Rev. Mat. Iberoam. **32** (2016), no. 4, 1127–1136 © European Mathematical Society
DOI 10.4171/RMI/909

Polynomial values in small subgroups of finite fields

Igor E. Shparlinski

Abstract. For a large prime p, and a polynomial f over a finite field $\mathbb{F}_p$ of p elements, we obtain a lower bound on the size of the multiplicative subgroup of $\mathbb{F}_p^*$ containing $H \ge 1$ consecutive values $f(x)$, $x = u+1, \dots, u+H$, uniformly over $f \in \mathbb{F}_p[X]$ and an $u \in \mathbb{F}_p$.

1. Introduction

1.1. Background

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

For a rational function $r(X) = f(X)/g(X) \in \mathbb{F}_p(X)$ with two relatively primes polynomials $f, g \in \mathbb{F}_p[X]$ and a set $\mathcal{S} \subseteq \mathbb{F}_p$, we use $r(\mathcal{S})$ to denote the value set

$$r(\mathcal{S}) = \{r(x) \; : \; x \in \mathcal{S}, \; g(x) \neq 0\} \subseteq \mathbb{F}_p.$$

Given two sets $\mathcal{S}, \mathcal{T} \subseteq \mathbb{F}_p$, we consider the size of the intersection of $r(\mathcal{S})$ and $\mathcal{T}$, that is,

$$N_r(\mathcal{S}, \mathcal{T}) = \#\left(r(\mathcal{S}) \cap \mathcal{T}\right).$$

A large variety of upper bounds on $N_r(\mathcal{S}, \mathcal{T})$ and its multivariate generalisations, for various sets and $\mathcal{S}$ and $\mathcal{T}$ (such as intervals, subgroups, zero-sets of algebraic varieties and their Cartesian products) and functions r, are given in [2], [3], [4], [6], [7], [8], [9], [10], [12], [16], [20], together with a broad scope of applications.

Here, we are mostly interested in studying $N_r(\mathcal{I}, \mathcal{G})$ for an interval $\mathcal{I}$ of several consecutive integers and a multiplicative subgroup $\mathcal{G}$ of $\mathbb{F}_p^*$.

We note that in the case when $\mathcal{G}$ is a group of quadratic residues, this question is essentially the classical question about the distribution of quadratic residues and non-residues in consecutive values of rational functions and polynomials. However here concentrate on the case of subgroups $\mathcal{G}$ of relatively small order.

Mathematics Subject Classification (2010): Primary 11D79; Secondary 11T06.
Keywords: Polynomial congruences, finite fields.

We also use $T_r(H)$ to denote the smallest possible T such that there is an interval $\mathcal{I} = \{u+1,\ldots,u+H\}$ of H consecutive integers and a multiplicative subgroup $\mathcal{G}$ of $\mathbb{F}_p^*$ of order T for which

$$r(\mathcal{I}) \subseteq \mathcal{G} \tag{1.1}$$

and thus $N_r(\mathcal{I},\mathcal{G}) = \#r(\mathcal{I})$.

It is shown in [15] that if $r(X) = f(X)/g(X) \in \mathbb{F}_p(X)$ with two relatively primes polynomials $f,g \in \mathbb{F}_p[X]$ then for any interval $\mathcal{I} = \{u+1,\ldots,u+H\}$ of H consecutive integers and a subgroup $\mathcal{G}$ of $\mathbb{F}_p^*$ of order T, the quantity $N_r(\mathcal{I},\mathcal{G})$ is "small".

To formulate the result precisely we recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the inequality $|U| \le c\,V$ with some constant $c > 0$. Throughout the paper, the implied constants in these symbols may occasionally depend, where obvious, on degrees (such as d) and the number of variables of various polynomials, as well as on the integer parameter $\nu \ge 1$, but are absolute otherwise. We also use $o(1)$ to denote a quantity that tends to zero when one of the indicated parameters (usually H or p) tends to infinity while d, ν and other similar parameters are fixed.

