The index of certain hyperelliptic curves over p-adic fields*

Van Geel J. Yanchevskii V.I. †

1 Introduction

Throughout k will be a local field of characteristic zero, i.e., k will be a finite extension of the field of p-adic numbers $\mathbb{Q}_p$. O_k will be the ring of integers in k, κ its residue field, and π a fixed uniformizing element, and v the corresponding valuation.

Let C be a geometrically connected smooth projective curve over k, the index of C, $I(C)$, is the greatest common divisor of the degrees of the divisors on C. For curves over local fields other interpretations of the index exist. For instance an important theorem of Roquette and Lichtenbaum (cf. [6]) tells us that

$$I(C) = \#[\ker(Br(k) \to Br(k(C))] \qquad (RL)$$

with $Br(k), Br(k(C))$ the Brauer groups of respectively k and $k(C)$.

Since the existence of a k-rational point implies clearly that the index is 1, the determination of the index of a curve C is related to the basic diophantine question whether or not the curve C has a k-rational point.

We like to determine the index of curves C defined by an affine equation of the form $Y^2 = h(X)$, with $h(X) \in k[X]$. There is always a rational point on such curves in some quadratic extension of k, so for such curves the index is necessarily 1 or 2. (This fact follows also from the other characterization, (RL), of the index. Namely $k(C) = k(X)(\sqrt{h(X)})$ so the kernel of $Br(k) \to Br(k(C))$ consists of quaternion algebras only. And there is only one quaternion division algebra over the local field

*This work originated in a RIP-program at Oberwolfach.

†Supported by TMR Network ERB FMRX CT-97-0107 and INTAS Project INTAS-99-00817
Received by the editors August 2002.
Communicated by M. M. Van den Bergh.

k.) It follows that $I(C) = 1$ if and only if C has a prime divisor of odd degree, so if and only if C has an l-rational point in some odd degree extension l/k.

Since the index is an invariant of the isomorphism class of the curve one can reduce the problem of determining the index to equations of type $Y^2 = \varepsilon f(X)$ with $f(X)$ a monic polynomial over O_k and $\varepsilon \in O_k$. Moreover if one multiplies ε by a square the index does not change. If ε is a square the index is 1 (the point or points at infinity will be k-rational points). This means that without loss of generality one can assume that $\varepsilon \in \{\alpha, \pi\}$, where α is a unit in O_k which is not a square. (Equations $Y^2 = \alpha\pi f(X)$ can then be dealt with by replacing the uniformizing element π by $\alpha\pi$.) So now we assume that the curve C is given by an equation $Y^2 = \varepsilon f(X)$, $f(X)$ monic over O_k and $\varepsilon \in \{\alpha, \pi\}$. (Moreover we restrict to the case $\deg f(X) > 2$, the other cases being known, therefore the curves we consider are all hyperelliptic curves.)

This note is a sequel to the papers [7], [8]. The starting point of these investigations was the fact that for certain polynomials $f(X)$ the characterization (RL) allows to find sufficient conditions for the index of C to be 2 (cf. [7, propositions 3.7, 3.10], proposition 1). For irreducible polynomials $f(X)$ the conditions we obtained depend only on the root field $L = k(\theta)$, with $f(\theta) = 0$. We wondered whether or not this was always the case. In [7] we were able to give necessary and sufficient conditions for the index to be equal to 2 under the assumption that $f(X)$ is an irreducible polynomial such that the ramification index of its root field is a power of 2. These conditions show that the index depends on the π_L-adic expansion of a root θ of $f(X)$. The proofs were based on norm calculations and an analysis of the parity of the values $v(f(x))$, with x an element in an odd degree extension of k. These techniques are algorithmic in nature, for instance in [8] using the same methods we were able to determine the index for equations $Y^2 = \varepsilon f(X)$ with $\deg f(X) = 4$, $f(X)$ not necessarily irreducible, (i.e., for equations that define elliptic curves over the algebraic closure $\overline{k}$). Results similar to ours were obtained by Poonen and Stoll in [5, lemma 15,16]. They use these results to obtain information on the Tate-Shafarevich group of the Jacobians of the curves. The problem to determine the index of hyperelliptic curves also turns up in [1, lemma 4] where Colliot-Thélène and Poonen investigate families of hyperelliptic curves. These papers motivated us to investigate further whether or not we could improve the results obtained in [7]. It turned out that at least for equations of type $Y^2 = \pi f(X)$, with $f(X)$ a monic irreducible polynomial over O_k, the index can be determined in the case the root field $L = k(\theta)$ of $f(X)$ is a tamely ramified extension of k, this is the main result of this note (cf. theorem 6). The proof is based on a reduction to the results in [7] by considering suitable Galois extensions of k.

