ON THE LOCATION OF THE ROOTS OF POLYNOMIAL CONGRUENCES

by C. HOOLEY

(Received 15 April, 1989)

We have indicated in our tract [9] that several interesting problems in the theory of numbers are related to results about the evenness of the distribution of the roots v of a polynomial congruence

$$f(v) \equiv 0 \pmod{k}, \tag{1}$$

where $f(x) = a_0x^n + \ldots + a_n$ is an irreducible polynomial having integral coefficients and degree $n \geqq 2$. We alluded, for example, to our work on the Chebyshev problem of the greatest prime factor of $n^2 - D$ [8], in which an essential component was our earlier demonstration [6] of the uniform distribution, modulo 1, of v/k when $f(x) = x^2 - D$. But, having pointed out that the quantitative descriptions of such uniformity had to be very sharp for substantial applications, we then noted with regret that little more than mere uniform distribution was obtained in our generalization [7] of [6] to congruences of higher degree. Indeed, it has only been for certain cubic polynomials that results have been produced that are comparable in power with those for quadratic polynomials, and even these depend on the assumption of the unproved hypothesis R^* regarding the size of incomplete Kloosterman sums [10].

The above results clearly give estimates of very uneven quality when they are applied to the special question of how closely v/k can approximate to a given real number α, modulo 1. Thus, to particularize, letting $\|u\|$ as usual denote the distance of u from the nearest integer, we can deduce that

$$\left\|\frac{v}{k} - \alpha\right\| < \frac{1}{\psi_n(k)} \tag{2}$$

infinitely often, where $\psi_2(k) = k^{1/4-\epsilon}$ but where $\psi_n(k)$ is a small power of $\log k$ when $n \geqq 3$. Moreover, although one possible route for strengthening the value of $\psi_2(k)$ would be to involve the refinements introduced by Deshouillers and Iwaniec [2] in their improvement of our work on the greatest prime factor of $n^2 - D$, a better one in the present context lies in merely slightly altering the way in which we count the moduli k with the consequence that $\psi_2(k)$ can actually be taken to be as large as $k^{1/2-\epsilon}$. Yet the interesting problem in Diophantine approximation thus raised appertains less to the property of uniform distribution than to the weaker one of the sequence v/k being dense, modulo 1. Fresh methods are therefore appropriate when seeking the substantial improvements in (2) that it is the purpose of the present communication to secure.

The only conditions we now place on the polynomial $f(x)$ is that it have integral coefficients and degree $n \geqq 2$, it being important to emphasize that the previously imposed requirement of irreducibility over the rational field is largely irrelevant to our present method. Nevertheless, as will be seen from a perusal of what we achieve, results for reducible polynomials containing non-linear irreducible factors can sometimes be obtained by applying our theorems to one such factor of lower degree. Next, having noted that we may assume for convenience that $a = a_0 > 0$, we let A, A_i denote positive constants depending at most on the form of $f(x)$ and, in particular, choose A_1 to be a

https://doi.org/10.1017/S0017089500009393 Published online by Cambridge University Press

positive integer such that $f(x)\geqq 1$ for $x\geqq A_1$. Also, the symbolism $\bar{b}$ is used to denote a solution y of a congruence $by\equiv 1 \pmod c$, whose modulus c is a number prime to b that may not be explicitly stated but that can always be inferred from the context.

We only consider the solutions of the congruence (1) for those necessarily positive moduli k that are generated from the binary form

$$\phi(s,t)=t^n f(s/t)$$

by integral values of s, t satisfying the conditions

$$(as,t)=1, \qquad t>0, \qquad A_1 t\leqq s<(A_1+1)t. \tag{3}$$

Hence, avoiding altogether the theory of the representation of numbers by binary forms, we see that infinitely many k arise whenever infinitely many t are used because the inequality

$$A_2 t^n < k < A_3 t^n \tag{4}$$

is implied by (3) and the definition of A_1. Also, the construction of k implying that $(t,k)=1$ and hence that $\bar{t}$ is defined relative to the modulus k, the multiplication of the equality $k=\phi(s,t)$ *by* $\bar{t}^n$ yields a root $s\bar{t}$ of (1) so that

