ON THE HIDDEN SHIFTED POWER PROBLEM

JEAN BOURGAIN, MOUBARIZ Z. GARAEV, SERGEI V. KONYAGIN, AND IGOR E. SHPARLINSKI

Abstract. We consider the problem of recovering a hidden element s of a finite field $\mathbb{F}_q$ of q elements from queries to an oracle that for a given $x \in \mathbb{F}_q$ returns $(x+s)^e$ for a given divisor $e \mid q-1$. We use some techniques from additive combinatorics and analytic number theory that lead to more efficient algorithms than the naive interpolation algorithm, for example, they use substantially fewer queries to the oracle.

1. Introduction

1.1. **Set-up and Motivation.** Let $\mathbb{F}_q$ be a finite field of q elements.

For a positive integer $e \mid q-1$ and an element $s \in \mathbb{F}_q$ we use $\mathcal{O}_{e,s}$ an oracle that on every input $x \in \mathbb{F}_q$ outputs $\mathcal{O}_{e,s}(x) = (x+s)^e$ for some "hidden" element $s \in \mathbb{F}_q$.

Here we consider the *Hidden Shifted Power Problem*:

> given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_q$, find s.

We also consider the following two versions of the *Shifted Power Identity Testing*:

> given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_q$ and known $t \in \mathbb{F}_q$, decide whether $s = t$ provided that the call $x = -t$ is forbidden;

and

> given two oracles $\mathcal{O}_{e,s}$ and $\mathcal{O}_{e,t}$ for some unknown $s, t \in \mathbb{F}_q$ decide whether $s = t$.

Certainly these problems are special cases of the more general problems of oracle (also sometimes called "black-box") polynomial interpolation and identity testing for arbitrary polynomials, see [4] and references therein.

We note that giving the values of $(x+s)^e$ is fully equivalent (modulo solving a discrete logarithm problem in the subgroup of $\mathbb{F}_q$ of order $(q-1)/e$) to giving the values of $\chi(x+s)$ for some fixed multiplicative character χ of $\mathbb{F}_q^*$, see [21, 22, 38], where several classical and quantum algorithms for this and some other similar problems are given. The

Hidden Shifted Power Problem, under the name of *Hidden Root Problem*, has also been re-introduced by Vercauteren [43] in relation to the so-called fault attack on pairing based cryptosystems on elliptic curves.

In the case when $\mathbb{F}_q$ has a subfield of an appropriate size some approaches to solving the Hidden Shifted Power Problem have been given in [43]. Here we concentrate on the case of prime fields.

For a prime $q = p \geq 3$ and $e = (p-1)/2$ the Hidden Shifted Power Problem has several other links to cryptography, and been considered in a number of works, see [1, 5, 23, 29] and references therein.

Furthermore, although for application to pairing based cryptography we usually have to solve the Hidden Shifted Power Problem in extension fields $q = p^k$ with $k > 1$, it has been shown by Koblitz and Menezes [31] that there are elliptic curves that lead to the case of $q = p$.

Certainly the most straightforward approach is to query $\mathcal{O}_{e,s}$ on $e+1$ arbitrary elements $x \in \mathbb{F}_q$ and then interpolate the results. Using a fast interpolation algorithm, see [27] leads to a deterministic algorithm of complexity $e(\log q)^{O(1)}$. For the Shifted Power Identity Testing, there is also a trivial probabilistic algorithm that is based on querying $\mathcal{O}_{e,s}$ (and $\mathcal{O}_{e,t}$) at randomly chosen elements $x \in \mathbb{F}_q$.

Here we mainly concentrate on the case of a prime $q = p \geq 3$. For the first variant of the Shifted Power Identity Testing (that is, when) t is known, using [9, Theorem 1] (see also [10]) that gives an upper bound on the intersection a conjugacy class of a subgroup of $\mathbb{F}_p^*$ with a set of Farey fractions of a given order, we can obtain a faster algorithm of complexity $e^{1/2}p^{o(1)}$, where $o(1)$ always, if the opposite is not indicated, denotes a quantity that tends to zero as $p \to \infty$.

Here we obtain further improvements and in particular show that there is an algorithm of complexity $e^{1/4}p^{o(1)}$ for any $e \leq (p-1)/2$.

The second question, that is, when t is unknown, seems to be harder, however we also obtain an improvement of the trivial interpolation algorithm and show that it can be solved by an algorithm of complexity $e^{2/3}p^{o(1)}$ for any $e \leq (p-1)/2$. Moreover, if $e = p^{o(1)}$ then we can achieve complexity $e^{o(1)}(\log p)^{O(1)}$.

1.2. **Our Approach.** Let $\mathcal{G}_e \subseteq \mathbb{F}_q^*$ be the multiplicative group of order $e \mid q-1$, that is,

$$\mathcal{G}_e = \{\mu \in \mathbb{F}_q \ : \ \mu^e = 1\}.$$

We now define the polynomials

$$F_{s,t}(X) = \prod_{\mu \in \mathcal{G}_e} \left(X + s - \mu(X + t)\right).$$

Our approach is based on the idea of choosing a small "test" set $\mathcal{X}$, which nevertheless is guaranteed to contain at least one non-zero of the polynomial $F_{s,t}$ for any $s \neq t$. This is based on a careful examination of the roots of $F_{s,t}$ and relating it to some classical number theoretic problems about the distribution of elements of small subgroups of finite fields.

Clearly, if $F_{s,t}(x) = 0$ for some $x \in \mathbb{F}_q^*$ then

$$\frac{x+s}{x+t} \in \mathcal{G}_e \tag{1}$$

(provided $x + t \neq 0$). If t is known, then we can choose the "test" set $\mathcal{X}$ in the form

$$\mathcal{X} = \{y^{-1} - t \ : \ y \in \mathcal{Y}\} \tag{2}$$

for some set $\mathcal{Y} \subseteq \mathbb{F}_q^*$. Then the condition (1) means that a shift of $\mathcal{Y}$ is contained inside of a coset of $\mathcal{G}_e$, that is

$$\mathcal{Y} + r \subseteq r\mathcal{G}_e \tag{3}$$

where $r = (s-t)^{-1}$.

So our goal is to find a "small" set $\mathcal{Y} \subseteq \mathbb{F}_q^*$ such that its shifts cannot be inside of any coset of $\mathcal{G}_e$ (we note that the value of r is unknown). Questions about the distribution of cosets of multiplicative groups have been considered in a number of works and have numerous applications, see [33] and also [6, 8, 12, 9, 11, 39, 41, 42] for several more recent results and applications to cryptographic and computational number theory problems.

Here we concentrate on the case of prime fields, that is, when $q = p$ is prime, where the tools we use are most developed and have rather sharp and explicit forms. This allows us to get a series of nontrivial estimates for both versions of the Shifted Power Identity Testing.

The idea is to choose $\mathcal{Y}$ as a short interval of h consecutive integers and to define $\mathcal{X}$ by (2). We then use a combination of results of Cilleruelo and Garaev [18] with the classical *Burgess and Weil bounds* (see [30]) to show that (3) fails (for some integer h significantly smaller than e).

Furthermore, for small values of e (for example, for $e = p^{o(1)}$) we obtain much stronger results and develop a new technique, which is based on several tools of commutative algebra and additive combinatorics. For example, we combine an explicit version of the Hilbert's *Nullstellensatz*, see [34, Theorem 1], with a generalisation of a result of [9].

For the Hidden Shifted Power Problem we have not been able to improve on the interpolation approach. However, assuming that oracle calls are expensive, one can consider algorithms that minimise the number of such calls, that is, algorithms of low *oracle complexity*. Here we use a result of [40] in a combination of some new bounds of character sums that are based on some ideas of Chang [16] to design several algorithms that require substantially less than e oracle calls that are needed for the interpolation approach.

Here we concentrate on the case of prime $q = p$ as in the general case several tools that exist in prime fields are unfortunately not available.

Besides concrete results we believe the present paper also introduces a number of new techniques to this area that can probably be used in several other questions.

1.3. **Notation.** Throughout the paper, the letter p always denotes a prime; k, m and n (as well as K, M and N) always denote positive integers.

Any implied constants in symbols O, $\ll$ and $\gg$ may occasionally depend, where obvious, on the integer parameter ν and the real positive parameters ε and δ, and are absolute otherwise. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that $|U| \le cV$ holds with some constant $c > 0$.

For a field $\mathbb{F}$, sets $\mathcal{A}_1, \ldots, \mathcal{A}_m \subseteq \mathbb{F}$ and a rational function

$$F(X_1, \ldots, X_m) \in \mathbb{F}(X_1, \ldots, X_m),$$

we define the set

$$F(\mathcal{A}_1, \ldots, \mathcal{A}_m) = \{F(a_1, \ldots, a_m) \ : \ a_1 \in \mathcal{A}_1, \ldots, a_m \in \mathcal{A}_m\}$$

(where the poles are ignored or alternatively the function F can be defined as zero at its poles). In particular, for an integer ν, $\mathcal{A}^{(\nu)}$ denotes ν-fold product sets. However, we reserve the notation $\nu\mathcal{A}$ for the element-wise multiplication by ν, that is, $\nu\mathcal{A} = \{\nu a \ : \ a \in \mathcal{A}\}$. We also reserve $\mathcal{A}^\nu$ for the ν-fold Cartesian product of $\mathcal{A}$.

2. Tools from Analytic Number Theory, Polynomial Algebra and Arithmetic Combinatorics

2.1. **Finding and Bounding the Number of Solutions of Some Congruences.** We start with the bound of Cilleruelo and Garaev [18, Theorem 1] on the number of points of modular hyperbolas in small boxes.

Lemma 1. *Uniformly over integers u and v with $\gcd(v,p)=1$, the congruence*

$$(x+u)(y+u) \equiv v \pmod p, \qquad 1 \le x, y \le H,$$

has at most $H^{3/2}p^{-1/2} + H^{o(1)}$ solutions as $H \to \infty$.

We also need an estimate from [19] that follows from a combination of a result of Garaev and Garcia [25] (or a slightly weaker result of Ayyad, Cochrane and Zheng [2, Theorem 1]) and Lemma 1.

Lemma 2. *Uniformly over integers a and H with $\gcd(v,p)=1$, the congruence*

$$(a+x_1)(a+x_2) \equiv (a+x_3)(a+x_4) \pmod p, \qquad 1 \le x_1, x_2, x_3, x_4 \le H,$$

has $H^4/p + O(H^{2+o(1)})$ solutions as $H \to \infty$.

The following result for $m=1$ is due to Garcia and Voloch [26]; another proof, with different constants, based on the method of Stepanov, can be found in [33, Lemma 3.2]. For any fixed $m \ge 1$ it follows instantly from [40, Lemma 4.1] by taking $s=1$, $t=e$, $k=m$ and $B = \left\lfloor t^{1/(2k+1)} \right\rfloor + 1$.

Lemma 3. *Assume that for a fixed integer $m \ge 1$ we have*

$$p \ge \left(2m \left\lfloor e^{1/(2m+1)} \right\rfloor + 2m + 2\right) e.$$

Then for pairwise distinct $\mu_1, \ldots, \mu_m \in \mathbb{F}_p^*$ and arbitrary $\lambda_1, \ldots, \lambda_m \in \mathbb{F}_p^*$ the bound

$$\# \left(\mathcal{G}_e \cap (\lambda_1 \mathcal{G}_e + \mu_1) \cap \ldots \cap (\lambda_m \mathcal{G}_e + \mu_m)\right) \ll e^{(m+1)/(2m+1)}$$

holds, where the implied constant depends on m.

For $x \in \mathbb{F}_p$, we denote by $|x|$ the minimum of absolute values of integers in the residue class of x modulo p. We say that a set $\mathcal{D} \subseteq \mathbb{F}_p$ is Δ-spaced if $|d_1 - d_2| \ge \Delta$ for any two distinct elements $d_1, d_2 \in \mathcal{D}$.

We now need a version of [16, Lemma 7].

Lemma 4. *Let $0 \le \beta < 1/2$, $\mathcal{I} = [1, p^\beta]$ and let $\mathcal{D} \subseteq \mathbb{F}_p$ be a p^β-spaced set of cardinality $\#\mathcal{D} = p^\sigma$. Then for any $\varepsilon > 0$ and sufficiently small $\beta_1, \ldots, \beta_j$ and sufficiently large p, the number of solutions $w(u)$ to the congruence*

$$x + d \equiv u z_1 \ldots z_j \pmod p,$$

with

$$(x, d, z_1, \ldots, z_j) \in \mathcal{I} \times \mathcal{D} \times \mathcal{J}_1 \times \ldots \times \mathcal{J}_j,$$

where $\mathcal{J}_i = [1, p^{\beta_i}]$, $i = 1, \ldots, j$, *satisfies the bound*

$$\sum_{u \in \mathbb{F}_p} w(u)^2 \ll p^{\beta + b + \sigma(b/(1-\beta)+1)+\varepsilon},$$

where

$$b = \sum_{i=1}^{j} \beta_i.$$

Corollary 5. *Let* $\mathcal{S} \subseteq \mathbb{F}_p$ *be set of cardinality* $\#\mathcal{S} = p^\alpha$. *Then under the conditions of Lemma 4 the number of solutions* $w(u, v)$ *to the systems of congruences*

$$x + d \equiv u z_1 \ldots z_j \pmod p \qquad \text{and} \qquad x + s \equiv v z_1 \ldots z_j \pmod p$$

with

$$(x, d, s, z_1, \ldots, z_j) \in \mathcal{I} \times \mathcal{D} \times \mathcal{S} \times \mathcal{J}_1 \times \ldots \times \mathcal{J}_j,$$

satisfies the bound

$$\sum_{u,v \in \mathbb{F}_p} w(u, v)^2 \ll p^{\alpha + \beta + b + \sigma(b/(1-\beta)+1)+\varepsilon}.$$

2.2. **Finding Solutions to Binomial Equations.**

Lemma 6. *Let* G *be a group of order* m, *and let* d *be relatively prime to* m. *Let* $a \in G$. *Then the equation* $x^d = a$ *has the unique solution* $x = a^f$ *where* $df \equiv 1 \pmod m$.

