Canad. Math. Bull. Vol. **54** (4), 2011 pp. 748–756
doi:10.4153/CMB-2011-053-0

On the Distribution of Irreducible Trinomials

Igor E. Shparlinski

Abstract. We obtain new results about the number of trinomials $t^n + at + b$ with integer coefficients in a box $(a, b) \in [C, C + A] \times [D, D + B]$ that are irreducible modulo a prime p. As a by-product we show that for any p there are irreducible polynomials of height at most $p^{1/2+o(1)}$, improving on the previous estimate of $p^{2/3+o(1)}$ obtained by the author in 1989.

1 Introduction

For a fixed integer $n \geq 2$, we consider the family of trinomials

$$f_{a,b}(T) = T^n + aT + b \tag{1}$$

with integer coefficients.

Given a prime p and a box

$$\Pi = [C, C + A] \times [D, D + B] \tag{2}$$

with some real numbers A, B, C, D we denote by $N_{n,p}(\Pi)$ the number of pairs of integers $(a, b) \in \Pi$, such that $f_{a,b}(T)$ is irreducible modulo p.

Using some ideas of [3], we obtain an asymptotic formula for $N_{n,p}(\Pi)$ that is nontrivial, provided that the side lengths A and B of Π satisfy

$$\min\{A, B\} \geq p^{1/4+\varepsilon} \quad \text{and} \quad AB \geq p^{1+\varepsilon}$$

for some fixed $\varepsilon > 0$ and sufficiently large p.

More precisely, we have the following result.

Theorem 1 *For a prime p and a box Π given by (2) for some real numbers A, B, C, D with $p > A, B \geq 1$, we have the bound*

$$\begin{aligned}\Big| N_{n,p}(\Pi) - \frac{1}{n}AB\Big| &\leq \min\{AB^{1-1/\nu} p^{(\nu+1)/(4\nu^2)} + A^{1/2}Bp^{1/4} + A^{1/2}B^{1/2}p^{1/2},\\ &\qquad A^{1-1/\nu}Bp^{(\nu+1)/(4\nu^2)} + AB^{1/2}p^{1/4} + A^{1/2}B^{1/2}p^{1/2}\}p^{o(1)}\end{aligned}$$

as $p \to \infty$ with any fixed integer $\nu \geq 1$, where the function implied by $o(1)$ depends only on n and ν.

Received by the editors September 25, 2008; revised February 6, 2009.
Published electronically March 24, 2011.
During the preparation of this paper, the author was supported in part by ARC Grant DP0556431.
AMS subject classification: **11L40**, 11T06.
Keywords: irreducible trinomials, character sums.

Let $h_n(p)$ denote the smallest height of monic polynomials of degree n over $\mathbb{Z}$ that are irreducible modulo p (recall the height is the largest absolute value of the coefficients).

In particular, taking $A = B = \lceil p^{1/2+\varepsilon} \rceil$ for some $\varepsilon > 0$ and $C = D = 0$, choosing $\nu = 1$ in Theorem 1, we obtain $N_{n,p}(\Pi) = p^{\varepsilon}/n + O(p^{\varepsilon/2})$ for the corresponding box Π. Since ε is arbitrary, we derive the following corollary.

Corollary 2 *For all primes p, $h_n(p) \le p^{1/2+o(1)}$ as $p \to \infty$.*

Corollary 2 improves the previous estimate of $h_n(p) \le p^{2/3+o(1)}$ of [8] obtained in 1989 (the proof also uses irreducible trinomials), see also [10, Theorem 3.11].

We also remark that it follows from a result of L. M. Adleman and H. W. Lenstra [1] that, under the Extended Riemann Hypothesis, there are irreducible modulo p monic polynomials of height $O(\log^{2n} p)$. It is further shown in [9] that for any fixed $n \ge 2$ and an arbitrary function $\vartheta(x) \to \infty$, for almost all primes p in the interval $[N - M, N]$ of length $M > N^{7/12+\varepsilon}$ (with arbitrary $\varepsilon > 0$) there is an irreducible modulo p polynomial of degree n and of height at most $\vartheta(p)$. However Corollary 2 appears to be the strongest known unconditional result that holds for all primes.

