Annals of Mathematics **173** (2011), 569–584
doi: 10.4007/annals.2011.173.1.13

Serre's uniformity problem in the split Cartan case

By Yuri Bilu and Pierre Parent

Abstract

We prove that there exists an integer p_0 such that $X_{\mathrm{split}}(p)(\mathbb{Q})$ is made of cusps and CM-points for any prime $p > p_0$. Equivalently, for any non-CM elliptic curve E over $\mathbb{Q}$ and any prime $p > p_0$ the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by the representation induced by the Galois action on the p-division points of E is not contained in the normalizer of a split Cartan subgroup. This gives a partial answer to an old question of Serre.

1. Introduction

Let N be a positive integer and G a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\det G = (\mathbb{Z}/N\mathbb{Z})^\times$. Then the corresponding modular curve X_G, defined as a complex curve as $\overline{\mathcal{H}}/\Gamma$, where $\overline{\mathcal{H}}$ is the extended Poincaré upper half-plane and Γ is the pullback of $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z})$, is actually defined over $\mathbb{Q}$, that is, it has a geometrically integral $\mathbb{Q}$-model. As usual, we denote by Y_G the finite part of X_G (that is, X_G deprived of the cusps). The curve X_G has a natural (modular) model over $\mathbb{Z}$ that we still denote by X_G. The cusps define a closed subscheme of X_G over $\mathbb{Z}$, and we define the relative curve Y_G over $\mathbb{Z}$ as X_G deprived of the cusps. The set of integral points $Y_G(\mathbb{Z})$ consists of those $P \in Y_G(\mathbb{Q})$ for which $j(P) \in \mathbb{Z}$, where j is, as usual, the modular invariant.

In the special case when G is the normalizer of a split (or nonsplit) Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the curve X_G is denoted by $X_{\mathrm{split}}(N)$ (or $X_{\mathrm{nonsplit}}(N)$, respectively). In this article we focus more precisely on the case when G is the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for p a prime number, that is, G is conjugate to the set of diagonal and anti-diagonal matrices mod p, and we prove the following theorem.

Theorem 1.1. *There exists an absolute effective constant C such that for any prime number p and any $P \in Y_{\mathrm{split}}(p)(\mathbb{Z})$, $\log|j(P)| \le 2\pi p^{1/2} + 6\log p + C$.*

This is proved in Section 4, by a variation of the method of Runge after some preparation in Sections 2 and 3. The terms $2\pi p^{1/2}$ and $6 \log p$ seem to be optimal for the method. The constant C may probably be replaced by $o(1)$ when p tends to infinity.

We apply Theorem 1.1 to the arithmetic of elliptic curves. Serre proved [23] that for any elliptic curve E without complex multiplication (CM in the sequel), there exists $p_0(E) > 0$ such that for every prime $p > p_0(E)$ the natural Galois representation

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p]) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

is surjective. Masser and Wüstholz [14], Kraus [10], and Pellarin [21] gave effective versions of Serre's result; for more recent work, see, for instance, Cojocaru and Hall [6], [7].

Serre asked whether p_0 can be made independent of E:

> *Does there exist an absolute constant p_0 such that for any non-*CM *elliptic curve E over $\mathbb{Q}$ and any prime $p > p_0$ the Galois representation $\rho_{E,p}$ is surjective?*

We refer to this as "Serre's uniformity problem". The general guess is that $p_0 = 37$ would probably do.

The group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has the following types of maximal proper subgroups: normalizers of (split and nonsplit) Cartan subgroups, Borel subgroups, and "exceptional" subgroups (those whose projective image is isomorphic to one of the groups A_4, S_4 or A_5). To solve Serre's uniformity problem, one has to show that for sufficiently large p, the image of the Galois representation is not contained in any of the above listed maximal subgroups. (See [16, §2] for an excellent introduction into this topic.) Serre himself settled the case of exceptional subgroups (see the introduction of [15]), and the work of Mazur [17] on rational isogenies implies Serre uniformity for the Borel subgroups; so to solve Serre's problem we are left with the Cartan cases. Equivalently, one would like to prove that, for large p, the only rational points of the modular curves $X_{\mathrm{split}}(p)$ and $X_{\mathrm{nonsplit}}(p)$ are the cusps and CM points, in which case we will say that the rational points are *trivial.*

In the present article we solve the split Cartan case of Serre's problem.

THEOREM 1.2. *There exists an absolute constant p_0 such that for $p > p_0$ every point in $X_{\mathrm{split}}(p)(\mathbb{Q})$ is either a* CM *point or a cusp.*

In other words, for any non-CM elliptic curve E over $\mathbb{Q}$ and any prime $p > p_0$ the image of the Galois representation $\rho_{E,p}$ is not contained in the normalizer of a split Cartan subgroup.

Several partial results in this direction were available before. In [20], [22] it was proved, by very different techniques, that $X_{\mathrm{split}}(p)(\mathbb{Q})$ is trivial for a (large) positive density of primes; but the methods of loc. cit. have failed to prevent a complementary set of primes from escaping them. In [2] we allowed ourselves to consider Cartan structures modulo higher powers of primes, and showed that, assuming the Generalized Riemann Hypothesis, $X_{\mathrm{split}}(p^5)(\mathbb{Q})$ is trivial for large enough p.

Regarding possible generalizations, note that Runge's method applies to the study of integral points on an affine curve Y, defined over $\mathbb{Q}$, if the following *Runge condition* is satisfied:

$$\text{(R)} \qquad \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \text{ acts nontransitively on the set } X \setminus Y,$$

where X is the projectivization of Y. The Runge condition is satisfied for the curve $X_{\mathrm{split}}(p)$ because it has two Galois orbits of cusps over $\mathbb{Q}$. Runge's method also applies to other modular curves such as $X_0(p)$, but, unfortunately, it does not work (under the form we use) with $X_{\mathrm{nonsplit}}(p)$, because all cusps of this curve are conjugate over $\mathbb{Q}$ and the Runge condition fails. Moreover, we need a weak version of Mazur's method to obtain integrality of rational points, and this is believed not to apply to $X_{\mathrm{nonsplit}}(p)$, because (the parity part of) the Birch and Swinnerton-Dyer conjecture predicts that the Jacobian of the latter curve has no nontrivial quotient of rank 0 over $\mathbb{Q}$; see [5] for more details. Actually, it is of interest that the Euler system constructed by Kato [9] to prove the triviality of the rank of Jacobian quotients in the modular cases relies on the same Siegel functions as those we use in Runge's method; so it seems that both obstructions in applying our method to the nonsplit case come from the lack of sufficiently many Galois orbits of cusps over $\mathbb{Q}$. Several other applications of our techniques are however possible, and at present we work on applying Runge's method to general modular curves over general number fields; see [2], [3]. For more on Runge's method the reader may consult [4], [12].