2 An application of the Roquette-Lichtenbaum theorem

From now on we assume that the curve C is defined by $Y^2 = \pi f(X)$, with $f(X)$ a monic polynomial over O_k.

As announced in the introduction a sufficient condition for $I(C) = 2$ is stated in [7], proposition 3.10 without proof. (Proposition 3.7 of the same paper gives a similar statement for curves of type $Y^2 = \alpha f(X)$.) For the sake of completeness we restate this result here with a proof. The proof is based on the theorem of Roquette and Lichtenbaum, i.e., the characterization (RL) of the index of C.

Proposition 1. *Let $f(X) = \prod_{i=1}^{r} f_i(X)$ with $f_i(X)$ different monic irreducible polynomials over O_k. Let $L_i \cong k[T]/(f_i(T))$, $i = 1, \ldots, r$. Let C be the smooth projective geometrically connected curve defined by the equation $Y^2 = \pi f(X)$.*

i) *If for all $i = 1, \ldots r$, $k(\sqrt{\alpha}) \subset L_i$ then $I(C) = 2$.*

ii) *If for all $i = 1, \ldots r$, $k(\sqrt{-\alpha\pi}) \subset L_i$ then $I(C) = 2$.*

Proof. Let $L_i = k(\theta_i)$ with $f_i(\theta_i) = 0$, then

$$k(X) \subset k(\sqrt{\alpha})(X) \subset k(\theta_i)(X) = L_i.$$

Define the polynomials $P_i(X) \in k(\sqrt{\alpha})[X]$ by $P_i(X) := N^{k(\theta_i)(X)}_{k(\sqrt{\alpha})(X)}(X - \theta_i)$. Let σ be the generator of the Galois group $\mathrm{Gal}(k(\sqrt{\alpha})/k)$, i.e., $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$, then $f_i(X) = P_i(X)^{\sigma} P_i(X)$ so $f(X) = P(X)^{\sigma} P(X)$ with $P(X) = \prod_{i=1}^{r} P_i(X)$. Consider over k the unique quaternion algebra $D = \left(\dfrac{\alpha, \pi}{k}\right)$ and put $D(X) = \left(\dfrac{\alpha, \pi}{k}\right) \otimes_k k(X)$. Then $D(X)$ is a quaternion algebra over k with as basis $\{1, I, J, K\}$; $I^2 = \alpha, J^2 = \pi, K = IJ = -JI$ and $K^2 = -\alpha\pi$. Conjugating with J defines an inner automorphism of $D(X)$ which restricted to $k(I) = k(\sqrt{\alpha}) \subset D(X)$ is σ. Let $P(X) \in k(\sqrt{\alpha})[X]$ be the polynomial defined above. Consider $JP(X) \in D(X)$. Then $(JP(X))^2 = JP(X)JP(X) = JJJ^{-1}P(X)JP(X) = J^2 P(X)^{\sigma} P(X) = \pi f(X)$. So $\pi f(X)$ is a square in $D(X)$, i.e., we have an embedding $k(X)(\sqrt{\pi f(X)}) \subset D(X)$. Since $D(X)$ is a quaternion division algebra over $k(X)$, i.e., a central simple algebra of index 2 over $k(X)$, this is equivalent with the fact that $k(X)(\sqrt{\pi f(X)})$ is a splitting field for $D(X)$. So the algebra $D(X) \otimes_k k(X)(\sqrt{\pi f(X)}) \cong D(X) \otimes_k k(C)$ is a full matrix algebra over $k(C)$ (cf. [2, Theorem 1.6.17]). It follows from the theorem of Roquette and Lichtenbaum (cf. [6]) that $I(C) = 2$.

