ON ZEROS OF p-ADIC FORMS

D. J. Lewis and Hugh L. Montgomery

1. Introduction. In the 1930's E. Artin conjectured (see [3, p. x]) that a form F of degree d in n variables with coefficients in a p-adic field Q_p must have a nontrivial zero in that field if $n > d^2$. He was aware that for each d and each p there is a form of degree d in d^2 variables with coefficients in Q_p with no nontrivial p-adic zero; e.g., the reduced norm of a central simple division algebra over Q_p. As a first step towards Artin's conjecture, R. Brauer [5] showed that there is a function $\phi_p(d)$ such that if $n > \phi_p(d)$, then F has a nontrivial p-adic zero. Terjanian [16] disproved Artin's conjecture by exhibiting a 2-adic quartic form in 18 variables with no nontrivial 2-adic zero; later [17] he gave such an example with 20 variables. Generalizing Terjanian's construction, Browkin [6] gave counterexamples for each prime p, but always in fewer than d^3 variables. Recently Arhipov and Karačuba [1, 2] greatly improved on this by showing that for each p there are infinitely many d such that

$$\phi_p(d) > \exp\left(\frac{d}{(\log d)^2 (\log\log d)^3}\right).$$

By introducing a more efficient principle of p-adic interpolation (Lemma 1), we sharpen their result slightly.

THEOREM 1. *Let p be a given prime and suppose $\epsilon > 0$. For infinitely many d there is a form F in $\mathbf{Z}[x_1, \ldots, x_n]$ of degree d with*

$$n > \exp\left(\frac{d}{(\log d)(\log\log d)^{1+\epsilon}}\right)$$

such that if $a_1, \ldots, a_n \in \mathbf{Z}$ and $F(a_1, \ldots, a_n) \equiv 0 \pmod{p^d}$, then $a_1 \equiv \cdots \equiv a_n \equiv 0 \pmod{p}$.

It is not clear how close to best possible the above might be. The upper bound for $\phi_p(d)$ that one obtains from Brauer's argument is an iterated exponential which is very much larger than the lower bound we have obtained.

It would be nice to know precisely when $\phi_p(d) = d^2$. Meyer [14] found that $\phi_p(2) = 4$ for all p. Demyanov [10] and Lewis [13] independently showed that $\phi_p(3) = 9$ for all p (for other proofs see Springer [15] and Davenport [9]). Ax and Kochen [4] and Ersov [11, 12] independently proved there exists a function $p_0(d)$ such that $\phi_p(d) = d^2$ for all $p > p_0(d)$. Cohen [8] demonstrated that it is possible, at least in principle, to compute an upper bound for $p_0(d)$. It is interesting to note that in all the known examples for which $\phi_p(d) > d^2$ one has d even, composite and divisible by $p-1$. Thus it could be that these are the only

Received July 6, 1982.
Research supported in part by NSF grant MCS 8002559.
Michigan Math. J. 30 (1983).

exceptions to $\phi_p(d)=d^2$, and more particularly that $\phi_p(d)=d^2$ when d is a prime. We note that for additive forms of degree d, d^2+1 variables suffice to imply the existence of p-adic zeros.

Our basic lemma yields the following result, which is of independent interest:

THEOREM 2. *Suppose that p is an odd prime and that M is a positive integer. Let*

$$S_\nu = S_\nu(\mathbf{x}) = \sum_{k=1}^{N} x_k^\nu. \tag{1}$$

If $x_1,\dots,x_N$ are integers, not all divisible by p, and if $S_{(p-1)m}\equiv 0 \pmod{p^{(p-1)M}}$ for $M\leqslant m<2M$, then $N\geqslant p^M$.

A similar result applies when $p=2$ (see Lemma 3). Arhipov and Karačuba obtained the weaker bound $N\geqslant p^{[M/\log M]}$. That Theorem 2 is essentially best possible can be seen from a result of Browkin [7, Lemma 4], which asserts that if $F_1,\dots,F_J$ are forms in $x_1,\dots,x_N$ of degrees $d_1,\dots,d_J$ respectively, then the system of congruences $F_j(\mathbf{x})\equiv 0 \pmod{p^{a_j}}$, $1\leqslant j\leqslant J$, has a solution with not all the x_k divisible by p, provided

$$N>\frac{1}{p-1}\sum_{j=1}^{J} d_j(p^{a_j}-1).$$

2. p-adic interpolation. We now establish an elementary result which enables us to interpolate p-adically the values of a polynomial. If α is a rational number and $\alpha=p^k a/b$, where $(a,p)=(b,p)=1$, $k\in\mathbf{Z}$, we say $\operatorname{ord}\alpha=k$.

