ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 44, Number 3, 2014

ON QUADRATIC TWISTS OF HYPERELLIPTIC CURVES

MOHAMMAD SADEK

ABSTRACT. Let C be a hyperelliptic curve of good reduction defined over a discrete valuation field K with algebraically closed residue field k. Assume moreover that $\operatorname{char} k \neq 2$. Given $d \in K^* \setminus K^{*2}$, we introduce an explicit description of the minimal regular model of the quadratic twist of C by d. As an application, we show that if $C/\mathbf{Q}$ is a nonsingular hyperelliptic curve given by $y^2 = f(x)$ with f an irreducible polynomial, there exists a positive density family of prime quadratic twists of C which are not everywhere locally soluble.

1. Introduction.

Let C be a nonsingular hyperelliptic curve defined over $\mathbf{Q}$ with an affine model given by the equation $y^2 = f(x) \in \mathbf{Z}[x]$, where $\deg(f) \geq 3$. The genus of C will be called g. If $d > 1$ is a square free integer, then we write C_d for the quadratic twist of C by d. In particular, C_d is defined by $dy^2 = f(x)$.

We try to find an explicit description of the minimal regular model of $C_d/\mathbf{Q}_p$ in terms of the minimal regular model of $C/\mathbf{Q}_p$ itself, when C has good reduction.

Let Δ denote the minimal discriminant of $C/\mathbf{Q}_p$, see [**2**, Section 2]. For every prime $p \nmid \Delta$, $C/\mathbf{Q}_p$ has good reduction. Hence, the minimal regular model of $C/\mathbf{Q}_p$ is smooth over $\mathbf{Z}_p$. The minimal regular model of $C_d/\mathbf{Q}_p$, $p \mid d$ is obtained as the minimal desingularization of a quotient of a smooth scheme by a twisted action of some finite group, see Section 3. In fact, we prefer to handle the problem over the maximal unramified extension of $\mathbf{Q}_p$ to avoid any complications which might appear because the residue field $\mathbf{F}_p$ is not algebraically closed.

As we investigate minimal regular models of quadratic twists of a hyperelliptic curve C over $\mathbf{Q}_p$, we cannot see how to do the curves C_d, where one of the prime divisors p of d is a bad prime of C and f has no simple root when reduced modulo p. The difficulty lies in the wide range of possibilities of the structure of the minimal regular model of

Received by the editors on October 5, 2010, and in revised form on January 27, 2012.

DOI:10.1216/RMJ-2014-44-3-1015

$C/\mathbf{Q}_p$ when C has bad reduction. Furthermore, we are not aware of any reference which discusses the desingularization of quotient singularities of models of algebraic curves when these singularities are not ordinary double points.

Now assume C is a hyperelliptic curve defined over $\mathbf{Q}$ given by the equation $y^2 = f(x)$, where $f(x)$ is an irreducible polynomial. Using the description of the minimal regular model of a quadratic twist of $C/\mathbf{Q}_p$, we show that there is an infinite number of quadratic twists of C with no $\mathbf{Q}_p$-rational points. In particular, for a nonsingular hyperelliptic curve $C/\mathbf{Q}$, there exists an infinite number of quadratic twists C_d of C such that $C_d(\mathbf{Q}_p) = \varnothing$ for some prime p, and hence $C_d(\mathbf{Q}) = \varnothing$.

2. Hyperelliptic curves.

The material in this section can be found in [**3**, subsection 7.4.3].

We assume K is a field with $\operatorname{char} K \neq 2$ and algebraic closure $\overline{K}$. Two hyperelliptic equations with coefficients in K

$$y^2 = f(x) \quad \text{and} \quad z^2 = f'(u)$$

represent isomorphic curves if and only if

$$x = \frac{au+b}{cu+d}, \qquad y = \frac{ez}{(cu+d)^{g+1}}$$

where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K), \quad e \in K^*.$$

We associate a discriminant Δ to a hyperelliptic equation $y^2 = f(x)$ as in [**2**, Section 2]. This equation defines a smooth curve if and only if $\Delta \neq 0$.