The proof of case (ii) is obtained in completely the same way. One considers the inner automorphism $K(-)K^{-1}$. ∎

Corollary 2. *Let $f(X)$ be a monic irreducible polynomial over O_k. Let $L \cong k[T]/(f(T))$. Let C be the smooth projective geometrically connected curve defined by the equation $Y^2 = \pi f(X)$. Then the index $I(C) = 2$ in the following cases:*

i) *The maximal unramified extension un of k in L is of even degree.*

ii) $k(\sqrt{-\alpha\pi}) \subset L$.

Proof. (ii) is immediate from the proposition.

(i) If $[L_{un} : k] \in 2\mathbb{Z}$ then since L_{un}/k is a cyclic Galois extension it contains $k(\sqrt{\alpha})$ as unique quadratic subextension. Now one can apply the theorem again. ∎

Corollary 3. *Let k be a dyadic field and $f(X)$ a monic irreducible polynomial over k defining a tamely ramified extension $L = k[T]/(f(T))$ over k. Let C be the smooth projective geometrically connected curve defined by the equation $Y^2 = \pi f(X)$. Then $I(C) = 1$ if and only if $[L : k]$ is odd.*

Proof. Since L/k is tamely ramified, the degree $[L : L_{un}]$ is odd. So either $[L_{un} : k]$ is odd, i.e., $f(X)$ is a polynomial of odd degree and then it has a zero in some odd degree extension of k. This immediately implies that $I(C) = 1$. Or $[L_{un} : k]$ is even in which case the previous corollary implies that $I(C) = 2$. ∎

3 The main result

From now on $f(X)$ will be a monic irreducible polynomial over O_k, defining a tamely ramified extension $L \cong k[T]/(f(T))$ of k and C will be the smooth projective geometrically connected curve over k defined by the equation $Y^2 = \pi f(X)$. From the above it follows that the only case where we do not yet have an answer for the index problem is the case in which neither $k(\sqrt{\alpha}) \subset L$ nor $k(\sqrt{-\alpha\pi}) \subset L$. In [7] we showed that in this case the determination of the index is more subtle. Namely we showed that in the case where the ramification index of L/k is a power of 2, the index of C not only depends on L but also on a π_L-adic expansion of a root θ of $f(X)$. This result can be generalized to tamely ramified extensions in general. We fix our notation first (compare with [7, 2.3]).

Notations 4.

- $f(X)$ is a monic irreducible polynomial over O_k of even degree, θ is a root of $f(X)$ in a fixed algebraic closure $\overline{k}$ of k.
- $L = k(\theta)$ is a tamely ramified extension with ramification index $e(L/k) = 2^m d$, d odd, $m \geq 1$
- L_{un} is the maximal unramified sub-extension of L/k and E/k the maximal unramified sub-extension of odd degree. We have $[L : k] = 2^\mu \delta$, $[L : L_{un}] = 2^m d$ and $[E : k] = \frac{\delta}{d}$.

  (In the remaining cases we are considering in this note, we always have $L_{un} = E$.)
- $\overline{\Omega}$ is the set of Teichmüller representatives in the maximal unramified extension $k^{un} \subset \overline{k}$ of k. Ω is the set of Teichmüller representatives in L_{un}, i.e., $\Omega = \overline{\Omega} \cap L_{un}$.
- α is a unit representing a non square in k. We choose $\alpha \in \Omega$ (cf. [7, page 320]).
- We choose a uniformizing element $\pi_L \in L$ such that $\pi_L^{2^m d} = u\pi$, $u \in \Omega$. This is possible since L/L_{un} is totally and tamely ramified, cf. [4]. It follows that $N^L_{L_{un}}(\pi_L) = -u\pi$ (a minus sign since the ramification index $e(L/k)$ is even). We denote the element $\pi_L^{2^m} \in L$ by $\sqrt[d]{u\pi}$.

