ACTA ARITHMETICA
127.4 (2007)

A class number criterion for the equation $(x^p - 1)/(x - 1) = py^q$

by

BENJAMIN DUPUY (Bordeaux)

1. Introduction. Let p be an odd prime number and let

$$\Phi(x) = \Phi_p(x) = \frac{x^p - 1}{x - 1}$$

be the pth cyclotomic polynomial. It is well-known that, for $x \in \mathbb{Z}$, the integer $\Phi(x)$ is divisible by at most the first power of p. More precisely, $p \nmid \Phi(x)$ if $x \not\equiv 1 \bmod p$, and $p \parallel \Phi(x)$ if $x \equiv 1 \bmod p$.

Indeed, if $p \mid \Phi(x)$ then $x^p \equiv 1 \bmod p$, which implies $x \equiv 1 \bmod p$. Now, using the binomial formula, we obtain

$$\Phi(x) = \frac{(1 + (x-1))^p - 1}{x - 1} = p + \sum_{k=2}^{p-1} \binom{p}{k} (x-1)^{k-1} + (x-1)^{p-1} \equiv p \bmod p^2,$$

which implies $p \parallel \Phi(x)$.

Let q be another prime number. A classical Diophantine problem, studied, most recently, by Mihăilescu [6, 7], is whether the p-free part of $\Phi(x)$ can be a qth power. This can be rephrased as follows: given $e \in \{0, 1\}$, does the equation $\Phi(x) = p^e y^q$ have a non-trivial solution in integers x and y? (By *trivial* solutions we mean those with $x = e = 0$ and $x = e = 1$.)

The case $e = 0$, that is, the equation $\Phi(x) = y^q$, is (a particular case of) the classical *Nagell–Ljunggren equation*. It is known to have several non-trivial solutions, and, as is commonly believed, no other solutions exist. See [3] for a comprehensive survey of results on this equation and methods for its analysis.

In the present note we study the case $e = 1$, that is, the equation

$$\frac{x^p - 1}{x - 1} = py^q. \tag{1}$$

(As we have seen above, any solution of this equation must satisfy $x \equiv 1 \bmod p$.)

2000 *Mathematics Subject Classification*: Primary 11D41; Secondary 11R18, 11S80.

Let h_p^- be the pth relative class number. Mihăilescu [7, Theorem 1] proved that (1) has no non-trivial solutions if $q \nmid h_p^-$ and, in addition, some complicated technical condition involving p and q is satisfied. In this note we show that this technical condition is not required.

THEOREM 1.1. *Let p and q be distinct odd prime numbers*, $p \geq 5$. *Assume that q does not divide the relative class number h_p^-. Then* (1) *has no solutions in integers $x, y \neq 1$.*

In particular, since $h_p^- = 1$ for $p \leq 19$, equation (1) has no non-trivial solutions when $5 \leq p \leq 19$. (Neither does it have solutions when $p = 3$, as was shown long ago by Nagell [8].)

The interest in equation (1) was inspired by the fact that it is closely related to the celebrated equation of Catalan $x^p - z^q = 1$. In fact, Cassels [4] showed that any non-trivial solution of Catalan's equation gives rise to a solution of (1). All major contributions to the theory of Catalan's equation, including Mihăilescu's recent solution [1, 5], have Cassels' result as the starting point.

This article is strongly inspired by the work of Mihăilescu [5, 6, 7]. In particular, the argument in the case $q \not\equiv 1 \bmod p$ (see Section 6) can be found in [6]. However, the case $q \equiv 1 \bmod p$ (see Section 7) requires new ideas.

2. The cyclotomic field. Let p be an odd prime number and let $\zeta = \zeta_p$ be a primitive pth root of unity. In this section we collect several facts about the pth cyclotomic field $K = \mathbb{Q}(\zeta)$. As usual, we denote by $K^+ = K \cap \mathbb{R} = \mathbb{Q}(\zeta + \overline{\zeta})$ the maximal real subfield of K. (Here and below, $z \mapsto \overline{z}$ stands for the "complex conjugation" map.) We denote by $\mathcal{O}$ the ring of integers of K; it is well-known that $\mathcal{O} = \mathbb{Z}[\zeta]$.