By a *hyperelliptic curve* C over K we mean a smooth curve of genus $g \geq 2$ endowed with a morphism $C \to \mathbf{P}^1_K$ of degree 2. There exists a hyperelliptic equation $y^2 = f(x) \in K[x]$ describing C with $\deg f \in \{2g+1, 2g+2\}$. The fact that C is smooth implies $f(x)$ is separable over $\overline{K}$. The equation $y^2 = f(x)$ has one singularity at infinity. If $\deg f = 2g+1$, the singularity at infinity corresponds to one point ∞ on the hyperelliptic equation. If $\deg f = 2g+2$, the singularity corresponds to two points ∞^+ and ∞^- on the hyperelliptic equation, and these can be distinguished by the value of the rational function y/x^{g+1}. If $\deg f = 2g+2$, then there exists a hyperelliptic equation $z^2 = f'(u)$ describing C over $\overline{K}$ with $\deg f' = 2g+1$, and it describes C/K if and only if $f(x)$ has a zero in K.

Let C be a smooth hyperelliptic curve of genus $g \geq 2$ defined over K by the equation $y^2 = f(x)$. We will denote the hyperelliptic involution on C by $\iota : C \to C$. Let $K' = K(\sqrt{d})$ be a separable quadratic extension of K where $d \in K \setminus K^{*2}$. By a quadratic twist C_d of C we mean the hyperelliptic curve obtained from the curve C/K' by twisting the curve C/K by the cohomology class corresponding to K' in $H^1(K, \langle\iota\rangle)$.

This means that if σ generates $\mathrm{Gal}\,(K'/K)$, then the twisted action of $\mathrm{Gal}\,(K'/K)$ on $C(K')$ is given by $Q \to \iota(\sigma Q)$. To produce an explicit equation describing C_d, we consider the quadratic character $\chi : \mathrm{Gal}\,(K'/K) \to \{\pm 1\}$ associated with K'/K, i.e., $\chi(\sigma) = \sqrt{d}^{\sigma}/\sqrt{d}$. Then we define a cocycle in

$$\begin{aligned} H^1(K, \langle\iota\rangle) &\cong H^1(K, \mathbf{Z}/2\mathbf{Z}) \\ &= \mathrm{Hom}\,(\mathrm{Gal}\,(\overline{K}/K), \mathbf{Z}/2\mathbf{Z}) \\ &= \mathrm{Hom}\,(\mathrm{Gal}\,(\overline{K}/K), \pm 1) \end{aligned}$$

by

$$\xi : \mathrm{Gal}\,(\overline{K}/K) \longrightarrow \{\pm 1\}; \quad \xi_\tau = [\chi(\tau)].$$

Now, $\overline{K}(C) = \overline{K}(x,y)$ and $\overline{K}(C_d) = \overline{K}(x,y)_\xi$ (the twist of the function field by the cocycle ξ). Since $\iota(x,y) = (x,-y)$, the action of σ on $\overline{K}(x,y)_\xi$ is described by

$$\sqrt{d}^{\sigma} = \chi(\sigma)\sqrt{d}, \quad x^\sigma = x, \ y^\sigma = \chi(\sigma)y.$$

Thus, the functions which are fixed by $\mathrm{Gal}\,(K'/K)$ in $\overline{K}(x,y)_\xi$ are $x' = x$, $y' = y/\sqrt{d}$; hence, they are in $K(C_d)$. They satisfy the equation

$$dy'^2 = f(x').$$

The curves C and C_d are isomorphic over K' via $(x', y') \mapsto (x', y'\sqrt{d})$.

3. Minimal regular models of hyperelliptic curves. We assume that K is a complete discrete valuation field with ring of integers $\mathcal{O}_K$, valuation ν, uniformizer t and residue field k with $\operatorname{char} k \neq 2$. Set $S = \operatorname{Spec} \mathcal{O}_K$.