2 Preparations

2.1 Notation

Throughout this paper, we use $U = O(V)$, $U \ll V$, and $V \gg U$ as equivalents of the inequality $|U| \le cV$ for some constant $c > 0$, which may depend only on the integer parameters n and ν.

We write $\log x$ for the maximum of 1 and the natural logarithm of x, thus we always have $\log x \ge 1$.

For a prime p, we use $\mathbb{F}_p$ to denote the field of p elements which we assume to be represented by the set $\{0, \dots, p-1\}$.

Let $\mathcal{X}_p$ be the set of multiplicative characters of $\mathbb{F}_p$; we refer to [7, Chapter 3] for the necessary background on multiplicative characters. We also use χ_0 to denote the principal character of $\mathbb{F}_p$, and $\mathcal{X}_p^* = \mathcal{X}_p \setminus \{\chi_0\}$ to denote the set of nonprincipal characters.

2.2 Character Sums

We recall the following orthogonality relations. For any divisor $d \mid p-1$,

$$\frac{1}{d} \sum_{\substack{\chi \in \mathcal{X}_p \\ \chi^d = \chi_0}} \chi(w) = \begin{cases} 1, & \text{if } w = u^d \text{ for some } u \in \mathbb{F}_p^*, \\ 0, & \text{otherwise,} \end{cases} \tag{3}$$

and

$$\frac{1}{p-1} \sum_{r \in \mathbb{F}_p} \chi_1(r)\overline{\chi}_2(r) = \begin{cases} 1, & \text{if } \chi_1 = \chi_2, \\ 0, & \text{otherwise,} \end{cases} \tag{4}$$

https://doi.org/10.4153/CMB-2011-053-0 Published online by Cambridge University Press

for all $\nu \in \mathbb{F}_p$ and $\chi_1, \chi_2 \in \mathcal{X}_p$ (here, $\overline{\chi}_2$ is the character obtained from χ_2 by complex conjugation).

The following result combines the Pólya–Vinogradov bound (for $\nu = 1$) with the Burgess bounds (for $\nu \geq 2$); see [7, Theorems 12.5 and 12.6]:

Lemma 3 *Uniformly for all primes p, and real X, Y with $p > X \geq 1$, for all characters $\chi \in \mathcal{X}_p^*$, we have*

$$\Big| \sum_{Y \leq x \leq Y+X} \chi(x) \Big| \leq p^{(\nu+1)/(4\nu^2)+o(1)} X^{1-1/\nu}$$

as $p \to \infty$ with any fixed integer $\nu \geq 1$, where the function implied by $o(1)$ depends only on ν.

The next bound is due to Ayyad, Cochrane and Zheng [2, Theorem 2]; see also the result of Friedlander and Iwaniec [6].

Lemma 4 *Uniformly for all real X, Y with $p > X \geq 1$, we have*

$$\sum_{\chi \in \mathcal{X}_p^*} \Big| \sum_{Y \leq x \leq Y+X} \chi(x) \Big|^4 \leq p X^{2+o(1)}$$

as $p \to \infty$.

2.3 Irreducibility

We recall a very special case of a result of S. D. Cohen [4] about the distribution of irreducible polynomials over a finite field $\mathbb{F}_q$ of q elements, see also [5].

Let $\mathcal{T}_{n,p}$ be the set of pairs (r, s) with $r, s \in \mathbb{F}_p^*$ such that $f_{r,s}(T)$ given by (1) is irreducible over $\mathbb{F}_p$.

Lemma 5 *For any prime p,*

$$\#\mathcal{T}_{n,p} = \frac{1}{n} p^2 + O(p^{3/2}).$$

We also make the following trivial observation.