Acknowledgments. We thank Daniel Bertrand, Imin Chen, Henri Cohen, Bas Edixhoven, Loïc Merel, Joseph Oesterlé, Federico Pellarin, Vinayak Vatsal, and Yuri Zarhin for stimulating discussions and useful suggestions. We also thank the anonymous referee for thorough reading of the manuscript.

Yuri Bilu thanks Michael Sazonov for hospitality and Elina Wojciechowska for inspiration on July 19, 2008 in the Swiss Alps, where one of the key ideas of his contribution to this work emerged.

Pierre Parent dedicates this work to Éric Sopena and Christophe Bavard.

Convention. Everywhere in this article the $O(\cdot)$-notation, as well as the Vinogradov notation "$\ll$" implies absolute effective constants.

2. **Siegel functions**

As above, we denote by $\mathcal{H}$ the Poincaré upper half-plane and put $\overline{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$. For $\tau \in \mathcal{H}$, as usual we put $q = q(\tau) = e^{2\pi i \tau}$. For a rational number a we define $q^a = e^{2\pi i a \tau}$. Let $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2$ be such that $\mathbf{a} \notin \mathbb{Z}^2$, and let $g_{\mathbf{a}} : \mathcal{H} \to \mathbb{C}$ be the corresponding *Siegel function* [11, §2.1]. Then we have the following infinite product presentation for $g_{\mathbf{a}}$ [11, p. 29]:

$$g_{\mathbf{a}}(\tau) = -q^{B_2(a_1)/2} e^{\pi i a_2(a_1-1)} \prod_{n=0}^{\infty} \left(1 - q^{n+a_1} e^{2\pi i a_2}\right)\left(1 - q^{n+1-a_1} e^{-2\pi i a_2}\right), \tag{1}$$

where $B_2(T) = T^2 - T + 1/6$ is the second Bernoulli polynomial. We also have [11, pp. 27–30] the relations

$$g_{\mathbf{a}} \circ \gamma = g_{\mathbf{a}\gamma} \cdot (\text{a root of unity}) \quad \text{for} \quad \gamma \in \mathrm{SL}_2(\mathbb{Z}), \tag{2}$$

$$g_{\mathbf{a}} = g_{\mathbf{a}'} \cdot (\text{a root of unity}) \quad \text{when} \quad \mathbf{a} \equiv \mathbf{a}' \mod \mathbb{Z}^2. \tag{3}$$

Note that the root of unity in (2) is of order dividing 12, and in (3) of order dividing $2N$, where N is the denominator of $\mathbf{a}$ (the common denominator of a_1 and a_2). (For (2) use properties **K 0** and **K 1** of loc. cit., and for (3) use **K 3** and the fact that Δ is modular of weight 12.) Moreover,

$$g_{\mathbf{a}} \circ \gamma = g_{\mathbf{a}} \cdot (\text{a root of unity}) \quad \text{for} \quad \gamma \in \Gamma(N), \tag{4}$$

the root of unity being of order dividing $12N$, because $g_{\mathbf{a}}^{12N}$ is a modular function on $\Gamma(N)$ by Theorem 1.2 in [11, p. 31].

The following is immediate from (1).

PROPOSITION 2.1. *Assume that $0 \le a_1 < 1$. Then for $\tau \in \mathcal{H}$ satisfying $|q(\tau)| \le 0.1$,*

$$\log|g_{\mathbf{a}}(\tau)| = \frac{1}{2}B_2(a_1)\log|q| + \log\left|1 - q^{a_1}e^{2\pi i a_2}\right| + \log\left|1 - q^{1-a_1}e^{-2\pi i a_2}\right| + O(|q|)$$

(*where we recall that, throughout this article, the notation $O(\cdot)$ as well as $\ll$ imply absolute effective constants*).

For $\mathbf{a} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ the Siegel function $g_{\mathbf{a}}$ is algebraic over the field $\mathbb{C}(j)$. This again follows from the fact that $g_{\mathbf{a}}^{12N}$ is $\Gamma(N)$-automorphic, where, as above, N is the denominator of $\mathbf{a}$. Since $g_{\mathbf{a}}$ is holomorphic and does not vanish on the upper half-plane $\mathcal{H}$ (again by Theorem 1.2 of loc. cit.), both $g_{\mathbf{a}}$ and $g_{\mathbf{a}}^{-1}$ must be integral over the ring $\mathbb{C}[j]$. Actually, a stronger assertion holds.

PROPOSITION 2.2. *Both $g_{\mathbf{a}}$ and $(1-\zeta_N)g_{\mathbf{a}}^{-1}$ are integral over $\mathbb{Z}[j]$. Here N is the denominator of $\mathbf{a}$ and ζ_N is a primitive N-th root of unity.*

This is, essentially, established in [11], but is not stated explicitly therein. Therefore we briefly indicate the proof here. A $\Gamma(N)$-automorphic function $f : \mathcal{H} \to \mathbb{C}$ admits the infinite q-expansion

$$f(\tau) = \sum_{k \in \mathbb{Z}} a_k q^{k/N}. \tag{5}$$

We call the q-series (5) *algebraic integral* if the following two conditions are satisfied: the negative part of (5) has only finitely many terms (that is, $a_k = 0$

for large negative k), and the coefficients a_k are algebraic integers. Algebraic integral q-series form a ring. The invertible elements of this ring are q-series with invertible leading coefficient. By the *leading coefficient* of an algebraic integral q-series we mean a_m, where $m \in \mathbb{Z}$ is defined by $a_m \neq 0$, but $a_k = 0$ for $k < m$.

LEMMA 2.3. *Let f be a $\Gamma(N)$-automorphic function regular on $\mathcal{H}$ such that for every $\gamma \in \Gamma(1)$ the q-expansion of $f \circ \gamma$ is algebraic integral. Then f is integral over $\mathbb{Z}[j]$.*

Proof. This is, essentially, Lemma 2.1 from [11, §2.2]. Since f is $\Gamma(N)$-automorphic, the set $\{f \circ \gamma : \gamma \in \Gamma(1)\}$ is finite. The coefficients of the polynomial $F(T) = \prod(T - f \circ \gamma)$ (where the product is taken over the finite set above) are $\Gamma(1)$-automorphic functions with algebraic integral q-expansions. Since they have no pole on $\mathcal{H}$, they belong to $\mathbb{C}[j]$ and even to $\overline{\mathbb{Z}}[j]$, where $\overline{\mathbb{Z}}$ is the ring of all algebraic integers, because the coefficients of their q-expansions are algebraic integers. It follows that f is integral over $\overline{\mathbb{Z}}[j]$, hence over $\mathbb{Z}[j]$. □

Proof of Proposition 2.2. The function $g_{\mathbf{a}}^{12N}$ is automorphic of level N and its q-expansion is algebraic integral (as one can easily see by transforming the infinite product (1) into an infinite series). By (2), the same is true for every $(g_{\mathbf{a}} \circ \gamma)^{12N}$. Lemma 2.3 now implies that $g_{\mathbf{a}}^{12N}$ is integral over $\mathbb{Z}[j]$, and so is $g_{\mathbf{a}}$.