LEMMA 1. *Let a be an integer and let $n_1,n_2,\dots,n_K$ be distinct integers such that $a\equiv n_1\equiv n_2\equiv\cdots\equiv n_K \pmod p$. Let $f\in\mathbf{Z}[z]$, and suppose that*

$$f(n_k)\equiv 0 \pmod{p^M},\quad k=1,2,\dots,K.$$

Then $\operatorname{ord} f(a)\geqslant \min(K,K-L+M-1)$ *where*

$$L=\max_k\left\{\operatorname{ord}\left(\prod_{\substack{j=1\\ j\neq k}}^{K}(n_j-n_k)\right)\right\}.$$

For our purposes the particular advantage of the above formulation is that L depends not on the minimum p-adic separation of the n_k but rather on an average of the distance from one n_k to the others.

Proof. Define the polynomial $h(z)\in\mathbf{Q}[z]$ by the relation:

$$f(z)=\sum_{k=1}^{K} f(n_k)\prod_{\substack{j=1\\ j\neq k}}^{K}\frac{(z-n_j)}{(n_k-n_j)}+h(z). \tag{2}$$

Let D be the least common denominator of the coefficients of $h(z)$. Clearly $\operatorname{ord} D\leqslant\max\{0,L-M\}$. Now $Dh(z)$ lies in $\mathbf{Z}[z]$ and is divisible by $\prod_k(z-n_k)$, so that by Gauss' lemma $Dh(z)=g(z)\prod_k(z-n_k)$ with $g(z)$ in $\mathbf{Z}[z]$. We insert this expression for $h(z)$ in (2) and put $z=a$ to obtain

$$f(a)=\sum_{k=1}^{K} f(n_k)\prod_{\substack{j=1\\ j\neq k}}^{K}\frac{(a-n_j)}{(n_k-n_j)}+\frac{g(a)}{D}\prod_{k=1}^{K}(a-n_k).$$

But

$$\operatorname{ord}\left(f(n_k)\prod_{\substack{j=1\\ j\neq k}}^{K}\frac{(a-n_j)}{(n_k-n_j)}\right)\geqslant K-L+M-1$$

and

$$\operatorname{ord}\left(\frac{g(a)}{D}\prod_{k=1}^{K}(a-n_k)\right)\geqslant K-\max(0,L-M)=\min(K,K-L+M).$$

Thus we have the stated result. □

On combining this result with the ideas of Arhipov and Karačuba, we obtain

LEMMA 2. *Suppose p is an odd prime. Let M be a positive integer, and let $\mathfrak{M}$ be a set of K integers in the range $[M,2M-1]$. Suppose that there are N integers $x_1,\dots,x_N$, not all divisible by p, such that*

(3) $$S_{(p-1)m}(\mathbf{x})\equiv 0 \pmod{p^{(p-1)M}}$$

for all m in $\mathfrak{M}$. Then $N\geqslant p^K$.

Proof. If $p\mid x_n$, then x_n makes no contribution to the congruences (3), and thus we may suppose $(x_n,p)=1$ for all n. Let g be a primitive root $(\operatorname{mod} p^2)$, so that g is a primitive root for all powers of p. Write $x_n\equiv g^{a_n} \pmod{p^{(p-1)M}}$ with $0\leqslant a_n<\phi(p^{(p-1)M})$. Put $f(z)=\sum_{n=1}^{N} z^{a_n}$. (The numbers a_n are not necessarily distinct.) We note that $f(1)=N$. We shall now apply Lemma 1 to this $f(z)$ with $a=1$ to show that N is divisible by a high power of p. We take the n_k of Lemma 1 to be the numbers $g^{(p-1)m}$ for $m\in\mathfrak{M}$. Note that the n_k are distinct and all are congruent to 1 (mod p). By hypothesis $f(g^{(p-1)m})\equiv 0 \pmod{p^{(p-1)M}}$ for $m\in\mathfrak{M}$. Thus, by Lemma 1, $\operatorname{ord} f(1)\geqslant\min(K,K-L+(p-1)M-1)$, where

$$L=\max_{m\in\mathfrak{M}}\operatorname{ord}\left(\prod_{\substack{r\in\mathfrak{M}\\ r\neq m}}\left(g^{(p-1)r}-g^{(p-1)m}\right)\right).$$

