ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 43, Number 1, 2013

# GENUS TWO CURVES WITH EVERYWHERE TWISTED GOOD REDUCTION

HOURIA BAAZIZ AND JOHN BOXALL

ABSTRACT. We construct examples of genus two curves $C$ over quadratic fields $K$ with everywhere twisted good reduction, i.e., for any finite prime $\mathfrak{p}$ of $K$, $C$ has a twist that has good reduction at $\mathfrak{p}$. An analogous construction for elliptic curves enables us to recover Setzer's family of curves with everywhere good reduction over an imaginary quadratic field.

**1. Introduction.** Let $K$ be a number field, and let $X/K$ be a smooth projective variety. We say that $X$ has good reduction at a finite prime $\mathfrak{p}$ of $K$ if $X$ has a smooth model $\mathcal{X}_{\mathfrak{p}}$ over the local ring at $\mathfrak{p}$. It is well known that $X$ has good reduction outside a finite set $\Sigma(X)$ of primes $\mathfrak{p}$; we say that $X$ has everywhere good reduction if $\Sigma(X)$ is empty. A well-known theorem of Fontaine [**4**] and Abrashkin [**1**] asserts that there are no abelian varieties with everywhere good reduction over $\mathbf{Q}$. On the other hand many authors have given examples of elliptic curves having everywhere good reduction over quadratic fields. By taking products, one obtains abelian varieties of arbitrary dimension with everywhere good reduction over quadratic fields.

When $X$ is a curve of genus at least one, one knows that if $X$ has good reduction at $\mathfrak{p}$ then the jacobian $J_X$ of $X$ also has good reduction at $\mathfrak{p}$. The converse is not true: if, for instance $X$ is of genus two and $J_X$ has good reduction at $\mathfrak{p}$, then the special fiber of $\mathcal{X}_{\mathfrak{p}}$ is either smooth or the union of two curves of genus one intersecting at a point.

This paper grew out of an attempt to find genus two curves over quadratic fields with everywhere good reduction. (Of course, the Fontaine-Abrashkin theorem implies that there are no such curves over $\mathbf{Q}$.) If $C$ is a (smooth projective) genus two curves over a number field $K$, then $C$ has an affine model of the form $y^2 = P(x)$ where $P$ is a square-free polynomial of degree 5 or 6 with coefficients in $K$ and all

2010 AMS *Mathematics subject classification.* Primary 11G05, 11G30.
*Keywords and phrases.* Genus two curves, elliptic curves, everywhere good reduction.
Received by the editors on March 22, 2009, and in revised form on July 6, 2010.
DOI:10.1216/RMJ-2013-43-1-55 

roots simple. If $\mathfrak{p}$ is a prime of $K$ with odd residue characteristic, then one knows that $C$ has good reduction at $\mathfrak{p}$ if and only if we can choose $P$ to have coefficients in the local ring $\mathcal{O}_{\mathfrak{p}}$ at $\mathfrak{p}$ and to remain square-free after reduction (mod $\mathfrak{p}$). (See [**6**].) This is equivalent to the discriminant of $P$ being a unit in $\mathcal{O}_{\mathfrak{p}}$. When the residue characteristic of $\mathfrak{p}$ is 2, we need to use a model

$$y^2 + Q(x)y = P(x), \tag{0.1}$$

where now $P$ and $Q$ have coefficients in $\mathcal{O}_{\mathfrak{p}}$ and $P + Q^2/4$ is square-free of degree 5 or 6 and without repeated roots. One knows that $C$ has good reduction at $\mathfrak{p}$ if and only if we can choose $P$ and $Q$ in such a way that $2^8$ times the discriminant of $P + Q^2/4$ is an invertible element of $\mathcal{O}_{\mathfrak{p}}$. To have a unified notation, we write $\Delta_C$ for $2^8$ times the discriminant of $P + Q^2/4$; of course, $\Delta_C$ depends upon the choice of $P$ and $Q$ and not just upon $C$.

We call a model of the form (0.1) a Weierstrass model of the genus two curve $C$. Let $\mathcal{O}_K$ denote the ring of integers of $K$. It follows from the previous paragraph that, if $C$ has a Weierstrass model (0.1) with $P$ and $Q$ having coefficients in $\mathcal{O}_K$ such that $\Delta_C$ is an invertible element of $\mathcal{O}_K$, then $C$ has everywhere good reduction.

While we know of no Weierstrass model having these properties with $K$ a quadratic field, we did discover the following result.

**Proposition 0.1.** *Let $p$, $b \in K$, and let $C$ have the Weierstrass model*

$$y^2 + (px^2 + px)y = x^5 + \left(\frac{b+5}{2}\right)x^4 + bx^3 + \left(\frac{b-5}{2}\right)x^2 - x. \tag{0.2}$$

*Then $\Delta_C = ((p^2 + 2b)^2 + 108)^2$.*

This can of course be checked directly, and leads to the following construction of an infinite family of pairs $(K, C)$ consisting of a quartic number field $K$ and a genus two curve $C$ having everywhere good reduction over $K$.

**Proposition 0.2.** *Let $b$ be an odd rational integer, let $p$ be an algebraic number such that either $(p^2 + 2b)^2 = -107$ or $(p^2 + 2b)^2 =$*

*$-109$, and let $K$ be the number field generated over $\mathbf{Q}$ by $p$. Then the curve* (0.2) *has everywhere good reduction over $K$.*

Since $b$ is a rational integer, it is clear that $p$ belongs to $\mathcal{O}_K$ and, since $b$ is odd, (0.2) has coefficients in $\mathcal{O}_K$. The condition that $(p^2+2b)^2 = -107$ or $-109$ implies that $\Delta_C = 1$.

It is clear that $K$ is a quartic extension of $\mathbf{Q}$, and it is easy to see that the Galois group of its Galois closure is the dihedral group of order 8. Also, $K$ always contains $\mathbf{Q}(\sqrt{-107})$ when $(p^2+2b)^2 = -107$ and $\mathbf{Q}(\sqrt{-109})$ when $(p^2+2b)^2 = -109$. Since we have been unable to find examples of genus two curves with everywhere good reduction over number fields of degree 2 or 3 in the literature, the fields $K$ in Proposition 0.2 seem at present to be the fields of smallest known degree that harbor examples of such curves.

The rest of this paper is devoted to the study of various properties of these curves as well as their use in the construction of genus two curves with various arithmetic properties.

Writing $w = p^2+2b$ and $Y = y + (px^2+px)/2$, we see that the curve $C$ with equation (0.2) is isomorphic to

$$Y^2 = x(x+1)\left(x^3 + \frac{1}{4}(w+6)x^2 + \frac{1}{4}(w-6)x - 1\right). \tag{0.3}$$

Furthermore, $\Delta_C = (w^2+108)^2$.