Let C be a hyperelliptic curve defined over K. In [**2**], Liu associates to C a projective model W, a *Weierstrass model* of C, defined over $\mathcal{O}_K$, arising from a hyperelliptic equation of C with integral coefficients. The discriminant Δ_W of W is the discriminant of this hyperelliptic equation. The model W is said to be *minimal* if Δ_W is minimal, i.e., $\nu(\Delta_W)$ is the least possible valuation among the valuations of the discriminants of the hyperelliptic equations related to our equation via the transformations of the form given in Section 2. If $C(K) \neq \varnothing$, then W being minimal implies that the minimal regular model of C is the minimal desingularization of W, see [**5**, Corollary 5].

Let W be a minimal Weierstrass model of C. The curve C has good reduction if $\nu(\Delta_W) = 0$. In fact, the latter statement is equivalent to saying that the minimal regular model $\mathcal{C}$ of C over S is smooth, see [**2**, Section 3]. Moreover, $\mathcal{C}$ is the unique smooth model of C over S, ([**3**, Proposition 10.1.21 (b)]).

Lemma 3.1. *Assume that C has good reduction over k. Let K'/K be a finite extension with residue extension k'/k. Then $C \times_K K'$ has good reduction over k'.*

Proof. Let $\mathcal{C}$ be a minimal Weierstrass model of C. Let ν' be the valuation corresponding to K'. Since $\nu' = e_{K'/K} \times \nu$, where $e_{K'/K}$ is the ramification index of K'/K, one has $\nu'(\Delta_{\mathcal{C}}) = e_{K'/K} \times \nu(\Delta_{\mathcal{C}}) = 0$. □

Recall the following results, which allow us to determine whether a curve defined over a complete discrete valuation field K has a K-rational point.

Lemma 3.2 [**3**, Corollary 9.1.32]. *Let C be an algebraic curve of genus $g \geq 1$ defined over K. Let $\mathcal{C} \to S$ be the minimal regular model of C. Assume that $C(K) \neq \varnothing$. Then a point $P \in C(K)$ is reduced to a point $\widetilde{P} \in \mathcal{C}_k(k)$ and $\mathcal{C}_k$ is smooth at $\widetilde{P}$. In particular, $\widetilde{P}$ belongs to a single irreducible component of multiplicity* 1 *in $\mathcal{C}_k$.*

Lemma 3.3. *Let C be a smooth hyperelliptic curve over K. Assume that C has good reduction over k. Let K'/K be a quadratic extension with residue field k'/k. Let $\mathcal{C}'$ be the minimal regular model of $C \times K'$. Then $\mathcal{C}'$ is smooth over $\mathcal{O}_K$. Moreover, $\mathcal{C}'_{k'}$ consists of one irreducible component of multiplicity* 1.

Proof. Since C has good reduction over k, then it extends to a smooth relative curve $\mathcal{C}/_{\mathcal{O}_K}$. This relative curve is the minimal regular model of C over $\mathcal{O}_K$. Hence, it consists of one irreducible component Γ. If $C(K) \neq \varnothing$, then $\operatorname{mult}(\Gamma) = 1$, see Lemma 3.2, otherwise $\operatorname{mult}(\Gamma) = 2$. The reason for the latter statement is as follows: Let D be the image of Γ in $\mathbf{P}^1_S$ under the morphism $g : \mathcal{C} \to \mathbf{P}^1_S$. We will denote the generic points of Γ and D by ξ and ξ', respectively. The morphism g restricts to $\mathcal{O}_{\Gamma,\xi} \to \mathcal{O}_{D,\xi'}$. The valuations ν_Γ and ν_D are the corresponding normalized valuations to Γ and D, respectively. Remember that $\nu_D(t) = 1$ because D is reduced. One has $[\operatorname{Frac}(\mathcal{O}_{\Gamma,\xi}) : \operatorname{Frac}(\mathcal{O}_{D,\xi'})] = 2$. Since Γ is not reduced, we deduce that t ramifies in $\operatorname{Frac}(\mathcal{O}_{\Gamma,\xi})$. Thus, $\nu_\Gamma(t) = 2$.