Further, the q-expansion of $g_{\mathbf{a}}$ is invertible if $a_1 \notin \mathbb{Z}$ and is $1 - e^{\pm 2\pi i a_2}$ times an invertible q-series if $a_1 \in \mathbb{Z}$. Hence the q-expansion of $g_{\mathbf{a}}^{-1}$ is algebraic integral when $a_1 \notin \mathbb{Z}$, and if $a_1 \in \mathbb{Z}$ the same is true for $\left(1 - e^{\pm 2\pi i a_2}\right) g_{\mathbf{a}}^{-1}$.

In the latter case N is the exact denominator of a_2, which implies that $(1 - \zeta_N)/(1 - e^{\pm 2\pi i a_2})$ is an algebraic unit. Hence, in any case, $(1 - \zeta_N) g_{\mathbf{a}}^{-1}$ has algebraic integral q-expansion, and the same is true with $g_{\mathbf{a}}$ replaced by $g_{\mathbf{a}} \circ \gamma$ for any $\gamma \in \Gamma(1)$. (We again use (2) and notice that $\mathbf{a}$ and $\mathbf{a}\gamma$ have the same order in $(\mathbb{Q}/\mathbb{Z})^2$.) Applying Lemma 2.3 to the function $\left((1 - \zeta_N) g_{\mathbf{a}}^{-1}\right)^{12N}$, we complete the proof. □

3. A modular unit

In this section we define a special "modular unit" (in the spirit of [11]) and study its asymptotic behavior at infinity. With the common abuse of speech, the modular invariant j, as well as the other modular functions used below, may be viewed, depending on the context, as either automorphic functions on the Poincaré upper half-plane, or rational functions on the corresponding modular curves.

Since the root of unity in (3) is of order dividing $2N$, where N is a denominator of $\mathbf{a}$, the function $g_{\mathbf{a}}^{12N}$ will be well-defined if we select $\mathbf{a}$ in the set $\left(N^{-1}\mathbb{Z}/\mathbb{Z}\right)^2$. Thus, fix a positive integer N and for a nonzero element $\mathbf{a}$ of $(N^{-1}\mathbb{Z}/\mathbb{Z})^2$ put $u_{\mathbf{a}} = g_{\mathbf{a}}^{12N}$. After fixing a choice for ζ_N in $\mathbb{C}$ (for instance $\zeta_N = e^{2i\pi/N}$), we see that the analytic modular curve $X(N)(\mathbb{C}) := \overline{\mathcal{H}}/\Gamma(N)$ has a modular model over $\mathbb{Q}(\zeta_N)$, parametrizing isomorphism classes of generalized elliptic curves endowed with a basis (S,T) of $E[N]$ such that the Weil pairing of S with T is ζ_N. As already noticed, the function $u_{\mathbf{a}}$ is $\Gamma(N)$-automorphic and hence defines a rational function on the modular curve $X(N)(\mathbb{C})$; in fact, it belongs to the field $\mathbb{Q}(\zeta_N)\big(X(N)\big)$. The Galois group of the latter field over $\mathbb{Q}(j)$ is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm1\}$, and we may identify the two groups to make the Galois action compatible with the natural action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $(N^{-1}\mathbb{Z}/\mathbb{Z})^2$ in the following sense: for any $\overline{\sigma} \in \mathrm{Gal}\Big(\mathbb{Q}\big(X(N)\big)/\mathbb{Q}(j)\Big) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm1\}$ and any nonzero $\mathbf{a} \in (N^{-1}\mathbb{Z}/\mathbb{Z})^2$ we have $u_{\mathbf{a}}^{\overline{\sigma}} = u_{\mathbf{a}\sigma}$, where $\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is a pullback of $\overline{\sigma}$. Notice that $u_{\mathbf{a}} = u_{-\mathbf{a}}$, which follows from (2). For the proof of the statements above the reader may consult [11, pp. 31–36], and especially Theorem 1.2, Proposition 1.3 and the beginning of Section 2.2 therein.

From now on we assume that $N = p \geq 3$ is an odd prime number, and that G is the normalizer of the diagonal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. In this case the curve $X_G = X_{\mathrm{split}}(p)$ has two Galois orbits of cusps over $\mathbb{Q}$, the first being the cusp at infinity, which is $\mathbb{Q}$-rational (we denote it by ∞), and the second consisting of the $(p-1)/2$ other cusps (denoted by $P_1, \ldots, P_{(p-1)/2}$), which are defined over the real cyclotomic field $\mathbb{Q}(\zeta_p)^+$. According to the theorem of Manin-Drinfeld, there exists $U \in \mathbb{Q}(X_G)$ such that the principal divisor (U) is of the form

$$m\big((p-1)/2 \cdot \infty - (P_1 + \cdots + P_{(p-1)/2})\big)$$

with some positive integer m. Below we use Siegel functions to find such U explicitly with $m = 2p(p-1)$. See Remark 3.4 for a more precise statement.

Remark 3.1. (a) The general form of units we build is more ripe for generalization, but in the present case, using the $\mathbb{Q}$-isomorphism between $X_{\mathrm{split}}(p)$ and $X_0(p^2)/w_p$, our unit could probably be expressed in terms of (products of) modular forms of shape $\Delta(nz)$.

(b) The assumption that $p \geq 3$ is purely technical: the content of this section extends, with insignificant changes, to $p = 2$.

Denote by $p^{-1}\mathbb{F}_p^\times$ the set of nonzero elements of $p^{-1}\mathbb{Z}/\mathbb{Z}$. Then the set

$$A = \left\{(a,0) : a \in p^{-1}\mathbb{F}_p^\times\right\} \cup \left\{(0,a) : a \in p^{-1}\mathbb{F}_p^\times\right\}$$

is G-invariant. Hence the function

$$U = \prod_{\mathbf{a}\in A} u_{\mathbf{a}}$$

belongs to the field $\mathbb{Q}(X_G)$. In particular, viewed as a function on $\mathcal{H}$, it is Γ-automorphic, where Γ is the pullback to $\Gamma(1)$ of $G \cap \mathrm{SL}_2(\mathbb{F}_p)$.

More generally, for $c \in \mathbb{Z}$ put

$$\beta_c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \qquad U_c = U \circ \beta_c = \prod_{\mathbf{a} \in A\beta_c} u_{\mathbf{a}}$$

(so that $U = U_0$).