- Let $\theta = a_0 + a_1\pi_L + a_2\pi_L^2 + \cdots$ be the π_L-adic expansion of θ, where the coefficients a_i are taken in Ω (cf. [7, 2.3]). Define $s = \min\{i | a_i\pi_L^i \notin E(\sqrt[d]{u\pi})\}$, $\theta_0 = \sum_{i=0}^{s-1} a_i\pi_L^i$ and $\theta_1 = \theta - \theta_0$.

  Note first that in the case $d = 1$ the definition of θ_0 and θ_1 is exactly the same as in [7]. Secondly if $[L_{un} : k]$ is odd then $L_{un} = E$ and so $u \in E$, this implies that $s = \min\{i | a_i \neq 0 \text{ and } i \notin 2^m\mathbb{Z}\}$.

Proposition 5. *Suppose the notations are as fixed above. Assume that $\sqrt{\alpha} \notin L$ and $\sqrt{-\alpha\pi} \notin L$ then $I(C) = 2$ if and only if $v_L(\theta - \theta_0) \in 2\mathbb{Z}$.*

Proof. Since L is tamely ramified and its ramification index is even the local field k is non-dyadic.

I. We assume that $v_L(\theta - \theta_0) \in 2\mathbb{Z}$ and we will show that $I(C) = 2$.

a)Assume some $\sqrt[d]{u} \in L_{un}$. This implies that $\sqrt[d]{\pi} := \frac{\pi_L^{2^m}}{\sqrt[d]{u}} \in L$.

Since L_{un} and $k(\sqrt[d]{\pi})$ are linearly disjoint over k we have $[L_{un}(\sqrt[d]{\pi}) : L_{un}] = d$ and $L_{un}(\sqrt[d]{\pi})$ is the maximal unramified extension in $L/k(\sqrt[d]{\pi})$.

Let $M = k(\zeta_d)(\sqrt[d]{\pi})$, ζ_d a primitive d-th root of unity.

Claim: For all odd degree extensions l/M and all $x \in l$, $\pi f(x)$ has odd valuation in l.

To proof the claim we consider the equation $Y^2 = \pi g^{\tau_1} g^{\tau_2} \cdots g^{\tau_r} = \pi g g^{\tau_2} \cdots g^{\tau_r}$, where $\mathrm{Gal}(M/k) = \{\tau_1 = id, \tau_2, \ldots, \tau_r\}$, and g is the minimal polynomial of θ over M. We want to apply the results of [7] to the extension $(L(\zeta_d) =)LM/M$ and its conjugates $(LM)^{\tau_i}$ (where the automorphism τ_i is extended to a k-embedding of $LM \hookrightarrow \overline{k}$). So let us first collect the properties of these extensions.

- Since L/k is tamely ramified, p does not divide d which implies that $k(\zeta_d)^{\tau_i}/k$ is an unramified Galois extension. The ramification index of $(LM)_i^{\tau}/M$ equals the ramification index of $L/L_{un}(\sqrt[d]{\pi})$ so it is equal to 2^m, $m \geq 1$.

- $(LM)^{\tau_i} = M(\theta^{\tau_i})$ and θ^{τ_i} is a root of the irreducible polynomial $g^{\tau_i}(X)$ over M, a polynomial of even degree (since $m \neq 1$).