We denote by $\mathfrak{p}$ the principal ideal $(1 - \zeta)$. It is the only prime ideal of the field K above p, and $\mathfrak{p}^{p-1} = (p)$. For $k \not\equiv l \bmod p$ the algebraic number

$$\frac{\zeta^k - \zeta^l}{1 - \zeta}$$

is a unit of K (called *cyclotomic* or *circular* unit); in other words, we have

$$(\zeta^k - \zeta^l) = \mathfrak{p}.$$

In particular,

$$\zeta^k + \zeta^l = \frac{\zeta^{2k} - \zeta^{2l}}{1 - \zeta} \Big/ \frac{\zeta^k - \zeta^l}{1 - \zeta}$$

is a unit in K. All this will be frequently used without special reference.

Finally, recall that $h_p^+ \mid h_p$, where h_p and h_p^+ are the class numbers of K and K^+, respectively, and the relative class number is defined by $h_p^- = h_p / h_p^+$.

The proofs of all statements above can be found in the first chapters of any course of the theory of cyclotomic fields; see, for instance, [9].

The following observation provides a convenient tool for calculating traces of algebraic integers from K modulo p. We denote by $\mathbb{F}_p$ the field of p elements, and we let $\mathrm{Tr} : K \to \mathbb{Q}$ be the trace map.

PROPOSITION 2.1. *Let $\varrho : \mathcal{O} \to \mathbb{F}_p$ be the reduction modulo $\mathfrak{p}$. Then for any $a \in \mathcal{O}$ we have*

$$\varrho(a) \equiv -\mathrm{Tr}(a) \bmod p. \tag{2}$$

Proof. We have $\varrho(\zeta^n) = 1$ for all $n \in \mathbb{Z}$, and

$$\mathrm{Tr}(\zeta^n) = \begin{cases} -1, & p \nmid n, \\ p-1, & p \mid n. \end{cases} \tag{3}$$

Hence (2) holds for $a = \zeta^n$. By linearity, it extends to $\mathcal{O} = \mathbb{Z}[\zeta]$. ∎

Here is an example of how one can use this.

COROLLARY 2.2. *For any $u \in \mathbb{Z}$ put*

$$\chi_u = \frac{\zeta^u - \zeta}{(1+\zeta^u)(1-\zeta)}. \tag{4}$$

Then

$$2\mathrm{Tr}(\chi_u) \equiv u - 1 \bmod p. \tag{5}$$

In particular, $\mathrm{Tr}(\chi_u) \not\equiv 0 \bmod p$ *unless* $u \equiv 1 \bmod p$.

Proof. For $u \equiv 1 \bmod p$ we have $\chi_u = 0$ and there is nothing to prove. Now let $u \not\equiv 1 \bmod p$. We may assume that $u > 0$. We have

$$\varrho\left(\frac{\zeta^u - \zeta}{1-\zeta}\right) = \varrho(-\zeta - \zeta^2 - \cdots - \zeta^{u-1}) = 1 - u.$$

Also, since $1 + \zeta^u$ is a unit, we have

$$\varrho\left(\frac{1}{1+\zeta^u}\right) = \varrho(1+\zeta^u)^{-1} = \frac{1}{2}.$$

Hence $\varrho(\chi_u) = (1-u)/2$, which implies (5). ∎

In the following example we cannot use (2) because the number we are interested in is not an algebraic integer.

