CHARACTER SUMS AND DETERMINISTIC POLYNOMIAL ROOT FINDING IN FINITE FIELDS

JEAN BOURGAIN, SERGEI V. KONYAGIN, AND IGOR E. SHPARLINSKI

Abstract. We obtain a new bound of certain double multiplicative character sums. We use this bound together with some other previously obtained results to obtain new algorithms for finding roots of polynomials modulo a prime $p$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of $q$ elements of characteristic $p$. The classical algorithm of Berlekamp [1] reduces the problem of factoring polynomials of degree $n$ over $\mathbb{F}_q$ to the problem of factoring squarefree polynomials of degree $n$ over $\mathbb{F}_p$ that fully split in $\mathbb{F}_p$, see also [7, Chapter 14]. Shoup [14, Theorem 3.1] has given a deterministic algorithm that fully factors any polynomial of degree $n$ over $\mathbb{F}_p$ in $O(n^{2+o(1)}p^{1/2}(\log p)^2)$ arithmetic operations over $\mathbb{F}_p$; in particular it runs in time $n^2p^{1/2+o(1)}$. Furthermore, Shoup [14, Remark 3.5] has also announced an algorithm of complexity $O(n^{3/2+o(1)}p^{1/2}(\log p)^2)$ for factoring arbitrary univariate polynomials of degree $n$ over $\mathbb{F}_p$.

We remark, that although the efficiency of deterministic polynomial factorisation algorithms falls far behind the fastest probabilistic algorithms, see, for example, [8, 10, 11], the question is of great theoretic interest.

Here we address a special case of the polynomial factorisation problem when the polynomial $f$ fully splits over $\mathbb{F}_p$ (as we have noticed there is a polynomial time reduction between factoring general polynomials and polynomials that split over $\mathbb{F}_p$). That is, here we deal with the root finding problem. We also note that in order to find a root (or all roots) of a polynomial $f \in \mathbb{F}_p[X]$, it is enough to do the same for the polynomial $\gcd(f(X), X^{p-1} - 1)$ which is squarefree fully splits over $\mathbb{F}_p$.

We consider two variants of the root finding problem:

2010 Mathematics Subject Classification. 11L40, 11T06, 11Y16, 68Q25.

Key words and phrases. finite field, root finding, character sums, multiplicative energy.
Given a polynomial \( f \in \mathbb{F}_p[X] \), find all roots of \( f \) in \( \mathbb{F}_p \).

Given a polynomial \( f \in \mathbb{F}_p[X] \), find at least one root of \( f \) in \( \mathbb{F}_p \).

For the case of finding all roots we show that essentially the initial approach of Shoup [14] together with the fast factor refinement procedure of Bernstein [2] lead to an algorithm of complexity \( np^{1/2+o(1)} \). In fact this result is already implicit in [14] but here we record it again with a very short proof. We use this as a benchmark for our algorithm for the second problem.

In the case of finding just one root, we obtain a faster algorithm, which is based on bounds of double multiplicative character sums

\[
T_\chi(I,S) = \left| \sum_{u \in I} \sum_{s \in S} \chi(u + s) \right|^2,
\]

where \( I = \{1, \ldots, h\} \) is an interval of \( h \) consecutive integers, \( S \subseteq \mathbb{F}_p \) is an arbitrary set and \( \chi \) is a multiplicative character of \( \mathbb{F}_p^* \). More precisely, here we use a new bound on \( T_\chi(I,S) \) to improve the bound \( np^{1/2+o(1)} \) in the case when \( n \) is large enough, namely if it grows as a power of \( p \). We believe that our new bound of the sums \( T_\chi(I,S) \) as well as several auxiliary results (based on some methods from additive combinatorics) are of independent interest as well.

