Research Article
Distribution of Roots of Polynomial Congruences
Igor E. Shparlinski
Received 7 March 2007; Accepted 7 June 2007
Recommended by George E. Andrews

For a prime $p$, we obtain an upper bound on the discrepancy of fractions $r/p$, where $r$ runs through all of roots modulo $p$ of all monic univariate polynomials of degree $d$ whose vector of coefficients belongs to a $d$-dimensional box $B$. The bound is nontrivial starting with boxes $B$ of size $|B| \geq p^{d/2+\varepsilon}$ for any fixed $\varepsilon < 0$ and sufficiently large $p$.

Copyright © 2007 Igor E. Shparlinski. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. Introduction
For an integer $m$ and a polynomial $f(X) \in \mathbb{Z}[X]$, we consider the set of fractions

$$R_{m,f} = \left\{ \frac{r}{m} \mid f(r) \equiv 0 \pmod{m}, 0 \leq r \leq m-1 \right\},$$

that is, the set of fractions $r/m$ where $r$ runs through all distinct roots of the congruence $f(r) \equiv 0(\text{mod } m)$.

Hooley [1] has proved that for any irreducible polynomial $f(X) \in \mathbb{Z}[X]$, the sequence $M_f(X)$ of all fractions $r/m \in R_{m,f}$ taken over all nonnegative integers $m \leq X$, that is,

$$M_f(X) = \left\{ \frac{r}{m} \right\}_{r \in R_{m,f}, m \leq X},$$

is asymptotically uniformly distributed in the $[0,1]$ interval when $X \to \infty$, although the bound on the discrepancy of the sequence $M_f(X)$ is rather weak. For quadratic polynomials $f$ a stronger bound on the discrepancy has been obtained using a different method by Hooley [2], see [3, 4] for further references to more recent improvements and applications.
Furthermore, for many applications it is desirable to have a result about the uniformity of distribution of the same fractions when the modulus \( m = p \) runs only through prime numbers \( p \leq X \). Accordingly, we define the sequence

\[
\mathcal{D}_f(X) = \left\{ \frac{r}{p} \right\}_{r \in \mathbb{R}_{p,f}, p \leq X}.
\]

(1.3)

For quadratic polynomials \( f \), the uniformity of distribution of the sequence \( \mathcal{D}_f(X) \) has been shown by Duke et al. [3] and Tóth [4]. However, for arbitrary polynomials this result appears to be out of reach nowadays. Here we consider a dual question when the prime \( p \) is fixed but the polynomial \( f \) varies over some natural family of polynomials.

More precisely, for a box \( \mathcal{B} = [g_0, g_0 + h_0] \times \cdots \times [g_{d-1}, g_{d-1} + h_{d-1}) \),

(1.4)

where \( g_0, \ldots, g_{d-1} \) are arbitrary integers and the side lengths \( h_0, \ldots, h_{d-1} \leq p \) are positive integers, we use \( \mathcal{F}_d(\mathcal{B}) \) to denote the set of monic polynomials

\[
f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbb{Z}[X], \quad (a_0, \ldots, a_{d-1}) \in \mathcal{B}.
\]

(1.5)

Assuming that all integers in the interval \([g_0, g_0 + h_0)\) are nonzero modulo \( p \), we obtain upper bounds for the discrepancy of the sequence

\[
\mathcal{F}_d(p; \mathcal{B}) = \left\{ \frac{r}{p} \right\}_{r \in \mathbb{R}_{p,f}, f \in \mathcal{F}_d(\mathcal{B})}
\]

(1.6)

which are nontrivial when, for any fixed \( \epsilon > 0 \) and sufficiently large \( p \),

\[
|\mathcal{B}| \geq p^{d/2+\epsilon},
\]

(1.7)

where \( |\mathcal{B}| = h_0 \cdots h_{d-1} \) is the volume of \( \mathcal{B} \).

As the following example shows, the condition \( a_0 \not\equiv 0(\text{mod } p) \) is necessary if one wants to treat “small” boxes \( \mathcal{B} \). Indeed, if \( h_0 = 1, h_1 = \cdots = h_{d-1} = p \), and \( g_0 = \cdots = g_{d-1} = 0 \), the set \( \mathcal{F}_d(\mathcal{B}) \) is of relatively large size \( \#\mathcal{F}_d(\mathcal{B}) = p^{d-1} \) but has a very biased distribution of roots as every polynomial \( f \in \mathcal{F}_d(\mathcal{B}) \) vanishes at zero.