This is the first part of [3, Theorem 7.3.1].

Now we consider equaitons $x^r = a$ in groups in the case when r is a prime dividing the order of the group. Considering the cyclic group of order m, we do not assume that we are given a generating element of the group. Instead, we assume that there is an oracle which gives some unique label to every elements of G and also that given $a, b \in G$ computes the product of these elements in time $(\log m)^{O(1)}$. A natural example is the multiplicative group $\mathbb{F}_p^*$. The following result is implicitly contained in [3, Theorem 7.3.2].

Lemma 7. *Let* G *be the cyclic group of order* m, *and let* r *be a prime dividing* m. *Given an element* $b \in G$ *so that the equation* $y^r = b$ *has no solutions in* G, *for any* $a \in G$ *there is a deterministic algorithm to find all solutions of the equation* $x^r = a$ *in time* $r(\log m)^{O(1)}$.

Although the algorithm analysed in [3, Theorem 7.3.2] is probabilistic, is easy to see that the only place where the randomisation is used is in finding b satisfying the conditions of Lemma 7.

Subsequently, applying Lemma 7 we get the following:

Lemma 8. *For a prime p, a positive integer $e \mid p-1$ and $A \in \mathbb{F}_p$, given ℓ-th power nonresidues for all prime divisors $\ell \mid e$, there is a deterministic algorithm to find all solutions of the equation $x^e = A$ in time $e(\log p)^{O(1)}$.*

Now we consider the solutions of the equation $x^r = A$ satisfying restrictions. Let ℓ be a prime divisor of e. For a positive integer α, we write $\ell^\alpha \| e$ if $\ell^\alpha \mid e$ and $\ell^{\alpha+1} \nmid e$. By $\operatorname{ind} x$ we denote the index of an element $x \in \mathbb{F}_p^*$ with respect to a fixed primitive root g modulo p, that is the unique integer $z \in [1, p-1]$ with $x = g^z$.

Lemma 9. *For a prime p, $A \in \mathbb{F}_p$, and a prime ℓ with $\ell^\alpha \| p-1$, there is a deterministic algorithm to find all solutions of the equation $x^\ell = A$ satisfying $\ell^\alpha \mid \operatorname{ind} x$ in time $\ell(\log p)^{O(1)}$.*

Proof. It is enough to apply Lemma 6 to the group $G = \{x \in \mathbb{F}_p^* \ : \ \ell^\alpha \mid \operatorname{ind} x\}$ of order $(p-1)/\ell^\alpha$ not divisible by ℓ. □

Lemma 10. *For a prime p, $A \in \mathbb{F}_p$, for a prime divisor $\ell \mid p-1$ with $\ell^\alpha \| p-1$ and a nonnegitive integer $\beta < \alpha$, given an $\ell^{\beta+1}$-th power nonresidue, there is a deterministic algorithm to find all solutions of the equation $x^\ell = A$ satisfying $\ell^\beta \mid \operatorname{ind} x$ in time $\ell(\log p)^{O(1)}$.*

Proof. Let a be an $\ell^{\beta+1}$-th power nonresidue. Then $\ell^\gamma \| \operatorname{ind} a$ for some $\gamma \le \beta$. Hence, $\ell^\beta \| \operatorname{ind} b$ for $b = a^{l^{\beta-\gamma}}$. Then we can apply Lemma 7 to

$$G = \{x \in \mathbb{F}_p^* \ : \ \ell^\beta \mid \operatorname{ind} x\}$$

and $r = \ell$. □

Subsequently applying Lemmas 9 and 10 we get the following.

Lemma 11. *Let p be a prime and $e \mid p-1$. For any prime divisor $\ell \mid e$ with $\ell^{\alpha_l} \| p-1$ we take either $\gamma_\ell = \alpha_\ell$ or $\gamma_\ell < \alpha_\ell$ so that we are given an $\ell^{\gamma_\ell+1}$-th power nonresidue. Let*

$$n = \prod_{\substack{\ell \mid e \\ \ell \text{ prime}}} \ell^{\gamma_\ell}$$

and $A \in \mathbb{F}_p$. Then there is a deterministic algorithm to find all solutions of the equation $x^e = A$ satisfying $n \mid \operatorname{ind} x$ in time $e(\log p)^{O(1)}$.

Lemma 12. *Assume that p, e, n satisfy the conditions of Lemma 11. Let $A_0, \dots, A_n \in \mathbb{F}_p$. Then there is a deteministic algorithm to find all solutions of the system of equations*

$$(x+j)^e = A_j, \qquad j = 0, \dots, n,$$

in time $e(\log p)^{O(1)} n^{O(1)}$.

Proof. If $A_j = 0$ for some j, then there is nothing to prove. We consider that $A_j \neq 0$ for all $j = 0, \ldots, n$. Let x be any solution of the system. By the pigeonhole principle, there are $j_1 \neq j_2$ so that

$$\operatorname{ind}(x + j_1) \equiv \operatorname{ind}(x + j_2) \pmod{n},$$

or, equivalently, $n \mid \operatorname{ind} y$ for $y = (x + j_2)/(x + j_1)$. We can extract all such x satisfying the above system of equations by applying Lemma 11 to the equation $y^e = A_{j_2}/A_{j_1}$ and testing all possible values of

$$x = \frac{j_2 - j_1}{y - 1} - j_1.$$

To complete the proof, we simply try all pairs (j_1, j_2) with $0 \le j_1 < j_2 \le n$. □

2.3. **Smooth Numbers and Their Reductions Modulo p.** Let $x, y > 0$. A positive integer n is called y-smooth if it is composed of prime numbers up to y. The $\Psi(x, y)$ function is defined as the number of y-smooth positive integers that are up to x.

We know the following estimate for $\Psi(x, y)$, see [28, Corollary 1.3]:

Lemma 13. *Let $x \ge y \ge 2$ and $u = (\log x)/\log y$. For any fixed $\delta > 0$ we have*

$$\Psi(x, y) = xu^{-(1+o(1))u},$$

as y and u tend to infinity, uniformly in the range $y \ge (\log x)^{1+\delta}$.

Corollary 14. *Let $0 < \varepsilon < 1/2$ be fixed and p be a prime. Then the order of the subgroup of $\mathbb{F}_p^*$ generated by $\{1, \ldots, \lfloor p^\varepsilon \rfloor\}$, is at least $p\varepsilon^{-c/\varepsilon}$ for some absolute constant $c > 0$.*

Proof. Let $x = p - 1$ and $y = \lfloor p^\varepsilon \rfloor$. Also, let $\mathcal{H}$ be the subgroup of $\mathbb{F}_p^*$ generated by $\{1, \ldots, y\}$. If $y < (\log p)^2$ then the result follows from the trivial estimate $\#\mathcal{H} \ge 1$. Assume that $y \ge (\log p)^2$. Observe that all y-smooth numbers belong to H. Hence, $\#\mathcal{H} \ge \Psi(x, y)$, and the result follows from Lemma 13. □

2.4. **Combinatorial Estimates.** We need the following result about covering an arbitrary set $\mathcal{S} \subseteq \mathbb{F}_p$ by $\sqrt{p}/3$-spaced sets.

Lemma 15. *Let $p \ge 37$, $\kappa > 0$ and $\xi = \left\lfloor \sqrt{p} \right\rfloor$. Then any set $\mathcal{S} \subseteq \mathbb{F}_p$ of size $\#\mathcal{S} \ge 16p^{2\kappa}$ contains disjoint subsets $\mathcal{D}_k$, $k = 1, \ldots, K$, and $\mathcal{E}_\ell$, $\ell = 1, \ldots, L$, such that*

- **(i)** $\#\mathcal{D}_k, \#\mathcal{E}_\ell \ge 0.25p^{-\kappa} (\#\mathcal{S})^{1/2}$, $k = 1, \ldots, K$, $\ell = 1, \ldots, L$;
- **(ii)** *$\mathcal{D}_k$ is a $\sqrt{p}/3$-spaced set, $k = 1, \ldots, K$;*
- **(iii)** *$\xi\mathcal{E}_\ell$ is a $\sqrt{p}/3$-spaced set, $\ell = 1, \ldots, L$;*
- **(iv)** $\#\left(\mathcal{S} \setminus (\mathcal{S}_0 \cup \mathcal{S}_1)\right) \le 2p^{-\kappa}\#\mathcal{S}$, *where* $\mathcal{S}_0 = \cup_{k=1}^K \mathcal{D}_k$, $\mathcal{S}_1 = \cup_{\ell=1}^L \mathcal{E}_\ell$.

Proof. Let $U = \sqrt{p}/3$. Extract from $\mathcal{S}$ a maximum (that is, not extendable any more) collection of disjointed U-spaced sets $\mathcal{D}_k$ with $\#\mathcal{D}_k \ge (\#\mathcal{S})^{1/2}$, $k = 1, \ldots, K$ and denote

$$\mathcal{T} = \mathcal{S} \setminus \mathcal{S}_0$$

where, as before, $\mathcal{S}_0 = \cup_{k=1}^{K} \mathcal{D}_k$.

Clearly

$$\mathcal{T} \subseteq \bigcup_{x \in \mathcal{X}} (x + \mathcal{I}),$$

for $\mathcal{I} = [-U, U]$ and some U-spaced set $\mathcal{X} \subseteq \mathbb{F}_p$ with $\#\mathcal{X} < (\#\mathcal{S})^{1/2}$. Let $\widetilde{\mathcal{E}}_\ell$, $\ell = 1, \ldots, L$, be the collection of the sets $\mathcal{T} \cap (x + \mathcal{I})$, $x \in \mathcal{X}$, for which $\#\left(\mathcal{T} \cap (x + \mathcal{I})\right) > p^{-\kappa} (\#\mathcal{S})^{1/2}$.

The total size of the remaining sets $\mathcal{T} \cap (x + \mathcal{I})$, $x \in \mathcal{X}$, is at most $p^{-\kappa} (\#\mathcal{S})^{1/2} \#\mathcal{X} \le p^{-\kappa} \#\mathcal{S}$.

Now we take disjoint subsets $\mathcal{E}_\ell \subseteq \widetilde{\mathcal{E}}_\ell$ so that

$$\bigcup_{\ell=1}^{L} \mathcal{E}_\ell = \bigcup_{\ell=1}^{L} \widetilde{\mathcal{E}}_\ell.$$

Thus, for any $\ell = 1, \ldots, L$ the set $\mathcal{E}_\ell$ is formed by all elements of $x \in \widetilde{\mathcal{E}}_\ell$ belonging to no other sets $x \in \widetilde{\mathcal{E}}_j$ and some elements shared by $\mathcal{E}_\ell$ and another set $\widetilde{\mathcal{E}}_j$.

Any element $x \in \mathbb{F}_p$ belongs to at most two sets $\widetilde{\mathcal{E}}_\ell$. Moreover, any set $\widetilde{\mathcal{E}}_\ell$ can have common elements with at most two sets $\widetilde{\mathcal{E}}_j$. If $\ell < j$ and $\widetilde{\mathcal{E}}_\ell$ and $\widetilde{\mathcal{E}}_j$ have n common elements, we send $\lfloor n/2 \rfloor$ of them to $\mathcal{E}_\ell$ and other $\lceil n/2 \rceil$ elements to $\mathcal{E}_j$. We obtain a collection of disjoint sets $\mathcal{E}_\ell$ of size

$$\#\mathcal{E}_\ell \ge \#\widetilde{\mathcal{E}}_\ell/2 - 1 \ge p^{-\kappa} (\#\mathcal{S})^{1/2}/2 - 1 \ge 0.25 p^{-\kappa} (\#\mathcal{S})^{1/2},$$

for $\ell = 1, \ldots, L$.

Hence, with $\mathcal{S}_1 = \cup_{\ell=1}^{L} \mathcal{E}_\ell$, we have

$$\#\left(\mathcal{S} \setminus (\mathcal{S}_0 \cup \mathcal{S}_1)\right) \le p^{-\kappa} \#\mathcal{S}.$$

Since $p \ge 37$, we have

$$2U(\xi + 1) < (2\sqrt{p}/3)(\sqrt{p} + 1) < (\sqrt{p} - 1)(\sqrt{p} + 1) < p,$$

or $2U \times \xi < p - U$. Also, $\xi > U$. Therefore, the set $\xi\mathcal{I}$ is U-spaced, and certainly the set $\xi\mathcal{E}_\ell$ is also U-spaced for every $\ell = 1, \ldots, L$. $\square$

2.5. **Bounds of Multiplicative Character Sums.** We need the following very special case of the Weil bound on sums of multiplicative characters (see [30, Theorem 11.23]).

Lemma 16. *For an arbitrary integer h with $1 \le h < p$, a positive integer f and a nonprincipal multiplicative character χ of $\mathbb{F}_p^*$, the bound*

$$\sum_{x=1}^{p} \chi\left(x^f + h\right) = O\left(fp^{1/2}\right)$$

holds.

Also, we need an estimate for character sums including both multiplicative and additive characters (see [35, Chapter 6, Theorem 3] or [44, Appendix 5, Example 12]).

