Mathematical Notes, Vol. 55, No. 6, 1994

ON POLYNOMIAL CONGRUENCES

S. V. Konyagin and T. Steger

1. Introduction. For natural numbers n and q we denote by M_n the set of all polynomials of power not higher than n with integer coefficients, by $M_n(q)$ the set of all polynomials of the form

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

with the condition $(a_n, \ldots, a_0, q) = 1$. For $f \in \mathbb{Z}[x]$ and a natural number P we denote by $\rho(f, P, q)$ the number of solutions of the congruence

$$f(x) \equiv 0 \pmod q, \qquad 0 \le x < P. \tag{1}$$

Let us put

$$N_n(P, q) = \max_{f \in M_n(q)} \rho(f, P, q); N_n(q) = N_n(q, q).$$

The quantity $N_n(q)$ is investigated in [1–3]. In [3] the best possible estimate

$$N_n(q) \ll q^{1-1/n} \tag{2}$$

is obtained. (Here and below constants of the symbol "$\ll$" may depend only on n and on $\varepsilon > 0$; in this case unimprovability of (2) means that for a fixed n the order of $N_n(q)$ is regular for infinitely many values of q.)

The quantity $N_n(P, q)$ is considered in [4–6]. In [6] it was shown that

$$N_n(P, q) \ll P^{\varepsilon}(P^{1-1/n+\theta_n} + Pq^{-1/n}), \tag{3}$$

where $\theta_n = (n-1)/n(n^3 - n^2 + 1)$.

In the present paper we show that the set $E(f, q)$ of roots of the congruence (1), which belong to the interval $[0, q)$, is uniformly distributed in some sense on this interval. The nonuniformity of the distribution of the set $E \subset [0, q) \cap \mathbb{Z}$ on $[0, q)$ can be measured by the quantity

$$D(E, q) = \sup_{0 \le P \le q} \big| |E \cap [0, P)| - P|E|/q \big|.$$

We denote by $v(q)$ the number of different prime divisors of q.

Theorem 1. *For any polynomial $f \in M_n$ the inequality*

$$D(E(f, q), q) < n^{v(q)} \tag{4}$$

is valid.

For fixed n the estimate (4) is regular with respect to the order.

The work of the first author was supported by the Russian Foundation for Fundamental Research, Grant 93-011-240.

Moscow State University. University of Georgia, Athens, Georgia, USA. Translated from Matematicheskie Zametki, Vol. 55, No. 6, pp. 73–79, June, 1994. Original article submitted November 25, 1993.

0001-4346/94/5556-0596$12.50

Theorem 2. *For any n and $q > 1$ there exists a polynomial $f \in M_n(q)$ such that*

$$D(E(f,q),q) \gg n^{v(q)}. \tag{5}$$

It follows from (2) and Theorem 1 that $N_n(P,q) \ll Pq^{-1/n} + q^{\varepsilon}$. For $P \ll q^{1/n}$ this inequality can be strengthened by using the arguments of [6].

Theorem 3. *For $P \geq 1$ the inequality*

$$N_n(P,q) \ll \frac{1+\ln P}{\ln(1+P^{-1}q^{1/n})} \tag{6}$$

is valid.

In particular, $N_n(P,q) \ll 1$ for $P \leq q^{\frac{1}{n}-\varepsilon}$. In [6] the corresponding result is established for $P < q^{1/n(n+1)}$.

Theorems 1 and 3 imply the following

Corollary. *The inequality*

$$N_n(P,q) \ll Pq^{-1/n} + P^{\varepsilon} \tag{7}$$

is valid.

For $P \ll q^{1/n}$ Theorem 3 states that $N_n(P,q) \ll \ln q$. However, we cannot rule out that in this case $N_n(P,q) \ll 1$.

The authors are grateful to A. Granville and K. Pomerance for their attention to this work.

2. Proof of Theorem 1. An integer-valued arithmetic progression whose difference is the power of a prime number p is called a p-progression.

Lemma 1. *Let q be the power of a prime number p, $f \in M_n$. Then the set of solutions of the congruence*

$$f(x) \equiv 0 \pmod{q} \tag{8}$$

is the union of at most n mutually disjoint p-progressions.

Proof. Let $q = p^t$. We use induction over t. For $t = 0$ the statement is obvious. Let us verify its validity for $t = t_0 > 0$, assuming that it holds for all $t < t_0$. If all coefficients of the polynomial f can be divided into p, then (8) is equivalent to the congruence $f(x)/p \equiv 0 \pmod{q/p}$, to which we can apply the inductive hypothesis. Now let us assume that $f \in M_n(p)$. In this case we need the following statement, easily obtained from the Hensele lemma [7], Theorem 2 in § 3 of Ch. 4.

