ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

JAN VAN GEEL
VYACHESLAV YANCHEVSKII

Indices of double coverings of genus 1 over p-adic fields

Annales de la faculté des sciences de Toulouse 6^e *série*, tome 8, n° 1 (1999), p. 155-172

<http://www.numdam.org/item?id=AFST_1999_6_8_1_155_0>

Annales de la Faculté des Sciences de Toulouse Vol. VIII, n° 1, 1999

Indices of double coverings of genus 1 over p-adic fields (*)

JAN VAN GEEL(1) and VYACHESLAV YANCHEVSKII(2)

RÉSUMÉ. — Soit k est un corps p-adique, avec corps résiduel de caractéristique impair, O_k l'anneau de valuation discrète dans k. Soit C une courbe de genre un, donnée par une équation affine $Y^2 = h(X)$. Nous étudions l'indice de C dans le cas $h(X) = \varepsilon f(X)$, avec ε une unité ou un élément uniformisant dans O_k et $f(X)$ le produit de deux polynômes irréductibles de degré 2 dans $O_k[X]$. Le théorème 4.1 résume les résultats.

ABSTRACT. — Let k be a p-adic field of odd residue characteristic and let C be a curve of genus one defined by the affine equation $Y^2 = h(X)$. We discuss the index of C if $h(X) = \varepsilon f(X)$, where ε is either a non-square unit or a uniformising element in O_k and $f(X)$ is the product of two monic irreducible polynomials of degree 2 over O_k. Theoreme 4.1 summarizes our results.

1. Introduction

Let k be a local non-dyadic field of characteristic zero, O_k the valuation ring in k and $v = v_k$ the associated value function. In [5] the authors investigated equations of the form

$$Y^2 = h(X)$$

with $h(X) = \sum_{i=0}^{n} h_i X^i$ a polynomial without multiple roots over such a field k. It is well known that such equations define an affine plane curve C_h^{aff}

(*) Reçu le 3 novembre 1997, accepté le 10 novembre 1998

(1) University of Gent, Department of Pure Mathematics and Computer Algebra, Galglaan 2, B-9000 Gent (Belgium)
E-mail: jvg@cage.rug.ac.be

(2) Institute of Mathematics, National Academy of Science of Belarus, Surganovstr. 11, Minsk 22072 (Belarus)
E-mail: yanch@im.bas-net.by

which is isomorphic with the affine part of a smooth geometrically connected projective curve C_h over k (*cf.* [6]). Let $\deg h = n$. If n is odd C_h has one point at infinity P_∞ defined over k and the genus is $g(C_h) = (n-1)/2$. If n is even then there are two points at infinity P_{∞_1} and P_{∞_2} both defined over the quadratic extension $k(\sqrt{h_n})$ of k, in this case the genus is $g(C_h) = (n-2)/2$. So C_h defines an elliptic curve over k^a (the algebraic closure of k) if and only if $n = 3$ or $n = 4$.

The index of C_h, $I(C_h)$, is by definition the greatest common divisor of the degrees of all k-rational divisors on C_h. Let π be a uniformising element in k and $\alpha \in O_k^*$ a unit which is not a square in k, then the square classes of k are represented by $\{1, \alpha, \pi, \alpha\pi\}$. The index is an invariant of the isomorphism class of the curve, so we may assume that $h(X) = \varepsilon f(X)$ with $f(X) \in O_k[X]$ a monic polynomial and $\varepsilon \in \{1, \alpha, \pi, \alpha\pi\}$. Since $Y^2 = \varepsilon f(X)$ has always a rational point in some quadratic extension of k, the index of $C_{\varepsilon f}$ is either 1 or 2. Moreover the index is 1 if and only if $C_{\varepsilon f}$ has a rational point over some odd degree extension of k. It follows that if $f(X)$ contains a factor of odd degree then $I(C_{\varepsilon f}) = 1$. The same is true if $\varepsilon = 1$, in that case the curve has one or two rational points at infinity. So we may assume that $\varepsilon \in \{\alpha, \pi\}$ (the choice of the uniformising parameter being arbitrary). In [5], the index of $C_{\varepsilon f}$ is determined in terms of invariants of the polynomial f, for all irreducible polynomials f of 2-primary degree. So if we restrict to the class of curves $C_{\varepsilon f}$ that define elliptic curves over k^a, i.e., curves of genus 1, then the index has been determined in all cases except when

$$f(X) = (X^2 + b_1X + b_0)(X^2 + c_1X + c_0)$$

with $X^2 + b_1X + b_0$ and $X^2 + c_1X + c_0$ irreducible quadratic polynomials over O_k.

In this paper we calculate the index $I(C_{\varepsilon f})$ for such polynomials f, thereby completing the results of [5] for all curves $C_{\varepsilon f}$ of genus 1. It follows from the Riemann–Roch theorem that in case $g(C_{\varepsilon f}) = 1$ the index $I(C_\varepsilon)$ equals 1 if and only if $C_{\varepsilon f}$ has a k-rational point. However the arguments we will use only simplify slightly if we would use this fact. Therefore we look for rational points in odd degree extensions of k, thereby avoiding the use of Riemann-Roch. Since with f as above and $\varepsilon \in \{\alpha, \pi\}$ the points at infinity of the curve $C_{\varepsilon f}$ are of degree 2, the problem reduces to decide whether or not the equation $Y^2 = \varepsilon f(X)$ has a solution in some odd degree extension of k. This is done by giving a complete analysis in terms of the p-adic values of the coefficients b_0, b_1, c_0, c_1. For the equations $Y^2 = \alpha f(X)$ this is done in Section 1, the equations $Y^2 = \pi f(X)$ are treated in Section 2.

