ANNALES

DE

L'INSTITUT FOURIER

Dino LORENZINI

Torsion and Tamagawa numbers

Tome 61, n° 5 (2011), p. 1995-2037.

<http://aif.cedram.org/item?id=AIF_2011__61_5_1995_0>

Ann. Inst. Fourier, Grenoble
61, 5 (2011) 1995-2037

TORSION AND TAMAGAWA NUMBERS

by Dino LORENZINI

ABSTRACT. — Let K be a number field, and let A/K be an abelian variety. Let c denote the product of the Tamagawa numbers of A/K, and let $A(K)_{\mathrm{tors}}$ denote the finite torsion subgroup of $A(K)$. The quotient $c/|A(K)_{\mathrm{tors}}|$ is a factor appearing in the leading term of the L-function of A/K in the conjecture of Birch and Swinnerton-Dyer. We investigate in this article possible cancellations in this ratio. Precise results are obtained for elliptic curves over $\mathbb{Q}$ or quadratic extensions $K/\mathbb{Q}$, and for abelian surfaces $A/\mathbb{Q}$. The smallest possible ratio $c/|E(\mathbb{Q})_{\mathrm{tors}}|$ for elliptic curves over $\mathbb{Q}$ is $1/5$, achieved only by the modular curve $X_1(11)$.

RÉSUMÉ. — Soit K un corps de nombres, et soit A/K une variété abélienne. Dénotons par c le produit des nombres de Tamagawa de A/K, et par $A(K)_{\mathrm{tors}}$ le sous-groupe fini des éléments de torsion de $A(K)$. Le quotient $c/|A(K)_{\mathrm{tors}}|$ apparaît dans la conjecture de Birch et Swinnerton-Dyer comme un facteur de la valeur du premier terme non-nul dans le développement limité en $s = 1$ de la fonction L de A/K. Nous nous intéressons dans cet article aux diviseurs communs des entiers c et $|A(K)_{\mathrm{tors}}|$. Nous obtenons des résultats précis pour les courbes elliptiques sur $\mathbb{Q}$ ou sur une extension quadratique, et pour les surfaces abéliennes sur $\mathbb{Q}$. La plus petite valeur de la fraction $c/|E(\mathbb{Q})_{\mathrm{tors}}|$ pour les courbes elliptiques sur $\mathbb{Q}$ est $1/5$, obtenue seulement par la courbe modulaire $X_1(11)/\mathbb{Q}$.

1. Introduction

Let K be any discrete valuation field with ring of integers $\mathcal{O}_K$, uniformizer π, and residue field k of characteristic $p \geqslant 0$. Let A/K be an abelian variety of dimension g. Let $\mathcal{A}/\mathcal{O}_K$ denote the Néron model of A/K. The special fiber $\mathcal{A}_k/k$ of $\mathcal{A}$ is the extension

$$(0) \longrightarrow \mathcal{A}_k^0 \longrightarrow \mathcal{A}_k \longrightarrow \Phi \longrightarrow (0)$$

of a finite étale group scheme Φ/k, called the *group of components*, by a connected smooth group scheme $\mathcal{A}_k^0/k$, the *connected component of* 0. The

Keywords: Abelian variety over a global field, torsion subgroup, Tamagawa number, elliptic curve, abelian surface, dual abelian variety, Weil restriction.
Math. classification: 11G05, 11G10, 11G30, 11G35, 11G40, 14G05, 14G10.

order of the finite abelian group $\Phi(k)$ is called the *Tamagawa number* of A/K.

Let now K be a global field, and v a non-archimedean place of K, with completion K_v and residue field k_v. Let c_v denote the Tamagawa number of A_{K_v}/K_v, and let $c = c(A/K) := \prod_v c_v$. The quotient $c(A/K)/|A(K)_{\mathrm{tors}}|$ is a factor appearing in the leading term of the L-function of A/K in the conjecture of Birch and Swinnerton-Dyer (see, *e.g.*, [30], F.4.1.6). We investigate in this article possible cancellations in this ratio.

Much can be said about the ratio $c/|A(\mathbb{Q})_{\mathrm{tors}}|$ for elliptic curves over $\mathbb{Q}$, due to the fact that the modular curves $X_1(N)/\mathbb{Q}$, parametrizing elliptic curves over $\mathbb{Q}$ with a $\mathbb{Q}$-rational torsion point of order N, are rational curves. The smallest ratio $c/|A(\mathbb{Q})_{\mathrm{tors}}|$ for elliptic curves over $\mathbb{Q}$ is $1/5$, achieved only by the modular curve $X_1(11)/\mathbb{Q}$ (2.23). For abelian varieties over $\mathbb{Q}$ of dimension $g > 1$, we did not find any ratio smaller than $(1/5)^g$, obtained by taking the product of g copies of $X_1(11)$. Precise results for elliptic curves are as follows.

PROPOSITION 1.1. — *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order N. The following statements hold with at most five explicit exceptions for a given N. The exceptions are given by their labels in Cremona's table* [12].

(a) *If $N = 4$, then $(N/2) \mid c$, except for $X_1(15)$, $15a7$, and $17a4$.*
(b) *If $N = 5$, 6, or 12, then $N \mid c$, except for $X_1(11)$, $X_1(14)$, $14a6$, and $20a2$.*
(c) *If $N = 10$, then $(N^2/2) \mid c$.*
(d) *If $N = 7$, 8, 9, then $N^2 \mid c$, except for $15a4$, $21a3$, $26b1$, $42a1$, $48a6$, $54b3$, and $102b1$.*

Without exception, $N \mid c$ if $N = 7$, 8, 9, 10, or 12.

Mazur [47] showed that N in the proposition can only take the values 1 through 10, and 12. A statement for $N = 7$ weaker than the one in Prop. 1.1 is proven in [14] (see 4.2). We note in 2.26 that there are infinitely many elliptic curves $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order $N = 3$ and $c = 1$.

PROPOSITION 1.2. — *Let K be a number field. Let E/K be an elliptic curve with a K-rational point of order N. If $N = 7$ or 9, then $N \mid c$, except possibly when E/K belongs to a list of at most $2^{9(\mathrm{rank}(\mathcal{O}_K^*)+1)}$ isomorphism classes of elliptic curves over K.*

PROPOSITION 1.3. — *Let $K/\mathbb{Q}$ be a quadratic field. Let E/K be an elliptic curve with a K-rational point of order N with $N = 11$ or 13. Then $N \mid c$.*

Kamienny [32] proved that the possible prime values of N in 1.3 are $2, 3, 5, 7, 11$, and 13. Propositions 1.1 and 1.2 are proven in the next section through a case-by-case analysis. Proposition 1.3 follows from 3.4. The case where $K/\mathbb{Q}$ is a cubic field is considered in [34].

The statement that $N \mid c$ in 1.1 above, in the cases $N = 5$ and $N = 7$, was verified numerically by A. Agashe for all optimal elliptic curves in Cremona's data base. This led him to ask whether the statement for these values of N was true for all optimal curves. I thank him for bringing this question to my attention.

Abelian varieties A/K of higher dimensions are considered in the third section. Optimal modular quotients are briefly considered in section four. We note in these sections two statements which may be of independent interest. Let K be a global field and let $A^\vee/K$ denote the dual of A/K. Then $c(A/K) = c(A^\vee/K)$ (4.3). Let L/K be a Galois extension, and let $\mathrm{Res}_{L/K}(B)/K$ denote the Weil restriction of B/L. Then $c(B/L) = c(\mathrm{Res}_{L/K}(B)/K)$ (3.19).

As for elliptic curves, one does not expect in higher dimension that the existence of a point $P \in A(K)$ of finite order N always produces a cancellation in the ratio $c/|A(K)_{\mathrm{tors}}|$. For instance, the Jacobians $A/\mathbb{Q}$ of certain Fermat quotients have dimension g with a $\mathbb{Q}$-rational torsion point of order $N = 2g + 1$ and $c = 1$ (see 3.7). On the other hand, let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of prime order N. Without stating our results here in complete generality, let us mention that if $N \geqslant 23$, then $N \mid c(A)$ (3.8).

In view of this latter result, it is natural to wonder whether the existence of a point $P \in A(\mathbb{Q})$ of prime order N with N "large" compared to $\dim(A)$ always forces a cancellation in the ratio $c/|A(\mathbb{Q})_{\mathrm{tors}}|$. Such a cancellation is frequently a consequence of the fact that there exists a place v of $\mathbb{Q}$ where the image in $\Phi_v(k_v)$ of the point P still has order N (see 2.28 and 3.1). How large $|A(\mathbb{Q})_{\mathrm{tors}}|$ can be for a given dimension, and how large N should be to force a cancellation in general, is not understood for $g = \dim(A) > 1$. For an example where a prime N is quite large compared to g, consider the Jacobian $J_1(59)/\mathbb{Q}$ of the modular curve $X_1(59)/\mathbb{Q}$. This abelian variety has dimension $g = 117$, has $c = 1$, and has a $\mathbb{Q}$-rational point of prime order $N = 998855361369139381235879427 1$, with $N > 12g^{13}$ (see 3.6, and [11], 6.6).

Explicit computations in this article were done using the Sage Mathematics Software [64] and Magma [8]. I thank A. Agashe, D. Benson, E. Howe, W. Stein, R. Varley, M. Watkins, and the referee, for useful comments. I

am grateful to N. Elkies for sending me a copy of [19], to A. Brumer for bringing to my attention [62], and to P. Clark for the reference [63]. I also thank J. Stankewicz for sharing a Sage program with me.

2. The case of elliptic curves

2.1. Let K be any field. Let E/K be an elliptic curve and $P \in E(K)$ be a point of order not equal to $1, 2$ or 3. Then E/K can be given by a Weierstrass equation

$$E(b,c)\colon y^2 + (1-c)xy - by = x^3 - bx^2 \tag{2.1}$$

with $P = (0,0)$. For this Weierstrass equation, we have

$$c_4(b,c) = 16b^2 + 8b(1-c)(c+2) + (1-c)^4,$$
$$\Delta(b,c) = b^3(16b^2 - b(8c^2+20c-1) - c(1-c)^3).$$

By setting the order of P to be N, one obtains an explicit relation between b and c. When $N = 4, \dots, 10$, and 12, the relation found between b and c defines a K-rational curve in the (b,c)-plane. We will denote by λ a parameter on the normalization of this plane curve. The relationship between b and c can be obtained using the following explicit points of the elliptic curve $E(b,c)$:

$$[\text{-}1]P = (0,b), \quad [\text{-}2]P = (b,0), \quad [\text{-}3]P = (c,c^2)$$
$$[2]P = (b,bc), \quad [3]P = (c,b-c), \quad [4]P = \left(\tfrac{b(b-c)}{c^2}, \tfrac{b^2(c^2+c-b)}{c^3}\right)$$
$$[5]P = \left(\tfrac{bc(c^2+c-b)}{(b-c)^2}, \tfrac{bc^2(b^2-bc-c^3)}{(b-c)^3}\right)$$
$$[7]P = \left(\tfrac{bc(b-r)c-c^2)(2b^2-bc^2-3bc+c^2)}{(b^2-bc-c^3)^2}, \tfrac{b^2(b-c-c^2)^2((b-c)^3+c^3(b-c-c^2))}{(b^2-bc-c^3)^3}\right)$$

Explicit formuli for each case $N = 4, \dots, 10$, and 12, can be found for instance in [35], page 217, or [31], page 319.

2.2. Let K be a discrete valuation field with ring of integers $\mathcal{O}_K$, uniformizer π, and residue field k. Let E/K be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with discriminant Δ, invariant c_4, and j-invariant $j(E) = c_4^3/\Delta$. Recall that this elliptic curve has *multiplicative reduction of type* I_n modulo π if there exists such an equation with $a_i \in \mathcal{O}_K$, $i = 1, 2, 3, 4$ and 6, with $n := \mathrm{ord}_\pi(\Delta) > 0$ and with $\mathrm{ord}_\pi(c_4) = 0$. Since $\pi \mid \Delta$, it is possible to

change coordinates so that in the new Weierstrass equation, $\pi \mid a_3, a_4$, and a_6. Then the condition to have multiplicative reduction is that $\pi \nmid a_1^2 + 4a_2$ (we set as usual $b_2 := a_1^2 + 4a_2$). The reduction is called *split* if, for the coefficients of the new equation, the congruence $t^2 + a_1 t - a_2 = 0$ has two (distinct) roots in k. When the reduction is split multiplicative, the Tamagawa number $c_{(\pi)}$ is equal to $\mathrm{ord}_\pi(\Delta)$ (see Tate's Algorithm [67], or [65], IV.9). When the reduction is not split multiplicative, the Tamagawa number $c_{(\pi)}$ is equal to 2 if $\mathrm{ord}_\pi(\Delta)$ is even, and 1 otherwise. When the reduction is potentially multiplicative, then the reduction modulo π is of type I_n^* for some $n > 0$, and $c_{(\pi)}$ is equal to 2 or 4 (see [45], 2.8).

2.3. We will use the fact reviewed below in several of the proofs in this section. Let K be a number field. Let A, $B \in K^*$, and consider the equation

$$AX + BY = 1$$

with $X, Y \in \mathcal{O}_K^*$. The number of solutions to this equation in $(\mathcal{O}_K^*)^2$ is bounded by the constant $2^{9(\mathrm{rank}(\mathcal{O}_K^*)+1)}$ (see [4], and [22] (1.5)).

We will apply this bound in this section for the equation $X - Y = 1$. When $[K\colon \mathbb{Q}] = 2$, its solutions can be explicitly determined as follows.

Let $X \in \mathcal{O}_K^*$, and assume that $X - 1 \in \mathcal{O}_K^*$. Let $\sigma(X)$ denote the conjugate of X in K. Then $X\sigma(X) = \pm 1$, and $(X-1)(\sigma(X)-1) = 1 - (X + \sigma(X)) + X\sigma(X) = \pm 1$. It follows that $X = (3 \pm \sqrt{5})/2$, or $X = (1 \pm \sqrt{5})/2$, or $X = (-1 \pm \sqrt{5})/2$ in $\mathbb{Q}(\sqrt{5})$, or $X = (1 \pm \sqrt{-3})/2$. (See also [55], 17, page 350.)

The results in the propositions below are stated only for $K = \mathbb{Q}$ or K a number field, although it will be clear from the proofs that similar results also hold when K is the function field of a curve.

PROPOSITION 2.4 (**Case N=4**). — *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order $N = 4$. Then $c(E)$ is even, except for the three curves denoted by 15a7, 15a8, and 17a4 in* [12]*, which have $c(E) = 1$.*

Proof. — Let K be any field. For the point P on the curve $E(b,c)$ in (2.1) to have order $N = 4$, we need $c = 0$. Set $\lambda := b$. The invariants of $E(b,c)$ expressed in terms of λ are:

$$\Delta(\lambda) = \lambda^4(1 + 16\lambda),$$
$$c_4(\lambda) = 16\lambda^2 + 16\lambda + 1,$$

with $\mathrm{res}(\Delta(\lambda), c_4(\lambda)) = 2^4$. It follows that there exists $\lambda \in K$ such that an elliptic curve E/K with a point of order $N = 4$ can be given by a

Weierstrass equation of the form

$$E_\lambda \colon y^2 + xy - \lambda y = x^3 - \lambda x^2.$$

Let now K be a number field. Assume that there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda) > 0$. Then we immediately find from the computations of Δ and c_4 that the reduction of E/K modulo $\mathfrak{P}$ is split of type I_{4m}.

Assume now that there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda) < 0$. Let π denote a uniformizer of the local ring $\mathcal{O}_{K,\mathfrak{P}}$, and write $\lambda = u\pi^m$, with $u \in \mathcal{O}^*_{K,\mathfrak{P}}$. The Weierstrass equation E_λ is not integral at $\mathfrak{P}$, but the following equations are:

$$\begin{aligned} &\text{If } |m| = 2z \quad\ \ : y^2 + \pi^z xy - u\pi^z y = x^3 - ux^2, \\ &\text{If } |m| = 2z+1 \ : y^2 + \pi^{z+1} xy - u\pi^{z+2} y = x^3 - u\pi x^2. \end{aligned}$$

When the residue characteristic is not 2, the first equation is minimal, with reduction of type I_{2z}, with component group of order 2 or $2z$. The second equation is such that over $K(\sqrt{\pi})$, the change of variables $x' = x\sqrt{\pi}^{-2}$ and $y' = y\sqrt{\pi}^{-3}$ produces a new equation with reduction of type I_{4z+2}. It follows that over K, the reduction of the elliptic curve is of type I^*_n for some $n > 0$, which has a component group of order 2 or 4 (see 2.2).

Let us assume now that $K = \mathbb{Q}$, and that $\lambda = \pm 2^{-m}$. An explicit computation of the valuation at (2) of the j-invariant of E shows that if $m > 8$, then E has potentially multiplicative reduction. Again, we find that the reduction over K is of type I^*_n for some $n > 0$, which has a component group of order 2 or 4. For the finitely many cases where the reduction is potentially good, an explicit case-by-case computation of the reduction type will confirm that for these cases too, the product $(\prod_{p \text{ prime}} c_p)$ is even, except when $\lambda = -2^{-8}, -1$, and 1, defining the curves $15a7$, $15a8$, and $17a4$, respectively. □

Remark 2.5. — Consider the curve E_λ in 2.4 with $\lambda = 1/p^2$, $p > 3$ prime. It has a minimal equation $y^2 + pxy - py = x^3 - x^2$, with discriminant $p^2(p^2+16)$, and $b_2 = a_1^2 + 4a_2 = p^2 - 4$. This curve has reduction of type I_2 at (p), and reduction of type I_s at a prime q such that $\mathrm{ord}_q(p^2+16) = s$.

Schinzel's Hypothesis H conjectures that the polynomials λ and (λ^2+16) take prime values at the same time infinitely often. For a prime p such that $p^2 + 16$ is squarefree, the curve has a point of order 4, and $c = 2$.

Consider the curve $E_t/\mathbb{Q}(t)$ with equation $y^2 + txy - ty = x^3 - x^2$ and discriminant $t^2(t^2+16)$. This curve has exactly four places of bad reduction over $\overline{\mathbb{Q}}(t)$, all semi-stable, with reduction of type I_2, I_1, I_1, and I_8. Such a curve is uniquely determined over $\mathbb{C}(t)$ [2].

