Searching for Primitive Roots in Finite Fields

Victor Shoup

Computer Sciences Department

University of Toronto

Toronto, Ontario M5S 1A4

Abstract

Let GF(p^n) be the finite field with p^n elements where p is prime. We consider the problem of how to *deterministically* generate in polynomial time a subset of GF(p^n) that contains a primitive root, i.e., an element that generates the multiplicative group of nonzero elements in GF(p^n). We present three results. First, we present a solution to this problem for the case where p is small, i.e., $p = n^{O(1)}$. Second, we present a solution to this problem under the assumption of the Extended Riemann Hypothesis (ERH) for the case where p is large and $n = 2$. Third, we give a quantitative improvement of a theorem of Wang on the least primitive root for GF(p) assuming the ERH.

Appeared in *Mathematics of Computation* 58, pp. 369–380, 1992. An earlier version of this paper appeared in the 22nd Annual ACM Symposium on Theory of Computing (1990), pp. 546-554.

1980 Mathematics Subject Classification (1985 revision): 11T06.

1. Introduction

Consider the problem of finding a primitive root in a finite field. For a finite field $\mathrm{GF}(p^n)$ (with p prime and $n \geq 1$), a nonzero element $g \in \mathrm{GF}(p^n)$ is called a primitive root if it generates the multiplicative group of units, $\mathrm{GF}(p^n)^*$. Although there are no known polynomial time algorithms for *constructing* a primitive root, or even for *testing* whether a given element is a primitive root (at least when the factorization of $p^n - 1$ is unknown), we can still raise the question of how to efficiently *search* for a primitive root. By a *search procedure* for primitive roots in $\mathrm{GF}(p^n)$, we mean an algorithm that generates a subset of $\mathrm{GF}(p^n)$ that contains (with high probability, in the case of a probabilistic algorithm) at least one primitive root.

It is well-known that the density of primitive roots in $\mathrm{GF}(p^n)$ is great enough so that the simple method of choosing a small number of elements in $\mathrm{GF}(p^n)$ at random is in fact a probabilistic polynomial time search procedure (here, polynomial time means $(n \log p)^{O(1)}$). However, the existence of a *deterministic* polynomial time search procedure for primitive roots in an arbitrary finite field is an open question—and it is this question that we address here.

An important result in this area is due to Wang [32], who shows that, assuming the Extended Riemann Hypothesis (ERH), there exists a positive integer $x = (\log p)^{O(1)}$ such that $x \bmod p$ is a primitive root for $\mathrm{GF}(p)$. More precisely, Wang shows that $x = O(r^6 (\log p)^2)$, where $r = \omega(p-1)$, the number of distinct prime divisors of $p - 1$. Note that for any integer m, $\omega(m) = O(\log m / \log\log m)$ (see, e.g., [13, p. 355]). Thus, if the ERH is true, the deterministic search procedure that simply enumerates the integers $1, 2, 3$, etc., will generate a primitive root in polynomial time.

We prove three results. Our first result applies to the problem searching for primitive roots in $\mathrm{GF}(2^n)$, and more generally, in $\mathrm{GF}(p^n)$ with p small. We show (unconditionally) that given any irreducible polynomial f of degree n in $\mathrm{GF}(2)[X]$, there exists a polynomial $\theta \in \mathrm{GF}(2)[X]$ (itself irreducible) such that $\deg \theta = O(\log n)$ and $(\theta \bmod f)$ is a primitive root for $\mathrm{GF}(2)[X]/(f) = \mathrm{GF}(2^n)$. More precisely, we prove the following:

Theorem 1. *Let f be an irreducible polynomial of degree n over GF(p), and let $r = \omega(p^n - 1)$. Let ℓ be chosen such that $p^\ell > cr^4(\log r + 1)^4 n^2$, where c is a certain absolute positive constant. Then there exists a monic irreducible polynomial $\theta \in GF(p)[X]$ of degree ℓ such that $(\theta \bmod f)$ is a primitive root for $GF(p)[X]/(f)$.*