So let

$$f(X) = f_1(X)f_2(X) = (X^2 + b_1X + b_0)(X^2 + c_1X + c_0)\,,$$

with f_1 and f_2 irreducible polynomials over O_k. Since we may change variables over k (the index being an invariant of the isomorphism class of the curve), further taking into account that the choice of the uniformising element is arbitrary and that we can interchange the role of f_1 and f_2, we may assume that the quadratic factors are in one of the following six forms:

$$\begin{aligned}
f_1(X) &= X^2 - \pi'^{2m}a^2\alpha & f_2(X) &= (X - c\pi'^t)^2 - \pi'^{2n}b^2\alpha \\
f_1(X) &= X^2 - \pi'^{2m}a^2\alpha & f_2(X) &= (X - c\pi'^t)^2 - \pi'^{2n+1}b^2\alpha \\
f_1(X) &= X^2 - \pi'^{2m+1}a^2 & f_2(X) &= (X - c\pi'^t)^2 - \pi'^{2n}b^2\alpha \\
f_1(X) &= X^2 - \pi'^{2m+1}a^2 & f_2(X) &= (X - c\pi'^t)^2 - \pi'^{2n+1}b^2\alpha \\
f_1(X) &= X^2 - \pi'^{2m+1}a^2 & f_2(X) &= (X - c\pi'^t)^2 - \pi'^{2n+1}b^2 \\
f_1(X) &= X^2 - \pi'^{2m+1}a^2\alpha & f_2(X) &= (X - c\pi'^t)^2 - \pi'^{2n+1}b^2\alpha
\end{aligned}$$

with a, $b \in O_k^*$, $c \in O_k^* \cup \{0\}$, and where π' is a uniformising element which can be chosen independently from the uniformiser π we fixed before. Note that the last term in the above equations is exactly the discriminant Δ_1 and Δ_2 of f_1 and f_2 respectively.

We will use frequently the following lemma and its corollary.

LEMMA 1.1. — *Let k be a non-dyadic local field and $\beta, \gamma \in O_k^*$. Let φ be the quadratic form*

$$\varphi \cong Z_1^2 + \beta Z_2^2 + \gamma Z_3^2\,,$$

over k. Then for the unramified extension, ℓ over k, of degree 1 or 3, there is an isotropic vector $v \in \ell^3$, i.e.,

$$\varphi(v) = 0\,,$$

with coordinates in O_ℓ^*.

Proof. — The reduction $\overline{\varphi}$ of φ defines a 3-dimensional form over the residue field $\overline{k} = \mathbb{F}_q$. Since $\overline{k}$ is a finite field, $\overline{\varphi}$ is isotropic. If $\#\overline{k} > 3$ let $\overline{\ell} = \overline{k}$, if $\#\overline{k} = 3$ let $\overline{\ell} = \mathbb{F}_{27}$. Then by theorem 8 in [1, p. 394] there is an

isotropic vector $\overline{w}$ with non-zero coordinates, $\overline{w} = (\overline{x}_1, \overline{x}_2, \overline{x}_3)$ and $\overline{x}_i \neq 0$ for $i = 1, 2, 3$. Let $w = (x_1, x_2, x_3)$ be a lift of $\overline{w}$ to the unique unramified extension ℓ/k of degree 1 or 3 over k. Then $\varphi(w) = u\pi_\ell$ with $u \in O_\ell$. So $x_1^2 - u\pi_\ell + x_2^2 + x_3^2 = 0$. But $x_1^2 - u\pi_\ell = x_1'^2$ with $x_1'^2$ a unit since ℓ is non-dyadic. It follows that $v = (x_1', x_2, x_3)$ is an isotropic vector of φ with coordinates in O_ℓ^*. □

COROLLARY 1.2.— *Let k, β and ℓ be as in the lemma. Then the equation*

$$X^2 + \beta \equiv a \bmod \ell^{*2}$$

with $a \in O_k^*$ has a solution $x \in O_\ell^*$.

Proof.— Apply the lemma to the quadratic form $Z_1^2 + \beta Z_2^2 - aZ_3^2$. Let x_1, x_2, x_3 be the isotropic vector with x_1, x_2, $x_3 \in O_\ell^*$. Then $x = x_1/x_2$ is a solution in O_ℓ^* of the given equation. □

2. The equation $Y^2 = \alpha f(X)$

Let k be a non-dyadic p-adic field of characteristic zero. In this section we consider the question whether or not the equation

$$Y^2 = \alpha f(X) = \alpha f_1(X) f_2(X)$$

with $f_1(X)$, $f_2(X)$ monic irreducible polynomials in $O_k[X]$ has a solution in some odd degree extension of k. Since the uniformising element π does not occur explicitly in this equation we may assume, as we remarked in the introduction, that we have one of the following cases:

(1) $f_1(X) = X^2 - \pi^{2m} a^2 \alpha$, $\quad f_2(X) = \left(X - c\pi^t\right)^2 - \pi^{2n} b^2 \alpha$,

(2) $f_1(X) = X^2 - \pi^{2m+1} a^2$, $\quad f_2(X) = \left(X - c\pi^t\right)^2 - \pi^{2n} b^2 \alpha$,

(3) $f_1(X) = X^2 - \pi^{2m+1} a^2$, $\quad f_2(X) = \left(X - c\pi^t\right)^2 - \pi^{2n+1} b^2 \alpha$,

(4) $f_1(X) = X^2 - \pi^{2m+1} a^2$, $\quad f_2(X) = \left(X - c\pi^t\right)^2 - \pi^{2n+1} b^2$.

The cases $\Delta_1 \equiv \alpha \bmod k^{*2}, \Delta_2 \equiv \alpha\pi \bmod k^{*2}$ and $\Delta_1 \equiv \alpha\pi \bmod k^{*2}$, $\Delta_2 \equiv \alpha\pi \bmod k^{*2}$ reduce to case (2) and (4) respectively, replacing the uniformiser π by $\alpha\pi$. In case (4) the splitting fields of f_1 and f_2 are both equal to $k(\sqrt{\pi})$. It follows from proposition 3.5 in [5] that the index of

the curve $C_{\alpha f}$ is 2 in this case. The calculation of the index in the three remaining cases is done in propositions 2.1, 2.2 and 2.3 respectively.

PROPOSITION 2.1.— *Let* $f(X) = f_1(X)f_2(X)$ *with*

$$f_1(X) = X^2 - \pi^{2m}a^2\alpha$$
$$f_2(X) = \left(X - c\pi^t\right)^2 - \pi^{2n}b^2\alpha,$$

where $a, b \in O_k^*$ *and* $c \in O_k^* \cup \{0\}$. *Then*

(i) $I(C_{\alpha f}) = 1$ *if* $m \neq n$ *or* $t < m$ *or* $X^2 - \bar{a}^2\bar{\alpha} \neq \left(X - \overline{c\pi^{t-m}}\right)^2 - \bar{b}^2\bar{\alpha}$ *over* $\bar{k}$;

(ii) $I(C_{\alpha f}) = 2$ *if* $m = n$ *and* $t \geq m$ *and* $X^2 - \bar{a}^2\bar{\alpha} = \left(X - \overline{c\pi^{t-m}}\right)^2 - \bar{b}^2\bar{\alpha}$ *over* $\bar{k}$.