PROPOSITION 2.3. *We have*

$$\mathrm{Tr}\left(\frac{\zeta}{(1-\zeta)^2}\right) = \frac{1-p^2}{12}.$$

Proof. Consider the rational function

$$F(t) = \sum_{k=1}^{p-1} \frac{\zeta^k t}{(1-\zeta^k t)^2}.$$

Using (3), we obtain

$$\begin{aligned} F(t) &= -\sum_{k=1}^{p-1}\sum_{n=1}^{\infty} n\zeta^{kn}t^n = -\sum_{n=1}^{\infty} n\mathrm{Tr}(\zeta^n)t^n \\ &= \sum_{n=1}^{\infty} nt^n - p^2\sum_{n=1}^{\infty} nt^{pn} = -\frac{t}{(1-t)^2} + \frac{p^2t^p}{(1-t^p)^2}. \end{aligned}$$

When $t \to 1$ we have

$$\begin{aligned} \frac{t}{(1-t)^2} &= \frac{1}{(t-1)^2} + \frac{1}{t-1}, \\ \frac{p^2t^p}{(1-t^p)^2} &= \frac{1}{(t-1)^2} + \frac{1}{t-1} + \frac{1-p^2}{12} + o(1). \end{aligned}$$

Hence

$$\mathrm{Tr}\left(\frac{\zeta}{(1-\zeta)^2}\right) = F(1) = \frac{1-p^2}{12}. \ \blacksquare$$

3. Binomial power series. We shall need a property of binomial power series in the non-archimedean domain. As usual, we denote by $\mathbb{Z}_p$ and $\mathbb{Q}_p$ the ring of p-adic integers and the field of p-adic numbers, and we extend the standard p-adic absolute value from $\mathbb{Q}_p$ to the algebraic closure $\overline{\mathbb{Q}}_p$.

Given $a \in \mathbb{Z}_p$, we let

$$R_a(t) = (1+t)^a = 1 + at + \binom{a}{2}t^2 + \binom{a}{3}t^3 + \cdots$$

be the binomial power series. Its coefficients are p-adic integers, and for any τ, algebraic over $\mathbb{Q}_p$ and with $|\tau|_p < 1$, our series converges at $t = \tau$ in the field $\mathbb{Q}_p(\tau)$. For any $n = 0, 1, \ldots$ we have the obvious inequality

$$\left| R_a(\tau) - \sum_{k=0}^{n} \binom{a}{k}\tau^k \right|_p \le |\tau|_p^{n+1}.$$

When a is p-adically small, a sharper inequality may hold. For instance,

$$|R_p(\tau) - (1+p\tau)|_p \le p|\tau|_p^2$$

when $|\tau|_p$ is sufficiently small. We shall need a result of this kind for the second order Taylor expansion.

It will be convenient to use the familiar notation $O(\cdot)$ in a slightly non-traditional fashion: we say $\tau = O(\upsilon)$ if $|\tau|_p \le |\upsilon|_p$.

Proposition 3.1. *Assume $p \ge 5$ and that $|\tau| \le p^{-1/(p-3)}$. Then*

$$R_a(\tau) = 1 + a\tau - \frac{a}{2}\tau^2 + O(a^2\tau^2) + O(a\tau^3). \tag{6}$$

Proof. Since

$$\frac{a(a-1)}{2}\,\tau^2 = -\frac{a}{2}\,\tau^2 + O(a^2\tau^2),$$

equality (6) is an immediate consequence of

$$R_a(\tau) = 1 + a\tau + \frac{a(a-1)}{2}\,\tau^2 + O(a\tau^3), \tag{7}$$

so it suffices to prove the latter.

We prove (7) by induction on the p-adic order of a. When $|a|_p = 1$, equality (7) is an immediate consequence of the binomial formula (and holds even under the weaker assumption $|\tau|_p < 1$). Now assume that (7) holds for some $a \in \mathbb{Z}_p$, and let us show that it holds with a replaced by pa.

By the induction hypothesis, $R_a(\tau) = 1 + \upsilon$, where

$$\upsilon = a\tau + \frac{a(a-1)}{2}\,\tau^2 + O(a\tau^3).$$

Then

$$\begin{aligned} R_{pa}(\tau) &= (1+\upsilon)^p = 1 + p\upsilon + \frac{p(p-1)}{2}\,\upsilon^2 + O(p\upsilon^3) + O(\upsilon^p) \\ &= 1 + pa\tau + \frac{pa(a-1)}{2}\,\tau^2 + \frac{pa^2(p-1)}{2}\,\tau^2 + O(pa\tau^3) + O((a\tau)^p) \\ &= 1 + pa\tau + \frac{pa(pa-1)}{2}\,\tau^2 + O(pa\tau^3) + O((a\tau)^p). \end{aligned} \tag{8}$$

