[7] G. Halász, *On the distribution of additive and mean values of multiplicative functions*, Acta Math. Acad. Sci. Hungar. 6 (1971), pp. 211–233.
[8] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, New York 1974.
[9] — — *On a result of R. R. Hall*, J. Number Theory (1) 11 (1979), pp. 76–89.
[10] R. R. Hall, *Halving an estimate obtained from Selberg's upper bound method*, Acta Arith. 25 (1974), pp. 347–351.
[11] A. Hildebrand, *Quantitative mean value theorems for nonnegative multiplicative functions I*, J. London Math. Soc. 30 (1985), pp. 394–406.
[12] J. Pintz, *Elementary methods in the theory of L-functions II*, Acta Arith. 31 (1976), pp. 273–289.
[13] A. Selberg, *Note on a paper by L. G. Sathe*, J. Indian Math. Soc. 18 (1954), pp. 83–87.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
Urbana, Illinois 61801, U.S.A.

Received on 15. 10. 1984
and in revised form on 10. 12. 1985 (1462)

ACTA ARITHMETICA
XLVIII (1987)

On zeros of diagonal forms over p-adic fields

by

YISMAW ALEMU (Addis Ababa)

1. Introduction. Let K be a finite extension of Q_p, the rational p-adic field, and O_K be its ring of integers. Assume that e and f are respectively the ramification index and residue class degree of the extension K/Q_p so that $n = ef = [K:Q_p]$. Let $\mathfrak{p}$ be the prime ideal of O_K and π a generator of the ideal. Unless indicated to the contrary, v denotes the normalized exponential valuation of K arising from the prime ideal (π).

Half a century ago, Artin conjectured that any homogeneous polynomial over K of degree k in at least k^2+1 variables represents (has a non-trivial) zero in K. This conjecture has drawn the attention of many authors (for details see the reference pages of [8], [9] and [10]).

Call a field L C_i if every form over L of degree k in at least k^i+1 variables represents zero in L. Given k, a field L is called $C_i(k)$ if every form over L of degree k in at least k^i+1 variables represents zero in L. In connection with Artin's conjecture, for any number field L, Ax and Kochen [2] have shown that:

$A(k, L) = \{\mathfrak{p}|\ \mathfrak{p}$ is a prime ideal of L such that $L_\mathfrak{p}$ is not $C_2(k)\}$, $L_\mathfrak{p}$ being the completion of L under $\mathfrak{p}$, is a finite set. In this sense, we can say that Artin's conjecture is almost true. On the negative side, the present author [1] has generalized the recent counterexamples to show that K, any finite extension of Q_p, for any p, is C_∞. The counterexamples obtained to Artin's conjecture have a common feature: the degrees of the forms are divisible by $p-1$ and powers of p. In view of this and the striking result of Ax and Kochen, it seems natural, to study Artin's conjecture in the following form.

CONJECTURE. *For a number field L and a natural number k, $\mathfrak{p} \in A(k, L)$ only if p and $p-1$ divide k, where p is the characteristic of the residue class field of $L_\mathfrak{p}$.*

Time will tell the validity of this conjecture.

In the present paper, we study the problem of diagonal forms over K, a finite extension of Q_p. Let k be a natural number. Let $\Gamma^*(k, \pi)$ denote the least s for which the congruence:

$$F = a_1 x_1^k + a_2 x_2^k + \ldots + a_s x_s^k \equiv 0 \pmod{\pi^t} \tag{1}$$

where $a_1, a_2, \ldots, a_s$ are arbitrary non-zero p-adic integers, has a non-trivial solution (i.e. not all x_i divisible by π), for any natural number t. It is well known that $\Gamma^*(k, \pi)$ is the minimum number of variables sufficient for F to represent zero in K. If $v(k) = 0$, a combination of Chevalley's theorem on finite fields and Hensel's Lemma proves that $\Gamma^*(k, \pi) \leqslant k^2+1$. The difficulty arises when $v(k) > 0$, which we assume henceforth. As the case $k = 2$ is well known (see [9], p. 126), we also assume that $k > 2$.

We need to define one more auxiliary function. For a fixed natural number t, $\gamma^*(k, \pi^t)$ denotes the least s for which the congruence

$$F = a_1 x_1^k + a_2 x_2^k + \ \ldots \ + a_s x_s^k \equiv 0 \ (\mathrm{mod}\, \pi^t) \tag{2}$$

where, now $a_1, a_2, \ldots, a_s$ are p-adic units, has a non-trivial solution.