Lemma 6 *If a trinomial $f_{r,s}(T) \in \mathbb{F}_p[T]$ is irreducible, then so are all trinomials $f_{ru^{n-1},su^n}(T)$ with $u \in \mathbb{F}_p^*$.*

Clearly, for $r, s \in \mathbb{F}_p^*$ there are exactly $p - 1$ distinct polynomials that can be obtained this way.

3 Proof of Theorem 1

3.1 Idea of the Proof

We see from Lemma 6 that in order to establish the desired result it is enough, for a given irreducible trinomial $f_{r,s}(T) \in \mathbb{F}_p[T]$, to estimate the cardinality of the set

https://doi.org/10.4153/CMB-2011-053-0 Published online by Cambridge University Press

$\mathcal{U}_{n,p}(\Pi; r, s)$ of $u \in \mathbb{F}_p^*$ such that the residues modulo p of ru^{n-1} and su^n which belong to the intervals $[C, C + A]$ and $[D, D + B]$, respectively, where Π is given by (2).

One certainly expects $\#\mathcal{U}_{n,p}(\Pi; r, s)$ to be about AB/p, and our task is to prove this for as small values of A and B as possible. We also note that it is enough to estimate the deviation $|\#\mathcal{U}_{n,p}(\Pi; r, s) - AB/p|$ on average over all $r, s \in \mathcal{T}_{n,p}$. Furthermore, since by Lemma 5 this is set very large, we can simply estimate the above deviation on average over all $r, s \in \mathbb{F}_p$. Thus we concentrate on the distribution of the set

$$\{(ru^{n-1}, su^n) : u \in \mathbb{F}_p\} \tag{5}$$

inside of the box Π, on average over $r, s \in \mathbb{F}_p$.

In fact, a similar argument has already been used in [8]. However, here we follow the technique of [3], which is based on the use of the character sum instead of exponential sums (which were used in [8]). This allows us to use some rather powerful tools which have no analogues for exponential sums (such as Lemmas 3 and 4). In turn, this leads to stronger results.

3.2 Simultaneous Distribution of Powers in Intervals

Let

$$\sigma_p(U) = \max_{\chi \in \mathcal{X}_p^*} \max_{V \in \mathbb{R}} \Big\{ 1, \Big| \sum_{V \le u \le V+U} \chi(u) \Big| \Big\}.$$

We begin by investigating the distribution of the second component su^n of the pairs (5). Accordingly, for an interval $\mathcal{J} = [D, D + B]$ and $s \in \mathbb{F}_p$ we define

$$\mathcal{U}_{n,p}(\mathcal{J}; s) = \{u \in \mathbb{F}_p^* : su^n \equiv w \pmod p, \text{ where } w \in \mathcal{J}\}.$$

We have the following asymptotic formula for the cardinality of $\mathcal{U}_{n,p}(\mathcal{J}; s)$:

Lemma 7 *For all primes p, intervals $\mathcal{J} = [D, D + B]$ with $p > B \ge 1$, and $s \in \mathbb{F}_p^*$, we have*

$$\#\mathcal{U}_{n,p}(\mathcal{J}; s) = B + O\big(\sigma_p(B)\big).$$

Proof Let $d = \gcd(n, p - 1)$. By the orthogonality relation (3), for all $w \in \mathbb{F}_p^*$ we have

$$\#\{u \in \mathbb{F}_p^* : u^n = w\} = \#\{u \in \mathbb{F}_p^* : u^d = w\} = \sum_{\substack{\chi \in \mathcal{X}_p \\ \chi^d = \chi_0}} \chi(w).$$