Lemma 3.1 implies that the minimal regular model of $C \times K'$ is smooth. Again it consists of one irreducible component Γ' of multiplicity 1. This is clear if $\operatorname{mult}(\Gamma) = 1$. If $\operatorname{mult}(\Gamma) = 2$, then $\operatorname{mult}(\Gamma') = \operatorname{mult}(\Gamma)/[K' : K]$, see for example [**4**, subsection 2.4]. It is true that the mentioned reference gives results when $\overline{k} = k$, but if we take a base change over the maximal unramified extension of K, then the multiplicity of components will not change. □

We have to mention that the statements of Lemmas 3.1 and 3.3 are true for any base extension. In other words, smoothness is preserved by arbitrary base change. We wrote down the proofs when the base change is quadratic for the convenience of the reader.

In what follows we assume k is algebraically closed. Hence, $K' = K(\sqrt{t})$ is the unique quadratic extension of K, and it is totally and tamely ramified. Furthermore, K'/K is Galois. Let $G := \operatorname{Gal}(K'/K) = \langle \sigma \rangle$.

Again C/K is a hyperelliptic curve. We assume that C/K has good reduction. We are concerned with the twisted action of σ on $C(K')$ given by $Q \to \iota(\sigma Q)$, where $\iota : C \to C$ is the hyperelliptic involution on C and $\sigma(Q)$ is the usual Galois action of σ on $C(K')$. Now the automorphism $\sigma : C \to C$ extends to the minimal regular models $\mathcal{C}$ and $\mathcal{C}'$ of C and $C \times K'$, respectively. We will denote the extended automorphism by σ again.

Let C_t be the quadratic twist of C by t. In what follows we obtain the minimal regular model of C_t/K as the minimal desingularization of the quotient scheme $\mathcal{C}'/\langle\sigma\rangle$ by the twisted action of σ. In other words, we construct the minimal regular model of C_t/K from the minimal regular model of C/K.

The first step is to find the fixed points of the twisted action of σ on $\mathcal{C}'$. This is because the singular points of $\mathcal{C}'/\langle\sigma\rangle$ lie among the images of the points of $\mathcal{C}'$ fixed by σ. Let $y^2 = f(x)$ be a minimal hyperelliptic equation describing C. Then the assumption that C has good reduction implies that $f(x)$ has no repeated roots over k. If $P \in C \times K'$, we denote its reduction by $\widetilde{P}$.

Proposition 3.4. *Let $P \in C \times K'$. The following are equivalent*:

(i) *P is fixed under the twisted action of σ.*

(ii) *$\widetilde{P} = (\widetilde{x}, \widetilde{y})$ is fixed under the twisted action of σ.*

(iii) *$f(\widetilde{x}) = 0$ over k.*

Proof. The twisted action of σ on P is given by $\iota(\sigma P)$. Let $P = (x_0 + x_1\sqrt{t}, y_0 + y_1\sqrt{t})$, where $x_0, x_1, y_0, y_1 \in K$ is fixed if and only if $(x_0 - x_1\sqrt{t}, -y_0 + y_1\sqrt{t}) = (x_0 + x_1\sqrt{t}, y_0 + y_1\sqrt{t})$. Hence, $x_1 = y_0 = 0$. Whence P is fixed if and only if $P = (x_0, y_1\sqrt{t})$ where $x_0, y_1 \in K$. The latter is equivalent to $\widetilde{P} = (\widetilde{x}_0, 0)$, or equivalently, $f(\widetilde{x}_0) = 0$ in k. Now if $(x, y) \in \mathcal{C}_k$, then it is σ-fixed if and only if $(x, y) = (x, -y)$, i.e., $2y = 0$ but $2 \in k^*$, hence $y = 0$. So (i) $\Leftrightarrow$ (ii) holds. □

Recall that C and C_t are isomorphic over K'. Therefore, both $C \times K'$ and $C_t \times K'$ have the same minimal regular model $\mathcal{C}' \to \operatorname{Spec} \mathcal{O}_{K'}$. The model $\mathcal{C}'$ is smooth. Since $\mathcal{C}'$ is projective, the S-quotient scheme $Z := \mathcal{C}'/\langle\sigma\rangle$ is constructed by gluing together the rings of invariants of $\langle\sigma\rangle$-invariant affine open sets of $\mathcal{C}'$. Moreover, Z is a normal scheme and hence its singular points are closed points of the special fiber.