Remark 2.6. — Let $E/\mathbb{Q}$ be an elliptic curve. One may define a Tamagawa number $c_\infty(E)$ for the place at infinity as follows: $c_\infty(E) = 1$ if $\Delta(E) < 0$, and $c_\infty(E) = 2$ if $\Delta(E) > 0$. This quantity is usually attached to the contribution of the real period in the conjecture of Birch and Swinnerton-Dyer (see [65], V.2.3.1, for the connection between the sign of the discriminant and the connectedness of $E(\mathbb{R})$).

The curve $15a8$ has negative discriminant, while $\Delta(15a7), \Delta(17a4) > 0$. Thus, the statement $N/2$ divides $c(E)c_\infty(E)$ is true for all but one exception, $15a8$. We do not know whether N divides $c(E)c_\infty(E)$ with only finitely many exceptions.

PROPOSITION 2.7 (**Case N=5**). — *Let E/K be an elliptic curve with a K-rational point of order $N = 5$.*

(a) *If $K = \mathbb{Q}$, then there exists at least one prime ideal (p) where $E/\mathbb{Q}$ has split multiplicative reduction of type I_n with $N \mid n$, except for the curve $11a3$ in* [12]*, with $c(E) = 1$.*

(b) *If K is an imaginary quadratic field, then there exists at least one prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$ where E/K has split multiplicative reduction of type $I_{n_\mathfrak{P}}$ with $N \mid n_\mathfrak{P}$, except for the curve $11a3$ and finitely many additional possible exceptions when $K = \mathbb{Q}(\sqrt{-1})$ and $K = \mathbb{Q}(\sqrt{-3})$.*

Proof. — Let K be any field. For the point P on the curve $E(b, c)$ in (2.1) to have order $N = 5$, we need $b = c$. Set $\lambda := b$. The invariants of $E(b, c)$ expressed in terms of λ are:

$$\Delta(\lambda) = \lambda^5(\lambda^2 - 11\lambda - 1),$$
$$c_4(\lambda) = 1 + 12\lambda + 14\lambda^2 - 12\lambda^3 + \lambda^4,$$

with $\operatorname{res}(\Delta(\lambda), c_4(\lambda)) = 5^2$. It follows that there exists $\lambda \in K$ such that an elliptic curve E/K with a point of order $N = 5$ can be given by a Weierstrass equation of the form

$$E_\lambda \colon y^2 + (1 - \lambda)xy - \lambda y = x^3 - \lambda x^2.$$

Let now K be a number field. Assume that there exists a prime $\mathfrak{P}$ such that $m := \operatorname{ord}_\mathfrak{P}(\lambda) > 0$. Then we immediately find from the computations of Δ and c_4 that the reduction of E/K modulo $\mathfrak{P}$ is split of type I_{5m}.

Assume now that there exists a prime $\mathfrak{P}$ such that $m := \operatorname{ord}_\mathfrak{P}(\lambda) < 0$. The Weierstrass equation E_λ is not integral at $\mathfrak{P}$, but the following equation is, where $\mu := \lambda^{-1}$:

$$y^2 + (\mu - 1)xy - \mu^2 y = x^3 - \mu x^2.$$

The discriminant of this new equation is $\mu^5(1-11\mu-\mu^2)$, and we find again that the reduction is split of type $I_{5|m|}$.

The cases where $\mathrm{ord}_{\mathfrak{P}}(\lambda)=0$ for all $\mathfrak{P}$, *i.e.*, when $\lambda\in\mathcal{O}_K^*$, have to be treated separately. When $K=\mathbb{Q}$, the units $\lambda=\pm1$ produce the same elliptic curve $y^2-y=x^3-x^2$, $11a3$ in [12], with $c(E)=1$. □

Remark 2.8. — The result above, that all but finitely many elliptic curves $E/\mathbb{Q}$ have $N\mid c(E)$ when $N=5$, is likely to be sharp. Indeed, Schinzel's Hypothesis H conjectures that the polynomials λ and $(\lambda^2-11\lambda-1)$ take prime values at the same time infinitely often. Thus, there conjecturally exist infinitely many prime numbers λ such that the discriminant of $E/\mathbb{Q}$, $\lambda^5(\lambda^2-11\lambda-1)$, is divisible by exactly two distinct primes, so that $E/\mathbb{Q}$ has reduction I_5 at λ, and I_1 at the prime $(\lambda^2-11\lambda-1)$. For such curves, $5^2\nmid c$.

It seems likely that the result in (b) cannot be extended to all number fields. To show this, it would suffice to produce a number field K, and an infinite number of units $\lambda\in\mathcal{O}_K^*$ such that the ideal $(\lambda^2-11\lambda-1)$ has a squarefree factorization in prime ideals of $\mathcal{O}_K$, or more generally, such that the order of $(\lambda^2-11\lambda-1)$ at any prime $\mathfrak{P}$ is not a multiple of 5. This would show the existence of infinitely many elliptic curves E/K with a point of order 5 and with $5\nmid c(E)$. Deciding whether such an infinite family of units exists may be out of reach with the current techniques.

PROPOSITION 2.9 (**Case N=6**). — *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order $N=6$. Then $N\mid c(E)$, except for the curves denoted by $14a4$, $14a6$, and $20a2$ in* [12], *which have $c(E)=2$, 2, and 3, respectively.*

Proof. — Let K be any field. For the point P on the curve $E(b,c)$ in (2.1) to have order $N=6$, we need $b=c+c^2$. Set $\lambda:=c$. The invariants of $E(b,c)$ expressed in terms of λ are:

$$\Delta(\lambda)=\lambda^6(\lambda+1)^3(9\lambda+1),$$
$$c_4(\lambda)=(3\lambda+1)(3\lambda^3+3\lambda^2+9\lambda+1),$$

with $\mathrm{res}(\Delta(\lambda),c_4(\lambda))=2^{16}3^2$. It follows that there exists $\lambda\in K$ such that an elliptic curve E/K with a point of order $N=6$ can be given by a Weierstrass equation of the form

$$E_\lambda\colon y^2+(1-\lambda)xy-\lambda(\lambda+1)y=x^3-\lambda(\lambda+1)x^2.$$

Let now K be a number field. Assume that there exists a prime $\mathfrak{P}$ such that $m:=\mathrm{ord}_{\mathfrak{P}}(\lambda)>0$. Then we immediately find from the computations

of Δ and c_4 that the reduction of E/K modulo $\mathfrak{P}$ is split of type I_{6m}, and the proposition is proved in this case.

Assume now that there exists a prime $\mathfrak{P}$ such that $m := -\operatorname{ord}_{\mathfrak{P}}(\lambda) > 0$. The Weierstrass equation E_λ is not integral at $\mathfrak{P}$, but the following equation is, where $\mu := \lambda^{-1}$:

$$y^2 + (\mu - 1)xy - \mu(\mu + 1)y = x^3 - (\mu + 1)x^2.$$

The discriminant of this new equation is $\mu^2(1 + \mu)^3(9 + \mu)$.

When the residue characteristic is not 3 at $\mathfrak{P}$, this equation is minimal at $\mathfrak{P}$, with reduction of type I_{2m}. When $\mu + 1$ is contained in a prime ideal $\mathfrak{Q}$ which does not contain 2, then the reduction of this Weierstrass equation at $\mathfrak{Q}$ is split of type I_{3s}, where $s := \operatorname{ord}_{\mathfrak{Q}}(\mu + 1)$. The proposition follows then in this case.

Let us assume now that $K = \mathbb{Q}$, and that $\mu = \pm 3^m$. Then Tate's algorithm shows that the reduction mod (3) is of type III, so with component group $\mathbb{Z}/2\mathbb{Z}$. The equation $\mu + 1 = \pm 2^s$ has only the solutions $\mu = 0$, $\mu = -2$, with $s = 0$, and $\mu = -3$ and $\mu = -3^2$. (The cases $\mu = 0$ and $\mu = -9$ need not be considered as in these cases $\Delta = 0$). Except for $\mu = -2, -3$, we find that $\mu + 1$ is divisible by an odd prime, and thus has a place with reduction of type I_{3s}. When $\mu = -2$, we have $14a4$, with $c(14a4) = 2$. When $\mu = -3$, we have $36a1$, with $c(36a1) = 6$.

Suppose now that μ is not a power of 3, and $\mu + 1 = \pm 2^s$. Consider first the case where $s \geqslant 4$. Then the equation

$$y^2 + (\mu - 1)xy - \mu(\mu + 1)y = x^3 - (\mu + 1)x^2.$$

is not minimal at (2). Since $\operatorname{ord}_2(\mu - 1) = 1$, we can "divide the equation" by 2^6, and obtain an minimal integral equation of the form

$$y^2 + \frac{(\mu - 1)}{2}xy - \frac{\mu(\mu + 1)}{2^3}y = x^3 - \frac{(\mu + 1)}{2^2}x^2,$$

with split multiplicative reduction. The discriminant of this equation is $\Delta = 2^{-12}\mu^2(\mu+1)^3(9+\mu)$, and since $s \geqslant 4$, we find that $\operatorname{ord}_2(\Delta) = 3s - 9$. It follows that the reduction at 2 is split of type $I_{3(s-3)}$.

It remains to consider the cases where $\mu = 1$ or -3 with $s = 1$ (curve $20a2$ with $c(20a2) = 3$, and $36a1$ with $c(36a1) = 6$), $\mu = 3$ or -5 with $s = 2$ (curves $36a2$ and $20a1$, both with $c = 6$), and $\mu = 7$ with $s = 3$ (curve $14a6$ with $c(14a6) = 2$). □

PROPOSITION 2.10 (**Case N=7**). — *Let E/K be an elliptic curve with a K-rational point of order $N = 7$.*

(a) *If $K=\mathbb{Q}$, there exist at least two prime ideals (p) where $E/\mathbb{Q}$ has split multiplicative reduction of type I_{n_p} with $N \mid n_p$, except for the curve $26b1$ in* [12], *with $c(E)=7$.*

(b) *If K is an imaginary quadratic field, then there exist at least two prime ideals $\mathfrak{P}$ in $\mathcal{O}_K$ where E/K has split multiplicative reduction of type $I_{n_\mathfrak{P}}$ with $N \mid n_\mathfrak{P}$, except possibly for the curve $26b1$ and finitely many additional possible exceptions when $K=\mathbb{Q}(\sqrt{-1})$ and $K=\mathbb{Q}(\sqrt{-3})$.*

(c) *If K is a real quadratic field, or $[K\colon \mathbb{Q}]>2$, then there exists at least one prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$ where E/K has split multiplicative reduction of type I_n with $N \mid n$, except when E/K belongs to a list of at most $2^{9(\operatorname{rank}(\mathcal{O}_K^*)+1)}$ isomorphism classes of elliptic curves over K. When K is real quadratic, the exceptions may include the curve $26b1$, and possibly six additional exceptions when $K=\mathbb{Q}(\sqrt{5})$.*

Proof. — Let K be any field. For the point P on the curve $E(b,c)$ in (2.1) to have order $N=7$, we need $b^2-bc-c^3=0$. Set $b=\lambda^3-\lambda^2$ and $c=\lambda^2-\lambda$. The invariants of $E(b,c)$ expressed in terms of λ are:

$$\Delta(\lambda)=\lambda^7(\lambda-1)^7(\lambda^3-8\lambda^2+5\lambda+1),$$
$$c_4(\lambda)=(\lambda^2-\lambda+1)(\lambda^6-11\lambda^5+30\lambda^4-15\lambda^3-10\lambda^2+5\lambda+1),$$

with $\operatorname{res}(\Delta(\lambda),c_4(\lambda))=7^2$. It follows that there exists $\lambda \in K\setminus\{0,1\}$ such that the elliptic curve E/K with a point of order N can be given by a Weierstrass equation of the form

$$y^2+(1-\lambda(\lambda-1))xy-\lambda^2(\lambda-1)y=x^3-\lambda^2(\lambda-1)x^2.$$

Let now K be a number field. Assume that there exists a prime $\mathfrak{P}$ such that $m:=\operatorname{ord}_\mathfrak{P}(\lambda)>0$. Then we immediately find from the computations of Δ and c_4 that the reduction of E/K modulo $\mathfrak{P}$ is split of type I_{7m}. If there exists a second maximal ideal $\mathfrak{P}'$ with $m':=\operatorname{ord}_{\mathfrak{P}'}(\lambda)>0$, then we have a second place where the reduction is split multiplicative, this time of type $I_{7m'}$.

Assume that there exists a prime $\mathfrak{P}$ such that $m:=\operatorname{ord}_\mathfrak{P}(\lambda)<0$. The Weierstrass equation E_λ is not integral at $\mathfrak{P}$, but the following equation is, where $\mu:=\lambda^{-1}$:

$$y^2+(\mu^2+\mu-1)xy-\mu^3(1-\mu)y=x^3-\mu(1-\mu)x^2.$$

The discriminant of this new equation is $\mu^7(1-\mu)^7(1-8\mu+5\mu^2+\mu^3)$, and the reduction at $\mathfrak{P}$ is split of type I_{7m}. It follows from the above considerations that the proposition is proved if there exist two distinct prime ideals $\mathfrak{P}$ such that $\operatorname{ord}_\mathfrak{P}(\lambda)\neq 0$.

Assume now that there exists a single prime ideal $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda) \neq 0$. Then either $\lambda \in \mathcal{O}_K$ or $\mu \in \mathcal{O}_K$. Assume first that $\lambda \in \mathcal{O}_K$. Then $\lambda \in \mathfrak{P}$. Consider the element $\lambda - 1$. Clearly, $\mathrm{ord}_{\mathfrak{P}}(\lambda - 1) = 0$. If there exists a maximal ideal $\mathfrak{Q} \neq \mathfrak{P}$ such that $m' := \mathrm{ord}_{\mathfrak{Q}}(\lambda - 1) > 0$, then we find that the elliptic curve has reduction modulo $\mathfrak{Q}$ of type $I_{7m'}$. Otherwise, $\lambda - 1 \in \mathcal{O}_K^*$. When $K = \mathbb{Q}$, the only possibility is $\lambda = 2$. When K is an imaginary quadratic field, the set of elements of the form $\lambda = 1 + u$, with u a unit, is finite.

The argument when $\mu \in \mathcal{O}_K$ is similar, and we find that a second place of multiplicative reduction of type $I_{7m'}$ exists, unless $1 - \mu$ is a unit. When $K = \mathbb{Q}$, the only possibility is $\lambda = 1/2$.

When $\mathrm{ord}_{\mathfrak{P}}(\lambda) = 0$ for all $\mathfrak{P}$, *i.e.*, when $\lambda \in \mathcal{O}_K^*$, we find that there may not be in general two places of multiplicative reduction with $7 \mid c_v$. There will be at least one such place if $\lambda - 1$ is not a unit in $\mathcal{O}_K^*$. As we recalled in 2.3, the equation $X + Y = 1$, with $X, Y \in \mathcal{O}_K^*$, has a number of solutions in $(\mathcal{O}_K^*)^2$ bounded by the constant $2^{9(\mathrm{rank}(\mathcal{O}_K^*)+1)}$. When $K = \mathbb{Q}$, the values $\lambda = -1, 2$, and $1/2$, all produce an equation for the curve $26b1$, with $c(26b1) = 7$. □

Remark 2.11. — Let $K = \mathbb{Q}(\sqrt{-3})$, with $\zeta_6 := (1 + \sqrt{-3})/2$. Consider the curve E_λ in the proof of 2.10 with $\lambda = \zeta_6$. The Weierstrass equation is

$$y^2 + 2xy + \zeta_6 y = x^3 + \zeta_6 x^2.$$

This curve has j-invariant $j = 0$, and discriminant ideal $(2 + \zeta_6)^2$, with $\mathrm{Norm}_{K/\mathbb{Q}}(2 + \zeta_6) = 7$. It has additive reduction of type II at $(2 + \zeta_6)$, so $c(E_\lambda) = 1$. The conjugate curve with $\lambda = \zeta_6^5$ similarly has $c = 1$. These curves appear in [53], Table 10, and are the only elliptic curves E/K over any quadratic field K which have integral j-invariant and a torsion point over K of order 7.

PROPOSITION 2.12 (**Case N=8**). — *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order $N = 8$. Then $N^2 \mid c(E)$, except for the curves denoted by* $15a4$, $21a3$, $42a1$, $48a6$, *and* $102b1$ *in* [12], *with* $c(E) = 16$, 8, 16, 32, *and* 32, *respectively.*

Proof. — Let K be any field. For the point P on the curve $E(b, c)$ in (2.1) to have order $N = 8$, we need the relation between b and c obtained by considering the x-coordinates of $[7]P = [-1]P$:

$$2b^2 - bc^2 - 3bc + c^2 = 0.$$

We find that $b=(2\lambda-1)(\lambda-1)$ and $c=(2\lambda-1)(\lambda-1)/\lambda$. The invariants of $E(b,c)$ expressed in terms of λ are:

$$\Delta(\lambda)=\frac{(1-8\lambda+8\lambda^2)(2\lambda-1)^4(\lambda-1)^8}{\lambda^4},$$
$$c_4(\lambda)=\frac{(16\lambda^8-64\lambda^7+224\lambda^6-448\lambda^5+480\lambda^4-288\lambda^3+96\lambda^2-16\lambda+1)}{\lambda^4}.$$

It follows that there exists $\lambda\in K$ such that an elliptic curve E/K with a point of order $N=8$ can be given by a Weierstrass equation of the form

$$E_\lambda\colon y^2+(1-c)xy-by=x^3-bx^2,$$

with b and c as above. The curves in this family indexed by λ and $1-\lambda$ are isomorphic. We collect here some explicit computations:

$\lambda=-1/2$	curve $21a3$	$c(E_\lambda)=8$
$\lambda=1/6$	curve $15a4$	$c(E_\lambda)=16$
$\lambda=1/3$	curve $42a1$	$c(E_\lambda)=16$
$\lambda=1/4$	curve $48a6$	$c(E_\lambda)=32$
$\lambda=2$	curve $102b1$	$c(E_\lambda)=32.$

Let now K be a number field. We begin the proof with a series of preliminary remarks in (a)–(d) below.

(a) Assume that there exists a prime $\mathfrak{P}$ such that $m:=\mathrm{ord}_{\mathfrak{P}}(\lambda-1)>0$. Then we immediately find from the computations of Δ and c_4 that the reduction of E/K modulo $\mathfrak{P}$ is of type I_{8m}. Similarly, if there exists a prime $\mathfrak{P}$ such that $m:=\mathrm{ord}_{\mathfrak{P}}(2\lambda-1)>0$, then the reduction of E/K modulo $\mathfrak{P}$ is of type I_{4m}.

