to an elliptic curve E. As P induces a point in $X_{\mathrm{split}}(p)(\mathbb{Q})$, it follows from results of Momose and Merel that, if $p > 13$, then $j = j(E)$ belongs to $\mathbb{Z}$, cf. [6, Theorem 3.1]. Replacing E, if necessary, by a quadratic twist, we may assume that, if $\ell \geqslant 5$ is a

prime number dividing N_E, then ℓ divides[1] either j or $j-1728$. The curve E has potentially good reduction at all primes, so $\mathrm{val}_\ell(N_E)=2$, and the exponents of the conductor at 2 and 3 are at most 8 and 5 respectively. Therefore $N_E \leqslant 2^8\cdot 3^5\cdot j^2(j-1728)^2$.

Now applying Theorem 1.1 to the curve $X_{\mathrm{split}}(p)$ (which has two Galois orbits of cusps) we obtain $\log|j(P)| = \mathrm{O}(p^4)$. On the other hand, by Proposition 3.1, for any $\varepsilon>0$ and large enough p one has $p^n \leqslant (\log N_E)^{1+\varepsilon}$. This implies that $p^n \leqslant p^{4+\varepsilon}$ for large p, so that $n\leqslant 4$. □

Acknowledgements

We thank H. Cohen, V. Vatsal and Yu. Zarhin for useful discussions. We thank the anonymous referee for a thorough report which helped us to improve on the presentation, and for drawing our attention to the work of Pellarin.

References

[1] Yu. Bilu, P. Parent, Explicit bounds for integral j-invariants and level of Cartan structures for elliptic curves, in preparation.
[2] E. Bombieri, On Weil's "théorème de décomposition", Amer. J. Math. 105 (1983) 295–308.
[3] E. Halberstadt, A. Kraus, Sur les modules de torsion des courbes elliptiques, Math. Ann. 310 (1998) 47–54.
[4] D.S. Kubert, S. Lang, Modular Units, Grundlehren der Mathematischen Wissenschaften, vol. 244, Springer-Verlag, New York-Berlin, 1981, xiii+358 pp.
[5] D.W. Masser, G. Wüstholz, Galois properties of division fields of elliptic curves, Bull. London Math. Soc. 25 (1993) 247–254.
[6] L. Merel, Normalizers of split Cartan subgroups and supersingular elliptic curves, in: Proceedings of the conference, Diophantine Geometry, Pisa, 2005.
[7] F. Pellarin, Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques, Acta Arith. 100 (2001) 203–243.
[8] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259–331.
[9] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, Publ. Math. IHES 54 (1981) 323–401.
[10] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Publ. Math. Soc. Japan, vol. 11, Iwanami Shoten, Tokyo, 1971, Princeton University Press, Princeton, NJ.

[1] Consider, for instance, the Weierstrass equation

$$(\mathcal{E}):\quad y^2+xy=x^3-\frac{36}{j-1728}x-\frac{1}{j-1728},$$

having discriminant $j^2/(j-1728)^3$. It defines an elliptic curve E_1 over $\mathbb{Q}$ with j-invariant equal to j, so E_1 is a quadratic twist of E over $\mathbb{Q}$. For ℓ a prime not dividing $j(j-1728)$ the equation $(\mathcal{E})$ defines a smooth model for E_1 over $\mathbb{Z}_{(\ell)}$, the localization of $\mathbb{Z}$ at ℓ. Therefore the minimal Weierstrass equation for E_1 over $\mathbb{Z}$ defines a scheme which is smooth over $\mathbb{Z}_{(\ell)}$, which means that ℓ does not divide the conductor of E_1.