Then, by the bound of [15] in the special case where $r = f \in \mathbb{F}_p[X]$ is a polynomial of degree $d \ge 2$, we have

$$N_f(\mathcal{I},\mathcal{G}) \ll (1 + H^{(d+1)/4} p^{-1/4d})\, H^{1/2d}\, T^{1/2}. \tag{1.2}$$

Note that we have $\#r(\mathcal{I}) \gg \mathcal{I}$. In particular, if (1.1) holds then the bound (1.2) implies that

$$H \ll (1 + H^{(d+1)/4} p^{-1/4d})\, H^{1/2d}\, T^{1/2},$$

from which we derive

$$T_f(H) \gg \min\{H^{2-1/d}, H^{-(d-1)(d-2)/2d} p^{1/2d}\}. \tag{1.3}$$

For a linear fractional function

$$r(X) = a\,\frac{X+s}{X+t}$$

with $s \not\equiv t \pmod p$, the bound of Lemma 35 in [3] implies that there is an absolute constant $c > 0$ such that if for some positive integer ν we have

$$H \le p^{c\nu^{-4}}, \tag{1.4}$$

then for the set

$$r(\mathcal{I}) = \left\{a\,\frac{x+s}{x+t} \;:\; x \in \mathcal{I}\right\} \subseteq \mathbb{F}_p$$

we have

$$\#\{a_1 \ldots a_\nu \;:\; a_1,\ldots,a_\nu \in r(\mathcal{I})\} \ge H^{\nu+o(1)}.$$

Thus, if $r(\mathcal{I}) \in \mathcal{G}$ then $\#\mathcal{G} \ge H^{\nu+o(1)}$. Therefore,

$$T_r(H) \ge H^{\nu+o(1)} \quad \text{as } H \to \infty. \tag{1.5}$$

Using a result of D'Andrea, Krick and Sombra, Theorem 2 in [14], instead of Lemma 23 in [3], one can improve Lemmas 35 and 38 in [3] and relax (1.4) as

$$H \le p^{c\nu^{-3}}.$$

For larger values of H, by bound (29) in [3], we have

$$N_r(\mathcal{I}, \mathcal{G}) \le \left(1 + H^{3/4} p^{-1/4}\right) T^{1/2} p^{o(1)},$$

as $p \to \infty$. Thus

$$T_r(H) \ge \min\left\{H^2, H^{1/2} p^{1/2}\right\} p^{o(1)}.$$

1.2. Our results

Here we use the methods of [3], based on an application effective Hilbert's Nullstellensatz, see [14], [18], to obtain a variant of the bound of (1.5) for polynomials and thus to improve (1.3) for small values of H.

Furthermore, combining some ideas from [15] with a bound on the number on integer points on quadrics (which replaces the bound of Bombieri and Pila [1] in the argument of [15]), we improve (1.2) for quadratic polynomials. In fact, this argument stems from that of Cilleruelo and Garaev [11].

Acknowledgements. The author is very grateful to Domingo Gómez–Pérez for discussions and very helpful comments, and to Harald Helfgott for pointing out to [19]. Thanks also go to the referee for a very careful reading of the manuscript and several useful comments.

This work was finished during a very enjoyable research stay of the author at the Max Planck Institute for Mathematics, Bonn.

2. Preparations

2.1. Effective Hilbert's Nullstellensatz

We recall that the logarithmic height of a nonzero polynomial $P \in \mathbb{Z}[Z_1, \dots, Z_n]$ is defined as the logarithm of the largest (by absolute value) coefficient of P.

Our argument uses the following quantitative version version of Hilbert's Nullstellensatz due to D'Andrea, Krick and Sombra [14], which in turn improves previous results of Krick, Pardo and Sombra (Theorem 1 in [18]). In fact we only need a very special form of Corollary 4.38 in [14].

Lemma 1. *Let $P_1, \dots, P_N \in \mathbb{Z}[Z_1, \dots, Z_n]$ be $N \ge 1$ polynomials in n variables without a common zero in $\mathbb{C}^n$ of degree at most $D \ge 3$ and of logarithmic height at most H. Then there is a positive integer b with*

$$\log b \le (n+1)D^n H + C(D, N, n),$$

where $C(D, N, n)$ is some constant, depending only on D, N and n, and polynomials $R_1, \dots, R_N \in \mathbb{Z}[Z_1, \dots, Z_n]$ such that

$$P_1 R_1 + \cdots + P_N R_N = b.$$

We note that Corollary 4.38 in [14] gives explicit estimates on all other parameters as well (that is, on the heights and degrees of the polynomials $R_1, \ldots, R_N$), see also [14].