(b) Assume now that there exists a prime $\mathfrak{P}$ such that $m:=\mathrm{ord}_{\mathfrak{P}}(\lambda)>0$. The above equation is not integral at $\mathfrak{P}$, but

$$y^2+(\lambda-(2\lambda-1)(\lambda-1))xy-\lambda^3(2\lambda-1)(\lambda-1)y=x^3-\lambda^2(2\lambda-1)(\lambda-1)x^2$$

is minimal. Its discriminant is $\lambda^8(\lambda-1)^8(2\lambda-1)^4(8\lambda^2-8\lambda+1)$. The reduction modulo $\mathfrak{P}$ is of type I_{8m}, and is split.

(c) Assume now that there exists a prime $\mathfrak{P}$ such that $m:=-\mathrm{ord}_{\mathfrak{P}}(\lambda)>0$. The Weierstrass equation E_λ is not integral at $\mathfrak{P}$, but the following equation is, where $\mu:=\lambda^{-1}$:

$$y^2+(\mu-(2-\mu)(1-\mu))xy-\mu(2-\mu)(1-\mu)y=x^3-(2-\mu)(1-\mu)x^2.$$

The discriminant of this new equation is $\mu^2(2-\mu)^4(1-\mu)^8(\mu^2-8\mu+8)$. When $2\notin\mathfrak{P}$, then the reduction modulo $\mathfrak{P}$ is of type I_{2m}. Modulo $\mathfrak{P}$, the reduction is $y^2-\bar{2}xy=x^3-\bar{2}x^2$, which may not be split. If $\mathrm{ord}_{\mathfrak{Q}}(2-\mu)=u>0$ for some prime ideal $\mathfrak{Q}$ with $2\notin\mathfrak{Q}$, then the reduction at $\mathfrak{Q}$ is split

multiplicative of type I_{4u}. If $\mathrm{ord}_{\mathfrak{L}}(1-\mu) = v > 0$ for some prime ideal $\mathfrak{L}$, then the reduction at $\mathfrak{L}$ is split multiplicative of type I_{8v}.

(d) Suppose that $\mathrm{ord}_{\mathfrak{P}}(2) = 1$, and that $\mu \in \mathfrak{P}$. Consider then the case where $\mathrm{ord}_{\mathfrak{P}}(2-\mu) = s > 1$, which corresponds to the case $\mathrm{ord}_{\mathfrak{P}}(\mu) = 1$ ($\mu \neq 2$). Then the equation is not minimal, but dividing by μ^6 leads to the equation

$$y^2 + (1 - \frac{(2-\mu)}{\mu}(1-\mu))xy - \frac{(2-\mu)}{\mu^2}(1-\mu)y = x^3 - \frac{(2-\mu)}{\mu^2}(1-\mu)x^2$$

which is minimal at (2). When $s > 2$, the reduction is split multiplicative of type I_{4s-8}, so $4 \mid c_{\mathfrak{P}}$. When $s = 2$, the reduction is good.

Suppose that $\mathrm{ord}_{\mathfrak{P}}(\mu) = m > 1$. It follows from Tate's algorithm that the equation

$$y^2 + (\mu - (2-\mu)(1-\mu))xy - \mu(2-\mu)(1-\mu)y = x^3 - (2-\mu)(1-\mu)x^2$$

is minimal at (2) and that it has reduction of type I_s^* for some $s > 0$. Therefore, 2 or $4 \mid c_{\mathfrak{P}}$. We claim that $4 = c_{\mathfrak{P}}$. To see this, it suffices to note that Tate's algorithm terminates when the equation $Y^2 + a_{3,i}Y - a_{6,2i}$ has distinct roots, and that $c_{\mathfrak{P}} = 4$ if the roots are in the residue field k. Since in our case, $a_6 = 0$, the latter condition is automatically satisfied.

We are now ready to proceed with the case $K = \mathbb{Q}$. Write $\lambda = \pm u/v$, with $u, v > 0$ coprime integers. If u is divisible by two distinct primes, then we conclude using (b) that $N^2 \mid c(E_\lambda)$.

2.13. We assume in this paragraph that u is divisible by a single prime. From (b), we find that $N \mid c(E_\lambda)$. If $v = 1$, then $u - 1$ is divisible by a prime unless $u = 2$. Except for this exception (curve 102*b*1), we find that $N^2 \mid c(E_\lambda)$ (use (a) and (b)). Assume now that u is divisible by a single prime, and that $v \neq 1$. If the numerator of $\lambda - 1$ is divisible by a prime, then $N^2 \mid c(E_\lambda)$ (use (a) and (b)). If the numerator of $2\lambda - 1$ is divisible by an odd prime and v is not a power of 2, then $N^2 \mid c(E_\lambda)$, where a factor N is contributed by the numerator of u/v, a factor 2 is contributed by an odd factor of the denominator of u/v, and a factor $N/2$ is contributed by the odd prime in the numerator of $2\lambda - 1$.

Assume now the numerator of $\lambda - 1$ is not divisible by a prime. Then $\lambda = u/v$, and $u - v = \pm 1$. If the numerator of $2(u/v) - 1$ is not divisible by an odd prime, then either $2u - v$ is even or $2u - v = \pm 1$. The former condition implies that v is even. Then, if v is divisible by an odd prime, we find that $N^2 \mid c(E_\lambda)$, a factor N being contributed by u, a factor 4 by the prime 2 in v, and a factor 2 by the odd prime in v. Assume now that

$2u - v = \pm 1$. Then, since $u - v = \pm 1$, $u \pm 1 = \pm 1$ has solution $u = 2$ with then $v = 3$, leading to the curve $42a1$.

Assume that v is not divisible by an odd prime. Then $u - v = \pm 1$ with $v = 2^s$ and $u = p^r$, p odd prime. In other words, $p^r - 2^s = \pm 1$. By Catalan's conjecture [50], we have $p^r = 3^2$ unless either $s = 1$ or $r = 1$. For the case $p^r = 3^2$, $2^s = 8$, we find that $2u - v = 10$ is divisible by an odd prime, thus contributing 4 to the divisibility of $c(E)$. The prime 2 in v also contributes 4 to $c(E)$, and the prime in u contributes 8. The proposition holds in this case. Assume now that $s = 1$. Then $p^r = 3$, leading to the case $\lambda = 3/2$ and the curve $21a3$, and to the case $\lambda = 3/4$ and the curve $48a6$.

Assume that $r = 1$, so that $p = 2^s \pm 1$, $s \geqslant 2$. Consider the numerator of $2\lambda - 1 = 2(p/2^s) - 1$, that is, $p - 2^{s-1}$. Then $p - 2^{s-1} = \pm 1 + 2^{s-1}$, and this numerator is divisible by a non-trivial prime unless $s = 2$ and $\lambda = 3/2$. The case $\lambda = 3/2$ was treated above already and gives the exception $21a3$. In all other cases, we can use (a) with a prime dividing the numerator of $2\lambda - 1$. Since $\mathrm{ord}_2(\mu) > 1$, we can also use (d), and we then conclude that the statement of the proposition holds in this subcase.

2.14. We now assume that $u = 1$, and set $\mu := \lambda^{-1} = \pm v \in \mathbb{Z}$. The case $\mu = 1$ need not be considered, as $\Delta = 0$ in this case. The case $\mu = -1$ is the curve $102b1$, with $c(102b1) = 32$. When $\mu \neq \pm 1$ is odd, $2 - \mu$ is divisible by an (odd) prime, unless $\mu = 3$, which gives the curve $42a1$ with $c(42a1) = 16$. The above considerations show that when μ is odd and $\mu \neq \pm 1$ or $\mu \neq 3$, then $N^2 \mid c(E)$.

Assume now that μ is even. If μ is divisible by an odd prime, then the proposition is proven if $2 - \mu$ is also divisible by an odd prime (see (c)). Consider then the case where $2 - \mu = \pm 2^s$. Since $\mu \neq 0$ and is divisible by an odd prime, we have $s > 1$. Then the reduction at (2) is of type I_{4s-8} (see (d)), and the proposition is proved in this case also, unless $\mu = 6$ and $s = 2$, which gives the curve $15a4$ with $c(15a4) = 16$.

It remains to consider the cases where μ is a power of 2. The case $\mu = 2$ is excluded since in this case $\Delta = 0$. The case $\mu = -2$ is the curve $21a3$ with $c(21a3) = 8$. Suppose that $\mu = \pm 2^m$ with $m > 1$. It follows from Tate's algorithm that the reduction is of type I_ℓ^* for some $\ell > 0$ (see (d)). Therefore, $4 \mid c_2$ in this case. The proposition is then proved when μ is a power of 2, since in this case $2 - \mu$ is divisible by an odd prime, unless $\mu = \pm 1, \pm 2, 4$. The case $\mu = 4$ is the curve $48a6$, with $c(48a6) = 32$. □

Remark 2.15. — Proving that the statement of the proposition is best possible, that is, that there exist infinitely many values of λ such that

$\mathrm{ord}_2(c(E_\lambda)) = 6$, does not seem to follow from standard conjectures. A computational search led to only finitely many values with $\mathrm{ord}_2(c(E_\lambda)) = 6$. Searching over $\lambda = 1/\mu$ with $\mu \in [3, 2 \cdot 10^5]$ produced the values $\mu = 9, 14, 54, 4374$ with $\mathrm{ord}_2(c(E_\lambda)) = 6$. When $\mu \in [-2 \cdot 10^5, -2]$, the values with $\mathrm{ord}_2(c(E_\lambda)) = 6$ are $\mu = -6, -10, -18, -26, -106, -162, -242, -2186$, and -8746. In view of c) in the above proof, an integer μ with:

(i) $|\mu| = 2p^r$ for some odd prime p and odd r, and
(ii) $|\mu - 1| = \ell^s$ for some prime ℓ and odd s, and
(iii) $|\mu - 2| = 4q^t$ for some odd prime q and odd t,

may produce an elliptic curve E with $\mathrm{ord}_2(c(E_\lambda)) = 6$ (more precisely, with good reduction at (2), and with $\mathrm{ord}_2(c_p) = 1$, $c_\ell = 8s$, and $c_q = 4t$). An integer $\mu = 2p^r$ with r even could also produce $c_p = 2$ if the reduction at p is not split. We searched through such integers to about 10^{500} and found only two additional values, $\mu = -1594322 = -3^{13} + 1$ and $\mu = -86093442 = -2 \cdot 3^{16}$, with $\mathrm{ord}_2(c(E_\lambda)) = 6$. We do not know whether there exist infinitely many integers with the properties (i)–(iii).

Remark 2.16. — Let $K = \mathbb{Q}(\sqrt{5})$. The prime (31) splits in K. Let λ be a root of $x^2 + x - 1$. The elliptic curve E/K given by $y^2 + (1-c)xy - by = x^3 - bx^2$, with $b = (2\lambda - 1)(\lambda - 1)$ and $c = (2\lambda - 1)(\lambda - 1)/\lambda$, has prime conductor $\mathfrak{P}$ one of the two prime ideals of K above (31), with reduction at $\mathfrak{P}$ of non-split multiplicative type I_1. Thus, E/K has $(0, 0)$ as K-rational torsion point of order 8, and $c(E/K) = 1$.

PROPOSITION 2.17 (**Case N=9**). — *Let E/K be an elliptic curve with a K-rational point of order $N = 9$.*

(a) *If $K = \mathbb{Q}$, then there exist at least two prime ideals (p) where $E/\mathbb{Q}$ has split multiplicative reduction of type I_{n_p} with $N \mid n_p$, except for the curve 54b3 in* [12]*, with $c(E) = 27$.*
(b) *If K is an imaginary quadratic field, then there exist at least two prime ideals $\mathfrak{P}$ in $\mathcal{O}_K$ where E/K has split multiplicative reduction of type $I_{n_\mathfrak{P}}$ with $N \mid n_\mathfrak{P}$, except for finitely many exceptions.*
(c) *If K is a real quadratic field, or $[K\colon \mathbb{Q}] > 2$, then there exists at least one prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$ where E/K has split multiplicative reduction of type I_n with $N \mid n$, except when E/K belongs to a list of at most $2^{9(\mathrm{rank}(\mathcal{O}_K^*)+1)}$ isomorphism classes of elliptic curves over K.*

Proof. — Let K be any field. For the point P on the curve $E(b, c)$ in (2.1) to have order $N = 9$, we need the relation between b and c obtained

by considering the y-coordinates of $[7]P = [-2]P$,

$$(b-c)^3 + c^3(b-c-c^2) = 0.$$

We find that $b = cd$, with $c := \lambda^2(\lambda-1)$, and $d := \lambda^2 - \lambda + 1$. The discriminant of $E(b,c)$ expressed in terms of λ is:

$$\Delta(\lambda) = \lambda^9(\lambda-1)^9(\lambda^2-\lambda+1)^3(\lambda^3-6\lambda^2+3\lambda+1).$$

For use in 2.24, let us note that

$$c_4(\lambda) = (\lambda^3-3\lambda^2+1)(\lambda^9-9\lambda^8+27\lambda^7-48\lambda^6+54\lambda^5-45\lambda^4+27\lambda^3-9\lambda^2+1).$$

It follows that there exists $\lambda \in K$ such that an elliptic curve E/K with a point of order $N = 9$ can be given by a Weierstrass equation of the form

$$E_\lambda : \quad y^2 + (1-\lambda^2(\lambda-1))xy - d\lambda^2(\lambda-1)y = x^3 - d\lambda^2(\lambda-1)x^2.$$

The curves in this family indexed by λ, $(\lambda-1)/\lambda$, and $-1/(\lambda-1)$, are isomorphic.

Let now K be a number field. Assume that there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda) > 0$. Then we immediately find from the computations of Δ and b_2 that the reduction of E/K modulo $\mathfrak{P}$ is split of type I_{9m}. If there exists a second maximal ideal $\mathfrak{P}'$ with $m' := \mathrm{ord}_{\mathfrak{P}'}(\lambda) > 0$, then we have a second place where the reduction is split multiplicative, this time of type $I_{9m'}$.

Assume now that there exists a prime $\mathfrak{P}$ such that $m := -\mathrm{ord}_{\mathfrak{P}}(\lambda) > 0$. The Weierstrass equation E_λ is not integral at $\mathfrak{P}$, but the following equation is, where $\mu := \lambda^{-1}$:

$$y^2 + (\mu^3 - (1-\mu))xy - \mu^4(\mu^2-\mu+1)(1-\mu)y = x^3 - \mu(\mu^2-\mu+1)(1-\mu)x^2.$$

The discriminant of this new equation is $\mu^9(1-\mu)^9(\mu^2-\mu+1)^3(1-6\mu+3\mu^2+\mu^3)$, and the reduction at $\mathfrak{P}$ is split of type I_{9m}. It follows from the above considerations that the proposition is proved if there exist two distinct prime ideals $\mathfrak{P}$ such that $\mathrm{ord}_{\mathfrak{P}}(\lambda) \neq 0$.

Assume now that there exists a single prime ideal $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda) \neq 0$. Then either $\lambda \in \mathcal{O}_K$ or $\mu \in \mathcal{O}_K$. Assume first that $\lambda \in \mathcal{O}_K$. Then $\lambda \in \mathfrak{P}$. Consider the element $\lambda - 1$. Clearly, $\mathrm{ord}_{\mathfrak{P}}(\lambda-1) = 0$. If there exists a maximal ideal $\mathfrak{Q} \neq \mathfrak{P}$ such that $m' := \mathrm{ord}_{\mathfrak{Q}}(\lambda-1) > 0$, then we find that the elliptic curve has reduction modulo $\mathfrak{Q}$ of type $I_{9m'}$. Otherwise, $\lambda - 1 \in \mathcal{O}_K^*$. When $K = \mathbb{Q}$, the only possibility is $\lambda = 2$. When K is an imaginary quadratic field, the set of elements of the form $\lambda = 1 + u$, with u a unit, is finite.

The argument when $\mu \in \mathcal{O}_K$ is similar, and we find that a second place of multiplicative reduction of type $I_{9m'}$ exists, unless $1-\mu$ is a unit. When $K=\mathbb{Q}$, the only possibility is $\lambda = 1/2$.

When $\mathrm{ord}_{\mathfrak{P}}(\lambda) = 0$ for all $\mathfrak{P}$, *i.e.*, when $\lambda \in \mathcal{O}_K^*$, we find that there may not be in general two places of multiplicative reduction with $9 \mid c_v$. There will be at least one such place if $\lambda - 1$ is not a unit in $\mathcal{O}_K^*$. As we recalled in 2.3, the equation $X+Y=1$, with $X, Y \in \mathcal{O}_K^*$, has a number of solutions in $(\mathcal{O}_K^*)^2$ bounded by the constant $2^{9(\mathrm{rank}(\mathcal{O}_K^*)+1)}$.

When $K=\mathbb{Q}$, the values $\lambda = -1, 2$, and $1/2$, all produce an equation for the curve $54b3$, with $c(54b3) = 27$. □

Remark 2.18. — Over $K=\mathbb{Q}(\zeta_3)$, the elliptic curve E/K obtained by setting $\lambda = \zeta_3$ has a K-rational point of order $N=9$ with $c(E)=27$.

Over $K=\mathbb{Q}(\sqrt{5})$, the elliptic curve E/K obtained by setting $\lambda = (3+\sqrt{5})/2$ has a K-rational point of order $N=9$ with $c(E)=3$. It has reduction of type I_1 at one of the prime ideals above (19), and reduction of type I_3 at the prime ideal (2).

Remark 2.19. — We did not find any elliptic curve $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order $N=9$ and $\mathrm{ord}_3(c(E)) = 4$. The curves $714i1$, $1482l1$, $1554n1$, and $6942n1$ (with $\lambda = -2, 3, -3$ and 4) have $\mathrm{ord}_3(c) = 5$. The curves E_λ with $\lambda = -4, 5, -8, 9, -31, 32, -127, 128, -8191$, and $8192 = 2^{13}$, have $\mathrm{ord}_3(c) = 6$. The curves with $\lambda = -2 \cdot 3^4$, $-2^5 3^2$, $2^7 3$, $-2^8 3$, $-2^4 3^5$, $-2^7 3^4$, 2^{19}, and 2^{31}, have $\mathrm{ord}_3(c) = 7$. It is not clear whether there exist infinitely many curves E_λ with $\mathrm{ord}_3(c) = 6$, or with $\mathrm{ord}_3(c) = 7$.