Proposition 3.5. *Let $\sigma_k : \mathcal{C'}_k \to \mathcal{C'}_k$ and $\sigma_k^{\mathrm{red}} : \mathcal{C'}_k^{\mathrm{red}} \to \mathcal{C'}_k^{\mathrm{red}}$ be the natural morphisms induced by σ. Then the natural map*

$$\mathcal{C'}_k^{\mathrm{red}}/\langle \sigma_k^{\mathrm{red}} \rangle \to Z_k^{\mathrm{red}} := (\mathcal{C}'/\langle \sigma \rangle)_k^{\mathrm{red}}$$

is an isomorphism over k.

Proof. See ([**6**, Facts II, III]). □

In fact, if $\alpha : \mathcal{C}' \to Z$ is the quotient map, then α induces a natural map $\mathcal{C}'_k \to Z_k^{\mathrm{red}}$ which factors as follows:

$$\mathcal{C}'_k \longrightarrow \mathcal{C}'_k/\langle \sigma_k \rangle \to Z_k^{\mathrm{red}}$$

where the second map is the normalization map of Z_k^{red}, see [**5**, page 21].

Proposition 3.6. *The generic fiber of $Z := \mathcal{C}'/\langle \sigma \rangle$ is isomorphic to C_t/K.*

Proof. The generic fiber of Z is given by

$$Z_K = Z \times_{\mathcal{O}_K} K = (\mathcal{C}'/\langle \sigma \rangle) \times_{\mathcal{O}_K} K = (\mathcal{C}' \times_{\mathcal{O}_K} K)/\langle \sigma \rangle.$$

But one has

$$\mathcal{C}' \times_{\mathcal{O}_K} K = \mathcal{C}' \times_{\mathcal{O}_{K'}} \mathcal{O}_{K'} \times_{\mathcal{O}_K} K = \mathcal{C}' \times_{\mathcal{O}_{K'}} K' = C \times K'.$$

Since we consider the twisted action of σ, we have $Z_K = C_t$. □

Now we aim to prove that the minimal desingularization $\widetilde{Z}$ of the S-quotient scheme $Z = \mathcal{C}'/\langle \sigma \rangle$ is the minimal regular model of C_t/K. Moreover, we will show that this model consists of one irreducible component of multiplicity 2, the image of the special fiber $\mathcal{C}'_k$ of $\mathcal{C}'$ in Z, and a finite number of multiplicity-1 irreducible components each of which corresponds to a singular point of Z. In particular, if $\rho : \mathcal{C}' \to Z$ is the quotient map, we will prove that, since $\mathcal{C}'$ is smooth, then the only singular points of Z are the images of the σ-fixed points of $\mathcal{C}'$ under ρ.

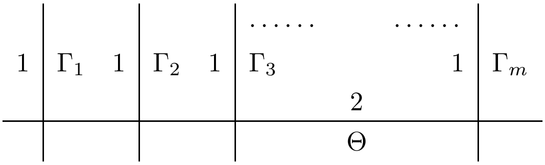
Consider the morphism

$$\mathcal{C}'_k \xrightarrow{\beta} \mathcal{C}'_k/\langle\sigma_k\rangle.$$

Let $y^2 = f(x)$ be a minimal hyperelliptic equation defining C. Since C is smooth, the minimal regular models $\mathcal{C}$ and $\mathcal{C}'$ are smooth, and they are still defined by this affine equation. The ramification points of β are the zeros of $f(x)$ over k plus the point at infinity when $\deg f = 2g+1$. Since $f(x)$ splits completely into linear factors over k, because $k = \overline{k}$, the number of the ramification points of β is $2g+2$.