This result implies that the deterministic search procedure that enumerates all linear polynomials, and then all quadratic polynomials, etc., will generate a primitive root in $\mathrm{GF}(p^n)$ in time $(np)^{O(1)}$. Furthermore, combining this result with the algorithm in [28] for deterministically constructing irreducible polynomials, we conclude that the problem of constructing a *primitive polynomial* (an irreducible polynomial f for which $(X \bmod f)$ is a primitive root) over $\mathrm{GF}(p)$ of degree n can be reduced in deterministic time $(np)^{O(1)}$ to the problem of testing primitivity. Previously known reductions of this type were probabilistic.

We note that Shparlinsky [30, Theorem 2.4] also gives a deterministic search procedure with running time $(np)^{O(1)}$; however, the method described in that paper does not in general construct a set of polynomials of small degree.

Our second result applies to the problem of searching for primitive roots in $\mathrm{GF}(p^2)$. We prove the following:

Theorem 2. *Assuming the ERH, there is a deterministic polynomial time search procedure for primitive roots in $GF(p^2)$.*

The statement of the theorem does not specify in which specific model of $\mathrm{GF}(p^2)$ a primitive root is sought, but this is not an issue, since isomorphisms between different models of $\mathrm{GF}(p^2)$ can be computed deterministically in polynomial time, and *some* model of $\mathrm{GF}(p^2)$ can be deterministically constructed in polynomial time assuming the ERH (see, e.g., [20]). In proving this theorem, we actually show the following: assuming the ERH, we can deterministically construct in polynomial time a certain model $\mathrm{GF}(p)(\alpha)$ of $\mathrm{GF}(p^2)$, and within this model there exists a primitive root of the form $a + b\alpha$, where a and b are integers of absolute value $(\log p)^{O(1)}$. Unfortunately, our proof of this theorem does not generalize to arbitrary finite fields $\mathrm{GF}(p^n)$, even for fixed $n > 2$.

Assuming the ERH, this theorem implies that one can deterministically construct a q-th nonresidue in $\mathrm{GF}(p^2)$ for a given prime q dividing $p^2 - 1$ in time $(\log p)^{O(1)}$—independent of q. Previous such methods (e.g., [15, 3]) required time at least q. One application of this is the following. For integer m, let $S(m)$ denote the largest prime dividing m. It is shown in [27], by refining the algorithm in [31], that assuming the ERH, polynomials of degree d over $\mathrm{GF}(p)$ can be factored deterministically in time $S(p-1)^{1/2}(d \log p)^{O(1)}$. By combining Theorem 2 with the techniques in [27] and [3], one can prove an analogous result with $S(p+1)$ replacing $S(p-1)$.

Our third result is a quantitative improvement of Wang's theorem. By using a better combinatorial sieve and a better character sum estimate than that used by Wang, we are able to prove the following:

Theorem 3. *Assuming the ERH, the least primitive root mod p is $O(r^4(\log r+1)^4(\log p)^2)$, where $r = \omega(p-1)$.*

Related Work

Besides the results of Wang and Shparlinsky referred to above, we mention the following work on primitive roots in finite fields.

Let $\mathrm{GF}(p^n) = \mathrm{GF}(p)(\alpha)$. Davenport [9] proves that for given n and sufficiently large p (depending on n), there exists a primitive root of the form $\alpha + a$, with $a \in \mathrm{GF}(p)$. Note that our Theorem 1 contains a more explicit version of this result as a special case. Carlitz [6] proves that for given n, ℓ, and sufficiently large p (depending on n, ℓ), there exists a primitive root of the form $\theta(\alpha)$, where θ is a monic polynomial of degree ℓ. Carlitz also shows that for given $\epsilon > 0$, for all sufficiently large p^n (depending on ϵ), and for $\ell > (1/2+\epsilon)n$, there exists a primitive root of the form $\theta(\alpha)$ where θ is a monic polynomial of degree ℓ.