PROPOSITION 2.20 (**Case N=10**). — *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order $N=10$. Then $50 \mid c(E)$.*

Proof. — We set

$$b := \frac{\lambda^3(\lambda-1)(2\lambda-1)}{(\lambda^2-3\lambda+1)^2} \quad \text{and} \quad c := \frac{-\lambda(\lambda-1)(2\lambda-1)}{(\lambda^2-3\lambda+1)}.$$

The discriminant of $E(b,c)$ expressed in terms of λ is:

$$\Delta(\lambda) = \frac{\lambda^{10}(\lambda-1)^{10}(2\lambda-1)^5(4\lambda^2-2\lambda-1)}{(\lambda^2-3\lambda+1)^{10}}.$$

There exists $\lambda \in K$ such that an elliptic curve E/K with a point of order $N=10$ can be given by a Weierstrass equation of the form

$$E_\lambda \colon y^2 + (1-c)xy - by = x^3 - bx^2,$$

with b and c as above. The curves in this family indexed by λ and $(\lambda - 1)/(2\lambda-1)$ are isomorphic. All isogenies between the curves below are of

degree 2, and are related by the formula $\lambda \to -1/2(\lambda - 1)$. We collect here some explicit computations:

$$\begin{array}{lll} \lambda = 2 & \text{curve } 66c1 & c(E_\lambda) = 50 \\ \lambda = -1/2 & \text{curve } 66c2 & c(E_\lambda) = 100 \\ \lambda = -1 & \text{curve } 150a3 & c(E_\lambda) = 100 \\ \lambda = 1/4 & \text{curve } 150a4 & c(E_\lambda) = 100 \\ \lambda = 3 & \text{curve } 870i1 & c(E_\lambda) = 500 \\ \lambda = -1/4 & \text{curve } 870i2 & c(E_\lambda) = 500. \end{array}$$

(a) Let now K be a number field. Assume that there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda) > 0$. Then we immediately find from the computations of Δ and b_2 that the reduction of E/K modulo $\mathfrak{P}$ is split of type I_{10m}. Similarly, if there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda - 1) > 0$, then the reduction of E/K modulo $\mathfrak{P}$ is split of type I_{10m}.

(b) Assume now that there exists a prime $\mathfrak{P}$ such that $m := -\mathrm{ord}_{\mathfrak{P}}(\lambda) > 0$. The Weierstrass equation E_λ is not integral at $\mathfrak{P}$, but the following equation is, where $\mu := \lambda^{-1}$. Write

$$b' := \frac{(2-\mu)(1-\mu)}{\mu(1-3\mu+\mu^2)^2} \quad \text{and} \quad c' := \frac{-(2-\mu)(1-\mu)}{\mu(1-3\mu+\mu^2)},$$

with equation

$$y^2 + \mu(1-c')xy - \mu^3 b' y = x^3 - \mu^2 b' x^2. \tag{2.2}$$

The discriminant of this new equation is

$$\frac{\mu^5(1-\mu)^{10}(2-\mu)^5(4-2\mu-\mu^2)}{(1-3\mu+\mu^2)^{10}}.$$

When $2 \notin \mathfrak{P}$, this equation is minimal, with reduction at $\mathfrak{P}$ split of type I_{5m}.

(c) Consider now the case where $K = \mathbb{Q}$. Assume that $\mathfrak{P} = (2)$. Then the new equation (2.2) is not minimal, and after an obvious change of variables (dividing the equation by 2^6), we obtain

$$y^2 + \left(\frac{\mu}{2} - \frac{-(2-\mu)(1-\mu)}{2(1-3\mu+\mu^2)}\right)xy - \frac{\mu^2(2-\mu)(1-\mu)}{8(1-3\mu+\mu^2)^2}y = x^3 - \frac{\mu(2-\mu)(1-\mu)}{4(1-3\mu+\mu^2)^2}x^2.$$

When $m := \mathrm{ord}_2(\mu) > 1$, this equation is minimal, with reduction split of type I_{5m-5}. When $\mathrm{ord}_2(\mu) = 1$, then the equation is also minimal, with reduction split of type I_{5n}, where $n = \mathrm{ord}_2((1-\mu/2))$. In each case, the Tamagawa number is divisible by 5.

(d) Assume now that $\mu \in \mathbb{Z}$. Let p be a prime dividing $d' := (1-3\mu+\mu^2)$. This prime is obviously coprime to any divisor of μ. The equation (2.2) is not integral at p, but the following one is:

$$y^2 + \mu d'(1-c')xy - \mu^3 d'^3 b' y = x^3 - \mu^2 d'^2 b' x^2.$$

The discriminant of this new equation is

$$\mu^5(1-\mu)^{10}(2-\mu)^5(4-2\mu-\mu^2)(1-3\mu+\mu^2)^2.$$

This equation is minimal with reduction modulo p of type I_{2s} with $s := \mathrm{ord}_p(d')$, unless $p = 5$. Indeed, it follows that Tate's algorithm that such a curve will have multiplicative reduction unless $p \mid b_2$. One easily verifies that $p \mid b_2$ and $p \mid d'$ if and only if $p = 5$.

When $p = 5$, it follows from Tate's algorithm that the reduction is of type III, since then $p^3 \nmid b_8$ (with here $b_8 = a_2 a_3^2$). In this case also, the Tamagawa number is even, with in fact $c_5 = 2$.

We may now prove the proposition as follows. Write $\lambda = \pm a/b$, $a, b > 0$ coprime integers. If a is divisible by two distinct primes, then we conclude using (a) that $100 \mid c(E_\lambda)$. If a is a power of a single prime p and $b = 1$, we note that $a - 1$ is not a unit unless $a = 2$. Then we conclude from (a) that $100 \mid c(E_\lambda)$, unless $a = 2$, $b = 1$. When $\lambda = a = 2$, we find the curve $66c1$ with $c = 50$.

If a is divisible by a single prime and $b \neq 1$, we use (a), and (b) and (c) to find that $50 \mid c(E)$. If $a = 1$ and b is divisible by at least two distinct primes, we use (b), (c), and (d) to find that $50 \mid c(E)$. If $a = 1$ and b is divisible by a single prime, then $(\pm 1/b) - 1$ has a numerator divisible by a prime unless $b = 2$. This case, $\lambda = 1/2$, need not be considered since the discriminant is 0. We then use (a), (c), and (d) to find that $50 \mid c(E)$. □

Remark 2.21. — Under the hypotheses of Proposition 2.20, one may wonder whether the conclusion $500 \mid c(E)$ holds, unless E is one of the four curves $66c1$, $66c2$, $150a3$, and $150a4$.

In our next proposition, one may wonder whether $N^2 \mid c(E)$ always holds. The curve $90c3$ has a point of order 12 and $c(E) = 12^2$. The curve $30a2$ has a torsion subgroup of order 12 which is not cyclic, with $c(E) = 24$.

PROPOSITION 2.22 (**Case N=12**). — *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order $N = 12$. Then $N \mid c(E)$.*

Proof. — We set

$$b := \frac{\lambda(2\lambda-1)(3\lambda^2-3\lambda+1)(2\lambda^2-2\lambda+1)}{(\lambda-1)^4},$$

and

$$c := \frac{-\lambda(2\lambda-1)(3\lambda^2-3\lambda+1)}{(\lambda-1)^3}.$$

The discriminant of $E(b,c)$ expressed in terms of λ is:

$$\Delta(\lambda) = \frac{\lambda^{12}(2\lambda-1)^6(3\lambda^2-3\lambda+1)^4(2\lambda^2-2\lambda+1)^3(1-6\lambda+6\lambda^2)}{(\lambda-1)^{24}}.$$

The curves in this family indexed by λ and $1-\lambda$ are isomorphic. We collect here some explicit computations:

$\lambda = 1/3$	curve $90c3$	$c(E_\lambda) = 12^2$
$\lambda = 1/4$	curve $210b5$	$c(E_\lambda) = 2 \cdot 12^2$
$\lambda = -1/2$	curve $4290bb4$	$c(E_\lambda) = 6 \cdot 12^2$
$\lambda = 2$ or $\lambda = -1$	curve $2730bd1$	$c(E_\lambda) = 6 \cdot 12^2$.

Let now K be a number field. Assume that there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda) > 0$. Then we immediately find from the computations of Δ and b_2 that the reduction of E/K modulo $\mathfrak{P}$ is split of type I_{12m}. The proposition is thus proved when there exists a prime $\mathfrak{P}$ such that $m := \mathrm{ord}_{\mathfrak{P}}(\lambda) > 0$. Consider then the case where $\mu := \lambda^{-1} \in \mathcal{O}_K$.

Assume now that there exists a prime $\mathfrak{P}$ such that $m := -\mathrm{ord}_{\mathfrak{P}}(\lambda) > 0$. The Weierstrass equation E_λ is not integral at $\mathfrak{P}$, but the equation with invariants a_1, a_2, a_3 given below, and $a_4 = a_6 = 0$, is integral, where $\mu := \lambda^{-1}$:

$$\begin{aligned} a_1 &= \mu(1-\mu)^3 + (2-\mu)(3-3\mu+\mu^2) \\ a_2 &= -(1-\mu)^2(2-\mu)(3-3\mu+\mu^2)(2-2\mu+\mu^2) \\ a_3 &= -\mu(1-\mu)^5(2-\mu)(3-3\mu+\mu^2)(2-2\mu+\mu^2) \end{aligned}$$

c The discriminant of this new equation is

$$\mu^2(1-\mu)^{12}(2-\mu)^6(3-3\mu+\mu^2)^4(2-2\mu+\mu^2)^3(\mu^2-6\mu+6).$$

We compute $b_2 := a_1^2 + 4a_2$ to be

$$\mu^8 + 168\mu^5 - 36\mu^6 - 372\mu^4 + 468\mu^3 - 336\mu^2 + 120\mu - 12.$$

When $2 \notin \mathfrak{P}$ or $3 \notin \mathfrak{P}$, the new equation is minimal, with reduction at $\mathfrak{P}$ of type I_{2m}. Assume that $\mu \in \mathbb{Z}$. Then $\mu - 1$ is divisible by a prime unless $\mu = 2$, and $\mu = 2$ need not be considered since in this case $\Delta = 0$. It is easy to check that for any $p \mid (1-\mu)$, the reduction is split of type $I_{12m'}$, and the proposition is proved. □

Proposition 2.23. — *Let $E/\mathbb{Q}$ be an elliptic curve with Tamagawa product $c(E)$. Then $c(E)/|E(\mathbb{Q})_{\mathrm{tors}}| \geqslant 1/5$, with equality only when $E = X_1(11)$.*

Proof. — Recall that the possible group structures for $E(\mathbb{Q})_{\mathrm{tors}}$ are $\mathbb{Z}/N\mathbb{Z}$ for $N = 1, \ldots, 10$ and 12, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $1 \leqslant N \leqslant 4$ (see [47], Thm. 8). Propositions 2.9, 2.10, 2.12, 2.17, 2.20, and 2.22, prove our claim when $E(\mathbb{Q})_{\mathrm{tors}}$ is cyclic. Note that in 2.7, the exception $11a3$ is isomorphic to $X_1(11)$.

In the case $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, our claim follows from the fact that the elliptic curves in 2.4 with $c = 1$ have a torsion subgroup of order exactly 4. Similarly, in the case $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, our claim follows from the fact that the elliptic curves in 2.9 with $c = 2$ or $c = 3$ have a torsion subgroup of order exactly 6. Finally, in the case $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, 2.12 shows that $8 \mid c(E)$. □

The complete list of possible subgroups $E(K)_{\mathrm{tors}}$ of an elliptic curve E/K over a quadratic number field can be found in [33]. One finds that $|E(K)_{\mathrm{tors}}| \in [1, 16] \cup \{18, 20, 24, 36\}$. We showed in 2.11 and 2.16 that $c(E)/|E(K)_{\mathrm{tors}}|$ can take the values $1/7$ and $1/8$ when $[K\colon \mathbb{Q}] = 2$. An example of an elliptic curve over a cubic field with $c(E)/|E(K)_{\mathrm{tors}}| = 1/13$ can be found in [34].

Our next proposition shows that when $N = 5, 7$ or 9, the number of exceptions to the divisibility $N \mid c$ or $N^2 \mid c$, for a given number field K, cannot be bounded by a constant independent of the number field.

PROPOSITION 2.24. — *Let $d > 0$ be any integer. Fix $N = 5, 7$, or 9. Then there exists a number field K such that at least d distinct isomorphism classes of elliptic curves E/K have distinct j-invariants in $\mathcal{O}_K^*$, have a point of order N, and $c(E) = 1$.*

Proof. — Let us denote by $c_4(x)$ and $\Delta(x)$ two integer polynomials such that $j(E_\lambda) = c_4(\lambda)^3/\Delta(\lambda)$ (see 2.7, 2.10, and 2.17). When $N = 5, 7$ or 9, we can choose these polynomials to be monic. Let K denote the extension of $\mathbb{Q}$ generated by a root ρ of the monic equation

$$1 + \prod_{i=1}^{d} c_4(x^i)\Delta(x^i) \prod_{i \neq j,\ i,j \in \{1,\ldots,d\}} \left(c_4(x^i)^3\Delta(x^j) - c_4(x^j)^3\Delta(x^i) - 2\right) = 0.$$

Set $\lambda = \rho^i$ and consider the elliptic curves E_{ρ^i}, $i = 1, \ldots, d$. Since $\lambda \in \mathcal{O}_K$, the associated Weierstrass equations are integral, with integral discriminant. By construction,

$$\prod_{i=1}^{d} c_4(\rho^i)\Delta(\rho^i) \prod_{i \neq j, i,j \in \{1,\ldots,d\}} \left[c_4(\rho^i)^3\Delta(\rho^j) - c_4(\rho^j)^3\Delta(\rho^i) - 2\right]$$

is a product of units in $\mathcal{O}_K^*$. In particular, $j(E_{\rho^i}) \in \mathcal{O}_K^*$ for $i = 1, \ldots, d$. Moreover, $j(E_{\rho^i}) \neq j(E_{\rho^j})$ if $i \neq j$, since 2 is not a unit in $\mathcal{O}_K$. Since the

discriminant of E_{ρ^i} is a unit, E_{ρ^i} has good reduction at all places of K, and $c = \prod_{\mathfrak{P}} c_{\mathfrak{P}} = 1$. □

Remark 2.25. — Consider the elliptic curve $E_3/\mathbb{Q}(\lambda)$, given by

$$y^2 - xy - \lambda y = x^3,$$

with $(0,0)$ as a 3-torsion point[(1)]. Its discriminant is $\lambda^3(1-27\lambda)$. It has reduction of type I_3 at (λ). Setting $\mu := \lambda^{-1}$, we consider the equation $y^2 - \mu xy - \mu^2 y = x^3$ to find that the reduction at ∞ is of type IV^*. The new discriminant is $\mu^8(\mu - 27)$. The reduction is non-split of type I_1 at $(\mu - 27)$.

Clearly, setting λ to be a prime p in $\mathbb{Z}$ produces an elliptic curve $E_{3,\lambda}/\mathbb{Q}$ with Tamagawa number $c_p = 3$. This gives infinitely many examples of curves $E_{3,\lambda}/\mathbb{Q}$ with a point of order 3 and with $3 \mid c$.

LEMMA 2.26. — *There are infinitely many values $\mu \in \mathbb{Z}$ such that the elliptic curve $y^2 - \mu xy - \mu^2 y = x^3$, with 3-torsion point $(0,0)$, has $c = 1$.*

Proof. — Choose $\mu = t^3$. Then the curve $y^2 - \mu xy - \mu^2 y = x^3$ can be given by the equation $y^2 - txy - y = x^3$, with discriminant $(t^3 - 27)$, and $c_4 = t^4 - 24t$. The polynomial $t^3 - 27$ takes infinitely many squarefree values [21]. Choose $t \in \mathbb{Z}$ such that $t^3 - 27$ is squarefree. Then $3 \nmid t$. Pick a prime p which divides $t^3 - 27$. It follows that $p \nmid c_4$, and so the reduction at p is multiplicative of type I_1. □

Remark 2.27. — The curve $E/\mathbb{Q}(t)$ defined by $y^2 - txy - y = x^3$ has exactly four semistable fibers over $\overline{\mathbb{Q}}$, with reduction of type I_1, I_1, I_1 and I_9. Over $\mathbb{C}$ there is a unique such fibration [2]. The equation $X^2Y + Y^2Z + Z^2X - tXYZ = 0$ is an alternate equation for E.

Remark 2.28. — Let K be a number field and let G/K be a smooth group scheme with an integral model of finite type $\mathcal{G}/\operatorname{Spec}(\mathcal{O}_K)$. The class group $C(\mathcal{G})$ is defined for instance in [26]. When $G = \mathbb{G}_{m,K}$ and $\mathcal{G} = \mathbb{G}_{m,\mathcal{O}_K}$, $C(\mathcal{G})$ is nothing but the ideal class group of K. When G/K is an abelian variety A/K and $\mathcal{G}/\operatorname{Spec}(\mathcal{O}_K)$ is the connected component of zero $\mathcal{A}^0$ of the Néron model $\mathcal{A}/\operatorname{Spec}(\mathcal{O}_K)$ of A/K, the group $C(\mathcal{A}^0)$ is identified with the cokernel of the product of the local reduction maps:

$$C(\mathcal{A}^0) = \operatorname{Coker}(A(K) \xrightarrow{\text{red}} \prod_v \Phi_v(k_v))$$

(1) This curve is not universal with this property. One also has the isotrivial curve $y^2 + \lambda y = x^3$ with reduction IV^* and IV and $j = 0$.