Lemma 17. *Let $\chi_1, \ldots, \chi_r$ be characters modulo p, and at least one of them is nonprincipal and let $f(X) \in \mathbb{F}_p[X]$ be an arbitrary polynomial of degree d. Then for any distinct $a_1, \ldots, a_r \in \mathbb{F}_p$ we have*

$$\left| \sum_{x \in \mathbb{F}_p} \chi_1(x + a_1) \ldots \chi_r(x + a_r) \exp\left(2\pi i f(x)/p\right) \right| \le (r + d)p^{1/2}.$$

The standard reduction of incomplete sums to complete ones (see [30, Section 12.2]) together with the bound of Lemma 17 lead to the following estimate:

Lemma 18. *For an arbitrary integer h with $1 \le h \le p$, distinct elements $s, t \in \mathbb{F}_p$ and a nonprincipal multiplicative character χ of $\mathbb{F}_p^*$, the bound*

$$\sum_{\substack{x=1 \\ x \ne t}}^{h} \chi\left(\frac{x+s}{x+t}\right) = O\left(p^{1/2} \log p\right)$$

holds.

The following result is a combination of the Pólya-Vinogradov (for $\nu = 1$) and Burgess (for $\nu \ge 2$) bounds, see [30, Theorems 12.5 and 12.6].

Lemma 19. *For an arbitrary integer h with $1 \le h < p$, and a nonprincipal multiplicative character χ of $\mathbb{F}_p^*$, the bound*

$$\left| \sum_{y=1}^{h} \chi(y) \right| \le h^{1-1/\nu} p^{(\nu+1)/4\nu^2 + o(1)}$$

holds with an arbitrary positive integer ν.

We use $\overline{\chi}$ to denote the complex conjugate character to χ. The following estimate is a generalisation of [16, Theorem 8].

Lemma 20. *Let $0 \le \beta < 1/2$, $\mathcal{I} = [0, p^\beta]$. Let $\mathcal{D} \subseteq \mathbb{F}_p$ be a p^β-spaced set of cardinality $\#\mathcal{D} = p^\sigma$ and let $\mathcal{S} \subseteq \mathbb{F}_p$ be set of cardinality $\#\mathcal{S} = p^\alpha$. For any $\delta > 0$ there is some $\eta > 0$ such that if*

$$2\beta + \alpha + \sigma\frac{1-2\beta}{1-\beta} > 1 + \delta$$

then for any nontrivial multiplicative character χ of $\mathbb{F}_p^*$ we have

$$\sum_{d\in\mathcal{D}}\sum_{s\in\mathcal{S}}\left|\sum_{x\in\mathcal{I}}\chi(x+d)\overline{\chi}(x+s)\right| < p^{\alpha+\beta+\sigma-\eta}.$$

Proof. We can assume that δ is sufficiently small. Take a sufficiently large j and set

$$\beta_0 = \frac{\delta}{6} \qquad \text{and} \qquad \gamma = \frac{\beta-\beta_0}{j+1}$$

and consider the intervals $\mathcal{J} = [1, p^\gamma]$ and $\mathcal{J}_0 = [1, p^{\beta_0}]$. It is easy to see that

$$\begin{aligned}\sum_{d\in\mathcal{D}}\sum_{s\in\mathcal{S}}&\left|\sum_{x\in\mathcal{I}}\chi(x+d)\overline{\chi}(x+s)\right| \\ &\ll p^{-\beta_0-j\gamma}\sum_{d\in\mathcal{D}}\sum_{s\in\mathcal{S}}\sum_{z_1,\ldots,z_j\in\mathcal{J}} \\ &\qquad \sum_{x\in\mathcal{I}}\left|\sum_{t\in\mathcal{J}_0}\chi\left(\frac{x+d}{z_1\ldots z_j}+t\right)\overline{\chi}\left(\frac{x+s}{z_1\ldots z_j}+t\right)\right| \\ &\qquad\qquad + p^{\alpha+\sigma+\beta_0+j\gamma}.\end{aligned}$$

Now, invoking Corollary 5 and using the same argument as in the proof of [16, Theorem 8] we obtain the desired result. □

Lemma 21. *Assume that $\alpha > 0$, $\delta > 0$ and $0 \le \beta < 1/2 - \delta$ satisfy*

$$2\beta + \alpha\frac{3-4\beta}{2-2\beta} > 1 + \delta.$$

Let $\mathcal{S} \subseteq \mathbb{F}_p$ be of cardinality $\#\mathcal{S} = p^\alpha$ and let $\mathcal{I} = [0, p^\beta]$. We denote

$$\xi = \lfloor\sqrt{p}\rfloor$$

and define ζ by the conditions

$$\zeta\xi \equiv 1 \pmod p \qquad \text{and} \qquad 1 \le \zeta < p.$$

There is a partition

$$\mathcal{S} = \mathcal{T}_0 \cup \mathcal{T}_1 \qquad \text{and} \qquad \mathcal{T}_0 \cap \mathcal{T}_1 = \emptyset$$

such that for any nontrivial multiplicative character χ of $\mathbb{F}_p^*$ we have

$$\sum_{s_1,s_2 \in \mathcal{T}_\nu} \left| \sum_{x \in \mathcal{I}} \chi(\zeta^\nu x + s_1)\overline{\chi}(\zeta^\nu x + s_2) \right| \ll \#\mathcal{I}(\#S)^2 p^{-\eta}, \qquad \nu = 0, 1,$$

for some $\eta > 0$ that depends only on δ.

Proof. We consider that p is so large that $p \ge 37$ and $p^\delta \ge 3$. Then $p^\beta < \sqrt{p}/3$. We take $\kappa = \delta/10$ and define set $\mathcal{S}_0$ and $\mathcal{S}_1$ as in Lemma 15. We now put $\mathcal{T}_1 = \mathcal{S}_1$ and then define $\mathcal{T}_0 = \mathcal{S} \setminus \mathcal{T}_1$.

Then in the notation of Lemma 15 we have

$$\begin{aligned}
&\sum_{s_1,s_2 \in \mathcal{T}_0} \left| \sum_{x \in \mathcal{I}} \chi(x + s_1)\overline{\chi}(x + s_2) \right| \\
&\qquad = \sum_{s_1,s_2 \in \mathcal{S}_0} \left| \sum_{x \in \mathcal{I}} \chi(x + d)\overline{\chi}(x + s) \right| + O\left((\#S)^2 \#\mathcal{I} p^{-\kappa}\right) \\
&\qquad = \sum_{k=1}^{K} \sum_{d \in \mathcal{D}_k} \sum_{s \in \mathcal{S}_0} \left| \sum_{x \in \mathcal{I}} \chi(x + d)\overline{\chi}(x + s) \right| + O\left((\#S)^2 \#\mathcal{I} p^{-\kappa}\right) \\
&\qquad \le \sum_{k=1}^{K} \sum_{d \in \mathcal{D}_k} \sum_{s \in \mathcal{S}} \left| \sum_{x \in \mathcal{I}} \chi(x + d)\overline{\chi}(x + s) \right| + O\left((\#S)^2 \#\mathcal{I} p^{-\kappa}\right).
\end{aligned}$$

Since $\mathcal{D}_k$ is a p^β-spaced of cardinality $\#\mathcal{D}_k \ge p^\sigma$ with $\sigma = \alpha/2 - \kappa$, $k = 1, \ldots, K$, we see that the conditions of Lemma 20 are satisfied, which implies the desired bound for the set $\mathcal{S}_0$.

For the set $\mathcal{T}_1$ we write

$$\begin{aligned}
&\sum_{s_1,s_2 \in \mathcal{T}_1} \left| \sum_{x \in \mathcal{I}} \chi(\zeta x + s_1)\overline{\chi}(\zeta x + s_2) \right| \\
&\qquad = \sum_{s_1,s_2 \in \mathcal{S}_1} \left| \sum_{x \in \mathcal{I}} \chi(x + \xi s_1)\overline{\chi}(x + \xi s_2) \right|
\end{aligned}$$

and then proceed as before, applying Lemma 20 with $\mathcal{S}$ replaced by the set $\xi\mathcal{S}$. □

2.6. **Quantitative Result on Polynomial Ideals.** We recall the following quantitative version of the Bézout theorem, that follows from a result of Krick, Pardo, and Sombra [34, Theorem 1] (that improves a series of previous estimates).

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

Lemma 22. *Let $P_1, \ldots, P_N \in \mathbb{Z}[Z_1, \ldots, Z_n]$ be $N \geq 1$ polynomials in n variables without common zero in $\mathbb{C}^n$ of degree at most $D \geq 3$ and of logarithmic height at most H. Then there is a positive integer b with*

$$\log b \leq c(n) D^n \left(H + \log N + D\right)$$

and polynomials $R_1, \ldots, R_N \in \mathbb{Z}[Z_1, \ldots, Z_n]$ such that

$$P_1 R_1 + \ldots + P_N R_N = b,$$

where $c(n)$ depends only on n.

Using the classical argument of Hilbert we obtain the following version of the Nullstellensatz (see [7] for several similar results and further references).

Lemma 23. *Let $P_1, \ldots, P_N, f \in \mathbb{Z}[Z_1, \ldots, Z_n]$ be $N + 1 \geq 2$ polynomials in n variables of degree at most $D \geq 3$ and of logarithmic height at most H such that f vanishes on the variety*

$$P_1(Z_1, \ldots, Z_n) = \ldots = P_N(Z_1, \ldots, Z_n) = 0.$$

There are positive integers b and r with

$$\log b \leq C(n) D^{n+1} \left(H + \log N + D\right)$$

and polynomials $Q_1, \ldots, Q_N \in \mathbb{Z}[Z_1, \ldots, Z_n]$ such that

$$P_1 Q_1 + \ldots + P_N Q_N = b f^r,$$

where $C(n)$ depends only on n.

Proof. We consider $N + 1$ polynomials

$$\widetilde{P}_0 = 1 - Tf \qquad \text{and} \qquad \widetilde{P}_j = TP_j, \ j = 1, \ldots, N,$$

in $\mathbb{Z}[Z_1, \ldots, Z_n, T]$. By the assumption on f, they have no common zero. Hence, by Lemma 22 we get

$$(1 - Tf)Q_0 + TP_1 Q_1 + \ldots + TP_N Q_N = b$$

for some polynomials $Q_0, Q_1, \ldots, Q_N \in \mathbb{Z}[Z_1, \ldots, Z_n]$ and a positive integer b satisfying the desired inequality. Replacing T by $1/f$ and clearing the denominators we obtain the desired relation. □

Finally, we need a slightly more general form of a result of Chang [15]. In fact, this is exactly the statement that is established in the proof of [15, Lemma 2.14], see [15, Equation (2.15)].

Lemma 24. *Let $P_1, \ldots, P_N, P \in \mathbb{Z}[Z_1, \ldots, Z_n]$ be $N+1 \ge 2$ polynomials in n variables of degree at most D and of logarithmic height at most $H \ge 1$. If the zero-set*

$$P_1(Z_1, \ldots, Z_n) = \ldots = P_N(Z_1, \ldots, Z_n) = 0 \quad \text{and} \quad P(Z_1, \ldots, Z_n) \ne 0$$

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

Finally, we recall the following well-known result, see, for example, [27, Theorem 6.32].

Lemma 25. *Let $P, Q \in \mathbb{Z}[Z]$ be two univariate non-zero polynomials with $Q \mid P$. If P is of logarithmic height at most $H \ge 1$ then Q is of logarithmic height at most $H + O(1)$, where the implied constant depends only on* $\deg P$.

2.7. **Product Sets in Number Fields.** Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$ and let $\mathbb{Z}_{\mathbb{K}}$ be the ring of integers in $\mathbb{K}$. We denote by $\mathcal{H}(\gamma)$ the logarithmic height of $\gamma \in \mathbb{K}$. We recall that the logarithmic height of an algebraic number α is defined as the logarithmic height of its minimal polynomial.

For an integral ideal $\mathfrak{a}$ of $\mathbb{Z}_{\mathbb{K}}$ we denote by $\mathrm{Nm}\,(\mathfrak{a})$ the norm of $\mathfrak{a}$, that is, the cardinality of the residue ring $\mathbb{Z}_{\mathbb{K}}/\mathfrak{a}\mathbb{Z}_{\mathbb{K}}$. We also use $\mathrm{Nm}\,(\alpha)$ to denote the norm of $\alpha \in \mathbb{Z}_{\mathbb{K}}$. In particular $\mathrm{Nm}\,(\alpha) = \mathrm{Nm}\,((\alpha))$ where (α) denotes the principal ideal generated by α.

First we recall the following well-known bound, which follows immediately from [37, Lemma 4.2] and the classical bound on the divisor function.

Lemma 26. *Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$ of degree $d = [\mathbb{K} : \mathbb{Q}]$. For any integer $N \ge 3$, in $\mathbb{K}$ there are at most $\exp\left(O(\log N/\log\log N)\right)$ integral ideals of norm N, where the implied constant depends on d.*

We also need a bound of Chang [15, Proposition 2.5] on the divisor function in algebraic number fields.

Lemma 27. *Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$ of degree $d = [\mathbb{K} : \mathbb{Q}]$. For any algebraic integer $\gamma \in \mathbb{Z}_K$ of logarithmic height at most $H \ge 2$, the number of pairs (γ_1, γ_2) of algebraic integers $\gamma_1, \gamma_2 \in \mathbb{Z}_K$ of logarithmic height at most H with $\gamma = \gamma_1\gamma_2$ is at most $\exp\left(O(H/\log H)\right)$, where the implied constant depends on d.*

We now derive the following generalisation of [9, Lemma 2].

Lemma 28. *Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$ of degree $d = [\mathbb{K} : \mathbb{Q}]$. Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{K}$ be finite sets with elements of logarithmic height at most H. Then we have*

$$\#(\mathcal{A}\mathcal{B}) > \exp\left(-c(d)\frac{H}{\sqrt{\log H}}\right)\#\mathcal{A}\#\mathcal{B},$$

where $c(d)$ depends only on d.