$$\frac{s\bar{t}}{\phi(s,t)} \pmod 1$$

is a value of v/k. From this, utilizing the congruential identity

$$\rho\bar{\rho}+\sigma\bar{\sigma}\equiv 1 \pmod{\rho\sigma} \tag{5}$$

that is valid for $(\rho,\sigma)=1$ when $\rho\bar{\rho}\equiv 1 \pmod\sigma$ and $\sigma\bar{\sigma}\equiv 1 \pmod\rho$, we obtain the determination

$$\frac{v}{k}\equiv -\frac{s\overline{\phi(s,t)}}{t}+\frac{s}{t\phi(s,t)}\equiv -\frac{\bar{a}\bar{s}^{n-1}}{t}+\frac{s}{t\phi(s,t)} \pmod 1, \tag{6}$$

where

$$0<\frac{s}{t\phi(s,t)}<\frac{A_4}{k}$$

by (3) and (4). We have therefore arrived at the inequality

$$\left\|\frac{v}{k}+\frac{\bar{a}\bar{s}^{n-1}}{t}\right\|<\frac{A_4}{k}, \tag{7}$$

from which approximation our future estimates will flow.

We first apply (7) to the quadratic case in order to approximate to a given real number α by means of v/k. Here, by the third constituent of (3), the numerator $-\bar{a}\bar{s}$ in the approximating function can run through a complete reduced set of residues (mod t), the maximum interval (mod t) between these being 2 if t be chosen to be a prime number exceeding a. Hence in this instance we can choose s in such a manner that

$$\left\|\alpha+\frac{\bar{a}\bar{s}}{t}\right\|\leqq\frac{1}{t},$$

https://doi.org/10.1017/S0017089500009393 Published online by Cambridge University Press

wherefore

$$\left\|\frac{v}{k}-\alpha\right\| \leqq \frac{1}{t}+\frac{A_4}{k} \leqq \frac{A_5}{k^{1/2}}+\frac{A_4}{k} \leqq \frac{A_6}{k^{1/2}}.$$

But, if α be irrational, we can do much better because Dirichlet's theorem then provides infinitely many fractions S/T in lowest terms with the property that

$$\left|\alpha-\frac{S}{T}\right| < \frac{1}{T^2}. \tag{8}$$

From any such fraction we derive another fraction b/t for which $(ab, t)=1$ by means of the indeterminate equations

$$St-Tb=1, \qquad t \equiv 1 \pmod{a'},$$

where a' is the product of those prime factors of a that do not divide T. Since the solutions of these in b, t correspond exactly to the solutions of the concordant simultaneous congruences

$$t \equiv \bar{S} (\operatorname{mod} T), \qquad t \equiv 1 \pmod{a'}, \tag{9}$$

which form a residue class $(\operatorname{mod} a'T)$, we find that

$$\left|\frac{b}{t}-\frac{S}{T}\right| = \frac{1}{tT} \leqq \frac{2a'}{t^2}, \qquad \left|\alpha-\frac{S}{T}\right| \leqq \frac{4a'^2}{t^2}, \qquad (ab, t)=1 \tag{10}$$

if we choose the solution of (9) satisfying $a'T < t \leqq 2a'T$. Infinitely many values of t being altogether formed in virtue of the last inequality, we then determine s in accordance with (3) so that $s \equiv -\bar{a}\bar{b} \pmod{t}$. Hence, by (10), (7) and (4),

$$\left\|\frac{v}{k}-\alpha\right\| < \frac{A_4}{k}+\frac{2a'}{t^2}+\frac{4a'^2}{t^2} < \frac{A_7}{k},$$

and we therefore have

THEOREM 1. *Let $f(x)$ be a quadratic polynomial. Then, for any real number α, there are infinitely many moduli k for which a root v of the congruence* (1) *satisfies*

$$\left\|\frac{v}{k}-\alpha\right\| < \frac{A}{k^{1/2}}$$

for some positive constant A. Indeed, if α be irrational, there are even infinitely many k for which

$$\left\|\frac{v}{k}-\alpha\right\| < \frac{A}{k}.$$

For higher values of n, the increasingly specialized nature of the expression $\bar{a}\bar{s}^{n-1}/t$ in (7) entails our using extensions of Dirichlet's theorem that are concerned with approximations to irrational numbers by means of rationals of restricted type. This accelerates the already inevitable deterioration of our results, the proof and enunciation of which depend on the parity of n when α is irrational. Yet this proof for odd n contains an initial transformation through which we dismiss at once all cases where α is rational.