2.2. Some facts on algebraic integers

We also need a bound of Chang, Proposition 2.5 in [5], on the divisor function in algebraic number fields. As usual, for algebraic number field $\mathbb{K}$ we use $\mathbb{Z}_\mathbb{K}$ to denote the ring of integers. As usual, we define the logarithmic height of an algebraic number $\alpha \neq 0$ as the logarithmic height of its minimal polynomial.

Lemma 2. *Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$ of degree $k = [\mathbb{K} : \mathbb{Q}]$. For any nonzero algebraic integer $\gamma \in \mathbb{Z}_\mathbb{K}$ of logarithmic height at most $H \geq 2$, the number of pairs (γ_1, γ_2) of algebraic integers $\gamma_1, \gamma_2 \in \mathbb{Z}_\mathbb{K}$ of logarithmic height at most H with $\gamma = \gamma_1\gamma_2$ is at most $\exp(O(H/\log H))$, where the implied constant depends on k.*

Finally, as in [3], we use the following result, this is exactly the statement that is established in the proof of Lemma 2.14 in [5] (see Equation (2.15) in [5]).

Lemma 3. *Let $P_1, \ldots, P_N, Q \in \mathbb{Z}[Z_1, \ldots, Z_n]$ be $N + 1 \geq 2$ polynomials in n variables of degree at most D and of logarithmic height at most $H \geq 1$. If the zero-set*

$$P_1(Z_1, \ldots, Z_n) = \cdots = P_N(Z_1, \ldots, Z_n) = 0 \quad \text{and} \quad Q(Z_1, \ldots, Z_n) \neq 0$$

is not empty, then it has a point $(\beta_1, \ldots, \beta_n)$ in an extension $\mathbb{K}$ of $\mathbb{Q}$ of degree $[\mathbb{K} : \mathbb{Q}] \leq C_1(D, n)$ such that their minimal polynomials are of logarithmic height at most $C_2(D, N, n)H$, where $C_1(D, n)$ depends only on D and n, and $C_2(D, N, n)$ depends only on D, N and n.

2.3. Integral points on quadrics

The following bound on the number of integral points on quadrics is given in Lemma 3 of [17]. We say that a quadratic polynomial $G(X, Y) \in \mathbb{Z}[X, Y]$ is *affinely equivalent to a parabola*, if there is a linear transformation of the variables which reduces G to the polynomial $X^2 - Y$, that is, if

$$G(a_{11}X + a_{12}Y + b_1, a_{21}X + a_{22}Y + b_2) = X^2 - Y$$

for some coefficients $a_{ij}, b_j \in \mathbb{C}$, $i, j = 1, 2$.

Lemma 4. *Let*

$$G(X, Y) = AX^2 + BXY + CY^2 + DX + EY + F \in \mathbb{Z}[X, Y]$$

be an irreducible quadratic polynomial with coefficients of size at most H. Assume that $G(X, Y)$ is not affinely equivalent to a parabola and has a nonzero determinant

$$\Delta = B^2 - 4AC \neq 0.$$

Then, as $H \to \infty$, the equation $G(x, y) = 0$ has at most $H^{o(1)}$ integral solutions $(x, y) \in [0, H] \times [0, H]$.

2.4. Small values of linear functions

We need a result about small values of residues modulo p of several linear functions. Such a result has been derived in [13], Lemma 3.2, from the Dirichlet pigeonhole principle. Here we use a slightly more precise and explicit form of this result which is derived in [15], Lemma 6, from the *Minkowski theorem*.

For an integer a we use $\langle a \rangle_p$ to denote the smallest by absolute value residue of a modulo p, that is

$$\langle a \rangle_p = \min_{k \in \mathbb{Z}} |a - kp|.$$

Lemma 5. *For any real numbers $V_1, \ldots, V_m$ with*

$$p > V_1, \ldots, V_m \geq 1 \quad \textit{and} \quad V_1 \ldots V_m > p^{m-1}$$

and integers $b_1, \ldots, b_m$, there exists an integer v with $\gcd(v, p) = 1$ such that

$$\langle b_i v \rangle_p \leq V_i, \quad i = 1, \ldots, m.$$

3. Main results

3.1. Arbitrary polynomials

For a set $\mathcal{A}$ in an arbitrary semi-group, we use $\mathcal{A}^{(\nu)}$ to denote the ν-fold product set, that is,

$$\mathcal{A}^{(\nu)} = \{a_1 \ldots a_\nu \ : \ a_1, \ldots, a_\nu \in \mathcal{A}\}.$$

First we note that in order to get a lower bound on $T_f(\mathcal{I}, \mathcal{G})$ it is enough to give a lower bound on the cardinality of $f(\mathcal{I})^{(\nu)}$ for any integer $\nu \geq 1$.