- $(\pi_L)^{\tau_i}$ is a uniformising element in $(LM)^{\tau_i}$ and $(\pi_L^{\tau_i})^{2^m} = (\sqrt[d]{u\pi})^{\tau_i}$, $(\sqrt[d]{u})^{\tau_i} \in \Omega$ (remember that we are assuming $\sqrt[d]{u} \in L_{un}$) and $N_{(LM)_{un}}^{(LM)^{\tau_i}}(\pi_L^{\tau_i}) = -(\sqrt[d]{u\pi})^{\tau_i}$.

- $\theta^{\tau_i} = a_0^{\tau_i} + a_1^{\tau_i}\pi_L^{\tau_i} + a_2^{\tau_i}(\pi_L^{\tau_i})^2 + \cdots$ are the π_L-adic expansion of the θ_i^{τ}'s, with the coefficients $(a_i)^{\tau_i}$ in Ω.
  Also $s = \min\{j | a_j\pi_L^j \notin E(\sqrt[d]{u\pi})\} = \min\{j | a_j \neq 0 \text{ and } j \notin 2^m\mathbb{Z}\} = \min\{j | a_j^{\tau_i} \neq 0 \text{ and } j \notin 2^m\mathbb{Z}\}$. It follows that s is the same for all θ^{τ_i} and that $(\theta_0)^{\tau_i} = (\theta^{\tau_i})_0$ and $(\theta_1)^{\tau_i} = (\theta^{\tau_i})_1$.
  The assumption $v_L(\theta_1) \in 2\mathbb{Z}$ then implies $v_{(LM)^{\tau_i}}(\theta_1^{\tau_i}) \in 2\mathbb{Z}$ for all $i = 1, \ldots, r$.

Let now l/M be an extension of odd degree and $x \in l$ then [7, lemma 2.5 (ii)] (see also the proof of proposition 3.9 in [7]) applied to the polynomials g^{τ_i}, which are irreducible over M, yields that $g^{\tau_i}(x) \equiv 1 \bmod l^{*2}$. Now π has odd valuation in M since d is odd and $k(\zeta_d)/k$ is unramified (as we remarked above). So the valuation of π in l is odd. It follows that for all odd degree extensions l/M and all $x \in l$,

$\pi g(x)g^{\tau_2}(x)\cdots g^{\tau_r}(x)$ has odd valuation in l, therefore it cannot be a square in l. This proves our claim.

Consequently the curve defined by the affine equation $y^2 = \pi f(X)$ has no rational point in any odd degree extension of M, so $I(C_M) = 2$. Therefore also $I(C) = 2$ for otherwise there is an extension l/k of odd degree such that $C(l) \neq \emptyset$. But lM/M is also of odd degree since M/k is a Galois extension (cf. [3]), so $C_M(lM) \neq \emptyset$ implying $I(C_M) = 1$, a contradiction.

b) To apply part a) we consider the unramified extension of odd degree $L_{un}(\sqrt[d]{u})/k$. We know (lemma 2.1 in [7]) that $I(C) = I(C_{L_{un}(\sqrt[d]{u})})$. Let $f(X) = p(X)p^{\gamma_2}(X)\cdots p^{\gamma_t}(X)$ be the factorization of $f(X)$ over $L_{un}(\sqrt[d]{u})$, $\{id = \gamma_1, \gamma_2, \dots, \gamma_t\}$ being the Galois group of $L_{un}(\sqrt[d]{u})/k$. We can apply the results of part (a) to the polynomials $p^{\gamma_i}(X)$. Note that θ^{γ_i} is a root of $p^{\gamma_i}(X)$ and that we have (similar to observations in part a) $\theta_0^{\gamma_i} = (\theta_0)^{\gamma_i}$ and $\theta_1^{\gamma_i} = (\theta_1)^{\gamma_i}$. Also $v_L(\theta - \theta_0) \in 2\mathbb{Z}$ is equivalent with $v_{L(\sqrt[d]{u})^{\gamma_i}}(\theta^{\gamma_i} - \theta_0^{\gamma_i}) \in 2\mathbb{Z}$ for all γ_i.
So if $v_L(\theta - \theta_0) \in 2\mathbb{Z}$ the claim proven in part (a) implies that for all $l/L_{un}(\sqrt[d]{u})(\sqrt[d]{\pi})$ of odd degree, for all $x \in l$ and for all $i = 1, \dots, t$ the valuation of $\pi g^{\gamma_i}(x)$ as an element of lM, with $M = L_{un}(\sqrt[d]{u}, \zeta_d, \sqrt[d]{\pi})$, is odd. Then these elements also have odd valuation as elements of l (Ml/l being unramified). Since t is odd it follows that the valuation of $\pi f(x)$ as an element of l is odd. This implies that $I(C_{L_{un}(\sqrt[d]{u})}) = I(C) = 2$.