Let D be the familiar fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$; that is, the hyperbolic triangle with vertices $e^{\pi i/3}$, $e^{2\pi i/3}$ and $i\infty$, together with the geodesic segments $[i, e^{2\pi i/3}]$ and $[e^{2\pi i/3}, i\infty]$. Let $D + \mathbb{Z}$ be the union of all translates of D by the rational integers. Recall also that j denotes the modular invariant.

Lemma 3.2. *For any $P \in Y_G(\mathbb{C})$ there exists $c \in \mathbb{Z}$ (even $c \in \{0, \dots$ $\dots, (p-1)/2\}$) and $\tau \in D + \mathbb{Z}$ such that $j(\tau) = j(P)$ and $U_c(\tau) = U(P)$.*

Proof. Let $\tau' \in \mathcal{H}$ be such that $j(\tau') = j(P)$ and $U(\tau') = U(P)$. There exists $\beta \in \Gamma(1)$ such that $\beta^{-1}(\tau') \in D$. Now observe that the set $\{\beta_0, \dots, \beta_{(p-1)/2}\}$ is a full system of representatives of the double cosets $\Gamma\backslash\Gamma(1)/\Gamma_\infty$, where Γ_∞ is the subgroup of $\Gamma(1)$ stabilizing ∞. Thus we may write $\beta = \gamma\beta_c\kappa$ with $\gamma \in \Gamma$, $c \in \{0, \dots, \lfloor p/2 \rfloor\}$ and $\kappa \in \Gamma_\infty$. Then $\tau = \kappa\beta^{-1}(\tau')$ is as desired. □

Proposition 3.3. *For $\tau \in \mathcal{H}$ such that $|q(\tau)| \le 1/p$,*

$$\Big|\log|U_c(\tau)| - (p-1)^2 \log|q(\tau)|\Big| \le 4\pi^2 \frac{p^2}{\log|q(\tau)^{-1}|} + O(p \log p) \tag{6}$$

if $p \mid c$, and

$$\Big|\log|U_c(\tau)| + 2(p-1)\log|q(\tau)|\Big| \le 8\pi^2 \frac{p^2}{\log|q(\tau)^{-1}|} + O(p) \tag{7}$$

if $p \nmid c$.

Remark 3.4. As suggested by the referee, it might perhaps be illuminating to re-state this proposition not in terms of U_c and q, but in terms of the original function U and the "q-parameter" $q_c = q \circ \beta_c^{-1}$ at the cusp $\beta_c(\infty)$. From this point of view (which is systematically taken in [3]) the proposition means that U behaves like $q_c^{(p-1)^2}$ near the cusp at infinity and like $q_c^{-2(p-1)}$ near the other cusps. Since $q_c^{1/p}$ is a uniformizer at the cusp $\beta_c(\infty)$, this implies, in particular, that the principal divisor (U) is $m\big((p-1)/2 \cdot \infty - (P_1 + \dots + P_{(p-1)/2})\big)$ with $m = 2p(p-1)$, as indicated above.

For the proof of Proposition 3.3 we need an elementary, but crucial lemma.

LEMMA 3.5. *Let z be a complex number, $|z|<1$, and N a positive integer. Then*

$$\left|\sum_{k=1}^{N}\log\left|1-z^k\right|\right| \le \frac{\pi^2}{6}\frac{1}{\log|z^{-1}|}+O(1). \tag{8}$$

Proof. We have $\left|\log|1+z|\right| \le -\log\left|1-|z|\right|$ for $|z|<1$. Applying this with $-z^k$ instead of z, we conclude that it suffices to bound $-\sum_{k=1}^{\infty}\log|1-q^k|$ with $q=|z|$. Since the left-hand side of (8) is bounded (independently of N) for $|z|\le 1/2$, we may assume that

$$1/2 \le q < 1. \tag{9}$$

Put $\tau=\log q/(2\pi i)$. Then

$$-\sum_{k=1}^{\infty}\log|1-q^k| = \frac{1}{24}\log q-\log|\eta(\tau)|,$$

where $\eta(\tau)$ is the Dedekind η-function. Since $|\eta(\tau)|=|\tau|^{-1/2}|\eta(-\tau^{-1})|$, we have

$$-\sum_{k=1}^{\infty}\log|1-q^k| = -\frac{1}{24}\log|Q|+\frac{1}{24}\log q+\frac{1}{2}\log|\tau|-\sum_{k=1}^{\infty}\log|1-Q^k| \tag{10}$$

with $Q=e^{-2\pi i\tau^{-1}}=e^{4\pi^2/\log q}$. The first term on the right-hand side of (10) is exactly $(\pi^2/6)/\log|z^{-1}|$, the second term is negative, the third term is again negative (here we use (9)), and the infinite sum is $O(1)$, again by (9). The lemma is proved. □

Proof of Proposition 3.3. Write $q=q(\tau)$. Recall that for a rational number α we define $q^\alpha=e^{2\pi i\alpha\tau}$. For $a\in\mathbb{Q}/\mathbb{Z}$ we denote by $\tilde{a}$ the lifting of a to the interval $[0,1)$. Then for $\tau\in\mathcal{H}$ satisfying $|q|\le 0.1$ we deduce from Proposition 2.1 that

(11)

$$\begin{aligned}\log|U_c(\tau)| &= 6p\sum_{\mathbf{a}\in A\beta_c}B_2(\tilde{a}_1)\log|q| \\ &\quad+12p\sum_{\mathbf{a}\in A\beta_c}\left(\log\left|1-q^{\tilde{a}_1}e^{2\pi i a_2}\right|+\log\left|1-q^{1-\tilde{a}_1}e^{-2\pi i a_2}\right|\right)+O(p^2|q|).\end{aligned}$$

The rest of the proof splits into two cases and relies on the identity

$$\sum_{k=1}^{N-1}B_2\left(\frac{k}{N}\right) = -\frac{(N-1)}{6N}.$$

The first case: $p \mid c$. In this case $A\beta_c = A$. Hence

$$\sum_{\mathbf{a}\in A\beta_c} B_2(\tilde{a}_1) = \sum_{k=1}^{p-1} B_1\left(\frac{k}{p}\right) + (p-1)B_2(0) = \frac{(p-1)^2}{6p}. \tag{12}$$

Further,

$$\sum_{\mathbf{a}\in A\beta_c} \left(\log\left|1 - q^{\tilde{a}_1}e^{2\pi i a_2}\right| + \log\left|1 - q^{1-\tilde{a}_1}e^{-2\pi i a_2}\right|\right) \tag{13}$$
$$= 2\sum_{k=1}^{p-1} \log\left|1 - q^{k/p}\right| + \log\left|\frac{1-q^p}{1-q}\right| + \log p.$$

Lemma 3.5 with $z = q^{1/p}$ implies that

$$\sum_{k=1}^{p-1} \log\left|1 - q^{k/p}\right| \le \frac{\pi^2}{6}\frac{p}{\log|q^{-1}|} + O(1).$$

Also, $\log|1-q^p| \ll |q|^p$ and $\log|1-q| \ll |q|$. Combining all this with (11), (12) and (13), we obtain (6).