Theorem 3.7. *Let C/K be a hyperelliptic curve of genus g. Assume that C has good reduction over k. Let $\mathcal{C}'$ be the minimal regular model of $C \times K'$. Again* $\mathrm{Gal}\,(K'/K) = \langle\sigma\rangle$*. Let Z denote the quotient of $\mathcal{C}'$ by the twisted action of σ by the hyperelliptic involution. Then Z is singular exactly at the images $x_1, \dots, x_m$, $m = 2g+2$, of the ramification points of the morphism $\beta : \mathcal{C}'_k \to \mathcal{C}'_k/\langle\sigma_k\rangle$ in Z.*

Let $\widetilde{Z} \to Z$ be the minimal desingularization of Z. Then $\widetilde{Z}$ is the minimal regular model of the quadratic twist C_t of C over K'. Moreover, $\widetilde{Z}_k$ consists of an irreducible component Θ of multiplicity 2 *and components $\Gamma_1, \dots, \Gamma_m$ of multiplicity* 1*, each of which corresponds to blowing-up one of the x_i's; moreover, Θ and Γ_i's are of genus zero, see the following figure.*



Proof. We have seen that the generic fiber Z_K is the curve C_t/K, Proposition 3.6. Furthermore Z is a normal scheme. As we know that $\mathcal{C}'_k$ consists of one irreducible component of multiplicity 1, Lemma 3.3, the image of this irreducible component in Z_k has multiplicity $[K' : K] = 2$, see [**6**, Fact IV].

To obtain the minimal desingularization of Z we only need to blow-up the singularities of Z. We will show first that $x_1, \dots, x_m$ are exactly the singular points of Z. If the points $x_1, \dots, x_m$ were regular, then the morphism $\alpha : \mathcal{C}' \to Z$ would be flat above $x_1, \dots, x_m$. Hence, by Zariski's purity theorem, the branch locus $\alpha(\mathcal{C}' \setminus U)$, where U is the largest open subscheme of $\mathcal{C}'$ such that $\alpha|_U : U \to Z$ is étale, is of codimension 1, see [**3**, Exercise 8.2.15], a contradiction.

Now we blow up Z at each x_i, $i = 1, \dots, m$, to construct the minimal desingularization $\widetilde{Z} \to Z$. Since x_i is a singular point of Z, it is known that if v_1, v_2 are local parameters of the local ring $\mathcal{O}_{Z,x_i}$, then the twisted action of σ_k on v_1, v_2 is described as follows:

$$\sigma_k(v_1) = -v_1, \ \sigma_k(v_2) = -v_2,$$

see [**12**, Lemma 2.2] or [**10**, Lemma 2]. Let $T = \operatorname{Spec} \widehat{\mathcal{O}}_{Z,x_i}$ and $T^G = \operatorname{Spec} \widehat{\mathcal{O}}^G_{Z,x_i}$. Because x_i is non-regular, then T^G is a non-regular local scheme. The monomials $s_1 = v_1^2$, $s_2 = v_1 v_2$ and $s_3 = v_2^2$ are invariant under the action of σ_k and any σ_k-invariant polynomial in v_1, v_2 is a polynomial in these. Therefore, desingularizing T^G is equivalent to desingularizing $\operatorname{Spec} k[s_1, s_2, s_3]/(s_2^2 - s_1 s_3)$. It is known that we need only one blow-up to desingularize $k[s_1, s_2, s_3]/(s_2^2 - s_1 s_3)$ at its only singular point corresponding to the maximal ideal $\mathfrak{m} = (s_1, s_2, s_3)$. In fact, the exceptional curve of the blowing-up is one irreducible component Γ_i isomorphic to $\mathbf{P}^1_k$, see for example [**3**, Example 8.1.5]. Since σ_k acts trivially on x_i, the multiplicity of the irreducible component Γ_i is 1, see [**1**, Proposition 7.3 (ii)].

Each Γ_i has self-intersection -2, whereas the multiplicity-2 component has self-intersection $-g-1 \leq -3$. Therefore, according to Castelnuovo's criterion $\widetilde{Z}$ contains no exceptional divisors, and hence $\widetilde{Z}$ is the minimal regular model of C_t/K.