Proof. We fix some maps $\mathfrak{a}(\gamma)$ and $\mathfrak{b}(\gamma)$ (not necessary uniquely defined) that for an algebraic number $\gamma \in \mathbb{K}$ produce relatively prime ideals $\mathfrak{a}(\gamma), \mathfrak{b}(\gamma) \in \mathbb{Z}_{\mathbb{K}}$ of norm $\exp\left(O\left(\mathcal{H}(\gamma)\right)\right)$ with

$$\gamma\mathfrak{b}(\gamma) = \mathfrak{a}(\gamma).$$

We also use $\mathcal{L}_H$ to denote the set of elements of $\mathbb{K}$ of logarithmic height at most H.

Clearly if the ideals $\mathfrak{a}(\gamma) = \mathfrak{a}$ and $\mathfrak{b}(\gamma) = \mathfrak{b}$ are fixed then γ is defined up to a multiplication by a unit. Thus as in the proof of [15, Proposition 2.5] we see that for any integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ we have

$$\#\left\{\gamma \in \mathcal{L}_H \ : \ \mathfrak{a}(\gamma) = \mathfrak{a},\ \mathfrak{b}(\gamma) = \mathfrak{b}\right\} = \exp\left(O\left(H/\log H\right)\right). \tag{4}$$

Denote

$$M_1 = \exp\left(c_1(d)\frac{H}{\sqrt{\log H}}\right) \qquad \text{and} \qquad M_2 = \exp\left(c_2(d)\frac{H}{\log H}\right)$$

for certain constants $c_1(d), c_2(d) > 0$ that depend only on d.

We claim that for an appropriate choice of $c_1(d)$ and $c_2(d)$ there is a subset $\mathcal{A}_0 \subseteq \mathcal{L}_H$ of cardinality

$$\#\mathcal{A}_0 > M_2^{-2H/\log M_1}\#\mathcal{A} = \exp\left(-2\frac{H}{\sqrt{\log H}}\right)\#\mathcal{A} \tag{5}$$

and two integral ideals $\mathfrak{s}_1$ and $\mathfrak{s}_2$ such that $\mathfrak{s}_1\mathcal{A}_0 \subseteq \mathfrak{s}_2\mathcal{A}$ and for any integral ideal $\mathfrak{m}$ with $\mathrm{Nm}\left(\mathfrak{m}\right) > M_1$, we have

$$\#\left\{\gamma \in \mathcal{A}_0 \ : \ \mathfrak{m} \mid \mathfrak{a}(\gamma) \quad \text{or} \quad \mathfrak{m} \mid \mathfrak{b}(\gamma)\right\} < \frac{2}{M_2}\#\mathcal{A}. \tag{6}$$

The construction is straightforward. For a real positive R we denote

$$\mathcal{E}_R = \left\{\gamma \in \mathbb{K} \ : \ \mathrm{Nm}\ \left(\mathfrak{a}(\gamma)\mathfrak{b}(\gamma)\right) \le R\right\}.$$

Hence $\mathcal{L}_H \subseteq \mathcal{E}_R$ where

$$R = \exp\left(O\left(H\right)\right). \tag{7}$$

If $\mathcal{A}_0 = \mathcal{A}$ does not satisfy (6), there is an integral ideal $\mathfrak{m}_1 \in \mathbb{Z}$ with $\mathrm{Nm}\left(\mathfrak{m}_1\right) > M_1$ and a subset $\mathcal{A}_1 \subseteq \mathcal{E}_{R/\mathrm{Nm}\left(\mathfrak{m}_1\right)} \subseteq \mathcal{E}_{R/M_1}$ of cardinality $\#\mathcal{A}_1 \ge M_2^{-1}\#\mathcal{A}$ and such that

- either
$$\mathfrak{m}_1\mathcal{A}_1 \subseteq \mathcal{A}$$
- or
$$\mathcal{A}_1 \subseteq \mathfrak{m}_1\mathcal{A}.$$

Repeat with $\mathcal{A}$ replaced by $\mathcal{A}_1$ until, after performing k steps, we obtain a subset $\mathcal{A}_k \subseteq \mathcal{E}_{RM_1^{-k}}$ such that $\mathfrak{s}_1\mathcal{A}_k \subseteq \mathfrak{s}_2\mathcal{A}$ for some two integral ideals $\mathfrak{s}_1$ and $\mathfrak{s}_2$ and such that (6) holds with $\mathcal{A}_k$ instead of $\mathcal{A}_0$. Assuming that $\mathcal{A}_k$ is the first set with this property, we derive

$$\#\mathcal{A}_k \ge \frac{1}{M_2}\#\mathcal{A}_{k-1} \ge \ldots \ge \frac{1}{M_2^k}\#\mathcal{A}.$$

Since we obviously have $R \ge M_1^k$, we see from (7) that $k \ll H/\log M_1$ which implies (5) provided that

$$c_1(d) = \frac{1}{2}c_2(d).$$

We now use a similar argument to choose a subset $\mathcal{B}_0 \subseteq \mathcal{L}_H$ of cardinality

$$\#\mathcal{B}_0 > M_2^{-2H/\log M_1}\#\mathcal{B} > \exp\left(-2\frac{H}{\sqrt{\log H}}\right)\#\mathcal{B} \tag{8}$$

and two integral ideals $\mathfrak{t}_1$ and $\mathfrak{t}_2$ such that $\mathfrak{t}_1\mathcal{B}_0 \subseteq \mathfrak{t}_2\mathcal{B}$ and for any integral ideal $\mathfrak{m}$ with $\mathrm{Nm}\,(\mathfrak{m}) > M_1$, we have

$$\#\left\{\gamma \in \mathcal{B}_0 \ : \ \mathfrak{m} \mid \mathfrak{a}(\gamma) \quad \text{or} \quad \mathfrak{m} \mid \mathfrak{b}(\gamma)\right\} < \frac{2}{M_2}\#\mathcal{B}.$$

We now establish a lower bound on $\#\left(\mathcal{A}_0\mathcal{B}_0\right)$.

Given $\gamma \in \mathcal{L}_H$, denote

$$\mathcal{A}_0(\gamma) = \{\vartheta \in \mathcal{A}_0 \ : \ \mathrm{Nm}\ (\gcd(\mathfrak{a}(\vartheta), \mathfrak{b}(\gamma))) \le M_1, \quad \mathrm{Nm}\ (\gcd(\mathfrak{b}(\vartheta), \mathfrak{a}(\gamma))) \le M_1\}.$$

We now recall the well known bound on the divisor function

$$\tau(m) \le \exp\left((\log 2 + o(1))\frac{\log m}{\log\log m}\right) \tag{9}$$

which is also a special case of Lemma 27.

As in the proof of [9, Lemma 2], we note that the bounds (6), (9) and Lemma 26 imply that, for a sufficiently large H,

$$\#\left(\mathcal{A}_0 \backslash \mathcal{A}_0(\gamma)\right) \le \frac{2}{M_2}\#\mathcal{A}_0 \exp\left(O\left(\frac{H}{\log H}\right)\right) < \frac{1}{2}\#\mathcal{A}_0$$

for an appropriate choice of $c_2(d)$ in the definition of M_2.

Defining $\mathcal{B}_0(\gamma)$ in a similar way, we conclude that

$$\#\mathcal{A}_0(\gamma) > \frac{1}{2}\#\mathcal{A}_0 \qquad \text{and} \qquad \#\mathcal{B}_0(\gamma) > \frac{1}{2}\#\mathcal{B}_0 \tag{10}$$

for every $\gamma \in \mathcal{L}_H$.

We have

$$\#(\mathcal{A}\mathcal{B}) \geq \#(\mathcal{A}_0\mathcal{B}_0) \geq \#\left(\bigcup_{\vartheta\in\mathcal{A}_0} \{\vartheta\rho \ : \ \rho \in \mathcal{B}_0(\vartheta)\}\right).$$

Using (10) we conclude that

$$\#(\mathcal{A}\mathcal{B}) \geq \frac{1}{2L}\#\mathcal{A}_0\#\mathcal{B}_0, \tag{11}$$

where

$$L = \max_{\gamma\in\mathcal{L}_H} \#\left\{(\vartheta,\rho) \ : \ \vartheta \in \mathcal{A}_0, \ \rho \in \mathcal{B}_0(\vartheta), \ \vartheta\rho = \gamma\right\}.$$

It remains to bound L.

Since

$$\mathfrak{a}(\vartheta)\mathfrak{a}(\rho)\mathfrak{b}(\gamma) = \mathfrak{b}(\vartheta)\mathfrak{b}(\rho)\mathfrak{a}(\gamma),$$

it follows from the definition of $\mathcal{B}_0(\alpha)$ that $\mathfrak{a}(\vartheta) = \mathfrak{q}\mathfrak{m}$ for some integral ideal $(\mathfrak{q})$ dividing $\mathfrak{a}(\gamma)$ and integral ideal $\mathfrak{m}$ with $\mathrm{Nm}(\mathfrak{m}) \leq M_1$. We recall that there are $O(M_1)$ integral ideals of norm at most M_1, see [37, Proposition 7.10]. Hence by (9) and Lemma 26, there are only at most $M_1 \exp(O(H/\log H))$ possible values that can be taken by the ideal $\mathfrak{a}(\vartheta)$.

Similarly, estimates also hold for the number of possible values that can be taken by $\mathfrak{a}(\rho)$, $\mathfrak{b}(\vartheta)$ and $\mathfrak{b}(\rho)$.

We now recall that all elements $\vartheta \in \mathcal{A}_0$ satisfy $\mathfrak{s}_1\vartheta = \eta\mathfrak{s}_2$ with $\vartheta \in \mathcal{L}_H$ and fixed integral ideals $\mathfrak{s}_1$ and $\mathfrak{s}_2$. We also have a similar property for all elements $\rho \in \mathcal{B}_0(\vartheta) \subseteq \mathcal{B}_0$. Therefore, using (4), we derive

$$L \leq M_1^4 \exp\left(O\left(\frac{H}{\log H}\right)\right) \leq \exp\left(5c_1(d)\frac{H}{\sqrt{\log H}}\right), \tag{12}$$

provided that H is large enough. Substituting (12) in (11), and using (5) and (8), we conclude the proof. □

We also have a full analogue of [9, Corollary 3]

Corollary 29. *Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$ of degree $d = [\mathbb{K} : \mathbb{Q}]$. Let $\mathcal{C} \subseteq \mathbb{K}$ be a finite set with elements of logarithmic height at most $H \geq 2$. Then we have*

$$\#(\mathcal{C}^{(\nu)}) > \exp\left(-c(d,\nu)\frac{H}{\sqrt{\log H}}\right)(\#\mathcal{C})^{\nu},$$

where $c(d, \nu)$ depends only on d and ν.

2.8. **Resultant bound.** Let $\nu \ge 2$ be an integer. For integers n, m with $2 \le n, m \le \nu$, we define the $(n+m-2)\times(m-1)$ matrix $A(\nu; n, m)$ as follows:

$$\left(\begin{array}{cccccccc} \nu-n+1 & \nu-n+2 & \dots & \nu & 0 & 0 & \dots & 0 \\ 0 & \nu-n+1 & \dots & \nu-1 & \nu & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \nu-n+1 & \nu-n+2 & \dots & \dots & \nu \end{array}\right)$$

Note that each row of $A(\nu; n, m)$ contains $m-2$ zeros.

Lemma 30. *Let $2 \le n, m \le \nu$ be integers. If in the $(n+m-2)\times(n+m-2)$ matrix*

$$X(\nu; n, m) = \left(\begin{array}{c} A(\nu; n, m) \\ A(\nu; m, n) \end{array}\right)$$

we mark $n+m-2$ nonzero elements such that each row and each column contains exactly one marked element then the sum of the marked elements is always equal to

$$\sigma = (\nu-n+1)(m-1) + \nu(n-1).$$

Proof. Let

$$X(\nu; n, m) = (x_{i,j})_{1 \le i,j \le n+m-2}$$

where i indicates the row. Since the sum of the diagonal elements of $X(\nu; n, m)$ is equal to $(\nu-n+1)(m-1)+\nu(n-1)$, it suffices to prove that the sum of the marked elements does not depend on the choice of marking. To see this, we transform the matrix $X(\nu; n, m)$ into a matrix

$$Y(\nu; n, m) = (y_{i,j})_{1 \le i,j \le n+m-2}$$

as follows

- If $x_{i,j} = 0$, then we put $y_{i,j} = 0$
- If $x_{i,j} \ne 0$, then we put

$$y_{i,j} = \begin{cases} x_{i,j} + n + 2i - \nu - 1, & \text{for } 1 \le i \le m-1, \\ x_{i,j} + 2i - \nu, & \text{for } m \le i \le n+m-2. \end{cases}$$

Since the marked elements occur in each row exactly once, from this transformation of $X(\nu; n, m)$ into $Y(\nu; n, m)$ the sum of the elements

at the marked positions changes only by

$$\begin{aligned}\sigma_1 =& \sum_{i=1}^{m-1}(n+2i-\nu-1) + \sum_{i=m}^{n+m-2}(2i-\nu)\\ =&(n-1)(m-1)-\nu(n+m-2)+2\sum_{i=1}^{n+m-2} i\\ =&(n-1)(m-1)-\nu(n+m-2)+(n+m-1)(n+m-2)\end{aligned} \tag{13}$$

and in particular does not depend on the choice of the marking. Therefore, it suffices to show that the corresponding marked elements of $Y(\nu; n, m)$ does not depend on the choice of marking. But this follows from the observation that when $x_{ij} \neq 0$, we have that

$$y_{i,j} = i + j.$$

Hence, the sum of the corresponding marked elements of $Y(\nu; n, m)$ is equal to

$$\sigma_2 = 2(1 + \ldots + (n + m - 2)) = (n + m - 1)(n + m - 2)$$

and does not depend on the choice of marking. Since $\sigma_2 - \sigma_1 = \sigma$, the result now follows. □

In particular, since $n, m \leq \nu$, the sum σ of the marked elements in Lemma 30 is monotonically increasing function of m. So replacing m with ν we derive

$$\sigma \leq (\nu - n + 1)(\nu - 1) + \nu(n - 1) = \nu(\nu - 1) + n - 1 \leq \nu^2 - 1.$$

Corollary 31. *Let $M \geq 1$ and let $2 \leq n, m \leq \nu$ be fixed integers. Let $P_1(Z)$ and $P_2(Z)$ be polynomials*

$$P_1(Z) = \sum_{i=0}^{n-1} a_i Z^i \qquad \text{and} \qquad P_2(Z) = \sum_{i=0}^{m-1} b_i Z^i$$

such that

$$a_{n-1}, b_{m-1} \neq 0 \qquad \text{and} \qquad |a_i|, |b_i| < M^{\nu-i},\ i = 0, \ldots, \nu - 1.$$

Then

$$|\mathrm{Res}(P_1, P_2)| \ll M^{\nu^2-1}.$$

Proof. We recall that

$$\mathrm{Res}(P_1, P_2) = \det \begin{pmatrix} A \\ B \end{pmatrix}$$

where

$$A = \begin{pmatrix} a_{n-1} & \dots & a_1 & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_{n-1} & \dots & \dots & a_1 & a_0 \end{pmatrix},$$

and

$$B = \begin{pmatrix} b_{m-1} & \dots & b_1 & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_{m-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & b_{m-1} & \dots & \dots & b_1 & b_0 \end{pmatrix}.$$

The result now follows from the representation of the determinant by sums of products of its elements and Lemma 30. □

2.9. **Product Sets in $\mathbb{F}_p$.** We believe the results of this section can be of independent interest and have several other applications. For example, the following result in the case $\nu = 4$ solves an open problem from [18].