Since $|\tau| \le p^{-1/(p-3)}$, we have $|(a\tau)^p|_p \le |pa^p\tau^3|_p \le |pa\tau^3|_p$. Hence the term $O((a\tau)^p)$ in (8) can be disregarded. This completes the proof of (7) and of the proposition. ■

4. A special unit of the cyclotomic field. We start the proof of Theorem 1.1. We fix, once and for all, distinct odd prime numbers p and q, and rational integers $x, y \ne 1$ satisfying (1). Recall that

$$x \equiv 1 \bmod p,$$

this congruence being frequently used below without special reference. Also, we use without special reference the notation of Section 2.

In this section, we construct a special unit of the field K, which plays the central role in the proof of Theorem 1.1. Our starting point is the following well-known statement.

PROPOSITION 4.1. *Put*

$$\alpha = \frac{x-\zeta}{1-\zeta}.$$

Then we have the following:

1. *The principal ideal* (α) *is a* q*th power of an ideal of* K*.*
2. *Assume that* q *does not divide the relative class number* h_p^-*. Then* $\overline{\alpha}/\alpha$ *is a* q*th power in* K*.*

Though the proof can be found in the literature, we include it here for the reader's convenience. We closely follow [2].

Proof. Since

$$\Phi_p(x) = (x-\zeta)\cdots(x-\zeta^{p-1}), \qquad p = \Phi_p(1) = (1-\zeta)\cdots(1-\zeta^{p-1}),$$

we may rewrite equation (1) as

$$\prod_{k=1}^{p-1} \frac{x-\zeta^k}{1-\zeta^k} = y^q. \tag{9}$$

Since $p = \mathfrak{p}^{p-1} \mid (x-1)$, we have $\mathfrak{p} \parallel (x-\zeta^k)$ for $k = 1, \ldots, p-1$. Hence the numbers

$$\alpha_k = \frac{x-\zeta^k}{1-\zeta^k} \qquad (k = 1, \ldots, p-1)$$

are algebraic integers coprime with $\mathfrak{p}$.

On the other hand, since

$$(1-\zeta^k)\alpha_k - (1-\zeta^l)\alpha_l = \zeta^l - \zeta^k,$$

the greatest common divisor of α_k and α_l should divide $\mathfrak{p} = (\zeta^k - \zeta^l)$. Hence the numbers $\alpha_1, \ldots, \alpha_{p-1}$ are pairwise coprime. (In particular, α and $\overline{\alpha}$ are coprime, to be used in the proof of Proposition 4.2.) Now (9) implies that each of the principal ideals (α_k) is a qth power of an ideal. This proves part 1.

Now write $(\alpha) = \mathfrak{a}^q$, where $\mathfrak{a}$ is an ideal of K. If $q \nmid h_p^-$ then the class of $\mathfrak{a}$ belongs to the real part of the class group. In other words, we have $\mathfrak{a} = \mathfrak{b}(\gamma)$, where $\gamma \in K^*$ and $\mathfrak{b}$ is a "real" ideal of K (that is, $\mathfrak{b} = \overline{\mathfrak{b}}$). Further, $\mathfrak{b}^q$ is a principal real ideal; in other words, $\mathfrak{b}^q = (\beta)$, where $\beta \in K^+$. We obtain $(\alpha) = (\beta\gamma^q)$, that is, α is equal to $\beta\gamma^q$ times a unit of K.

Recall that if η is a unit of a cyclotomic field then $\overline{\eta}/\eta$ is a root of unity. Since $\overline{\beta} = \beta$, we deduce that $\overline{\alpha}/\alpha$ is $(\overline{\gamma}/\gamma)^q$ times a root of unity. Since every root of unity in K is a qth power, we have shown that $\overline{\alpha}/\alpha$ is a qth power. This proves part 2. ∎

From now on *we assume that* q *does not divide* h_p^-. In particular, Proposition 4.1 implies that there exists $\mu \in K$ such that $\overline{\alpha}/\alpha = \mu^q$. Moreover, this μ is unique because K does not contain non-trivial qth roots of unity. Similarly, the field K contains exactly one qth root of $\alpha/\overline{\alpha}$. Since both $\overline{\mu}$ and μ^{-1} are qth roots of $\alpha/\overline{\alpha}$, we have

$$\mu^{-1} = \overline{\mu}. \tag{10}$$

This will be used in Section 5.

