ACTA ARITHMETICA
XLV (1985)

On zeros of forms over local fields*

by

YISMAW ALEMU (Addis Abeba, Ethiopia)

1. Introduction. E. Artin conjectured that the field Q_p of p-adic numbers is C_2 for all p. The first counterexample to the conjecture has been given by G. Terjanian [7]. Recently G. I. Arkhipov and A. A. Karatsuba [1], [2] proved that Q_p is C_∞. By using a p-adic interpolation lemma based on the Lagrange interpolation formula their argument has been improved by D. J. Lewis and H. L. Montgomery [6]. Adapting the use of the Newton interpolation formula from [1] W. D. Brownawell ([3] and [4]) independently obtained a slightly sharper result.

In the present paper we use the methods of [4] and [6] to prove that also every finite extension of the field of p-adic numbers is C_∞.

Acknowledgement. I thank Doc. J. Browkin for valuable remarks. I have also profited from Prof. A. Schinzel's constructive comment on the thesis.

Suppose that K is a finite extension of Q_p with the ramification index e and the residue class degree f. Let O_K be the ring of integers of K and let π be a prime element of O_K. Denote $e' = e/(p-1)$. For any positive integer r let U_r be the group of one-units of level r, i.e.

$$U_r = 1+\pi^r O_K.$$

Denote by $v = v_\pi$ the normalized exponential valuation of K, i.e. $v(\pi) = 1$.

2. The interpolation lemma. Let $x = 1+y\pi^r \in U_r$, and consider the series

(1) $$f(x) = \sum_{m=0}^{\infty} \alpha_m (y\pi^r)^m, \qquad \alpha_m \in K.$$

Assume that

(2) $$v(\alpha_m) > -(m\varrho+\sigma), \qquad m = 0, 1, 2, \ldots,$$

for some $0 < \varrho < r$ and σ. Then the series (1) is convergent in U_r.

* The substance of this paper formed part of the author's Ph. D. Thesis, Warsaw University, 1983.

LEMMA 1. *Let $f(x)$ be given by series (1) satisfying (2). For $a \in U_r$, put*

$$f_1(x) = \frac{f(x)-f(a)}{x-a}.$$

Then

$$f_1(x) = \sum_{m=0}^{\infty} \alpha_{m,1} (y\pi^r)^m$$

for some $\alpha_{m,1} \in K$ satisfying

$$v(\alpha_{m,1}) > -((m+1)\varrho+\sigma), \quad m = 0, 1, 2, \ldots$$

Proof. Denote $a = 1+c\pi^r$. We have then

$$f_1(x) = \frac{1}{x-a} \sum_{k=1}^{\infty} \alpha_k \big((y\pi^r)^k - (c\pi^r)^k\big) = \sum_{k=1}^{\infty} \alpha_k \sum_{m=0}^{k-1} (y\pi^r)^m (c\pi^r)^{k-m-1}$$

$$= \sum_{m=0}^{\infty} \Big(\sum_{k=m+1}^{\infty} \alpha_k (c\pi^r)^{k-m-1}\Big)(y\pi^r)^m.$$

Therefore we can take

$$\alpha_{m,1} = \sum_{k=0}^{\infty} \alpha_{k+m+1} (c\pi^r)^k.$$

In view of (2) for $k \geqslant 0$ we have

$$v\big(\alpha_{k+m+1}(c\pi^r)^k\big) > -((k+m+1)\varrho+\sigma)+kr = -((m+1)\varrho+\sigma)+k(r-\varrho).$$

Therefore

$$v(\alpha_{m,1}) > -((m+1)\varrho+\sigma). \quad ■$$

LEMMA 2. *Let $f(x)$ be given by the series (1) satisfying (2). For $a_1, a_2, \ldots, a_n \in U_r$ define inductively:*

$$f_0(x) = f(x),$$

$$f_{i+1}(x) = \frac{f_i(x)-f_i(a_{i+1})}{x-a_{i+1}} \quad \textit{for} \quad i = 0, 1, \ldots, n-1.$$

Denote $b_i = f_i(a_{i+1})$ for $i = 0, 1, \ldots, n-1$.
Then

(3)
$$f(x) = b_0 + b_1(x-a_1) + b_2 \prod_{j=1}^{2}(x-a_j) + \ldots + b_{n-1}\prod_{j=1}^{n-1}(x-a_j) + f_n(x)\prod_{j=1}^{n}(x-a_j).$$

Moreover

(4)
$$v(f_n(1)) > -(\varrho n+\sigma).$$

Proof. The interpolation formula (3) follows easily by induction from the definition of $f_i(x)$ and b_i.