Consequently we have shown that if $v_L(\theta - \theta_0) \in 2\mathbb{Z}$ then $I(C) = 2$.

II) Let us now assume that $v_L(\theta_1) \notin 2\mathbb{Z}$. We want to prove that $I(C) = 1$.

We claim that given the hypotheses $\sqrt{\alpha} \notin L$, $\sqrt{-\alpha\pi} \notin L$ and $v_L(\theta_1) \notin 2\mathbb{Z}$, $\pi f(\theta_0)$ is a square in $L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})$. If this is true then the curve C has a rational point over the odd degree extension $L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})$, so $I(C) = 1$.

The calculation of the square class of $\pi f(\theta_0)$ is implicitly in lemma 2.5 of [7]. For the sake of completeness we give it here explicitly for this special case.

$L_{un}(\sqrt[d]{u})/k$ is a Galois extension so $f(X) = \prod_{\sigma \in \mathrm{Gal}(L_{un}(\sqrt[d]{u})/k)} g^\sigma(X)$, with $g(X)$ the minimal polynomial of θ over $L_{un}(\sqrt[d]{u})$, it is a polynomial of even degree since $[L_{un}(\sqrt[d]{u}) : k]$ is odd. $L_{un}(\sqrt[d]{u})$ is an unramified extension over L_{un}, it follows that L/L_{un} is linearly disjoint from $L_{un}(\sqrt[d]{u})$, so we can extend the σ's to embeddings of $L(\sqrt[d]{u})$ leaving the uniformising element π_L invariant.

We can now determine the square class of $g^\sigma(\theta_0)$ (we abreviate in the calculations $N^{L(\sqrt[d]{u})}_{L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})}$ simply with N):

$$\begin{aligned} g^\sigma(\theta_0) &= N(\theta_0 - \theta^\sigma) \\ &= N(\theta_0 - \theta_0^\sigma - \theta_1^\sigma) \end{aligned}$$

If $v_{L(\sqrt[d]{u})}(\theta_0 - \theta_0^\sigma) < v_{L(\sqrt[d]{u})}(\theta_1^\sigma)$ then $\theta_0 - \theta_0^\sigma - \theta_1^\sigma = (\theta_0 - \theta_0^\sigma)(1 + z)$ with $z \in \pi_L O_L$. The one-unit $1 + z$ is a square in $L(\sqrt[d]{u})$, this yields:

$$\begin{aligned} g^\sigma(\theta_0) &= N((\theta_0 - \theta_0^\sigma)(1 + z)) \\ &\equiv N(\theta_0 - \theta_0^\sigma) \bmod L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi}) \\ &\equiv (\theta_0 - \theta_0^\sigma)^{[L(\sqrt[d]{u}):L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})]} \bmod L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})^{*2} \\ &\equiv (\theta_0 - \theta_0^\sigma)^{2m} \bmod L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})^{*2} \\ &\equiv 1 \bmod L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})^{*2} \end{aligned}$$

Here we used the fact that $L_{un}(\sqrt[d]{u})$ is an unramified extension (k being non-dyadic), this implies that $L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})$ is the maximal unramified extension in $L(\sqrt[d]{u}, \sqrt[d]{\pi})$ and that the ramification index of $L(\sqrt[d]{u}, \sqrt[d]{\pi})/k$ is equal to $e(L/k) = 2^m$, yielding $[L(\sqrt[d]{u}) : L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})] = 2^m \in 2\mathbb{Z}$.