Now we are ready to construct the promised unit.

PROPOSITION 4.2. *Let u be the inverse of q modulo p (that is, we have $uq \equiv 1 \bmod p$). Then the algebraic number $\phi = \alpha(\mu + \zeta^u)^q$ is a unit of the field K.*

Proof. Write the principal ideal (μ) as $\mathfrak{a}\mathfrak{b}^{-1}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime integral ideals of K. Then $(\overline{\alpha}/\alpha) = \mathfrak{a}^q\mathfrak{b}^{-q}$. Moreover, since α and $\overline{\alpha}$ are coprime (see the proof of Proposition 4.1), we have $(\overline{\alpha}) = \mathfrak{a}^q$ and $(\alpha) = \mathfrak{b}^q$.

Further, we have $(\mu + \zeta^u) = \mathfrak{c}\mathfrak{b}^{-1}$, where $\mathfrak{c}$ is yet another integral ideal of K. We obtain $(\phi) = \mathfrak{b}^q\mathfrak{c}^q\mathfrak{b}^{-q} = \mathfrak{c}^q$, which shows that ϕ is an algebraic integer.

Next, put

$$\phi' = \alpha^{q-1}\Big(\sum_{k=0}^{q-1}\mu^k(-\zeta^u)^{q-1-k}\Big)^q.$$

The same argument as above proves that ϕ' is an algebraic integer as well. Further,

$$\phi\phi' = \alpha^q\Big((\mu+\zeta^u)\sum_{k=0}^{q-1}\mu^k(-\zeta^u)^{q-1-k}\Big)^q = (\alpha(\mu^q + \zeta^{uq}))^q.$$

Now recall that $\mu^q = \overline{\alpha}/\alpha$ and that $uq \equiv 1 \bmod p$. The latter congruence implies that $\zeta^{uq} = \zeta$, and we obtain

$$\phi\phi' = (\alpha(\overline{\alpha}/\alpha + \zeta))^q = (\overline{\alpha} + \zeta\alpha)^q = (1+\zeta)^q.$$

Since $1+\zeta$ is a unit of K, so are ϕ and ϕ'. ∎

5. An analytic expression for μ. We shall work in the local field $K_{\mathfrak{p}} = \mathbb{Q}_p(\zeta)$. As before, we extend p-adic absolute value from $\mathbb{Q}_p$ to $K_{\mathfrak{p}}$, so that $|1-\zeta|_p = p^{-1/(p-1)}$.

Since p totally ramifies in K, every automorphism σ of $K/\mathbb{Q}$ extends to an automorphism of $K_{\mathfrak{p}}/\mathbb{Q}_p$. In particular, the "complex conjugation" $z \mapsto \overline{z}$ extends to an automorphism of $K_{\mathfrak{p}}/\mathbb{Q}_p$ (we continue to call it "complex conjugation").

Let $R_a(t)$ be the binomial power series, introduced in Section 3. Since the automorphisms of $K_{\mathfrak{p}}/\mathbb{Q}_p$ (in particular the "complex conjugation") are continuous in the $\mathfrak{p}$-adic topology, for any $\tau \in K_{\mathfrak{p}}$ with $|\tau|_p < 1$ and for any $\sigma \in \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$ we have $R_a(\tau)^\sigma = R_a(\tau^\sigma)$. In particular, $\overline{R_a(\tau)} = R_a(\overline{\tau})$.

