Irreducibility and deterministic r-th root finding over finite fields

Vishwas Bhargava*
CSE, IIT Kanpur, India
Kanpur
vishwas1384@gmail.com

Gábor Ivanyos
MTA SZTAKI, Hungary
Budapest
Gabor.Ivanyos@sztaki.hu

Rajat Mittal
IIT Kanpur
rmittal@iitk.ac.in

Nitin Saxena
IIT Kanpur
nitin@cse.iitk.ac.in

ABSTRACT

Constructing r-th nonresidue over a finite field is a fundamental computational problem. A related problem is to construct an irreducible polynomial of degree r^e (where r is a prime) over a given finite field $\mathbb{F}_q$ of characteristic p (equivalently, constructing the bigger field $\mathbb{F}_{q^{r^e}}$). Both these problems have famous randomized algorithms but the derandomization is an open question. We give some new connections between these two problems and their variants.

In 1897, Stickelberger proved that if a polynomial has an odd number of even degree factors, then its discriminant is a quadratic nonresidue in the field. We give an extension of Stickelberger's Lemma; we construct r-th nonresidues from a polynomial f for which there is a d, such that, $r|d$ and $r \nmid \#$(irreducible factors of $f(x)$ of degree d). Our theorem has the following interesting consequences: (1) we can construct $\mathbb{F}_{q^m}$ in deterministic poly(deg(f), $m \log q$)-time if m is an r-power and f is known; (2) we can find r-th roots in $\mathbb{F}_{p^m}$ in deterministic poly($m \log p$)-time if r is constant and $r|\gcd(m, p-1)$.

We also discuss a conjecture significantly weaker than the Generalized Riemann hypothesis to get a deterministic poly-time algorithm for r-th root finding.

CCS CONCEPTS

•**Theory of computation → Algebraic complexity theory; Pseudorandomness and derandomization;** *Problems, reductions and completeness;*

ACM Reference format:
Vishwas Bhargava, Gábor Ivanyos, Rajat Mittal, and Nitin Saxena. 2017. Irreducibility and deterministic r-th root finding over finite fields . In *Proceedings of ISSAC '17, Kaiserslautern, Germany, July 25-28, 2017,* 8 pages.
DOI: 10.1145/3087604.3087620

*Visiting Scholar, Centre for Quantum Technologies, NUS, Singapore

ISSAC '17, Kaiserslautern, Germany

DOI: 10.1145/3087604.3087620

1 INTRODUCTION

The problem of finding r-th roots in a finite field, say $\mathbb{F}_q$, is to solve $x^r = a$ given an r-th residue $a \in \mathbb{F}_q{}^*$. Note that, without loss of generality, we can assume r to be prime, otherwise for $r = r_1 \cdot r_2$, we can solve the problem iteratively by first solving $x^{r_1} = a$ and then solving $y^{r_2} = x$. Moreover, we can assume $r|(q-1)$, otherwise $x = a^{r^{-1} \bmod (q-1)}$ is an easy solution.

It can be shown that $x^r = a$ has a solution iff $a^{\frac{q-1}{r}} = 1$. If $a^{\frac{q-1}{r}} \neq 1$ then we call a an *r-th nonresidue*. Interestingly, the problem of finding an r-th nonresidue is *equivalent* to that of finding r-th roots in $\mathbb{F}_q$ [2, 22, 30]. This gives a randomized poly-time algorithm for finding r-th roots and, thus, solves the problem for practical applications. Also, assuming Generalized Riemann hypothesis (GRH) there is a deterministic poly-time algorithm for finding r-th nonresidue in any finite field [3, 5, 8, 13]. For a detailed survey, see [6, Chap. 7].

The special case of $r = 2$ is particularly well studied. The problem now is to find square-roots in $\mathbb{F}_q$, which is equivalent to finding a *quadratic nonresidue* in $\mathbb{F}_q$. For this problem, apart from Tonelli-Shanks algorithm [30], there are other randomized algorithms as well – Cipolla's algorithm [10], singular elliptic curves based algorithm [19], etc. There are also deterministic solutions for some special cases:

- Schoof [21] gave an algorithm using point counting on elliptic curves having complex-multiplication to find square-roots of *fixed* numbers over prime fields.
- Sze [29] gave an algorithm to take square-roots over $\mathbb{F}_q$, when $q - 1 = r^e t$ and $r + t = \text{poly}(\log p)$.

However, computing square-roots over finite fields in deterministic polynomial time is still an open problem. The best known deterministic complexity for this problem is exponential, namely, $\tilde{O}(p^{1/4\sqrt{e}})$; which is also a bound on the least quadratic nonresidue [9]. The distribution of quadratic nonresidues in a finite field is still mostly a mystery; it relates to some interesting properties of the zeta function, see Thm. 6.7.

In 1897, L. Stickelberger [27] proved that if p is a prime, K is an algebraic number field of degree n of discriminant D, and integer ring O_K where the ideal (p) factorizes as $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \ldots \mathfrak{p}_s$ into distinct prime ideals then

$$\left(\frac{D}{p}\right) = (-1)^{n-s} \qquad \text{Stickelberger's Lemma .} \tag{1}$$

Equivalently, if the number of even degree irreducible factors of a squarefree $f(x) \mod p$ are odd, then the discriminant of f will be a quadratic nonresidue in $\mathbb{F}_p$. Swan [28] and Dalen [11] gave alternative proofs of Stickelberger lemma. Stickelberger lemma is used in factorization of polynomials over finite fields and in constructing irreducible polynomials of a given degree over finite fields [12, 28, 32].

We generalize this idea of constructing quadratic nonresidues from Stickelberger's lemma to constructing r-th nonresidues from "special", possibly reducible, polynomials. Formally, these "special" polynomials are over $\mathbb{F}_q$ and satisfy the following factorization pattern,

Property 1.1. Let r be a prime and $f(x) \in \mathbb{F}_q[x]$ be a squarefree polynomial. f satisfies *Stickelberger property* with respect to r, if $\exists d$, such that, $r|d$ and $r \nmid \#\Big(\text{irreducible factors of } f(x) \text{ of degree } d\Big)$.

Our goal is to show that the construction of such a, possibly reducible, polynomial solves many of the open problems. It is somewhat surprising that a reducible polynomial be related so strongly to non-residuosity and irreducibility.

Our first main result relates Property 1.1 to the construction of r-th nonresidues in *any* field above $\mathbb{F}_p$ (equivalently, finding r-th roots there). We will denote a *primitive* r-th root of unity by ζ_r.

Theorem 1.2. *Given $\zeta_r \in \mathbb{F}_q$ and any polynomial f satisfying Property 1.1, we can find r-th roots in* any *finite field $\mathbb{F}_{q'}$ of characteristic p, in deterministic poly$(\deg(f), \log qq')$-time.*

We get a stronger result in the case when we have $\mathbb{F}_{p^r}$ available and $r = O(1)$. Even $r = 2$ is an interesting special case.

Corollary 1.3. *We can find r-th roots in $\mathbb{F}_{p^m}$ in deterministic poly$(m \log p)$-time if r is constant and $r| \gcd(m, p-1)$.*

Remark: In the proof of Corollary 1.3, we will use the fact that we have an irreducible polynomial of degree m over $\mathbb{F}_p$, see section 2.