But $\operatorname{ord}(g^{(p-1)s}-1)=1+\operatorname{ord} s$ for any natural number s, and hence

$$\operatorname{ord}(g^{(p-1)r}-g^{(p-1)m})=1+\operatorname{ord}(r-m).$$

However, the product $\prod_{\substack{r\in\mathfrak{M}\\ r\neq m}}(r-m)$ is a factor of $(m-M)!(2M-m-1)!$, which in turn is a factor of $(M-1)!$ since the binomial coefficient $\binom{M-1}{m-M}$ is an integer. Thus $L\leqslant K-1+\operatorname{ord}((M-1)!)$. But

$$\operatorname{ord}((M-1)!)=\sum_{j=1}^{\infty}\left[\frac{M-1}{p^j}\right]<\sum_{j=1}^{\infty}\frac{M-1}{p^j}=\frac{M-1}{p-1},$$

so that

$$K-L+(p-1)M-1\geqslant(p-1)M-\frac{M-1}{p-1}\geqslant M\geqslant K.$$

Hence $p^K\mid f(1)$ and the proof is complete. □

The argument above does not apply to the case $p=2$, because the group $(\mathbf{Z}/2^m\mathbf{Z})^\times$ is not cyclic when $m \geqslant 3$. By making suitable alterations we can establish

LEMMA 3. *Let M be a positive integer, and let $\mathfrak{M}$ be a set of K integers in the range $[M, 2M-1]$. Suppose that there are N integers $x_1, \ldots, x_N$, not all of them even, such that $S_{6m}(\mathbf{x}) \equiv 0 \pmod{2^{6M}}$ for all m in $\mathfrak{M}$. Then $N \geqslant 2^K$.*

3. Proofs of the theorems. To obtain Theorem 2 we have only to take $K=M$ in Lemma 2.

In proving Theorem 1 we restrict our attention to odd primes; the argument for $p=2$ is similar. For each natural number r we define a form F_r of degree d_r in n_r variables with coefficients in $\mathbf{Z}$ as follows. Let $F_1(\mathbf{x}) = x_1^2 - a x_2^2 + p x_3^2 - p a x_4^2$, where $\left(\frac{a}{p}\right) = -1$. Then $d_1 = 2$, $n_1 = 4$, and the congruence $F_1(\mathbf{z}) \equiv 0 \pmod{p^2}$ has only the trivial solution. For $r \geqslant 2$, the form F_r is defined in terms of F_{r-1}. Let $M = n_{r-1}$ and $N = n_r = p^{M/2} - 1$. From the fact that n_{r-1} is even and p is odd it follows that n_r is also an even integer. We then set $F_r(\mathbf{x}) = F_{r-1}(\mathbf{u})$, where $\mathbf{u} = (u_1, \ldots, u_{n_{r-1}})$ and

$$u_m = S_{(M+m-1)(p-1)}(\mathbf{x}) S_{(2M-m)(p-1)}(\mathbf{x}), \quad 1 \leqslant m \leqslant M = n_{r-1}. \tag{4}$$

Thus each u_m is a form of degree $(3M-1)(p-1)$ in $n_r = N$ variables, and hence F_r is a form of degree $d_r = (3M-1)(p-1)d_{r-1}$ in $n_r = N = p^{M/2} - 1$ variables, with coefficients in $\mathbf{Z}$.

We now show that if $F_r(\mathbf{x}) \equiv 0 \pmod{p^{d_r}}$ then $\mathbf{x} \equiv \mathbf{0} \pmod{p}$. Since F_{r-1} has this property, we see that

$$\operatorname{ord} F_{r-1}(\mathbf{u}) \leqslant d_{r-1} - 1 + d_{r-1} \min_{1 \leqslant m \leqslant M} \{\operatorname{ord} u_m\}.$$

But $\operatorname{ord} F_r(\mathbf{x}) \geqslant d_r = (3M-1)(p-1)d_{r-1}$, so that $\operatorname{ord} u_m \geqslant (3M-1)(p-1)$ for $1 \leqslant m \leqslant M$. Thus in particular (since $M \geqslant 2$)

$$u_m \equiv \mathbf{0} \pmod{p^{2M(p-1)}} \quad \text{for } 1 \leqslant m \leqslant M. \tag{5}$$