https://doi.org/10.1017/S0017089500009393 Published online by Cambridge University Press

This preliminary step concerns a simple consequence of the assumption that there be infinitely many pairs of co-prime positive integers s', t with the properties that

$$\left|\frac{a^{n-2}}{(2-\alpha)}-\frac{t}{(s')^{n-1}}\right|<\frac{A_8}{(s')^M} \quad\text{and}\quad (a,t)=1 \tag{11}$$

for some suitable number $M=M(n)\geqq n-1$, wherein it is supposed that $0\leqq\alpha<1$ since we are ultimately only interested in approximations to α, modulo 1. This implies first that

$$A_9<\frac{(s')^{n-1}}{t}<A_{10}$$

and hence that there are infinitely many values of t prime to a for which

$$\left|\alpha+\frac{a^{n-2}(s')^{n-1}}{t}-2\right|=\frac{(s')^{n-1}(2-\alpha)}{t}\left|\frac{a^{n-2}}{(2-\alpha)}-\frac{t}{(s')^{n-1}}\right|<\frac{A_{11}}{(s')^M}$$

for some value of s' prime to t, wherefore, choosing s in accordance with (3) so that $s\equiv\bar a\bar s'\pmod t$, we would conclude that

$$\left\|\alpha+\frac{\bar a\bar s^{n-1}}{t}\right\|<\frac{A_{11}}{(s')^M}<\frac{A_{12}}{t^{M/(n-1)}}<\frac{A_{13}}{k^{M/n(n-1)}} \tag{12}$$

in virtue of (4). Alternatively, however, we could have derived (12) from a variant of (11) by employing the congruential identity (5) to replace $\bar a\bar s^{n-1}/t$ by $-\bar t/as^{n-1}+1/as^{n-1}t$.

If α be rational, we take s' to be a prime number and then use the only value $n-1$ of M that is legitimate in the situation thus created. There are therefore infinitely many moduli k for which

$$\left\|\frac{v}{k}-\alpha\right\|<\frac{A_{14}}{k^{1/n}}$$

because of (7).

Progressing to the more important case where α is irrational, we first assume that n is odd and then endeavour to find a favourably large value of M in (11) by the methods of Heilbronn [**5**] and Danicic [**1**]. Applied to the problem of the size of $\|m^h\theta\|$ when θ is irrational, these procedures demonstrate that

$$\|m^h\theta\|<\frac{1}{m^{H'-\epsilon}}$$

for infinitely many m when $H'=2^{1-h}$ but do not immediately supply an answer to our question because the numbers m, l in the equivalent inequality

$$|m^h\theta-l|<\frac{1}{m^{H'-\epsilon}}$$

are not shewn to satisfy the condition $(am,l)=1$. Indeed, our apparently innocuous extra requirement not only entails a not uninteresting additional ingredient in the method but exacts the penalty of a loss of precision that is expressed by the replacement of H' by the

https://doi.org/10.1017/S0017089500009393 Published online by Cambridge University Press

inferior exponent

$$H = H(h) = \begin{cases} \frac{2}{5}, & \text{if } h = 2, \\ \dfrac{1}{2^h - 1}, & \text{if } h > 2. \end{cases} \tag{13}$$

However, a full description here of this result would be somewhat alien to our current theme if only because of the disproportionate amount of space it would occupy, and we therefore reserve its demonstration for a further publication devoted to this other aspect of Diophantine approximation [**11**].

We therefore immediately apply (13) to (12) and (7) via (11) when α is irrational and n is odd, deducing that there are infinitely many moduli k for which

$$\left\|\frac{v}{k} - \alpha\right\| < \frac{1}{k^{1/n + N/n(n-1) - \epsilon}} \tag{14}$$

where $N = H(n-1)$.