Finding an r-th nonresidue a in $\mathbb{F}_q$ suffices to construct an extension $\mathbb{F}_{q^r}$. For example, we have $\mathbb{F}_q[a^{1/r}] \cong \mathbb{F}_{q^r}$; equivalently, $X^r - a$ is an irreducible polynomial. However, it is not clear how to find r-th nonresidue given $\mathbb{F}_{q^r}$. Anyways, the question of constructing $\mathbb{F}_{q^r}$ efficiently is of great interest [1, 24, 25] and still open.

Our second main result relates Property 1.1 to the construction of an irreducible polynomial of degree m, where m is *any* r-power. We are able to remove the dependence on ζ_r in this case.

Theorem 1.4. *Given a polynomial satisfying Property 1.1, we can construct the field $\mathbb{F}_{q^m}$, for any r-power m, in deterministic poly$(\deg(f), m \log q)$-time.*

Note that, if we are given fields $\mathbb{F}_{q^{m_1}}$ and $\mathbb{F}_{q^{m_2}}$ (for coprime m_1, m_2), we can combine them to get the field $\mathbb{F}_{q^{m_1 m_2}}$ [23, Lem. 3.4]. Hence, it is sufficient to be able to construct fields whose sizes are prime powers.

Organization of the paper

In this paper, the main results and ideas are presented in Sec. 3. Sec. 2 has notation and preliminaries. For concreteness, Sec. 4 sketches our algorithm for finding an r-th nonresidue in any finite field, given a polynomial (in $\mathbb{F}_p[x]$) satisfying Property 1.1. We discuss some special cases of our analysis in Sec. 5.

In Sec. 6, we discuss few conjectures; particularly in Sec. 6.2 we introduce a strictly weaker version of Generalized Riemann hypothesis to get poly-time algorithms for finding nonresidues over finite fields.

2 PRELIMINARIES

We are going to work in the finite field $\mathbb{F}_q$, where $q = p^d$ for some prime p. We will assume that $\mathbb{F}_q$ is specified by a degree d irreducible polynomial over $\mathbb{F}_p$. This can be assumed without loss of generality, see [15, Thm. 1.1].

Given a finite field $\mathbb{F}_q$ and its extension $\mathbb{F}_{q^k}$, the multiplicative *norm* of an element $\alpha \in \mathbb{F}_{q^k}$ is defined as,

$$N(\alpha) = N_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha) = \alpha^{\frac{q^k-1}{q-1}}.$$

The following properties of finite fields will be useful (for proofs refer standard texts, eg. [16]).

Theorem 2.1 (Finite fields). *Given a finite field $\mathbb{F}_q$ with characteristic p and algebraic closure $\overline{\mathbb{F}}_p$,*

- *For any $a \in \overline{\mathbb{F}}_p$, $a^q = a$ if and only if $a \in \mathbb{F}_q$.*
- *For any $a, b \in \mathbb{F}_q$, $(a+b)^p = a^p + b^p$.*
- *The multiplicative group $\mathbb{F}_q^*$ is cyclic.*
- *Any polynomial $f \in \mathbb{F}_q[x]$ of degree k has at most k roots in $\mathbb{F}_q$. The notation $\mathcal{Z}(f)$ will be used to denote the set of $\overline{\mathbb{F}}_q$-zeros of polynomial $f(x)$.*

We are interested in finding r-th nonresidue in $\mathbb{F}_q$ for a prime r. An element $a \in \mathbb{F}_q$ is called an r-th nonresidue iff $x^r = a$ has no roots in $\mathbb{F}_q$. This possibility is there only if $r|(q-1)$. In that case, a is an r-th nonresidue iff $a^{\frac{q-1}{r}} \neq 1$ [6]. Using this characterization, the following lemma constructs an r-th nonresidue in $\mathbb{F}_q$ given an r-th nonresidue in $\mathbb{F}_{q^k}$.

Lemma 2.2 (Projection). *Let r be a prime which divides $q-1$. Then, $\alpha \in \mathbb{F}_{q^k}$ is an r-th nonresidue iff $N_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha)$ is an r-th nonresidue in $\mathbb{F}_q$.*

Proof. We know that,

$$N_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha) = \prod_{i=1}^{k-1} \alpha^{q^i} = \alpha^{\frac{q^k-1}{q-1}}.$$

Also, $\alpha \in \mathbb{F}_{q^k}$ is an r-th nonresidue iff $\alpha^{\frac{q^k-1}{r}} \neq 1$.

Hence, the proof follows from the bi-implication,

$$\alpha^{\frac{q^k-1}{r}} \neq 1 \iff \left(\alpha^{\frac{q^k-1}{q-1}}\right)^{\frac{q-1}{r}} = \left(N_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha)\right)^{\frac{q-1}{r}} \neq 1.$$

□

We can define a multiplicative character, $\chi_r(a) := a^{\frac{q-1}{r}}$, of $\mathbb{F}_q^*$. Notice that $\chi_r(a) \neq 1$ iff a is an r-th nonresidue in $\mathbb{F}_q$. Multiplicativity follows from the definition, i.e.,

$$\chi_r(ab) = \chi_r(a)\chi_r(b).$$

Since $a^{q-1} = 1$, $\chi_r(a)$ is an r-th root of unity. We will denote a *primitive* r-th root of unity by ζ_r.

Since $\mathbb{F}_q^*$ is cyclic and $r \mid q-1$, we have that ζ_r exists in $\mathbb{F}_q$. Note that ζ_r^i, $i \in \mathbb{F}_r^*$, are the $(r-1)$ primitive r-th roots of unity in $\mathbb{F}_q$.

Resultant and Discriminant. One of the central algebraic tool used in our analysis is the *resultant* of two polynomials. Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ be two polynomials over a field $\mathbb{F}$.

Definition 2.3 (Resultant). The resultant of two polynomials f, g in $\mathbb{F}[x]$ is is defined as,

$$R(f,g) := a_m^m b_n^n \prod_{\substack{\alpha \in \mathcal{Z}(f) \\ \beta \in \mathcal{Z}(g)}} (\alpha - \beta) = a_m^m \prod_{\alpha \in \mathcal{Z}(f)} g(\alpha)\,.$$

So, if f is monic,

$$R(f,g) := \prod_{\alpha \in \mathcal{Z}(f)} g(\alpha)\,.$$

We will use the following properties of resultant (for proof see [16, Chap. 1]).