If $X$ is a smooth projective variety over the number field $K$, a *twist* of $X$ is a second smooth projective variety over $K$ that becomes isomorphic to $X$ over an algebraic closure of $K$. It is easy to see that a twist of $X$ is in fact isomorphic to $X$ over some finite extension of $K$.

As an example that will be used later, consider a genus 2 curve $C$ with equation $y^2 = x^5 + ax^4 + bx^3 + cx^2 + dx + e$, where $a$, $b$, $c$, $d$, $e \in K$. If $\lambda \in K^\times$, the curve $C^{(\lambda)}$ with equation $y^2 = x^5 + \lambda a x^4 + \lambda^2 b x^3 + \lambda^3 c x^2 + \lambda^4 d x + \lambda^5 e$ becomes isomorphic to $C$ over $K(\sqrt{\lambda})$, as may be seen by replacing $x$ by $x/\lambda$ and $y$ by $y/\sqrt{\lambda^5}$. Note that $\Delta_{C^{(\lambda)}} = \lambda^{10}\Delta_C$. We call $C^{(\lambda)}$ the *twist of $C$ by $\sqrt{\lambda}$* (or by $K(\sqrt{\lambda})$ if no confusion is possible). We use a similar language for elliptic curves: if $C$ is an elliptic curve with Weierstrass model $y^2 = x^3 + ax + b$, $a$, $b \in K$ and if $\lambda \in K^\times$, the twist of $C$ by $\sqrt{\lambda}$ or by $K(\sqrt{\lambda})$ is the

curve with equation $y^2 = x^3 + \lambda^2 ax + \lambda^3 b$; it becomes isomorphic to $C$ over $K(\sqrt{\lambda})$.

Let $\mathfrak{p}$ be a prime of $K$. We say that $X$ has *twisted good reduction at* $\mathfrak{p}$ if there exists a twist of $X$ that has good reduction at $\mathfrak{p}$. We say that $X$ has *everywhere twisted good reduction* over $K$ if $X$ has twisted good reduction at every prime of $K$. By specializing to the cases $w^2 = -107$, and $w^2 = -109$, we shall give two constructions, each leading to the following result.

**Theorem 0.3.** *There are infinitely many pairs $(K, C)$ consisting of a quadratic number field $K$ and a genus two curve $C$ that have everywhere twisted good reduction over $K$.*

It should be noted that the Jacobian varieties of the curves (0.2) or (0.3) are not absolutely simple, and it follows by specialization that this is also the case for the curves used to prove Theorem 0.3. Thus, the question of the existence of genus two curves that have absolutely simple Jacobians and everywhere twisted good reduction over quadratic fields remains open. However, we shall prove that a further extension of degree divisible by three is necessary for the Jacobians of our curves to become isogenous to a product of elliptic curves.

Here is an outline of the paper. In Section 1, we bring together a few simple properties of everywhere twisted good reduction. In particular, we show that there do not exist elliptic curves over $\mathbf{Q}$ with everywhere twisted good reduction and that, if $K$ is a number field and $\Sigma$ a finite set of primes of $K$, then there are only finitely $j \in K$ that are the $j$-invariants of elliptic curves having twisted good reduction at all primes not in $\Sigma$. The proof is an adaption of Shafarevich's well-known proof [**9**] of the corresponding assertions for usual good reduction (see, for instance, Silverman [**11**, page 263]). In Section 2 we briefly study the curve $C_w$, viewing $w$ as an indeterminate; we show, in particular, that the Jacobian $J_w$ of $C_w$ becomes isogenous to a product of two elliptic curves over a suitable six degree Galois extension of $\mathbf{Q}(w)$ with cyclic Galois group. In Section 3, we study genus two curves obtained from the curve (0.3) specialized to $w^2 = -107$ and give a first construction proving Theorem 0.3. Section 4 is devoted to a similar study of $C_w$ specialized to $w^2 = -109$. In the final Section 5, we explain briefly how

the family (0.2) was discovered and show how, by applying a similar strategy to elliptic curves, we obtain Setzer's [**8**] examples of elliptic curves having everywhere good reduction over imaginary quadratic fields.

**1. Everywhere twisted good reduction.** Let $K$ be a number field, and let $\mathfrak{p}$ be a prime of $K$. As in the introduction, we say that the smooth projective variety $X$ over $K$ has *twisted good reduction* at $\mathfrak{p}$ if some twist of $X$ has good reduction at $\mathfrak{p}$. It is clear from the Jacobian criterion applied to any smooth model of $X$ that $X$ has good reduction outside a finite set of primes. If $X$ does not have good reduction at $\mathfrak{p}$ but some twist $X'$ of $X$ does, then $X'$ becomes isomorphic to $X$ over some finite extension $K'$ of $K$, so that $X$ acquires good reduction over $K'$ or, as one says, that $X$ has *potential good reduction* at $\mathfrak{p}$.

Let $\Sigma$ be a set of primes of $K$. By reiterating this procedure, we deduce that, if $X$ has twisted good reduction at all primes of $K$ that do not belong to $\Sigma$, then it has *potentially good reduction* outside of $\Sigma$, i.e., it acquires good reduction at every prime of $K$ over some finite extension of $K$.

From now on, $X$ will always be either a curve or an abelian variety. If $X$ is a curve of genus $g \geq 1$, it is well known that, if $X$ has good reduction at $\mathfrak{p}$, then the Jacobian variety $J_X$ also has good reduction at $\mathfrak{p}$. The converse is false in general; if $X$ is a genus two curve, then $J_X$ may have good reduction while the stable reduction of $X$ is the union of two genus one curves meeting at a point. Thus, we cannot, a priori, use abelian surfaces with everywhere good reduction to construct genus two curves with everywhere good reduction.

Let $E$ be an elliptic curve over $K$, and fix a Weierstrass model

$$y^2 = x^3 + ax + b, \quad a,\ b \in K. \tag{1.1}$$

Then one knows that, if $ab \neq 0$, every twist of $E$ has a Weierstrass model of the form $E^{(\lambda)} : y^2 = x^3 + \lambda^2 ax + \lambda^3 b$, where $\lambda \in K^\times$, and two such twists $E^{(\lambda)}$ and $E^{(\lambda')}$ are $K$-isomorphic if and only $\lambda'/\lambda$ is a square of $K$.

When $a = 0$, every twist of $E$ has a model $y^2 = x^3 + \lambda b$ with $\lambda \in K^\times$ and becomes isomorphic to $E$ over $K(\sqrt[6]{\lambda})$, while when $b = 0$, every twist of $E$ has a model $y^2 = x^3 + \lambda ax$ with $\lambda \in K^\times$ and becomes

isomorphic to $E$ over $K(\sqrt[4]{\lambda})$. These cases correspond respectively to elliptic curves with $j$-invariant 0 and 1728.