Lemma 32. *Let $\nu \ge 1$ be a fixed integer, $\lambda \not\equiv 0 \pmod p$. Assume that for some sufficiently large positive integer h and prime p we have*

$$h < p^{1/\max\{\nu^2-1,1\}}.$$

Then for any $s \in \mathbb{F}_p$ for the number $J_\nu(\lambda; h)$ of solutions of the congruence

$$(x_1 + s) \dots (x_\nu + s) \equiv \lambda \pmod p, \quad 1 \le x_1, \dots, x_\nu \le h,$$

we have the bound

$$J_\nu(\lambda; h) < \exp\left(c(\nu)\frac{\log h}{\log\log h}\right),$$

where $c(\nu)$ depends only on ν.

Proof. We note that for $\nu = 1$ the result it trivial and we prove it for $\nu \ge 2$ by induction on ν.

Let $\varepsilon < 1$ be a sufficiently small positive number, to be chosen later. We split the interval $[1, h]$ into $\lceil 1/\varepsilon \rceil$ intervals of length at most εh. Then for some collection $\mathcal{I}_1, \dots, \mathcal{I}_\nu$ of these intervals, we have the bound

$$J_\nu(\lambda; h) \le \lceil 1/\varepsilon \rceil^\nu J^*, \tag{14}$$

where J^* is the number of solutions of the congruence

$$(x_1 + s) \dots (x_\nu + s) \equiv \lambda \pmod p, \quad x_1 \in \mathcal{I}_1, \dots, x_\nu \in \mathcal{I}_\nu. \tag{15}$$

Thus, it suffices to prove the desired bound for J^*.

We can assume that $J^* > \nu!$. In particular, we can fix two solutions $(x_1, \dots, x_\nu) = (a_1, \dots, a_\nu)$ and $(x_1, \dots, x_\nu) = (b_1, \dots, b_\nu)$ of (15) such that the polynomial

$$P_0(Z) = (a_1 + Z) \dots (a_\nu + Z) - (b_1 + Z) \dots (b_\nu + Z)$$

is not a zero polynomial. Since $1 \le a_i, b_i \le h$, this implies that $P_0(Z)$ is not a zero polynomial modulo p. In particular, $P_0(Z)$ is not a constant polynomial.

We note that by the induction hypothesis, the set $(x_1, \dots, x_\nu)$ of solutions of the congruence (15) for which $x_i \in \{b_1, \dots, b_\nu\}$ for some i, contributes to J^* at most

$$\nu^2 \exp\left(c(\nu-1)\frac{\log h}{\log\log h}\right) \le \exp\left(0.5c(\nu)\frac{\log h}{\log\log h}\right), \tag{16}$$

provided that h is large enough (and $c(\nu) > 2c(\nu-1)$).

Consider now the set of polynomials of the form

$$P(Z) = (x_1 + Z) \dots (x_\nu + Z) - (b_1 + Z) \dots (b_\nu + Z),$$

where $(x_1, \dots, x_\nu)$ runs through the set of all solutions of the congruence (15) such that

$$\{x_1, \dots, x_\nu\} \cap \{b_1, \dots, b_\nu\} = \emptyset.$$

We note that each such polynomial $P(Z)$ is nonzero and has a form

$$P(Z) = c_1 Z^{\nu-1} + \dots + c_{\nu-1} Z + c_\nu,$$

with $|c_i| \le c_0(\nu)\varepsilon h^i$, $i = 1, \dots, \nu$, where $c_0(\nu)$ depends only on ν. In particular, since $P(s) \equiv 0 \pmod p$, it follows that $P(Z)$ is not a constant polynomial.

Since we have $P(s) \equiv P_0(s) \equiv 0 \pmod p$, we see that their resultant $\mathrm{Res}(P, P_0)$ satisfies

$$\mathrm{Res}(P, P_0) \equiv 0 \pmod p. \tag{17}$$

On the other hand, from Corollary 31, we have that

$$|\mathrm{Res}(P, P_0)| \le C_0(\nu)\varepsilon h^{\nu^2-1},$$

with come constant $C_0(\nu)$ that depends only on ν. Therefore, taking $\varepsilon = (C_0(\nu)+1)^{-1/(\nu^2-1)}$ we have $|\mathrm{Res}(P, P_0)| < p$, which in view of (17) implies that $\mathrm{Res}(P, P_0) = 0$.

Hence, every polynomial $P(Z)$ has a common root with $P_0(Z)$.

Let $\beta_1, \dots, \beta_{n-1}$, $n \le \nu$, be all the roots of $P_0(Z)$. For each $\beta \in \{\beta_1, \dots, \beta_{n-1}\}$ we collect together all solutions $(x_1, \dots, x_\nu)$ to (15) for

which $P(\beta) = 0$. Thus, for some $\beta \in \{\beta_1, \ldots, \beta_{n-1}\}$ we have

$$J^* \le \exp\left(0.5c(\nu)\frac{\log h}{\log\log h}\right) + (\nu-1)J^{**}, \tag{18}$$

where J^{**} is the number of solutions of the equation

$$(x_1+\beta)\ldots(x_\nu+\beta) = (b_1+\beta)\ldots(b_\nu+\beta) \tag{19}$$

with $1 \le x_i \le h$ such that $x_i \ne b_j$. This implies, in particular, that the left hand side of (19) is distinct from zero

By Lemma 25, we conclude that β is an algebraic number of logarithmic height $O(\log h)$ in an extension $\mathbb{K}$ of $\mathbb{Q}$ of degree $[\mathbb{K}:\mathbb{Q}] \le \nu$. Now we have that

$$\beta = \frac{\alpha}{q},$$

where α is an algebraic integer of height at most $O(\log h)$ and q is a positive integer $q \ll h^\nu$. From the basic properties of algebraic numbers it now follows that the numbers

$$qx_i + \alpha,\ i = 1, \ldots, \nu, \qquad \text{and} \qquad \prod_{i=1}^{\nu}(qb_i + \alpha)$$

are algebraic integers of $\mathbb{K}$ of height at most $O(\log h)$.

Therefore, we conclude that for a sufficiently large h the equation (19) has at most

$$\exp\left(C(\nu)\frac{\log h}{\log\log h}\right) \le \exp\left(0.5c(\nu)\frac{\log h}{\log\log h}\right) \tag{20}$$

solutions, where $C(\nu)$ is the implied constant of Lemma 27 and we also assume that $c(\nu) > 2C(\nu)$. Collecting (18) and (20) together and using (14), we conclude the proof. □

Corollary 33. *Let $\nu \ge 2$ be a fixed integer. Assume that for some sufficiently large positive integer h and prime p we have*

$$h < p^{1/(\nu^2-1)}.$$

For $s \in \mathbb{F}_p$ we consider the set

$$\mathcal{A} = \{x + s \ :\ 1 \le x \le h\} \subseteq \mathbb{F}_p.$$

Then

$$\#(\mathcal{A}^{(\nu)}) > \exp\left(-c(\nu)\frac{\log h}{\log\log h}\right) h^\nu,$$

where $c(\nu)$ depends only on ν.

We now obtain similar results for the set of fractions $(x+s)/(x+t)$.

Lemma 34. *Let $\nu \ge 1$ be a fixed integer. Assume that for some sufficiently large positive integer h and prime p we have*

$$h < p^{c\nu^{-4}},$$

where c is a certain absolute constant. For pairwise distinct $s, t \in \mathbb{F}_p$ we consider the set

$$\mathcal{A} = \left\{ \frac{x+s}{x+t} \ : \ 1 \le x \le h \right\} \subseteq \mathbb{F}_p.$$

Then

$$\#(\mathcal{A}^{(\nu)}) > \exp\left(-c(\nu)\frac{\log h}{\sqrt{\log\log h}}\right) h^{\nu},$$

where $c(\nu)$ depends only on ν.

Proof. We consider the collection $\mathcal{P} \subseteq \mathbb{Z}[Z_1, Z_2]$ of polynomials

$$P_{\mathbf{x},\mathbf{y}}(Z_1, Z_2) = \prod_{i=1}^{\nu}(x_i + Z_1)\prod_{j=1}^{\nu}(y_j + Z_2) - \prod_{i=1}^{\nu}(x_i + Z_2)\prod_{j=1}^{\nu}(y_j + Z_1),$$

where $\mathbf{x} = (x_1, \ldots, x_\nu)$ and $\mathbf{y} = (y_1, \ldots, y_\nu)$ are integral vectors with entries in $[0, h]$ and such that

$$P_{\mathbf{x},\mathbf{y}}(s, t) \equiv 0 \pmod p.$$

As in the proof of Lemma 32, we can assume that $\mathcal{P}$ contains non-zero polynomials.

Clearly, every $P \in \mathcal{P}$ if of degree at most $2\nu - 1$ and of logarithmic height at most $3\nu \log h$.

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

$$N \le (\nu + 1)^2 - 1$$

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

$$\mathcal{V} : \ P_1(Z_1, Z_2) = \ldots = P_N(Z_1, Z_2) = 0.$$

We claim that $f(Z_1, Z_2) = Z_1 - Z_2$ does not vanish on $\mathcal{V}$.

Indeed, if $f(Z_1, Z_2)$ vanishes on $\mathcal{V}$ then by Lemma 23 we see that there are polynomials $Q_1, \ldots, Q_N \in \mathbb{Z}[Z_1, Z_2]$ and positive integers b and r with

$$\log b \le c_0\nu^3(\nu \log h + \nu) \le 2c_0\nu^4 \log h \tag{21}$$

for some absolute constant c_0 (provided that h is large enough) and such that

$$P_1Q_1 + \ldots + P_NQ_N = b(Z_1 - Z_2)^r.$$

Substituting $(Z_1, Z_2) = (s, t)$ and using that s and t are disctinct elements of $\mathbb{F}_p$ we obtain $p \mid b$. Taking $c = 1/(2c_0 + 1)$ in the condition of the theorem, we see from (21) that this is impossible.

Hence for the set

$$\mathcal{U} = \mathcal{V} \cap [Z_1 - Z_2 \neq 0]$$

is nonempty. Applying Lemma 24 we see that it has a point (β_1, β_2) with components of logarithmic height $O(\log h)$ in an extension $\mathbb{K}$ of $\mathbb{Q}$ of degree $[\mathbb{K} : \mathbb{Q}] = O(1)$.

Let $\mathcal{I} = \{0, 1, \ldots, h\}$. Consider the maps $\Phi : \mathcal{I}^\nu \to \mathbb{F}_p$ given by

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

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

$$\Psi : \mathbf{x} = (x_1, \ldots, x_\nu) \mapsto \prod_{j=1}^{\nu} \frac{x_j + \beta_1}{x_j + \beta_2}.$$

By construction of (β_1, β_2) we have that $\Psi(\mathbf{x}) = \Psi(\mathbf{y})$ if $\Phi(\mathbf{x}) = \Phi(\mathbf{y})$. Hence

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

where $\mathrm{Im}\Psi$ is the image set of the map Ψ and

$$\mathcal{C} = \left\{ \frac{x + \beta_1}{x + \beta_2} \ : \ 1 \leq x \leq h \right\} \subseteq \mathbb{K}.$$

Using Corollary 29 derive the result. □

2.10. **Shifted Sets in Conjugacy Classes of $\mathcal{G}_e$.** We are now able to present our main technical tools.

Lemma 35. *Let α, β, δ, ζ, $\mathcal{I}$ and $\mathcal{S}$ be as in Lemma 21. For $x \in \mathbb{F}_p$ we define*

$$r(x) = \max_{A_0, A_1 \in \mathbb{F}_p} \#\{t \in \mathcal{S} \ : \ (t + \zeta^\nu x)^e \equiv A_\nu \pmod p, \ \nu = 0, 1\}.$$

Then for $e \leq p^{1-\delta}$ we have

$$\min_{x \in \mathcal{I}} r(x) \ll p^{-\xi} \#\mathcal{S},$$

where $\xi > 0$ depends only on δ.