(see [26]). It is natural to also consider the intermediate quotient $\prod_v \Phi_v(k_v) \to C(\mathcal{A}^0)_t \to C(\mathcal{A}^0)$, with

$$C(\mathcal{A}^0)_t := \mathrm{Coker}(A(K)_{\mathrm{tors}} \xrightarrow{\mathrm{red}} \prod_v \Phi_v(k_v)).$$

Let $P \in A(K)_{\mathrm{tors}}$ be a point of order N. We remark here that many of the results in this article, proving that $N \mid |\prod_v \Phi_v(k_v)|$, can be sharpened to state that $\mathrm{red}(P)$ has order N in $\prod_v \Phi_v(k_v)$, thus providing some information on the quotient $C(\mathcal{A}^0)_t$. Indeed, in many of our arguments, the torsion point P is the point $(0,0)$ on a curve $y^2+(1-c)xy-by = x^3-bx^2$, and we consider this equation modulo a prime $\mathfrak{P}$ with $b \in \mathfrak{P}$ and $1-c \notin \mathfrak{P}$ resulting in a reduction of split multiplicative type. We note then that the point $(0,0)$ reduces modulo $\mathfrak{P}$ to the singular point. When such is the case, the image of P is not trivial in $\Phi_{\mathfrak{P}}(\mathcal{O}_K/\mathfrak{P})$, and has order exactly N when N is prime.

We note however that it is not always the case when $N \mid |\prod_v \Phi_v(k_v)|$ that $\mathrm{red}(P)$ has order N in $\prod_v \Phi_v(k_v)$, as the following examples show. Consider an abelian variety A/K with $c = 1$ (so that $\mathrm{red}(P)$ is trivial). Assume that A/K has everywhere semi-stable reduction (such as $11a3$ with $N = 5$). Then it is always possible to find a finite extension L/K such that at some place w of L over a place v of bad reduction of A/K, the Tamagawa number of A_L/L is divisible by N. On the other hand, by construction, $P \in A_L(L)$, and $\mathrm{red}_L(P)$ is trivial.

To find an example over $\mathbb{Q}$, consider the elliptic curve $E_t/\mathbb{Q}$ given by the equation $y^2 - txy - y = x^3$, with $\Delta = t^3 - 27$ and $c_4 = t^4 - 24t$. The point $P := (0,0)$ has order 3. Choose $t \in \mathbb{Z}$ coprime to 3 such that there exists a prime p with $3 \mid \mathrm{ord}_p(t-3)$, and $p \equiv 1 \pmod 3$ (say $t = 7^3+3$). We claim that $\mathrm{red}(P)$ is trivial in $\prod_v \Phi_v(k_v)$, and that $\Phi_p(\mathbb{F}_p)$ has order divisible by 3.

Indeed, any prime $q \neq 3$ dividing the discriminant does not divide c_4. Thus the equation $y^2 - txy - y = x^3$ is minimal at q and the curve has multiplicative reduction. Clearly, $(0,0)$ is not a singular point on the reduced equation modulo q. It follows that the point P reduces to a point of order 3 in the connected component of zero of the Néron model of E_t at q. Since the reduction is multiplicative, we find that the reduction is split if $q \equiv 1 \pmod 3$, and not split if $q \equiv 2 \pmod 3$. When the reduction is split, $|\Phi_q(\mathbb{F}_q)| = \mathrm{ord}_q(\Delta)$.

Remark 2.29. — Let us remark here that when $E/\mathbb{Q}$ has a subgroup $G/\mathbb{Q}$ of order $N = 5$ or 7 defined over $\mathbb{Q}$, one does not expect in general that $N \mid c(E)$. Indeed, consider the isogeny class $\mathcal{C} = \{858k1, 858k2\}$ in [12].

Then $858k1$ has a $\mathbb{Q}$-rational point P of order 7, and $c(858k1) = 2 \cdot 7^3$. The curve $858k2$ is the quotient of $858k1$ by the subgroup generated by P, and this quotient does not have any non-trivial $\mathbb{Q}$-rational point. The kernel of the isogeny between $858k2$ and $858k1$ is defined over $\mathbb{Q}$ and has order 7, and one finds in [12] that $c(858k2) = 2$.

A similar example is obtained for $N = 5$ by considering the isogeny class $\mathcal{C}' = \{880g1, 880g2\}$, where the curves are linked by 5-isogenies. Both curves have trivial Mordell-Weil groups over $\mathbb{Q}$, with $c(880g1) = 20$ and $c(880g2) = 4$.

We now use $\mathcal{C}$ and $\mathcal{C}'$ to answer negatively the following question. There are several "special" curves in a given isogeny class $\mathcal{C}$ of conductor N. For instance, $\mathcal{C}$ contains the optimal quotient E_0 of $J_0(N)$, and the optimal quotient E_1 of $J_1(N)$. One may wonder whether the minimal value of the ratio $c(E)/|E_{\mathrm{tors}}(\mathbb{Q})|^2$ over all curves $E \in \mathcal{C}$ is always achieved with $E = E_1$. While this statement is true for many isogeny classes $\mathcal{C}$, it is not true in general. Indeed, it is known that there is an isogeny $E_1 \to E_0$ with constant kernel (see, *e.g.*, [69], Remark 1.8). Thus, when an isogeny class consists of two curves only, and either both curves have trivial torsion, or only the optimal quotient E_0 has non-trivial torsion, then we find that $E_1 = E_0$. This is the case for both $\mathcal{C}$ and $\mathcal{C}'$.

3. Abelian varieties of higher dimension

Most of the results in this section are variations on the following simple proposition. A refinement of the argument used in the proposition, for abelian surfaces, is presented in 3.8.

PROPOSITION 3.1. — *Let $K/\mathbb{Q}$ be a number field. Let p be prime, and let $\mathfrak{P}$ denote a prime ideal of $\mathcal{O}_K$ containing p. Let $k := \mathcal{O}_K/\mathfrak{P}$. Let A/K be any abelian variety of dimension g. Let $c_{\mathfrak{P}}$ denote the Tamagawa number of A at $\mathfrak{P}$. Let N be prime, $N \neq p$. Assume that for some $d \geqslant 1$,*

$$N^d \mid |A(K)_{\mathrm{tors}}|, \text{ and } N^d > (\lfloor 1 + 2\sqrt{|k|} + |k| \rfloor)^g.$$

Then $N \mid c_{\mathfrak{P}}$. More precisely, $N^a \mid c_{\mathfrak{P}}$ whenever $N^{d+1-a} > (\lfloor 1 + 2\sqrt{|k|} + |k| \rfloor)^{g-1}(1 + |k|)$. Moreover, when $N > 2g + 1$, the reduction at $\mathfrak{P}$ has positive toric rank, and is thus not potentially good.

Proof. — Let $\mathcal{A}_k/k$ denote the special fiber of the Néron model at $\mathfrak{P}$. Consider the natural reduction map red: $A(K) \to \mathcal{A}_k(k)$. It is well-known that this map is injective when restricted to the subgroup of K-rational

torsion points of order prime to p. The connected component of zero $\mathcal{A}_k^0/k$ of the special fiber of the Néron model of A/K at $\mathfrak{P}$ is a smooth connected commutative group scheme of dimension g over k. Such a group scheme contains at most $(\lfloor 1+2\sqrt{|k|}+|k|\rfloor)^g$ k-rational points (see, *e.g.*, [10], 3.2, Prop. 11, and note that the proof in the case of tori needs to be modified).

Our hypothesis shows that $\Phi_{\mathfrak{P}}(k) \neq (0)$. Since $\mathcal{A}_k^0 = \mathcal{A}_k$ when the reduction is good, we find that under our hypothesis, $|\mathcal{A}_k^0(k)| \leqslant (\lfloor 1+2\sqrt{|k|}+|k|\rfloor)^{g-1}(1+|k|)$.

It is shown in [43] that if q is a prime dividing the order of the component group of the special fiber of a Néron model with toric rank $t=0$, then either $q=p$, or $q \leqslant 2g+1$. To see this, apply [43], 2.15, in the case where $t_K = 0$. Since in our case the component group is divisible by the prime $N > 2g+1$, we find that the reduction at $\mathfrak{P}$ has positive toric rank. □

COROLLARY 3.2. — *Let $A/\mathbb{Q}$ be an abelian variety of dimension g. If 7^g or 9^g divides $|A(\mathbb{Q})_{\mathrm{tors}}|$, then $7^{g-\lfloor 0.8271g\rfloor} \geqslant 7$, or $3^{2g-\lfloor 1.465g\rfloor} \geqslant 3$, divides c_2, respectively.*

Proof. — This follows immediately from the previous proposition, noting that $\lfloor 1+2\sqrt{2}+2\rfloor = 5$. □

Remark 3.3. — The statement of the corollary is sharp, in the sense that there exists an elliptic curve over $\mathbb{Q}$ with a point of order 5 and $c=1$ (see 2.7). In view of the fact that there exists an elliptic curve with a point of order 7 and $c=7$ (see 2.10), the strongest conclusion that could possibly hold with the hypotheses of Corollary 3.2 is that $N^g \mid c$.

When $N > 7$ is prime and N^g divides $|A(\mathbb{Q})_{\mathrm{tors}}|$, the proposition also implies that $N \mid c_2$. However, we do not know of any example of an abelian variety $A/\mathbb{Q}$ of dimension $g > 1$ such that N^g divides $|A(\mathbb{Q})_{\mathrm{tors}}|$ and $N \geqslant 11$. One may wonder whether a principally polarized abelian variety $A/\mathbb{Q}$ of dimension $g > 1$ can have $(\mathbb{Z}/N\mathbb{Z})^g$ isomorphic to a subgroup of $A(\mathbb{Q})$ when $N = 11$ or $N > 12$.

COROLLARY 3.4. — *Let $[K\colon \mathbb{Q}] = 2$ and let A/K be an abelian variety of dimension g. If $N \geqslant 11$ is prime and $N^g \mid |A(K)_{\mathrm{tors}}|$, then $N \mid c_{\mathfrak{P}}$ for all $\mathfrak{P}$ above (2).*

Proof. — The statement follows from the previous proposition, noting that the residue field at $\mathfrak{P}$ can be $\mathbb{F}_4$, and that $\lfloor 1+2\sqrt{2^2}+2^2\rfloor = 9$. □

Remark 3.5. — Examples of quadratic extensions K with an elliptic curve E/K having a torsion point of order $N = 11$ or $N = 13$ are given in [63], Table I and Table II. As predicted by the above proposition, the

reduction at any $\mathfrak{P}$ above (2) is of type I_n with $N \mid n$. For $N = 11$ one finds in Table I an example of an elliptic curve E/K with exactly one single prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ such that $N \mid c_{\mathfrak{P}}$.

The hypothesis $N \geqslant 11$ of the corollary is sharp. Indeed, there exists an elliptic curve $E/\mathbb{Q}(\sqrt{-3})$ with a $\mathbb{Q}(\sqrt{-3})$-rational point of order 7 and $7 \nmid c$ (see 2.11). One may wonder whether $N^g \mid c$ holds under the hypotheses of 3.4.

Example 3.6. — Let $p > 3$ be prime, and let $J_1(p)/\mathbb{Q}$ denote the Jacobian of the modular curve $X_1(p)/\mathbb{Q}$. Then $J_1(p)/\mathbb{Q}$ has bad reduction only at the prime p, and its component group Φ_p is trivial [11]. The $\mathbb{Q}$-rational cuspidal torsion subgroup of the modular Jacobian $J_1(p)$ is computed in [11] for primes $11 \leqslant p \leqslant 71$, and for $p \leqslant 100$ in [70]. For each prime N dividing the order of the cuspidal subgroup of $J_1(p)(\mathbb{Q})$, we find that N does not divide the order of the product c of the Tamagawa numbers of $J_1(p)$.

The modular Jacobians $J_0(p^n)/\mathbb{Q}$ also have bad reduction only at the prime p. The relationship between the torsion in $J_0(p^n)(\mathbb{Q})$ and the component group Φ_p is completely established in [47] when $n = 1$. Partial results are obtained for $n > 1$ in [44]. The cuspidal subgroup of $J_0(p^n)(\mathbb{Q})$ is computed in [40], and we find that the order of the p-part of this subgroup is in general larger than the order of the p-part of the component group at p. Optimal quotients of $J_0(p)$ are discussed in [20].

Modular Jacobians of genus 1 have already appeared in the previous section. In 2.4, the curve $15a8$ with $c = 1$ is $X_1(15)$. In 2.7, the curve $11a3$ with $c = 1$ is $X_1(11)$. In 2.9, the curve $14a4$ with $c = 2$ is $X_1(14)$ and the curve $14a6$ with $c = 2$ is $X_1(14)/w_2$. In 2.12, the curve $21a3$ with $c = 8$ is $X_0(21)/w_7$ (see [18]). It can also be noted that $17a4$ in 2.4, $20a2$ in 2.9, and $42a1$ in 2.12, are optimal quotients of $J_1(17)$, $J_1(20)$, and $J_1(42)$, respectively. This can be checked as follows: Each of these curves in the numbering of the Antwerp Tables (also included in [12]) is the A-curve in its isogeny class. One finds in [66], page 104, Numerical Evidence, that indeed these A-curves are optimal quotient of $J_1(N)$.

Example 3.7. — Let $p \geqslant 5$ be prime, and consider the Fermat curve F_p given by $x^p + y^p = z^p$. The Fermat quotient $C_a/\mathbb{Q}$ is the smooth projective curve associated with the plane curve given by the equation $y^p = x^a(1-x)$, with $1 \leqslant a \leqslant p-2$. The Fermat Jacobian $\mathrm{Jac}(F_p)/\mathbb{Q}$ and the Jacobian $J_a/\mathbb{Q}$ of C_a are other examples of abelian varieties which have bad reduction only at p. The group $J_a(\mathbb{Q})$ has a point of order p and $\mathrm{Jac}(F_p)(\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^2$ ([68], Thm. 1).

Regular models for $C_a/\mathbb{Q}_p$ are provided in full generality in [49], Section 6. We find for instance that when p is not a Wieferich prime, the minimal regular model of $C_1/\mathbb{Q}_p$ has an integral special fiber. It follows that the Jacobian $J_1/\mathbb{Q}$, of dimension $g = (p-1)/2$, has a point of order $2g+1$ and Tamagawa product $c = 1$.

We conclude this section by considering the case of abelian surfaces, where the general bound for the number of points of a smooth commutative group scheme over a finite field can be refined as follows. Let $A/\mathbb{F}_q$ be an abelian surface. Then (see, *e.g.*, [10], 5.3):

$$|A(\mathbb{F}_2)| \in \{1,\dots,16\} \cup \{19,20\} \cup \{25\},$$
$$|A(\mathbb{F}_3)| \in \{1,\dots,16\} \cup \{18,\dots,25\} \cup \{28,29,30\} \cup \{34,35,36,42,49\}.$$

Let $T/\mathbb{F}_q$ be a torus of dimension 2. Then

$$T(\mathbb{F}_q) \in \left\{(q-1)^2, q^2-q+1, q^2-1, q^2+1, q^2+q+1, (q+1)^2\right\}.$$

In particular, $|T(\mathbb{F}_2)| \in \{1,3,5,7,9\}$ and $|T(\mathbb{F}_3)| \in \{4,7,8,10,13,16\}$. When $|T(\mathbb{F}_2)| = 9$, note that $T(\mathbb{F}_2) = (\mathbb{Z}/3\mathbb{Z})^2$.

PROPOSITION 3.8. — *Let $A/\mathbb{Q}$ be an abelian surface with a $\mathbb{Q}$-rational point of order N.*

(a) *If $N = 17, 23$, or if $N \geqslant 29$ is coprime to 210, then $N \mid c_2$.*
(b) *If $N = 22$ or 26, then $N/2 \mid c_2$. If $N = 26$, either 2 or 13 divide c_3.*
(c) *If $N = 27$, then $3 \mid c_2$ and $3 \mid c_3$.*
(d) *If $A(\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/9\mathbb{Z})^2$, then $9 \mid c_2$ and $9 \mid c_3$.*
(e) *If $A(\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$, then $7 \mid c_2$ and the reduction at 2 is purely multiplicative.*
(f) *If $N = 11$ or 13, and $A/\mathbb{Q}$ has bad reduction at (2), then $N \mid c_2$. Moreover, the reduction at (2) has positive toric rank, and is thus not potentially good. If $N = 11$, and $A/\mathbb{Q}$ has bad reduction at (3), then $N \mid c_3$ and the reduction at (3) has positive toric rank.*

Proof. — Recall that a $\mathbb{Q}$-rational point of prime order $N > 2$ reduces injectively in the special fiber $\mathcal{A}_{\mathbb{F}_2}/\mathbb{F}_2$ of the Néron model at (2). The smooth group scheme $\mathcal{A}_{\mathbb{F}_2}/\mathbb{F}_2$ is an extension of the connected component of 0, $\mathcal{A}^0_{\mathbb{F}_2}/\mathbb{F}_2$, be a finite étale group scheme. To show that $N \mid c_2$, it suffices to show that $N \nmid |\mathcal{A}^0_{\mathbb{F}_2}(\mathbb{F}_2)|$.

(a) Our hypothesis on N insures that A cannot have good reduction at 2. Moreover, no multiple mP of the point P of order N can reduce to a point in the connected component of 0 of the special fiber of the Néron model at 2, except for $m = N$. It follows that $N \mid c_2$.

(b) When $N = 22$ or 26, the reduction at 2 cannot be good. Since the reduction of a $\mathbb{Q}$-rational point of order 2 may be trivial in the special fiber of the Néron model at 2, we find that $N/2 \mid c_2$. When $N = 26$, the reduction at 3 is not good. If the connected component of zero in the special fiber is a torus of dimension 2 with $|T(\mathbb{F}_3)| = 13$, we find that $2 \mid c_3$. If the connected component of zero is any other group scheme, it cannot contain a point of order 13 and, hence, $13 \mid c_3$.

(c) Assume now that $N = 27$. Then the reduction at 2 is not good. The group $\mathcal{A}_k^0(k)$ may have order 9 when the reduction is purely toric, but in this case, the group is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$. The group $\mathcal{A}_k^0(k)$ may also have order 9, and thus a point of order 9, when the reduction is an extension of a torus by an elliptic curve. Hence, we can only conclude that $3 \mid c_2$. The reduction at 3 is also not good, and this time it could happen that $\mathcal{A}_k^0(k)$ has a point of order 9 when the reduction is purely additive (see [61], p. 73, for an example where $\mathcal{A}_k^0(k)$ is a non-split Witt group). So $3 \mid c_3$.

(d) Note first that the reduction at 2 cannot be good. The connected component of 0 can have order at most 9, and thus $9 \mid c_2$. The reduction at 3 cannot be good. If it is purely toric, then $9^2 \mid c_3$. In all other cases, $9 \mid c_3$.