2. Notation

We recall that the discrepancy \( \Delta(\mathcal{A}) \) of a finite sequence \( \mathcal{A} \) of (not necessarily distinct) real numbers in the unit interval \([0, 1)\) is defined by

\[
\Delta(\mathcal{A}) = \sup_{\beta \in [0,1)} \left| \frac{N(\mathcal{J}, \mathcal{A})}{\#\mathcal{A}} - |\mathcal{J}| \right|,
\]

(2.1)

where the supremum is taken over all subintervals \( \mathcal{J} = [\beta, \gamma) \) of the interval \([0, 1)\), \( N(\mathcal{J}, \mathcal{A}) \) is the number of \( \alpha \in \mathcal{A} \cap \mathcal{J} \), and \( |\mathcal{J}| = \gamma - \beta \) is the length of \( \mathcal{J} \).

For a prime \( p \) and a real \( z \), we denote

\[
e_p(z) = \exp \frac{2\pi iz}{p}.
\]

(2.2)
We also define the “delta”-function on the residue classes modulo $p$

\[
\delta_p(v) = \begin{cases} 
1, & \text{if } v \equiv 0 \pmod{p}, \\
0, & \text{if } v \not\equiv 0 \pmod{p}.
\end{cases}
\]  

(2.3)

In particular, we use the identity

\[
\frac{1}{p} \sum_{u=0}^{p-1} e_p(uv) = \delta_p(v)
\]  

(2.4)

to express various counting functions via exponential sums.

Throughout the paper, any implied constants in symbols $O$ and $\ll$ may depend on the degree of the polynomial but are absolute otherwise. We recall that the notations $U \ll V$ and $U = O(V)$ are both equivalent to the statement that $|U| \leq cV$ holds with some constant $c > 0$.

3. Main result

**Theorem 3.1.** Suppose that the box $\mathcal{B}$ is given by (1.4) with $0 < g_0 \leq g_0 + h_0 \leq p$. Then for the discrepancy $\Delta(\mathcal{T}_d(p; \mathcal{B}))$ of the set $\mathcal{T}_d(p; \mathcal{B})$, one has

\[
\Delta(\mathcal{T}_d(p; \mathcal{B})) \ll |\mathcal{B}|^{-2/d}p(\log p)^2.
\]  

(3.1)

**Proof.** For an integer $r$, we use $\mathcal{G}_d(r, p; \mathcal{B})$ to denote the set of polynomials $f \in \mathcal{F}_d(\mathcal{B})$ with $r \in \mathcal{R}_{p,f}$. Using the identity (2.4), we write

\[
\#\mathcal{G}_d(r, p; \mathcal{B}) = \frac{1}{p} \sum_{u=0}^{p-1} e_p(u r^d) \prod_{y=0}^{d-1} \sum_{a_y = g_y} e_p(u a_y r^y)
\]  

(3.2)

Let us fix an interval $I = [\beta, \gamma) \subseteq [0, 1)$. We also recall that the condition of the theorem implies that $\mathcal{G}_d(0, p; \mathcal{B}) = \emptyset$. Then, for the number $N(I, \mathcal{T}_d(p; \mathcal{B}))$ of $r/p \in \mathcal{T}_d(p; \mathcal{B}) \cap I$ we have

\[
N(I, \mathcal{T}_d(p; \mathcal{B})) = \sum_{\beta \leq r < \gamma p} \#\mathcal{G}_d(r, p; \mathcal{B}) = \frac{|\mathcal{B}|}{p} \left( (\gamma - \beta)p + O(1) \right) + \frac{1}{p} E,
\]  

(3.3)

where

\[
|E| \leq \sum_{\beta \leq r < \gamma m} \sum_{u=1}^{p-1} \prod_{y=0}^{d-1} \sum_{a_y = g_y} e_p(u a_y r^y).
\]  

(3.4)