Lemma 2.4 (Properties of $R(\cdot)$). *Given polynomials $f, g, h \in \mathbb{F}[x]$, we have that,*

1. $R(f,g) \in \mathbb{F}$.
2. *Resultant is multiplicative,* $R(fh, g) = R(f,g) \cdot R(h,g)$.
3. *There is a nearly linear-time,* $\tilde{O}(m+n, \log^{O(1)} p)$ *algorithm to compute* $R(f,g)$. *see [6, Pg. 347].*
4. *Resultant is the determinant of* Sylvester matrix *of order* $m+n$ *[16, Chap. 1]. In fact, this determinant definition can be taken as the general definition of resultant, as it makes the resultant efficient to compute even when the base ring is not a field. Eg. there are efficient algorithms known for computing Resultant of bivariate polynomials, see [17].*

Another tool, closely related to resultant, is called the *discriminant.*

Definition 2.5 (Discriminant). The discriminant of a polynomial $f \in \mathbb{F}[x]$ with roots $\mathcal{Z}(f) = \{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ is defined by,

$$\Delta(p) := a_m^{2m-2} \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j)^2\,.$$

It is known that $\Delta(f) = (-1)^{m(m-1)/2} a_m^{-1} \cdot R(f, f')$ [16, Eqn.1.11], where f' is the formal derivative of f. Hence, $\Delta(f) \in \mathbb{F}$ and it can be computed in poly(m) field operations.

Note that although resultant (resp. discriminant) is defined in terms of the zeros of the polynomials, it can be computed without the knowledge of the zeros. This relationship between the zeros and the coefficients is very useful computationally.

3 MAIN RESULTS

We will prove the main theorems in this section. We are interested in finding r-th nonresidue in the finite field $\mathbb{F}_q$. So we will assume that $r \mid q-1$ in Sec. 3.1 and Sec. 3.2 (we will not assume $r \mid q-1$ in Sec. 3.3). Moreover, for $r = 2$ and a field of characteristic $p = 4k+3$, -1 is a quadratic non-residue, hence we can assume $4 \mid (q-1)$.

Our first step will be to construct an r-th nonresidue using an irreducible polynomial f of degree divisible by r.

3.1 From an irreducible polynomial f – Proof of Cor. 1.3

Given an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $d = rk$, define the following polynomial (inspired from *Lagrange resolvents*):

$$L_{f,r} := \sum_{i=0}^{r-1} x^{(q^k)^i} {\zeta_r}^i \mod f.$$

The following theorem finds an r-th nonresidue in $\mathbb{F}_q$ using f. A different proof of Thm. 3.1 can be found in [31, Sec. 8.5], we present our proof for completeness.

Theorem 3.1 (Irreducibility to nonresiduosity). *Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree $d = rk$ and $\gcd(2, r) \cdot r \mid q-1$. If $L_{f,r} := \sum_{i=0}^{r-1} x^{q^{k\cdot i}} {\zeta_r}^i \mod f$, then*

$$\left(L_{f,r}\right)^{\frac{q^d-1}{r}} = \zeta_r^{-1}\,.$$

This implies that $L_{f,r}$ is an r-th nonresidue in $\mathbb{F}_{q^d} = \mathbb{F}_q[x]/\langle f \rangle$. Also, $N_{\mathbb{F}_{q^d}/\mathbb{F}_q}(L_{f,r})$ is an r-th nonresidue in $\mathbb{F}_q$.

Proof. We know that $L_{f,r} \in \mathbb{F}_{q^d}$ and $\zeta_r \in \mathbb{F}_q$. Taking the q^k-th power,

$$\begin{aligned}(L_{f,r})^{q^k} &= \left(\sum_{i=0}^{r-1} x^{q^{ki}} {\zeta_r}^i\right)^{q^k} \\ &= \sum_{i=0}^{r-1} x^{q^{k\cdot(i+1)}} {\zeta_r}^i = {\zeta_r}^{-1} \cdot L_{f,r}\,.\end{aligned}$$

Using the above equation,

$$\begin{aligned}(L_{f,r})^{\frac{q^d-1}{r}} &= (L_{f,r})^{(\frac{q^d-1}{q^k-1})\cdot(\frac{q^k-1}{r})} \\ &= (L_{f,r})^{(1+q^k+q^{2k}\ldots+q^{(r-1)k})\cdot(\frac{q^k-1}{r})} \\ &= (L_{f,r} \cdot \zeta_r^{-1} L_{f,r} \cdot \zeta_r^{-2} L_{f,r} \cdots \zeta_r^{-(r-1)} L_{f,r})^{(\frac{q^k-1}{r})} \\ &= \left((L_{f,r})^r (\zeta_r^{-1})^{\binom{r}{2}}\right)^{(\frac{q^k-1}{r})}\,.\end{aligned}$$

When r is an odd prime, $(\zeta_r^{-1})^{\binom{r}{2}}$ is 1. If r is 2 then we have $4 \mid (q-1)$, thus the factor of -1 can be ignored. Simplifying,

$$\begin{aligned}(L_{f,r})^{\frac{q^d-1}{r}} &= \left((L_{f,r})^r\right)^{(\frac{q^k-1}{r})} \\ &= (L_{f,r})^{(q^k-1)} = \zeta_r^{-1}\,.\end{aligned}$$

By definition of r-th nonresidue, this implies that $L_{f,r}$ is an r-th nonresidue in $\mathbb{F}_{q^d}$. Applying Lem. 2.2, we get that $N_{\mathbb{F}_{q^d}/\mathbb{F}_q}(L_{f,r})$ is an r-th nonresidue in $\mathbb{F}_q$. □

Thm. 3.1 gives the Cor. 1.3.

Proof of Cor. 1.3. Since $\mathbb{F}_{p^m}$ is specified by an irreducible polynomial of degree m (and we know $r \mid \gcd(m, p-1)$), we get an r-th nonresidue by Thm. 3.1 if we can find ζ_r in $\mathbb{F}_p$. The latter can be done using Pila's algorithm based on arithmetic algebraic-geometry

[20, Thm. D]. Once we have an r-th nonresidue, we get an r-th root finding algorithm [22, 30]. □

Thm. 3.1 also gives us a way to construct r-th nonresidue, in $\mathbb{F}_{p^n}$ for any n, using an irreducible polynomial of degree divisible by r.

Corollary 3.2 (Any field). *Suppose we have an irreducible $f \in \mathbb{F}_q[x]$ with degree $d = rk$ and $\zeta_r \in \mathbb{F}_q$, where $\mathbb{F}_q$ has characteristic p. Then, we can find r-th nonresidue in any finite field $\mathbb{F}_{q'}$ of characteristic p (assuming $r|(q'-1)$).*

Proof. Let $\mathbb{F}_{p^m}$ be the *smallest* subfield of $\mathbb{F}_q$, with $r|(p^m-1)$. Using Thm. 3.1 & Lem. 2.2 on f, we can find an r-th nonresidue in $\mathbb{F}_{p^m}$.

Now consider the given field $\mathbb{F}_{q'}$ with, say, $p^{m\ell}$ elements (since $r|q'-1$, $\ell \in \mathbb{N}$). It has a subfield $\mathbb{F}'$ of size p^m, and so by [15, Thm. 1.2], we also get an r-th nonresidue in $\mathbb{F}'$, say a. We intend to lift this nonresidue to the bigger field $\mathbb{F}_{q'}$; to do that we consider two cases.

- Case 1: If $r \nmid \ell$ then a is an r-th nonresidue in $\mathbb{F}_{q'}$. Because,

$$a^{\frac{q'-1}{r}} = (a^{\frac{p^m-1}{r}})^{\frac{q'-1}{p^m-1}} = (\zeta_r^{-1})^{\frac{q'-1}{p^m-1}} \neq 1\,.$$

  Last inequality holds because $\frac{q'-1}{p^m-1} = \frac{p^{m\ell}-1}{p^m-1}$ is not divisible by r.
- Case 2: If $r \mid \ell$ then we have an irreducible polynomial that defines $\mathbb{F}_{p^{m\ell}}$ and on that we can apply Thm. 3.1 to get an r-th nonresidue in $\mathbb{F}_{q'}$.