Let $\bar{s}$ be an integer such that $s\bar{s} \equiv 1 \pmod p$. Separating the contribution of $B+O(1)$ from the principal character χ_0, we see that

$$\#\mathcal{U}_{n,p}(\mathcal{J}; s) = \sum_{w \in \mathcal{J}} \sum_{\substack{\chi \in \mathcal{X}_p \\ \chi^d = \chi_0}} \chi(\bar{s}w) = B + O(1) + \sum_{\substack{\chi \in \mathcal{X}_p^* \\ \chi^d = \chi_0}} \overline{\chi}(s) \sum_{w \in \mathcal{J}} \chi(w).$$

Since the inner sum is bounded by $\sigma_p(B)$ and

$$\#\{\chi \in \mathcal{X}_p^* : \chi^d = \chi_0\} = d - 1 < n,$$

the result follows. ∎

https://doi.org/10.4153/CMB-2011-053-0 Published online by Cambridge University Press

We now take into account the distribution of the first component ru^{n-1} of the pairs (5). For a box Π given by (2) and $r, s \in \mathbb{F}_p$ we define

$$\#\mathcal{U}_{n,p}(\Pi; s, r) = \{u \in \mathcal{U}_{n,p}(\mathcal{J}; s) : ru^{n-1} \equiv v \pmod p, \text{ where } v \in \mathcal{I}\},$$

where $\mathcal{I} = [C, C + A]$ and, as before, $\mathcal{J} = [D, D + B]$.

Lemma 8 *For all primes p, boxes Π given by (2) for some real numbers A, B, C, D with $p > A, B \geq 1$, and $s \in \mathbb{F}_p^*$, we have*

$$\sum_{r \in \mathbb{F}_p} \left| \#\mathcal{U}_{n,p}(\Pi; s, r) - \frac{A \cdot \#\mathcal{U}_{n,p}(\mathcal{J}; s)}{p} \right| \leq A^{1/2} B p^{1/4+o(1)} + A^{1/2} B^{1/2} p^{1/2+o(1)}$$

as $p \to \infty$.

Proof We can assume that $AB > p$, since the result is trivial otherwise. Indeed, if $AB \leq p$, then $A^{1/2}B^{1/2}p^{1/2} \geq AB$, while

$$\begin{aligned}\sum_{r \in \mathbb{F}_p} &\left| \#\mathcal{U}_{n,p}(\Pi; s, r) - \frac{A \cdot \#\mathcal{U}_{n,p}(\mathcal{J}; s)}{p} \right| \\ &\leq \sum_{r \in \mathbb{F}_p} \#\mathcal{U}_{n,p}(\Pi; s, r) + A \cdot \#\mathcal{U}_{n,p}(\mathcal{J}; s) \ll AB.\end{aligned}$$

For every $a \in \mathbb{F}_p^*$, let $\overline{a}$ be an integer such that $a\overline{a} \equiv 1 \pmod p$. Using (3) and separating the contribution of $\big(A + O(1)\big)\, \#\mathcal{U}_{n,p}(\mathcal{J}; s)$ from the principal character χ_0, it follows that

$$\begin{aligned}\#&\mathcal{U}_{r,s}(A, B; p) \\ &= \sum_{u \in \mathcal{U}_{n,p}(\mathcal{J}; s)} \sum_{a \in \mathcal{I}} \frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p} \chi(ru^{n-1}\overline{a}) \\ &= \frac{A \cdot \#\mathcal{U}_{n,p}(\mathcal{J}; s)}{p-1} + O(1) \frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p^*} \chi(r) \sum_{u \in \mathcal{U}_{n,p}(\mathcal{J}; s)} \chi(u^{n-1}) \sum_{a \in \mathcal{I}} \overline{\chi}(a).\end{aligned}$$