From Lemma 1 by induction it follows that

$$f_i(x) = \sum_{m=0}^{\infty} \alpha_{m,i} (y\pi^r)^m$$

for some $\alpha_{m,i} \in K$ satisfying $v(\alpha_{m,i}) > -(\varrho(m+i)+\sigma)$, $m = 0, 1, 2, \ldots$ In particular, since $f_n(1) = \alpha_{0,n}$, we have $v(f_n(1)) > -(\varrho n+\sigma)$. ■

For $x = 1+y\pi^r \in U_r$ and $w \in O_K$ we define

(5)
$$x^w = \sum_{m=0}^{\infty} \binom{w}{m} (y\pi^r)^m.$$

Since

(6)
$$v\left(\binom{w}{m}\right) \geqslant -v(m!) = -e'(m-s(m)) \geqslant -e'(m-1),$$

where $s(m)$ is the sum of digits of m when expressed in base p with respect to the least residue system mod p, the series (5) is convergent for $r > e'$.

COROLLARY. *Let $w_k, c_k \in O_K$ for $k = 1, 2, \ldots, N$ and consider*

(7)
$$f(x) = \sum_{k=1}^{N} c_k x^{w_k}, \quad \textit{where } x \in U_r,\ r > e'.$$

Then

$$v(f_n(1)) > -e'(n-1), \quad \textit{where } f_n(x) \textit{ is defined in Lemma 2.}$$

Proof. In view of (5) and (6) it is sufficient to put $\varrho = e'$, $\sigma = -e'$ in (2) and the corollary follows from Lemma 2.

Henceforth we assume that $r > e'$. Moreover let $m_1 < m_2 < \ldots < m_n$ be positive integers, and put

(8)
$$a_i = g^{m_i} \quad \text{for} \quad i = 1, 2, \ldots, n,$$

where $g = 1+a\pi^r$ with some $a \in K$ satisfying $v(a) = 0$.

LEMMA 3. (i) $v(g^{m_i}-1) = r+v(m_i)$,

(ii) $v\big(\prod_{i=1}^{k}(a_{k+1}-a_i)\big) \leqslant rk+e'(m_{k+1}-m_1)$ *for* $1 \leqslant k \leqslant n-1$.

Proof. Since $r > e'$, we have (cf. [5], p. 275)

$$v(g^{m_i}-1) = v(\log g^{m_i}) = v(m_i \log g) = v(m_i)+v(\log g) = r+v(m_i).$$

To prove (ii), we observe that in view of (i) for any k

$$v(a_{k+1}-a_i) = v(g^{m_{k+1}}-g^{m_i}) = v(g^{m_{k+1}-m_i}-1) = r+v(m_{k+1}-m_i).$$

Consequently

$$v\Big(\prod_{i=1}^{k}(a_{k+1}-a_i)\Big) = rk+v\Big(\prod_{i=1}^{k}(m_{k+1}-m_i)\Big)$$
$$\leqslant rk+v\big((m_{k+1}-m_1)!\big) \leqslant rk+e'(m_{k+1}-m_1). \ \blacksquare$$

3. Systems of congruences.

LEMMA 4. *Suppose that $f(x)$ defined by (7) with $c_1 = c_2 = \ldots = c_N = 1$ satisfies*

$$f(a_i) \equiv 0 \bmod \pi^m \quad \textit{for} \quad i = 1, 2, \ldots, n,$$

where a_i are given by (8).

Then, under the notations of Lemma 2,

(9) $$v(b_i) \geqslant m-ri-e'(m_{i+1}-m_1) \quad \textit{for} \quad i = 0, 1, \ldots, n-1.$$

Moreover

(10) $$v(N) \geqslant \min\{m,\ m+\lambda_1-e'(m_2-m_1),\ \ldots$$
$$\ldots,\ m+\lambda_{n-1}-e'(m_n-m_1),\ rn+\lambda_n-e'(n-1)\},$$

where $\lambda_i = \sum_{j=1}^{i} v(m_j)$ for $i = 1, 2, \ldots, n$.