Put

$$\lambda = \frac{x-1}{1-\zeta},$$

so that

$$\alpha = 1+\lambda, \qquad \overline{\alpha} = 1 + \overline{\lambda} = 1 - \zeta\lambda$$

(recall that α is defined in Proposition 4.1). Then

$$|\lambda|_p = |x-1|_p p^{1/(p-1)} \le p^{-(p-2)/(p-1)} < 1,$$

and similarly for $\overline{\lambda}$. In particular, for any $a \in \mathbb{Z}_p$, the series $R_a(t)$ converges at $t=\lambda$ and $t=\overline{\lambda}$.

We wish to express the quantity μ, introduced in Section 4, in terms of the binomial power series. Since both μ and $R_{1/q}(\overline{\lambda})R_{-1/q}(\lambda)$ are qth roots of $\overline{\alpha}/\alpha$, we have

$$\mu = R_{1/q}(\overline{\lambda})R_{-1/q}(\lambda)\xi, \tag{11}$$

where $\xi \in K_{\mathfrak{p}}$ is a qth root of unity. We want to show that $\xi = 1$.

The field $\mathbb{Q}_p(\xi)$ is an unramified sub-extension of the totally ramified extension $K_{\mathfrak{p}}$. Hence $\mathbb{Q}_p(\xi) = \mathbb{Q}_p$, that is, $\xi \in \mathbb{Q}_p$. It follows that ξ is stable with respect to all automorphisms of $K_{\mathfrak{p}}/\mathbb{Q}_p$; in particular, it is stable with respect to the "complex conjugation": $\overline{\xi} = \xi$.

Applying the "complex conjugation" to (11) and using (10), we obtain $\mu^{-1} = R_{1/q}(\lambda)R_{-1/q}(\overline{\lambda})\xi$, which, together with (11), implies that $\xi^2 = 1$. Since ξ is a qth root of unity, this is possible only if $\xi = 1$.

We have shown that

$$\mu = R_{1/q}(\overline{\lambda})R_{-1/q}(\lambda) = R_{1/q}(-\zeta\lambda)R_{-1/q}(\lambda). \tag{12}$$

The rest of the proof splits into two cases, depending on whether $q \not\equiv 1 \bmod p$ or $q \equiv 1 \bmod p$. The arguments in both cases are quite similar, but the latter case is technically more involved.

6. The case $q \not\equiv 1 \bmod p$.

We have

$$\mu = R_{1/q}(-\zeta\lambda)R_{-1/q}(\lambda) = 1 - \frac{1+\zeta}{q}\,\lambda + O(\lambda^2),$$

where, as in Section 3, we say that $\tau = O(\upsilon)$ if $|\tau|_p \le |\upsilon|_p$.

Hence, for the quantity ϕ, introduced in Proposition 4.2, we have

$$\begin{aligned} \phi &= (1+\lambda)\left(1+\zeta^u - \frac{1+\zeta}{q}\,\lambda + O(\lambda^2)\right)^q \\ &= (1+\zeta^u)^q(1+\lambda)\left(1 - \frac{1+\zeta}{1+\zeta^u}\,\lambda\right) + O(\lambda^2) \\ &= (1+\zeta^u)^q\left(1 + \frac{\zeta^u-\zeta}{1+\zeta^u}\,\lambda\right) + O(\lambda^2) \\ &= (1+\zeta^u)^q(1+(x-1)\chi_u) + O(\lambda^2), \end{aligned} \tag{13}$$

where χ_u is defined in (4).

Since the automorphisms of $K/\mathbb{Q}$ extend to automorphisms of $K_{\mathfrak{p}}/\mathbb{Q}_p$, the same is true for the norm and the trace maps: for any $a \in K$ we have

$$\mathcal{N}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(a) = \mathcal{N}_{K/\mathbb{Q}}(a), \qquad \mathrm{Tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(a) = \mathrm{Tr}_{K/\mathbb{Q}}(a).$$

Below, we shall simply write $\mathcal{N}(a)$ and $\mathrm{Tr}(a)$. Also, since the automorphisms are continuous, we have $|\mathcal{N}(a)|_p \le |a|_p^{p-1}$ and $|\mathrm{Tr}(a)|_p \le |a|_p$.