Since

$$\frac{A \cdot \#\mathcal{U}_{n,p}(\mathcal{J}; s)}{p} - \frac{A \cdot \#\mathcal{U}_{n,p}(\mathcal{J}; s)}{p-1} \ll \frac{A \cdot \#\mathcal{U}_{n,p}(\mathcal{J}; s)}{p^2} \ll \frac{AB}{p^2} \ll 1,$$

we have

$$\sum_{r \in \mathbb{F}_p} \left| \#\mathcal{U}_{n,p}(\Pi; s, r) - \frac{A \cdot \#\mathcal{U}_{n,p}(\mathcal{J}; s)}{p} \right| \ll p + W, \tag{6}$$

where

$$W = \frac{1}{p} \sum_{r \in \mathbb{F}_p} \Big| \sum_{\chi \in \mathcal{X}_p^*} \chi(r) \sum_{u \in \mathcal{U}_{n,p}(\mathcal{J};s)} \chi(u^{n-1}) \sum_{a \in \mathcal{I}} \overline{\chi}(a) \Big|.$$

By the Cauchy inequality,

$$\begin{aligned} W^2 &\le \frac{1}{p} \sum_{r \in \mathbb{F}_p} \Big| \sum_{\chi \in \mathcal{X}_p^*} \chi(r) \sum_{u \in \mathcal{U}_{n,p}(\mathcal{J};s)} \chi(u^{n-1}) \sum_{a \in \mathcal{I}} \overline{\chi}(a) \Big|^2 \\ &= \frac{1}{p} \sum_{\chi_1, \chi_2 \in \mathcal{X}_p^*} \sum_{u_1, u_2 \in \mathcal{U}_{n,p}(\mathcal{J};s)} \chi_1(u_1^{n-1}) \overline{\chi}_2(u_2^{n-1}) \\ &\qquad \sum_{a_1, a_2 \in \mathcal{I}} \overline{\chi}_1(a_1) \chi_2(a_2) \sum_{r \in \mathbb{F}_p} \chi_1(r) \overline{\chi}_2(r). \end{aligned}$$

Using the orthogonality relation (4) we deduce that

$$W^2 \le \sum_{\chi \in \mathcal{X}_p^*} \Big| \sum_{u \in \mathcal{U}_{n,p}(\mathcal{J};s)} \chi(u^{n-1}) \Big|^2 \Big| \sum_{|a| \le A} \chi(a) \Big|^2.$$

Applying the Cauchy inequality again, it follows that

$$W^4 \le \sum_{\chi \in \mathcal{X}_p^*} \Big| \sum_{u \in \mathcal{U}_{n,p}(\mathcal{J};s)} \chi(u^{n-1}) \Big|^4 \cdot \sum_{\chi \in \mathcal{X}_p^*} \Big| \sum_{|a| \le A} \chi(a) \Big|^4. \tag{7}$$

The second sum is of size $O(p^{1+o(1)}A^2)$ by Lemma 4. For the first sum, we extend the summation to include the trivial character $\chi = \chi_0$, obtaining

$$\sum_{\chi \in \mathcal{X}_p^*} \Big| \sum_{u \in \mathcal{U}_{n,p}(\mathcal{J};s)} \chi(u^{n-1}) \Big|^4 \le \sum_{\chi \in \mathcal{X}_p} \Big| \sum_{u \in \mathcal{U}_{n,p}(\mathcal{J};s)} \chi(u^{n-1}) \Big|^4 = pT,$$

where T is the number of solutions to the congruence

$$u_1^{n-1} u_2^{n-1} \equiv u_3^{n-1} u_4^{n-1} \pmod{p}, \quad u_1, u_2, u_3, u_4 \in \mathcal{U}_{n,p}(\mathcal{J};s).$$

Note that T does not exceed the number of quadruples (u_1, u_2, u_3, u_4) in $\mathcal{U}_{n,p}(\mathcal{J};s)^4$ for which

$$u_1^{n(n-1)} u_2^{n(n-1)} \equiv u_3^{n(n-1)} u_4^{n(n-1)} \pmod{p}.$$

Since $su_j^n \equiv w_j \pmod{p}$ for some w_j with $w_j \in \mathcal{J}$, and each w_j corresponds to at most n values of u_j, it follows that $T \le n^4 R$, where R is the number of solutions to the congruence

$$w_1^{n-1} w_2^{n-1} \equiv w_3^{n-1} w_4^{n-1} \pmod{p}, \quad w_1, w_2, w_3, w_4 \in \mathcal{J}.$$

https://doi.org/10.4153/CMB-2011-053-0 Published online by Cambridge University Press