Proof. Since $b_0 = f(a_1) \equiv 0 \bmod \pi^m$, (9) holds for $i = 0$. Assume that we have proved (9) for all $i < t \leqslant n-1$; we shall prove it for $i = t$. Since, in view of (3),

$$f(a_{t+1}) = b_0+b_1(a_{t+1}-a_1)+b_2\prod_{j=1}^{2}(a_{t+1}-a_j)+\ldots+b_t\prod_{j=1}^{t}(a_{t+1}-a_j),$$

we have

$$v\Big(b_t\prod_{j=1}^{t}(a_{t+1}-a_j)\Big)$$
$$\geqslant \min\Big\{m,\ v\big(b_1(a_{t+1}-a_1)\big),\ v\Big(b_2\prod_{j=1}^{2}(a_{t+1}-a_j)\Big),\ \ldots,\ v\Big(b_{t-1}\prod_{j=1}^{t-1}(a_{t+1}-a_j)\Big)\Big\}.$$

If the minimum is m, we have in view of Lemma 3(ii):

$$v(b_t) \geqslant m-v\Big(\prod_{j=1}^{t}(a_{t+1}-a_j)\Big) \geqslant m-rt-e'(m_{t+1}-m_1),$$

and hence (9) holds in this case for $i = t$.

If the minimum occurs at $v\big(b_k\prod_{j=1}^{k}(a_{t+1}-a_j)\big)$ for some $1 \leqslant k \leqslant t-1$, then by the inductive assumption and Lemma 3(ii) we have

$$v(b_t) \geqslant v(b_k)-v\Big(\prod_{j=k+1}^{t}(a_{t+1}-a_j)\Big)$$
$$\geqslant m-rk-e'(m_{k+1}-m_1)-r(t-k)-e'(m_{t+1}-m_{k+1})$$
$$= m-rt-e'(m_{t+1}-m_1).$$

Consequently (9) holds for $i = t$, and the proof of (9) is complete by induction.

To prove (10) we note that $N = f(1)$, since $c_1 = c_2 = \ldots = c_N = 1$ in (7). Consequently from (3), Corollary to Lemma 2, Lemma 3 and (9) it follows that

$$v\big(f(1)\big) \geqslant \min\Big\{v(b_0),\ v\big(b_1(1-a_1)\big),\ v\Big(b_2\prod_{j=1}^{2}(1-a_j)\Big),\ \ldots$$
$$\ldots,\ v\Big(b_{n-1}\prod_{j=1}^{n-1}(1-a_j)\Big),\ v\Big(f_n(1)\prod_{j=1}^{n}(1-a_j)\Big)\Big\}$$
$$\geqslant \min\{m,\ m+\lambda_1-e'(m_2-m_1),\ m+\lambda_2-e'(m_3-m_1),\ \ldots$$
$$\ldots,\ m+\lambda_{n-1}-e'(m_n-m_1),\ rn+\lambda_n-e'(n-1)\}$$

and this completes the proof of the lemma. ∎

For any natural number m set

(11) $$S_m(\boldsymbol{x}) = \sum_{i=1}^{N} x_i^m, \quad \text{where} \quad \boldsymbol{x} = (x_1, x_2, \ldots, x_N).$$

Let $\bar{e} = [e']+1$, and put $q = p^{\bar{e}-1}(p^f-1)$, where f is the residue class degree of the extension K/Q_p. Then $\bar{e} \leqslant q$. Let t be an integer satisfying $2 \leqslant t \leqslant 1+q/\bar{e}$.

THEOREM 1. *In the above notation if the system of congruences*

$$S_{qm_i}(\boldsymbol{x}) \equiv 0 \bmod \pi^{qM}, \quad i = 1, 2, \ldots, n$$

with natural numbers $m_1 < m_2 < \ldots < m_n$ in $[M, tM-1]$ has a nontrivial solution, then

$$v(N) \geqslant n(\bar{e}-e')+e'.$$

Proof. Without loss of generality we can assume that

$$x_i \not\equiv 0 \bmod \pi \quad \text{for} \quad i = 1, 2, \ldots, N.$$

Then, by the definition of q, $x_i^q \equiv 1 \bmod \pi^{\bar{e}}$, i.e. $x_i^q \in U_{\bar{e}}$ for $i = 1, 2, \ldots, N$.

The one-unit group of level $\bar{e}$, $U_{\bar{e}}$, considered as an O_K-module is cyclic (see [5], p. 275). Let $g = 1+a\pi^{\bar{e}}$, with $v(a) = 0$, be a generator of this group.