We conclude by computing the genus of the irreducible components of $\widetilde{Z}_k$. We see that the genus of each of the components Γ_i, $1 \leq i \leq 2g+2$, is 0, because $\Gamma_i \cong \mathbf{P}^1_k$. We can apply Hurwitz's formula, see [**3**, Remark 10.4.8], in order to find the genus of the multiplicity-2 irreducible component Θ. In fact, if p_a denotes the genus, then we have

$$2p_a(\mathcal{C}'_k)-2=2(2p_a(\Theta)-2)+\sum_{1\le i\le m}1=4p_a(\Theta)+2g-2.$$

Therefore, we deduce $p_a(\Theta)=0$ and $\Theta\cong\mathbf{P}^1_k$. $\square$

In Theorem 3.7 we proved that the quadratic twist C_t/K of a hyperelliptic curve C/K of genus $g\ge 2$ and with good reduction has a minimal regular model consisting of a component $\Theta\cong\mathbf{P}^1_k$ of multiplicity 2, and $2g+2$ irreducible components $\Gamma_1,\dots,\Gamma_{2g+2}$ each is isomorphic to $\mathbf{P}^1_k$ and of multiplicity 1. The intersection numbers are given by $\Theta\cdot\Gamma_i=1$ for every i and $\Gamma_i\cdot\Gamma_j=0$ for every $i\neq j$. In case $g=1$, this is reduction type I_0^*, see [**11**, Chapter IV, Section 9], while for $g=2$, this is reduction type $[\mathrm{I}^*_{0-0-0}]$ given, for example, in [**9**, page 155].

4. Quadratic twists which are not everywhere locally soluble.

We start this section with the following result on irreducible polynomials over $\mathbf{Q}$.

Lemma 4.1. *Let $f(x)\in\mathbf{Z}[x]$ be an irreducible polynomial over $\mathbf{Q}$. Then there exists an infinite set of primes S_f in $\mathbf{Q}$ with positive density such that $f(x)$ has no linear factors over $\mathbf{F}_p$ for every $p\in S_f$.*

Proof. There exists an infinite set of primes S_f such that $f(x)$ has no linear factors over $\mathbf{F}_p$ for every $p\in S_f$, see [**7**, Remark 8.40 (d)]. The Chebotarev density theorem implies that the density $\delta(S_f)$ of S_f exists and satisfies $\delta(S_f)>0$, see for example, [**8**, Exercise 11.3.7]. $\square$

Let C be a hyperelliptic curve over $\mathbf{Q}$ of genus $g\ge 1$. Then C has good reduction over all but finitely many finite places of $\mathbf{Q}$, see [**3**, Proposition 10.1.21 (a)]. The finite set of primes in $\mathbf{Q}$ of bad reduction of C will be denoted by S_Δ.

Let C_d be a quadratic twist of C with $d>1$ a square free integer. Since C and C_d are isomorphic over $K=\mathbf{Q}(\sqrt{d})$, it follows that they have the same minimal regular model over the ring of integers of any completion of K at one of its finite places. If $p\notin S_\Delta$, then this implies that for every prime $\mathfrak{p} \in K$ lying above p, both $C \times K_{\mathfrak{p}}$ and $C_d \times K_{\mathfrak{p}}$ have good reduction, see Lemma 3.1, where $K_{\mathfrak{p}}$ denotes the completion of K at $\mathfrak{p}$. In particular, the minimal regular model of $C_d \times K_{\mathfrak{p}}$ is smooth.

We will denote the maximal unramified extension of the p-adic field $\mathbf{Q}_p$ by $\mathbf{Q}_p^{un}$. The residue field of $\mathbf{Q}_p^{un}$ is $\overline{\mathbf{F}}_p$. We write $\mathbf{Z}_p^{un}$ for the ring of integers of $\mathbf{Q}_p^{un}$. The following fact follows directly from Theorem 3.7.

Corollary 4.2. *Let $C : y^2 = f(x) \in \mathbf{Z}[x]$ be a hyperelliptic curve of genus $g \geq 1$ over $\mathbf{Q}$. Assume, moreover, that $f(x)$ is of even degree and irreducible over $\mathbf{Q}$. Let C_d be a quadratic twist of C with $d > 1$ a square free integer. If d has an odd prime factor $p \in S_f \setminus S_\Delta$, then $C_d(\mathbf{Q}_p^{un}) = \varnothing$. Hence, $C_d(\mathbf{Q}_p) = C_d(\mathbf{Q}) = \varnothing$.*

In particular, there is a positive density family of prime quadratic twists of C which are not everywhere locally soluble, and hence have no $\mathbf{Q}$-rational points.