□

The following lemma relates $N_{\mathbb{F}_{q^d}/\mathbb{F}_q}(g)$ to the resultant $R(f,g)$ when f is irreducible.

Lemma 3.3 (Resultant as a norm). *[6, Ex. 6.15] If f is an irreducible polynomial of degree d in $\mathbb{F}_q[x]$, then*

$$R(f,g) = N_{\mathbb{F}_{q^d}/\mathbb{F}_q}(g).$$

Proof. We know that the roots of polynomial f are $\mathcal{Z}(f) = \{\alpha, \alpha^q, \cdots, \alpha^{q^{d-1}}\}$. Using the definition of resultant,

$$\begin{aligned} R(f,g) &= \prod_{\alpha\in\mathcal{Z}(f)} g(\alpha) \\ &= \prod_{i=0}^{d-1} g(\alpha^{q^i}) \\ &= \prod_{i=0}^{d-1} g(\alpha)^{q^i} \\ &= g(\alpha)^{\sum_{i=0}^{d-1} q^i} \\ &= N_{\mathbb{F}_{q^d}/\mathbb{F}_q}(g)\,. \end{aligned}$$

□

Corollary 3.4 (Resultant of resolvent). *In the notation of Thm. 3.1, $R(L_{f,r}, f)$ is an r-th nonresidue in $\mathbb{F}_q$.*

In particular, $\chi_r(R(L_{f,r}, f)) = \zeta_r^{-1}$.

3.2 From a reducible polynomial f – Proof of Thm. 1.2

We will look at the case of reducible polynomials now. The Thm. 1.2 shows that a reducible polynomial satisfying Property 1.1 will give us an r-th nonresidue. Note that an irreducible polynomial of a degree divisible by r will trivially satisfy Property 1.1.

Proof of Thm. 1.2. By distinct degree factorization [6, Thm. 7.5.3], the polynomial f can be decomposed as $f = h_1 h_2 \cdots h_n$, s.t.,

- For all i, h_i has irreducible factors of same degree.
- For all $i \neq j$, irreducible factors of h_i and h_j have different degree.

We know that f satisfies Property 1.1. So, the distinct degree factorization guarantees a factor $h_i = f_1 f_2 \cdots f_{r'}$ of f such that,

- f_i's are irreducible of degree $d = rk$.
- $r \nmid r'$.

For convenience we shall denote $f_1 f_2 \cdots f_{r'}$ as f from now on. Define $g(x)$ to be the Lagrange resolvent inspired polynomial,

$$g(x) := \sum_{i=0}^{r-1} x^{q^{ki}} {\zeta_r}^i\,.$$

We will show that $R(f, g \bmod f)$ is an r-th nonresidue in $\mathbb{F}_q$. Here $g \bmod f$ refers to some representative in $\mathbb{F}_{q^d}[x]$. We will now show that the resultant is independent of the representative chosen.

Claim 1. Let f, g be two polynomials over any field. Then,

$$R(f, g \bmod f) = R(f,g)\,.$$

Proof. Let $g' := g \bmod f$ be a representative. Using the definition of resultant,

$$\begin{aligned} R(f,g') &= \prod_{\alpha\in\mathcal{Z}(f)} g'(\alpha) \\ &= \prod_{\alpha\in\mathcal{Z}(f)} g(\alpha) \quad [\because g'(\alpha) = g(\alpha)] \\ &= R(f,g)\,. \end{aligned}$$

□

Clm. 1 implies that,

$$R(f, g \bmod f) = R(f,g) = \prod_{i=1}^{r'} R(f_i, g) = \prod_{i=1}^{r'} R(f_i, g \bmod f_i).$$

Since χ_r is multiplicative, we have,

$$\chi_r(R(f, g \bmod f)) = \prod_{i=1}^{r'} \chi_r(R(f_i, g \bmod f_i)) = (\zeta_r^{-1})^{r'}.$$

The last step follows from Cor. 3.4 and the fact that f_i are irreducible. Since $r \nmid r'$, we get $\chi_r(R(f, g \bmod f)) \neq 1$ and hence $R(f, g \bmod f)$ is an r-th nonresidue in $\mathbb{F}_q$.

The last statement of the theorem (about fields of characteristic p) follows in the same way as in the proof of Cor. 3.2.

The time complexity is straightforward and further discussed in Sec. 4.

□

3.3 Constructing fields – Proof of Thm. 1.4

The result in the previous subsection required the existence and knowledge of ζ_r. Now we would like to eliminate both these assumptions. In particular, we will not assume that $r \mid q-1$ in this section. We will show that if we have a reducible polynomial f satisfying Property 1.1 then we can construct $\mathbb{F}_{q^r}$ (equivalently, we can construct an irreducible polynomial of degree r). The concepts that we will use are inspired from the proof of [15, Thm. 5.2].

The starting idea is to work with a "virtual" ζ_r, i.e. define the ring $\mathbb{F}_q[\zeta] := \mathbb{F}_q[Y]/\langle \varphi_r(Y)\rangle$, where $\varphi_r(Y) := \sum_{0\le i\le r-1} Y^i$. Let ζ be the residue-class of Y mod $\varphi_r(Y)$ in $\mathbb{F}_q[\zeta]$. Let e be the smallest positive integer such that $r|q^e-1$, in other words, the multiplicative order of q modulo r. Then $\varphi_r(Y)$ completely splits over $\mathbb{F}_{q^e}$ as

$$\varphi_r(Y) \;=\; \prod_{i\in\mathbb{F}_r^*} (Y-\eta^i)\,,$$

where $\eta \in \mathbb{F}_{q^e}$ is a primitive r-th root of unity, but we may not have access to η and in general not even to $\mathbb{F}_{q^e}$. So we will do computations over the *ring* $\mathbb{F}_q[\zeta]$ and try to construct the field $\mathbb{F}_{q^r}$.

Clearly, ζ has order r in the unit group $\mathbb{F}_q[\zeta]^*$. For each integer $a \in \mathbb{F}_r^*$ there is a unique ring automorphism ρ_a of $\mathbb{F}_q[\zeta]$ that fixes $\mathbb{F}_q$ and maps $\zeta \mapsto \zeta^a$. The set $\{\rho_a \mid a \in \mathbb{F}_r^*\} =: \Delta$ forms a group (under map composition) that is isomorphic to $\mathbb{F}_r^*$. If we consider the elements of the ring fixed under Δ then we get back $\mathbb{F}_q$, i.e. $\mathbb{F}_q[\zeta]^\Delta = \mathbb{F}_q$ [15, Prop. 4.1].

Like Sec. 3.2, suppose we have an $f = f_1 f_2 \cdots f_{r'} \in \mathbb{F}_q[x]$ with f_i's being irreducibles of degree $d = rk$ and $r \nmid r'$. When we move to $\mathbb{F}_{q^e}$, f_i factors into $\ell := \gcd(k,e) = \gcd(d,e)$ many irreducibles each of degree $d/\ell = kr/\gcd(k,e) =: k'r$. Since $r \nmid e$, we have that $r \nmid \ell$.