If $K = Q_p$, Davenport and Lewis [5] have shown that $\Gamma^*(k, p) \leqslant k^2+1$ with equality if $k+1 = p$ (for further developments, see [7]). Thus, Artin's conjecture for such forms over Q_p holds. To the best of the author's knowledge, Artin's conjecture for diagonal forms over $K \neq Q_p$, is neither proved nor disproved. There are certain difficulties to generalize the argument of Davenport and Lewis. In the first place one of their crucial lemmas (Lemma 1) is not in general true. Even in the cases where this lemma holds, the method does not yield the conjectured bound.

Recently Dodson [8] showed that

$$\Gamma^*(k, \pi) < 16n^2 (\log k)^2 k^2; \quad n = ef.$$

In the present paper, we prove

THEOREM 1. *If $p \geqslant 3$, then*

$$\Gamma^*(k, \pi) \leqslant \max\{3nk^2 - nk + 1, 2k^3 - k^2\}.$$

If $p = 2$, then

$$\Gamma^*(k, \pi) \leqslant 4nk^2 - nk + 1.$$

We use a result of Olson [11] on finite Abelian p-groups and a lemma of Browkin [4]. The method employed seems more natural, but even in the p-adic case, it does not yield the best possible bound obtained by Davenport and Lewis.

2. Basic lemmas. We first need to generalize Hensel's lemma. Let $\bar{e}$ denote $\left[\frac{e}{p-1}\right]+1$.

LEMMA 1. *Let M be a non-negative integer. Assume that $f(x) \in O_K[x]$ is of degree k and $\{a_n\}_{n=0}^{\infty}$ is a sequence given by*

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

satisfying:

$$f(a_0) \equiv 0 \ (\mathrm{mod}\, \pi^{M+\bar{e}}), \tag{2.1}$$

and for any $n = 0, 1, 2, \ldots$:

$$f^{(i)}(a_n) \equiv 0 \ (\mathrm{mod}\, \pi^M), \tag{2.2}$$

$$f^{(i)}(a_n) \not\equiv 0 \ (\mathrm{mod}\, \pi^{M+1}), \quad i = 1, 2, 3, \ldots, k. \tag{2.3}$$

Then there exists $\xi \in O_K$ such that

$$\xi \equiv a_0 (\mathrm{mod}\, \pi^{\bar{e}}) \quad \text{and} \quad f(\xi) = 0.$$

Proof. For any $a \in O_K$, let

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \ \ldots \ + \frac{f^{(k)}(a)}{k!}(x-a)^k$$

where $k =$ degree of f, be the Taylor's expansion of f at a.

For each $n = 0, 1, 2, \ldots$, let $t_n = M + \bar{e} + n$. We shall first prove that for each integer n,

$$f(a_n) \equiv 0 \ (\mathrm{mod}\, \pi^{t_n}) \tag{2.4}$$

and

$$a_{n+1} \equiv a_n \ (\mathrm{mod}\, \pi^{n+\bar{e}}). \tag{2.5}$$

By assumption, (2.4) is true for $n = 0$. Hence, we can proceed to prove (2.4) by induction on n. Using the Taylor's expansion of f and the definition of the sequence $\{a_n\}_{n=0}^{\infty}$ we have

$$\begin{aligned} f(a_n) &= f(a_{n-1}) + f'(a_{n-1})(a_n - a_{n-1}) + \ \ldots \ + \frac{f^{(k)}(a_{n-1})}{k!}(a_n - a_{n-1})^k \\ &= f(a_{n-1}) + f'(a_{n-1})\left(\frac{-f(a_{n-1})}{f'(a_{n-1})}\right) + \ \ldots \ + \frac{f^{(k)}(a_{n-1})}{k!}\left(\frac{-f(a_{n-1})}{f'(a_{n-1})}\right)^k \\ &= \frac{f''(a_{n-1})}{2!}\left(\frac{-f(a_{n-1})}{f'(a_{n-1})}\right)^2 + \ \ldots \ + \frac{f^{(k)}(a_{n-1})}{k!}\left(\frac{-f(a_{n-1})}{f'(a_{n-1})}\right)^k. \end{aligned}$$