Proof.— Let ℓ/k be any extension of odd degree of k and let $e = e(\ell/k)$ be its ramification index. Let π_ℓ be a uniformising element of ℓ, then $\pi(= \pi_k) = \pi_\ell^e w$ with $w \in O_\ell^*$. Put $x = \pi_\ell^{me}s$, $s \in \ell$. Then

$$f_1(x) = \pi_\ell^{2me}(s^2 - a^2w^{2m}\alpha)$$
$$f_2(x) = \left(\pi_\ell^{me}s - \pi_\ell^{te}w^tc\right)^2 - \pi_\ell^{2ne}w^{2n}b^2\alpha$$
$$= \pi_\ell^{2me}s^2 - 2\pi_\ell^{(m+t)e}sw^tc + \pi_\ell^{2te}w^{2t}c^2 - \pi_\ell^{2ne}w^{2n}b^2\alpha\,.$$

Assume $t < m$. Then one verifies that

$$\begin{cases} f_2(x) \in \ell^{*2} & \text{if } m \leq n \\ f_2(x) \equiv (\pi_\ell^{2te}w^{2t}c^2 - \pi_\ell^{2ne}w^{2n}b^2\alpha) \bmod \pi_\ell^{2te+1}O_\ell & \text{if } m > n. \end{cases}$$

In both cases the square class of $f_2(x)$ does not depend on the choice of $x = \pi_\ell^{me}s$, i.e. does not depend on the choice of $s \in O_\ell^*$.

Applying corollary 1.2 to the equation

$$s^2 - a^2w^{2m}\alpha,$$

we find ℓ unramified of odd degree over k and an element $s \in O_\ell^*$ such that

$$(s^2 - a^2w^{2m}\alpha)f_2(\pi_\ell^{me}s) \equiv \alpha \bmod \ell^{*2} \not\equiv 1 \bmod \ell^{*2}\,.$$

It follows that $\alpha f(x) = \alpha f_1(x) f_2(x) \in \ell^{*2}$ so $Y^2 = \alpha f(X)$ has an ℓ-rational point, i.e.,

$$I(C_{\alpha f}) = 1 .$$

If $t > m$ or $c = 0$ then

$$f_2(x) \equiv \begin{cases} 1 \bmod \ell^{*2} & \text{if } n > m \\ -b^2\alpha \bmod \ell^{*2} & \text{if } m > n \\ s^2 - b^2\alpha \bmod \ell^{*2} & \text{if } m = n. \end{cases}$$

We see that in case $m \neq n$, $f_2(x) \bmod \ell^{*2}$ is independent of the choice of s. The same argument as in the case $t < m$ can be applied to obtain $I(C_{\alpha f}) = 1$.

If $t = m$ then

$$f_2(x) \equiv \begin{cases} \left(s - cw^t\right)^2 - \pi_\ell^{2e(n-m)} b^2\alpha \bmod \ell^{*2} & \text{if } n > m \\ -b^2\alpha \bmod \ell^{*2} & \text{if } m > n \\ \left(s - cw^t\right)^2 - b^2\alpha \bmod \ell^{*2} & \text{if } m = n. \end{cases}$$

In case $m > n$ the square class does not depend on s and as above we conclude that $I(C_{\alpha f}) = 1$. On the other hand, if $m < n$, we take ℓ as in corollary 1.2. Then $\pi_\ell = \pi$, $w = 1$. We choose $s = c + \pi^{n-m} v$ with $v^2 - b^2\alpha \equiv \alpha(c^2 - a^2\alpha) \bmod \ell^{*2}$. It follows that $\alpha f(x) \in \ell^2$, so $I(C_{\alpha f}) = 1$.

We have already proven one part of point (i) of the proposition, namely that $m \neq n$ or $t < m$ implies $I(C_{\alpha f}) = 1$. Now let $m = n$ and $t \geq m$. Put

$$g_1(Z) = Z^2 - a^2\alpha$$

$$g_2(Z) = \begin{cases} Z^2 - b^2\alpha & \text{if } t > m = n \\ \left(Z^2 - cw\right)^2 - b^2\alpha & \text{if } t = m = n. \end{cases}$$

The reductions $\bar{g}_1(Z), \bar{g}_2(Z)$ are irreducible polynomials of degree 2 over $\bar{k}$ since $\bar{\alpha} \notin \bar{k}^2$. If $\bar{g}_1(Z) \neq \bar{g}_2(Z)$ then $\bar{g}_1(Z)\bar{g}_2(Z)$ has no multiple roots. Using Weil's bound on the number of points on a smooth curve over a finite field one finds that for an odd degree extension $\bar{\ell}/\bar{k}$ of sufficiently large degree there exists an element $\bar{x} \in \bar{\ell}$ such that $\bar{\alpha}\bar{g}_1(\bar{x})\bar{g}_2(\bar{x}) \in \bar{\ell}^{*2}$. A lift of $\bar{x}$ to an element of O_ℓ^*, with ℓ the unramified extension with residue field $\bar{\ell}$, then satifies $\alpha g_1(x) g_2(x) \in \ell^{*2}$. (In proposition 3.1 of [5] the argument

is worked out in detail.) It follows that $\alpha f(x) = \alpha\pi^{2m} g_1(x) g_2(x) \in \ell^2$ and therefore

$$I(C_{\alpha f}) = 1$$

in this case.