Our ring $\mathbb{F}_q[\zeta]$ is a semisimple algebra that decomposes as:

$$\mathbb{F}_q[\zeta] \;\cong \bigtimes_{i\,\in\,\mathbb{F}_r^*/\langle q\rangle} \mathbb{F}_{q^e}[Y]/\langle Y-\eta^i\rangle\,,$$

and the proof given in Sec. 3.2 holds simultaneously over each of the component fields ($\cong \mathbb{F}_{q^e}$) of $\mathbb{F}_q[\zeta]$. Hence, simply by Chinese remaindering, we get the equality:

$$R(f, g \bmod f)^{\frac{q^e-1}{r}} \;=\; \zeta^{-r'\ell}\,, \tag{2}$$

where, as expected, $g(x)$ is the following Lagrange resolvent over $\mathbb{F}_q[\zeta]$,

$$g(x) \;:=\; \sum_{i=0}^{r-1} x^{q^{ek'i}} \zeta^i\,.$$

(Also, note that we are now computing mod and resultant over the base ring $\mathbb{F}_q[\zeta]$.)

Teichmüller subgroup. Let r'' be an integer representative for $(r'\ell)^{-1} \bmod r$. Let $q^e - 1 = ur^t$ such that $r \nmid u$ and $t \ge 1$. Define $\delta := R(f, g \bmod f)^{ur''}$. Then, by Eqn.2, we have $\delta^{r^{t-1}} = \zeta^{-1}$. In particular, δ has order r^t in $\mathbb{F}_q[\zeta]^*$. Define a function ω that maps any integer a to $a^{r^{t-1}} \bmod r^t$. Note that, by binomial expansion, $(a+r)^{r^{t-1}} \equiv a^{r^{t-1}} \bmod r^t$. In other words, value of $\omega(a)$ only depends on $a \bmod r$. Now we come to the key definition, inspired from [15],

$$c \;:=\; \left(\prod_{a\in[r-1]} \rho_a^{-1}\left(\delta^{\omega(a)}\right)\right).$$

The following properties can be easily verified:

- $c^{r^{t-1}} = \zeta$,
- c has order r^t in $\mathbb{F}_q[\zeta]^*$, and
- for all $\rho_b \in \Delta$, $\rho_b(c) = c^{\omega(b)}$.

At this point recall the definition of *Teichmüller subgroup* w.r.t. $\mathbb{F}_q$:

$$T_{\mathbb{F}_q} \;:=\; \Big\{\epsilon \in \mathbb{F}_q[\zeta]^* \;\mid \epsilon \text{ has } r\text{-power order, and } \forall \rho_a \in \Delta,\ \rho_a(\epsilon) = \epsilon^{\omega(a)}\Big\}\,.$$

By the properties above and invoking [15, Thm. 5.1], we can deduce that c is a generator of $T_{\mathbb{F}_q}$.

Consider the extension ring $\mathbb{F}_q[\zeta][c^{1/r}] := \mathbb{F}_q[\zeta][X]/\langle X^r - c\rangle$, where $c^{1/r}$ is the residue class of X mod $X^r - c$ in the ring. By [15, Prop. 4.3] we have: $\forall b \in \mathbb{F}_r^*$, ρ_b extends uniquely to a ring automorphism of $\mathbb{F}_q[\zeta][c^{1/r}]$ such that $c^{1/r} \mapsto (c^{1/r})^{\omega(b)}$. Thus, Δ can now be seen as a *group of ring automorphisms* of $\mathbb{F}_q[\zeta][c^{1/r}]$.

Now we have the following nice way to construct a field extension.

Theorem 3.5 (Field extension). *The fixed subring $\mathbb{F}_q[\zeta][c^{1/r}]^\Delta$ is isomorphic to $\mathbb{F}_{q^r}$. Moreover, given f satisfying property 1.1, $\mathbb{F}_{q^r}$ can be constructed in deterministic poly$(\deg(f), r\log q)$-time.*

Proof. It directly follows from [15, Thm. 5.1] that $\mathbb{F}_q[\zeta][c^{1/r}]^\Delta \cong \mathbb{F}_{q^r}$.

From the above discussion it can be seen that, given f, we can compute c. Hence, we have a representation of the ring $\mathbb{F}_q[\zeta][c^{1/r}]$ in terms of a linear basis $\mathcal{B}$ over $\mathbb{F}_q$ (& their multiplication relations). Because of the properties of $\rho_b(\zeta)$ and $\rho_b(c^{1/r})$ we also have a description of the action of Δ on $\mathbb{F}_q[\zeta][c^{1/r}]$ in terms of $\mathcal{B}$. Thus, we can compute the fixed subring $\mathbb{F}_q[\zeta][c^{1/r}]^\Delta$ efficiently. It is straightforward to get the time complexity estimate. □

Proof of Thm. 1.4. From f, by Thm. 3.5, we can get an irreducible polynomial g over $\mathbb{F}_q$ of degree r. Let m be any r-power. Then, by [15, Thm. 1.1], we can construct $\mathbb{F}_{q^m}$ using g efficiently. □

4 ALGORITHM

For concreteness, we state our algorithm (Algo.1) for constructing r-th nonresidue in this section. The proof of correctness for this algorithm follows directly from Thm. 1.2.

The input to this algorithm is a polynomial $f(x) \in \mathbb{F}_p[x]$ satisfying Property 1.1, $\zeta_r \in \mathbb{F}_p$, and the finite field $\mathbb{F}_{q'}$ of characteristic p where we want to construct r-th nonresidue. The algorithm outputs an r-th nonresidue in $\mathbb{F}_{q'}$.

Note that, since $f(x)$ satisfies Property 1.1, wlog (by the distinct degree factorization) $f = f_1 f_2 \cdots f_{r'}$ such that,

- f_i's are irreducible of degree $d = rk$, and
- $r \nmid r'$.

Time complexity analysis-

One can refer to [26] for basic arithmetic operations. Polynomial computation in Step 2, takes time $\tilde{O}(rn\log p\log q')$ using repeated squaring. Similarly, Step 5 can be done in $\tilde{O}(r^2k\log p\,\deg(f))$. The computation in Step 6 can be done in time $\tilde{O}(\deg(f)\log p)$, using fast Resultant computation [6, Pg. 347].

Algorithm 1 Non-residue computation over finite fields

Input : $f(x)$, $\zeta_r \in \mathbb{F}_p$, $\mathbb{F}_{q'}$, where $q' = p^n$.
Output : r-th nonresidue in $\mathbb{F}_{q'}$.
1: **if** $(r|n)$ **then**
2: Define $g(x) = \sum_{i=0}^{r-1} x^{v^i} {\zeta_r}^i \mod h(x)$ ▷ where $v := p^{n/r}$ and $h(x)$ is the minimal polynomial of $\mathbb{F}_{q'}$ over $\mathbb{F}_p$.
3: Output $g(x)$.
4: **else**
5: Define $g(x) = \sum_{i=0}^{r-1} x^{v^i} {\zeta_r}^i \mod f(x)$ ▷ where $v := p^k$.
6: Output $R(g(x), f(x))$.
7: **end if**

5 SOME SPECIAL CASE APPLICATIONS

5.1 The special case of $r = 2$

Notice that for $r = 2$, we have $\zeta_2 = -1$ available in any finite field with odd characteristic. Thus, using Thm. 1.2 and an f (Property 1.1), we can construct a quadratic nonresidue. The same can also be calculated using Stickelberger lemma directly.