Using (2.2), (2.3) and the induction assumption on $f(a_{n-1})$, for any $i \in \{2, 3, \ldots, k\}$,

$$v\left(\frac{f^{(i)}(a_{n-1})}{i!}\left(\frac{-f(a_{n-1})}{f'(a_{n-1})}\right)^i\right) \geqslant M + i(t_{n-1} - M) - e \cdot \frac{i - s(i)}{p-1}$$

where $s(i)$ is the sum of the digits of i when i is written in base p with respect to the least residue system mod p. To prove (2.4) for n, it suffices to show that, for any $i \in \{2, 3, \ldots, k\}$,

$$M + i(t_{n-1} - M) - e \cdot \frac{i - s(i)}{p-1} > t_{n-1}. \tag{2.6}$$

But this last inequality is equivalent to

$$t_{n-1} > M + e \cdot \frac{i - s(i)}{(p-1)(i-1)}.$$

Since $s(i) \geqslant 1$, it is evident that

$$e \cdot \frac{i - s(i)}{(p-1)(i-1)} \leqslant \frac{e}{p-1} < \bar{e}$$

and as $t_{n-1} \geqslant t_0 = M + \bar{e}$, the inequality (2.6) holds. The inductive proof verifies the assertion in (2.4).

The proof of (2.5) is now immediate from the definition of the sequence, (2.3) and (2.4).

Since we are working with a Cauchy sequence in a complete field and f is continuous, we have

$$0 = \lim_{n \to \infty} f(a_n) = f(\lim_{n \to \infty} a_n) = f(\xi)$$

and $\xi \equiv a_0 \pmod{\pi^{\bar{e}}}$. This completes the proof of Lemma 1.

Remark 1. Let $k = p^m k_0$, with $(p, k_0) = 1$, and recall the notions introduced in the introduction. Suppose that

$$f(x) = b_1 x^k + b_2 \in O_K[x] \tag{3}$$

with $v(b_1) = 0$. Assume that there exists $a_0 \in O_K$ such that $b_1 a_0^k + b_2 \equiv 0 \pmod{\pi^{em+\bar{e}}}$ and $v(a_0) = 0$. It is clear that for any $c \in O_K$,

$$f^{(i)}(c) \equiv 0 \pmod{\pi^{em}} \quad \text{for} \quad i = 1, 2, \ldots, k,$$

and

$$f'(c) \not\equiv 0 \pmod{\pi^{em+1}}$$

provided $v(c) = 0$; in particular for any element of the sequence $\{a_n\}_{n=0}^{\infty}$ as defined in Lemma 1 using a_0. Hence by the lemma, f has a non-trivial zero.

When working with a diagonal form over O_K, to assert the existence of a non-trivial zero of the form, it evidently suffices to construct a polynomial of type (3) from the given form.

We need to formulate a group theoretic lemma. Suppose that G is a finite Abelian group, written additively. Define

$$s = s(G)$$

to be the smallest positive integer such that every sequence in G with at least s elements has a non-empty subsequence whose sum equals 0, the identity of the group. It is clear that $s(G) \leqslant |G|$, with equality if G is cyclic. In general the explicit value of $s(G)$ is not known but for p-groups, Olson [11] (see also [13]), obtained the following.

LEMMA 2. *Let G be a finite Abelian p-group with invariants $p^{e_1}, p^{e_2}, \ldots, p^{e_r}$. Then*

$$s(G) = 1 + \sum_{i=1}^{r} (p^{e_i} - 1).$$

3. Different bounds for $\Gamma^*(k, \pi)$. With our standing notations, let F be a diagonal form over O_K of degree k. F can be normalized as

$$F = F_0 + \pi F_1 + \ldots + \pi^{k-1} F_{k-1}, \tag{4}$$

where F_i is a diagonal form of degree k in r_i variables whose coefficients are units of O_K, F_i and F_j $(i \neq j)$ do not have common variables so that $s = r_0 + \ldots + r_{k-1}$, the number of variables of F. There are other possible normalizations that can further be applied to F, but for the moment, we evidently can assume that $r_0 \geqslant r_i$, $i = 0, 1, 2, \ldots, k-1$.

