Hindawi Publishing Corporation
International Journal of Mathematics and Mathematical Sciences
Volume 2007, Article ID 37853, 5 pages
doi:10.1155/2007/37853

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 $\mathcal{B}$. The bound is nontrivial starting with boxes $\mathcal{B}$ of size $|\mathcal{B}| \geq p^{d/2+\varepsilon}$ for any fixed $\varepsilon < 0$ and sufficiently large p.

1. Introduction

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

$$\mathcal{R}_{m,f} = \left\{ \frac{r}{m} \mid f(r) \equiv 0 \ (\operatorname{mod} m),\ 0 \leq r \leq m-1 \right\}, \tag{1.1}$$

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

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

$$\mathcal{M}_f(X) = \left\{ \frac{r}{m} \right\}_{r \in \mathcal{R}_{m,f},\, m \leq X}, \tag{1.2}$$

is asymptotically uniformly distributed in the $[0,1]$ interval when $X \to \infty$, although the bound on the *discrepancy* of the sequence $\mathcal{M}_f(X)$ 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 $p \le X$. Accordingly, we define the sequence

$$\mathcal{Q}_f(X) = \left\{\frac{r}{p}\right\}_{r\in\mathcal{R}_{p,f},\, p\le X}. \tag{1.3}$$

For quadratic polynomials f, the uniformity of distribution of the sequence $\mathcal{Q}_f(X)$ 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

$$\mathcal{B} = [g_0, g_0 + h_0) \times \cdots \times [g_{d-1}, g_{d-1} + h_{d-1}), \tag{1.4}$$

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

$$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbb{Z}[X], \quad (a_0,\dots,a_{d-1}) \in \mathcal{B}. \tag{1.5}$$

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

$$\mathcal{T}_d(p;\mathcal{B}) = \left\{\frac{r}{p}\right\}_{r\in\mathcal{R}_{p,f},\, f\in\mathcal{F}_d(\mathcal{B})} \tag{1.6}$$

which are nontrivial when, for any fixed $\varepsilon > 0$ and sufficiently large p,

$$|\mathcal{B}| \ge p^{d/2+\varepsilon}, \tag{1.7}$$

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

As the following example shows, the condition $a_0 \not\equiv 0 \pmod p$ 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

$$\Delta(\mathcal{A}) = \sup_{\mathcal{I}\subseteq[0,1)} \left| \frac{N(\mathcal{I},\mathcal{A})}{\#\mathcal{A}} - |\mathcal{I}| \right|, \tag{2.1}$$

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

For a prime p and a real z, we denote

$$\mathbf{e}_p(z) = \exp\frac{2\pi i z}{p}. \tag{2.2}$$

We also define the "delta"-function on the residue classes modulo p

$$\delta_p(v) = \begin{cases} 1, & \text{if } v \equiv 0 (\operatorname{mod} p), \\ 0, & \text{if } v \not\equiv 0 (\operatorname{mod} p). \end{cases} \tag{2.3}$$

In particular, we use the identity

$$\frac{1}{p} \sum_{u=0}^{p-1} \mathbf{e}_p(uv) = \delta_p(v) \tag{2.4}$$

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 $|U| \le cV$ holds with some constant $c > 0$.

3. Main result

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

$$\Delta(\mathcal{T}_d(p;\mathcal{B})) \ll |\mathcal{B}|^{-2/d} p (\log p)^2. \tag{3.1}$$

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

$$\begin{aligned} \#\mathcal{G}_d(r,p;\mathcal{B}) &= \frac{1}{p} \sum_{u=0}^{p-1} \mathbf{e}_p(ur^d) \prod_{\nu=0}^{d-1} \sum_{a_\nu = g_\nu}^{g_\nu + h_\nu - 1} \mathbf{e}_p(ua_\nu r^\nu) \\ &= \frac{|\mathcal{B}|}{p} + \frac{1}{p} \sum_{u=1}^{p-1} \mathbf{e}_p(ur^d) \prod_{\nu=0}^{d-1} \sum_{a_\nu = g_\nu}^{g_\nu + h_\nu - 1} \mathbf{e}_p(ua_\nu r^\nu). \end{aligned} \tag{3.2}$$

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

$$N(\mathcal{I}, \mathcal{T}_d(p;\mathcal{B})) = \sum_{\beta p \le r < \gamma p} \#\mathcal{G}_d(r,p;\mathcal{B}) = \frac{|\mathcal{B}|}{p}((\gamma - \beta)p + O(1)) + \frac{1}{p} E, \tag{3.3}$$

where

$$|E| \le \sum_{\substack{\beta m \le r < \gamma m \\ r \ne 0}} \sum_{u=1}^{p-1} \prod_{\nu=0}^{d-1} \left| \sum_{a_\nu = g_\nu}^{g_\nu + h_\nu - 1} \mathbf{e}_p(ua_\nu r^\nu) \right|. \tag{3.4}$$

Let h_i and h_j be the two largest side lengths.