Theorem 6. *For every positive integers d and ν there is a constant $c(d, \nu) > 0$, depending only on d and ν, such that for any polynomial $f \in \mathbb{F}_p[X]$ of degree d and interval $\mathcal{I}$ of*

$$H \leq c(d, \nu)\, p^{1/(d+1)\nu_0^{d+1}}$$

consecutive integers, where $\nu_0 = \max\{3, \nu\}$, we have

$$\# f(\mathcal{I})^{(\nu)} \geq H^{\nu + o(1)} \quad \textit{as } H \to \infty.$$

Proof. Clearly, we can assume that

$$f(X) = X^d + \sum_{k=0}^{d-1} a_{d-k}\, X^k$$

is monic.

It is also clear that we can assume that $\mathcal{I} = \{1, \ldots, H\}$.

We consider the collection $\mathcal{P} \subseteq \mathbb{Z}[Z_1, \ldots, Z_d]$ of polynomials

$$P_{\mathbf{x},\mathbf{y}}(Z_1, \ldots, Z_d) = \prod_{i=1}^{\nu} \Big(x_i^d + \sum_{k=0}^{d-1} Z_{d-k}\, x_i^k \Big) - \prod_{i=1}^{\nu} \Big(y_i^d + \sum_{k=0}^{d-1} Z_{d-k}\, y_i^k \Big),$$

where $\mathbf{x} = (x_1, \ldots, x_\nu)$ and $\mathbf{y} = (y_1, \ldots, y_\nu)$ are integral vectors with entries in $[1, H]$, and such that

$$P_{\mathbf{x},\mathbf{y}}(a_1, \ldots, a_d) \equiv 0 \pmod p.$$

Note that

$$P_{\mathbf{x},\mathbf{y}}(a_1, \ldots, a_d) \equiv \prod_{i=1}^{\nu} f(x_i) - \prod_{i=1}^{\nu} f(y_i) \pmod p.$$

Clearly if $P_{\mathbf{x},\mathbf{y}}$ is identical to zero then, by the uniqueness of polynomial factorisation in the ring $\mathbb{Z}[Z_1, \ldots, Z_d]$, the components of $\mathbf{y}$ are permutations of those of $\mathbf{x}$. So, if $\mathcal{P}$ does not contain any nonzero polynomial, we obviously obtain

$$\# f(\mathcal{I})^{(\nu)} \geq \frac{1}{\nu!} \left(\# f(\mathcal{I})\right)^{\nu} \gg H^{\nu}.$$

Hence, we now assume that $\mathcal{P}$ contains non-zero polynomials.

Note that every $P \in \mathcal{P}$ is of degree at most ν and of logarithmic height at most $\nu \log H + O(1)$.

We take a family $\mathcal{P}_0$ containing the largest possible number

$$N \leq (\nu + 1)^d$$

of linearly independent polynomials $P_1, \ldots, P_N \in \mathcal{P}$, and consider the variety

$$\mathcal{V} : \ \{(Z_1, \ldots, Z_d) \in \mathbb{C}^d \ : \ P_1(Z_1, \ldots, Z_d) = \cdots = P_N(Z_1, \ldots, Z_d) = 0\}.$$

Assume that $\mathcal{V} = \emptyset$. Then by Lemma 1 we see that there are polynomials $R_1, \ldots, R_N \in \mathbb{Z}[Z_1, \ldots, Z_d]$ and a positive integer b with

$$\log b \leq (d+1)\, \nu_0^{d+1} \log H + O(1) \tag{3.1}$$

and such that

$$P_1 R_1 + \cdots + P_N R_N = b \tag{3.2}$$

Substituting

$$(Z_1, \ldots, Z_d) = (a_1, \ldots, a_k)$$

in (3.2), we see that the left hand side of (3.2) is divisible by p. Since $b \geq 1$ we obtain $p \leq b$. Taking an appropriately small value of $c(d, \nu)$ in the condition of the theorem, we see from (3.1) that this is impossible.