Put

$$x_i^q = g^{w_i}, \quad i = 1, 2, \ldots, N$$

with $w_i \in O_K$, and let

$$f(x) = \sum_{i=1}^{N} x^{w_i}.$$

With $a_k = g^{m_k}$, $k = 1, 2, \ldots, n$, we have

$$f(a_k) = \sum_{i=1}^{N} (g^{m_k})^{w_i} = \sum_{i=1}^{N} (g^{w_i})^{m_k} = \sum_{i=1}^{N} x_i^{qm_k} \equiv 0 \bmod \pi^{qM}.$$

Since $\lambda_i \geqslant 0$, $m_j - m_1 \leqslant (t-1)M-1$, $q \geqslant (t-1)\bar{e}$ and $(t-1)M \geqslant n$ we have

$$qM + \lambda_i - e'(m_{i+1} - m_1) \geqslant (t-1)\bar{e}M - e'((t-1)M-1)$$
$$= (t-1)M(\bar{e}-e') + e' \geqslant n(\bar{e}-e') + e',$$

and similarly

$$\bar{e}n + \lambda_n - e'(n-1) \geqslant n(\bar{e}-e') + e'.$$

Consequently from inequality (10) we obtain the result. ∎

4. Main result. Let $A > 1$ be a fixed real number and define $\varepsilon_A(x)$, for $x > 1$, to be the least positive integer r such that the r times iterated logarithm $\log_A^{(r)} x$ is less than 1. Furthermore let

$$\lambda_A(x) = \prod_{k=1}^{\varepsilon_A(x)-1} \log_A^{(k)} x \quad \text{for} \quad x > 1.$$

From the definition it follows that ε_A and λ_A are non-decreasing functions.

We need two lemmas.

LEMMA 5. *For every $A > 1$ there exists $c = c(A)$ such that for $n > c$ the inequalities $A^n > n$ and $A^{n+2} > A^n + 1$ hold.*

Proof. Clear. ∎

LEMMA 6. *For $A > 1$ let $c = c(A)$ be the constant of Lemma 5. Put $n_1 > c$ and define inductively*

$$(12) \qquad n_k = [A^{n_{k-1}}] + 1 \quad \textit{for } k = 2, 3, \ldots$$

Then the sequence $\{n_k\}_{k=1}^{\infty}$ is strictly increasing. Moreover

$$\varepsilon_A(n_k) \geqslant k \quad \textit{and} \quad \lambda_A(n_k) \geqslant n_1 n_2 \ldots n_{k-1}.$$

Proof. From (12) and Lemma 5 it follows that

$$n_k > A^{n_{k-1}} > n_{k-1} \quad \text{for } k = 2, 3, \ldots$$

Consequently $\log_A n_k > n_{k-1}$, and hence by induction

$$(13) \qquad \log_A^{(i)} n_k > n_{k-i} \quad \text{for} \quad 1 \leqslant i < k.$$

Therefore

$$\varepsilon_A(n_k) \geqslant (k-1) + \varepsilon_A(n_1) \geqslant k.$$

Moreover, in view of (13), we have

$$\lambda_A(n_k) = \prod_{i=1}^{\varepsilon_A(n_k)-1} \log_A^{(i)} n_k \geqslant \prod_{i=1}^{k-1} n_{k-i}. \ ∎$$

THEOREM 2. *Suppose that K is a finite extension of Q_p with the ramification index e and the residue class degree f, and let O_K be the ring of integers of K. For infinitely many d there exists a form F in $O_K[x_1, x_2, \ldots, x_n]$ of degree d without a nontrivial zero* mod π^d *with*

$$n > \exp \frac{Cd}{\lambda_A(d) \cdot (3q)^{\varepsilon_A(d)}},$$

where

$$A = p^{1/2e(p-1)}, \quad q = p^{\bar{e}-1}(p^f - 1), \quad \bar{e} = \left[\frac{e}{p-1}\right] + 1$$

and C is a positive constant explicitly given below.

Proof. For $A = p^{1/2e(p-1)}$ let $c = c(A)$ be the constant of Lemma 5. Take a positive integer t such that $n_1 := p^t(p^f-1)(p-1) > c$ and put $d_1 = p^t(p^f - 1)$. Consider the form

$$F_1(x) = \sum_{i=1}^{p-1} x_i^{d_1} + \pi \sum_{i=p}^{2p-2} x_i^{d_1} + \ldots + \pi^{d_1-1} \sum_{i=n_1+2-p}^{n_1} x_i^{d_1}.$$

Applying the usual argument one shows that

$$F_1(x) \equiv 0 \bmod \pi^{d_1}$$

has no nontrivial solution in O_K.

For $k \geqslant 2$ we define inductively a form F_k in terms of F_{k-1}. Put $M = n_{k-1}$, the number of variables of F_{k-1}, and let

$$n_k = [A^M] + 1, \quad \text{where} \quad A = p^{1/2e(p-1)}.$$

In view of Lemma 5 the sequence $\{n_k\}_{k=1}^{\infty}$ is strictly increasing.