The validity of (14) does not depend on the parity of n. But a much sharper result for even values of n is obtained by shifting our attention from the small values of $\|m^h\theta\|$ to those of $\|P_2\alpha\|$, where P_2 is a product of two primes exceeding a that are congruent to $2 \pmod{n-1}$. In the new context, the apposite counterpart of the Heilbronn-Danicic results is a theorem due to Harman [**4**], the proof of which can be readily modified to yield the proposition that there are infinitely many numbers of type P_2 such that

$$\|P_2\alpha\| \leqq \frac{A_{15} \log^{4/3} P_2}{P_2^{1/3}}$$

when α is irrational. There thus being infinitely many (distinct) rationals l'/P_2 for which

$$\left|\alpha - \frac{l'}{P_2}\right| < \frac{A_{15} \log^{4/3} P_2}{P_2^{4/3}},$$

the process of clearing l', P_2' of at most one common prime factor shews that the inequality

$$\left|\alpha - \frac{l}{t}\right| < \frac{A_{15} \log^{4/3} t}{t^{4/3}}$$

is satisfied by infinitely many fractions l/t in lowest terms whose denominators t are products of one or two primes exceeding a that are congruent to $2 \pmod{n-1}$. Hence, since there is an integer u prime to t such that $\bar{l} \equiv -au^{n-1} \pmod t$ when t is of the above form, we infer that we can choose s in conformity with (3) so that

$$\left\|\alpha + \frac{\bar{a}\bar{s}^{n-1}}{t}\right\| < \frac{A_{15} \log^{4/3} t}{t^{4/3}},$$

on account of which there are infinitely many moduli k for which

$$\left\|\frac{v}{k} - \alpha\right\| < \frac{A_{16} \log^{4/3} k}{k^{4/3n}}$$

because of (4) and (7).

https://doi.org/10.1017/S0017089500009393 Published online by Cambridge University Press

Assembling all the properties garnered since Theorem 1, we complete the statement of our results by enuciating

Theorem 2. *Let $f(x)$ be a polynomial of degree n exceeding 2. Then, for any given real number α, there are infinitely many moduli k for which a root of the congruence* (1) *satisfies an inequality of the form*

$$\left\|\frac{v}{k}-\alpha\right\|<\frac{1}{\psi_n(k)},$$

where

$$\psi_n(k)=\begin{cases} Ak^{1/n}, & \text{if } \alpha \text{ be rational,}\\ k^{1/n+N/n(n-1)-\epsilon}, & \text{if } \alpha \text{ be irrational and } n \text{ odd,}\\ Ak^{4/3n}\log^{-4/3}k, & \text{if } \alpha \text{ be irrational and } n \text{ even,}\end{cases}$$

with $N=H(n-1)$ as in (13).

We end with some remarks about the extent to which these results may understate the situation we wish to describe.

The more satisfactory answer is given by Theorem 1, the first part of which is best possible apart from the value of A. Its second part is also essentially best possible in relation to its application to the most obvious arithmetical question about the location of v, modulo k, since it shews that there are infinitely many moduli k for which v differs from αk by less than some constant. That it furthermore supplies the best universal bound for $\psi_2(k)$ when α is irrational can be demonstrated by choosing α to be $\eta=\frac{1}{2}(\sqrt{5}+1)$ and $f(x)$ to be x^2+7. In this case, as the class number of positive binary quadratic forms of determinant -7 is one, a reference to §6 of our paper [6] confirms that the special case

$$\frac{v}{k}\equiv-\frac{\bar{s}}{t}+\frac{s}{t(s^2+7t^2)}\ (\mathrm{mod}\ 1)$$

of our formula (6) provides all values of v/k, where $k=s^2+7t^2$ and the only restrictions placed on s, t are $(s,t)=1$ and $t>0$. Hence, if there be infinitely many k for which the inequality

$$\left\|\frac{v}{k}-\eta\right\|<\frac{b}{k}$$

holds, then

$$\left\|-\frac{\bar{s}}{t}-\eta\right\|<\frac{b}{k}+\frac{|s|}{t(s^2+7t^2)}<\frac{b+1}{k^{1/2}},$$

from which it is first inferred that t also takes infinitely many values because η is irrational. Next, for given t, the upper bound

$$\frac{|s|+bt}{t(s^2+7t^2)}$$

for $\|-\bar{s}/t-\eta\|$ cannot exceed the maximum value it achieves when s is the positive root

$\{\sqrt{(b^2+7)}-b\}t$ of

$$(s^2+7t^2)-2s(s+bt)=0,$$

whence

$$\left\| -\frac{\bar{s}}{t}-\eta \right\| < \frac{1}{2(\sqrt{(b^2+7)}-b)t^2}$$

infinitely often. Therefore, by the familiar limits to the approximations of η by rational numbers, we deduce that b exceeds the root b' of

$$2(\sqrt{(b'^2+7)}-b')=\sqrt{5},$$

which is seen to be $23\sqrt{5}/20$ by observing that

$$\frac{1}{14}(\sqrt{(b'^2+7)}+b')=\frac{1}{\sqrt{5}}.$$

Consequently the constant A in the second part of Theorem 1 is certainly subject to the constraint $A>23\sqrt{5}/20>5/2$.