Let $\mathfrak{M}$ be the set of those natural numbers of the form $M+m-1$, with $1 \leqslant m \leqslant M$, such that $S_{(M+m-1)(p-1)} \equiv 0 \pmod{p^{(p-1)M}}$. From (4) and (5) we see that for each m at least one of the two numbers $M+m-1$ and $2M-m$ is in $\mathfrak{M}$. Hence $\operatorname{card} \mathfrak{M} \geqslant \frac{1}{2}M$. Since the number N of variables is smaller than $p^{M/2}$, it follows from Lemma 2 that $x_1 \equiv x_2 \equiv \cdots \equiv x_N \equiv 0 \pmod{p}$. Hence F_r has the desired property.

We now consider the relative sizes of n_r and d_r. Since $d_r = (3n_{r-1} - 1) \times (p-1)d_{r-1}$, we see that $(3p)^r n_{r-1} n_{r-2} \ldots n_1 > d_r > n_{r-1} n_{r-2} \ldots n_1$. Since $n_r = p^{n_{r-1}/2} - 1$, we observe that $n_{r-1} \approx \log n_r$. Thus if λ_r is chosen so that

$$d_r = (\log n_r)(\log\log n_r)(\log\log\log n_r)^{\lambda_r},$$

then $\lambda_r \to 1$ as $r \to \infty$. Hence, for each $\epsilon > 0$,

$$\log n_r > \frac{d_r}{(\log d_r)(\log\log d_r)^{1+\epsilon}}$$

for all sufficiently large r, and the proof is complete. □

Note added in proof: Recently Dale Brownawell established results comparable to ours, and Wolfgang Schmidt showed that $\phi_p(d) < \exp(2^d d!)$, by refining Brauer's method. The papers of these authors will appear in the *Journal of Number Theory*.

REFERENCES

1. G. I. Arhipov and A. A. Karačuba, *Local representation of zero by a form* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 45 (1981), 948-961.
2. ———, *On the representation of zero by a form in a p-adic field* (Russian), Dokl. Akad. Nauk SSSR 262 (1982), 11-13.
3. E. Artin, *The collected papers of Emil Artin,* Addison-Wesley, 1965, Preface, p. x.
4. J. Ax and S. Kochen, *Diophantine problems over local fields, I,* Amer. J. Math. 87 (1965), 605-630.
5. R. Brauer, *A note on systems of homogeneous algebraic equations,* Bull. Amer. Math. Soc. 51 (1945), 749-755.
6. J. Browkin, *On forms over p-adic fields,* Bull. Acad. Polon. Sci. Math. Astronom. Phys. 14 (1966), 489-492.
7. ———, *On zeros of forms,* Bull. Acad. Polon. Sci. Ser. Sci. Math. 17 (1969), 611-616.
8. Paul J. Cohen, *Decision procedures for real and p-adic fields,* Comm. Pure Appl. Math. 22 (1969), 131-151.
9. H. Davenport, *Cubic forms in thirty two variables,* Philos. Trans. Roy. Soc. London Ser. A 251 (1959), 193-232.
10. V. B. Demyanov, *On cubic forms in discretely normed fields* (Russian), Dokl. Akad. Nauk SSSR (N.S) 74 (1950), 889-891.
11. Ju. L. Eršov, *On the elementary theory of maximal normed fields* (Russian), Dokl. Akad. Nauk SSSR 165 (1965), 21-23; Soviet Math. Dokl. 6 (1965), 1390-1393.
12. ———, *On elementary theories of local fields* (Russian), Algebra i Logika Sem. 4 (1965), no. 2, 5-30.
13. D. J. Lewis, *Cubic homogeneous polynomials over p-adic number fields,* Ann. of Math. 56 (1952), 473-478.
14. A. Meyer, *Zur Theorie der indefiniten quadratischen Formen,* J. Reine Angew. Math. 108 (1891), 125-139.
15. T. A. Springer, *Some properties of cubic forms over fields with a discrete valuation,* Indag. Math. 17 (1955), 512-516.
16. G. Terjanian, *Un contre-example à une conjecture d'Artin,* C.R. Acad. Sci. Paris Ser. AB 262 (1966), A612.
17. ———, *Formes p-adiques anisotropes,* J. Reine Angew Math. 313 (1980), 217-220.

Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48109