Finally let $\bar{g}_1(Z) = \bar{g}_2(Z)$, then $b = \pm a + a'\pi$ and necessarily $t > m$. Let ℓ/k be an odd degree extension and let $x = \pi_\ell^r s$, $s \in O_\ell^*$ be any element in ℓ. Put $\pi_\ell^e w = \pi$, $w \in O_\ell^*$. If $r < 0$ then $\pi_\ell^{-4r} f(x) \in s^4 + \pi_\ell O_\ell \subset \ell^{*2}$. If $r \geq 0$, then

$$f(x) \equiv \begin{cases} a^2 b^2 w^{2m} \pi_\ell^{2me} \alpha^2 \bmod \pi_\ell^{2me+1} O_\ell & \text{if } r > em = en \\ s^4 \pi_\ell^{4r} \bmod \pi_\ell^{4r+1} O_\ell & \text{if } r < em = en. \end{cases}$$

So it remains to consider $x = \pi_\ell^{me} s$, $s \in O_\ell^*$. But now $b \in \pm a + \pi O_k$, this implies

$$f(X) = f_1(X) f_2(X) = \left(X^2 - \pi^{2m} a^2 \alpha\right)^2 + (X^2 - \pi^{2m} a^2 \alpha) \pi^{wm} O_k[X].$$

And since $s^2 - a^2\alpha$ is a unit (otherwise the equation $Z^2 - a^2\alpha^2$ would have a solution in an odd degree extension of k, which is impossible since α is not a square in k), it follows that

$$f(x) \equiv \pi_\ell^{4me} \left(s^2 - a^2\alpha\right)^2 \bmod \pi_\ell^{4me+1} O_\ell,$$

is a non-zero square in ℓ. We obtained that for every odd degree extension ℓ/k and any $x \in \ell$, $\alpha f(x) \notin \ell^{*2}$, so

$$I(C_{\alpha f}) = 2$$

in this case. □

PROPOSITION 2.2.— *Let* $f(X) = f_1(X) f_2(X)$ *with*

$$f_1(X) = X^2 - \pi^{2m+1} a^2$$
$$f_2(X) = \left(X - c\pi^t\right)^2 - \pi^{2n} b^2 \alpha,$$

where $a, b \in O_k^*$ *and* $c \in O_k^* \cup \{0\}$. *Then*

(i) $I(C_{\alpha f}) = 1$ *if* $t \leq \min(m, n)$ *or* $n \leq m$;
(ii) $I(C_{\alpha f}) = 2$ *if* $t > \min(m, n) = m$.

Proof. — Assume $t \leq \min(m, n)$. Let ℓ/k be the unramified extension of odd degree determined in corollary 1.2. The uniformising element π in k is also a uniformising element for ℓ. Take $x = \pi^t s$, $s \in O_\ell^*$. Then since $t \leq m$,

$$v_\ell(x^2 - \pi^{2m+1}a^2) = 2v_\ell(x) \in 2\mathbb{Z}\,.$$

It follows that

$$\pi^{2t}s^2 - \pi^{2m+1}a^2 \in \ell^{*2}$$

for all $s \in O_\ell^*$. Choose $s \in O_\ell^*$ such that $s = c + \pi^{n-t}s'$, this is possible since $t \leq n$, with $s' \in O_\ell^*$ such that (apply corollary 1.2),

$$s'^2 - b^2\alpha \notin \ell^{*2}\,.$$

So

$$f_2(x) = \pi^{2n}(s'^2 - b^2\alpha) \equiv \alpha \bmod \ell^{*2}$$

and

$$f(x) = f_1(x)f_2(x) \equiv \alpha \bmod \ell^{*2}\,.$$

Therefore

$$I(C_{\alpha f}) = 1\,.$$

Next assume $t > \min(m, n) = n \leq m$. Let ℓ be as before and take $x = \pi^n s$. Then

$$f_1(x) = \pi^{2n}s^2 - \pi^{2m+1}a^2 \in \pi^{2n}s^2 + \pi^{2n+1}O_\ell$$
$$f_2(x) = \left(\pi^n s - c\pi^t\right)^2 - \pi^{2n}b^2\alpha \in \pi^{2n}(s^2 - b^2\alpha) + \pi^{2n+1}O_\ell\,.$$

Take ℓ as in corollary 1.2 and s such that $s^2 - b^2\alpha \notin \ell^{*2}$, then

$$f(x) \equiv \alpha \bmod \ell^{*2}\,.$$

Again we see that $I(C_{\alpha f}) = 1$.

This proves part (i). Assume $t > \min(m, n) = m < n$. Now let ℓ be any odd degree extension of k and $e = e(\ell/k)$ its ramification index. Let π_ℓ be a uniformising element in ℓ and, say, $\pi_\ell^e w = \pi$. Suppose $x = \pi_\ell^r s \in \ell$.

If $n > t > m$ then for $v_\ell(x) \neq v_\ell(c\pi^t) = et$,

$$f_2(x) \in \left(x - c\pi_\ell^{te}w^t\right)^2 + \pi_\ell^{2v_\ell(x - c\pi_\ell^t w^t)+1}O_\ell\,.$$

But then

$$f(x) \in \begin{cases} \left(x - c\pi_\ell^t w^t\right)^2 x^2 + \pi^{v_\ell((x-c\pi_\ell^t w^t)^2 x^2)+1} O_\ell \\ \qquad\qquad\qquad\qquad \text{if } v_\ell(x) \le m \\ \left(x - c\pi_\ell^t w^t\right)^2 (-\pi^{2m+1} a^2) + \pi^{v_\ell((x-c\pi_\ell^t w^t)^2 + 2m+1} O_\ell \\ \qquad\qquad\qquad\qquad \text{if } v_\ell(x) > m. \end{cases}$$

Both possibilities imply $\alpha f(x) \notin \ell^2$.

If $r = v_\ell(x) = v_\ell(c\pi^t = et)$ then

$$f_1(x) \in -\pi^{2m+1} a^2 + \pi^{2m+2} O_\ell \,.$$

We claim that the valuation of $f_2(x)$ is even. If so, $v_\ell\big(f(x)\big) = v_\ell\big(\alpha f(x)\big)$ is odd, implying $\alpha f(x) \notin \ell^2$. To see that the claim is true, note that $v_\ell\big(f_2(x)\big)$ is even if

$$2v_\ell(x - c\pi_\ell^{te} w^t) \neq 2ne \,.$$

If $2v_\ell(x - c\pi_\ell^{te} w^t) = 2ne$ then $x = c\pi^{te} w^t + u\pi_\ell^{ne}$, with $u \in O_\ell^*$. From this we obtain

$$f_2(x) = u^2 \pi_\ell^{2ne} - \alpha b^2 \pi_\ell^{2ne} = \pi_\ell^{2ne}(u^2 - \alpha b^2) \,.$$

But $u^2 - \alpha b^2$ is a unit ($\bar{\alpha}$ is not a square in $\bar{\ell}$), so $v_\ell\big(f_2(x)\big) = 2ne$, thereby proving the claim.