The second case: $p \nmid c$. In this case

$$A\beta_c = \{(a,0) : a \in p^{-1}\mathbb{F}_p^\times\} \cup \{(a,ab) : a \in p^{-1}\mathbb{F}_p^\times\},$$

where $b \in \mathbb{Z}$ satisfies $bc \equiv 1 \bmod p$. Hence

$$\sum_{\mathbf{a}\in A\beta_c} B_2(\tilde{a}_1) = 2\sum_{k=1}^{p-1} B_2\left(\frac{k}{p}\right) = -\frac{p-1}{3p}.$$

Further,

$$\sum_{\mathbf{a}\in A\beta_c} \left(\log\left|1 - q^{\tilde{a}_1}e^{2\pi i a_2}\right| + \log\left|1 - q^{1-\tilde{a}_1}e^{-2\pi i a_2}\right|\right)$$
$$= 2\sum_{k=1}^{p-1} \log\left|1 - q^{k/p}\right| + 2\sum_{k=1}^{p-1} \log\left|1 - (q^{1/p}e^{2\pi i b/p})^k\right|.$$

Again using Lemma 3.5, we complete the proof. $\square$

4. Proof of Theorem 1.1

In this section p is a prime number and G is the normalizer of the diagonal subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Define the "modular units" U_c as in Section 3. Recall that $U = U_0$ belongs to the field $\mathbb{Q}(X_G)$. Theorem 1.1 is a consequence of the following two statements.

PROPOSITION 4.1. *Assume that $p \geq 3$. For any $P \in Y_G(\mathbb{C})$ we have either*

$$\log|j(P)| \leq 2\pi p^{1/2} + 6\log p + O(1)$$

or

$$\log|j(P)| \leq \frac{1}{2(p-1)}\Big|\log|U(P)|\Big| + 2\pi p^{1/2} - 6\log p + O\big(1\big). \tag{14}$$

PROPOSITION 4.2. *For $P \in Y_G(\mathbb{Z})$ we have $0 \leq \log|U(P)| \leq 24p\log p$.*

Combining the two propositions, we find that for $P \in Y_{\mathrm{split}}(p)(\mathbb{Z})$ we have

$$\log|j(P)| \leq 2\pi p^{1/2} + 6\log p + O(1),$$

which proves Theorem 1.1 for $p \geq 3$.

A similar approach can be used for $p = 2$ as well, but in this case it is easier to appeal to the general Runge theorem: If an affine curve Y, defined over $\mathbb{Q}$, has 2 (or more) rational points at infinity, then integral points on Y are effectively bounded; see, for instance, [4], [12].

Proof of Proposition 4.1. According to Lemma 3.2, there exist $\tau \in D + \mathbb{Z}$ and $c \in \mathbb{Z}$ with $U_c(\tau) = U(P)$ and $j(\tau) = j(P)$. (As in Remark 3.4, one may say here that P is "close" to the cusp $\beta_c(\infty)$ with respect to the archimedean metric on our curve.) We write $q = q(\tau)$. Since $\tau \in D + \mathbb{Z}$, we have

$$j(\tau) = q^{-1} + O(1), \tag{15}$$

which implies that either $\log|j(P)| \leq 2\pi p^{1/2} + 6\log p + O(1)$ or $\log|q^{-1}| \geq 2\pi p^{1/2} + 6\log p$. In the latter case we apply Proposition 3.3. When $p \nmid c$ it yields

$$\begin{aligned}\left|\log|q| + \frac{1}{2(p-1)}\log|U_c(\tau)|\right| &\leq \frac{8\pi^2p^2}{2(p-1)(2\pi p^{1/2} + 6\log p)} + O(1)\\ &= 2\pi p^{1/2} - 6\log p + O(1),\end{aligned}$$

which, together with (15), implies the result. In the case $p \mid c$ Proposition 3.3 gives

$$\left|\log|q| - \frac{1}{(p-1)^2}\log|U_c(\tau)|\right| \leq \frac{4\pi^2p^2}{(p-1)^2(2\pi p^{1/2} + 6\log p)} + O(1) = O(1),$$

which implies an even better bound than needed. □

Proof of Proposition 4.2. Since U belongs to $\mathbb{Q}(X_G)$ and has no pole or zero outside the cusps, $U(P)$ is a nonzero rational number. Let $\zeta = \zeta_p$ be a primitive p-th root of unity. Since U is a product of $24p(p-1)$ Siegel functions, Proposition 2.2 implies that both U and $(1-\zeta)^{24p(p-1)}U^{-1}$ are integral over $\mathbb{Z}[j]$. Hence for $P \in Y_G(\mathbb{Z})$ both the numbers $U(P)$ and $(1-\zeta)^{24p(p-1)}U(P)^{-1}$ are algebraic integers. Since $U(P) \in \mathbb{Q}^\times$, it is a nonzero rational integer; in particular, $\log|U(P)| \geq 0$. Further, $U(P)$ divides $(1-\zeta)^{24p(p-1)}$. Taking the $\mathbb{Q}(\zeta)/\mathbb{Q}$-norm, we see that $U(P)^{p-1}$ divides $p^{24p(p-1)}$. This proves the proposition. □

5. Proof of Theorem 1.2

First of all, recall the following *integrality property* of the j-invariant.

THEOREM 5.1 (Mazur, Momose, Merel). *For a prime $p = 11$ or $p \geq 17$, the j-invariant $j(P)$ of any noncuspidal point of $X_{\mathrm{split}}(p)(\mathbb{Q})$ belongs to $\mathbb{Z}$.*

This is a combination of results of Mazur [17], Momose [19], and Merel [18]. For more details see the Appendix (§6), where we give a short unified proof.

Denote by $\mathrm{h}(\alpha)$ the absolute logarithmic height of an algebraic number α. If α is a nonzero rational integer, then $\mathrm{h}(\alpha) = \log|\alpha|$. It follows from Theorem 5.1 that if E is an elliptic curve over $\mathbb{Q}$ endowed with a normalizer of split Cartan mod p structure[1] with $p \geq 17$, then $\mathrm{h}(j_E) = \log|j_E|$.

In view of Theorem 5.1, Theorem 1.2 is a straightforward consequence of Theorem 1.1 and the following proposition, whose proof will be the goal of this section.