Let $\mathfrak{p}$ be a prime of $K$, and let $\mathcal{O}_\mathfrak{p}$ be the local ring of $K$ at $\mathfrak{p}$. If $E$ is an elliptic curve over $K$, then we can find a generalized Weierstrass model

$$\begin{gathered} y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6, \\ a_i \in \mathcal{O}_\mathfrak{p} \quad \text{for all } i \in \{1, 2, 3, 4, 6\} \end{gathered} \tag{1.2}$$

of $E$ over $\mathcal{O}_\mathfrak{p}$. Let $\Delta_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$ denote the discriminant of this model, and let $v_E(\mathfrak{p})$ denote the $\mathfrak{p}$-adic valuation of $\Delta_\mathfrak{p}$: if $\Delta'_\mathfrak{p}$ is the discriminant of a second Weierstrass model over $\mathcal{O}_\mathfrak{p}$ and $v'_E(\mathfrak{p})$ its $\mathfrak{p}$-adic valuation, then $v'_E(\mathfrak{p}) \equiv v_E(\mathfrak{p}) \pmod{12}$. Finally, one knows that $E$ has good reduction at $\mathfrak{p}$ if and only if we can find a model (1.2) with $v_E(\mathfrak{p}) = 0$.

Suppose that $E$ has a Weierstrass model (1.1), and that the $j$-invariant of $E$ is different from 0 and 1728. If $E$ has twisted good reduction at $\mathfrak{p}$, then it acquires good reduction over some quadratic extension $K'$ of $K$. If $\mathfrak{P}$ is a prime of $K'$ dividing $\mathfrak{p}$, then, by what has just been said, $v_E(\mathfrak{P}) \equiv 0 \pmod{12}$. It follows that $v_E(\mathfrak{p}) \equiv 0 \pmod 6$ (and in fact $v_E(\mathfrak{p}) \equiv 0 \pmod{12}$ if $\mathfrak{p}$ is unramified in $K'$). By varying $\mathfrak{p}$, we obtain the following lemma.

**Lemma 1.1.** *Let $\Sigma$ be a finite set of primes of $K$, and let $E$ be an elliptic curve with equation* (1.1)*, with discriminant $D = 16(4a^3+27b^2)$. If $ab \neq 0$ and if $E$ has twisted good reduction everywhere outside $\Sigma$, then $D$ is the sixth power of a fractional $\mathcal{O}_{K,\Sigma}$-ideal of $K$.*

Here $\mathcal{O}_{K,\Sigma}$ denotes the ring of all elements of $K$ that are integral at every prime of $K$ that doesn't belong to $\Sigma$. We use the lemma to prove the following results, using a mild variant of Shafarevich's arguments showing that there are no elliptic curves with everywhere good reduction over $\mathbf{Q}$ and only finitely many isomorphism classes of elliptic curves over a number field $K$ having good reduction outside a finite set of primes of $K$.

**Theorem 1.2.** *There are no elliptic curves over $\mathbf{Q}$ with everywhere twisted good reduction.*

*Proof.* We again consider elliptic curves with Weierstrass model (1.1), supposing during the proof that $a$, $b \in \mathbf{Q}$. We take $\Sigma$ to be empty.

If $a = 0$, then every twist of $E$ is of the form $y^2 = x^3 + b$, and the discriminant is $16 \cdot 27b^2$. But such a curve cannot have good reduction at 3, since the 3-adic valuation of $16 \cdot 27b^2$ is odd for any $b \in \mathbf{Q}^\times$, so it cannot be divisible by 12.

If $b = 0$, then every twist of $E$ is of the form $y^2 = x^3 + ax$ with $a \in \mathbf{Q}^\times$. Write $a = 2^m A$, with $A$ a unit at 2. We can suppose that $0 \leq m \leq 3$. The discriminant is now $2^{6+3m}A^3$; since $v_E(2) \equiv 0 \pmod{12}$, we have $m = 2$. An analysis using Tate's algorithm [**12**] shows that $E$ cannot have good reduction at 2.

Suppose then that $ab \neq 0$. Then Lemma 1.1 shows that $D = \varepsilon d^6$ for some $d \in \mathbf{Q}^\times$ and $\varepsilon \in \{\pm 1\}$, so that

$$16(4a^3 + 27b^2) = \varepsilon d^6.$$

Hence, writing $\xi = -(3 \cdot 2^2 \cdot a)/d^2$, $\eta = (3^3 \cdot 2^2 \cdot b)/d^3$, we find that $\eta^2 = \xi^3 + 27\varepsilon$. Thus, $(\xi, \eta)$ is a rational point on one of the elliptic curves $y^2 = x^3 + 27\varepsilon$. But it is well known that both of these curves have rank 0 and that their rational torsion is of order 2. Hence, $(\xi, \eta) = (-3\varepsilon, 0)$ and therefore $b = 0$, a case which has already been excluded. □

Two elliptic curves are twists of each other if and only if they have the same $j$-invariant, so it is natural to consider twisted good reduction as a property of $j$-invariants.

**Theorem 1.3.** *Let $K$ be a number field and $\Sigma$ a finite set of primes of $K$. Then there are only finitely many $j \in K$ that are $j$-invariants of elliptic curves with twisted good reduction at all primes of $K$ not in $\Sigma$.*

*Proof.* We first enlarge $\Sigma$ by adding all the primes of $K$ that divide 2, and then in such a way that the ring of $\Sigma$-integers $\mathcal{O}_{K,\Sigma}$ is a principal ideal ring. We can suppose that $j \neq 0$, 1728, as this excludes only finitely many $j$-invariants. If $j \neq 0$, 1728, the curve $E_j : y^2 = x^3 + [(j - 1728)^2/4]x^2 - 36(j - 1728)^3 x - (j - 1728)^5$ has $j$-invariant $j$ and discriminant $j^2(j - 1728)^9$. Suppose that, for every $\mathfrak{p} \notin \Sigma$, $E_j$ has a twist having good reduction at $\mathfrak{p}$. Then, assuming

that $\mathcal{O}_{K,\Sigma}$ is principal and that $\Sigma$ contains the primes above 2, the discriminant of $E$ is of the form $\varepsilon\delta^6$ with $\varepsilon \in \mathcal{O}_{K,\Sigma}^\times$, $\delta \in \mathcal{O}_{K,\Sigma}$. Also, $j \in \mathcal{O}_{K,\Sigma}$ since $E_j$ has potential good reduction outside $\Sigma$. Since $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^6$ is a finite group, we can assume that $\varepsilon$ belongs to a finite set of representatives of $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^6$ in $\mathcal{O}_{K,\Sigma}^\times$. To conclude, therefore, it suffices to show that, given $\varepsilon \in \mathcal{O}_{K,\Sigma}^\times$, there are only finitely many $(j,\delta) \in \mathcal{O}_{K,\Sigma}^2$ satisfying $j^2(j-1728)^9 = \varepsilon\delta^6$. Now the curve with affine model $y^2(y-1728)^9 = \varepsilon x^6$ is of genus one, birational over $K$ to the elliptic curve $y^2 = x^3 - 27\varepsilon$. By a theorem of Siegel [**7, 10**], it therefore has only finitely many points $(x,y) \in \mathcal{O}_{K,\Sigma}^2$. In particular, there are only finitely many possible values of $j$. □