Clearly, $R \le (n-1)Q$, where Q is the largest number of solutions to the congruence

$$w_1 w_2 \equiv \rho w_3 w_4 \pmod p, \qquad w_1, w_2, w_3, w_4 \in \mathcal{J},$$

taken over all integers ρ with $\rho^{n-1} \equiv 1 \pmod p$. Writing

$$\begin{aligned} Q &= \frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p} \sum_{w_1, w_2, w_3, w_4 \in \mathcal{J}} \chi(w_1 w_2) \overline{\chi}(\rho w_3 w_4) \\ &\le \frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p} \Big| \sum_{w \in \mathcal{J}} \chi(w) \Big|^4 \\ &= \frac{\big(B + O(1)\big)^4}{p-1} + \frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p^*} \Big| \sum_{w \in \mathcal{J}} \chi(w) \Big|^4 \end{aligned}$$

and using Lemma 4 again, we see that

$$T \ll R \ll Q \ll B^4 p^{-1} + B^2 p^{o(1)}.$$

Collecting the above estimates and substituting them into (7) we deduce that

$$W^4 \ll p^{2+o(1)} A^2 (B^4 p^{-1} + B^2),$$

which together with (6) implies that

$$\begin{aligned} \sum_{r \in \mathbb{F}_p} \Big| \# \mathcal{U}_{n,p}(\Pi; s, r) - \frac{A \cdot \# \mathcal{U}_{n,p}(\mathcal{J}; s)}{p} \Big| \\ \ll p + A^{1/2} B p^{1/4+o(1)} + A^{1/2} B^{1/2} p^{1/2+o(1)}. \end{aligned}$$

Finally, for $AB > p$ we have $p < A^{1/2} B^{1/2} p^{1/2}$, and the result follows. ∎

Combining Lemmas 7 and 8 we immediately obtain:

Corollary 9 *For all primes p, boxes Π given by (2) for some real numbers A, B, C, D with $p > A, B \ge 1$, and $s \in \mathbb{F}_p^*$, we have*

$$\begin{aligned} \sum_{r \in \mathbb{F}_p} \Big| \# \mathcal{U}_{n,p}(\Pi; s, r) - \frac{AB}{p} \Big| \\ \ll A \sigma_p(B) + A^{1/2} B p^{1/4+o(1)} + A^{1/2} B^{1/2} p^{1/2+o(1)}. \end{aligned}$$

https://doi.org/10.4153/CMB-2011-053-0 Published online by Cambridge University Press

3.3 Concluding the Proof

We say that two trinomials $f_{r_1,s_1}(T), f_{r_2,s_2}(T) \in \mathbb{F}_p[T]$ are equivalent if $r_1 = u^{n-1}r_2$ and $s_1 = u^n s_2$ for some $u \in \mathbb{F}_p$. Clearly all trinomials $f_{r,s}(T) \in \mathbb{F}_p[T]$ with $r, s \in \mathbb{F}_p^*$ fall into $p-1$ equivalent classes of $p-1$ elements each.

Thus, we see from Lemma 6 that

$$N_{n,p}(\Pi; r, s) = \frac{1}{p-1} \sum_{(r,s)\in \mathfrak{T}_{n,p}} \#\mathfrak{U}_{n,p}(\Pi; r, s) + O(p)$$

(where the term $O(p)$ accounts for the contribution coming from irreducible binomials).