Lemma 2. *Suppose that $f \in M_n(p)$, $\overline{f} \in (\mathbb{Z}/p)[x]$ is the reduction of f modulo p, and $\overline{f} = \overline{g}\overline{h}$, where polynomials $\overline{g}$ and $\overline{h}$ are relatively prime in $(\mathbb{Z}/p)[x]$. Then there exist polynomials g and h such that their reductions modulo p yield $\overline{g}$ and $\overline{h}$, respectively;* $\deg g = \deg \overline{g}$ *and* $f \equiv gh \pmod{q}$.

The polynomial $\overline{f}$ can be represented in the form

$$\overline{f} = \overline{g}_0 \cdots \overline{g}_{p-1}\overline{h},$$

where $\overline{g}_j(x) = (x-j)^{n_j}$ and $\overline{h}$ has no roots in $\mathbb{Z}/p$. Note that

$$n = \deg f \geq \deg \overline{f} \geq \deg \overline{g}_0 + \cdots + \deg \overline{g}_{p-1} = n_0 + \cdots + n_{p-1}. \tag{9}$$

Applying p times Lemma 2, we see that there exist polynomials $g_0, \dots g_{p-1}, h$ such that $g_j \equiv (x-j)^{n_j} \pmod{p}$ $(j = 0, \dots, p-1)$, $h(x) \not\equiv 0 \pmod{p}$ for $x \in \mathbb{Z}, \deg g_j = n_j$ $(j = 0, \dots, p-1)$, and $f \equiv g_0 \dots g_{p-1} h \pmod{q}$. It follows from these properties that if E is the set of solutions of the congruence (8) and E_j is the set of solutions of the congruence

$$g_j(x) \equiv 0 \pmod{q} \tag{10}$$

for $j = 0, \ldots, p-1$, then

$$E_j = \{x \in E : x \equiv j \,(\bmod\, p)\}. \tag{11}$$

For $n_j = 0$ we have $g_j \equiv 1 \,(\bmod\, p)$ and $E_j = \varnothing$. Let $n_j \geq 1$. By (11) each number $x \in E_j$ is representable in the form $j + py$, where $y \in \mathbb{Z}$. Moreover,

$$g_j \equiv (py)^{n_j} \,(\bmod\, p) \equiv 0 \,(\bmod\, p),$$

that is, $g_j(x) = ph_j(y)$, where $h_j \in \mathbb{Z}[y]$. The congruence (10) is equivalent to the congruence $h_j(y) \equiv 0 \,(\bmod\, q/p)$. By the inductive hypothesis the set of solutions of the last congruence, and therefore the set E_j, are representable as the union of at most n_j mutually disjoint p-progressions. By (11) the set E of solutions of the congruence (8) is the union of mutually disjoint p-progressions, whose amount does not exceed $n_0 + \cdots + n_{p-1}$. Taking (9) into account, from this we obtain the statement of the lemma.

Now we pass directly to the proof of Theorem 1. Let us represent q in the form $\prod_{i=1}^{v(q)} p_i^{t_i}$, where $p_1, \ldots, p_{v(q)}$ are prime divisors of q. We denote

$$X = \{x : f(x) \equiv 0 \,(\bmod\, q)\},$$
$$X_i = \{x : f(x) \equiv 0 \,(\bmod\, p_i^{t_i})\} \quad (i = 1, \ldots, v(q)).$$

Then $X = \bigcap_{i=1}^{v(q)} X_i$. By Lemma 1 each of the sets X_i is representable in the form $\bigcup_{j=1}^{N_i} X_{i,j}, N_i \leq n$, where $X_{i,j}$ $(j = 1, \ldots, N_i)$ are mutually disjoint p_i-progressions. Therefore,

$$X = \bigcup_{j=1}^{N} Y_j, \tag{12}$$

where

$$N = \prod_{i=1}^{v(q)} N_i \leq \prod_{i=1}^{v(q)} n = n^{v(q)}, \tag{13}$$

Y_j are all possible intersections of the form $\bigcap_{i=1}^{v(q)} X_{i,j_i}$ $(1 \leq j_i \leq N_i)$. Note that the sets Y_j are mutually disjoint, and each of them is an arithmetic progression; therefore, for any P, $0 \leq P \leq q$, we have

$$\big||Y_j \cap [0,P)| - P|Y_J|\big| < 1,$$

and by (12)

$$\big||X \cap [0,P)| - P|X|\big| \leq \sum_{j=1}^{N} \big||E \cap [0,P)| - P|E|\big| < N,$$

whence and from (13) we obtain the conclusion of the theorem.