PROPOSITION 5.2. *There exists an absolute effective constant κ such that the following holds. Let p be a prime number, and E a non-*CM *elliptic curve over $\mathbb{Q}$, endowed with a structure of normalizer of split Cartan subgroup in level p. Then*

$$\mathrm{h}(j_E) = \log|j_E| \geq \kappa p. \tag{16}$$

The proof of Proposition 5.2 relies on Pellarin's refinement [21] of the Masser-Wüstholz famous upper bound [13] for the smallest degree of an isogeny between two isogenous elliptic curves.

THEOREM 5.3 (Masser-Wüstholz, Pellarin). *Let E be an elliptic curve defined over a number field K of degree d. Let E' be another elliptic curve, defined over K and isogenous to E. Then there exists an isogeny $\psi : E \to E'$ of degree at most $\kappa(d)\,(1+\mathrm{h}(j_E))^2$, where the constant $\kappa(d)$ depends only on d and is effective.*

Masser and Wüstholz had exponent 4 (they actually proved similar statements for general abelian varieties) and Pellarin reduced it to 2, which is crucial for us; in fact, any exponent below 4 would do. Pellarin gave an explicit expression for $\kappa(d)$ of the shape $\lambda d^4(1+\log d)^2$ with an absolute constant λ. See

[1] That is, whose mod p Galois representation has image contained in a normalizer of a split Cartan.

also the work [25] of E. Viada, who obtains exponent 3, but smaller $\kappa(d)$. In [1, App. B] Bertrand remarks (refering to the exponent as C):

> *En fait, tout porte à croire [...] que du point de vue transcendant, la valeur optimale de C est 2. La tradition folklorique veut sans doute que C vaille 0 [...], mais cela paraît sans espoir du côté transcendant.*

COROLLARY 5.4. *Let E be a non-*CM *elliptic curve defined over a number field K of degree d, and admitting a cyclic isogeny over K of degree δ. Then $\delta \le \kappa(d)\,(1 + \mathrm{h}(j_E))^2$.*

Proof. Let ϕ be a cyclic isogeny from E to E', and let $\phi^D\colon E' \to E$ be the dual isogeny. Let $\psi\colon E \to E'$ be an isogeny of degree bounded by $\kappa(d)\,(1 + \mathrm{h}(j_E))^2$; without loss of generality, ψ may be assumed cyclic. As E has no CM, the composed map $\phi^D \circ \psi$ must be multiplication by some integer, so that $\phi = \pm\psi$. □

Proof of Proposition 5.2. For an elliptic curve E endowed with a structure of normalizer of split Cartan subgroup in level p over $\mathbb{Q}$, write C_1 and C_2 for the obvious two independent p-subgroups in $E[p]$ which are Galois conjugates over a quadratic extension $K/\mathbb{Q}$. Set $\varphi_i\colon E \to E_i := E/C_i$ and recall that there is a cyclic p^2-isogeny over K from E_1 to E_2, factorizing as the product:

$$\varphi\colon E_1 \overset{\varphi_1^*}{\to} E \overset{\varphi_2}{\to} E_2.$$

It follows from Corollary 5.4 that $\mathrm{h}(j_{E_i}) \ge \kappa_1 p$ for $i = 1, 2$, where κ_1 is some constant independent of p and E.

A result of Faltings [8, Lemma 5] asserts that $\mathrm{h}_{\mathcal{F}}(E_1) \le \mathrm{h}_{\mathcal{F}}(E) + \frac{1}{2}\log p$, where $\mathrm{h}_{\mathcal{F}}$ is Faltings' semistable height. Finally, for any elliptic curve $\mathcal{E}$ over a number field we have

$$\left|\mathrm{h}(j_{\mathcal{E}}) - 12\mathrm{h}_{\mathcal{F}}(\mathcal{E})\right| \le 6\log\bigl(1 + \mathrm{h}(j_{\mathcal{E}})\bigr) + O(1);$$

see [24, Prop. 2.1]. (Pellarin shows that $O(1)$ can be replaced by 47.15; see [21, eq. (51), p. 240].) This completes the proof of Proposition 5.2 and of Theorem 1.2. □

6. Appendix: Integrality of the j-invariant

Here we prove that rational points on $X_{\mathrm{split}}(p)$ are, in fact, integral.

THEOREM 6.1 (Mazur, Momose, Merel). *For a prime $p = 11$ or $p \ge 17$, the j-invariant $j(P)$ of any noncuspidal point of $X_{\mathrm{split}}(p)(\mathbb{Q})$ belongs to $\mathbb{Z}$.*

The proof of this theorem is somehow scattered in the literature. Mazur [17, Cor. 4.8] proved that a prime divisor ℓ of the denominator of $j(P)$ must either be 2, or p, or satisfy $\ell \equiv \pm 1 \mod p$. The cases $\ell \equiv \pm 1 \mod p$ and $\ell = p$ were settled by Momose [19, Prop. 3.1], together with the case $\ell = 2$ when $p \equiv 1 \mod 8$ [19, Cor. 3.6]. Finally the case $\ell = 2$ with $p \not\equiv 1 \mod 8$ was treated by Merel [18, Th. 5]. The aim of this appendix is to present a short unified proof. To avoid some technicalities occurring only for small p, we assume in the sequel that $p \geq 37$.

Recall that the curve $X_{\mathrm{split}}(p)$ parametrizes (isomorphism classes of) elliptic curves endowed with an *unordered* pair of independent p-isogenies. Let $P = \big(E, \{A, B\}\big)$ be a $\mathbb{Q}$-point on $X_{\mathrm{split}}(p)$, which we may assume to be non-CM. Then the isogenies A and B are defined over a number field K with degree at most 2.

Proposition 6.2. *Let $P = \big(E, \{A, B\}\big) \in X_{\mathrm{split}}(p)(\mathbb{Q})$ and K be defined as above. Let $\mathcal{O}_K$ be its ring of integers. Then we have the following*:

(a) *The curve E is not potentially supersingular at p.*
(b) *The points (E, B) and $(E/A, E[p]/A) = (E/A, A^*)$, where A^* is the isogeny dual to A, coincide in the fibers of characteristic p of $X_0(p)_{/\mathcal{O}_K}$.*

Proof. Part (a) is proved in [19, Lemma 1.3]. Part (b) follows from [20, proof of Prop. 3.1]. For the convenience of the reader we sketch somewhat different (and simpler) arguments.