(e) Assume that the reduction is not purely multiplicative at (2). Then our hypothesis implies that $(\mathbb{Z}/7\mathbb{Z})^2$ is a subgroup of the component group $\Phi(\overline{\mathbb{F}_2})$ at (2). The prime-to-2 part of such a component group contains a subgroup Σ which can be generated by t elements, where t is the toric rank of the Néron model at (2). The prime-to-2 part of the quotient $\Phi(\overline{\mathbb{F}_2})/\Sigma$ has order divisible only by primes $q \leqslant 2g+1$ ([43], 2.15). Hence, it follows that $t = 2$ under our hypothesis, a contradiction.

(f) Since an elliptic curve over $\mathbb{F}_2$ has at most five $\mathbb{F}_2$-rational points, and a torus of dimension 2 has at most nine points, we find that when $N \geqslant 11$, $N \nmid |\mathcal{A}_{\mathbb{F}_2}^0(\mathbb{F}_2)|$.

It is shown in [43] that if q is a prime dividing the order of the component group of the special fiber of a Néron model with toric rank 0, then either $q = p$ (p is the residue characteristic), or $q \leqslant 2g+1$. To see this, apply [43], 2.15, in the case where $t_K = 0$. Since in our case the component group is divisible by the prime $N \geqslant 11$, we find that the reduction at (2) has positive toric rank. □

Remark 3.9. — Curves of genus 2 whose Jacobians have $\mathbb{Q}$-rational points of order $N \in \{13, 15, 17\} \cup \{19, \ldots, 27\} \cup \{29\}$ can be found in [37], [38] and [39]. See [17] for examples with $N = 32, 34, 39$ and 40. No examples

are known with $N = 31$ or 37 (for these values of N, we would have $N \mid c_2$ and $N \mid c_3$), or with $N = 61$, when N would divide c_2, c_3, and c_5.

Remark 3.10. — E. Howe has kindly informed us that no abelian surfaces $A/\mathbb{F}_2$ have $A(\mathbb{F}_2)$ cyclic of order 25. We do not know whether there exists a semiabelian variety $V/\mathbb{F}_2$ of the form $0 \to T \to V \to E \to 0$, with $T/\mathbb{F}_2$ a 1-dimensional torus and $E/\mathbb{F}_2$ an elliptic curve, and with $V(\mathbb{F}_2)$ cyclic of order 9.

We now consider abelian surfaces defined over the rational function field $\mathbb{Q}(\lambda)$.

PROPOSITION 3.11. — *Let $A/\mathbb{Q}(\lambda)$ be an abelian surface such that $A(\mathbb{Q}(\lambda))$ contains a point of prime order $N \geqslant 11$. Suppose that $A/\mathbb{Q}(\lambda)$ has a place v of bad reduction which has degree 1. Then $N \mid c_v$. Moreover, the reduction at v has positive toric rank.*

Proof. — Since v is a place of $\mathbb{Q}(\lambda)$ of degree 1, the special fiber of the Néron model is a commutative group scheme $\mathcal{A}_v/\mathbb{Q}$, of dimension 2. To show that $N \mid c_v$, it suffices to show that $N \nmid |\mathcal{A}_v^0(\mathbb{Q})_{\mathrm{tors}}|$.

Recall that if $G/\mathbb{Q}$ is a smooth connected commutative group scheme of dimension 1, then either $|G(\mathbb{Q})_{\mathrm{tors}}| = 1$ (G unipotent), $|G(\mathbb{Q})_{\mathrm{tors}}| \mid 12$ (G toric), or $|G(\mathbb{Q})_{\mathrm{tors}}| \in \{1, \ldots, 10, 12\}$ (G elliptic curve).

If $\mathcal{A}_v^0/\mathbb{Q}$ is purely unipotent, it is isomorphic to $\mathbb{G}_a^2/\mathbb{Q}$, and $\mathcal{A}_v^0(\mathbb{Q})_{\mathrm{tors}} = (0)$. Tori of dimension 2 are described for instance in [36], 4.5. The group $\mathrm{GL}_2(\mathbb{Z})$ contains two maximal finite subgroups, of order 8 and 12. Thus, a torus $T/\mathbb{Q}$ of dimension 2 is split by an extension $L/\mathbb{Q}$ of degree dividing 8 or 12. Since $T(L)$ is isomorphic to $L^* \times L^*$, the torsion subgroup of $T(\mathbb{Q})$ does not contain elements of order $\geqslant 11$. It follows that $N \nmid |\mathcal{A}_v^0(\mathbb{Q})_{\mathrm{tors}}|$. That the reduction at v has positive toric rank follows as in 3.8 (f). □

Remark 3.12. — In view of the previous proposition, we recall here that an abelian variety $B/\mathbb{Q}(\lambda)$ of dimension $g > 0$ has at least one place of bad reduction [59], 2.3. Similarly, an abelian variety $A/\mathbb{Q}$ of dimension $g > 0$ has at least one place of bad reduction [25].

There are examples of curves $X/\mathbb{Q}(\lambda)$ of genus 2 whose Jacobians have a point of order N with $N = 11, 13, 15, 17, 19$, 20, 21, and 23 ([23], [37], [39], [58]). See [17] for $N = 32$. In each case, such a curve has bad reduction at at least one place of degree 1. In fact, the number of such places of bad reduction is (roughly) increasing with N: Two for $N = 11, 13, 20$, three for $N = 15, 17, 21, 23$, and four for $N = 19$.

An equation for a curve $X/\mathbb{Q}(\lambda)$ of genus 2 whose Jacobian has a point of order $N = 22$ is given in [60], page 355. Unfortunately, the Jacobian

of the curve defined by the given equation does not have a $\mathbb{Q}(\lambda)$-rational torsion point of order 22. But the curve over $\mathbb{Q}$ in this family obtained by setting $\lambda = 1$, $y^2 = x^6 + 2x^4 + 4x^3 - 7x^2 - 4x + 4$, has a Jacobian with a $\mathbb{Q}$-rational point of order $N = 22$.

Example 3.13. — We exhibit below an abelian surface $B/\mathbb{Q}(\lambda)$ with a $\mathbb{Q}(\lambda)$-rational point of order $N = 11$ and two places of bad reduction of degree 1, one of which is not semi-stable. Proposition 3.11 shows that the reduction type is then of mixed additive-toric type. Indeed, we find in [23], 3.1, that the hyperelliptic curve $X/\mathbb{Q}(\lambda)$ of genus 2 given by the equation

$$y^2 = x^6 + 2x^5 + (2\lambda + 3)x^4 + 2x^3 + (\lambda^2 + 1)x^2 + 2\lambda(1 - \lambda)x + \lambda^2$$

has a Jacobian $B/\mathbb{Q}(\lambda)$ with a point of order $N = 11$. The discriminant of this equation is

$$d := -4096\lambda^7(16\lambda^3 + 432\lambda^2 - 104\lambda + 9).$$

This curve over $\mathbb{Q}(\lambda)$ has two places of bad reduction of degree 1, at (λ) and at (λ^{-1}) (*i.e.*, at 0 and at ∞).

The curve $X/\mathbb{Q}(\lambda)$ has semi-stable reduction modulo (λ). Indeed, the given equation reduced modulo (λ) is $y^2 = x^2(x^2 + x + 1)^2$, which shows that the stable reduction of X is the union of two projective lines over $\mathbb{Q}$ meeting in three points (over $\overline{\mathbb{Q}}$). The thicknesses of the singular points are $(e_1, e_2, e_3) = (1, 1, 5)$ (with $(\ell, m, n) = (7, 2, 1)$), so that the component group has order 11 (Liu's algorithm [41], Prop. 2).

Let us consider now the reduction of X at the place (λ^{-1}). Set $s := 1/\lambda$. We find that X can be represented by the integral equation

$$y^2 = z^6 + 2sz^5 + (2s + 3s^2)z^4 + 2s^3z^3 + (s^2 + s^4)z^2 + (2s^4 - 2s^3)z + s^4. \tag{3.1}$$

We claim that the reduction of X is semi-stable after a quadratic extension. Indeed, substitute $u^2 = s$ in the above equation, and divide both sides by u^6, to get the new equation over $\mathbb{Q}(u)$:

$$Y^2 = Z^6 + 2uZ^5 + (2 + 3u^2)Z^4 + 2u^3Z^3 + (1 + u^4)Z^2 + (2u^3 - 2u^2)Z + u^2.$$

The reduction of this equation modulo (u) is $Y^2 = Z^2(Z^2 + 1)^2$, which shows that the stable reduction of X over $\mathbb{Q}(u)$ at (u) is the union of two projective lines over $\mathbb{Q}$ meeting in three points (over $\overline{\mathbb{Q}}$).

The reduction of X at (s) is not stable. Indeed, if it were, it would have to be of the same type as over $\mathbb{Q}(u)$, and the structure of the geometric component group $\Phi(\overline{\mathbb{Q}})$ at (s) of the Néron model of B could be computed using Liu's algorithm [41], Prop. 2. However, in this example, the computation leads to a thickness that is not an integer. On the other hand, after

the quadratic extension of the form $u^2 = s$, the component group $\Phi(\overline{\mathbb{Q}})$ is cyclic of order 33.

Example 3.14. — Consider the fibers $X_1/\mathbb{Q}$ and $X_{-1}/\mathbb{Q}$ at $\lambda = \pm 1$ in the family $X/\mathbb{Q}(\lambda)$ introduced in Example 3.13. The Jacobian $J_{\pm 1}/\mathbb{Q}$ of $X_{\pm 1}/\mathbb{Q}$ is an abelian surface with a $\mathbb{Q}$-rational point of order $N = 11$, and such that $c(J_{\pm 1}/\mathbb{Q}) = 1$.

The reduction data for the proper smooth genus 2 curve $X_1/\mathbb{Q}$, given by the hyperelliptic equation

$$y^2 = x^6 + 2x^5 + 5x^4 + 2x^3 + 2x^2 + 1,$$

can be computed using Liu's Algorithm [42], implemented in [64]. Thisq curve has bad reduction at a single prime, $p = 353$, with conductor $p = 353$. Indeed, it has semistable reduction at $p = 353$, with a special fiber consisting of an elliptic curve with a double point. The reduction type is I_{1-0-0} on page 170 of [56]. The component group of the Jacobian $J_1/\mathbb{Q}$ is trivial at $p = 353$. At $p = 2$, Liu's Algorithm only computes the type of potential stable reduction. One finds that the curve X_1 has potentially good reduction. It follows from 3.8 (f) that it has then good reduction at $p = 2$.

The curve $X_{-1}/\mathbb{Q}$, given by the hyperelliptic equation

$$y^2 = x^6+2x^5+x^4+2x^3+2x^2-4x+1 = (x^3-x^2+2x-1)(x^3+3x^2+2x-1),$$

has bad reduction at a single prime, $p = 23$. At $p = 23$, the reduction is semistable, and consists in a projective line with two double points: I_{1-1-0} on page 179 of [56], with exponent of the conductor $f = 2$. The component group of the Jacobian $J_{-1}/\mathbb{Q}$ is trivial at $p = 23$. At $p = 2$, Liu's Algorithm computes that the curve X_{-1} has potentially good reduction. It follows from 3.8 (f) that it has then good reduction at $p = 2$.

Recall that the modular curve $X_0(23)/\mathbb{Q}$ has genus 2, with equation $y^2 = (x^3 - 8x^2 + 3x - 7)(x^3 - x + 1)$. This curve has bad reduction only at $p = 23$ with $f = 2$, with special fiber the union of two projective lines intersecting in three points. Its Jacobian has a $\mathbb{Q}$-rational point of order 11, as does J_{-1}, but the component group of $J_0(23)$ at $p = 23$ has order 11. It is possible that J_{-1} and $J_0(23)$ are isogenous over $\mathbb{Q}$. Indeed, these two curves have the same number of points over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ for all primes $p \leqslant 1000$, $p \neq 2, 23$. We find in [11] that $J_1(23)/\mathbb{Q}$, of dimension 12, has an optimal quotient A of dimension 2 (denoted by **23A** in [11, Table 4]). The conjecture of Birch and Swinnerton-Dyer and the computations in [11, Table 4], imply conjecturally that 11^2 divides $|A(\mathbb{Q})||A^\vee(\mathbb{Q})|$, and that $c_{23}(A) = 1$. Here $A^\vee/\mathbb{Q}$ denotes the dual abelian variety of $A/\mathbb{Q}$. The abelian variety A is

the dual of the image of $J_0(23)$ in $J_1(23)$ under the map $J_0(23) \to J_1(23)$ obtained by functoriality from the natural morphism $X_1(23) \to X_0(23)$. Thus, A is $\mathbb{Q}$-isogenous to $J_0(23)$, and it could be that A is also isogenous to J_{-1}.

We found in the literature two more examples of abelian varieties over $\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order 11 and trivial Tamagawa number. Indeed, the Jacobian of the curve $y^2 = -3x^6 + 18x^4 + 6x^3 + 9x^2 - 54x + 57$ is such an abelian variety, as a computer check will show. This curve is denoted by $587a$ in [9, Table 2], and its Jacobian has prime conductor 587.

In [11, Table 4], one also finds an optimal quotient[(2)] $B/\mathbb{Q}$ of dimension 2 of $J_1(67)/\mathbb{Q}$ (denoted by **67B**), which conjecturally has 11^2 dividing $|B(\mathbb{Q})||B^\vee(\mathbb{Q})|$, and $11 \nmid c_{67}(B)$. We thank A. Brumer for communicating to us the following curve,

$$y^2 = -3x^6 - 20x^5 - 26x^4 + 42x^3 + 45x^2 - 62x + 17,$$

whose Jacobian $D/\mathbb{Q}$ has conductor 67^2, has a $\mathbb{Q}$-rational torsion point of order 11, and Tamagawa number $c(D/\mathbb{Q}) = 1$. It is likely that $D/\mathbb{Q}$ is isogenous to the abelian variety **67B**.

Example 3.15. — We note here an example of an abelian surface $A/\mathbb{Q}$ with a point of order $N = 13$, with good reduction at (2), and with $c(A/\mathbb{Q}) = 1$. The hyperelliptic curve

$$y^2 = -2\lambda x^5 + (10\lambda + \lambda^2 + 1)x^4 - (16\lambda + 8\lambda^2)x^3 + (8\lambda + 24\lambda^2)x^2 - 32\lambda^2 x + 16\lambda^2$$

has a Jacobian with a point of order 13 ([24], Result 2, with $g = 2$ and $r = 0$). The curves with $\lambda = 1$ and $\lambda = -1$ have the same Igusa invariants and are isomorphic, with conductor $p = 349$, and reduction at p of type I_{1-0-0} on page 170 of [56]. Their Jacobians have trivial Tamagawa product c.

Remark 3.16. — According to the Paramodular Conjecture of Brumer and Kramer, the primes 349 and 353, appearing in 3.15 and 3.14, are the second and third smallest possible prime conductors for an abelian surface over $\mathbb{Q}$ with $\mathrm{End}_{\mathbb{Q}}(A) = \mathbb{Z}$ ([62], 1.1 and 1.2, and [9], 1.4). The smallest one is conjectured to be $p = 277$. Brumer has given the equation $y^2 = x^6 - 2x^5 - x^4 + 4x^3 + 3x^2 + 2x + 1$ for a curve whose Jacobian has prime conductor $p = 277$, has a $\mathbb{Q}$-rational point of order 15, and has trivial Tamagawa number. One more example of prime conductor in the literature

(2) A second optimal quotient of $J_1(67)/\mathbb{Q}$ of dimension 2, denoted by **67C**, is probably isogenous to the Jacobian of the curve $X^*(67)/\mathbb{Q}$ given by the equation $y^2 = x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1$ [27, Table 2, C_{67}]. It is amusing to note that this latter equation is surprisingly close to the equation of the curve X_{-1} given above. A different equation was given earlier for $X^*(67)/\mathbb{Q}$ in [54], page 407.

([24], after Cor. 1): the Jacobian of the curve $y^2 + y = x^5 + x^4 + x^2$ has prime conductor $p = 3637$, has a $\mathbb{Q}$-rational point of order 5, and has trivial Tamagawa number.

We can use three of the above examples to exhibit abelian surfaces which do *not* have a principal polarization. Indeed, 2.1 in [71] implies that $\mathrm{End}(\mathrm{Jac}(C)) = \mathbb{Z}$ if the curve $C/\mathbb{Q}$ is given by an equation $y^2 = f(x)$ and the Galois group of the separable polynomial $f(x)$ of degree $n \geqslant 5$ is isomorphic to S_n or A_n. Using this criterion, we find that three of the above curves have no non-trivial endomorphisms, namely the curve of conductor 349 whose Jacobian has a $\mathbb{Q}$-rational torsion point of order 13, Brumer's curve, and the curve $y^2 + y = x^5 + x^4 + x^2$.

Let now A/K be any principally polarized abelian variety of dimension $g > 1$ such that $\mathrm{End}_K(A) = \mathbb{Z}$. Let $r\colon A \to B$ be a non-trivial isogeny of prime degree d. We claim that B does not have a principal polarization. Indeed, using r, a principal polarization $s\colon B \to B^\vee$ induces a polarization $A \to A^\vee$ of degree d^2. Since A has a principal polarization, we obtain by composition an endomorphism of A of degree d^2. Since $\mathrm{End}_K(A) = \mathbb{Z}$, any endomorphism of A has degree n^{2g} for some n. Since $g > 1$, our claim follows.

We can apply the above claim to each of the three curves $C/\mathbb{Q}$ with $\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(C)) = \mathbb{Z}$. Since in each case $\mathrm{Jac}(C)$ has a non-trivial $\mathbb{Q}$-rational torsion point P of prime order, the abelian variety $\mathrm{Jac}(C)/\langle P\rangle$ does not have a principal polarization. We do not know how to compute the rational torsion subgroup and the Tamagawa product of such an abelian variety.

Example 3.17. — The modular curve $X_1(13)/\mathbb{Q}$ has genus 2, and bad reduction only at $p = 13$. Its Jacobian has a $\mathbb{Q}$-rational point of order $N = 19$, with trivial component group at $p = 13$.

For completeness, let us note that $J_1(16)/\mathbb{Q}$ and $J_1(18)/\mathbb{Q}$ are also abelian surfaces, with a $\mathbb{Q}$-rational point of order 10 and 21, respectively. Equations for the modular curves can be found for instance in [39], and Liu's Algorithm for $J_1(18)/\mathbb{Q}$ shows that $c_3(X_1(18)) = 1$.