3. Proof of Theorem 2. For $f(x) = x^n$ we have $E(f,q) = \{0\}$ and $D(E(f,q)) = 1 - 1/q \geq 1/2$, which implies the validity of Theorem 2 in the case where $v(q)$ is bounded by a value dependent only on n. Therefore, we can assume that

$$v(q) > N = 4n^2. \tag{14}$$

Let $q = \prod_{i=1}^{v(q)} p_i^{t_i}$, where $p_1, \ldots, p_{v(q)}$ are increase-ordered prime divisors of q, $q_i = q/p_i^{t_i} (i = 1, \ldots, v(q))$. By the Chinese theorem there exists a number x_1 which satisfies the congruences $x_1 \equiv 0 \,(\bmod\, p_i^{t_i})$ $(1 \leq i \leq N)$ and $x_1 \equiv q_i \,(\bmod\, p_i^{t_i})$ $(N < i \leq v(q))$. We put $g(x) = \prod_{j=1}^{n}(x - jx_1)$. A number x satisfies the congruence $g(x) \equiv 0 \,(\bmod\, q)$ if and only if for $1 \leq i \leq N$ the congruences $x \equiv 0 \,(\bmod\, p_i^{t_i})$ are fulfilled and there exist numbers $j_{N+1}, \ldots, j_{v(q)}$ $(1 \leq j_i \leq n)$ such that $x \equiv j_i q_i \,(\bmod\, p_i^{t_i})$ for $N < i \leq v(q)$.

The system of congruences for x that we have written is equivalent to the congruence $x \equiv m \pmod q$, where $m = \sum_{i=N+1}^{v(q)} j_i q_i$. Note that values of m incongruent modulo q correspond to different sets $(j_{N+1}, \dots, j_{v(q)})$. Denoting by M the set of all possible values of m, we have

$$|M| = n^{v(q)-N} \gg n^{v(q)}. \tag{15}$$

One can consider M as the set of values for the sum of a stochastic quantity $\xi = \xi_{N+1} + \cdots + \xi_{v(q)}$, where $\xi_{N+1}, \dots, \xi_{v(q)}$ are independent stochastic quantities and ξ_i takes each value jq_i $(j = 1, \dots, n)$ with probability $1/n$. Let us estimate the dispersion of ξ

$$\begin{aligned}\mathbf{D}\xi = \sum_{i=N+1}^{v(q)} \mathbf{D}[\xi_i] &= \sum_{i=N+1}^{v(q)} \frac{n^2-1}{12} q_i^2 \\ &< \frac{q^2 n^2}{12} \sum_{i=N+1}^{v(q)} \frac{1}{p_i^2} < \frac{q^2 n^2}{12} \sum_{i=N+1}^{\infty} \frac{1}{i^2} < \frac{q^2 n^2}{12N}.\end{aligned}$$

We denote by $\mathbf{E}\xi$ the mathematical expectation of ξ. It follows from (14) and the Chebyshev inequality that

$$\Pr(|\xi - \mathbf{E}\xi| > q/4) < \frac{\mathbf{E}\xi}{(q/4)^2} < \frac{3n^2}{4N} = \frac{1}{3}.$$

Hence,

$$|M \cap [\mathbf{E}\xi - q/4, \mathbf{E}\xi + q/4]| > \frac{2}{3}|M|. \tag{16}$$

We put $l = [\mathbf{E}\xi - q/4]$, $f(x) = g(x + l)$. Let us calculate the lowest bound for $D(E(f,q),q)$. Taking into account (16), we get

$$\begin{aligned}|E(f,q) \cap [0, [2 + q/2])| &> |E \cap [0, [\mathbf{E}\xi + q/4]]| \\ &= |M \cap [\mathbf{E}\xi - q/4, \mathbf{E}\xi + q/4]| > \frac{2}{3}|M|.\end{aligned}$$

Consequently,

$$\begin{aligned}D(E(f,q),q) &\geq |E(f,q) \cap [0, [2 + q/2])| - [2 + q/2]|E(f,q)|/q \\ &\geq \left(\frac{2}{3} - \frac{[2+q/2]}{q}\right)|M| > 0.1|M|.\end{aligned}$$

From this and from (15) we obtain the conclusion of Theorem 2.