Proof. Clearly $r(x) \leq r_0(x) + r_1(x)$, where

$$r_\nu(x) = \max_{A_\nu \in \mathbb{F}_p} \#\{t \in \mathcal{T}_\nu \ : \ (t + \zeta^\nu x) \equiv A_\nu \pmod p\}$$

and $\mathcal{T}_0$ and $\mathcal{T}_1$ are as in Lemma 21. Let $d = (p-1)/e$. We denote by χ_0 the principal character modulo p and by $\chi_1, \ldots, \chi_{d-1}$ the other characters with $\chi_j^d = \chi_0$. Then, using the orthogonality of multiplicative characters (see [30, Section 3.1]), we write

$$r_\nu(x) = \frac{1}{d} \sum_{t \in \mathcal{T}_\nu} \sum_{j=0}^{d-1} \chi_j(t + \zeta^\nu x) \overline{\chi}_j(A_\nu).$$

Thus, for $\nu = 0, 1$,

$$\sum_{x \in \mathcal{I}} r_\nu(x)^2 \leq \frac{1}{d} \sum_{j=0}^{d-1} \left| \sum_{x \in \mathcal{I}} \sum_{t_1, t_2 \in \mathcal{T}_\nu} \chi_j(\zeta^\nu x + t_1) \overline{\chi}_j(\zeta^\nu x + t_2) \right|.$$

The contribution of the principal character χ_0 is $\#\mathcal{I}(\#S)^2$. Furthermore, by Lemma 21 the contribution from any nonprincipal character is $\#\mathcal{I}(\#S)^2 p^{-\eta}$. Therefore,

$$\sum_{x \in \mathcal{I}} r_\nu(x)^2 \ll \frac{e}{p-1} \#\mathcal{I}(\#S)^2 + \#\mathcal{I}(\#S)^2 p^{-\eta}, \qquad \nu = 0, 1,$$

which concludes the proof. □

We also see that Corollary 33 yields:

Lemma 36. *Let $\delta > 0$ be fixed. Let $\mathcal{A}$ be as in Corollary 33. If $\mathcal{A} \subseteq r\mathcal{G}_e$ where $r \in \mathbb{F}_p^*$ and $e < p^\delta$ then,*

$$h = O\left(e^{c_0 \delta}\right)$$

where c_0 is some absolute constant.

Finally, we immediately derive from Lemma 34:

Lemma 37. *Let $\delta > 0$ be fixed. Let $\mathcal{A}$ be as in Lemma 34. If $\mathcal{A} \subseteq \mathcal{G}_e$ where $e < p^\delta$ then,*

$$h = O\left(e^{c_0 \delta^{1/3}}\right)$$

where c_0 is some absolute constant.

3. Main Results

3.1. **Hidden Shifted Power Problem.** Here we give deterministic and probabilistic algorithms for the Hidden Shifted Power Problem that runs in about the same time as the interpolation algorithm, but use significantly less oracle calls.

Theorem 38. *For a prime p and a positive integer $e \mid p-1$ with $e \le p^{1-\delta}$, given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in S_0$ with a known $S_0 \subseteq \mathbb{F}_p$, $\#S_0 \le e$, there is a deterministic algorithm that for any fixed $\varepsilon > 0$ makes $O(1)$ calls to the oracle $\mathcal{O}_{e,s}$ and finds s in time $e^{1+\varepsilon}(\log p)^{O(1)}$.*

Proof. Let $e = p^\rho$. First we consider the case of large e when $\rho \ge 0.65$.

We fix some integer $m \ge 3$ so that p and e satisfy the condition of Lemma 3. We now make m calls to $\mathcal{O}_{e,s}$ with $j = 1, \ldots, m$, getting $A_j = (s+j)^e$.

We now take a set S_m that consists of all elements $t \in S_0$, for which

$$(t+j)^e = A_j, \qquad j = 1, \ldots, m.$$

Thus, S_m is the set of candidates for s after m calls. To find S_m, we can test all elements $t \in S_0$. This requires the running time $e(\log p)^{O(1)}$. Clearly, there are some $a_j \in \mathbb{F}_p^*$, $j = 1, \ldots, m$, so that

$$s \in S_m \subseteq S_0 \cap \left(\bigcap_{j=1}^{m} (a_j \mathcal{G}_e - j) \right).$$

By Lemma 3 we see that $\#S_m = O(e^{m/(2m-1)})$. The second part of our algorithm is iterative which starts with the set $S = S_m$ with $s \in S$ described in the above with an appropriate choice of $m = O(1)$ so that it is of cardinality $\#S \le e^{1/2+\varepsilon}$ (which can be constructed after $O(1)$ calls), and then at each step it makes a call to $\mathcal{O}_{e,s}$ so that after its reply we get a substantially smaller set of candidates.

More precisely, denote

$$\vartheta = \frac{1}{4}\left(3 + \rho - \sqrt{1+\rho^2}\right)$$

and assume that at some stage we are given a set $S \subseteq \mathbb{F}_p$ with $s \in S$ of cardinality $p^{0.05} < \#S \le e^{1/2+\varepsilon}$. We show how to make a call to $\mathcal{O}_{e,s}$ so that after its reply we get a set of candidates of the size reduced by a small power of p.

Define α by $\#S = p^\alpha$ and note that for any

$$\beta > \frac{1}{4}\left(3 - 2\alpha - \sqrt{1+4\alpha^2}\right) \tag{22}$$

and an appropriate $\delta > 0$ the condition of Lemma 21 is satisfied so Lemma 35 applies.

Take

$$h = \left\lceil p^\beta \right\rceil$$

and for all $t \in S$ and $x \in [0, h]$ compute the pairs $((t+x)^e, (t+\zeta x)^e)$, where ζ is as in Lemma 21. We now order, for each x, the list of pairs

in the ascending order with respect to the first component and then with respect to the second component. Scanning this ordered list we find x that satisfies the bound of Lemma 35. We use this x for the next two calls to get $A = (x+s)^e$ and $B = (\zeta x + s)^e$. Then the new set of the candidates is defined as

$$T = \{t \in S \ : \ (t+x)^e = A, \ (t+\zeta x)^e = B\}.$$

Clearly, we have

$$\#T \ll \#S p^{-\xi} \tag{23}$$

for some $\xi > 0$ that depends only on α and β.

The total cost of this step is $p^{\beta+o(1)}\#S$. Since β is an arbitrary number satisfying (22), we see that it is possible to find this set in time $O\left(p^{\left(3+2\alpha-\sqrt{1+4\alpha^2}\right)/4+\eta}\right)$ for an arbitrary $\eta > 0$. Since the above exponent is a monotonically increasing function of α and $\alpha < \rho/2 + \varepsilon$ we see that the cost of each step can be made at most $p^{\vartheta+0.03}$ provided that ε is small enough.

The procedure terminates when we get the set S of candidates with $\#S \le p^{0.05}$. It is obvious that (23) implies that the procedure terminates after $O(1)$ steps and has the time compelxity $e(\log p)^{O(1)} + O\left(p^{\vartheta+0.03}\right)$. Since $\vartheta < \rho - 0.03$ for $\rho \ge 0.65$, the total complexity of the above procedure is $O(e)$.

The final part of our algorithm is also iterative which starts with the set S with $\#S \le p^{0.05}$. We take

$$h = \left\lceil e^{0.56} \right\rceil \qquad \text{and} \qquad \mathcal{I} = [0, h).$$

For $x \in \mathbb{F}_p$ we define

$$R(x) = \#\left\{(s_1, s_2) \in S \times S \ : \ s_1 \ne s_2, \ \frac{x+s_1}{x+s_2} \in \mathcal{G}_e\right\}.$$

Clearly

$$\sum_{x \in \mathcal{I}} R(x) = Q, \tag{24}$$

where

$$Q = \#\left\{(x, s, t) \in \mathcal{I} \times S \times S \ : \ s \ne t, \ \frac{x+s}{x+t} \in \mathcal{G}_e\right\}.$$

We write

$$Q = \sum_{\substack{s,t \in S \\ s \ne t}} Q(s,t), \tag{25}$$

where

$$Q(s,t) = \#\mathcal{Q}(s,t) \qquad \text{and} \qquad \mathcal{Q}(s,t) = \left\{x \in \mathcal{I} \ : \ \frac{x+s}{x+t} \in \mathcal{G}_e\right\}.$$

As in the proof of Lemma 35 we put $d = (p-1)/e$, denote by χ_0 be the principal characters modulo p and by $\chi_1, \ldots, \chi_{d-1}$ the other characters with $\chi_j^d = \chi_0$. We have

$$Q(s,t) = \frac{1}{d} \sum_{x \in \mathcal{I}} \sum_{j=0}^{d-1} \chi_j \left(\frac{x+s}{x+t}\right).$$

Using Lemma 18 we get

$$Q(s,t) \le \frac{h}{d} + O\left(p^{1/2} \log p\right).$$

The substitution in (25) and then using (24) implies

$$\sum_{x \in \mathcal{I}} R(x) \le (\#S)^2 \, h \left(\frac{e}{p-1} + O\left(\frac{p^{1/2} \log p}{h}\right)\right).$$

Therefore, we see there is $x \in \{0, \ldots, h-1\}$such that

$$R(x) \le (\#S)^2 \left(\frac{e}{p-1} + O\left(\frac{p^{1/2} \log p}{h}\right)\right). \tag{26}$$

We can consider that $\delta \le 0.05$. By the supposition on e and the choice of h we get

$$R(x) \ll (\#S)^2 \, p^{-\delta}.$$

To find the desired value of x for which (26) holds, we simply compute $(x+t)^e$ for all $x = 0, \ldots, h-1$ and $t \in S$ in time $h\#S(\log p)^{O(1)} \ll p^{0.62} \le e$.

We now use any x that satisfies (26) for the next call and get $A = (x+s)^e$. Then the new set of the candidates is defined as

$$T = \{t \in S \ : \ (x+t)^e = A\}.$$

Clearly, we have

$$\#T \ll R(x)^{1/2} + 1 \ll \#S p^{-\delta/2} + 1.$$

We now repeat the same with T instead of S and search for a new appropriate value of x.

Thus in $O(1)$ steps this procedure produces a set T of cardinality $\#T = O(1)$ with $s \in T$. Checking whether $s = t$ for every element $t \in T$ takes at most $\#T = O(1)$ calls to $\mathcal{O}_{e,s}$ with $x = -t$ with $t \in T$, until $\mathcal{O}_{e,s}$ returns zero. This completes the proof when $\rho \ge 0.65$.

Finally, to prove the result for $\rho < 0.65$, we again start the algorithm with $O(1)$ calls to produce a set S such that $s \in S$ and $\#S \leq e^{1/2+\varepsilon/4}$.

We now take

$$h = \left\lceil e^{1/2+\varepsilon/2} \right\rceil \qquad \text{and} \qquad \mathcal{I} = [0, h).$$

Next, we define $R(x), Q, Q(s,t), \mathcal{Q}(s,t)$ as in the previous case.

Denote

$$\mathcal{Q}(s,t) \times \mathcal{Q}(s,t) = \{(x,y) \ : \ x \in \mathcal{Q}(s,t),\, y \in \mathcal{Q}(s,t)\}.$$

Clearly

$$\#(\mathcal{Q}(s,t) \times \mathcal{Q}(s,t)) = Q(s,t)^2.$$

Note that if

$$\frac{(x+s)(y+s)}{(x+t)(y+t)} = 1$$

then (since $s \neq t$) for each $x \in \mathcal{Q}(s,t)$ there is at most one value of $y \in \{0, \ldots, h-1\}$. So such solutions contribute at most $Q(s,t)$ to $\mathcal{Q}(s,t) \times \mathcal{Q}(s,t)$. Thus

$$Q(s,t)^2 - Q(s,t) \leq \# \left\{ x, y \in \mathcal{I} \ : \ \frac{(x+s)(y+s)}{(x+t)(y+t)} \in \mathcal{G}_e \setminus \{1\} \right\}. \tag{27}$$

If for some $a \in \mathcal{G}_e \setminus \{1\}$, we have

$$\frac{(x+s)(y+s)}{(x+t)(y+t)} = a \tag{28}$$

then we can write (28) in the form

$$(a-1)xy + (at-s)(x+y) + (at^2 - s^2) = 0,$$

or

$$(x+u)(y+u) = v,$$

where

$$u = \frac{at-s}{a-1} \qquad \text{and} \qquad v = \frac{s^2 - at^2}{(a-1)} + u^2.$$

Since $v \in \mathbb{F}_p^*$, using Lemma 1, we see that the equation (28) has at most $h^{3/2+o(1)}p^{-1/2} + h^{o(1)}$ solutions. We now see from (27)

$$Q(s,t)^2 \leq e\left(h^{3/2+o(1)}p^{-1/2} + h^{o(1)}\right), \tag{29}$$

(here and throughout the proof we write $o(1)$ for a quantity that tends to zero provided that $e \to \infty$).

Furthermore, under the assumption that $\rho < 0.65$, taking a sufficiently small ε, we have $h \leq p^{1/3}$. Therefore the bound (29) simplifies as

$$Q(s,t) \leq e^{1/2} h^{o(1)}.$$

Therefore, the substitution in (25) and then using (24) implies

$$\sum_{x \in \mathcal{I}} R(x) \le (\#S)^2 e^{1/2} h^{o(1)}.$$

Thus, recalling the definition of h, we see there is $x \in \{0, \ldots, h-1\}$ such that

$$R(x) \le (\#S)^2 e^{1/2} h^{-1+o(1)} = (\#S)^2 e^{-\varepsilon/2+o(1)} \ll (\#S)^2 e^{-\varepsilon/3}. \tag{30}$$

To find the desired value of x for which (30) holds, we simply compute $(x+t)^e$ for all $x = 0, \ldots, h$ and $t \in S$ in time $h\#S(\log p)^{O(1)} \le e^{1+\varepsilon}(\log p)^{O(1)}$.

We now use any x that satisfies (30) for the next call and get $A = (x+s)^e$. Then the new set of the candidates is defined as

$$T = \{t \in S \ : \ (x+t)^e = A\}.$$

Clearly, we have

$$\#T \ll \#S e^{-\xi} + 1$$

for some $\xi > 0$ that depends only on ε.