*Remark* 1.4. (1) When $j \neq 0$, 1728, the existence of curve $E_j$ with discriminant $j^2(j-1728)^9$ shows that, if $\mathfrak{p}$ is a prime of $K$ not dividing $2j(j-1728)$, then there is an elliptic curve over $K$ with $j$-invariant $j$ having good reduction at $\mathfrak{p}$. The elliptic curve $y^2 + y = x^3$ has $j$-invariant 0 and good reduction outside 3, and the elliptic curve $y^2 = x^3 - 1$ has $j$-invariant 1728 and good reduction outside 2. Thus, whatever the value of $j \in K$, we can find an explicit finite set of primes $\Sigma$ such that if $\mathfrak{p} \notin \Sigma$ is a prime of $K$, there exists an elliptic curve over $K$ with invariant $j$ and good reduction at $\mathfrak{p}$.

(2) Let $\mathcal{Z}$ be a $\overline{K}$-isomorphism class of smooth projective varieties over $K$, and let $\Sigma_{\mathcal{Z}}^{\mathrm{bad}}$ be the set of primes of $K$ at which all members of $\mathcal{Z}$ have bad reduction. Then Theorem 1.2 asserts that, if $K = \mathbf{Q}$ and $\mathcal{Z}$ consists of elliptic curves, we have $\Sigma_{\mathcal{Z}}^{\mathrm{bad}} \neq \varnothing$. On the other hand, Theorem 1.3 asserts that, given any finite set of primes $\Sigma$ of $K$, there are only finitely many $\overline{K}$-isomorphism classes $\mathcal{Z}$ of elliptic curves over $K$ with $\Sigma_{\mathcal{Z}}^{\mathrm{bad}} \subseteq \Sigma$. It would be interesting to know whether these results can be generalized to higher genus curves or higher dimensional abelian varieties. In Sections 3 and 4 we shall construct infinitely many examples of quadratic fields $K$ and $\overline{K}$-isomorphism classes $\mathcal{Z}$ of genus two curves over $K$ with $\Sigma_{\mathcal{Z}}^{\mathrm{bad}} = \varnothing$.

**2. The curve $C_w$ over $k(w)$.** Let $k$ be a field of characteristic different from 2 and 3, let $w$ be an indeterminate and let $K$ be the rational function field $k(w)$. In this section, we bring together a few properties of the genus two curve (0.3) of the introduction, viewed as

a curve over $K$. Fix an algebraic closure $\Omega$ of $K$.

It is convenient to replace $x$ by $x-1$ so that the equation of $C_w$ becomes

$$\begin{aligned} y^2 &= x(x-1)W(x), \\ W(x) &= x^3 + \frac{1}{4}(w-6)x^2 - \frac{1}{4}(w+6)x + 1. \end{aligned} \tag{2.1}$$

The discriminant of $W$ is $(w^2+108)^2$. If $\alpha$ is one of the roots of $W$ in $\Omega$, one sees easily that the other two roots are $1/(1-\alpha)$ and $1-1/\alpha$. Using the fact that the coefficient of $x^2$ in $W$ is minus the sum of the roots of $W$, we find that

$$\begin{aligned} w &= -2\frac{(\alpha-2)(\alpha+1)(2\alpha-1)}{\alpha(\alpha-1)}, \\ w^2+108 &= 16\frac{(\alpha^2-\alpha+1)^3}{\alpha^2(\alpha-1)^2}. \end{aligned} \tag{2.2}$$

**Lemma 2.1.** *The polynomial $W$ is irreducible over $K$ with cyclic Galois group.*

*Proof.* Suppose $W$ reducible. Since $W$ is of degree 3, one of its roots, $\alpha$ say, lies in $K$. It then follows that the other roots $1/(1-\alpha)$ and $1-1/\alpha$ also lie in $K$. On the other hand, $W$ is a monic polynomial whose coefficients lie in the integrally closed subring $k[w]$ of $K$. It follows that $\alpha$ and $1-1/\alpha$ are both polynomials in $w$, and this can only happen if $\alpha \in k$. Hence, $W(\alpha) = ((\alpha^2/4)-(\alpha/4))w+(\alpha^3-(3/2)\alpha^2-(3/2)\alpha+1)$ is the zero polynomial. Comparing coefficients of $w$ shows that either $\alpha = 0$ or $\alpha = 1$, neither of which make the constant coefficient vanish.

This proves that $W$ is irreducible. Since its discriminant is a non zero square, it follows that it is separable with cyclic Galois group. □

One sees easily that $C_w$ has an automorphism of order 3, defined by $(x,y) \mapsto ((1/1-x),(y/(1-x)^3))$. When $k = \mathbf{C}$, it was proved by Bolza [**2**] that this implies that $C_w$ also has an automorphism $\iota$ of order two, different from the hyperelliptic involution. Such an automorphism must transform the set of Weierstrass points $\{\infty,(0,0),(1,0)\}$ to the

set of Weierstrass points $\{(\alpha,0),(1/(1-\alpha),0),(1-1/\alpha,0)\}$, and one finds that it is given, in our situation and up to composition with the hyperelliptic involution, by

$$x \longmapsto \frac{\alpha x+1-\alpha}{x-\alpha}, \qquad y \longmapsto \frac{\alpha(\alpha-1)uy}{4(x-\alpha)^3}, \tag{2.3}$$

where $u$ is a square root of $w^2+108$ in $\Omega$. Since $k$ is of characteristic different to 2 and 3, $w^2+108$ is not a square of $K$, so that $K(u)$ is a quadratic extension of $K$ and $K(\alpha,u)$ is a degree 6 extension of $K$ which is Galois with cyclic Galois group.