Therefore,

$$\begin{aligned} N_{n,p}(\Pi) - \frac{\#\mathfrak{T}_{n,p}}{p(p-1)} AB &= \frac{1}{p-1} \sum_{(r,s)\in \mathfrak{T}_{n,p}} \Big(\#\mathfrak{U}_{n,p}(\Pi; s, r) - \frac{AB}{p} \Big) + O(p) \\ &\le \frac{1}{p-1} \sum_{(r,s)\in \mathfrak{T}_{n,p}} \Big| \#\mathfrak{U}_{n,p}(\Pi; s, r) - \frac{AB}{p} \Big| + O(p) \\ &\le \frac{1}{p-1} \sum_{s\in \mathbb{F}_p^*} \sum_{r\in \mathbb{F}_p} \Big| \#\mathfrak{U}_{n,p}(\Pi; s, r) - \frac{AB}{p} \Big| + O(p). \end{aligned}$$

Applying Lemma 5 and Corollary 9 we obtain

$$\begin{aligned} &N_{n,p}(\Pi) - \frac{1}{n}AB \\ &\qquad \ll ABp^{-1/2} + A\sigma_p(B) + A^{1/2}Bp^{1/4+o(1)} + A^{1/2}B^{1/2}p^{1/2+o(1)} + p. \end{aligned}$$

As in the proof of Lemma 8, we can assume that $AB > p$ since the bound of Theorem 1 is trivial otherwise. In this case

$$A^{1/2}B^{1/2}p^{1/2} \ge p.$$

Since $p > A, B \ge 1$, we also have

$$A^{1/2}B^{1/2}p^{1/2} \ge ABp^{-1/2}.$$

Therefore (3.3) simplifies as

$$N_{n,p}(\Pi) - \frac{1}{n}AB \ll A\sigma_p(B) + A^{1/2}Bp^{1/4+o(1)} + A^{1/2}B^{1/2}p^{1/2+o(1)}.$$

It is easy to see that the roles of r and s can be interchanged in the above arguments, and this leads to the bound

$$N_{n,p}(\Pi) - \frac{1}{n}AB \ll \sigma_p(A)B + AB^{1/2}p^{1/4+o(1)} + A^{1/2}B^{1/2}p^{1/2+o(1)}.$$

Recalling Lemma 3, we conclude the proof.

References

[1] L. M. Adleman and H. W. Lenstra, *Finding irreducible polynomials over finite fields.* In: Proc. 18th ACM Symp. Theory Comput. (Berkeley, 1986), ACM, New York, 1986, 350–355.

[2] A. Ayyad, T. Cochrane and Z. Zheng, *The congruence* $x_1x_2 \equiv x_3x_4 \pmod{p}$, *the equation* $x_1x_2 = x_3x_4$ *and the mean value of character sums.* J. Number Theory **59** (1996), 398–413. doi:10.1006/jnth.1996.0105

[3] W. D. Banks and I. E. Shparlinski, *Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height.* Israel J. Math. **173**(2009), 253–277. doi:10.1007/s11856-009-0091-0

[4] S. D. Cohen, *The distribution of polynomials over finite fields.* Acta Arith. **17** (1970), 255–271.

[5] ———, *Uniform distribution of polynomials over finite fields.* J. London Math. Soc. **6** (1972), 93–102. doi:10.1112/jlms/s2-6.1.93

[6] J. B. Friedlander and H. Iwaniec, *The divisor problem for arithmetic progressions.* Acta Arith. **45** (1985), 273–277.

[7] H. Iwaniec and E. Kowalski, *Analytic number theory.* Amer. Math. Soc., Providence, RI, 2004.

[8] I. E. Shparlinski, *Distribution of primitive and irreducible polynomials modulo a prime.* (Russian) Diskret. Mat. **1** (1989), 117–124; translation in Discrete Math. Appl. **1** (1991), 59–67.

[9] ———, *On irreducible polynomials of small height in finite fields.* Appl. Algebra Engrg. Comm. Comput. **4**(1996), no. 6, 427–431. doi:10.1007/s002000050043

[10] ———, *Finite fields: Theory and computation.* Kluwer Acad. Publ., Dordrecht, 1999.

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor@ics.mq.edu.au