We now repeat the same with T instead of S and search for a new appropriate value of x.

Thus in $O(1)$ steps this procedure produces a set T of cardinality $\#T = O(1)$ with $s \in T$. Checking whether $s = t$ for every element $t \in T$ takes at most $\#T = O(1)$ calls to $\mathcal{O}_{e,s}$ with $x = -t$ with $t \in T$, until $\mathcal{O}_{e,s}$ returns zero. This completes the proof. □

Corollary 39. *For a prime p and a positive integer $e \mid p-1$ with $e \le p^{1-\delta}$, given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_p$ and ℓ-th power nonresidues for all prime divisors $\ell \mid e$, there is a deterministic algorithm that for any fixed $\varepsilon > 0$ makes $O(1)$ calls to the oracle $\mathcal{O}_{e,s}$ and finds s in time $e^{1+\varepsilon}(\log p)^{O(1)}$.*

Proof. We make the first call to $\mathcal{O}_{e,s}$ with $x = 0$, getting $A_0 = s^e$. If $A_0 = 0$ then $s = 0$ and we are done. Now assume that $A_0 \ne 0$.

We see from Lemma 8 that we can construct the set

$$S_0 = \{t \ : \ t^e = A_0\} \tag{31}$$

of candidates for s in time $e(\log p)^{O(1)}$. Now it suffices to use Theorem 38. □

Corollary 40. *For a prime p and a positive integer $e \mid p-1$ with $e \le p^{1-\delta}$, given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_p$, there is a deterministic algorithm that for any fixed $\varepsilon > 0$ makes $O(1)$ calls to the oracle $\mathcal{O}_{e,s}$ and finds s in time $O\left(ep^{\varepsilon}\right)$.*

Proof. We can consider that $\varepsilon < 1/2$. Trivially, e can be factored in time $e^{1/2+o(1)}$. For any prime $\ell \mid e$ we take α_ℓ so that $\ell^{\alpha_\ell} \| p-1$. Denote $y = \lfloor p^\varepsilon \rfloor$. For any $x = 1, \ldots, y$ we take $\gamma_\ell(x)$ as the largest nonnegative integer $\gamma \le \alpha_\ell$ so that

$$x^{(p-1)/\ell^\gamma} \equiv 1 \pmod{p}.$$

Next, we denote

$$\gamma_\ell = \min\{\gamma_\ell(x) \ : \ 1 \le x \le y\}$$

and for any prime $\ell \mid e$ we choose $x = x(\ell)$ so that $\gamma_\ell(x) = \gamma_\ell$. Let

$$n = \prod_{\substack{\ell \mid e \\ \ell \text{ prime}}} \ell^{\gamma_\ell}.$$

We have $x^{(p-1)/n} \equiv 1 \pmod{p}$ for all $x = 1, \ldots, y$. Therefore, from Corollary 14 we deduce that $n \le (1/\varepsilon)^{c/\varepsilon}$ for some absolute constant c. The running time for finding n and all $x(\ell)$ is $p^\varepsilon (\log p)^{O(1)}$. Using Lemma 12, we find a set S_0 of candidates for s of cardinality at most e in time $e(\log p)^{O(1)} n^{O(1)}$. By Theorem 38, we find s in time $O\left(\left(e^{1+\varepsilon} + p^\varepsilon\right)(\log p)^{O(1)}\right)$. Replacing ε with $\varepsilon/2$, we get the running time

$$O\left(\left(e^{1+\varepsilon/2} + p^{\varepsilon/2}\right)(\log p)^{O(1)}\right) = O\left(e^{1+\varepsilon} + p^\varepsilon\right) = O(ep^\varepsilon)$$

as required. □

More precisely, it is easy to see that in the algorithm of Corollary 40 the number of calls to the oracle $\mathcal{O}_{e,s}$ needed to find S_0 and the running time for this step are bounded by

$$(1/\varepsilon)^{c/\varepsilon} \qquad \text{and} \qquad p^\varepsilon (\log p)^{O(1)} + e(\log p)^{O(1)} (1/\varepsilon)^{O(1/\varepsilon)},$$

respectively, where c is an absolute constant.

We note that the Extended Riemann Hypothesis implies that for the smallest ℓ-th power nonresidue modulo p is $O((\log p)^2)$ (uniformly over primes $\ell \mid p-1$), see [36, Chapter 9, Corollary 1]. Hence, we obtain:

Corollary 41. *Assuming the Extended Riemann Hypothesis, for a prime p and a positive integer $e \mid p-1$ with $e \le p^{1-\delta}$, given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_p$, there is a deterministic algorithm that for any fixed $\varepsilon > 0$ makes $O(1)$ calls to the oracle $\mathcal{O}_{e,s}$ and finds s in time $e^{1+\varepsilon}(\log p)^{O(1)}$.*

We also note that by a result of Burgess and Elliott [13] for almost all primes p the smallest primitive root is $(\log p)^{2+\varepsilon}$ for any $\varepsilon > 0$, see also [24]. Thus for almost all primes we have an unconditional version of Corollary 41.

We now present a probabilistic algorithm which is slightly more efficient in some cases.

Theorem 42. *For a prime p and a positive integer $e \mid p-1$ with $e \le p^{1-\delta}$, given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_p$, there is a probabilistic algorithm that makes in average $O(1)$ calls to the oracle $\mathcal{O}_{e,s}$ and finds s in the expected time $e(\log p)^{O(1)}$*

Proof. We again start from the first call to $\mathcal{O}_{e,s}$ with $x = 0$. Using a probabilistic algorithm, we can find the set S_0 given by (31) in the expected time $e(\log p)^{O(1)}$, see [27, Corollary 14.16]. Then we make next calls with random $x_1, \ldots, x_\nu$ where

$$\nu = \left\lfloor \frac{3 \log p}{\log(p/e)} \right\rfloor + 1.$$

For any j and any $s_1 \ne s_2$ the probability of the event

$$(x_j + s_1)/(x_j + s_2) \in \mathcal{G}_e \tag{32}$$

is at most e/p. Hence, by the choice of ν, the probability of the event $(x_j + s_1)/(x_j + s_2) \in \mathcal{G}_e$ for all j is at most $(e/p)^\nu < p^{-3}$. Next, the probability that for some $s_1 \ne s_2$ we have (32) for all j is at most $1/p$. Therefore, the random choice of $x_1, \ldots, x_\nu$ determines s with high probability. To find s we have to test elements from S_0. This can be done in time $e(\log p)^{O(1)}$, and the result follows. □

The following result is applicable to the case when e does not satisfy the restriction in Theorem 38 (namely, to $e = p^{1+o(1)}$ as $p \to \infty$).

Theorem 43. *For a prime p and a positive integer $e \mid p-1$, given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_p$, there is a deterministic algorithm that makes $O\left(\log p/(\log(p/e))\right)$ calls to the oracle $\mathcal{O}_{e,s}$ and finds s in time $p(\log p)^{O(1)}$.*

Proof. For $e \le p^{0.9}$ the result follows immediately from Theorem 38. We now assume that $e > p^{0.9}$.

Again, we fix some integer $m \ge 1$ and now make m calls to $\mathcal{O}_{e,s}$ with $j = 1, \ldots, m$, getting $A_j = (s+j)^e$. If $A_j = 0$ for some j, then $s = -j$ and we are done. Hence we can assume that $A_j \ne 0$ for $j = 1, \ldots, \mu$. Our immediate aim is to estimate the cardinality of the set S_m of candidates after m calls:

$$S_m = \{x \in \mathbb{F}_p \ : \ (x+j)^e = a_j, \ j = 1, \ldots, m\}.$$

As in the proof of Lemma 35 we put $d = (p-1)/e$, denote by χ_0 be the principal characters modulo p and by $\chi_1, \ldots, \chi_{d-1}$ the other

characters with $\chi_i^d = \chi_0$. The condition $x^e = A_j$ determines the values $\chi_i(x) = a_{i,j}$. We have

$$\#S_m = d^{-m} \sum_{i_1,\ldots,i_m=0}^{d-1} \prod_{j=1}^{m} \chi_{i_j}(x+j)\overline{a_{i_j,j}}.$$

Applying Lemma 17 we get

$$\#S_m = d^{-m}(p-m) + O(mp^{1/2}).$$

Setting

$$m = \left\lfloor \frac{\log p}{2\log(p-1)/\log e} \right\rfloor + 1,$$

we have $\#S_m \le p^{1/2+o(1)}$. We need the running time $p(\log p)^{O(1)}$ to find S_m.

Now we proceed as in the proof of Theorem 38 with

$$h = \left\lfloor \frac{p}{e} p^{1/2} (\log p)^2 \right\rfloor.$$

After the j-th call, $j \ge m$, we get the set $S = S_j$ of candidates for s. Next, we define $R(x), Q, Q(s,t), \mathcal{Q}(s,t)$ as in Theorem 38. Using (26) we get the new set $S = S_j$ of candidates for s with

$$\#S_{j+1} \le \max\left\{1, (1+o(1))(e/p)^{1/2} \#S_j\right\}.$$

Thus in $\ll \log p/(\log p/\log e)$ steps this procedure produces a set T of cardinality $\#T = O(1)$ with $s \in T$. Checking whether $s = t$ for every element $t \in T$ takes at most $\#T = O(1)$ calls to $\mathcal{O}_{e,s}$ with $x = -t$ with $t \in T$, until $\mathcal{O}_{e,s}$ returns zero. Since the time to find S_{j+1} is $(\log p)^{O(1)} h \#S_j \le p(\log p)^{O(1)}$, we obtain the desired result. □

Combining Corollary 39 and Theorem 43 we get the following result:

Corollary 44. *For a prime p and a positive integer $e \mid p-1$, given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_p$, and ℓ-th power nonresidues for all prime divisors $\ell \mid e$, there is a deterministic algorithm that for any fixed $\varepsilon > 0$ makes $O(\log p/(\log(p/e)))$ calls to the oracle $\mathcal{O}_{e,s}$ and finds s in time $e^{1+\varepsilon}(\log p)^{O(1)}$.*

3.2. **Shifted Power Identity Testing with Known t.**

Theorem 45. *For a prime p and a positive integer $e \mid p-1$ with $e \le p^{1-\delta}$ for some fixed $\delta > 0$, given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_p$ and $t \in \mathbb{F}_p$, there is a deterministic algorithm to decide whether $s = t$ in time $e^{1/4+o(1)}(\log p)^{O(1)}$ as $e \to \infty$.*

Proof. For integers a and H with $0 \le a < a + H < p$, we consider the interval $\mathcal{I} = [a+1, a+H]$ of size $H < p^{1/3}$.

Fix some integer $m \ge 1$ so that p and e satisfy the condition of Lemma 3. We put $\ell = m!$, $\ell_s = m!/(s+1)$, $s = 1, \ldots, m-1$, and $K = \lfloor H/\ell \rfloor$.

Let $\mathcal{J} = \{a + \ell, \ldots, a + \ell K\}$. Thus $\mathcal{J} \subseteq \mathcal{I}$. Let $\mathcal{A} = \mathcal{J}/\mathcal{J}$, that is,

$$\mathcal{A} = \{j_1/j_2 \ : \ j_1, j_2 \in \mathcal{J}\}.$$

By Lemma 2 we see that

$$\frac{a + \ell h}{a + \ell i} = \frac{a + \ell j}{a + \ell k}, \quad i, j, h, k \in [1, H],$$

has $H^{2+o(1)}$ solutions as $H \to \infty$. Therefore,

$$\#\mathcal{A} \ge H^{2+o(1)}. \tag{33}$$

Next we observe that

$$\mathcal{A} + s \subseteq \{(s+1)u \ : \ u \in \mathcal{I}/\mathcal{I}\},$$

since

$$\frac{a + \ell h}{a + \ell i} + s = (s+1)\frac{a + s\ell_s i + \ell_s h}{a + \ell i}.$$

and $s\ell_s i + \ell_s h \le (s+1)\ell_s K \le H$.

Clearly if $\mathcal{I} \in r\mathcal{G}_e$ then $\mathcal{A} \subseteq \mathcal{G}_e$ and $\mathcal{A} + s \subseteq (s+1)\mathcal{G}_e$. The system of equations

$$x_0 + s = x_s, \quad x_s \in (s+1)\mathcal{G}_e, \quad s = 0, \ldots, m-1,$$

has at least $\#\mathcal{A}$ solutions of the form $x_0 \in \mathcal{A}$, $x_s = x_0 + s$, $s = 1, \ldots, m$. We now set

$$H = \left\lfloor e^{1/4+\varepsilon} \right\rfloor$$

for a sufficiently small $\varepsilon > 0$. By Lemma 3 we have $\#\mathcal{A} \ll e^{(m+1)/(2m+1)}$ which, for a sufficiently large m and the above choice of H, contradicts (33). Since $\varepsilon > 0$ is arbitrary, we now complete the proof by simply choosing $\mathcal{Y} = [1, H]$ and recalling (3). □

For large values of e we can use bounds of character sums.

Theorem 46. *For a prime p and a positive integer $e \mid p-1$ with $e \le (p-1)/2$, given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_p$ and $t \in \mathbb{F}_p$, there is a deterministic algorithm to decide whether $s = t$ in time $p^{1/4+o(1)}$ as $p \to \infty$.*

Proof. We argue as in the proof of Theorem 45. Recalling (3), we see that for any multiplicative character χ of order e of $\mathbb{F}_p^*$ we have

$$\left|\sum_{y\in\mathcal{Y}}\chi(y-r)\right| = \#\mathcal{Y}.$$

We now fix a sufficiently small $\varepsilon > 0$ and take $\mathcal{Y} = \{1,\ldots,h\}$ where $h = \left\lceil p^{1/4+\varepsilon}\right\rceil$. Applying Lemma 19 with a large enough ν, we obtain a contradiction. Since $\varepsilon > 0$ is arbitrary, the result now follows. □

Collecting the results of Theorems 45 and 46, we obtain an algorithm of complexity $e^{1/4}p^{o(1)}$ for any $e \le (p-1)/2$.