**Proposition 2.2.** *We keep the notation that has just been introduced.*

(1) *Let $J_w$ be the Jacobian variety of $C_w$. Then $J_w$ becomes isogenous, over the cyclic degree 6 extension $K(\alpha,u)$ of $K$, to a product of two elliptic curves.*

(2) *When $k=\mathbf{Q}$, $J_w$ is not isogenous to a product of elliptic curves over any extension of $K$ of degree strictly less than 6.*

*Proof.* (1) We have already seen that $K(\alpha,u)$ is a cyclic degree 6 extension of $K$. If $\iota$ is the automorphism of order two of $C_w$ defined by (2.3), then $\iota$ is rational over $K(\alpha,u)$. Since $\iota$ is not the hyperelliptic involution, the quotient curve $E_w$ of $C_w$ by the group generated by $\iota$ is of genus one and, since $C_w(K)$, and hence $C_w(K(\alpha,u))$, is non empty, $E_w(K(\alpha,u))$ is non empty. Thus, $E_w$ can be given the structure of an elliptic curve over $K(\alpha,u)$. By the Albanese property of Jacobians, the quotient map $C_w \to E_w$ can be extended to a homomorphism $\phi : J_w \to E_w$. But then $J_w$ is isogenous over $K(\alpha,u)$ to $E_w \times F_w$, where $F_w$ is the connected component of the identity of $\ker\phi$, which is well known to be an elliptic curve.

(2) It suffices to show that $J_w$ has a specialization $J_{w_0}$ which is not isogenous to a product of elliptic curves over an extension of $\mathbf{Q}(w_0)$ of degree strictly smaller than 6. To do this, we take $w_0=\sqrt{-109}$. The prime 11 splits in $\mathbf{Q}(\sqrt{-109})$, and the curve $C_{\sqrt{-109}}$ has good reduction at the primes of $K$ above 11. The same is therefore true for $J_{\sqrt{-109}}$. Let $L$ be a finite extension of $\mathbf{Q}(\sqrt{-109})$, let $\mathfrak{P}$ be a prime of $L$ dividing 11 and let $k_{\mathfrak{P}}$ be the residue field of $L$ at $\mathfrak{P}$. If $\phi : J_{w_0} \to E \times F$ is an isogeny defined over $L$, with $E$ and $F$ elliptic

curves over $L$, then $E$ and $F$ would have good reduction at $\mathfrak{P}$ and $\phi$ would induce an isogeny between the fibers $J_{\mathfrak{P}}$ of $J_{\sqrt{-109}}$ and $E_{\mathfrak{P}} \times F_{\mathfrak{P}}$ of $E \times F$ over $k_{\mathfrak{P}}$. Now, $k_{\mathfrak{P}}$ is a finite field, and it is well known that the Frobenius endomorphisms of isogenous abelian varieties over a finite field have the same characteristic polynomial. Hence, the existence of an isogeny $J_{\mathfrak{P}} \to E_{\mathfrak{P}} \times F_{\mathfrak{P}}$ would imply that the characteristic polynomial $\chi_{L,\mathfrak{P}}(t) \in \mathbf{Q}[t]$ of the Frobenius endomorphism of $J_{\mathfrak{P}}$ is the product of that of $E_{\mathfrak{P}}$ and that of $F_{\mathfrak{P}}$. This would in turn imply that $\chi_{L,\mathfrak{P}}(t)$ factorizes in $\mathbf{Q}[t]$ as the product of two quadratic polynomials. A method for calculating $\chi_{L,\mathfrak{P}}(t)$ is explained in [**5**]. Applying it when $L = \mathbf{Q}(\sqrt{-109})$, we find that $\chi_{\mathbf{Q}(\sqrt{-109}),\mathfrak{P}}(t) = t^4+9t^3+38t^2+99t+121$, which is irreducible in $\mathbf{Q}[t]$. Let $L$ be a finite extension of $\mathbf{Q}(\sqrt{-109})$, and let $d$ be the residue class degree of $L$ over $\mathbf{Q}(\sqrt{-109})$ at $\mathfrak{P}$. Then one knows that if $\chi_{\mathbf{Q}(\sqrt{-109}),\mathfrak{P}}(t)$ factorizes as

$$\chi_{\mathbf{Q}(\sqrt{-109}),\mathfrak{P}}(t) = (t-\alpha)(t-\beta)(t-\gamma)(t-\delta),$$

where $\alpha$, $\beta$, $\gamma$, $\delta \in \mathbf{C}$, then

$$\chi_{L,\mathfrak{P}}(t) = (t-\alpha^d)(t-\beta^d)(t-\gamma^d)(t-\delta^d).$$

The coefficients of $\chi_{L,\mathfrak{P}}(t)$ can then be calculated as symmetric functions of $\alpha$, $\beta$, $\gamma$ and $\delta$ and the calculation shows that $\chi_{L,\mathfrak{P}}(t)$ is irreducible when $d \leq 5$. □

We end this section by remarking that $C_w$ has a twist defined over $k(w^2)$. To see this, note that substituting $x+(1/2)$ for $x$ in $x(x-1)W(x)$ shows that $C_w$ also has the equation

$$y^2 = x^5 + \frac{1}{4}wx^4 - \frac{5}{2}x^3 - \frac{1}{8}wx^2 + \frac{9}{16}x + \frac{1}{64}w.$$

Substituting $x/w$ for $x$, multiplying by $w^5$ and writing $v$ for $w^2$ gives the following result:

**Proposition 2.3.** *Let $v = w^2$. The smooth projective curve $\mathcal{C}_v$ defined over $k(v)$ by the affine equation*

$$y^2 = x^5 + \frac{1}{4}vx^4 - \frac{5}{2}vx^3 - \frac{1}{8}v^2x^2 + \frac{9}{16}v^2x + \frac{1}{64}v^3$$

*becomes isomorphic to $C_w$ over $k(\sqrt{w})$.*

*Remark* 2.4. If $k$ were equal to $\mathbf{C}$, a classical result of Bolza [**2**] would show that there exists an $s \in \Omega$ such that $C_w$ is isomorphic to the curve $y^2 = x^6 + sx^3 + 1$. A calculation shows that this remains true in our situation, with $s$ a square root of $4w^2/(w^2 + 108)$. □

**3. The curve $\mathcal{C}_{-107}$ and its twists.** In this section, we specialize to the case $w = \sqrt{-107}$, and write $C_{\sqrt{-107}}$ for the corresponding curve (0.3) or (2.4). It is defined over $\mathbf{Q}(\sqrt{-107})$ and has discriminant 1. Since its coefficients are algebraic integers outside 2, $C_{\sqrt{-107}}$ has good reduction away from 2.