Finally assume $t \ge n > m$. If $r \le m$ then

$$f(x) \in \pi_\ell^{4r} s^4 + \pi_\ell^{4r+1} O_\ell$$

and so $\alpha f(x) \notin \ell^2$.

For $r > m$ we have $v_\ell\big(f_1(x)\big)$ is odd. In order that x is the X-coordinate of a rational point in $C_{\alpha f}(\ell)$, we need to have that $v_\ell\big(f_2(x)\big)$ is odd too. This can only happen if $2v_\ell(\pi_\ell^r s - c\pi_\ell^{te} w^t) = 2ne$, so $\pi_\ell^r s - c\pi_\ell^{te} w^t = \pi_\ell^{ne} v$ with $v \in O_\ell^*$. But then

$$f_2(x) = \pi_\ell^{2ne}(v^2 - b^2\alpha) \,,$$

which has even valuation since $v^2 - b^2\alpha$ is a unit ($\bar{\alpha}$ being a non-square in $\bar{\ell}$). We have shown that if $v(c) > \min(m, n) = m \le n$, $\alpha f(x) \notin \ell^2$ for any ℓ over k of odd degree and all $x \in \ell$. So $I(C_{\alpha f}) = 2$ in this case. □

PROPOSITION 2.3.— *Let* $f(X) = f_1(X)f_2(X)$ *with*

$$f_1(X) = X^2 - \pi^{2m+1}a^2$$
$$f_2(X) = \left(X - c\pi^t\right)^2 - \pi^{2n+1}b^2\alpha\,,$$

where $a, b \in O_k^*$ *and* $c \in O_k^* \cup \{0\}$. *Then*

(i) $I(C_{\alpha f}) = 1$ *if* $t > \min(m, n)$;
(ii) $I(C_{\alpha f}) = 2$ *if* $t \leq \min(m, n)$.

Proof.— In the case $t > n$,

$$f(0) = \pi^{2m+2n+2}a^2b^2\alpha + \pi^{2n+2m+3}O_k\,,$$

so $\alpha f(0) \in k^2$ and $I(C_{\alpha f}) = 1$.

Put $x = \pi_\ell^r s$, where s is in some extension ℓ/k of odd degree, with $e(\ell/k) = e$, $\pi_\ell^e u = \pi$, $u \in O_\ell^*$. We have the following posibilities for the value of $f(x)$:

$v_\ell(f_1(x))=$	$2me+e$	$2re$	$2me+e$	$2re$
$v_\ell(f_2(x))=$	$2v_\ell(x-c)$	$2v_\ell(x-c)$	$2ne+e$	$2ne+e$

The only case in which x can be the X-coordinate of a point of $C_{\alpha f}$ over ℓ is when $v_\ell(f_1(x)) = 2me + e$ and $v_\ell(f_2(x)) = 2ne + e$, in the other cases $\alpha f(x) \notin \ell^2$. But then $v_\ell(x) > me$ and $v_\ell(x - c\pi_\ell^{te}w^t) > ne$. Since $te \leq ne$ we must have $v_\ell(x) = te > me$. Therefore we obtain already that for $t \leq \min(m, n)$, $I(C_{\alpha f}) = 2$. On the other hand if $m < t \leq n$ (the only case left), we take $x = c\pi^t + \pi^{n+1} \in k$ and we obtain

$$f(x) = \pi^{2m+2n+2}a^2b^2\alpha + \pi^{2m+2n+3}O_k\,,$$

i.e.,

$$I(C_{\alpha f}) = 1\,. \square$$

Remark 2.4.— One can verify directly that in propositions 2.1, 2.2 and 2.3 the conditions for the index to be 1 are complementary to those that imply the index to be 2. (So in these propositions the "if" may be replaced by "if and only if".)

3. The equation $Y^2 = \pi f(X)$

Let k be as before. We now fix a uniformiser π and consider the equation

$$Y^2 = \pi f(X) = \pi f_1(X) f_2(X),$$

with $f_1(X), f_2(X)$ monic irreducible polynomials in $O_k[X]$. As we saw in the introduction we may assume that one of the following six cases occurs (taking $\pi' = -\pi$ and changing the sign of the coefficient c if necessary):

$$\begin{aligned}
f_1(X) &= X^2 - \pi^{2m} a^2 \alpha & f_2(X) &= (X - c\pi^t)^2 - \pi^{2n} b^2 \alpha \\
f_1(X) &= X^2 - \pi^{2m} a^2 \alpha & f_2(X) &= (X - c\pi^t)^2 + \pi^{2n+1} b^2 \alpha \\
f_1(X) &= X^2 + \pi^{2m+1} a^2 & f_2(X) &= (X - c\pi^t)^2 - \pi^{2n} b^2 \alpha \\
f_1(X) &= X^2 + \pi^{2m+1} a^2 & f_2(X) &= (X - c\pi^t)^2 + \pi^{2n+1} b^2 \alpha \\
f_1(X) &= X^2 + \pi^{2m+1} a^2 & f_2(X) &= (X - c\pi^t)^2 + \pi^{2n+1} b^2 \\
f_1(X) &= X^2 + \pi^{2m+1} a^2 \alpha & f_2(X) &= (X - c\pi^t)^2 + \pi^{2n+1} b^2 \alpha .
\end{aligned}$$

(The choice $\pi' = -\pi$ avoids making a distinction between fields k in which -1 is a square and those in which $-1 \equiv \alpha \bmod k^{*2}$.) In the first case the splitting fields of f_1 and f_2 are both equal to $k(\sqrt{\alpha})$ and in the last case they are both equal to $k(\sqrt{-\alpha\pi})$. Proposition 3.8 in [5] then implies that the index of $C_{\pi f}$ is 2 in both these cases. Propositions 3.1, 3.2, 3.4 and 3.6 determine the index in the remaining four cases.

PROPOSITION 3.1.— *Let* $f(X) = f_1(X) f_2(X)$ *with*

$$\begin{aligned}
f_1(X) &= X^2 + \pi^{2n+1} a^2 \\
f_2(X) &= (X - c)^2 + \pi^{2m+1} b^2 ,
\end{aligned}$$

where $a, b \in O_k^*$ *and* $c \in O_k$. *Let* v_k *be the valuation on* k *normalised such that* $v_k(\pi) = 1$. *Then*

(i) $I(C_{\pi f}) = 1$ *if* $m \neq n$ *or* $v_k(c) \leq m$;
(ii) $I(C_{\pi f}) = 2$ *if* $m = n$ *and* $v_k(c) > m$.