For small values of e we can use Lemma 36 to derive the following result:

Theorem 47. *For a prime p and a positive integer $e \mid p-1$ with $e \le p^{\delta}$ for some fixed $\delta > 0$, given an oracle $\mathcal{O}_{e,s}$ for some unknown $s \in \mathbb{F}_p$ and $t \in \mathbb{F}_p$, there is a deterministic algorithm to decide whether $s = t$ in time $e^{c_0\delta}(\log p)^{O(1)}$, where c_0 is some absolute constant.*

For $e \mid p-1$ with $e \le (p-1)/2$ we define $N(e)$ as the largest H such that for some $x \in \mathbb{F}_p$ and $r \in \mathbb{F}_p^*$ we have $x+1,\ldots,x+H \in r\mathcal{G}_e$. We see from the proofs of Theorems 45 and 46 that

$$N(e) \le e^{1/4+o(1)} \tag{34}$$

as $e \to \infty$.

Lemma 36 gives the following improvement of (34) for small e. If $e \le p^{\delta}$ then

$$N(e) = O\left(e^{c_0\delta}\right). \tag{35}$$

In particular,

$$N(e) = e^{o(1)}$$

as $e = p^{o(1)}$ and $e \to \infty$.

3.3. **Shifted Power Identity Testing with Unknown t.** For large values of e we have the following simple result.

Theorem 48. *For a prime p and a positive integer $e \mid p-1$ with $e \le (p-1)/2$, given two oracles $\mathcal{O}_{e,s}$ and $\mathcal{O}_{e,t}$ for some unknown $s,t \in \mathbb{F}_p$, there is a deterministic algorithm to decide whether $s = t$ in time $p^{1/2+o(1)}$.*

Proof. We note that by Lemma 17, if $s \ne t$ then for $h = \left\lceil p^{1/2}(\log p)^2\right\rceil$ and sufficiently large p, the condition (1) fails for at least one $x = 1,\ldots,h$. The algorithm is now immediate. □

For $e \le p^{3/4}$ we have a stronger result.

Theorem 49. *For a prime p and a positive integer $e \mid p-1$ with $e \le (p-1)/2$, given two oracles $\mathcal{O}_{e,s}$ and $\mathcal{O}_{e,t}$ for some unknown $s, t \in \mathbb{F}_p$, there is a deterministic algorithm to decide whether $s = t$ in time $\max\{e^{1/2}p^{o(1)}, e^2p^{-1+o(1)}\}$.*

Proof. We fix some integer h and assume that (1) holds for every $x \in \{0, \ldots, h\}$ and $s \ne t$.

Then there are $(h+1)^2$ values of $x, y \in \{0, \ldots, h\}$ we have

$$\frac{(x+s)(y+s)}{(x+t)(y+t)} \in \mathcal{G}_e.$$

On the other hand, as we have shown in the proof of Theorem 38 (see the bound (29)), there are at most $e(h^{3/2+o(1)}p^{-1/2} + h^{o(1)})$ such pairs (x, y).

Thus, fixing an arbitrary $\varepsilon > 0$ and taking

$$h = \max\{e^{1/2}p^{\varepsilon}, e^2p^{-1+\varepsilon}\},$$

we see that (1) cannot hold for every $x \in \{0, \ldots, h\}$ unless $s = t$. Since $\varepsilon > 0$ is arbitrary, the result follows. □

Combining Theorems 48 and 49, we obtain an algorithm of complexity

$$T_p(e) = p^{o(1)} \begin{cases} e^{1/2} & \text{if } e < p^{2/3}, \\ e^2p^{-1} & \text{if } p^{2/3} \le e < p^{3/4}, \\ p^{1/2} & \text{if } p^{3/4} \le e \le (p-1)/2. \end{cases}$$

In particular, $T_p(e) \le e^{2/3}p^{o(1)}$ for any $e \le (p-1)/2$.

For small values of e we can use Lemma 37 to derive the following result:

Theorem 50. *For a prime p and a positive integer $e \mid p-1$ with $e \le p^{\delta}$ for some fixed $\delta > 0$, given two oracles $\mathcal{O}_{e,s}$ and $\mathcal{O}_{e,t}$ for some unknown $s, t \in \mathbb{F}_p$, there is a deterministic algorithm to decide whether $s = t$ in time $e^{c_0\delta^{1/3}}(\log p)^{O(1)}$, where c_0 is some absolute constant.*

In particular, we see from Theorem 50 that if $e = p^{o(1)}$ and $e \to \infty$ then we can test whether $s = t$ in time $e^{o(1)}(\log p)^{O(1)}$ in $e^{o(1)}$ oracle calls.

4. Comments and Open Questions

Probably the most challenging question is to design a deterministic algorithm for the Hidden Shifted Power Problem which is faster than interpolation.

We note that the constants in Lemmas 36 and 37 and the bound (35), can easily be made explicit. It is a natural question to obtain good numerical values for these constants and thus fully explicit versions of Theorem 47 and 49.

As we have mentioned, Lemma 32 solves an open problem from [18]. Furthermore, the arguments used in the proof of Lemmas 32 and 34 can be used for several other problems. They can also be used to generalise and improve some of the results of [11] about intersections of intervals and subgroups of $\mathbb{F}_p^*$.

We have proven that for any $e \le (p-1)/2$ the minimal number of calls to oracle $\mathcal{O}_{e,s}$ to find s is $p^{o(1)}$. However, one can study a more general problem. Let $\mathcal{A} \subseteq \mathbb{F}_p$. We define $\mathcal{O}_{\mathcal{A},s}$ as an oracle that on every input $x \in \mathbb{F}_p$ outputs 1 is $x + s \in \mathcal{A}$ and 0 otherwise, where s is a "hidden" element $s \in \mathbb{F}_p$.

Open Question 51. *Is it true that for any fixed $\delta \in (0, 1/2)$ and for any set $\mathcal{A} \subseteq \mathbb{F}_p$ with $\delta p \le \#A \le (1-\delta)p$ there is a deterministic algorithm that finds s after $p^{o(1)}$ calls (or even $O(\log p)$ calls) to the oracle $\mathcal{O}_{\mathcal{A},s}$ as $p \to \infty$?*

It is also important for applications to pairing based cryptography to extend our results to arbitrary finite fields. We note that analogues of some of the results we have used are also known for arbitrary finite fields. For example, versions of Lemma 19 has recently been obtained for arbitrary finite fields, see [16, 17, 32]. Lemmas 16, 17 and 18 can also be easily extended to arbitrary fields. However analogues of many other results, such as Lemmas 1, 3 and 21 are not known for arbitrary finite fields.

As we have mentioned, there are efficient quantum algorithms to solve the Hidden Shifted Power Problem. However they require a *quantum* oracle $\mathcal{O}_{e,s}$. It is certainly natural to investigate how much speed-up quantum algorithms can provide in the case of a *classically* given oracle $\mathcal{O}_{e,s}$ (that is, as in all results of this work).

Finally, it is also interesting to consider similar problems in the case when the "noisy" oracles, which, with a certain probability, for a given input does not return any answer or even may return a wrong answer.

Acknowledgement

The authors would like to thank Alfred Menezes for drawing out attention to this problem, to Luis Pardo for discussions of the arithmetic Nullstellensatz and to Lajos Rónyai for fruitful discussions of the algorithm of Lemma 8.

The idea of this work started while the third author was visiting the University of Waterloo whose hospitality and perfect working conditions are gratefully appreciated.

The research of J. B. was partially supported by National Science Foundation Grant DMS-0808042, that of S. K. by Russian Fund for Basic Research Grant N. 11-01-00329 and that of I. S. by Australian Research Council Grant DP1092835.

References

[1] M. Anshel and D. Goldfeld, 'Zeta functions, one-way functions, and pseudorandom number generators', *Duke Math. J.*, **88** (1997), 371–390.

[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.

[3] E. Bach and J. Shallit, *Algorithmic number theory*, MIT Press, 1996.

[4] M. Beecken, J. Mittmann and N. Saxena, 'Algebraic independence and blackbox identity testing', *Electronic Coll. on Comput. Compl.*, Report No. 22, (2011), 1–32.

[5] D. Boneh and R. Lipton, 'Algorithms for black-box fields and their applications to cryptography', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** (1996), 283–297.

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

[7] E. Bombieri, J. Bourgain and S. V. Konyagin, 'Roots of polynomials in subgroups of $\mathbb{F}_p^*$ and applications to congruences', *Int. Math. Res. Notices*, **2009** (2009), Art. ID rnn 802, 1–33.

[8] J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, 'On the divisibility of Fermat quotients', *Michigan Math. J.*, **59** (2010), 313–328.

[9] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Research Notices*, **2008** (2008), Article ID rnn090, 1–29.

[10] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Corrigenda to: Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Research Notices*, **2009** (2009), 3146–3147.

[11] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Distribution of elements of cosets of small subgroups and applications', *Intern. Math. Research Notices*, (to appear).

[12] J. Bourgain, S. Konyagin, C. Pomerance and I. E. Shparlinski, 'On the smallest pseudopower', *Acta Arith.*, **140** (2009), 43–55.

[13] D. A. Burgess and P. D. T. A. Elliott, 'The average of the least primitive root, *Mathematika*, **15** (1968), 39–50.

[14] R. J. Burthe, 'Upper bounds for least witnesses and generating sets', *Acta Arith.*, **80** (1997), 311–326.

[15] M.-C. Chang, 'Factorization in generalized arithmetic progressions and applications to the Erdős-Szemerédi sum-product problems', *Geom. Funct. Anal.*, **13** (2003), 720–736.
[16] M.-C. Chang, 'On a question of Davenport and Lewis and new character sum bounds in finite fields', *Duke Math. J.*, **145** (2008), 409–442.
[17] M.-C. Chang, 'Burgess inequality in $\mathbb{F}_{p^2}$', *Geom. and Func. Anal.*, **19** (2009), 1001–1016.
[18] J. Cilleruelo and M. Z. Garaev, 'Concentration of points on two and three dimensional modular hyperbolas and applications', *Geom. and Func. Anal.*, **21** (2011), 892–904.
[19] J. Cilleruelo, I. E. Shparlinski and A. Zumalacárregui, 'Isomorphism classes of elliptic curves over a finite field in some thin families', *Preprint*, 2011, 1–12.
[20] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, Springer-Verlag, Berlin, 2005.
[21] W. van Dam, 'Quantum algorithms for weighing matrices and quadratic residues', *Algorithmica*, **34** (2002), 413–428.
[22] W. van Dam, S. Hallgren and L. Ip, 'Quantum algorithms for some hidden shift problems', *SIAM J. Comp.*, **6** (2006), 763–778.
[23] I. B. Damgård, 'On the randomness of Legendre and Jacobi sequences', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **403** (1990), 163–172.
[24] P. D. T. A. Elliott and L. Murata, 'On the average of the least primitive root modulo p.', *J. London Math. Soc.* **56** (1997), , 435–454.
[25] M. Z. Garaev and V. Garcia, 'The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications', *J. Number Theory*, **128** (2008), 2520–2537.
[26] A. Garcia and J. F. Voloch, 'Fermat curves over finite fields', *J. Number Theory*, **30** (1988), 345–356.
[27] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, 2003.
[28] A. Hildebrand and G. Tenenbaum, 'Integers without large prime factors', *J. Théorie des Nombres de Bordeaux*, **5** (1993), 411–484.
[29] J. Hoffstein and D. Lieman, 'The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher', *Proc. Workshop on Cryptography and Computational Number Theory, Singapore 1999*, Birkhäuser, 2001, 59–68.
[30] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.
[31] N. Koblitz and A. Menezes, 'Pairing-based cryptography at high security levels', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **3796** (2005), 13–36.
[32] S. V. Konyagin, 'Estimates of character sums in finite fields', *Matem. Zametki*, **88** (2010), 529–542 (in Russian).
[33] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.
[34] T. Krick, L. M. Pardo, and M. Sombra, 'Sharp estimates for the arithmetic Nullstellensatz', *Duke Math. J.*, **109** (2001), 521–598.
[35] W.-C. W. Li, *Number theory with applications*, World Scientific, Singapore, 1996.
[36] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, Amer. Math. Soc., Providence, RI, 1994.

[37] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Polish Sci. Publ., Warszawa, 1990.
[38] A. C. Russell and I. E. Shparlinski, 'Classical and quantum algorithms for function reconstruction via character evaluation', *J. Compl.*, **20** (2004), 404–422.
[39] A. Ostafe and I. E. Shparlinski, 'Pseudorandomness and dynamics of Fermat quotients', *SIAM J. Discr. Math.*, **25** (2011), 50–71.
[40] I. D. Shkredov and I. V. Vyugin, 'On additive shifts of multiplicative subgroups', *Preprint*, 2011 (available from `http://arxiv.org/abs/1102.1172`).
[41] I. E. Shparlinski, 'On the value set of Fermat quotients', *Proc. Amer. Math. Soc.*, **140** (2012), 1199–1206.
[42] I. E. Shparlinski, 'On vanishing Fermat quotients and a bound of the Ihara sum', *Preprint*, 2011.
[43] F. Vercauteren, 'Hidden root problem', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **5209** (2008), 89–99.
[44] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974.

Institute for Advanced Study, Princeton, NJ 08540, USA
E-mail address: `bourgain@ias.edu`

Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México
E-mail address: `garaev@matmor.unam.mx`

Steklov Mathematical Institute, 8, Gubkin Street, Moscow, 119991, Russia
E-mail address: `konyagin@mi.ras.ru`

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: `igor.shparlinski@mq.edu.au`