Recall that

$$k = p^m k_0, \quad \text{with} \quad (p, k_0) = 1 \text{ and } m \geqslant 1.$$

We have defined $\gamma^*(k, \pi^{em+\bar{e}})$ as the least number of variables of F_0 such that

$$F_0 \equiv 0 \pmod{\pi^{em+\bar{e}}}$$

has a non-trivial zero; which by Lemma 1 is equivalent to saying that F_0 represents zero in K.

3.1. Some known bounds of $\gamma^*(k, \pi^{em+\bar{e}})$ and $\Gamma^*(k, \pi)$. It is obvious that

$$\Gamma^*(k, \pi) \leqslant (\gamma^*(k, \pi^{em+\bar{e}}) - 1)k + 1. \tag{5}$$

Since

$$|O_K / \pi^{em+\bar{e}} O_K| = p^{efm+f\bar{e}},$$

if $r_0 \geqslant p^{efm+f\bar{e}}$, by using $\{a_1, a_1 + a_2, \ldots, a_1 + a_2 + \ldots + a_{r_0}\}$ where $a_1, a_2, \ldots, a_{r_0}$ are the coefficients of F_0, the well-known box argument guarantees that

$$F_0 \equiv 0 \pmod{\pi^{em+\bar{e}}}$$

has a solution with some $x_i = 1$. Hence,

$$\gamma^*(k, \pi^{em+\bar{e}}) \leqslant p^{efm+f\bar{e}}.$$

CLAIM: $p^{efm+f\bar{e}} \leqslant k^{2ef}$.

Indeed,

$$p^{em+\bar{e}} \leqslant k^{2e}$$

since when $p \neq 2$, $\bar{e} < e$ so that

$$p^{em+\bar{e}} \leqslant k^e k^{\bar{e}/m} \leqslant k^{2e};$$

and when $p=2$, $\bar{e}=e+1$ and $k=2^m t$, so that

$$p^{em+\bar{e}} = 2^{e(m+1)+1} \leqslant k^e \cdot 2^{e+1} \leqslant k^{2e}.$$

Hence

$$p^{efm+f\bar{e}} \leqslant k^{2ef}$$

and the claim is established.

Using $\gamma^*(k, \pi^{em+\bar{e}}) \leqslant p^{efm+f\bar{e}}$ and the above claim, we have

$$\Gamma^*(k, \pi) \leqslant (p^{efm+f\bar{e}}-1)k+1 \leqslant k^{2ef+1}-k+1 = k^{2n+1}-k+1.$$

Observe this bound when $K=Q_p$. The above upper bound for $\Gamma^*(k, \pi)$ is better than $4k^{2n+3}+1$ which was given by Peck [12]. Actually the recent result of Dodson [8] shows that:

$$\Gamma^*(k, \pi) < 16n^2(\log k)^2 k^2.$$

Indeed, the often large exponent of k that appears in the estimate of Peck can actually be made a factor. If n is large compared to the degree, the bounds we obtain are better than the result given by Dodson. However, I have been unable to give a reasonably good bound of $\Gamma^*(k, \pi)$ which only depends on k. Birch [3] has shown that

$$\Gamma^*(k, \pi) < (2m+3)^k (d^2 k)^{k-1}, \quad d=(k, p^f-1)$$

but this seems very far from the truth for large k.

3.2. The additive structure of $O_K/\pi^t O_K$ and its consequence. Let t be any natural number and put

$$t = qe+r, \quad 0 \leqslant r < e.$$

Assume that $w_1, w_2, \ldots, w_f$ is an integral basis of the maximal unramified subfield of K. It is well known that

$$B = \{w_i \pi^j : 1 \leqslant i \leqslant f, 0 \leqslant j < e\} \tag{6}$$

is an integral basis of K over Q_p.

To determine the additive structure of the p-group, $G_t = O_K/\pi^t O_K$, we distinguish two cases:

Case 1. $r=0$. In this case, it is easy to see that each of the elements of B is of order p^q. Moreover, if we denote the cyclic group generated by $w_i \pi^j$ by C_{ij}, since B is an integral basis of K/Q_p, the group

$$G_t \simeq \bigoplus_{\substack{1 \leqslant i \leqslant f \\ 0 \leqslant j < e}} C_{ij}.$$

Hence G_t is a direct sum of ef cyclic groups of order p^q.