Example 3.18. — Let $K := \mathbb{Q}(\sqrt{-3})$. Consider the elliptic curve E/K introduced in 2.11 with a K-rational point of order 7, and $c(E/K) = 1$. Let $A/\mathbb{Q}$ denote the Weil restriction of E from K to $\mathbb{Q}$. This abelian surface has a $\mathbb{Q}$-rational point of order $N = 7$, and Proposition 3.19 below shows that $c(A/\mathbb{Q}) = 1$.

Let $K := \mathbb{Q}(\sqrt{5})$. Consider the elliptic curve E/K introduced in 2.16 with a K-rational point of order 8, and $c(E/K) = 1$. Let $A/\mathbb{Q}$ denote the

Weil restriction of E from K to $\mathbb{Q}$. This abelian surface has a $\mathbb{Q}$-rational point of order $N = 8$, and Proposition 3.19 shows that $c(A/\mathbb{Q}) = 1$.

Let again $K := \mathbb{Q}(\sqrt{5})$. Consider the elliptic curve E/K introduced in 2.18 with a K-rational point of order 9, and $c(E/K) = 3$. Let $A/\mathbb{Q}$ denote the Weil restriction of E from K to $\mathbb{Q}$. This abelian surface has a $\mathbb{Q}$-rational point of order $N = 9$, and Proposition 3.19 shows that $c(A/\mathbb{Q}) = 3$.

The following proposition may be well-known to experts, but we have been unable to find a reference for it in the literature. We introduce the following notation. Let $\mathcal{O}_K$ be a Dedekind domain with field of fractions K. Let L/K be a Galois extension and denote by $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L. *Assume that all residue fields of $\mathcal{O}_K$ are perfect.* Let B/L be an abelian variety. Let A/K denote the Weil restriction of B/L to K. Let $\mathcal{B}/\mathcal{O}_L$ denote the Néron model of B/L. Let $\mathcal{A}/\mathcal{O}_K$ denote the Néron model of A/K, and recall that $\mathcal{A}/\mathcal{O}_K$ is isomorphic to the Weil restriction of $\mathcal{B}/\mathcal{O}_L$ from $\mathcal{O}_L$ to $\mathcal{O}_K$ (see, *e.g.*, [7], 7.6/6).

For each prime $\mathfrak{P}$ of $\mathcal{O}_L$ with residue field $k_\mathfrak{P}$, denote by $\Phi_{B,\mathfrak{P}}/k_\mathfrak{P}$ the group scheme of connected components of the Néron model $\mathcal{B}/\mathcal{O}_L$ at $\mathfrak{P}$. Similarly, for P a prime of $\mathcal{O}_K$, we denote by $\Phi_{A,P}/k_P$ the group scheme of connected components of the Néron model $\mathcal{A}/\mathcal{O}_K$ at P.

Let P be a prime of $\mathcal{O}_K$ and write $P\mathcal{O}_L = (\prod_{i=1}^{s} \mathfrak{P}_i)^e$. Fix an algebraic closure $\overline{k_P}$ of k_P. For each i, fix an embedding of $k_{\mathfrak{P}_i}$ into $\overline{k_P}$. Use this embedding to identify $\mathrm{Gal}(\overline{k_{\mathfrak{P}_i}}/k_{\mathfrak{P}_i})$ with a subgroup H_i of $\mathrm{Gal}(\overline{k_P}/k_P)$, and to view $\Phi_{B,\mathfrak{P}_i}(\overline{k_{\mathfrak{P}_i}})$ as an H_i-module.

Proposition 3.19. — *Let L/K be a Galois extension. Let B/L be an abelian variety and let A/K denote the Weil restriction of B/L to K. Keep the notation and hypotheses introduced above. Then $\Phi_{A,P}(\overline{k_P})$ is isomorphic, as $\mathrm{Gal}(\overline{k_P}/k_P)$-module, to*

$$\prod_{i=1}^{s} \mathrm{Ind}_{H_i}^{\mathrm{Gal}(\overline{k_P}/k_P)} \Phi_{B,\mathfrak{P}_i}(\overline{k_{\mathfrak{P}_i}}).$$

Moreover, when K is a global field, then $c(A/K) = c(B/L)$.

Proof. — We may assume that $\mathcal{O}_K$ is local. There exist two intermediate extensions $K \subseteq K' \subseteq K'' \subseteq L$ such that L/K'' is totally ramified at every maximal ideal of $\mathcal{O}_{K''}$, every maximal ideal of $\mathcal{O}_{K'}$ is inert in $\mathcal{O}_{K''}$, and P splits completely in $\mathcal{O}_{K'}$. Since the formation of the Weil restriction is transitive, it suffices to prove the proposition in each of the three above cases.

a) Let us assume first that $\mathcal{O}_K$ is local and P is totally ramified in $\mathcal{O}_L$, so that $P\mathcal{O}_L = \mathfrak{P}^{[L\colon K]}$. In particular, $k_P = k_{\mathfrak{P}}$. We claim that $\Phi_{A,P}(\overline{k_P})$ is isomorphic, as $\mathrm{Gal}(\overline{k_P}/k_P)$-module, to $\Phi_{B,\mathfrak{P}}(\overline{k_{\mathfrak{P}}})$.

Let $R := (\mathcal{O}_L/P\mathcal{O}_L)$. The ring R is an Artin k_P-algebra with residue field $k_{\mathfrak{P}} = k_P$. Consider the smooth commutative group scheme $\mathcal{G} := \mathcal{B} \times_{\mathcal{O}_L} R$ over R. By construction, the Weil restriction $\mathrm{Res}_{R/k_P}(\mathcal{G})$ is isomorphic over k_P to the special fiber of $\mathcal{A}/\mathcal{O}_K$. The base change $\mathcal{G} \times_R k_P$ is isomorphic to the special fiber of $\mathcal{B}/\mathcal{O}_L$.

Given any group scheme D/R, the universal property of the Weil restriction produces a natural morphism of k_P-group schemes $\mathrm{Res}_{R/k_P}(D) \to D \times_R k_P$. The natural morphism $\mathrm{Res}_{R/k_P}(\mathcal{G}) \to \mathcal{B}_{k_{\mathfrak{P}}}$ has connected fibers. To show this, one shows that the group scheme $\mathrm{Res}_{R/k_P}(\mathcal{G})$ has a filtration by subgroup schemes $F_{i+1} \subset F_i$, with $F_1 = \mathrm{Ker}(\mathrm{Res}_{R/k_P}(\mathcal{G}) \to \mathcal{B}_{k_{\mathfrak{P}}})$, and the quotients F_i/F_{i+1} for $i \geqslant 1$ isomorphic to affine spaces; see *e.g.*, [16], proof of Theorem 1, or [15], 5.1 (the proof given there is done with an abelian variety B/L of the form C_L/L for some C/K, but the same proof applies more generally to any B/L). See also [57], A.3.5, when B/L is affine. It follows from this fact that $\Phi_{\mathrm{Res}_{R/k_P}(\mathcal{G})}$ is isomorphic to $\Phi_{\mathcal{B}_{k_{\mathfrak{P}}}}$.

b) Let us assume now that $\mathcal{O}_K$ is local and P is inert in $\mathcal{O}_L$, so that $P\mathcal{O}_L = \mathfrak{P}$, with $[k_{\mathfrak{P}}\colon k_P] = [L\colon K]$. We claim that $\Phi_{A,P}(\overline{k_P})$ is isomorphic, as $\mathrm{Gal}(\overline{k_P}/k_P)$-module, to $\mathrm{Ind}_H^{\mathrm{Gal}(\overline{k_P}/k_P)}\, \Phi_{B,\mathfrak{P}}(\overline{k_{\mathfrak{P}}})$, with H identified with $\mathrm{Gal}(\overline{k_P}/k_{\mathfrak{P}})$. Consider the exact sequence of H-modules

$$(0) \longrightarrow \mathcal{B}^0_{k_{\mathfrak{P}}}(\overline{k}_P) \longrightarrow \mathcal{B}_{k_{\mathfrak{P}}}(\overline{k}_P) \longrightarrow \Phi_{\mathcal{B}}(\overline{k}_P) \longrightarrow (0).$$

We then have an exact sequence of $\mathrm{Gal}(\overline{k_P}/k_P)$-modules,

$$\begin{aligned}(0) \longrightarrow \mathrm{Ind}_H^{\mathrm{Gal}(\overline{k_P}/k_P)}\, \mathcal{B}^0_{k_{\mathfrak{P}}}(\overline{k}_P) \longrightarrow \mathrm{Ind}_H^{\mathrm{Gal}(\overline{k_P}/k_P)}\, \mathcal{B}_{k_{\mathfrak{P}}}(\overline{k}_P)\\ \longrightarrow \mathrm{Ind}_H^{\mathrm{Gal}(\overline{k_P}/k_P)}\, \Phi_{\mathcal{B}}(\overline{k}_P) \longrightarrow (0).\end{aligned}$$

Consider now the exact sequence of $\mathrm{Gal}(\overline{k_P}/k_P)$-modules associated with the Weil restriction:

$$(0) \longrightarrow (\mathcal{A}_{k_P})^0(\overline{k}_P) \longrightarrow \mathcal{A}_{k_P}(\overline{k}_P) \longrightarrow \Phi_{\mathcal{A}}(\overline{k}_P) \longrightarrow (0).$$

Recall that $\mathcal{A}_{k_P}/k_P$ is isomorphic to the Weil restriction $\mathrm{Res}_{k_{\mathfrak{P}}/k_P}(\mathcal{B}_{k_{\mathfrak{P}}}/k_{\mathfrak{P}})$. We claim that $(\mathcal{A}_{k_P})^0/k_P$ is isomorphic to $\mathrm{Res}_{k_{\mathfrak{P}}/k_P}(\mathcal{B}^0_{k_{\mathfrak{P}}}/k_{\mathfrak{P}})$. Indeed, this follows because $\mathrm{Res}_{k_{\mathfrak{P}}/k_P}(\mathcal{B}^0_{k_{\mathfrak{P}}}/k_{\mathfrak{P}})$ is connected. That this is the case can be seen as follows: since $k_{\mathfrak{P}}/k_P$ is separable, the base change of $\mathrm{Res}_{k_{\mathfrak{P}}/k_P}(\mathcal{B}^0_{k_{\mathfrak{P}}}/k_{\mathfrak{P}})$ to $k_{\mathfrak{P}}$ is isomorphic over $k_{\mathfrak{P}}$ to the product of the conjugates of $\mathcal{B}^0_{k_{\mathfrak{P}}}$. Since $\mathcal{B}^0_{k_{\mathfrak{P}}}$ is smooth over $k_{\mathfrak{P}}$, this product is connected ([28], IV.4.5.8).

Since $k_{\mathfrak{P}}/k_P$ is separable, the $\mathrm{Gal}(\overline{k_P}/k_P)$-module structure on $\mathcal{A}^0_{k_P}(\overline{k}_P)$ can be identified with the module $\mathrm{Ind}_H^{\mathrm{Gal}(\overline{k_P}/k_P)} \mathcal{B}^0_{k_{\mathfrak{P}}}(\overline{k}_P)$, and similarly for the $\mathrm{Gal}(\overline{k_P}/k_P)$-module structure on $\mathcal{A}_{k_P}(\overline{k}_P)$. This is briefly mentioned in [51], or [13], 1.3.2, for abelian varieties. The same argument works for any smooth group scheme $\mathcal{G}/k_{\mathfrak{P}}$. The key fact is that $k_{\mathfrak{P}}/k_P$ is separable, so that $\mathrm{Res}_{k_{\mathfrak{P}}/k_P}(\mathcal{G}) \times_{k_P} k_{\mathfrak{P}}$ is isomorphic to the product of the conjugates of $\mathcal{G}/k_{\mathfrak{P}}$. It follows then from the above exact sequences that there is a natural isomorphism of $\mathrm{Gal}(\overline{k_P}/k_P)$-modules between $\mathrm{Ind}_H^{\mathrm{Gal}(\overline{k_P}/k_P)} \Phi_{\mathcal{B}}(\overline{k}_P)$ and $\Phi_{\mathcal{A}}(\overline{k}_P)$.

c) Finally, let us assume that $\mathcal{O}_K$ is local and P splits completely in $\mathcal{O}_L$, so that $P\mathcal{O}_L = \prod_{i=1}^{[L:K]} \mathfrak{P}_i$. We claim that $\Phi_{A,P}(\overline{k_P})$ is isomorphic, as $\mathrm{Gal}(\overline{k_P}/k_P)$-module, to $\prod_{i=1}^{s} \Phi_{B,\mathfrak{P}_i}(\overline{k_{\mathfrak{P}_i}})$. This follows from the fact that $\mathrm{Spec}(\mathcal{O}_L/P\mathcal{O}_L)$ is isomorphic to $\coprod \mathrm{Spec}(k_{\mathfrak{P}_i})$, so that the Weil restriction of the scheme $\mathcal{B} \times_{\mathcal{O}_L} (\mathcal{O}_L/P\mathcal{O}_L)$ is simply the direct product $\prod_i \mathcal{B}_{k_{\mathfrak{P}_i}}$. Since the product of smooth connected schemes is again connected ([28], IV.4.5.8), we find that $(\prod_i \mathcal{B}_{k_{\mathfrak{P}_i}})^0 = \prod_i \mathcal{B}^0_{k_{\mathfrak{P}_i}}$.

The last statement of the proposition, regarding the case when K is a global field, follows immediately from the first part of the proposition, and the following standard fact about invariants of induced representations:

$$(\mathrm{Ind}_H^{\mathrm{Gal}(\overline{k_P}/k_P)} \Phi_{B,\mathfrak{P}}(\overline{k_{\mathfrak{P}}}))^{\mathrm{Gal}(\overline{k_P}/k_P)} \simeq \Phi_{B,\mathfrak{P}}(\overline{k_{\mathfrak{P}}})^H \simeq \Phi_{B,\mathfrak{P}}(k_{\mathfrak{P}}).$$

□

Remark 3.20. — Putting together the examples presented in this section, we see that:

(1) For $N = 7, 8, 9, 11, 13$ and 19, there exists at least one abelian surface $A/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order N such that N does not divide $c(A)$ (see 3.14–3.18).

Let $N = 11, 13$, or 19. Consider the set of isomorphism classes of abelian surfaces $A/\mathbb{Q}$ having a $\mathbb{Q}$-rational point of order N and such that $N \nmid c(A)$. It is natural to wonder whether this set is finite.

(2) For $N = 16, 22, 25, 26$, and 27, we do not know whether $N \mid c(A)$ for all abelian surfaces $A/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order N. (This is mainly due to the fact that there is as of yet no known algorithm to compute the reduction type of a genus 2 curve $X/\mathbb{Q}$ modulo 2.)

(3) For $N = 3, 5, 6, 12, 15, 21, 24$, and 30, there exists infinitely many abelian surfaces $A/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order N such that $N \nmid c(A)$.

To prove this statement, we use products of elliptic curves. Recall that the curve $E/\mathbb{Q}$ with label $11a3$ has a $\mathbb{Q}$-rational point of order $N = 5$ and $c(E) = 1$. Consider now any elliptic curve $E'/\mathbb{Q}$ with integral j-invariant. Then E' has potentially good reduction everywhere, and $c(E')$ can only divisible by the primes $p = 2$ and 3. It follows that there are infinitely many abelian surfaces $E \times E'$ with a $\mathbb{Q}$-rational point of order $N = 5$ and $N \nmid c(E \times E')$.

For each $k = 1, 2, 4, 5, 7, 8, 10$, choose and elliptic curve $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order k and $c(E)$ coprime to 3. Recall that there exists infinitely many elliptic curves $E'/\mathbb{Q}$ having a point of order 3 and $c = 1$ (see 2.26). It follows that there are infinitely many abelian surfaces $E \times E'$ with a $\mathbb{Q}$-rational point of order $N = 3k$ and $N \nmid c(E \times E')$.

(4) For $N = 2, 4, 10, 14, 18, 20, 28, 36$, there exists at least one abelian surface $A/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order N such that N does not divide $c(A)$.

Choose an elliptic curve $E/\mathbb{Q}$ having a $\mathbb{Q}$-rational 2-torsion point and $c = 1$. For $k = 1, 5, 7, 9$, choose an elliptic curve $E'/\mathbb{Q}$ with a $\mathbb{Q}$-rational k-torsion point and c odd. Then for $n = 2k$, $N \nmid c(E \times E')$. Similarly, pick an elliptic curve $E''/\mathbb{Q}$ having a $\mathbb{Q}$-rational 4-torsion point and $c = 2$. Then for $N = 4k$, $N \nmid c(E'' \times E')$.

4. Optimal modular quotients

4.1. Consider an abelian variety $A/\mathbb{Q}$ which has *analytic rank* 0 and is an optimal quotient of $J_0(N)/\mathbb{Q}$ attached to a newform. Let $A^\vee/\mathbb{Q}$ denote the abelian variety dual to A. Then the Birch and Swinnerton-Dyer conjecture, together with the conjecture that the Manin constant is 1, imply that

$$\text{the odd part of } |A^\vee(\mathbb{Q})| \text{ divides } c(A) \cdot |Ш(A)|,$$

as proved in [1], end of Section 4.3. Here $Ш(A)$ denotes as usual the Tate-Shafarevich group of A, and $c(A)$ is the Tamagawa number. When A is principally polarized, such as when $\dim(A) = 1$, we find that under the above hypotheses, the odd part of $|A(\mathbb{Q})|$ conjecturally divides $c(A) \cdot |Ш(A)|$. Our work on elliptic curves in the second section of this article, as summarized in 1.1, immediately implies the following, independently of any conjecture:

PROPOSITION 4.2. — *Let $E/\mathbb{Q}$ be an optimal elliptic curve with a $\mathbb{Q}$-rational point of order N, and Tamagawa number $c(E)$. If $N = 5, \ldots, 10$, or 12, then $N \mid c(E)$.*

Proof. — Proposition 1.1 states that $N \mid c(E)$ when $N = 7, 8, 9, 10$, or 12, even when the elliptic curve is not optimal. When $N = 5$ or 6, one verifies that none of the four exceptions to the statement $N \mid c(E)$ in 2.7 and 2.9 are optimal elliptic curves. □

That $N \mid c(E)|Ш(E)|$ when $N = 7$ is proved in [14]. The statement of the proposition does not hold when $N = 3$ (*e.g.*, it does not hold for $189b1$ with rank 1, and $10621c1$ with rank 0), or $N = 4$ (*e.g.*, it does not hold for $205a1$ with rank 1, and for $2405d1$ with rank 0; both curves have $c = 2$). Note also that Mazur shows how to construct curves $E/\mathbb{Q}$ of rank 0 with a 3-torsion point and with trivial 3-part of Ш in [46], just before 10.2; examples can also be obtained with, in addition, $c = 1$.