On the other hand, we can form the $\sqrt[4]{-107}$-twist of $C_{\sqrt{-107}}$ as in Proposition 2.3. This gives the curve $\mathcal{C}_{-107}$ defined over $\mathbf{Q}$ by the equation

$$y^2 = x^5 - \frac{107}{4}x^4 + \frac{535}{2}x^3 - \frac{11449}{8}x^2 + \frac{103041}{16}x - \frac{1225043}{64},$$

which has good reduction away from 2 and 107. Twisting $\mathcal{C}_{-107}$ by $\sqrt{-1}$, gives the curve $\mathcal{C}'_{-107}$

$$y^2 = x^5 + \frac{107}{4}x^4 + \frac{535}{2}x^3 + \frac{11449}{8}x^2 + \frac{103041}{16}x + \frac{1225043}{64}$$

which has $\Delta_{\mathcal{C}'_{-107}} = 107^{10}$. The advantage is that this curve has good reduction at 2, as can be seen by replacing $x$ by $x - (1/2)$ and then $y$ by $y + (x^2 + x + 1/2)$. This gives the equation

$$y^2 + (x^2 + x + 1)y = x^5 + 24x^4 + 216x^3 + 1068x^2 + 5196x + 16247$$

with integral coefficients.

Since $C_{\sqrt{-107}}$ has good reduction away from $\sqrt{-107}$, and $\mathcal{C}'_{-107}$, viewed as a curve over $\mathbf{Q}(\sqrt{-107})$, is a twist of $C_{\sqrt{-107}}$ and has good reduction away from 2, we deduce that $C_{\sqrt{-107}}$ has everywhere twisted good reduction over $\mathbf{Q}(\sqrt{-107})$.

We can generalize this construction to prove

**Theorem 3.1.** *Let $m$ be a non zero, square-free integer prime to* 107*, and let $K = \mathbf{Q}(\sqrt{-107m})$. Then $\mathcal{C}_{-107}$ acquires twisted good reduction everywhere over $K$.*

*Proof.* Since $\mathcal{C}'_{-107}$ is a twist of $\mathcal{C}_{-107}$ that has good reduction away from 107, we need only consider the prime of $K$ lying above 107. Let $\alpha = \sqrt{-107m}$. Then the twist $C^{(1/\alpha)}_{-107}$ of $\mathcal{C}_{-107}$ by $1/\sqrt{\alpha}$ over $K$ has equation

$$y^2 = x^5 - \frac{107}{4\alpha}x^4 + \frac{535}{2\alpha^2}x^3 - \frac{11449}{8\alpha^3}x^2 + \frac{103041}{16\alpha^4}x - \frac{1225043}{64\alpha^5},$$

so that $\Delta_{C^{(1/\alpha)}_{-107}} = 107^{10}/\alpha^{20} = 1/m^{10}$. By the construction of $\alpha$, this model is integral at 107 and $\Delta_{C^{(1/\alpha)}_{-107}}$ is a unit at 107. Hence, $C^{(1/\alpha)}_{-107}$ has good reduction above 107. □

*Remark* 3.2. When $w = \sqrt{-107}$, a root of the polynomial $W(x)$ of (2.1) generates the Hilbert class field of $\mathbf{Q}(\sqrt{-107})$. Hence the 2-torsion on the Jacobian of $C_{\sqrt{-107}}$ is rational over the Hilbert class field $L$ of $\mathbf{Q}(\sqrt{-107})$. In this case, the Jacobian of $C_{\sqrt{-107}}$ also becomes isogenous to a product of two elliptic curves over $L$. Recall that $u$ denotes a square root of $w^2+108$. Thus, when $w = \sqrt{-107}$, $u$ specializes to $\pm 1$, so that the specialization of the isogeny of Proposition 2.2 is defined over $\mathbf{Q}(\sqrt{-107}, \alpha) = L$. The characteristic polynomial $t^4 + t^3 - 2t^2 + 3t + 9$ of $C_{\sqrt{-107}}$ at a prime of $\mathbf{Q}(\sqrt{-107})$ above 3 is irreducible so, arguing as in the proof of Proposition 2.2 (2), we see that the extension to $L$ is necessary to realize the isogeny.

**4. The curve $\mathcal{C}_{-109}$ and its twists.** This time, we specialize to the case $w = \sqrt{-109}$ and write $C_{\sqrt{-109}}$ for the corresponding curve (0.3) or (2.4). We start with the model obtained by substituting $w = \sqrt{-109}$ in (0.3):

$$y^2 = x(x+1)\left(x^3 + \frac{1}{4}(\sqrt{-109}+6)x^2 + \frac{1}{4}(\sqrt{-109}-6)x - 1\right).$$

It is defined over $\mathbf{Q}(\sqrt{-109})$, and again has discriminant 1. Since its coefficients are algebraic integers outside 2, $C_{\sqrt{-109}}$ has good reduction away from 2. Twisting by $\sqrt{2+\sqrt{-109}}$ gives the curve $C^{(2+\sqrt{-109})}_{\sqrt{-109}}$

with equation

$$y^2 = x^5 + \left(\frac{12\sqrt{-109} - 89}{4}\right)x^4 - \left(\frac{105\sqrt{-109} + 436}{2}\right)x^3 + \left(\frac{324\sqrt{-109} + 17033}{4}\right)x^2 + (840\sqrt{-109} - 9281)x,$$

which also has the integral model

$$y^2 + (\sqrt{-109}x^2 + x)y = x^5 + (3\sqrt{-109} + 5)x^4 - (53\sqrt{-109} + 218)x^3 + (81\sqrt{-109} + 4258)x^2 + (840\sqrt{-109} - 9281)x.$$

Since $2 + \sqrt{-109}$ is one of the primes of $\mathbf{Q}(\sqrt{-109})$ above 113, $C^{(2+\sqrt{-109})}_{\sqrt{-109}}$ has good reduction outside $2 + \sqrt{-109}$ and, in particular, at the prime of $\mathbf{Q}(\sqrt{-109})$ lying above 2. It follows that $C_{\sqrt{-109}}$ has everywhere twisted good reduction over $\mathbf{Q}(\sqrt{-109})$.

By Proposition 2.3, the $\sqrt[4]{-109}$-twist $\mathcal{C}_{-109}$ of $C_{\sqrt{-109}}$ has equation

$$y^2 = x^5 - \frac{109}{4}x^4 + \frac{545}{2}x^3 - \frac{11881}{8}x^2 + \frac{106929}{16}x - \frac{1295029}{64}.$$

It has good reduction outside 2 and 109.

**Theorem 4.1.** *Let $m$ be a square-free integer prime to* 109 *and such that $m \equiv 1 \pmod 8$, and let $K = \mathbf{Q}(\sqrt{-109m})$. Then $\mathcal{C}_{-109}$ has everywhere twisted good reduction over $K$.*

*Proof.* Since $\mathcal{C}_{-109}$ has good reduction outside 2 and 109, we only need to construct twists with good reduction at the primes above 2 and 109 of $K$. Let $\beta = \sqrt{-109m}$. Then the twist $C^{(1/\beta)}_{-109}$ of $\mathcal{C}_{-109}$ over $K$ has equation

$$y^2 = x^5 - \frac{109}{4\beta}x^4 + \frac{545}{2\beta^2}x^3 - \frac{11881}{8\beta^3}x^2 + \frac{106929}{16\beta^4}x - \frac{1295029}{64\beta^5}$$

and $\Delta_{C^{(1/\beta)}_{-109}} = 1/m^{10}$. Since $m$ is prime to 109, $C^{(1/\beta)}_{-109}$ has good reduction at the prime of $K$ above 109.