Throughout the paper, any implied constants in symbols \( O \) and \( \ll \) may depend on two real positive parameters \( \varepsilon \) and \( \delta \) and are absolute otherwise. We recall that the notations \( U = O(V) \) and \( U \ll V \) are all equivalent to the statement that \( |U| \leq cV \) holds with some constant \( c > 0 \). We also use \( U \asymp V \) to denote that \( U \ll V \ll U \).

2. Bounds on the Number Solutions to Some Equations and Character Sums

2.1. Uniform distribution and exponential sums. The following result is well-known and can be found, for example, in [12, Chapter 1, Theorem 1] (which is a more precise form of the celebrated Erdős–Turán inequality).

**Lemma 1.** Let \( \xi_1, \ldots, \xi_M \) be a sequence of \( M \) points of the unit interval \([0, 1]\). Then for any integer \( K \geq 1 \), and an interval \([0, \rho] \subseteq [0, 1] \), we have

\[
\# \{ m = 1, \ldots, M : \gamma_m \in [0, \rho] \} - \rho M \ll \frac{M}{K} + \sum_{k=1}^{K} \left( \frac{1}{K} + \min\{\rho, 1/k\} \right) \left| \sum_{m=1}^{M} \exp(2\pi ik\xi_m) \right|.
\]
2.2. Preliminary bounds. Throughout this section we fix some set \( S \subseteq \mathbb{F}_p \) of and interval \( I = \{1, \ldots, h\} \) of \( h \leq p^{1/2} \) consecutive integers.

We say that a set \( D \subseteq \mathbb{F}_p \) is \( \Delta \)-spaced if no elements \( d_1, d_2 \in D \) and positive integer \( k \leq \Delta \) satisfy the equality \( d_1 + k = d_2 \).

Here we always assume that the set \( S \) is \( h \)-spaced.

Finally, we also fix some \( L \) and denote by \( \mathcal{L} \) the set of primes of the interval \([L, 2L]\).

We denote

\[
\mathcal{W} = \left\{ (u_1, u_2, \ell_1, \ell_2, s_1, s_2) \in I^2 \times \mathcal{L}^2 \times S^2 : \frac{u_1 + s_1}{\ell_1} \equiv \frac{u_2 + s_2}{\ell_2} \pmod{p} \right\}.
\]

The following result is based on some ideas of Shao [13].

**Lemma 2.** If \( L < h \) and \( 2hL < p \) then

\[
\#\mathcal{W} \ll (\#ShL)^2 p^{-1} + \#ShLp^{o(1)}.
\]

**Proof.** Clearly

(1) \[
\#\mathcal{W} = \#\mathcal{W}^* + O(\#ShL),
\]

where

\[
\mathcal{W}^* = \{(u_1, u_2, \ell_1, \ell_2, s_1, s_2) \in \mathcal{W} : \ell_1 \neq \ell_2\}.
\]

Denote

\[
\mathcal{S} = S + I = \{u + s : (u, v) \in I \times S\}, \quad I = \{-h, \ldots, h\}.
\]

Clearly

\[
\mathcal{W}^* \ll h^{-2} \left\{ (u_1, u_2, \ell_1, \ell_2, s_1, s_2) \in I^2 \times \mathcal{L}^2 \times \mathcal{S}^2 : \ell_1 \neq \ell_2,
\frac{u_1 + s_1}{\ell_1} \equiv \frac{u_2 + s_2}{\ell_2} \pmod{p} \right\}.
\]

Note that for fixed \( \ell_1, \ell_2 \in \mathcal{L}, \ell_1 \neq \ell_2 \) and integer \( x, |x| \leq 2hL \) the congruence

\[u_1\ell_2 - u_2\ell_1 \equiv x \pmod{p}\]

is equivalent to the equation \( u_1\ell_2 - u_2\ell_1 = x \) (since \( 2hL < p \)) and thus has \( O(h/L) \) solutions. We rewrite

\[
\frac{u_1 + s_1}{\ell_1} \equiv \frac{u_2 + s_2}{\ell_2} \pmod{p}
\]

as

\[
s_1\ell_2 - s_2\ell_1 \equiv x \equiv u_1\ell_2 - u_2\ell_1 \pmod{p}.
\]
One can consider that $x \geq 0$. We now bound the cardinality of
\[ U = \left\{ (x, \ell_1, \ell_2, s_1, s_2) \in [0, 2hL] \times \mathbb{L}^2 \times \mathbb{S}^2 : s_1 \ell_2 - s_2 \ell_1 \equiv x \pmod{p} \right\}. \]