Karacuba [18], extending the work of Burgess [5], Wang [32], and Davenport and Lewis [10], proves the existence of a primitive root in $\mathrm{GF}(p^n)$ of the form $a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$, where the a_i's are bounded by $p^{1/4+\epsilon}$ (for all $\epsilon > 0$ and all sufficiently large p). See also the work of Friedlander [12] and Hinz [14].

The results in this paper bear on the basic issue in Computer Science of the power of probabilistic versus deterministic models of computation—and more specifically, the problem of eliminating the need for randomness in algorithms. Recently, there has been much work on this problem in the area of number-theoretic and algebraic algorithms. In this regard, we mention the deterministic algorithms for constructing irreducible polynomials of degree n over $\mathrm{GF}(p)$ in the papers [1, 11] and [8, 26, 28]. The running times of the algorithms in [1, 11] are $(n\log p)^{O(1)}$ assuming the ERH, whereas the running times of the algorithms in [8, 26, 28] are unconditionally $(np)^{O(1)}$. We also mention the result of Lenstra [20] that isomorphisms between two different models of a $\mathrm{GF}(p^n)$ can be computed in deterministic time $(n\log p)^{O(1)}$ (unconditionally). Also relevant is recent work on factoring polynomials over finite fields [3, 15, 24, 23, 25, 29, 31].

Acknowledgements

The author would like to thank Eric Bach, Jeff Lagarias, and Andrew Odlyzko for helpful discussions, and Hendrik Lenstra for comments on earlier versions of this paper that led to the simplification of several proofs.

2. Preliminaries

As does Wang, we shall make use of a combinatorial sieve. However, we will use a sieve due to Iwaniec [17] that is easier to apply and gives sharper upper bounds. Iwaniec specifically considers a problem known as Jacobsthal's problem, which is to estimate for a given r the maximum length $C(r)$ of a sequence of consecutive integers each divisible by one of r arbitrarily chosen primes. Iwaniec proves that $C(r) = O(r^2(\log r)^2)$. However, Iwaniec's arguments can easily be generalized to obtain the following:

Proposition 1. (Iwaniec's Shifted Sieve) *Let Γ be a finite set, and let $U : \Gamma \to \mathbf{Z}$, $W : \Gamma \to \mathbf{R}_{\geq 0}$. Let $q_1, \ldots, q_r$ be distinct primes with $Q = q_1 \cdots q_r$. Define*

$$T = \sum_{\substack{\gamma \in \Gamma \\ \gcd(U(\gamma), Q) = 1}} W(\gamma)$$

and for $d \mid Q$

$$S_d = \sum_{\substack{\gamma \in \Gamma \\ U(\gamma) \equiv 0 \pmod{d}}} W(\gamma).$$

Suppose there exist A and B such that for all $d \mid Q$,

$$|S_d - A/d| \leq B.$$

Then

$$T \geq c_1 A/(\log r + 1)^2 - c_2 r^2 B,$$

where c_1, c_2 are absolute positive constants.

Proof. We sketch here the modifications of Iwaniec's proof required to obtain the proposition. We can assume that $r > 1$; otherwise, the proposition is immediate.

Assume that $q_1 < \cdots < q_r$. Let $p_1 < \cdots < p_r$ be the first r primes, and let $P = p_1 \cdots p_r$. Let $\{\lambda_n : n \mid P\}$ be a set of real numbers, and let $\sigma_n = \sum_{m \mid n} \lambda_m$ for $n \mid P$. Assume that $\sigma_n \leq \sum_{m \mid n} \mu(m)$ for all $n \mid P$.

Lemma 1 in [17] can be easily generalized to obtain

$$T \geq A \prod_{i=1}^{r} (1 - \frac{1}{q_i}) G_1 - B G_2, \tag{2}$$

where

$$G_1 = \sum_{n|P} \frac{\sigma_n}{\prod_{p_i|n}(p_i - 1)},$$

and

$$G_2 = \sum_{n|P} |\lambda_n|.$$

Let $z = p_r$, and let y satisfy $z^2 \leq y \leq z^4$. By choosing the numbers λ_n appropriately (see the definition on p. 5 of [17]), the following estimates are derived in [16]:

$$G_1 = 2e^k \cdot \frac{\log(s-1)}{s} + O(1/\log y), \tag{3}$$

and

$$G_2 = O(y/(\log y)^2), \tag{4}$$

where $s = \log y / \log z$ and k is Euler's constant.