Therefore the variety $\mathcal{V}$ is nonempty. Applying Lemma 3 (with the polynomial $Q = 1$) we see that it has a point $(\beta_1, \ldots, \beta_d)$ with components of logarithmic height $O(\log H)$ in an extension $\mathbb{K}$ of $\mathbb{Q}$ of degree $[\mathbb{K} : \mathbb{Q}] = O(1)$.

Consider the maps $\Phi : \ \mathcal{I}^{\nu} \to \mathbb{F}_p$ given by

$$\Phi : \ \mathbf{x} = (x_1, \ldots, x_\nu) \mapsto \prod_{j=1}^{\nu} f(x_j)$$

and $\Psi : \mathcal{I}^\nu \to \mathbb{K}$ given by

$$\Psi : \ \mathbf{x} = (x_1, \ldots, x_\nu) \mapsto \prod_{j=1}^{\nu} \Bigl(x_i^d + \sum_{k=0}^{d-1} \beta_{d-k}\, x_i^k \Bigr).$$

Clearly, if $\Phi(\mathbf{x}) = \Phi(\mathbf{y})$ then

$$P_{\mathbf{x},\mathbf{y}}(a_1, \ldots, a_k) \equiv 0 \pmod p,$$

thus $P_{\mathbf{x},\mathbf{y}}(Z_1, \ldots, Z_d) \in \mathcal{P}$. Recalling the definitions of the family $\mathcal{P}_0$ and of $(\beta_1, \ldots, \beta_d)$, we see that $P_{\mathbf{x},\mathbf{y}}(\beta_1, \ldots, \beta_d) = 0$. Hence $\Psi(\mathbf{x}) = \Psi(\mathbf{y})$. We now conclude that for every $\mathbf{x}$ the multiplicity of the value $\Phi(\mathbf{x})$ in the image set $\mathrm{Im}\Phi$ of the map Φ is at most the multiplicity of the value $\Phi(\mathbf{x})$ in the image set $\mathrm{Im}\Psi$ of the map Ψ. Thus,

$$\# f(\mathcal{I})^{(\nu)} = \#\mathrm{Im}\Phi \geq \#\mathrm{Im}\Psi = \#\mathcal{C}^{(\nu)},$$

where

$$\mathcal{C} = \Bigl\{ x^d + \sum_{k=0}^{d-1} \beta_{d-k}\, x^d \ : \ 1 \leq x \leq H \Bigr\} \subseteq \mathbb{K}.$$

Using Lemma 2 inductively, we see that for any $\gamma \in \mathbb{C}$ there are at most $H^{o(1)}$ representations $\gamma = \gamma_1 \ldots \gamma_\nu$ with $\gamma_1 \ldots \gamma_\nu \in \mathbb{C}$. Thus, we now conclude that $\#\mathcal{C}^{(\nu)} \geq H^{\nu + o(1)}$, as $H \to \infty$, and derive the result. □

3.2. Quadratic polynomials

For quadratic square-free polynomials f, using Lemma 4 instead of the bound of Bombieri and Pila [1] in the argument of [15] we immediately obtain the following result.

Theorem 7. *Let $f(X) \in \mathbb{F}_p[X]$ be a square-free quadratic polynomial. For any interval $\mathcal{I}$ of H consecutive integers and a subgroup $\mathcal{G}$ of $\mathbb{F}_p^*$ of order T, we have*

$$N_f(\mathcal{I}, \mathcal{G}) \leq \bigl(1 + H^{3/4} p^{-1/8}\bigr) T^{1/2} p^{o(1)}, \quad \text{as } H \to \infty.$$

Proof. We follow closely the argument of [15]. We can assume that

$$H \leq c\, p^{1/2} \tag{3.3}$$

for some constant $c > 0$ as otherwise the desired bound is weaker than the trivial estimate

$$N_f(\mathcal{I}, \mathcal{G}) \leq \min\{H, T\} \leq H^{1/2} T^{1/2}.$$

Making the transformation $X \mapsto X + u$ we reduce the problem to the case where $\mathcal{I} = \{1, \ldots, H\}$.

Let $1 \leq x_1 < \ldots < x_k \leq H$ be all $k = N_f(\mathcal{I}, \mathcal{G})$ values of $x \in \mathcal{I}$ with $f(x) \in \mathcal{G}$.