The above argument shows that
\[ W^* \leq h^{-2} (h/L) \#U = h^{-1} L^{-1} \#U. \]

We now apply Lemma 1 to the sequence of fractional parts
\[ \left\{ \frac{s_1 \ell_2 - s_2 \ell_1}{p} \right\}, \quad (\ell_1, \ell_2, s_1, s_2) \in \mathbb{L}^2 \times \mathbb{S}^2, \]
with $M = (\#L)^2 (\#S)^2$, $\rho = 2hLp^{-1}$ and $K = \lceil \rho^{-1} \rceil$. This yields the bound
\[ \#U \ll (\#L)^2 (\#S)^2 \rho \]
\[ + \rho \sum_{k=1}^{K} \left| \left| \sum_{(\ell_1, \ell_2, s_1, s_2) \in \mathbb{L}^2 \times \mathbb{S}^2} \exp \left( 2\pi i k (s_1 \ell_2 - s_2 \ell_1) \right) \right| \right|^2 = (\#L)^2 (\#S)^2 \rho + \rho \sum_{k=1}^{K} \left| \left| \sum_{(\ell, s) \in \mathbb{L} \times \mathbb{S}} \exp \left( 2\pi i k s \ell \right) \right| \right|^2. \]

Using the Cauchy inequality, denoting $r = k\ell$ and then using the classical bound on the divisor function, we derive
\[ \#U \ll (\#L)^2 (\#S)^2 \rho + \rho \sum_{k=1}^{K} \left| \left| \sum_{\ell \in \mathbb{L}} \sum_{s \in \mathbb{S}} \exp \left( 2\pi i k s \ell \right) \right| \right|^2 \]
\[ \ll (\#L)^2 (\#S)^2 \rho + \rho \sum_{r=0}^{p-1} \left| \sum_{s \in \mathbb{S}} \exp \left( 2\pi i r s \right) \right|^2, \]
since $r \in [1, 2KL] \subseteq [0, p-1]$ provided that $p$ is sufficiently large. Thus, using the Parseval inequality and recalling the values of our parameters, we obtain
\[ \#U \ll hL^3 (\#S)^2 p^{-1} + hL^2 \#S \rho^{\alpha(1)} \]

Using the trivial bound $\#S \ll \#S h$, we obtain
\[ \#U \ll h^3 L^3 (\#S)^2 p^{-1} + h^2 L^2 \#S \rho^{\alpha(1)} \]

Thus, recalling (1) and (2) we conclude the proof. \qed
Denote 
\[ W(x, y) = \# \left\{ (u, \ell, s, t) \in I \times L \times S^2 : \frac{u + s}{\ell} = x, \frac{u + s_2}{\ell} = y \right\}. \] (3)

**Lemma 3.** We have 
\[ \sum_{x, y \in \mathbb{F}_p} W(x, y)^2 \ll (\#S)^3(hL)^2p^{-1} + (\#S)^2hLp^\omega(1). \]

**Proof.** Clearly 
\[ \sum_{x, y \in \mathbb{F}_p} W(x, y)^2 = \# \left\{ (u_1, u_2, \ell_1, s_1, t_1, s_2, t_2) \in I^2 \times L^2 \times S^4 : \frac{u_1 + s_1}{\ell_1} = \frac{u_2 + s_2}{\ell_2}, \frac{u_1 + t_1}{\ell_1} = \frac{u_2 + t_2}{\ell_2} \right\}. \]

For each \((u_1, u_2, \ell_1, s_1, s_2) \in W\) and \(t_1 \in S\) there is only one possible values for \(t_2\). The result now follows from Lemma 2. \(\square\)

2.3. **Character sum estimates.** The following estimate improves and generalises [4, Lemma 14] and [5, Theorem 8].