Proof. Note that $K := \mathbf{Q}_p^{un}(\sqrt{d}) = \mathbf{Q}_p^{un}(\sqrt{p})$ because the residue field $\overline{\mathbf{F}}_p$ is algebraically closed. Since $p \notin S_\Delta$, one has $C \times K$ is smooth and $f(x)$ factors completely into linear factors over $\overline{\mathbf{F}}_p$.

Let $\mathcal{C} \to \operatorname{Spec} \mathcal{O}_K$ be the minimal regular model of $C \times K$ and $\mathcal{C}_d \to \operatorname{Spec} \mathbf{Z}_p^{un}$ the minimal regular model of $C_d/\mathbf{Q}_p^{un}$. According to Theorem 3.7, the special fiber $(\mathcal{C}_d)_{\overline{\mathbf{F}}_p}$ consists of an irreducible component of multiplicity 2 and multiplicity-1 irreducible components $\Gamma_1, \ldots \Gamma_m$, $m = 2g+2$, corresponding to blowing-up the singular points of $\mathcal{C}/\langle\sigma\rangle$, where $\operatorname{Gal}(K/\mathbf{Q}_p^{un}) = \langle\sigma\rangle$ and the action of σ on $\mathcal{C}$ is the twisted action by the hyperelliptic involution introduced in Section 3. These singular points correspond to the simple roots of $f(x)$ over $\overline{\mathbf{F}}_p$ (plus the point at infinity if $\deg f = 2g+1$). But since $f(x)$ has no simple root over $\mathbf{F}_p$ as $p \in S_f$, and $\deg f = 2g+2$, it follows that each Γ_i is defined over $\overline{\mathbf{F}}_p$ and none of the Γ_i's is defined over $\mathbf{F}_p$. Indeed, $\mathcal{C}_d \to \operatorname{Spec} \mathbf{Z}_p$ consists only of the multiplicity-2 component. According to Lemma 3.2, $C_d(\mathbf{Q}_p) = \varnothing$. □

Acknowledgments. We would like to thank the anonymous referee for many valuable suggestions and useful comments that allowed us to improve the manuscript.

REFERENCES

1. L. Halle, *Stable reduction of curves and tame ramification*, Math. Z. **265** (2009), 529–550.

2. Q. Liu, *Modèles entiers des courbes hyperelliptiques sur un corps de valuations discrète*, Trans. Amer. Math. Soc. **348** (1996), 4577–4610.

3. ———, *Algebraic geometry and arithmetic curves*, Oxford Grad. Texts Math. **6**, Oxford University Press, Oxford, 2002.

4. D. Lorenzini, *Models of curves and wild ramification*, Pure Appl. Math. Quart., to appear.

5. ———, *Wild quotient singularities of surfaces*, preprint.

6. ———, *Dual graphs of degenerating curves*, Math. Ann. **287** (1990), 135–150.

7. J.S. Milne, *Algebraic number theory* (v3.01), 2008, available at `www.jmilne.org/math/`.

8. M.R. Murty and J. Esmonde, *Problems in algebraic number theory*, Grad. Texts Math. **190**, Springer-Verlag, 2005.

9. Y. Namikawa and K. Ueno, *The complete classification of fibres in pencils of curves of genus two*, Manuscr. Math. **9** (1973), 143–186.

10. A.N. Paršin, *Minimal models of curves of genus* 2 *and homomorphisms of abelian varieties defined over a field of finite characteristic*, Math. USSR **6** (1972), 65–108.

11. J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts Math. **151**, Springer-Verlag, 1995.

12. H. Xue, *Minimal resolution of Atkin-Lehner quotients of $X_0(N)$*, J. Number Theor. **129** (2009), 2072–2092.

Department of Mathematics and Actuarial Science, American University in Cairo, New Cairo, Egypt 11835
Email address: mmsadek@aucegypt.edu