A striking difference, in the case of $r = 2$, is that using Stickelberger lemma (Eqn.1) discriminant is the quadratic nonresidue. This implies that over even degree finite field extensions, the derivative of the minimal polynomial of the extension is a quadratic nonresidue. We formally state this property below.

Lemma 5.1 (Derivative). *Given a finite field $\mathbb{F}_{q^d} = \mathbb{F}_q[x]/\langle f\rangle$ with even $d = \deg(f)$ and $4|(q-1)$, f' is a quadratic nonresidue in $\mathbb{F}_q[x]/\langle f\rangle$.*

Proof. Using Stickelberger lemma (Eqn.1) we know that the discriminant is a quadratic nonresidue in $\mathbb{F}_q$. Since,

$$\Delta(f) \;=\; (-1)^{d(d-1)/2} a_d^{-1} \cdot R(f, f')\,,$$

where $a_d = 1$ is the leading coefficient of $f(x)$, we can deduce that $R(f, f')$ is a quadratic nonresidue in $\mathbb{F}_q$.

Using Lem. 3.3 we get that $N_{\mathbb{F}_{q^d}/\mathbb{F}_q}(f')$ is a quadratic nonresidue in $\mathbb{F}_q$, and using Lem. 2.2 we get that $f'(x)$ is a quadratic nonresidue in $\mathbb{F}_q[x]/\langle f\rangle$. □

5.2 Cases for which ζ_r is known

Since our first main theorem, Thm. 1.2, requires ζ_r, in this section we state some known methods to construct the same.

One of the most significant results on this is by Pila [20]. He generalized Schoof's [21] elliptic curve point-counting algorithm to Fermat curves, and as an application gave an algorithm for factoring the r-th cyclotomic polynomial over $\mathbb{F}_p$. The algorithm is deterministic and runs in time polynomial in $\log p$ for a fixed r. If $r|p-1$ then the factorization of the r-th cyclotomic will give us $\zeta_r \in \mathbb{F}_p$.

A limitation of Pila's algorithm is that it can give us ζ_r only in prime fields. Below we state few results that can give ζ_r in extensions of prime fields.

The following theorem by Bach, von zur Gathen and Lenstra [7] gives an elegant way to construct $\zeta_r \in \mathbb{F}_q$ using "special" irreducible polynomials.

Theorem 5.2. *[7, Thm. 2] Given two prime numbers p and r, the $h = ord_r(p)$, the explicit data for $\mathbb{F}_{p^h}$; given for each prime $\ell|(r-1)$ but not dividing h, an irreducible polynomial g_ℓ of degree ℓ in $\mathbb{F}_p[X]$, there is a deterministic poly$(rh\log(p))$-time algorithm to construct a primitive r-th root of unity in $\mathbb{F}_{p^h}$.*

We immediately get the following.

Corollary 5.3 (Inspired by BGL [7]). *Let prime $r|q-1$. If for each prime $\ell \mid (r-1)$ we are given an irreducible polynomial $h_\ell \in \mathbb{F}_q[x]$ of degree divisible by ℓ, then we can construct $\zeta_r \in \mathbb{F}_q$.*

Proof. Using h_ℓ we can construct an irreducible polynomial of degree ℓ [15, Thm. 1.1]. Using Thm. 5.2 on these, we can construct $\zeta_r \in \mathbb{F}_q$. □

There are also some other methods for finding $\zeta_r \in \mathbb{F}_q$ that are based on the factorization pattern of $q-1$. We present one such result and its proof.

Theorem 5.4 (Sze [29]). *We can find $\zeta_r \in \mathbb{F}_q$ if $q-1 = r^e t$, where $r + t = poly(\log q)$.*

Proof. The number of elements whose order is not a multiple of r is t. So if we take $t+1$ elements in $\mathbb{F}_q$, this will give us an element a that has order a multiple of r. Then, a^t is an element with an r-power order. Let $\mathrm{ord}(a^t) =: r^s$, where $s \geq 1$. Finally, $a^{t \cdot r^{s-1}}$ is an element of order r in $\mathbb{F}_q$. □

5.3 Necessary condition for the irreducibility of a polynomial

Our analysis provides a necessary condition for checking irreducibility of a polynomial.

Lemma 5.5. *If $f \in \mathbb{F}_q[x]$ is irreducible and prime $r|\deg(f)$ with $\gcd(2, r) \cdot r \mid (q-1)$, then $R(L_{f,r}, f(x))$ is an r-th nonresidue in $\mathbb{F}_q$.*

Proof. This follows directly from Thm. 3.1. □

Lem. 5.5 for $r = 2$ is used by von zur Gathen in his paper to prove properties about irreducible trinomials [32, Cor. 3]. We hope that this generalized lemma gives conditions that can help construct additional polynomial families.

5.4 Efficient construction of nonresidues over finite field extension, assuming GRH

It is well known that over prime fields $\mathbb{F}_p$ one can construct r-th nonresidue in $O(\log^2 p)$ time [3]. However, the proof in [3] does not work for finite field extensions. Huang generalized Ankeny's result to prove the following theorem.

Theorem 5.6 (Huang [13]). *Let $\{1, w, w^2, \ldots, w^{m-1}\}$ be the basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$. Assuming GRH, there exists an r-th nonresidue $a \in \mathbb{F}_{p^m}$ such that $a = \sum_{i=0}^{m-1} a_i w^i$ and $|a_i| < O(\log^2 pr)$.*

Note that, constructing r-th nonresidue using the previous theorem will be exponential in m. We give a construction of an r-th nonresidue over finite field extensions which runs in time polynomial in m.

Corollary 5.7. *Assuming GRH, we can construct r-th nonresidue in any finite field $\mathbb{F}_{p^m}$ in time poly$(m, r, \log p)$.*

Proof. If $r \nmid m$, then an r-th nonresidue in $\mathbb{F}_p$ will also be an r-th nonresidue in $\mathbb{F}_p^m$ (See Case 1, proof of Cor. 3.2). Thus we will pick the least r-th nonresidue, which is bounded by $O(\log^2 p)$. On the other hand, if $r|m$ then construction of r-th nonresidue is similar to that in Case 2, proof of Cor. 3.2. Note that, Cor. 3.2 requires $\zeta_r \in \mathbb{F}_{p^m}$, the same can be constructed assuming GRH using [7, Thm. 2] and [1]. □

6 SOME CONJECTURES

6.1 Finding polynomials satisfying Property 1.1

A natural question that arises from our analysis is: How can one construct a polynomial satisfying Property 1.1? An approach can be to come up with a polynomial family $\mathcal{F}$ such that at least one of the polynomial in $\mathcal{F}$ satisfies Property 1.1. We leave the construction of such a polynomial family as an open question.