Case 2. Assume that $r>0$. In this case, the rf elements of

$\{w_i \pi^j : 1 \leqslant i \leqslant f, 0 \leqslant j < r\}$ are each of order p^{q+1} while the elements of $\{w_i \pi^j : 1 \leqslant i \leqslant f, r \leqslant j < e\}$ are each of order p^q. Hence, with a similar reasoning as above, G_t is a direct sum of rf cyclic groups of order p^{q+1} and $(e-r)f$ cyclic groups or order p^q.

For an easier reference, we document the above as

LEMMA 3. *G_t is isomorphic to a direct sum of rf cyclic groups of order p^{q+1} and $(e-r)f$ cyclic groups of order p^q. Moreover,*

$$s_t = s(G_t) = rfp^q(p-1)+ef(p^q-1)+1.$$

Let us particularize Lemma 3 for $t=em+\bar{e}$. If $p=2$ then

$$s_t = f\big((e+1)2^{m+1}-e\big)+1. \tag{7}$$

Otherwise, it is easy to see that

$$s_t = \begin{cases} ef(p^{m+1}-1)+1 & \text{if } e=1 \text{ or } (p=3 \text{ and } e=2), \\ \bar{e}fp^m(p-1)+ef(p^m-1)+1 & \text{otherwise.} \end{cases} \tag{8}$$

Unless stated to the contrary, in the discussions to follow s_t denotes $s_{em+\bar{e}}$, $em=v(k)$, as explicitly given by (7) or (8).

COROLLARY 1. $\gamma^*(k, \pi^{em+\bar{e}}) \leqslant s_t$.

Proof. Let $\{a_1, a_2, \ldots, a_{r_0}\}$ be the coefficients of F_0 with $r_0 \geqslant s_t$. By Lemma 3 and Lemma 2, there exists a subsequence, say $a_{i_1}, a_{i_2}, \ldots, a_{i_n}$ such that

$$\sum_{j=1}^{n} a_{i_j} \equiv 0 \pmod{\pi^{em+\bar{e}}}.$$

Put

$$x_g = \begin{cases} 1 & \text{if } g \in \{i_1, i_2, \ldots, i_n\}, \\ 0 & \text{otherwise} \end{cases}$$

and let x be the r_0-tuple whose coordinates are 0's and 1's as chosen above. Then

$$F_0(x) \equiv 0 \pmod{\pi^{em+\bar{e}}}.$$

An application of Lemma 1, completes the proof of the corollary.

It is now immediate from (5), the normalization of F as (4) and Corollary 1, that

$$\Gamma^*(k, \pi) \leqslant (s_t-1)k+1. \tag{9}$$

In general, the bound $(\gamma^*(k, \pi^{em+\bar{e}})-1)k+1$ for $\Gamma^*(k, \pi)$ is far from the value of $\Gamma^*(k, \pi)$. This is obviously so since one does not essentially use the variables in F_i, $i \geqslant 1$, when giving this bound for $\Gamma^*(k, \pi)$. If $e \geqslant k+\bar{e}$, Theorem 2 below gives a bound for $\Gamma^*(k, \pi)$ better than that of (9).

Let $k+em+\bar{e}-1 = qe+r,\ 0 \leqslant r < e.$

LEMMA 4. *If F is a diagonal form of degree k in s variables and $s \geqslant rfp^q(p-1)+(e-r)f(p^q-1)+1$, then F represents zero in O_K.*

Proof. Using Lemma 3,

$$s(O_K/\pi^{k+em+\bar{e}-1}O_K) = rfp^q(p-1)+(e-r)f(p^q-1)+1.$$

From the hypothesis on the number of variables of F and Lemma 2, there is a subset of the set of coefficients of F, say $\{a_{i_1}, a_{i_2}, \ldots, a_{i_n}\}$ such that

$$\sum_{j=1}^{n} a_{i_j} \equiv 0 \pmod{\pi^{k+em+\bar{e}-1}}.$$

Set

$$x_g = \begin{cases} 1 & \text{if } g \in \{i_1, i_2, \ldots, i_n\}, \\ 0 & \text{otherwise} \end{cases}$$

and let $\boldsymbol{x}$ be the s-tuple whose coordinates are 0's and 1's as chosen above. Then

$$F(\boldsymbol{x}) \equiv 0 \pmod{\pi^{k+em+\bar{e}-1}}.$$

We note that $0 \leqslant v(a_{i_j}) \leqslant k-1$ for $j = 1, 2, \ldots, n$. Hence for any $i_j \in \{i_1, i_2, \ldots, i_n\}$,

$$\frac{\partial F}{\partial x_{i_j}}(\boldsymbol{x}) \not\equiv 0 \pmod{\pi^{k+em}}.$$