Let $h_i$ and $h_j$ be the two largest side lengths.
Estimating the sums over $a_\nu$ with $\nu \neq i, j$ trivially as $h_\nu$, and extending the range of summation to all $r = 1, \ldots, p - 1$, we obtain

$$|E| \ll \left| \mathcal{B} \right| \frac{p}{h_i h_j} \sum_{r=1}^{p-1} \sum_{u=1}^{p-1} |g_i h_j - 1| e_p(u a_r r') \left| \sum_{a_j = g_j} e_p(u a_j r') \right|. \quad (3.5)$$

Let $\|v\|_p$ denote the unique integer $w$ in the interval $|w| < p/2$ with $w \equiv u (\mod p)$. We now recall that for any $\nu \neq 0 (\mod p)$, we have the bound

$$\left| \sum_{a_f = f} e_p(\nu v) \right| \ll \frac{p}{\|v\|_p}, \quad (3.6)$$

that (in a more general form) dates back to Weyl [5], see also [6, Bound (8.6)].

From this bound we derive

$$|E| \ll \left| \mathcal{B} \right| \frac{p^2}{h_i h_j} \sum_{r=1}^{p-1} \sum_{u=1}^{p-1} \frac{1}{\|u r\|_p \|u r'\|_p}. \quad (3.7)$$

For each pair of integers $(s, t) \in [1, p-1]^2$ there are at most $d$ pairs of $(u, r) \in [1, p-1]^2$ with

$$u r^i \equiv s (\mod p), \quad u r^j \equiv t (\mod p), \quad (3.8)$$

(since they imply that $r^{i-j} \equiv s/t (\mod p)$ which leads to at most $|i - j| \leq d - 1$ values for $r$, each of which then leads to a unique value of $u$). Hence

$$|E| \ll \left| \mathcal{B} \right| \frac{p^2}{h_i h_j} \sum_{s=1}^{p-1} \frac{1}{\|s\|_p \|t\|_p} = \left| \mathcal{B} \right| \frac{p^2}{h_i h_j} \left( \sum_{s=1}^{p-1} \frac{1}{\|s\|_p} \right)^2 \ll \frac{\left| \mathcal{B} \right| p^2 (\log p)^2}{h_i h_j}. \quad (3.9)$$

Remarking that $h_i h_j \geq \left| \mathcal{B} \right|^{2/d}$ and using (3.3), we obtain

$$N(\mathcal{A}, \mathcal{P}_d(p; \mathcal{B})) = (\gamma - \beta) |\mathcal{B}| + O\left( |\mathcal{B}| p^{-1} + |\mathcal{B}|^{-1/2} p (\log p)^2 \right). \quad (3.10)$$

Since $|\mathcal{B}| \leq p^d$, the first term never dominates and we obtain

$$N(\mathcal{A}, \mathcal{P}_d(p; \mathcal{B})) = (\gamma - \beta) |\mathcal{B}| + O\left( |\mathcal{B}|^{-1/2} p (\log p)^2 \right). \quad (3.11)$$

Using the above bound also with $\beta = 0, \gamma = 1$, we conclude the proof. \qed

4. Remarks

There are several natural generalisations of our result which lead to interesting open questions.

For example, motivated by the approach of [7] one can ask the following question.
Open Question. Obtain an upper bound on the discrepancy of the point set \((r_1/p, \ldots, r_k/p)\) formed by the roots of systems of \(k\) polynomial congruences in \(k\) variables

\[ f_j(r_1, \ldots, r_k) \equiv 0 \pmod{p}, \quad j = 1, \ldots, k, \quad (4.1) \]

with all polynomials of total degree \(d\) whose coefficients belong to a prescribed box.

It is well known that using the Bombieri bound \([8]\), one can prove that the discrepancy \(D_{p,f}\) of the point set \((r_1/p, r_2/p)\) arising from points on an absolutely irreducible curve

\[ f(r_1, r_2) \equiv 0 \pmod{p} \quad (4.2) \]

of degree \(d \geq 2\) satisfies

\[ D_{p,f} = O\left(p^{-1/2} (\log p)^2\right); \quad (4.3) \]

see \([9]\) for various generalisations of this result and further references.

References

Submit your manuscripts at http://www.hindawi.com