To conclude, we need to prove that $\mathcal{C}_{-109}$ has a twist over $K$ that has good reduction at the prime above 2. Since $m \equiv 1 \pmod 8$, $m$ is a square of $\mathbf{Q}_2$, and so $\mathbf{Q}_2(\sqrt{-109}) = \mathbf{Q}_2(\sqrt{-109m})$ (in some fixed algebraic closure of $\mathbf{Q}_2$). Furthermore, $C_{-109}^{(1/\beta)}$ is isomorphic to $C_{-109}$ over $\mathbf{Q}_2(\sqrt{-109})$. Again, since $2 + \sqrt{-109m}$ is invertible as a 2-adic integer, the condition $m \equiv 1 \pmod 8$ implies that $(2+\sqrt{-109m})/(2+\sqrt{-109}) \equiv 1 \pmod 8$ and is therefore a square of $\mathbf{Q}_2(\sqrt{-109})$. It follows that the twist $C_{-109}^{(1/\beta,2+\beta)}$ of $C_{-109}^{(1/\beta)}$ by $\sqrt{2+\beta}$ is isomorphic over $\mathbf{Q}_2(\sqrt{-109})$ to $C_{\sqrt{-109}}^{(2+\sqrt{-109})}$. Since we have already seen that the latter has good reduction at the prime above 2 of $\mathbf{Q}(\sqrt{-109})$ and therefore also over $\mathbf{Q}_2(\sqrt{-109})$, it follows that the former also has good reduction over $\mathbf{Q}_2(\sqrt{-109})$. Since good reduction at a prime of a number field is equivalent to good reduction over the completion, we conclude that $C_{-109}^{(1/\beta,2+\beta)}$ has good reduction at the prime of $K$ above 2. □

*Remark* 4.2. When $w = \sqrt{-109}$, the roots of the polynomial $W(x)$ of (2.1) generate a cubic cyclic extension $L$ of $\mathbf{Q}(\sqrt{-109})$ which is everywhere unramified. It follows that the 2-torsion on the Jacobian of $C_{\sqrt{-109}}$ is rational over $L$. We have $u = \pm\sqrt{-1}$, and $L(u)$ is the Hilbert class field of $\mathbf{Q}(\sqrt{-109})$. By specializing from Proposition 2.2, we see that the Jacobian of $C_{\sqrt{-109}}$ becomes isogenous to the product of two elliptic curves over $L(u)$. Thus, as with the twists of $C_{\sqrt{-107}}$, an extension of degree divisible by 3 is necessary for the Jacobian of $\mathcal{C}_{-109}$ to become isogenous to a product of elliptic curves.

**5. Setzer's curves revisited.** As promised in the introduction, we shall explain briefly how the genus 2 curves (0.2) were found. Let $L$ be a number field. We search for genus 2 curves over $L$ with everywhere good reduction. Inspired by the fact that Setzer's elliptic curves over imaginary quadratic fields $K$ with everywhere good reduction have a $K$-rational two-torsion point, we decided to start with genus two curves having two $L$-rational Weierstrass points. Such curves have a model of the form

$$y^2 + (px^2 + qx)y = x^5 + ax^4 + bx^3 + cx^2 + dx, \quad a, b, c, d, p, q \in L,$$

the Weierstrass points being the unique point at infinity and $(0, 0)$. When $q = p$, it turns out that $\Delta_C$ is of degree 10 as a polynomial in $p$

with only even powers of $p$ occurring. Furthermore, the coefficient of $p^{10}$ is $d^2(d+1-a+b-c)$). This vanishes if and only if $d = a-b+c-1$. (If $d = 0$, then $(0,0)$ is a singular point of $C$, which is therefore not of genus 2.) Substituting this value for $d$ in $\Delta_C$ gives a polynomial of degree 4 in $p^2$ whose leading coefficient is

$$(a - b + c - 1)^2(3a - 2b + c - 4)^2.$$

A check now shows that, if $a - b + c - 1 = 0$ or if $3a - 2b + c - 4 = 0$, then $\Delta_C = 0$, so we cannot reduce the degree of $\Delta_C$ in $p$ any further. We therefore try to arrange for the leading coefficient of $\Delta_C$ to be a unit. If this is the case, if $a$, $b$, $c$ are algebraic integers, if $\varepsilon \in L$ is a unit and if $p$ is a root of $\Delta_C = \varepsilon$, then $C$ has everywhere good reduction over $L$.

To simplify, we therefore suppose that $a - b + c - 1 = \pm 1$ and $3a - 2b + c - 4 = \pm 1$. These conditions are equivalent to $d \in \{\pm 1\}$ and $2a - b \in \{1, 3, 5\}$. Calculating $\Delta_C$ for each of these possibilities for $d$ and $2a - b$ shows that, up to simple transformations, there are two cases, one leading to the curves (0.2) whose discriminant is a square and the other to a family of curves with everywhere good reduction over degree 8 number fields and whose discriminant has a more complicated form.

After these calculations had been completed, we decided to make a similar search for elliptic curves with everywhere good reduction. This led to the parametric families of elliptic curves with Weierstrass equation

$$E = E^{\varepsilon}_{p,a} : \; y^2 + pxy = x^3 + ax^2 + \varepsilon x, \quad \varepsilon \in \{\pm 1\}, \tag{5.1}$$

with discriminant $\Delta = (p^2 + 4a)^2 - 64\varepsilon$ and $j$-invariant $(\Delta + 16\varepsilon)^3/\Delta$.

Again, if $a \in \mathbf{Z}$ and $p$ is a root of one of the four polynomials $(t^2 + 4a)^2 \pm 64 = \pm 1$, then $E$ acquires everywhere good reduction over any field $L$ containing $p$.

Recall that Setzer [**8**] determined all elliptic curves with everywhere good reduction over imaginary quadratic fields $K$ and having a $K$-rational torsion point of order 2.

**Theorem 5.1** (Setzer). *Let $K$ be an imaginary quadratic field, and write $K = \mathbf{Q}(\sqrt{-m})$ with $m$ a square-free positive integer. There exists*

*an elliptic curve $E/K$ with everywhere good reduction and a $K$-rational 2-torsion point if and only if $m = 65m_1$, where $m_1$ is a square* $\pmod 5$ *and* $\pmod{13}$ *and* 65 *is a square* $\pmod{m_1}$.

We now give an alternative description of Setzer's curves, starting with the curves $E = E^{\varepsilon}_{p,a}$ as in (5.1).