If $v_{L(\sqrt[d]{u})}(\theta_0 - \theta_0^\sigma) \geq v_{L(\sqrt[d]{u})}(\theta_1^\sigma)$ then necessarily $\theta_0 = \theta_0^\sigma$. To see this note that $\theta_0 = \sum_{i=0}^{s-1} a_i \pi_L^i$ and $\theta_0^\sigma = \sum_{i=0}^{s-1} a_i^\sigma (\pi_L^\sigma)^i = \sum_{i=0}^{s-1} a_i^\sigma \pi_L^i$. If $\theta_0 \neq \theta_0^\sigma$ then $a_i \neq a_i^\sigma$ for some $i = 1, \ldots, s-1$. But then $v(\theta_0 - \theta_0^\sigma) \leq i \leq v(\theta_1^\sigma)$.

So in the case $v_{L(\sqrt[d]{u})}(\theta_0 - \theta_0^\sigma) \geq v_{L(\sqrt[d]{u})}(\theta_1^\sigma)$ we have (again we denote $N^{L(\sqrt[d]{u})}_{L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})}$ simply with N)

$$\begin{aligned} g^\sigma(\theta_0) &= N(\theta_1^\sigma) \\ &\equiv N(a_s \pi_L)^s \bmod L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})^{*2} \\ &\equiv N(a_s)N(\pi_L) \bmod L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})^{*2} \\ &\equiv -u^\sigma \pi \bmod L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})^{*2} \end{aligned}$$

Here we used that $N^{L(\sqrt[d]{u})}_{L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})}(a_s)$ is a square since $a_s \in L_{un}$ and $[L(\sqrt[d]{u}) : L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})] = 2^m$ is even. We used also our hypothesis that $v_L(\theta_1) = s$ is odd.

Now if, still under the assumption that $v_{L(\sqrt[d]{u})}(\theta_0 - \theta_0^\sigma) \geq v_{L(\sqrt[d]{u})}(\theta_1^\sigma)$, $\pi g^\sigma(\theta_0)$ is not a square in $L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})$, then necessarily, since α represents the non-squares in the odd degree extension $L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})$ of k, $-u^\sigma \equiv \alpha^\sigma (= \alpha)$ or equivalently $-u \equiv \alpha$. This would imply $\sqrt{-\alpha\pi} = \sqrt{u\pi} \in L$ contrary to our assumptions.

So recapitulating what we found, for all $\sigma \in \mathrm{Gal}(L_{un}(\sqrt[d]{u})/k)$ with $\theta_0^\sigma \neq \theta_0$ we have that $g^\sigma(\theta_0)$ is a square in $L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})$. For all σ's with $\theta_0^\sigma = \theta_0$, i.e., for all σ's in $H := \mathrm{Gal}(L_{un}(\sqrt[d]{u})/k(a_0, \ldots, a_{s-1})$, we have that $\pi g^\sigma(\theta_0)$ is a square in $L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})$. Note that there is an odd number $t = \#\mathrm{Gal}(L_{un}(\sqrt[d]{u})/k(a_0, \ldots, a_{s-1}))$ of σ's satisfying the latter property. We obtain

$$\begin{aligned} \pi f(\theta_0) &\equiv \left(\prod_{\sigma \in H} \pi g^\sigma(\theta_0)\right) \left(\prod_{\tau \notin H} g^\tau(\theta_0)\right) \bmod L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})^{*2} \\ &\equiv 1 \bmod L_{un}(\sqrt[d]{u}, \sqrt[d]{\pi})^{*2} \end{aligned}$$

This proves our claim and so we obtain $I(C) = 1$ as desired. ∎

Corollary 2, corollary 3 and proposition 5 together cover the calculation of the index for a curve C defined by $Y^2 = \pi f(X)$, with $f(X)$ an irreducible monic polynomial over O_k such that a root of $f(X)$ generates a tamely ramified extension of k. We summarize the result in the following theorem.