Moreover,

$$\frac{\partial F}{\partial x_{i_j}}(\boldsymbol{x}) \equiv 0 \pmod{\pi^{v(a_{i_j})+em}}$$

with $k+em+\bar{e}-1-v(a_{i_j})-em \geqslant \bar{e}$ for each $i_j \in \{i_1, \ldots, i_n\}$.

Lemma 1 shows that F represents zero in O_K.

THEOREM 2. *If $k+\bar{e} \leqslant e$, then*

$$\Gamma^*(k, \pi) \leqslant (k+\bar{e}-1)fp^m(p-1)+(e-k-\bar{e}+1)f(p^m-1)+1.$$

Proof. In Lemma 4,

$$q = \left[\frac{k+\bar{e}-1}{e}+m\right]$$

where $[x]$ is the largest integer not exceeding x.

If $k+\bar{e} \leqslant e$, then $\left[\frac{k+e-1}{e}+m\right] = m$. Hence it is immediate from the lemma that

$$\Gamma^*(k, \pi) \leqslant (k+\bar{e}-1)fp^m(p-1)+(e-k-\bar{e}+1)f(p^m-1)+1.$$

This bound can be shown to be better than that of (9).

As is well known, when k is odd, the number of variables sufficient for F to represent zero is much less. The usual estimate for $\Gamma^*(k, \pi)$ is based on the inequality (5) but it is more effective to argue directly as follows.

THEOREM 3. *If k is odd and $m \geqslant 1$, then*

$$\Gamma^*(k, \pi) \leqslant \left[\frac{f(k+e+\bar{e}-1)\log k}{\log 2}\right]+2.$$

Proof. Let F be a diagonal form of type

$$\sum_{i=1}^{s} a_i x_i^k$$

with

$$s \geqslant \left[\frac{f(k+e+\bar{e}-1)\log k}{\log 2}\right]+2 \quad \text{and} \quad 0 \leqslant v(a_i) \leqslant k-1,\ i = 1, 2, \ldots, s.$$

Evidently it suffices to show that $F \equiv 0 \pmod{\pi^{k+em+\bar{e}-1}}$ has a non-trivial solution. For this, consider all possible sums of non-empty subsets of $A = \{a_1, a_2, \ldots, a_s\}$. We have 2^s-1 such subsets. If one of these sums is $0 \pmod{\pi^{k+em+\bar{e}-1}}$, we work with it. Otherwise if

$$2^s-1 \geqslant |O_K/\pi^{k+em+\bar{e}-1}O_K| = p^{f(k+em+\bar{e}-1)},$$

by the box principle, there exist two different subsets B_1 and B_2 of A such that

$$\sum_{b \in B_1} b \equiv \sum_{b \in B_2} b \pmod{\pi^{k+em+\bar{e}-1}}.$$

If necessary by eliminating elements of B_1 and B_2 with the same indices, we can assume that B_1 and B_2 are disjoint (in the sense that their elements have different indices).

Put

$$x_i = \begin{cases} 1 & \text{if } i \text{ is an index of an element in } B_1, \\ -1 & \text{if } i \text{ is an index of an element in } B_2, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$F(\boldsymbol{x}) = \sum_{b \in B_1} b - \sum_{b \in B_2} b \equiv 0 \pmod{\pi^{k+em+\bar{e}-1}}.$$

Hence F represents zero provided $2^s-1 \geqslant p^{f(k+em+\bar{e}-1)}$. On the other hand

$$2^s-1 \geqslant p^{f(k+em+\bar{e}-1)}$$

holds if

$$s \geqslant \frac{f(k-em+\bar{e}-1)\log p}{\log 2}+1.$$

Hence

$$\begin{aligned}\Gamma^*(k,\pi) &\leqslant \left[\frac{f(k+em+\bar{e}-1)\log p}{\log 2}\right]+2\\ &\leqslant \left[\frac{f(k+em+\bar{e}-1)\log k}{\frac{m}{\log 2}}\right]+2\\ &\leqslant \left[\frac{f(k+e+\bar{e}-1)\log k}{\log 2}\right]+2\end{aligned}$$

as asserted in the theorem.