The conjectural statement in 4.1 can be replaced by an equivalent statement depending only on $A^\vee$, namely: the odd part of $|A^\vee(\mathbb{Q})|$ divides $c(A^\vee)|Ш(A^\vee)|$. Indeed, $|Ш(A^\vee)| = |Ш(A)|$ since the Cassels-Tate pairing is non-degenerate [52], I.6.26, and $c(A^\vee) = c(A)$, as we now explain.

Let K be a discrete valuation field, with residue field k assumed to be perfect. Let A/K be an abelian variety that is not necessarily principally polarized. Let $A^\vee/K$ denote the abelian variety dual to A/K. Let Φ_A/k and $\Phi_{A^\vee}/k$ denote the groups of components of the Néron models of A and $A^\vee$ over $\mathcal{O}_K$. Grothendieck defined in [29], IX, 1.2, a $\mathrm{Gal}(\overline{k}/k)$-invariant pairing

$$\langle\ ,\ \rangle \colon \Phi_A(\overline{k}) \times \Phi_{A^\vee}(\overline{k}) \longrightarrow \mathbb{Q}/\mathbb{Z},$$

and he conjectured that this pairing was non-degenerate. This conjecture is proved for instance in [3] when K is of characteristic 0, in [6], 4.7, for Jacobians of curves X/K having a K-rational point, and in [48], 4.8, when the residue field is finite. Clearly, when the pairing is non-degenerate, $|\Phi_A(\overline{k})| = |\Phi_{A^\vee}(\overline{k})|$, and the $\mathrm{Gal}(\overline{k}/k)$-module $\Phi_A(\overline{k})$ is isomorphic, as $\mathrm{Gal}(\overline{k}/k)$-module, to the $\mathrm{Gal}(\overline{k}/k)$-module $\mathrm{Hom}_{\mathbb{Z}}(\Phi_{A^\vee}(\overline{k}), \mathbb{Q}/\mathbb{Z})$ (endowed with the natural structure $(\sigma \cdot f)(x) := f(\sigma^{-1}x)$). Since in general it is not known that $\Phi_{A^\vee}(\overline{k})$ is isomorphic, as $\mathrm{Gal}(\overline{k}/k)$-module, to $\mathrm{Hom}_{\mathbb{Z}}(\Phi_{A^\vee}(\overline{k}), \mathbb{Q}/\mathbb{Z})$, we cannot conclude without further arguments that $|\Phi_A(k)| = |\Phi_{A^\vee}(k)|$. However, in the case most important to number theorists, we have the following application of [48], 4.8:

Proposition 4.3. — *Assume that the residue field k is finite. Then $|\Phi_A(k)| = |\Phi_{A^\vee}(k)|$. In particular, if A/F is an abelian variety over a global field F, then $c(A/F) = c(A^\vee/F)$.*

Proof. — When the residue field is finite, Grothendieck's pairing is perfect ([48], 4.8). The action of $\mathrm{Gal}(\overline{k}/k)$ on the finite abelian group $\Phi =$

$\Phi_A(\overline{k})$ factors through a finite Galois extension F/k. When the residue field is finite, the extension F/k is cyclic, with Galois group G generated by an element σ. The sequence

$$0 \longrightarrow \Phi^G \longrightarrow \Phi \stackrel{\sigma-1}{\longrightarrow} \Phi \longrightarrow \Phi/(\sigma-1)(\Phi) \longrightarrow 0$$

is exact, and shows that $|\Phi^G| = |\Phi/(\sigma-1)(\Phi)|$. Dualizing this sequence using $M^* := \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ gives that $(\Phi^*)^G$ is isomorphic to $(\Phi/(\sigma-1)(\Phi))^*$. □

Example 4.4. — We thank D. Benson for the following example of a G-module M where M^G and $(M^*)^G$ have different orders. Consider the action of the symmetric group S_3 on $M' := (\mathbb{F}_3)^3$ by permutations of the standard basis $\{e_1, e_2, e_3\}$. Clearly, the action is trivial on the span M'' of $e_1 + e_2 + e_3$, and we let $M := M'/M''$. Then $M^G = (0)$, while an easy computation of $\langle (\sigma - 1)(x), x \in M, \sigma \in S_3 \rangle$ shows that this submodule has $\mathbb{F}_3$-rank 1, generated by the class of $e_2 - e_1$. It follows that $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})^G$ has $\mathbb{F}_3$-rank 1 too.

We further note the following facts.

LEMMA 4.5. — *Assume that Grothendieck's pairing is non-degenerate. Let q be prime. Then*

(i) *The exponents of the abelian groups $\Phi_A(\overline{k})/\Phi_A(k)$ and $\Phi_{A^\vee}(\overline{k})/\Phi_{A^\vee}(k)$ are equal. In particular,*
   (a) *If the groups $\Phi_A(k)$ and $\Phi_A(\overline{k})$ have the same q-parts, then the groups $\Phi_{A^\vee}(k)$ and $\Phi_{A^\vee}(\overline{k})$ have the same q-parts.*
   (b) *If the q-part of $\Phi_A(\overline{k})$ is cyclic, then the q-parts of $|\Phi_A(k)|$ and $|\Phi_{A^\vee}(k)|$ are equal.*

(ii) *Suppose that k'/k is a Galois extension such that $Gal(\overline{k}/k')$ acts trivially on $\Phi_A(\overline{k})$. If q does not divide $[k' : k]$, then the q-parts of $|\Phi_A(k)|$ and $|\Phi_{A^\vee}(k)|$ are equal.*

Proof.

(i) Let $y \in \Phi_{A^\vee}(\overline{k})$. Assume that the exponent of $\Phi_A(\overline{k})/\Phi_A(k)$ equals m. For any $x \in \Phi_A(\overline{k})$ and for any $\sigma \in \mathrm{Gal}(\overline{k}/k)$, we find that $\langle mx, \sigma(y) - y \rangle = 0$. Since $\langle mx, \sigma(y) - y \rangle = \langle x, \sigma(my) - my \rangle$, and since the pairing is non-degenerate, we find that $\sigma(my) - my = 0$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$. It follows that $my \in \Phi_{A^\vee}(k)$, and the exponent of $\Phi_{A^\vee}(\overline{k})/\Phi_{A^\vee}(k)$ divides m. Repeating the argument with $x \in \Phi_A(\overline{k})$ shows that m divides the exponent of $\Phi_{A^\vee}(\overline{k})/\Phi_{A^\vee}(k)$.

(ii) This is well-known.

□

It is shown in [5], 4.3 (i), that when the reduction of A/K is split semistable (*i.e.*, the special fiber of the Néron model is an extension of an abelian variety by a split torus), then $\Phi_A(k) = \Phi_A(\overline{k})$.

When A/K is an abelian surface and $q > 5$ is prime, $q \neq p$, then the q-part of $\Phi_A(\overline{k})$ is cyclic when the toric rank t of A/K is equal to 1. Indeed, the prime-to-p part of such a component group contains a subgroup Σ which can be generated by t elements, and such that the prime-to-p part of the quotient $\Phi(\overline{k})/\Sigma$ has order divisible only by primes $\ell \leqslant 2g+1$ ([43], 2.15).

BIBLIOGRAPHY

[1] A. Agashe & W. Stein, "Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero", *Math. Comp.* **74** (2005), no. 249, p. 455-484, With an appendix by J. Cremona and B. Mazur.

[2] A. Beauville, "Les familles stables de courbes elliptiques sur $\mathbf{P}^1$ admettant quatre fibres singulières", *C. R. Acad. Sci. Paris Sér. I Math.* **294** (1982), no. 19, p. 657-660.

[3] L. Bégueri, "Dualité sur un corps local à corps résiduel algébriquement clos", *Mém. Soc. Math. France (N.S.)* (1980/81), no. 4, p. 121.

[4] F. Beukers & H. P. Schlickewei, "The equation $x + y = 1$ in finitely generated groups", *Acta Arith.* **78** (1996), no. 2, p. 189-199.

[5] S. Bosch & Q. Liu, "Rational points of the group of components of a Néron model", *Manuscripta Math.* **98** (1999), no. 3, p. 275-293.

[6] S. Bosch & D. Lorenzini, "Grothendieck's pairing on component groups of Jacobians", *Invent. Math.* **148** (2002), no. 2, p. 353-396.

[7] S. Bosch, W. Lütkebohmert & M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990, x+325 pages.

[8] W. Bosma, J. Cannon & C. Playoust, "The Magma algebra system. I. The user language", *J. Symbolic Comput.* **24** (1997), no. 3-4, p. 235-265, Computational algebra and number theory (London, 1993), `http://magma.maths.usyd.edu.au/magma/`.

[9] A. Brumer & K. Kramer, "Paramodular abelian varieties of odd conductor", arXiv:1004.4699, 2010.

[10] P. L. Clark & X. Xarles, "Local bounds for torsion points on abelian varieties", *Canad. J. Math.* **60** (2008), no. 3, p. 532-555.

[11] B. Conrad, B. Edixhoven & W. Stein, "$J_1(p)$ has connected fibers", *Doc. Math.* **8** (2003), p. 331-408 (electronic).

[12] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, vi+376 pages.

[13] C. Diem, "A Study on Theoretical and Practical Aspects of Weil-Restrictions of Varieties", Dissertation (Essen), `http://www.math.uni-leipzig.de/~diem/preprints/english.html`.

[14] N. Dummigan, "Rational points of order 7", *Bull. Lond. Math. Soc.* **40** (2008), no. 6, p. 1091-1093.

[15] B. Edixhoven, "Néron models and tame ramification", *Compositio Math.* **81** (1992), no. 3, p. 291-306.

[16] B. Edixhoven, Q. Liu & D. Lorenzini, "The p-part of the group of components of a Néron model", *J. Algebraic Geom.* **5** (1996), no. 4, p. 801-813.

[17] N. Elkies, "Curves of genus 2 over $\mathbb{Q}$ whose Jacobians are absolutely simple abelian surfaces with torsion points of high order", `http://www.math.harvard.edu/~elkies/g2_tors.html`.

[18] ———, "Elliptic curves in nature", `http://math.harvard.edu/~elkies/nature.html`.

[19] ———, "Examples of high-order torsion points on simple genus-2 Jacobians", Manuscript, April 2001.

[20] M. Emerton, "Optimal quotients of modular Jacobians", *Math. Ann.* **327** (2003), no. 3, p. 429-458.

[21] P. Erdös, "Arithmetical properties of polynomials", *J. London Math. Soc.* **28** (1953), p. 416-425.

[22] J.-H. Evertse, H. P. Schlickewei & W. M. Schmidt, "Linear equations in variables which lie in a multiplicative group", *Ann. of Math. (2)* **155** (2002), no. 3, p. 807-836.

[23] E. V. Flynn, "Large rational torsion on abelian varieties", *J. Number Theory* **36** (1990), no. 3, p. 257-265.

[24] ———, "Large rational torsion on abelian varieties", *J. Number Theory* **36** (1990), no. 3, p. 257-265.

[25] J.-M. Fontaine, "Il n'y a pas de variété abélienne sur $\mathbf{Z}$", *Invent. Math.* **81** (1985), no. 3, p. 515-538.

[26] C. Gonzalez-Aviles, "On Néron class group of abelian varieties", Preprint 2009, arXiv:0909.4803v2 [math.NT] 5 Oct 2009.

[27] E. González-Jiménez & J. González, "Modular curves of genus 2", *Math. Comp.* **72** (2003), no. 241, p. 397-418 (electronic).

[28] A. Grothendieck, "Éléments de géométrie algébrique. Étude locale des schémas et des morphismes de schémas", *Inst. Hautes Études Sci. Publ. Math.* (1966-1967), no. 24, 28, 32, p. 231, 255, 361.

[29] ———, *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim, viii+523 pages.

[30] M. Hindry & J. H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction, xiv+558 pages.

[31] E. W. Howe, F. Leprévost & B. Poonen, "Large torsion subgroups of split Jacobians of curves of genus two or three", *Forum Math.* **12** (2000), no. 3, p. 315-364.

[32] S. Kamienny, "Torsion points on elliptic curves and q-coefficients of modular forms", *Invent. Math.* **109** (1992), no. 2, p. 221-229.

[33] M. A. Kenku & F. Momose, "Torsion points on elliptic curves defined over quadratic fields", *Nagoya Math. J.* **109** (1988), p. 125-149.

[34] D. Krumm, "Tamagawa numbers of elliptic curves over cubic fields", in preparation.

[35] D. S. Kubert, "Universal bounds on the torsion of elliptic curves", *Proc. London Math. Soc. (3)* **33** (1976), no. 2, p. 193-237.

[36] B. Kunyavskiĭ & J.-J. Sansuc, "Réduction des groupes algébriques commutatifs", *J. Math. Soc. Japan* **53** (2001), no. 2, p. 457-483.

[37] F. Leprévost, "Torsion sur des familles de courbes de genre g", *Manuscripta Math.* **75** (1992), no. 3, p. 303-326.

[38] ———, "Jacobiennes de certaines courbes de genre 2: torsion et simplicité", *J. Théor. Nombres Bordeaux* **7** (1995), no. 1, p. 283-306, Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[39] ———, "Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genre $g \geqslant 1$", *Manuscripta Math.* **92** (1997), no. 1, p. 47-63.

[40] S. Ling, "On the **Q**-rational cuspidal subgroup and the component group of $J_0(p^r)$", *Israel J. Math.* **99** (1997), p. 29-54.

[41] Q. Liu, "Courbes stables de genre 2 et leur schéma de modules", *Math. Ann.* **295** (1993), no. 2, p. 201-222.

[42] ———, "Modèles minimaux des courbes de genre deux", *J. Reine Angew. Math.* **453** (1994), p. 137-164.

[43] D. J. Lorenzini, "On the group of components of a Néron model", *J. Reine Angew. Math.* **445** (1993), p. 109-160.

[44] ———, "Torsion points on the modular Jacobian $J_0(N)$", *Compositio Math.* **96** (1995), no. 2, p. 149-172.

[45] ———, "Models of curves and wild ramification", *Pure Appl. Math. Q.* **6** (2010), no. 1, Special Issue: In honor of John Tate. Part 2, p. 41-82.

[46] B. Mazur, "Rational points of abelian varieties with values in towers of number fields", *Invent. Math.* **18** (1972), p. 183-266.

[47] ———, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* (1977), no. 47, p. 33-186 (1978).

[48] W. G. McCallum, "Duality theorems for Néron models", *Duke Math. J.* **53** (1986), no. 4, p. 1093-1124.

[49] ———, "On the method of Coleman and Chabauty", *Math. Ann.* **299** (1994), no. 3, p. 565-596.

[50] P. Mihăilescu, "Primary cyclotomic units and a proof of Catalan's conjecture", *J. Reine Angew. Math.* **572** (2004), p. 167-195.

[51] J. S. Milne, "On the arithmetic of abelian varieties", *Invent. Math.* **17** (1972), p. 177-190.

[52] ———, *Arithmetic duality theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006, viii+339 pages.

[53] H. H. Müller, H. Ströher & H. G. Zimmer, "Torsion groups of elliptic curves with integral j-invariant over quadratic fields", *J. Reine Angew. Math.* **397** (1989), p. 100-161.

[54] N. Murabayashi, "On normal forms of modular curves of genus 2", *Osaka J. Math.* **29** (1992), no. 2, p. 405-418.

[55] T. Nagell, "Les points exceptionnels rationnels sur certaines cubiques du premier genre", *Acta Arith.* **5** (1959), p. 333-357.

[56] Y. Namikawa & K. Ueno, "On fibres in families of curves of genus two. I. Singular fibres of elliptic type", in *Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki*, Kinokuniya, Tokyo, 1973, p. 297-371.

[57] J. Oesterlé, "Nombres de Tamagawa et groupes unipotents en caractéristique p", *Invent. Math.* **78** (1984), no. 1, p. 13-88.

[58] H. Ogawa, "Curves of genus 2 with a rational torsion divisor of order 23", *Proc. Japan Acad. Ser. A Math. Sci.* **70** (1994), no. 9, p. 295-298.

[59] F. Oort, "Subvarieties of moduli spaces", *Invent. Math.* **24** (1974), p. 95-119.

[60] R. D. Patterson, A. J. van der Poorten & H. C. Williams, "Sequences of Jacobian varieties with torsion divisors of quadratic order", *Funct. Approx. Comment. Math.* **39** (2008), no. part 2, p. 345-360.

[61] D. Penniston, "Unipotent groups and curves of genus two", *Math. Ann.* **317** (2000), no. 1, p. 57-78.

[62] C. Poor & D. Yuen, "Paramodular cusp forms", Preprint (2009), available at `http://arxiv.org/PS_cache/arxiv/pdf/0912/0912.0049v1.pdf`.

[63] M. A. Reichert, "Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields", *Math. Comp.* **46** (1986), no. 174, p. 637-658.

[64] "Sage Mathematics Software", `http://www.sagemath.org/`.

[65] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994, xiv+525 pages.

[66] G. Stevens, "Stickelberger elements and modular parametrizations of elliptic curves", *Invent. Math.* **98** (1989), no. 1, p. 75-106.

[67] J. Tate, "Algorithm for determining the type of a singular fiber in an elliptic pencil", in *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Springer, Berlin, 1975, p. 33-52. Lecture Notes in Math., Vol. 476.

[68] P. Tzermias, "Torsion parts of Mordell-Weil groups of Fermat Jacobians", *Internat. Math. Res. Notices* (1998), no. 7, p. 359-369.

[69] V. Vatsal, "Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves", *J. Inst. Math. Jussieu* **4** (2005), no. 2, p. 281-316.

[70] Y. Yang, "Modular units and cuspidal divisor class groups of $X_1(N)$", *J. Algebra* **322** (2009), no. 2, p. 514-553.

[71] Y. G. Zarhin, "Hyperelliptic Jacobians without complex multiplication", *Math. Res. Lett.* **7** (2000), no. 1, p. 123-132.

Manuscrit reçu le 12 mars 2010,
accepté le 26 novembre 2010.

Dino LORENZINI
University of Georgia
Department of mathematics
Athens, GA 30602 (USA)