Theorem 6. *Let $f(X) \in O_k[X]$ be a monic irreducible polynomial of degree $2^\mu \delta$. Let $L = k(\theta)$, with θ a root of $f(X)$. Let the ramification index $e(L/k) = 2^m d$, be prime to the characteristic of k, i.e., L/k is tamely ramified. Let C be the hyperelliptic curve defined by the affine equation $Y^2 = \pi f(X)$. Then*

1) *If k is dyadic then $I(C) = 1$ if and only if $\mu = 0$, i.e., $[L : k]$ is odd.*

2) *If k is non-dyadic then $I(C) = 2$ if and only if $\mu \geq 1$ ($f(X)$ is of even degree) and one of the following conditions hold: $k(\sqrt{\alpha}) \subset L$, or $k(\sqrt{-\alpha\pi}) \subset L$ or $v_L(\theta - \theta_0) \in 2\mathbb{Z}$ (where θ_0 is defined as in 4.)*

Remark 7. 1. It is not difficult to obtain from theorem 6 examples of equations $Y^2 = \pi f(X)$ for which the associated curves are of index 2 as well as examples of such equations for which the curves have index 1. The idea is to look for an integral primitive element θ in some tamely ramified extension of k of even degree having the π_L-adic expansion with the desired properties. Then one takes $f(X)$ as the minimal polynomial of θ. One can start even with a uniformizing element π_L and look at $a_s\pi_L^s$ for suitable s and a_s.

2. For hyperelliptic curves defined by an equation of the form $Y^2 = \pi f(X)$ our main result followed (at least partially) from the result we obtained in [7] (the case where the ramification index $e(L/k)$ is a power of 2). The reduction does not immediately work for curves defined by equations $Y^2 = \alpha f(X)$ for different reasons. First of all by going over to extensions $k(\zeta_d)$, ζ_d a d-root of unity, α becomes a square. This already complicates things. But more seriously since cases where $L_{un} \neq E$ have to be considered, the definition of θ_0 and θ_1 does not behave well under galois congugation, this is bad since the fact (cf. page 349) that s is the same for the different θ^{τ_i} plays an essential role in the proof.

References

[1] Colliot-Thélène, J.-L., Poonen, B., *Algebraic families of nonzero elements of Shafarevich-Tate groups,* J. Amer. Math. Soc. **13** nr. 1, 83-99, (2000).

[2] Jacobson, N., *Finite-Dimensional Division Algebras over Fields,* Heidelberg, Springer-Verlag, 1996.

[3] Lang, S., *Algebra,* Third edition, London, Addison Wesley, 1993.

[4] Lang, S., *Algebraic number theory,* London, Addison Wesley, 1970.

[5] Poonen, B., Stoll, M., *The Cassels-Tate pairing on polarized Abelian varieties,* Ann. of Math., **150**, 1109-1149, (1999).

[6] Lichtenbaum, S., *Duality theorems for curves over p-adic fields,* Invent. Math. **7**, 120-136, (1969).

[7] Van Geel, J., Yanchevskii, V.I., *Indices of hyperelliptic curves over p-adic fields,* Manuscripta math. **96**, 317-333, (1998).

[8] Van Geel, J., Yanchevskii, V.I., *Indices of double coverings of genus 1 over p-adic fields,* An. de la Fac. de Toulouse, Vol. VIII, nr. 1, 155-172, (1999)

Ghent University,
Department of Pure Mathematics and Computer Algebra,
Galglaan 2,
B-9000 Gent, Belgium.
email: jvg@cage.rug.ac.be

Institute of Mathematics,
Academy of Science of Belarus,
Surganov str. 11,
220072 Minsk, Belarus.
email: yanch@im.bas-net.by