Let $f(X) = a_0 X^2 + a_1 X + a_2$, $a_0 \neq 0$.

Let us consider the quadratic polynomial

$$
\begin{aligned}
Q_\lambda(X,Y) &= f(X) - \lambda f(Y) \\
&= a_0X^2 - \lambda a_0 Y^2 + a_1 X - \lambda a_1 Y + a_2(1-\lambda).
\end{aligned} \tag{3.4}
$$

One easily verifies that $Q_\lambda(X,Y)$ is irreducible for $\lambda \ne 1$.

We see that there are only at most $2k$ pairs (x_i, x_j), $1 \le i,j \le k$, for which $f(x_i)/f(x_j) = 1$. Indeed, if x_j is fixed, then $f(x_i)$ is also fixed, and thus x_i can take at most 2 values.

We now assume that $k \ge 4$ as otherwise there is nothing to prove. Therefore, there is $\lambda \in \mathcal{G} \setminus \{1\}$ such that

$$
f(x) \equiv \lambda f(y) \pmod p \tag{3.5}
$$

for at least

$$
\frac{k^2-2k}{T} \ge \frac{k^2}{2T} \tag{3.6}
$$

pairs (x,y) with $x, y \in \{1, \ldots, H\}$.

We now apply Lemma 5 with $m = 4$,

$$
b_1 = a_0 \quad b_2 = -\lambda a_0, \quad b_3 = a_1, \quad b_4 = -\lambda a_1
$$

and

$$
V_1 = V_2 = 2p^{3/4}H^{-1/2}, \quad V_3 = V_4 = 2p^{3/4}H^{1/2}.
$$

Thus

$$
V_1V_2V_3V_4 = 16p^3 > p^3.
$$

We also assume that the constant c in (3.3) is small enough so the condition

$$
V_i \le 2\,p^{3/4}H^{1/2} < p, \quad i = 1, \ldots, 4,
$$

is satisfied. Note that

$$
V_1H^2 = V_2H^2 = V_3H = V_4H = 2\,p^{3/4}H^{3/2}. \tag{3.7}
$$

Let v be the corresponding integer.

We now consider the quadratic polynomial $F(X,Y) \in \mathbb{Z}[X,Y]$ with coefficients in the interval $[-p/2, p/2]$, obtained by reducing the coefficients of the polynomial $vQ_\lambda(X,Y)$ modulo p. Clearly (3.5) implies

$$
F(x,y) \equiv 0 \pmod p. \tag{3.8}
$$

Furthermore, since $x, y \in \{1, \ldots, H\}$, we see from (3.7) and the trivial estimate $|F(0,0)| \le p/2$ that

$$
|F(x,y)| \le 8\,p^{3/4}H^{3/2} + p/2.
$$

In turn, together with (3.8) this implies that

$$
F(x,y) - zp = 0 \tag{3.9}
$$

for some integer $z \ll 1 + H^{3/2}p^{-1/4}$.

Clearly, for any integer z the reducibility of $F(X,Y) - pz$ over $\mathbb{C}$ implies the reducibility of $F(X,Y)$ and then in turn of $Q_\lambda(X,Y)$ over $\mathbb{F}_p$, which is impossible as $\lambda \neq 1$.

It is also easy to see that completing the polynomials $f(X)$ and $\lambda f(Y)$ full squares, we see that $Q_\lambda(X,Y)$ is affinely equivalent to a polynomial of the shape $X^2 - \lambda Y^2 + \mu$. So it is not affinely equivalent to a parabola over $\mathbb{F}_p$ and thus the same holds for $F(X,Y)$ over $\mathbb{C}$. The non-vanishing of the determinant is straightforward as well. Hence, the condition of Lemma 4 are satisfied for $F(X,Y)$ and we see that, as $p \to \infty$, for every z the equation (3.9) has $p^{o(1)}$ solutions. Thus the congruence (3.5) has at most $\left(1 + H^{3/2}p^{-1/4}\right) p^{o(1)}$ solutions. Together with (3.6), this yields the inequality

$$\frac{k^2}{2T} \le \left(1 + H^{3/2}p^{-1/4}\right)p^{o(1)},$$

which concludes the proof. □

4. Comments

We remark that Mendes da Costa [19] has recently given an improvement of the bound of Bombieri and Pila [1] in the case of a class of elliptic curves. It is quite possible that the results and ideas of [19] can be used to improve (1.2) for some cubic polynomials. Regardless of this application, extending the bound of [19] to more general cubic curves and also obtaining a more explicit bounds are both very interesting questions.