It follows from Serre's study of the action of inertia groups I_p at p on the formal group of elliptic curves that if E is potentially supersingular then I_p (potentially) acts via a "fundamental character of level 2" (at least if E has j-invariant different from 1728 mod p), so that the image of inertia contains a subgroup of index 4 or 6 in a nonsplit Cartan subgroup of $\mathrm{GL}(E[p])$ (see [23, Paragraph 1]). This gives a contradiction to the fact that a subgroup of index 2 in the absolute Galois group of $\mathbb{Q}$ preserves two lines in $E[p]$; for the remaining case of $j = 1728$ mod p we refer to the article of Momose, loc. cit., whence part (a).

For (b) we remark that we may assume the schematic closure of A to be étale over $\mathcal{O}$ (the ring of integers of a completion $K_{\mathcal{P}}$ of K at a prime $\mathcal{P}$ above p, whose residue field we denote by $k_{\mathcal{P}}$); indeed, as E is not potentially supersingular at $\mathcal{P}$, at most one line in $E[p]$ can be purely radicial over $k_{\mathcal{P}}$. Up to replacing $K_{\mathcal{P}}$ by a finite ramified extension, we shall also assume E is semistable over $K_{\mathcal{P}}$. Now E/A is isomorphic over $\bar{k}_{\mathcal{P}}$ to $E^{(p)}$ via the Verschiebung isogeny, and the latter is in turn isomorphic to $E_{/k_{\mathcal{P}}}$ as E has a model over $\mathbb{Z}$. Moreover the isomorphism between B and $E[p]/A$ as K-group schemes induced by the projection $E \to E/A$ extends to an isomorphism over $\mathcal{O}$ by Raynaud's theorem on group schemes of type $(p, \ldots, p)$, as recalled in [19, Proof of Lemma 1.3]. It follows that $(E, B)_{k_{\mathcal{P}}}$ is isomorphic to $(E/A, E[p]/A)_{k_{\mathcal{P}}} = (w_p(E, A))_{k_{\mathcal{P}}}$, whence (b). This completes the proof. □

The curve $X_{\mathrm{split}}(p)$ admits an obvious double covering by the curve $X_{\mathrm{sp.Car.}}(p)$, parametrizing elliptic curves endowed with an *ordered* pair of p-isogenies. We denote by w the generator of the Galois group of this covering; that is, w modularly exchanges the two p-isogenies. If $\big(E,(A,B)\big)$ is a point on $X_{\mathrm{sp.Car.}}(p)$, then $w\big(E,(A,B)\big)=\big(E,(B,A)\big)$. We recall certain properties of the modular Jacobian $J_0(p)$ and its *Eisenstein quotient* $\tilde{J}(p)$ (see [15]).

PROPOSITION 6.3. *Let p be a prime number. Then we have the following.*

(a) [15, Th. 1] *The group $J_0(p)(\mathbb{Q})_{\mathrm{tors}}$ is cyclic and generated by* $\mathrm{cl}(0-\infty)$, *where* 0 *and* ∞ *are the cusps of $X_0(p)$. Its order is equal to the numerator of the quotient $(p-1)/12$.*

(b) [15, Th. 4] *The group $\tilde{J}(p)(\mathbb{Q})$ is finite. Moreover, the natural projection $J_0(p)\to\tilde{J}(p)$ defines an isomorphism $J_0(p)(\mathbb{Q})_{\mathrm{tors}}\to\tilde{J}(p)(\mathbb{Q})$.*

As Mazur remarks, Raynaud's theorem on group schemes of type $(p,\dots,p)$ insures that $J_0(p)(\mathbb{Q})_{\mathrm{tors}}$ defines a $\mathbb{Z}$-group scheme which, being constant in the generic fiber, is étale outside 2, and which at 2 has étale quotient of rank at least half that of $J_0(p)(\mathbb{Q})_{\mathrm{tors}}$.

Proof of Theorem 6.1. For an element t in the $\mathbb{Z}$-Hecke algebra for $\Gamma_0(p)$, define the morphism g_t from $X^{\mathrm{smooth}}_{\mathrm{sp.Car.}}(p)_{/\mathbb{Z}}$ to $J_0(p)_{/\mathbb{Z}}$ which extends the morphism on generic fibers:

$$g_t\colon\left\{\begin{array}{rcl} X_{\mathrm{sp.Car.}}(p) & \to & J_0(p)\\ Q=\big(E,(A,B)\big) & \mapsto & t\cdot\mathrm{cl}\big((E,A)-(E/B,E[p]/B)\big).\end{array}\right.$$

Let $J_0(p)\stackrel{\pi}{\to}\tilde{J}(p)$ be the projection to the Eisenstein quotient, and $\tilde{g}_t:=\pi\circ g_t$. One checks that $g_t\circ w=-w_p\circ g_t$ and one knows that $(1+w_p)$ acts trivially on $\tilde{J}(p)$ from [15, Prop. 17.10]. Therefore $\tilde{g}_t$ actually factorizes through a $\mathbb{Q}$-morphism from $X_{\mathrm{split}}(p)$ to $\tilde{J}(p)$, which we extend by the universal property of Néron models to a map from $X^{\mathrm{smooth}}_{\mathrm{split}}(p)_{/\mathbb{Z}}$ to $\tilde{J}(p)_{/\mathbb{Z}}$. We still denote this morphism by $\tilde{g}_t$ and we put $\tilde{g}=\tilde{g}_1$.

Let P be a rational point on $X_{\mathrm{split}}(p)$, and ℓ a prime divisor of the denominator of $j(P)$. Then P specializes to a cusp at ℓ. Recall that $X_{\mathrm{split}}(p)$ has one cusp defined over $\mathbb{Q}$ (the *rational cusp*), and $(p-1)/2$ other cusps, conjugate over $\mathbb{Q}$. We first claim that P specializes to the rational cusp. Indeed, it follows from Proposition 6.2 (a) that P does extend to a section of $X^{\mathrm{smooth}}_{\mathrm{split}}(p)_{/\mathbb{Z}_p}$, from Proposition 6.2 (b) that $\tilde{g}(P)(\mathbb{F}_p)=0(\mathbb{F}_p)$, and from the remark after Proposition 6.3 that $\tilde{g}(P)(\mathbb{Q})=0(\mathbb{Q})$ (recall $p\neq 2$). The nonrational cusps of $X_{\mathrm{split}}(p)(\mathbb{C})$ map to $\mathrm{cl}(0-\infty)$ in $J_0(p)(\mathbb{C})$ (this can be seen with the above modular interpretation of $\tilde{g}_t$, by the fact that the nonrational cusps specialize at p to a generalized elliptic curve endowed with a pair of *étale* isogenies. Or, if f denotes the map $f\colon X_{\mathrm{sp.C.}}(p)\to X_0(p)$, $(E,(A,B))\mapsto(E,A)$, one has $g_1 = \mathrm{cl}(f - w_p f w)$, and as $f(c_i) = 0 \in X_0(p)$ for c_i a nonrational cusp and w permutes the c_is, one sees that $\tilde{g}(c_i) = \mathrm{cl}(0 - \infty)$. For more details see, for instance, the proof of Proposition 2.5 in [19]). Therefore, as we assumed $p \geq 37$, Proposition 6.3 implies that if P specializes to a nonrational cusp at ℓ then $\tilde{g}(P)$ would not be 0 at ℓ, a contradiction.