**Lemma 4.** For any positive \(\delta > 0\) there is some \(\eta > 0\) such that for an interval \(I = \{1, \ldots, h\}\) of \(h \leq p^{1/2}\) consecutive integers and any \(h\)-spaced set \(S \subseteq \mathbb{F}_p\) with 
\[ \#S h > p^{1/2+\delta}, \]
for any nontrivial multiplicative character \(\chi\) of \(\mathbb{F}_p^*\) we have 
\[ T_\chi(I, S) \ll (\#S)^2hp^{-\eta}. \]

**Proof.** We choose a sufficiently small \(\varepsilon\) and define 
\[ L = \left\lfloor hp^{-2\varepsilon} \right\rfloor \quad \text{and} \quad T = \left\lfloor p^{\delta} \right\rfloor. \]

As in Section 2.2, we denote by \(\mathcal{L}\) the set of primes of the interval \([L, 2L]\). Note that 
\[ (\#S)^2TL \ll (\#S)^2hp^{-\varepsilon}. \]

Then 
\[ T_\chi(I, S) = \frac{1}{(T + 1)\#\mathcal{L}^\sigma} + O((\#S)^2TL) \]
(4) 
\[ = \frac{1}{(T + 1)\#\mathcal{L}^\sigma} + O((\#S)^2hp^{-\varepsilon}), \]
where

\[
\sigma = \sum_{\ell \in \mathcal{L}} \sum_{t=0}^{T} \sum_{u \in \tilde{I}} \sum_{s_1, s_2 \in S} \chi(u + s_1 + t\ell) \overline{\chi}(u + s_2 + t\ell)
= \sum_{t=0}^{T} \sum_{\ell \in \mathcal{L}} \sum_{s_1, s_2 \in S} \chi\left(\frac{u + s_1}{\ell} + t\right) \overline{\chi}\left(\frac{u + s_2}{\ell} + t\right).
\]

Furthermore,

\[
\sigma = \sum_{x, y \in \mathbb{F}_p} W(x, y) \sum_{t=0}^{T} \chi(x + t) \overline{\chi}(y + t),
\]

where \(W(x, y)\) is defined by (3).

Therefore, for any integer \(\nu \geq 1\) by the Hölder inequality, we have

\[
\sigma^{2\nu} \leq \sum_{x, y \in \mathbb{F}_p} W(x, y)^2 \left(\sum_{x, y \in \mathbb{F}_p} W(x, y)\right)^{2\nu - 2} \sum_{x, y \in \mathbb{F}_p} \left| \sum_{t=0}^{T} \chi(x + t) \overline{\chi}(y + t) \right|^{2\nu}.
\]

(5)

Clearly

\[
\sum_{x, y \in \mathbb{F}_p} W(x, y) \ll \#I \#\mathcal{L} (\#S)^2 \ll (\#S)^2 hL.
\]

(6)

We also have

\[
\sum_{x, y \in \mathbb{F}_p} \left| \sum_{t=0}^{T} \chi(x + t) \overline{\chi}(y + t) \right|^{2\nu} = \sum_{t_1, \ldots, t_{2\nu} = 0}^{T} \left| \sum_{x \in \mathbb{F}_p} \prod_{i=1}^{\nu} \chi(x + t_i) \prod_{i=\nu + 1}^{2\nu} \overline{\chi}(x + t_i) \right|^2.
\]