Taking the norm in (13), we obtain

$$\mathcal{N}\left(\frac{\phi}{(1+\zeta^u)^q}\right) = 1 + (x-1)\mathrm{Tr}(\chi_u) + O(\lambda^2).$$

Since both ϕ and $1+\zeta^u$ are units, the norm on the left is ± 1. Since $-1 \not\equiv 1 \bmod p$, the norm is 1, and we obtain $(x-1)\mathrm{Tr}(\chi_u) = O(\lambda^2)$.

But, since $q \not\equiv 1 \bmod p$, we also have $u \not\equiv 1 \bmod p$. Corollary 2.2 implies that $\mathrm{Tr}(\chi_u)$ is not divisible by p. We obtain

$$|x-1|_p \le |\lambda|_p^2 = |x-1|_p^2\, p^{2/(p-1)},$$

which implies $|x-1|_p \ge p^{-2/(p-1)}$. Since $p \mid (x-1)$, this is impossible as soon as $p \ge 5$.

This proves the theorem in the case $q \not\equiv 1 \bmod p$.

7. The case $q \equiv 1 \bmod p$. We have (12). Also, $u \equiv 1 \bmod p$ and $\chi_u = 0$, which means that the first order Taylor expansions are no longer sufficient. We shall use the second order expansion. Put $a = (q-1)/q$, so that $|a|_p \le p^{-1}$, and rewrite (12) as

$$\mu = (1-\zeta\lambda)R_{-a}(-\zeta\lambda)(1+\lambda)^{-1}R_a(\lambda). \tag{14}$$

For $p \ge 5$ we have

$$|\lambda|_p \le p^{-(p-2)/(p-1)} \le p^{-1/(p-3)},$$

which means that Proposition 3.1 applies to $\tau = \lambda$. We obtain

$$R_{-a}(-\zeta\lambda) = 1 + a\zeta\lambda + \frac{\zeta^2}{2}\, a\lambda^2 + O(a\lambda^3) + O(a^2\lambda^2),$$
$$R_a(\lambda) = 1 + a\lambda - \frac{a}{2}\,\lambda^2 + O(a\lambda^3) + O(a^2\lambda^2).$$

Substituting this into (14), we get

$$\begin{aligned}\mu &= (1-\zeta\lambda)\left(1 + a\zeta\lambda + \frac{a}{2}\,\zeta^2\lambda^2\right)(1+\lambda)^{-1}\left(1 + a\lambda - \frac{a}{2}\,\lambda^2\right)\\ &\quad + O(a\lambda^3) + O(a^2\lambda^2)\\ &= \left(1 + (-\zeta + a + a\zeta)\lambda - \frac{(1+\zeta)^2}{2}\, a\lambda^2\right)(1+\lambda)^{-1}\\ &\quad + O(a\lambda^3) + O(a^2\lambda^2).\end{aligned}$$

It follows that

$$\begin{aligned}\phi &= (1+\lambda)(\mu+\zeta)^q \\ &= \left(1+(-\zeta+a+a\zeta)\lambda - \frac{(1+\zeta)^2}{2}\,a\lambda^2 + \zeta(1+\lambda)\right)^q (1+\lambda)^{1-q} \\ &\quad + O(a\lambda^3) + O(a^2\lambda^2) \\ &= (1+\zeta)^q\left(1+a\lambda-\frac{1+\zeta}{2}\,a\lambda^2\right)^{1+a/(1-a)}(1+\lambda)^{-a/(1-a)} \\ &\quad + O(a\lambda^3)+O(a^2\lambda^2).\end{aligned}$$

Applying Proposition 3.1 with the exponents $\pm a/(1-a)$ and taking into account the inequality $|a|_p < 1$, we find

$$\begin{aligned}\left(1+a\lambda-\frac{1+\zeta}{2}\,a\lambda^2\right)^{a/(1-a)} &= 1+\frac{a^2}{1-a}\,\lambda+O(a^2\lambda^2), \\ (1+\lambda)^{-a/(1-a)} &= 1-\frac{a}{1-a}\,\lambda+\frac{a}{2(1-a)}\,\lambda^2+O(a\lambda^3) \\ &= 1-\frac{a}{1-a}\,\lambda+\frac{a}{2}\,\lambda^2+O(a\lambda^3)+O(a^2\lambda^2).\end{aligned}$$