Now we use the winding quotient (see, for instance, [18]). Take an ℓ-adically maximal element t in the Hecke algebra which kills the winding ideal I_e. Again, as $t(1+w_p) = 0$, the above morphism g_t factorizes through a morphism g_t^+ from $X_{\mathrm{split}}^{\mathrm{smooth}}(p)_{/\mathbb{Z}}$ to $t \cdot J_0(p)_{/\mathbb{Z}}$. Moreover $g_t^+(P)$ belongs to $t \cdot J_0(p)(\mathbb{Q})$, hence is a torsion point, as $t \cdot J_0(p)$ is isogenous to a quotient of the winding quotient of $J_0(p)$. As above, by looking at the fiber at p, we see that $g_t^+(P) = 0$ at p, hence at the generic fiber as well. We then easily check by use of the q-expansion principle, as in [18, Th. 5], that g_t^+ is a formal immersion at the specialization $\infty(\mathbb{F}_\ell)$ of the rational cusp on $X_{\mathrm{split}}(p)$. This allows us to apply the classical argument of Mazur (see e.g. [17, proof of Cor. 4.3]), yielding a contradiction; therefore P is not cuspidal at ℓ. □

References

[1] D. Bertrand, Hauteurs et isogénies, *Astérisque* **183** (1990), 107–125. MR 1065157. Zbl 0729.14025.

[2] Y. Bilu and P. Parent, Integral j-invariants and Cartan structures for elliptic curves, *C. R. Math. Acad. Sci. Paris* **346** (2008), 599–602. MR 2423260. Zbl 1165.11053. doi: 10.1016/j.crma.2008.04.002.

[3] ———, Runge's method and modular curves, *Internat. Math. Res. Notes* (2010), 31 pages, article ID rnq141. doi: 10.1093/imrn/rnq141.

[4] E. Bombieri, On Weil's "théorème de décomposition", *Amer. J. Math.* **105** (1983), 295–308. MR 701562. doi: 10.2307/2374261.

[5] I. Chen, Jacobians of modular curves associated to normalizers of Cartan subgroups of level p^n, *C. R. Math. Acad. Sci. Paris* **339** (2004), 187–192. MR 2078072. Zbl 1106.11020. doi: 10.1016/j.crma.2004.04.027.

[6] A. C. Cojocaru, On the surjectivity of the Galois representations associated to non-CM elliptic curves, *Canad. Math. Bull.* **48** (2005), 16–31, with an appendix by Ernst Kani. MR 2118760. Zbl 1062.11031.

[7] A. C. Cojocaru and C. Hall, Uniform results for Serre's theorem for elliptic curves, *Int. Math. Res. Not.* **2005** (2005), 3065–3080. MR 189500. Zbl 1178.11045. doi: 10.1155/IMRN.2005.3065.

[8] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366. MR 718935. doi: 10.1007/BF01388432.

[9] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, *Astérisque* **295** (2004), ix, 117–290. MR 2104361.

[10] A. Kraus, Une remarque sur les points de torsion des courbes elliptiques, *C. R. Acad. Sci. Paris Sér. I Math.* **321** (1995), 1143–1146. MR 1360773. Zbl 0862.11037.

[11] D. S. Kubert and S. Lang, *Modular Units*, *Grundl. Math. Wissen.* **244**, Springer-Verlag, New York, 1981. MR 648603. Zbl 0492.12002.

[12] A. Levin, Variations on a theme of Runge: effective determination of integral points on certain varieties, *J. Théor. Nombres Bordeaux* **20** (2008), 385–417. MR 2477511. Zbl 1179.11018.

[13] D. W. Masser and G. Wüstholz, Estimating isogenies on elliptic curves, *Invent. Math.* **100** (1990), 1–24. MR 1037140. doi: 10.1007/BF01231178.

[14] ———, Galois properties of division fields of elliptic curves, *Bull. London Math. Soc.* **25** (1993), 247–254. MR 1209248. doi: 10.1112/blms/25.3.247.

[15] B. Mazur, Modular curves and the Eisenstein ideal, *Inst. Hautes Études Sci. Publ. Math.* (1977), 33–186 (1978). MR 488287. Zbl 0394.14008.

[16] ———, Rational points on modular curves, in *Modular Functions of One Variable*, V, *Lecture Notes in Math.* **601**, Springer-Verlag, New York, 1977, pp. 107–148. MR 56 #8579. Zbl 0357.14005.

[17] ———, Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.* **44** (1978), 129–162. MR 482230. doi: 10.1007/BF01390348.

[18] L. Merel, Normalizers of split Cartan subgroups and supersingular elliptic curves, in *Diophantine Geometry*, *CRM Series* **4**, Ed. Norm., Pisa, 2007, pp. 237–255. MR 2349658. Zbl 05263288.

[19] F. Momose, Rational points on the modular curves $X_{\mathrm{split}}(p)$, *Compositio Math.* **52** (1984), 115–137. MR 742701. Zbl 0574.14023.

[20] P. J. R. Parent, Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$, *Compositio Math.* **141** (2005), 561–572. MR 2135276. doi: 10.1112/S0010437X04001022.

[21] F. Pellarin, Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques, *Acta Arith.* **100** (2001), 203–243. MR 1865384. Zbl 0986.11046. doi: 10.4064/aa100-3-1.

[22] M. Rebolledo, Module supersingulier, formule de Gross-Kudla et points rationnels de courbes modulaires, *Pacific J. Math.* **234** (2008), 167–184. MR 2375318. Zbl 1167.11023. doi: 10.2140/pjm.2008.234.167.

[23] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331. MR 52 #8126. Zbl 0235.14012. doi: 10.1007/BF01405086.

[24] J. H. Silverman, Heights and elliptic curves, in *Arithmetic Geometry*, Springer-Verlag, New York, 1986, pp. 253–265. MR 861979. Zbl 0603.14020.

[25] E. Viada, Minimal elliptic isogenies, preprint.

(Received: March 2, 2009)

Institut de Mathématiques de Bordeaux,
Université Bordeaux 1, Talence, France
E-mail: Yuri.Bilu@math.u-bordeaux1.fr
http://www.math.u-bordeaux1.fr/~yuri/

Institut de Mathématiques de Bordeaux,
Université Bordeaux 1, Talence, France
E-mail: Pierre.Parent@math.u-bordeaux1.fr