4. Proofs of Theorem 3 and of the Corollary.

Proof of Theorem 3. Let

$$1 \leq T \leq \frac{1}{2} q^{1/n}, \qquad N = 2 + [\frac{\ln T}{\ln(T^{-1} q^{1/n})}], \tag{17}$$

M be an arbitrary number, $f \in M_n(q)$. Suppose that $x_1, \dots, x_{nN}$ are different solutions of the congruence (8); moreover,

$$x_i \in [M, M + T) \quad (i = 1, \dots, nN). \tag{18}$$

When proving Lemma 1 in [3], it was established that there exists a polynomial $g \in M_n(q)$ with coefficient 1 of the term x^n such that any solution of (8) satisfies the congruence $g(x) \equiv 0 \pmod q$. Thus,

$$g(x_i) \equiv 0 \pmod q \quad (i = 1, \dots, nN). \tag{19}$$

Let us consider the Vandermonde determinant

$$\Delta = \det(x_i^{j-1})_{i,j=1}^{nN}.$$

If to columns of the matrix $\|x_i^{j-1}\|_{i,j=1}^{nN}$, beginning with the $(n+1)$th one, we add suitable linear combinations of previous columns, then we obtain the matrix $\|a_{i,j}\|_{i,j=1}^{nN}$,whose ith row is of the form

$$(1, x_i, \dots, x_i^{n-1}, g(x_i), x_i g(x_i), \dots, x_i^{n-1} g(x_i), \dots, x_i^{n-1}(g(x_i))^{N-1});$$

moreover, $\Delta = \det(a_{i,j})_{i,j=1}^{nN}$. Taking into account that by (19) all elements of the jth column are divided by q^s for $j > ns$, we see that Δ is divided by $q^{nN(N-1)/2}$. On the other hand,

$$\Delta = \prod_{1 \le i < j \le nN} (x_j - x_i),$$

whence and from (18) it follows that $0 < |\Delta| < T^{nN(nN-1)/2}$. Hence $q^{nN(N-1)/2} < T^{nN(nN-1)/2}$, which, taking into account (17), is equivalent to the inequality $N - 1 < \frac{n-1}{(\ln q/\ln T) - n}$, contradicting the choice of N.

We have shown that under the conditions (17) the number of solutions of the congruence (8) on the half-interval $[M, M+T)$ is less than nN. This implies immediately the conclusion of the theorem for $P \le P_0 = \max([\frac{1}{2}q^{1/n}], 1)$. But if $P > P_0$, then the interval $[0, P)$ is covered by $[P/P_0] + 1$ intervals of the form $[jP_0, (j+1)P_0)$; on each of these intervals the number of solutions of the congruence (8) $\ll 1 + \ln q$ by what has been proved. Consequently, in this case

$$N_n(P,q) \ll (1 + \ln q)([P/P_0] + 1) \ll (1 + \ln q) P q^{-1/n},$$

and the estimate (6) also holds in this case. The theorem has been proved.

Proof of the corollary. For $P \le q^{1/(2n)}$ the statement is valid, since in this case $N_n(P,q) \ll 1$ by Theorem 3. Let $q^{1/(2n)} < P \le q$; then for any polynomial $f \in M_n$ we have

$$\rho(f,P,q) \le \frac{P}{q}\rho(f,q,q) + D(E(f,q),q) \le \frac{P}{q} N_n(q,q) + D(E(f,q),q).$$

Substituting inequalities (2) and (4), we obtain $\rho(f,P,q) \ll Pq^{-1/n} + n^{v(q)}$ or $N_n(P,q) \ll Pq^{-1/n} + n^{v(q)}$. Since $v(q) = o(\ln q)$, we have $n^{v(q)} \ll q^{2n\varepsilon} < P^{\varepsilon}$, and for the case $q^{1/(2n)} < P \le q$ the corollary has been proved. Finally, if $P > q$, then $N_n(P,q) \le ([P/q] + 1)N_n(q)$ and to complete the proof it remains to use the inequality (2).

REFERENCES

1. E. Kamke, “Zur Arithmetik der Polynome,” *Math. Z.*, **19**, 247–264 (1923/24).
2. S. B. Stechkin, “Estimate of a total rational trigonometric sum,” *Tr. Mat. Inst. Steklov Akad. Nauk SSSR*, **143**, 188–207 (1977).
3. S. V. Konyagin, “On the number of solutions for a congruence of the nth power in one unknown,” *Mat. Sb.*, **109**, No. 2, 171–187 (1979); **110**, No. 1, 158 (1979).
4. N. M. Korobov, “Double trigonometrical sums and their applications,” *Mat. Zametki*, **6**, No. 1, 25–34 (1969).
5. D. A. Mit'kin, “On estimates and asymptotic formulas for rational trigonometric sums close to total ones,” *Mat. Sb.*, **122**, No. 4, 527–545 (1983).
6. I. E. Shparlinskii, “On polynomial congruences,” *Acta Arith.*, **58**, No. 2, 153–156 (1991).
7. Z. I. Borevich and I. R. Shafarevich, *Number Theory* [in Russian], Nauka, Moscow (1985).