Proof.— Let $v_k(c) \leq m$ then

$$f(0) \in \pi^{2n+1} a^2 c^2 + \pi^{2n+2m+2} O_k \in \pi O_k^{*2},$$

so $\pi f(0) \in k^2$ and $I(C_{\pi f}) = 1$.

Secondly, let $v_k(c) > m$ and assume $m \neq n$. Take $x = \pi^t$ with $t = \max\{m, n\}$. Then

$$f(x) = (\pi^t + \pi^{2n+1}a^2)\Big((\pi^t - c)^2 + \pi^{2m+1}b^2\Big)$$
$$\equiv \begin{cases} \pi^{2n+2m+1}b^2 \bmod \pi^{2n+2m+2}O_k & \text{if } m < n \\ \pi^{2n+2m+1}a^2 \bmod \pi^{2n+2m+2}O_k & \text{if } m > n. \end{cases}$$

It follows that $\pi f(x) \in k^2$, so $I(C_{\pi f}) = 1$.

Finally let $v_k(c) > m$ and $m = n$. Let ℓ/k be an extension of odd degree and ramification index $e = e(\ell/k)$. Let π_ℓ a uniformising element in ℓ and v_ℓ the normalised valuation on ℓ. Let $x = \pi_\ell^t s$ with $s \in O_\ell^*$. Then

$$f(x) \equiv \begin{cases} \pi^{2n+2m+2}a^2b^2 \bmod \pi^{2n+2m+3}O_\ell & \text{if } t > me = ne \\ \pi_\ell^{4t} \bmod \pi_\ell^{4t+1}O_\ell & \text{if } t \leq me = ne. \end{cases}$$

It follows that for all odd degree extensions ℓ and for all $x \in \ell$, $\pi f(x) \notin \ell^2$, so $I(C_{\pi f}) = 2$ in this case. □

PROPOSITION 3.2.— *Let* $f(X) = f_1(X)f_2(X)$ *with*

$$f_1(X) = X^2 + \pi^{2n+1}a^2$$
$$f_2(X) = (X - c)^2 - \pi^{2m}\alpha b^2,$$

where $a, b \in O_k^*$ *and* $c \in O_k$. *Let* v_k *be the valuation on* k *normalised such that* $v_k(\pi) = 1$. *Then*

(i) $I(C_{\pi f}) = 1$ *if* $m > n$;
(ii) $I(C_{\pi f}) = 1$ *if* $m \leq n$ *and* $v_k(c) < m$;
(iii) $I(C_{\pi f}) = 1$ *if* $m \leq n$, $v_k(c) \geq m$ *and* $c^2 - \pi^{2m}\alpha b^2 \in k^2$;
(iv) $I(C_{\pi f}) = 2$ *if* $m \leq n$, $v_k(c) \geq m$ *and* $c^2 - \pi^{2m}\alpha b^2 \notin k^2$.

Remark 3.3.— The condition $c^2 - \pi^{2m}\alpha b^2 \in k^2$ is equivalent with $-1 \notin k^2$ in the case $v_k(c) > m$.

Proof.— Let $m > n$ put $x = \pi^m s$. Choose ℓ/k, unramified of odd degree as in corollary 1.2, with $s \in O_k^*$ such that

$$\begin{cases} s^2 - \alpha b^2 \in O_\ell^{*2} & \text{if } v_k(c) > m \\ (s - c')^2 - \alpha b^2 \in O_\ell^{*2} & \text{if } v_k(c) \leq m \end{cases}$$

with $c = \pi^t c'$, $c' \in O_k^*$, this is possible by corollary 1.2. It follows that

$$f(x) \equiv \begin{cases} \pi^{2m+2n+1}(s^2 - \alpha b^2)a^2 \bmod \pi^{2m+2n+2}O_\ell & \text{if } v_k(c) > m \\ \pi^{2m+2n+1}\Big((s-c')^2 - \alpha b^2\Big)a^2 \bmod \pi^{2m+2n+2}O_\ell & \text{if } v_k(c) = m \\ \pi^{2n+1}a^2c^2 \bmod \pi^{2n+2}O_\ell & \text{if } v_k(c) < m. \end{cases}$$

It follows that $\pi f(x) \in \ell^2$, i.e. $I(C_{\pi f}) = 1$, in all these cases.

Let $m \leq n$. If $v_k(c) < m$ then (since automatically $m \neq 0$)

$$f(0) \equiv \pi^{2n+1}a^2c^2 \bmod \pi^{2n+2}O_k\,,$$

so $\pi f(0) \in k^2$ and $I(C_{\alpha f}) = 1$.

Finally the case $m \leq n$ and $v_k(c) \geq m$. If x is the X-coordinate of a point of $C_{\pi f}$ over some odd degree extension ℓ/k with odd ramification index $e = e(\ell/k)$ and $\pi_\ell^e w = \pi$, then $v_\ell(f(x))$ is odd. But

$$v_\ell(f(x)) = v_\ell\Big((x^2 + \pi^{2n+1}a^2)\Big((x-c)^2 - \pi^{2m}\alpha b^2\Big)\Big)$$

moreover the value of $(x-c)^2 - \pi^{2m}\alpha b^2$ is even since $\overline{\alpha b^2} \notin \bar{k}^2$. It follows from these observations that $v_\ell(x) > en$. We obtain

if $v_k(c) = m\,(\Leftrightarrow v_\ell(c) = me)$

then $f(x) \in (\pi_\ell^{2ne+e}w^2a^2)\pi_\ell^{2me}(c'^2 - \alpha b^2) + \pi_\ell^{2ne+2me+e+1}O_\ell$

if $v_k(c) > m\,(\Leftrightarrow v_\ell(c) > me)$

then $f(x) \in (\pi_\ell^{2ne+e}w^2a^2)\pi_\ell^{2me}(-\alpha b^2) + \pi_\ell^{2ne+2me+e+1}O_\ell\,.$