Using the Weil bound in the form given by [9, Corollary 11.24] if \((t_1, \ldots, t_{\nu})\) is not a permutation of \((t_{\nu+1}, \ldots, t_{2\nu})\) and the trivial bound otherwise, we derive

\[
\sum_{x, y \in \mathbb{F}_p} \left| \sum_{t=0}^{T} \chi(x + t) \overline{\chi}(y + t) \right|^{2\nu} \ll T^{2\nu} p + T^\nu p^2.
\]
(see also [9, Lemma 12.8] that underlies the Burgess method). Taking \( \nu \) to be large enough so that \( T^{2\nu}p > T^\nu p^2 \) we obtain

\[
(7) \quad \sum_{x,y \in \mathbb{F}_p} \left| \sum_{t=0}^T \chi(x+t) \chi(y+t) \right|^{2\nu} \ll T^{2\nu}p.
\]

Substituting (6) and (7) in (5) we obtain

\[
\sigma^{2\nu} \ll T^{2\nu}p \left( (\#S)^2 hL \right)^{2\nu-2} \sum_{x,y \in \mathbb{F}_p} W(x,y)^2.
\]

We now apply Lemma 3 to derive

\[
(8) \quad \sigma^{2\nu} \ll T^{2\nu}p \left( (\#S)^2 hL \right)^{2\nu-2} \left( (\#S)^3 hLp^{-1} + (\#S)^2 hLp^{o(1)} \right)
\ll T^{2\nu}p^{1+o(1)} \left( (\#S)^2 hL \right)^{2\nu} \left( (\#S)^{-1} p^{-1} + (\#S)^{-2} h^{-1} L^{-1} \right).
\]

Taking a sufficiently small \( \epsilon > 0 \), we obtain

\[
(\#S)^2 hL > p^{1+\epsilon}
\]

which together with (4) concludes the proof. \( \square \)

3. Root Finding Algorithms

3.1. Finding all roots. Here we address the question of finding all roots of a polynomial \( f \in \mathbb{F}_p[X] \).

We refer to [7] for description of efficient (in particular, polynomial time) algorithms of polynomial arithmetic over finite fields such as multiplication, division with remainder and computing the greatest common divisor.

**Theorem 5.** There is a deterministic algorithm that, given a squarefree polynomial \( f \in \mathbb{F}_p[X] \) of degree \( n \) that fully splits over \( \mathbb{F}_p \), finds all roots of \( f \) in time \( np^{1/2+o(1)} \).

**Proof.** We set

\[
h = \left[ p^{1/2}(\log p)^2 \right].
\]

We now compute the polynomials

\[
(9) \quad g_u(X) = \gcd \left( f(X), (X+u)^{(p-1)/2} - 1 \right), \quad u = 0, \ldots, h.
\]

We remark that to compute the greatest common divisor in (9) we first use repeated squaring to compute the residue

\[
H_u(X) \equiv (X+u)^{(p-1)/2} \pmod{f(X)}, \quad \deg H_u < n
\]

and then compute

\[
g_u(X) = \gcd \left( f(X), H_u(X) \right).
\]
If \( a \in \mathbb{F}_p \) is a root of \( f \) then \((X - a) | g_u(X)\) if and only if \( a + u \neq 0 \) and \( a + u \) is a quadratic residue in \( \mathbb{F}_p \).

We now note that the Weil bound on incomplete character sums implies that for any two roots \( a, b \in \mathbb{F}_p \) of \( f \) there is \( u \in [0, h] \) such that
\[
(X - a) | g_u(X) \quad \text{and} \quad (X - b) \nmid g_u(X).
\]

Note that the argument of [15, Theorem 1.1] shows that one can take \( h = \left\lfloor Cp^{1/2} \right\rfloor \) for some absolute constant \( C > 0 \) just getting some minor speed up of this and the original algorithm of Shoup [14].