We take the curve $E^{-1}_{p,a}$ and assume that the discriminant is 1. Thus, $(p^2 + 4a)^2 = 65$, $j = 17^3$ and $E$ has everywhere good reduction over the field $\mathbf{Q}(p)$ whenever $a \in \mathbf{Z}$.

Replacing $y$ by $y + (1/2)px$, we obtain the model

$$E' : y^2 = x^3 + \frac{\sqrt{65}}{4}x^2 + x \tag{5.2}$$

over $\mathbf{Q}(\sqrt{65})$ which has good reduction over that field away from the primes dividing 2.

Twisting $E'$ by $\sqrt[4]{65}$ gives the elliptic curve with equation $y^2 = x^3 + (65/4)x^2 + 65x$, which has rational coefficients. Writing this in the form

$$E_{65} : y^2 + xy = x^3 + 16x^2 + 65x, \tag{5.3}$$

we find that $E_{65}$ now has discriminant $65^3$ so, in particular, it has good reduction at 2. In fact, the conductor of $E_{65}$ is $65^2 = 4225$, and we can identify it in Cremona's tables [**3**] as the curve $4225m_1$, though we shall not use this. By construction, we know that $E_{65}$ acquires everywhere good reduction over $\mathbf{Q}(\sqrt[4]{65})$.

**Proposition 5.2.** *Let $K$ be an imaginary quadratic field satisfying the following conditions.*

(1) *The primes* 5 *and* 13 *are ramified in $K$ and $\mathbf{Q}(\sqrt{65})$ have isomorphic completions at the primes above* 5 *and* 13.

(2) *$K$ has a quadratic extension $L$, unramified outside* 5 *and* 13, *such that $L$ and $\mathbf{Q}(\sqrt[4]{65})$ have isomorphic completions at the primes above* 5 *and* 13.

*Then the twist $C$ by $L$ of $E_{65}$ (viewed as an elliptic curve over $K$) has everywhere good reduction over $K$.*

*Proof.* As $L$ is unramified outside 5 and 13, and $E_{65}$ has good reduction away from 5 and 13, $C$ also has good reduction away from the primes of $K$ dividing 5 and 13. To see that $C$ has good reduction above 5, we use the fact that $E'$ is the $\sqrt[4]{65}$-twist of $E_{65}$ and $C$ the $L$-twist of $E_{65}$; conditions (1) and (2) imply that $E'$ and $C$ become isomorphic over the 5-adic completions of $K$ and $\mathbf{Q}(\sqrt{65})$. Since $E'$ has good reduction at the prime above 5, it follows that $C$ also has good reduction there. Since good reduction at a prime of a number field is equivalent to good reduction over the completion, we deduce that $C$ has good reduction at the prime of $K$ above 5. A similar argument shows that $C$ has good reduction at the prime above 13. □

Now let $K$ be a quadratic field in which 5 and 13 are ramified, and denote by $\mathfrak{p}_5$ and $\mathfrak{p}_{13}$ the primes of $K$ above 5 and 13. Condition (2) of Proposition 5.2 shows that $L$ is ramified at $\mathfrak{p}_5$ and at $\mathfrak{p}_{13}$. This implies that there exists a $\theta \in \mathcal{O}_K$ such that $L = K(\sqrt{\theta})$ and

$$\theta\mathcal{O}_K = \mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{b}^2,$$

where $\mathfrak{b}$ is an integral ideal of $K$. If, further, $L/K$ is unramified at 2, then $\mathfrak{b}$ is prime to $2\mathcal{O}_K$ and $\theta$ is a square $\pmod{4\mathcal{O}_K}$. Conversely, if $\theta \in \mathcal{O}_K$ verifies these conditions, and if $L = K(\sqrt{\theta})$, then $L/K$ is ramified at $\mathfrak{p}_5$ and at $\mathfrak{p}_{13}$ and unramified elsewhere. These conditions already occur in [**8**] and, as explained there, genus theory shows that they are equivalent to $K$ being of the form described in Theorem 5.1. Thus Proposition 5.2 gives a proof of the "if" part of Theorem 5.1.

*Remark* 5.3. In fact, Setzer not only also proves the "only if" part of Theorem 5.1 but also proves that, when $K$ is of the form stated in the Theorem, there are exactly $2^t$ isomorphism classes of elliptic curves with everywhere good reduction over $K$, where $t \geq 2$ is the number of primes ramified in $K$. Recall that the 2-part of the class group of $K$ is then isomorphic to a product of $t-1$ groups of order 2. Now if $C$ is a curve as in Proposition 5.2, then $C$ and the twists of $C$ by the $2^{t-1}-1$ unramifed quadratic extensions of $K$ are mutually non isomorphic and have everywhere good reduction over $K$. This accounts for half of Setzer's curves. The others are obtained by applying the same argument to the quotient of $C$ by the subgroup generated by its $K$-rational subgroup of order 2.

## REFERENCES

**1.** V. Abrashkin, *Galois modules of period p group schemes over the ring of Witt vectors*, Izv. Akad. Nauk SSSR **51** (1987), 691–736 (in Russian); Math. USSR Izv. **31** (1988), 1–46 (in English).

**2.** O. Bolza, *On binary sextics with linear transformations into themselves*, Amer. Math. J. **10** (1888), 47–70.

**3.** J.E. Cremona, *Elliptic curve database*, available at `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html`.

**4.** J.-M. Fontaine, *Il n'y a pas de variété abélienne sur* **Z**, Invent. Math. **81** (1985), 515–538.

**5.** F. Leprévost, *Jacobiennes de certaines courbes de genre deux: Torsion et simplicité*, J. Theor. Nombr. Bordeaux **7** (1995), 283–306.

**6.** P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. **342** (1994), 729–752.

**7.** J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects Math. **15**, Vieweg, Berlin, 1989.

**8.** B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific. J. Math. **74** (1978), 235–250.

**9.** I.R. Shafarevich, *Algebraic number fields*, AMS Transl. 2nd series **31**, 25–39.

**10.** C.L. Siegel, *Über einige Anwendungen diophantscher Approximationen*, Abh. Pr. Akad. Wiss. **1** (1929), 209–266.

**11.** J.H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1986.

**12.** J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Lect. Notes Math. **476**, Springer-Verlag, Berlin, 1975.

Faculté de Mathématiques, Université des Sciences et de la Technologie Houari Boumedienne, BP 32 El Alia, Bab Ezzouar, Alger, 16111 Algeria
**Email address: houriarz@yahoo.com**

Laboratoire de Mathématiques Nicolas Oresme, UFR Sciences, Campus 2, Université de Caen Basse-Normandie, 14032 Caen cedex, France
**Email address: john.boxall@unicaen.fr**