The remaining statements of the proposition follow from this. □

PROPOSITION 3.4.— *Let* $f(X) = f_1(X)f_2(X)$ *with*

$$f_1(X) = X^2 - \pi^{2n}\alpha a^2$$
$$f_2(X) = (X-c)^2 + \pi^{2m+1}\alpha b^2\,,$$

where $a, b \in O_k^*$ *and* $c \in O_k$. *Let* v_k *be the valuation on* k *normalised such that* $v_k(\pi) = 1$. *Then*

(i) $m < n$ *and* $m < v_k(c)$ *then* $I(C_{\pi f}) = 1$;

(ii) $m < n$ *and* $m \geq v_k(c)$ *then* $I(C_{\pi f}) = 2$;

(iii) $m \geq n$ *and* $v_k(c) < n$ *then* $I(C_{\pi f}) = 2$;

(iv) $m \geq n$ *and* $v_k(c) \geq n$ *then* $I(C_{\pi f}) = 1$ *if and only if* $c^2 - \pi^{2n}\alpha a^2 \notin k^2$.

Proof.— We observe that in order for $C_{\pi f}$ to have a point (x, y) over a field extension ℓ of odd degree over k with ramification index $e = e(\ell/k)$ and $\pi_\ell^e w = \pi$, $v_\ell\big(f(x)\big)$ must be odd. Since $v_\ell(x^2 - \pi^{2n}\alpha a^2) \in 2\mathbb{Z}$, otherwise $\bar{\alpha}$ would be a square in $\bar{\ell}$, we must have $2v_\ell(x-c) > 2me+e$, so $v_\ell(x-c) > me$. Moreover x must be such that $x^2 - \pi^{2n}\alpha a^2 \notin \ell^2$. The latter is only possible if $v_\ell(x) \geq ne$. (If $v_\ell(x) = ne$ then $x = \pi_\ell^{en} w^2 s'^2 = \pi^n s^2$ with $s \in O_\ell^*$. By corollary 1.2 we can choose ℓ and s such that $s^2 - \alpha a^2 \notin \ell^{*2}$.)

First let $m < n$. If $m < v_k(c)$ then take ℓ as in corollary 1.2 and $x = \pi^n s \in \ell$ (ℓ/k is unramified so $\pi_\ell = \pi$), such that $s^2 - \alpha a^2 \notin \ell^{*2}$. The above conditions on x are satisfied so $I(C_{\pi f}) = 1$. If $v_k(c) \leq m$ then $v_\ell(x - c) > me$ implies $v_\ell(x) = v_\ell(c) \leq me < ne$. So the conditions for $C_{\pi f}$ to have a point in some odd degree extension cannot be satisfied, i.e. $I(C_{\pi f}) = 2$ in this case. (This proves (i) and (ii)).

Secondly, let $n \leq m$. If $v_k(c) < n$ then $v_\ell(x - c) > me$ implies $v_\ell(x) = v_\ell(c) < ne$, so also in this case the conditions for $C_{\pi f}$ to have an ℓ-point cannot be satisfied and $I(C_{\pi f}) = 2$ follows. If $v_k(c) \geq n$, in order to have $2v_\ell(x - c) > 2me + e$, we must choose $x \in \ell$ to be of the form $x = c + \pi^k d$ with $d \in O_\ell$, and $2k > m + 1$. Now

$$\begin{aligned} f_1(x) &= \big(c + \pi^k d\big)^2 - \pi^{2n}\alpha a^2 \\ &\equiv (c^2 - \pi^{2n}\alpha a^2) \bmod \pi_\ell^{2ne+1} O_\ell \,. \end{aligned}$$

And we see that

$$\pi f(x) = \pi f_1(x) f_2(x) \equiv \pi^{2m+2}\alpha b^2 (c^2 - \pi^{2n}\alpha a^2) \bmod \pi_\ell^{2ne+2me+1} O_\ell$$

is a square if and only if $c^2 - \pi^{2n}\alpha a^2 \notin k^2$. □

Remark 3.5.— In case $v_k(c) > n$ the condition $c^2 - \pi^{2n}\alpha a^2 \notin k^2$ is equivalent with $-1 \notin k^2$.

PROPOSITION 3.6.— *Let* $f(X) = f_1(X)f_2(X)$ *with*

$$f_1(X) = X^2 + \pi^{2n+1}a^2$$
$$f_2(X) = (X-c)^2 + \pi^{2m+1}\alpha b^2,$$

where $a, b \in O_k^*$ *and* $c \in O_k$. *Let* v_k *be the valuation on* k *normalised such that* $v_k(\pi) = 1$. *Then*

(i) $I(C_{\pi f}) = 1$ *if* $v_k(c) \leq m$;
(ii) $I(C_{\pi f}) = 1$ *if* $v_k(c) > m$ *and* $m > n$;
(iii) $I(C_{\pi f}) = 2$ *if* $v_k(c) > m$, $m \leq n$.

Proof.— If $v_k(c) \leq m$ then

$$f(0) \in \pi^{2n+1}a^2c^2 + \pi^{2n+2}O_k$$

and so $\pi f(0) \in k^2$, implying $I(C_{\pi f}) = 1$.

If $v_k(c) > m > n$ then

$$f(\pi^m) \in \pi^{2n+2m+1}a^2 + \pi^{2m+2n+2}O_k$$

and we have the same conclusion.

If $v_k(c) > m$ and $m \leq n$ take ℓ any odd degree extension of k with ramification index $e = e(\ell/k)$ and v_ℓ its normalised valuation, i.e., $v_\ell(\pi_\ell) = 1$. First we remark that for $x \in \ell$ with $v_\ell(x) \leq ne$, $\pi f(x)$ cannot be a square. This since

$$\pi x^2\Big((x-c)^2 + \pi^{2m+1}\alpha b^2\Big) \notin \ell^2,$$

since it either has odd valuation (if $2v(x-c) > 2m+1$) or it is congruent to α modulo squares (if $2v(x-c) < 2m+1$). So assume $v_\ell(x) > ne \geq me$. This implies $v_\ell(x-c) > me$ and therefore

$$v_\ell\big(\pi f(x)\big) \text{ is odd}.$$

It follows that for every ℓ/k of odd degree and for every $x \in \ell$, $f(x) \notin \ell^2$. Therefore $I(C_{\pi f}) = 2$. □

Remark 3.7.— One can verify directly that in propositions 3.1, 3.2, 3.4 and 3.6 the conditions for the index to be 1 are complementary to those that imply the index to be 2.