Another bound of $\Gamma^*(k,\pi)$ is obtainable from the following lemma, due to Browkin [4] and whose generalization will be discussed elsewhere.

LEMMA 5. *Let* $F \in O_K[x_1, x_2, \ldots, x_s]$ *be a form of degree* k *and let*

$$s > \begin{cases} kt, & \text{if } t \leqslant e,\\ ke(1+p+p^2+\ \ldots\ +p^{m-1})+k(e_1+1)p^m, & \text{if } t > e,\end{cases}$$

where $t-1 = me+e_1$ *and* $0 \leqslant e_1 < e$. *Then the congruence*

$$F(x_1, x_2, \ldots, x_s) \equiv 0 \pmod{\pi^t}$$

has a non-trivial solution.

Now if F is a diagonal form of degree k whose coefficients are units of O_K and $t = em+\bar{e}$, $em = v(k)$, the lemma guarantees that the congruence

$$F \equiv 0 \pmod{\pi^{em+\bar{e}}}$$

has a non-trivial solution provided

$$s > ke\left(\frac{p^m-1}{p-1}\right)+\bar{e}kp^m \quad \text{and} \quad p \neq 2.$$

Hence, if $p \neq 2$,

$$\gamma^*(k, \pi^{em+\bar{e}}) \leqslant ke\left(\frac{p^m-1}{p-1}\right)+k\bar{e}p^m+1$$

and from (5), we get

$$\Gamma^*(k,\pi) \leqslant k^2\left(e\frac{p^m-1}{p-1}+\bar{e}p^m\right)+1, \quad p \neq 2. \tag{10}$$

If $p = 2$, however, we get

$$\Gamma^*(k,\pi) \leqslant k^2\left((e+1)p^{m+1}-e\right)+1. \tag{11}$$

COROLLARY 2. *If* $p \geqslant 3$,

$$\Gamma^*(k,\pi) \leqslant (e+1)k^3-\frac{e}{k-1}k^2+1.$$

Proof. From (10)

$$\begin{aligned}\Gamma^*(k,\pi) &\leqslant k^2\left(e\frac{p^m-1}{p-1}+\bar{e}p^m\right)+1\\ &\leqslant k^2\left(e\frac{p^m-1}{p-1}+\left(1+\frac{e}{p-1}\right)p^m\right)+1\\ &= k^2\left(\frac{2ep^m+(p-1)p^m-e}{p-1}\right)+1\\ &= k^2\left(\frac{2e}{p-1}+1\right)p^m-\frac{k^2e}{p-1}+1\\ &\leqslant (e+1)k^3-\frac{k^2e}{k-1}+1\end{aligned}$$

as asserted.

4. Proof of Theorem 1 and concluding remarks. We are now ready to give the proof of

THEOREM 1. *If* $p \geqslant 3$,

$$\Gamma^*(k,\pi) \leqslant \max\{3nk^2-nk+1,\ 2k^3-k^2\}.$$

If $p = 2$,

$$\Gamma^*(k,\pi) \leqslant 4nk^2-nk+1.$$

Proof. We appeal to the results in Corollary 1, the relations in (5) and (10).

Consider the case $p \geqslant 3$. If $e \geqslant p-1$, using Corollary 1, the relation in (5) and (10), we have

$$\begin{aligned}\Gamma^*(k,\pi) &\leqslant \left(\bar{e}fp^m(p-1)+ef(p^m-1)\right)k+1\\ &\leqslant \left(\left(1+\frac{e}{p-1}\right)fp^m(p-1)+ef(p^m-1)\right)k+1\\ &= \left((p-1+e)fp^m+ef(p^m-1)\right)k+1.\end{aligned}$$

Hence, if $e \geqslant p-1$,

$$\Gamma^*(k, \pi) \leqslant 3efp^m k - efk + 1 \leqslant 3nk^2 - nk + 1. \tag{12}$$

If $e < p-1$, using (10), we get

$$\Gamma^*(k, \pi) \leqslant k^2\left(e\frac{p^m-1}{p-1} + \bar{e}p^m\right) + 1 \tag{13}$$

$$< k^2(p^m - 1 + p^m) \leqslant 2k^3 - k^2.$$

It now remains to study the case $p = 2$. Using (7) and the relation in (5), we get

$$\Gamma^*(k, \pi) \leqslant f\left((e+1)p^{m+1} - 1\right)k + 1.$$

It can be shown that

$$(e+1)p^{m+1} - 1 \leqslant 4ek - e.$$

Consequently, we have

$$\Gamma^*(k, \pi) \leqslant 4efk^2 - efk + 1 = 4nk^2 - nk + 1. \tag{14}$$

The proof of the theorem follows from (12), (13) and (14).