This question for $r = 2$ will also be very interesting. For $r = 2$, if we can construct a polynomial satisfying Property 1.1 then its discriminant will be a quadratic nonresidue by Stickelberger's lemma.

A well studied polynomial family for such properties are trinomials. *Trinomials* are univariate polynomials with sparsity three:

$$\mathcal{T}_{(n,k,a,b)} = \{x^n + ax^k + b \mid n > k > 0; a, b \in \mathbb{Z}^*\}.$$

An elegant property of trinomials is the closed form expression for their discriminant and, thus, it can be computed efficiently. (Even if the degree of the trinomial is exponential.)

Theorem 6.1 (Swan [28]). *Let $n > k > 0$. Let $d = \gcd(n, k)$ and $n = n_1 d, k = k_1 d$. Then,*

$$\Delta(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} E^d,$$

where $E = n^{n_1} b^{n_1 - k_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1} k^{k_1} a^{n_1}$.

Trinomials are used to construct irreducible polynomials in [28, 32]. Based on our experiments we give the following conjecture.

Conjecture 6.2. *The following polynomial family has at least one polynomial that satisfy property 1.1 for $r = 2$,*

$$\mathcal{F} = \{\mathcal{T}_{(2i,k,a,b)} \mid 1 \le i, k, a, b \le \log^2 p\}.$$

We leave the proof, or a refutation, of this conjecture as an open question.

6.2 Weaker Generalized Riemann Hypothesis

In 1952, Ankeny [3] proved that if the Generalized Riemann Hypothesis is true then the least quadratic nonresidue in $\mathbb{F}_p$ is $O(\log^2 p)$. The Generalized Riemann hypothesis(GRH) says that all the nontrivial roots ρ of the Dirichlet L function are on real line $z = \frac{1}{2}$, but what if we consider a weaker form of it? Instead of saying that all the nontrivial roots lie on $\mathrm{Re}(\rho) = \frac{1}{2}$, we "merely" conjecture that all the nontrivial roots lie in a wider strip $[\frac{1}{2} - \epsilon, \frac{1}{2} + \epsilon]$, for a constant ϵ. Can we prove poly$(\log p)$ upper bound on the least quadratic nonresidue in $\mathbb{F}_p$ assuming this conjecture?

We proved that the answer to this question is affirmative[1].

[1]We thank the reviewer for pointing out that [5, Pg. 293] stated a similar result.

Conjecture 6.3 (Weak GRH). *Let χ be a Dirichlet character, i.e. $\chi : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$. There exists a constant $\frac{1}{2} > \epsilon \ge 0$ such that the Dirichlet L function $L(s, \chi) = \sum \frac{\chi(n)}{n^s}$ have all its nontrivial roots in the interval $\frac{1}{2} - \epsilon < Re(s) < \frac{1}{2} + \epsilon$.*

We will now use some known facts from Analytic number theory, for detailed proofs of these facts see [18, Chap. 7]. Let Λ be the Mangoldt function and $\zeta(s)$ be the Riemann zeta function.

Lemma 6.4 (Bounds for $\psi(x, \chi)$). *Let $\psi(x, \chi) = \sum_{i \le x} \Lambda(i)\chi(i)$ and χ be a primitive Dirichlet character of $\mathbb{F}_p^*$, then*

$$\psi(x, \chi) = -\sum_{|\gamma| < \sqrt{x}} \frac{x^\rho}{\rho} + O\Big(\log^2 px\Big),$$

where $\rho = \sigma + i\gamma$ are the nontrivial roots of the Dirichlet L function $L(s, \chi)$. Also, $\sum_{|\gamma|<\sqrt{x}} \frac{1}{|\rho|} = O(\log^2 px)$.

Lemma 6.5 (Bounds for $\psi(x)$). *Let $\psi(x) = \sum_{i \le x} \Lambda(i)$, then*

$$\psi(x) = x - \sum_{|\gamma| < \sqrt{x}} \frac{x^\rho}{\rho} + O\Big(\sqrt{x}\log^2 x\Big),$$

where $\rho = \sigma + i\gamma$ are the nontrivial roots of the Riemann zeta function $\zeta(s)$. Also, $\sum_{|\gamma|<\sqrt{x}} \frac{1}{|\rho|} = O(\log^2 x)$.

We will now prove bounds on $\psi(x)$ and $\psi(x, \chi)$ assuming Weak GRH.

Lemma 6.6 (New bounds). *Assuming Weak GRH,*

(1) $\psi(x, \chi) = O(x^{\frac{1}{2}+\epsilon} \log^2 px)$, *and*
(2) $\psi(x) = x + O(x^{\frac{1}{2}+\epsilon} \log^2 x)$.

Proof. (1) Using the notation in Lem. 6.4,

$$\begin{aligned}\Big|\sum_{\gamma<\sqrt{x}} \frac{x^\rho}{\rho}\Big| &\le (\max_\rho |x^\rho|) \cdot \Big|\sum_\rho \frac{1}{\rho}\Big| \\ &\le x^{\frac{1}{2}+\epsilon} \cdot \Big|\sum_{\gamma<\sqrt{x}} \frac{1}{|\rho|}\Big| \\ &= O(x^{\frac{1}{2}+\epsilon} \log^2 px).\end{aligned}$$

Since, $\psi(x, \chi) = -\sum_{|\gamma|<\sqrt{x}} \frac{x^\rho}{\rho} + O\Big(\log^2 px\Big)$, we get that $\psi(x, \chi) = O(x^{\frac{1}{2}+\epsilon} \log^2 px)$.

(2) Using the notation in Lem. 6.5,

$$\begin{aligned}\Big|\sum_{\gamma<\sqrt{x}} \frac{x^\rho}{\rho}\Big| &\le (\max_\rho |x^\rho|) \cdot \Big|\sum_\rho \frac{1}{\rho}\Big| \\ &\le x^{\frac{1}{2}+\epsilon} \cdot \Big|\sum_{\gamma<\sqrt{x}} \frac{1}{|\rho|}\Big| \\ &= O(x^{\frac{1}{2}+\epsilon} \log^2 x).\end{aligned}$$

Since, $\psi(x) = x - \sum_{|\gamma|<\sqrt{x}} \frac{x^\rho}{\rho} + O\Big(\sqrt{x}\log^2 x\Big)$, we get that $\psi(x) = x + O(x^{\frac{1}{2}+\epsilon} \log^2 x)$.

□

Using this lemma we will bound the least r-th nonresidue in $\mathbb{F}_p$.

Theorem 6.7. *Let n(p,r) denote the least r-th nonresidue in $\mathbb{F}_p^*$. Then, assuming the Weak GRH,*

$$n(p,r) \;=\; O(\log^{\frac{4}{1-2\epsilon}} p)\,.$$

Proof. Let $\chi_r(a) := a^{\frac{p-1}{r}} \bmod p$, and χ_o be the trivial character i.e., $\chi_0(a) = 1, \forall a \in \mathbb{F}_p^*$. Consider

$$S(M) \;:=\; \sum_{1\le a\le M} \chi_o(a)\Lambda(a) - \sum_{1\le a\le M} \chi_r(a)\Lambda(a)\,.$$

Note that, S(M) is zero iff there is no r-th nonresidue in the initial interval $[M]$.