4. Summary

Let

$$f(X) = f_1(X)f_2(X) = (X^2 + b_1X + b_0)(X^2 + c_1X + c_0)\,.$$

It is easy to translate the conditions obtained in the previous sections to determine the index of $C_{\alpha f}$ and $C_{\pi f}$ into conditions on the coefficients b_1, b_0, c_1, c_0. In this way we get theorem 4.1, thereby summarizing our results.

THEOREM 4.1.— *Let k be a non-dyadic local field of characteristic zero. Let*

$$f(X) = (X^2 + b_1X + b_0)(X^2 + c_1X + c_0)$$

be a polynomial over O_k, $\Delta_1 = b_1^2 - 4b_0^2 = \delta_1\pi^r \notin k^2$ and $\Delta_2 = c_1^2 - 4c_0^2 = \delta_2\pi^s \notin k^2$ with $\delta_1, \delta_2 \in O_k^*$. Put $\gamma = (b_1 - c_1)/2$.

(A) Let $C_{\alpha f}$ be the curve defined by the equation $Y^2 = \alpha f(X)$.

(1) If $\Delta_1 \equiv \alpha \bmod k^{*2}$ and $\Delta_2 \equiv \alpha \bmod k^{*2}$ then $I(C_{\alpha f}) = 2$ if and only if

$$v(\gamma) > v(\Delta_1) = v(\Delta_2) \quad \text{and} \quad \bar{\delta}_1 = \bar{\delta}_2\,.$$

(2) If $\Delta_1 \equiv \pi \bmod k^{*2}$ and $\Delta_2 \equiv \alpha \bmod k^{*2}$ then $I(C_{\alpha f}) = 2$ if and only if

$$v(\gamma) > \min\big(v(\Delta_1), v(\Delta_2)\big) = v(\Delta_1)\,.$$

(3) If $\Delta_1 \equiv \pi \bmod k^{*2}$ and $\Delta_2 \equiv \alpha\pi \bmod k^{*2}$ then $I(C_{\alpha f}) = 2$ if and only if

$$v(\gamma) \leq \min\big(v(\Delta_1), v(\Delta_2)\big)\,.$$

(4) If $\Delta_1 \equiv \pi \bmod k^{*2}$ and $\Delta_2 \equiv \pi \bmod k^{*2}$ then $I(C_{\alpha f}) = 2$.

(B) Let $C_{\pi f}$ be the curve defined by the equation $Y^2 = \pi f(X)$.

(1) If $\Delta_1 \equiv \pi \bmod k^{*2}$ and $\Delta_2 \equiv \pi \bmod k^{*2}$ then $I(C_{\pi f}) = 2$ if and only if

$$v(\gamma) > v(\Delta_1) = v(\Delta_2).$$

(2) If $\Delta_1 \equiv \pi \bmod k^{*2}$ *and* $\Delta_2 \equiv \alpha \bmod k^{*2}$ *then* $I(C_{\pi f}) = 2$ *if and only if*

$$v(\gamma) \geq v(\Delta_1), \quad v(\Delta_2) \geq v(\Delta_2) \quad \textit{and} \quad \gamma^2 - \Delta_2 \notin k^{*2}.$$

(3) If $\Delta_1 \equiv \alpha \bmod k^{*2}$ *and* $\Delta_2 \equiv \alpha\pi \bmod k^{*2}$ *then* $I(C_{\pi f}) = 2$ *if and only if one of the following conditions hold:*
(i) $v(\gamma) \leq v(\Delta_1) < v(\Delta_2)$,
(ii) $v(\gamma) < v(\Delta_2) \leq v(\Delta_1)$.

(4) If $\Delta_1 \equiv \pi \bmod k^{*2}$ *and* $\Delta_2 \equiv \alpha\pi \bmod k^{*2}$ *then* $I(C_{\pi f}) = 2$ *if and only if*

$$v(\gamma) > v(\Delta_1) \quad \textit{and} \quad v(\Delta_1) \leq v(\Delta_2).$$

(5) If $\Delta_1 \equiv \Delta_2 \equiv \alpha \bmod k^{*2}$ *or if* $\Delta_1 \equiv \Delta_2 \equiv -\alpha\pi \bmod k^{*2}$ *then* $I(C_{\pi f}) = 2$.

Remark 4.2. — We only summarized the conditions for the index of the $C_{\alpha f}$, respectively $C_{\pi f}$ to be 2. The complementary conditions yield that the respective curves have index 1. So there exists a k-rational divisor $\mathcal{D}$ of degree 1 on C. By the Riemann-Roch theorem one can find a function $h \in k(C)$ such that $\mathcal{D} + (h)$ is a positive divisor which, since it has degree one, must be a k-rational point.

A theorem of Roquette and Lichtenbaum [2] tells us that for any smooth geometrically connected projective curve C over a local field k,

$$I(C) = \#\left[\ker(\mathrm{Br}(k) \to \mathrm{Br}\big(k(C)\big)\right]$$

with $\mathrm{Br}(k)$, $\mathrm{Br}\big(k(C)\big)$ the Brauer groups of k and $k(C)$ respectively. It follows that for the curves, $C_{\alpha f}$ and $C_{\pi f}$, of genus 1 satisfying the conditions summed up in theorem 4.1, this kernel equals $\Big\{[M_2(k)], [H]\Big\}$, with H the unique quaternion division algebra over k. ($[D]$ indicates the class in the Brauer group of the algebra D.)

References

[1] Borevich (Z. I.) and Shafarevich (I. R.) .— *Number theory*, Academic press, New York, 1966.

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

[3] Scharlau (W.) .— *Quadratic and Hermitian Forms*, Springer-Verlag, Heidelberg, 1985.

[4] Serre (J.-P.) .— *Corps locaux*, Hermann, Paris, 1963.

[5] Van Geel (J.) and Yanchevskii (V. I.) .— *Indices of hyperelliptic curves over p-adic fields*, Manuscripta Math. **96** (1998), pp. 317-333.

[6] Yanchevskii (V.) and Margolin (G.) .— *Brauer Groups of Local Elliptic and Hyperelliptic Curves and Central Division Algebras over their Function Fields*, St. Petersburg Math. J. **7**, No 6 (1996), pp. 1033-1048.