Yet there are cases where Theorem 1 substantially underestimates the rapidity of the approximation of v/k to α. To see this, we need only express η as the continued fraction

$$1+\frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\cdots,$$

whose convergents p_n/q_n satisfy

$$p_nq_{n+1}-p_{n+1}q_n=(-1)^n, \qquad p_n=q_{n+1}$$

with the consequence that

$$p_n^2\equiv(-1)^n \pmod{q_n}.$$

Therefore, if we now take $f(x)$ to be x^2+1, the convergents p_n/q_n of odd order provide values of v/k for which

$$\left\| \frac{v}{k}-\eta \right\| < \frac{1}{(\sqrt{5}-\epsilon)k^2}$$

for infinitely many k. Approximations as good as this, however, are exceptional, since a familiar metrical argument (see, for example, the reasoning used to prove Theorem 198 in Hardy and Wright [4]) easily shews that there are almost no numbers α with the property that (2) holds for infinitely many k if the series

$$\sum_{k=1}^{\infty}\frac{1}{\psi_n(k)}\sum_{\substack{f(v)\equiv 0 \pmod{k}\\ 0<v\leq k}}1=\sum_{k=1}^{\infty}\frac{\rho(k)}{\psi_n(k)}, \text{ say,}$$

be convergent. In addition, confining ourselves for the sake of illustration to the case where $f(x)$ is irreducible, we even see from the asymptotic formula

$$\sum_{k\leq x}\rho(k)\sim A_{17}x$$

that the second part of Theorem 1 is not far from best possible for almost all α.

https://doi.org/10.1017/S0017089500009393 Published online by Cambridge University Press

Theorem 2, on the other hand, is almost certainly inherently imperfect owing to the restricted set of moduli k for which v has been constructed. But, so far, it has only been for $\alpha = 0$ that we have been able to make a substantial improvement in its estimate, using the trivial observation that $A_{18}\{f(v)\}^{1/n} < v < A_{19}\{f(v)\}^{1/n}$ to get the value $Ak^{1-1/n}$ that is best possible in this instance. However, minor improvements for larger odd values of n can probably be derived by combining the methods of **[11]** with those of Vinogradov.

REFERENCES

1. I. Danicic, An extension of a theorem of Heilbronn, *Mathematika,* **5** (1958), 30–37.

2. J. M. Deshouillers and H. Iwaniec, On the greatest prime factor of n^2+1, *Ann. Inst. Fourier* (*Grenoble*) **32** no 4 (1982), 1–11.

3. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers,* third edition (Oxford, 1954).

4. G. Harman, Trigonometric sums over primes II, *Glasgow Math. J.* **24** (1983), 23–37.

5. H. A. Heilbronn, On the distribution of the sequence $\theta^2 n$ (mod 1), *Quart. J. Math. Oxford* (2), **19** (1948), 249–256.

6. C. Hooley, On the number of divisors of quadratic polynomials, *Acta Math.*, **110** (1963), 97–114.

7. C. Hooley, On the distribution of the roots of polynomial congruences, *Mathematika,* **11** (1964), 39–49.

8. C. Hooley, On the greatest prime factor of a quadratic polynomial, *Acta Math.*, **117** (1967), 281–299.

9. C. Hooley, *Applications of sieve methods to the theory of numbers* (Cambridge, 1976).

10. C. Hooley, On the greatest prime factor of a cubic polynomial, *J. reine angew. Math.* **303/304** (1978), 21–50.

11. C. Hooley, On a problem in Diophantine approximation (to appear).

School of Mathematics,
University of Wales College of Cardiff,
Cardiff,
Great Britain.

https://doi.org/10.1017/S0017089500009393 Published online by Cambridge University Press