Estimating the sums over a_ν with $\nu \neq i, j$ trivially as h_ν, and extending the range of summation to all $r = 1, \dots, p-1$, we obtain

$$|E| \ll \frac{|\mathcal{B}|}{h_i h_j} \sum_{r=1}^{p-1} \sum_{u=1}^{p-1} \left| \sum_{a_i=g_i}^{g_i+h_i-1} \mathbf{e}_p\left(u a_i r^i\right) \right| \left| \sum_{a_j=g_j}^{g_j+h_j-1} \mathbf{e}_p\left(u a_j r^j\right) \right|. \tag{3.5}$$

Let $\|v\|_p$ denote the unique integer w in the interval $|w| < p/2$ with $w \equiv u(\operatorname{mod} p)$. We now recall that for any $v \not\equiv 0(\operatorname{mod} p)$, we have the bound

$$\left| \sum_{a=f}^{f+h-1} \mathbf{e}_p(av) \right| \ll \frac{p}{\|v\|_p}, \tag{3.6}$$

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

From this bound we derive

$$|E| \ll \frac{|\mathcal{B}| p^2}{h_i h_j} \sum_{r=1}^{p-1} \sum_{u=1}^{p-1} \frac{1}{\|ur^i\|_p \|ur^j\|_p}. \tag{3.7}$$

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

$$ur^i \equiv s(\operatorname{mod} p), \qquad ur^j \equiv t(\operatorname{mod} p), \tag{3.8}$$

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

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

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

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

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

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

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

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

$$f_j(r_1,\ldots,r_s) \equiv 0 (\operatorname{mod} p), \quad j = 1,\ldots,k, \tag{4.1}$$

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

$$f(r_1, r_2) \equiv 0 (\operatorname{mod} p) \tag{4.2}$$

of degree $d \geq 2$ satifies

$$D_{p,f} = O(p^{-1/2}(\log p)^2); \tag{4.3}$$

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

References

[1] C. Hooley, "On the distribution of the roots of polynomial congruences," *Mathematika*, vol. 11, pp. 39–49, 1964.

[2] C. Hooley, "On the greatest prime factor of a quadratic polynomial," *Acta Mathematica*, vol. 117, no. 1, pp. 281–299, 1967.

[3] W. Duke, J. B. Friedlander, and H. Iwaniec, "Equidistribution of roots of a quadratic congruence to prime moduli," *Annals of Mathematics*, vol. 141, no. 2, pp. 423–441, 1995.

[4] Á. Tóth, "Roots of quadratic congruences," *International Mathematics Research Notices*, vol. 2000, no. 14, pp. 719–739, 2000.

[5] H. Weyl, "Zur Abschätzung von $\zeta(1+it)$," *Annals of Mathematics*, vol. 10, pp. 88–101, 1921.

[6] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, vol. 53 of *American Mathematical Society Colloquium Publications*, American Mathematical Society, Providence, RI, USA, 2004.

[7] B. Poonen and J. F. Voloch, "Random Diophantine equations," in *Arithmetic of Higher-Dimensional Algebraic Varieties (Palo Alto, Calif, 2002)*, vol. 226 of *Progr. Math.*, pp. 175–184, Birkhäuser, Boston, Mass, USA, 2004.

[8] E. Bombieri, "On exponential sums in finite fields," *American Journal of Mathematics*, vol. 88, no. 1, pp. 71–105, 1966.

[9] A. Granville, I. E. Shparlinski, and A. Zaharescu, "On the distribution of rational functions along a curve over $\mathbb{F}_p$ and residue races," *Journal of Number Theory*, vol. 112, no. 2, pp. 216–237, 2005.

Igor E. Shparlinski: Department of Computing, Macquarie University, Sydney 2109, NSW, Australia
Email address: igor@ics.mq.edu.au