Concluding remarks. 1. Suppose that for any $x \not\equiv 0 \pmod{\pi}$, $x^k \equiv 1 \pmod{\pi^{em+\bar{e}}}$. Since the lemma of Olson is best possible, we have $\gamma^*(k, \pi^{em+\bar{e}}) = s_t$, $t = em + \bar{e}$. From this, when $k = p^m(p^f - 1)$ it might seem that s_t can be made large enough so that $\Gamma^*(k, \pi) > k^2$, by taking a large value of e (since f is otherwise insignificant for such an objective). Quite to the contrary, if $x \not\equiv 0 \pmod{\pi}$, $x^k \equiv 1 \pmod{\pi^{em+\bar{e}}}$, then e cannot be large as well. If $x = 1 + \pi$, for instance, and $e \geqslant p$, then $x^{p(p^f-1)} \equiv 1 \pmod{\pi^p}$ but not mod π^{p+1}. More generally, it can be shown that if $x^{p^m(p^f-1)} \equiv 1 \pmod{\pi^{em+\bar{e}}}$ for all $x \not\equiv 0 \pmod{\pi}$ then $e \leqslant p-1$. I still believe that Artin's conjecture is highly probable for diagonal forms.

2. In Theorem 2, a better bound than $\left(\gamma^*(k, \pi^{em+\bar{e}}) - 1\right)k + 1$ for $\Gamma^*(k, \pi)$ was obtained under the assumption $e \geqslant k + \bar{e}$. Actually, such a better bound of $\Gamma^*(k, \pi)$ can also be obtained even if $e < k + \bar{e}$. This will be discussed elsewhere.

I am grateful to Doc. J. Browkin for valuable discussion in the preparation of this paper. I also thank a referee who pointed out a mistake in an earlier version of Lemma 1 and for detailed comments and suggestions on the manuscript.

References

[1] Y. Alemu, *On zeros of forms over local fields*, Acta Arith. 45 (1985), pp. 163–171.
[2] J. Ax and S. Kochen, *Diophantine problems over local fields I*, Amer. J. Math. 87 (1965), pp. 606–630.
[3] B. J. Birch, *Diagonal equations over p-adic fields*, Acta Arith. 9 (1964), pp. 291–300.
[4] J. Browkin, *On zeros of forms*, Bull. Acad. Polon. Sci., Ser. Sci. Math. Astronom. et Phys. 17 (1969), pp. 611–616.
[5] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. A. 274 (1963), pp. 443–460.
[6] — — *Simultaneous equations of additive type*, Phil. Trans. Roy. Soc. London 246 (1969), pp. 557–595.
[7] M. M. Dodson, *Homogeneous additive congruences*, Phil. Trans. Roy. Soc. London, Ser. A, 261 (1967), pp. 167–210.
[8] — *Some estimates for diagonal equations over p-adic fields*, Acta Arith. 40 (1981), pp. 117–124.
[9] M. J. Greenberg, *Lectures on Forms in Many Variables*, New York 1969.
[10] D. J. Lewis and H. L. Montgomery, *On zeros of p-adic forms*, Michigan Math. Journ. 30 (1983), pp. 83–87.
[11] J. E. Olson, *A combinatorial problem on finite abelian groups*, I and II, J. Number Theory 1 (1969), pp. 8–10 and 195–199.
[12] L. G. Peck, *Diophantine equations in algebraic number fields*, Amer. J. Math. 71 (1949), pp. 387–402.
[13] S. H. Schanuel, *An extension of Chevalley's theorem to congruences modulo prime powers*, J. Number Theory 6 (1974), pp. 284–290.

DEPARTMENT OF MATHEMATICS
ADDIS ABABA UNIVERSITY
Ethiopia

Received on 11. 2. 1985
and in revised form on 8. 11. 1985 (1492)