We have,

$$\begin{aligned} S(M) \;&=\; \psi(M,\chi_o) - \psi(M,\chi_r) \\ &=\; M + O(M^{0.5+\epsilon}\log^2 pM) \qquad [\text{ Using Lem. 6.6 }] \end{aligned}$$

We are interested in finding the maximum M_0 such that $S(M_0) = 0$. The above estimate implies that $M_0 = O(M_0^{0.5+\epsilon}\log^2 pM_0)$.

Therefore, $n(p,r) = O(\log^{\frac{4}{1-2\epsilon}} p)$. □

This elementary analysis, assuming Weak GRH, has remarkable consequences. Ankeny's result has been used in derandomizing many computational problems under the assumption of GRH. Some of them are primality testing [6, Chap. 9], r-th root finding [2], constructing irreducible polynomials over finite fields [1] and cases of polynomial factoring over finite fields [1, 7]. (Also, see [4, 14] and the references therein.) Our result implies that, for derandomizing these problems, proving the Weak GRH suffices.

7 CONCLUSION

We give a significant generalization of Stickelberger Lemma (Eqn.1); we can construct an r-th nonresidue in $\mathbb{F}_q$ given $\zeta_r \in \mathbb{F}_q$ and a polynomial f satisfying Stickelberger property 1.1. Using this, we also gave an algorithm to find r-th roots in $\mathbb{F}_{q^m}$ if $r = O(1)$ and $r|\gcd(m, p-1)$. An interesting open question here is whether one can weaken the Stickelberger property (eg. remove the nondivisibility by r condition?).

Our result along with some known results on finding $\zeta_r \in \mathbb{F}_q$ gives us some interesting applications. It seems that finding $\zeta_r \in \mathbb{F}_q$ is an inherent requirement in our analysis. We leave removing the requirement of ζ_r from our algorithm as an open question. This we have been able to achieve, if the goal is only to construct a degree r irreducible (given f) instead of an r-th nonresidue.

We also leave the concrete conjectures Conj. 6.2 & 6.3 open.

ACKNOWLEDGEMENTS

Part of the research was accomplished while the first two authors were visiting CQT, NUS. V.B. would also like to thank CSE and IITK for their generous hospitality. N.S. thanks the funding support from DST (DST/SJF/MSA-01/2013-14). R.M. would like to thank DST Inspire grant. We thank Manindra Agrawal, Alin Bostan and Igor Shparlinski for their useful comments.

REFERENCES

[1] L. M. Adleman and H. W. Lenstra. Finding irreducible polynomials over finite fields. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 350–355. ACM, 1986.

[2] L. M. Adleman, K. L. Manders, and G. L. Miller. On taking roots in finite fields. In *18th Annual Symposium on Foundations of Computer Science, Providence, Rhode Island, USA, 31 October - 1 November 1977*, pages 175–178. IEEE Computer Society, 1977.

[3] N. C. Ankeny. The least quadratic non residue. *Annals of Mathematics*, 55(1):65–72, 1952.

[4] M. Arora, G. Ivanyos, M. Karpinski, and N. Saxena. Deterministic polynomial factoring and association schemes. *LMS J. Comput. Math.*, 17(1):123–140, 2014.

[5] E. Bach. Fast algorithms under the extended riemann hypothesis: A concrete estimate. In *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, STOC '82, pages 290–295, New York, NY, USA, 1982. ACM.

[6] E. Bach and J. Shallit. *Algorithmic Number Theory.* MIT Press, Cambridge, MA, USA, 1996.

[7] E. Bach, J. von zur Gathen, and H. W. Lenstra. Factoring polynomials over special finite fields. *Finite Fields and Their Applications*, 7(1):5 – 28, 2001.

[8] J. Buchmann and V. Shoup. Constructing nonresidues in finite fields and the Extended Riemann hypothesis. *Mathematics of Computation*, 65(215):1311–1326, 1996.

[9] D. A. Burgess. The distribution of quadratic residues and non-residues. *Mathematika*, pages 4:106–112, 1957.

[10] M. Cipolla. Un metodo per la risoluzione della congruenza di secondo grado. *Napoli Rend*, 9:153–163, 1903.

[11] K. Dalen. *MATHEMATICA SCANDINAVICA*, 3(0):124–126, 1955.

[12] B. Hanson, D. Panario, and D. Thomson. Swan-like results for binomials and trinomials over finite fields of odd characteristic. *Designs, Codes and Cryptography*, 61(3):273–283, 2011.

[13] M. Huang. Riemann hypothesis and finding roots over finite fields. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 121–130. ACM, 1985.

[14] G. Ivanyos, M. Karpinski, and N. Saxena. Schemes for deterministic polynomial factoring. In *Symbolic and Algebraic Computation, International Symposium, ISSAC 2009, Proceedings*, pages 191–198, 2009.

[15] H. W. Lenstra. Finding isomorphisms between finite fields. *Mathematics of Computation*, 56(193):329–347, 1991.

[16] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, Cambridge, UK, 1997.

[17] G. Moroz and E. Schost. A fast algorithm for computing the truncated resultant. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 341–348, 2016.

[18] M. R. Murty. *Problems in Analytic Number Theory.* Springer, New York, 2001.

[19] E. Ozdemir. Computing square roots in finite fields. *IEEE Trans. Information Theory*, 59(9):5613–5615, 2013.

[20] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):745–763, 1990.

[21] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7(1):219–254, 1995.

[22] D. Shanks. Five number-theoretic algorithms. In *Proceedings of the second Manitoba conference on numerical mathematics*, volume 51, page 70, 1972.

[23] V. Shoup. *Removing randomness from Computational Number Theory.* PhD thesis, University of Wisconsin-Madison, 1989.

[24] V. Shoup. New algorithms for finding irreducible polynomials over finite fields. *Mathematics of Computation*, 54(189):435–447, 1990.

[25] V. Shoup. Fast construction of irreducible polynomials over finite fields. *Journal of Symbolic Computation*, 17(5):371–391, 1994.

[26] V. Shoup. *A Computational Introduction to Number Theory and Algebra.* Cambridge University Press, New York, NY, USA, 2005.

[27] L. Stickelberger. Über eine neue eigenschaft der diskriminanten algebraischer zahlkörper. *Verhandlungen des ersten Internationalen Mathematiker-Kongresses, Zürich*, 1:182–193, 1897.

[28] R. G. Swan. Factorization of polynomials over finite fields. *Pacific J. Math.*, 12(3):1099–1106, 1962.

[29] T.-W. Sze. On taking square roots without quadratic nonresidues over finite fields. *Mathematics of Computation*, 80(275):1797–1811, 2011.

[30] A. Tonelli. Bemerkung über die auflösung quadratischer congruenzen. *Nachrichten von der Königl. Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen*, 1891:344–346, 1891.

[31] B. Van der Waerden. *Algebra Vol. 1.* 1970.

[32] J. von zur Gathen. Irreducible trinomials over finite fields. *Math. Comput.*, 72(244):1987–2000, 2003. (Extended abstract in ISSAC'01).