Taking everything together, we obtain

$$\begin{aligned}\frac{\phi}{(1+\zeta)^q} &= \left(1+a\lambda-\frac{1+\zeta}{2}\,a\lambda^2\right)\left(1+\frac{a^2}{1-a}\,\lambda\right)\left(1-\frac{a}{1-a}\,\lambda+\frac{a}{2}\,\lambda^2\right) \\ &\quad + O(a\lambda^3)+O(a^2\lambda^2) \\ &= 1-\frac{\zeta}{2}\,a\lambda^2+O(a\lambda^3)+O(a^2\lambda^2) \\ &= 1-\frac{\zeta}{2(1-\zeta)^2}\,a(x-1)^2+O(a\lambda^3)+O(a^2\lambda^2).\end{aligned}$$

Now we complete the proof in the same fashion as in Section 6. Taking the norm, we find

$$\pm 1 = 1-\frac{1}{2}\,\mathrm{Tr}\left(\frac{\zeta}{(1-\zeta)^2}\right)a(x-1)^2+O(a\lambda^3)+O(a^2\lambda^2). \tag{15}$$

The -1 on the left is again impossible, and if we have 1, then, in view of Proposition 2.3, we must have the inequality

$$\begin{aligned}|x-1|_p^2 &\le \max\{|\lambda|_p^3, |a|_p|\lambda|_p^2\} \\ &= \max\{|x-1|_p^3\,p^{3/(p-1)}, |a|_p|x-1|_p^2\,p^{2/(p-1)}\},\end{aligned}$$

which means that either $|x-1|_p \ge p^{-3/(p-1)}$ or $|a|_p \ge p^{-2/(p-1)}$. But, for $p \ge 5$, neither of the latter inequalities can hold, because $|x-1|_p \le p^{-1}$ and $|a|_p \le p^{-1}$. The theorem is proved in the case $q \equiv 1 \bmod p$ as well.

Acknowledgments. I thank Yuri Bilu for helping me to polish the exposition, and for indicating and correcting a mistake in the previous version of the proof. I also thank Professor P. Mihăilescu for a useful discussion, and Professor A. Schinzel for a helpful suggestion.

References

[1] Y. Bilu, *Catalan's conjecture* (*after Mihăilescu*), Séminaire Bourbaki, Vol. 2002–2003, Exp. 909, Astérisque 294 (2004), 1–26.

[2] Y. Bilu, Y. Bugeaud and M. Mignotte, *The Problem of Catalan*, Springer, to appear.

[3] Y. Bugeaud et M. Mignotte, *L'équation de Nagell–Ljunggren* $(x^n-1)/(x-1)=y^q$, Enseign. Math. (2) 48 (2002), 147–168.

[4] J. W. S. Cassels, *On the equation* $a^x - b^y = 1$, *II*, Proc. Cambridge Philos. Soc. 56 (1960), 97–103; corrigendum, ibid. 57 (1961), 187.

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

[6] —, *On the class groups of cyclotomic extensions in presence of a solution to Catalan's equation*, J. Number Theory 118 (2006), 123–144.

[7] —, *New bounds and conditions for the equation of Nagell–Ljunggren*, J. Number Theory, to appear.

[8] T. Nagell, *Des équations indéterminées* $x^2+x+1=y^n$ *et* $x^2+x+1=3y^n$, Norsk Matem. Forenings Skrifter I, 2 (1921), 14 pp.; see also: *Collected Papers of Trygve Nagell*, ed. by P. Ribenboim, Vol. 1, Queen's Papers in Pure and Appl. Math. 121, Kingston, 2002, 79–94.

[9] L. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.

Institut de Mathématiques
Université Bordeaux 1
351 cours de la Libération
33405 Talence, France
E-mail: Benjamin.Dupuy@math.u-bordeaux1.fr

Received on 21.9.2006
and in revised form on 4.1.2007 (5279)