Define

$$F_k(x) = F_{k-1}(u),$$

where $x = (x_1, x_2, \ldots, x_{n_k})$ and $u = (u_1, u_2, \ldots, u_M)$ is given by

(14) $$u_m(x) = S_{q(M+m-1)}(x) \cdot S_{q(2M-m)}(x), \quad m = 1, 2, \ldots, M,$$

where $S_t(x)$ is defined by (11) with $N = n_k$.

Then $u_m(x)$ is a form of degree $(3M-1)q$ in n_k variables. Consequently $F_k(x)$ is a form of degree $d_k = (3M-1)qd_{k-1}$, where d_{k-1} is the degree of F_{k-1}, in n_k variables.

We now show by induction on k that

(15) *if* $F_k(x) \equiv 0 \bmod \pi^{d_k}$, *then* $x \equiv 0 \bmod \pi$.

Since (15) is true for F_{k-1}, it follows that

$$v(F_k(x)) = v(F_{k-1}(u)) \leqslant d_{k-1} \cdot \min_{1 \leqslant m \leqslant M} \{v(u_m(x))\} + d_{k-1} - 1.$$

But $v(F_k(x)) \geqslant d_k = (3M-1)q \cdot d_{k-1}$ by assumption.

Therefore, for $1 \leqslant m \leqslant M$,

(16) $$v(u_m(x)) \geqslant (3M-1)q.$$

Let $\mathcal{M}$ be the set of natural numbers $m \in \{1, 2, \ldots, M\}$ satisfying

(17) $$S_{q(M+m-1)}(x) \equiv 0 \bmod \pi^{qM}.$$

Since $M \geqslant 1$, from (14), (16) and (17), we have either m or $M+1-m$ belongs to $\mathcal{M}$. Therefore card $\mathcal{M} \geqslant M/2$.

From Theorem 1 with $t = 2$ it follows that the system (17) has a nontrivial solution only if

$$v(n_k) \geqslant (M+2)/2(p-1).$$

Hence $n_k \geqslant A^{M+2}$. But from the definition of n_k we have $n_k \leqslant A^M + 1$. In view of Lemma 5 we obtain a contradiction. Consequently $x \equiv 0 \bmod \pi$, and (15) holds for all k.

From the relation $d_k = (3n_{k-1} - 1)qd_{k-1}$, $k = 2, 3, \ldots$, it follows that

$$n_{k-1} < d_k < (3q)^{k-1} d_1 n_1 n_2 \ldots n_{k-1} \quad \text{for } k = 2, 3, \ldots$$

Hence

$$\lambda_A(d_k) \geqslant \lambda_A(n_{k-1}) \quad \text{and} \quad \varepsilon_A(d_k) \geqslant \varepsilon_A(n_{k-1}).$$

Consequently, in view of Lemma 6, we have

$$\frac{d_k}{\lambda_A(d_k)(3q)^{\varepsilon_A(d_k)}} \leqslant \frac{d_k}{n_1 n_2 \ldots n_{k-2}(3q)^{k-1}} < d_1 n_{k-1} < d_1 \log_A n_k.$$

Hence

$$n_k > \exp \frac{Cd_k}{\lambda_A(d_k)(3q)^{\varepsilon_A(d_k)}} \quad \text{with} \quad C = \frac{\log A}{d_1}. \ \blacksquare$$

Corollary. *If K is a finite extension of Q_p then K is C_∞.*

References

[1] Г. И. Архипов, А.А. Карацуба, *О локальном представлении нуля формой*, Изв. АН СССР, Сер. Мат. 45 (1981), pp. 948–961.

[2] —,— *О представлении нуля формой в поле p-адических чисел*, Доклады АН СССР 262 (1982), pp. 11–13.

[3] W. Dale Brownawell, *Big counterexamples to Artin conjecture*, Abstracts of AMS 3 (1982), 797–10–177, p. 416.

[4] — *On p-adic-zeros of forms*, to appear in J. Number Theory.

[5] H. Hasse, *Number Theory*, Springer-Verlag, Berlin, Heidelberg, New York 1980.

[6] D. J. Lewis and H. L. Montgomery, *On zeros of p-adic forms*, Michigan Math. J. 30 (1983), pp. 83–87.

[7] G. Terjanian, *Un contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci., Paris, Ser. A, 262 (1966), p. 612.

DEPARTMENT OF MATHEMATICS
ADDIS ABEBA UNIVERSITY
Ethiopia

Received on 20.12.1983
and in revised form on 2.3.1984 (1390)