We now recall the factor refinement algorithm of Bernstein [2], that, in particular, for any set of \( N \) polynomial \( G_1, \ldots, G_N \in \mathbb{F}_p[X] \) of degree \( n \) over \( \mathbb{F}_p \) in time \( O(nNp^{o(1)}) \) finds a set of relatively prime polynomials \( H_1, \ldots, H_M \in \mathbb{F}_p[X] \) such that any polynomial \( G_i, i = 1, \ldots, N, \) is a product of powers of the polynomials \( H_1, \ldots, H_M \). Applying this algorithm to the family of polynomials \( g_u, u = 0, \ldots, h, \) and recalling (10), we see that it outputs the set of polynomials with
\[
\{H_1, \ldots, H_M\} = \{X - a : f(a) = 0\},
\]
which concludes the proof. \( \square \)

### 3.2. Finding one root

Here we give an algorithm that finds one root of a polynomial over \( \mathbb{F}_p \). It is easy to see that up to a logarithmic factor this problem is equivalent to a problem of finding any nontrivial factor of a polynomial.

**Lemma 6.** There is a deterministic algorithm that, given a squarefree polynomial \( f \in \mathbb{F}_p[X] \) of degree \( n \) that fully splits over \( \mathbb{F}_p \), finds in time \( (n + p^{1/2})p^{o(1)} \) a factor \( g \mid f \) of degree \( 1 \leq \deg g < n \).

**Proof.** It suffices to prove that for any \( \delta > 0 \) there is a desirable algorithm with running time at most \( (n + p^{1/2})p^{\delta + o(1)} \). If \( n \leq p^{\delta} \) then the result follows from Theorem 5. Now assume that \( \delta \) is small and \( n > p^{\delta} \). Let
\[
h = \left\lfloor (1 + n^{-1}p^{1/2})p^{\delta/2} \right\rfloor.
\]

We start with computing the polynomials
\[
gcd(f(X), f(X + u)), \quad u = 1, \ldots, h,
\]
see [7] for fast greatest common divisor algorithms. Clearly, if \( f \) has two distinct roots \( a \) and \( b \) with \( |a - b| \leq h \) then one of the polynomials (11) gives a nontrivial factor of \( f \). It is also easy to see that the complexity of this step is at most \( nhp^{o(1)} \).
If this step does not produce any nontrivial factor of $f$ then we note that the set $S$ of the roots of $f$ is $h$-spaced. We now again compute the polynomials $g_u(X)$, given by (9), for every $u \in \mathcal{I}$.

So, we see that for the above choice of $h$ the condition of Lemma 4 holds and implies that there is $u \in \mathcal{I}$ with

$$\left| \sum_{s \in S} \left( \frac{s + u}{p} \right) \right| \ll \#S p^{-\eta} = np^{-\eta}.$$  

for some $\eta > 0$ that depends only on $\delta$, and thus the sequence of Legendre symbols $((s + u)/p)$, $s \in S$, cannot be constant.

Therefore, at least one of the polynomials (9) gives a nontrivial factor of $f$. As in [14], we see that the complexity of this algorithm is again $O\left(nh(\log p)^{O(1)}\right)$. Since $\delta > 0$ is an arbitrary, we obtain the desired result.

\[\square\]

**Theorem 7.** There is a deterministic algorithm that, given a squarefree polynomial $f \in \mathbb{F}_p[X]$ of degree $n$ that fully splits over $\mathbb{F}_p$, finds in time $(n + p^{1/2})p^{o(1)}$ a root of $f$.

**Proof.** We use Lemma 6 to find a polynomial factor $g_1$ of $f$ with $1 \leq \deg g \leq 0.5 \deg f$. Next, we find a polynomial factor $g_2$ of $g_1$ with $1 \leq \deg g_2 \leq 0.5 \deg g_1$, and so on. The number of iterations is $O(\log n)$, and the complexity of each iteration, by Lemma 6, does not exceed $(n + p^{1/2})p^{o(1)}$. This completes the proof. \[\square\]

**References**


Institute for Advanced Study, Princeton, NJ 08540, USA

E-mail address: bourgain@ias.edu

Steklov Mathematical Institute, 8, Gubkin Street, Moscow, 119991, Russia

E-mail address: konyagin@mi.ras.ru

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au