References

[1] Bombieri, E. and Pila, J.: The number of integral points on arcs and ovals. *Duke Math. J.* **59** (1989), no. 2, 337–357.

[2] Bourgain, J.: On the distribution of the residues of small multiplicative subgroups of $\mathbb{F}_p$. *Israel J. Math.* **172** (2009), 61–74.

[3] Bourgain, J., Garaev, M. Z., Konyagin, S. V. and Shparlinski, I. E.: On the hidden shifted power problem. *SIAM J. Comput.* **41** (2012), no. 6, 1524–1557.

[4] Bourgain, J., Garaev, M. Z., Konyagin, S. V. and Shparlinski, I. E.: Multiplicative congruences with variables from short intervals. *J. Anal. Math.* **124** (2014), 117–147.

[5] Chang, M.-C.: Factorization in generalized arithmetic progressions and applications to the Erdős–Szemerédi sum-product problems. *Geom. Funct. Anal.* **13** (2003), no. 4, 720–736.

[6] Chang, M.-C.: Order of Gauss periods in large characteristic. *Taiwanese J. Math.* **17** (2013), no. 2, 621–628.

[7] Chang, M.-C.: Elements of large order in prime finite fields. *Bull. Aust. Math. Soc.* **88** (2013), no. 1, 169–176.

[8] Chang, M.-C.: Sparsity of the intersection of polynomial images of an interval. *Acta Arith.* **165** (2014), no. 3, 243–249.

[9] Chang, M.-C., Cilleruelo, J., Garaev, M. Z., Hernández, J., Shparlinski, I. E. and Zumalacárregui, A.: Points on curves in small boxes and applications. *Michigan Math. J.* **63** (2014), 503–534.

[10] Chang, M.-C., Kerr, B., Shparlinski, I. E. and Zannier, U.: Elements of large order on varieties over prime finite fields. *J. Théor. Nombres Bordeaux* **26** (2014), no. 3, 579–594.

[11] Cilleruelo, J. and Garaev, M. Z.: Concentration of points on two and three dimensional modular hyperbolas and applications. *Geom. Funct. Anal.* **21** (2011), no. 4, 892–904.

[12] Cilleruelo, J., Garaev, M. Z., Ostafe, A. and Shparlinski, I. E.: On the concentration of points of polynomial maps and applications. *Math. Z.* **272** (2012), no. 3-4, 825–837.

[13] Cilleruelo, J., Shparlinski, I. E. and Zumalacárregui, A.: Isomorphism classes of elliptic curves over a finite field in some thin families. *Math. Res. Lett.* **19** (2012), no. 2, 335–343.

[14] D'Andrea, C., Krick, T. and Sombra, M.: Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze. *Ann. Sci. Éc. Norm. Supér. (4)* **46** (2013), no. 4, 549–627.

[15] Gómez–Pérez, D. and Shparlinski, I. E.: Subgroups generated by rational functions in finite fields. *Monatsh. Math.* **176** (2015), no. 2, 241–253.

[16] Kerr, B.: Solutions to polynomial congruences in well shaped sets. *Bull. Aust. Math. Soc.* **88** (2013), no. 3, 435–447.

[17] Konyagin, S. V. and Shparlinski, I. E.: On convex hull of points on modular hyperbolas. *Mosc. J. Comb. Number Theory* **1** (2011), no. 1, 43–51.

[18] Krick, T., Pardo, L. M. and Sombra, M.: Sharp estimates for the arithmetic Nullstellensatz. *Duke Math. J.* **109** (2001), no. 3, 521–598.

[19] Mendes da Costa, D.: Integral points on elliptic curves and the Bombieri–Pila bounds. Preprint, ArXiv: `1301.4116`, 2013.

[20] Shparlinski, I. E.: Groups generated by iterations of polynomials over finite fields. *Proc. Edinburgh Math. Soc. (2)* **59** (2016), no. 1, 235–245.

Received August 18, 2014; revised January 27, 2015.

Igor E. Shparlinski: Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia.
E-mail: igor.shparlinski@unsw.edu.au

During the preparation of this paper the author was supported by the Australian Research Council Grant DP130100237.