By setting $y = Cz^2$ for a suffiently large absolute constant C (which depends on the big-'O' constant in (3)), from these estimates and the prime number theorem, one can easily show that $G_2 = O(r^2)$ and $G_1 = \Omega(1/\log r)$. Combining this with (2), the proposition follows. $\square$

We will make extensive use of characters on finite abelian groups. We summarize the basic facts here (see, e.g., [4, pp. 415 ff.].) Let G be a finite abelian group. A character χ on G is a homomorphism from G into the complex unit circle. The characters on G form a group under the multiplication law $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$. The character that is 1 on G is called the principal character, and is denoted by χ_0. It is known that the character group of G is isomorphic to G. Furthermore, suppose that H is a subgroup of G, and that H' is the subgroup of the character group of G that is 1 on H. Then it is easy to show that the order of H' is $[G : H]$, and that

$$\sum_{\chi \in H'} \chi(a) = \begin{cases} [G:H] & \text{if } a \in H, \\ 0 & \text{otherwise.} \end{cases}$$

3. Proof of Theorem 1

Let $F = \mathrm{GF}(p)$. We use the following notation:

For $\ell \geq 0$, M_ℓ is the set of monic polynomials in $F[X]$ of degree ℓ;

For $\ell \geq 1$, I_ℓ is the set of monic irreducible polynomials in $F[X]$ of degree ℓ;

$M = \cup_{\ell \geq 0} M_\ell$;

$I = \cup_{\ell \geq 1} I_\ell$;

Λ is the Von Mangoldt function for $F[X]$: $\Lambda(\theta)$ is equal to $\deg P$ if θ is a power of the irreducible polynomial P, and is otherwise equal to 0.

We begin with the following character sum estimate.

Proposition 5. *Let $f \in M_n$, and let χ be a nontrivial character on $(F[X]/(f))^*$, extended by zero to all polynomials. Then for all $\ell \geq 1$, we have*

$$\left| \sum_{\theta \in M_\ell} \chi(\theta)\Lambda(\theta) \right| \leq (n-1)p^{\ell/2}.$$

Proof. To prove this, we use the L-function

$$L(\chi, T) = \sum_{\theta \in M} \chi(\theta) T^{\deg \theta}.$$

As written, this is a formal power series in T; however, it is easy to see that since χ is nontrivial, it is actually a polynomial in T of degree less than n. Therefore, we have the factorization

$$L(\chi, T) = \prod_{i=1}^{n-1} (1 - \alpha_i T), \tag{6}$$

where the α_i's are complex numbers.

It is a consequence of Weil's theorem on the Riemann hypothesis for function fields that each α_i is bounded by $p^{1/2}$ in absolute value. We briefly sketch why this is so.

Let g be the conductor of χ (so g is a divisor of f, different from 1), and let χ' be the corresponding primitive character modulo g. Then by Euler's product formula, we have

$$L(\chi, T) = L(\chi', T) \prod_{\substack{\theta | f \\ \theta \nmid g}} (1 - \chi'(\theta) T^{\deg \theta}),$$

where the product ranges over all monic irreducible θ that divide f but not g.

It follows from the discussion in Appendix V of Weil's book [33] that

$$L(\chi', T) = \prod_{i=1}^{\deg g - 1} (1 - \beta_i T),$$

if χ' is nontrivial on F, and otherwise

$$L(\chi', T) = (1 - T) \prod_{i=1}^{\deg g - 2} (1 - \beta_i T),$$

where in either case, all of the β_i's have absolute value equal to $p^{1/2}$. This fact can be seen by using χ' to define a character ω on the idele group for $F[X]$ in the manner described in § 6 of Appendix V, with $\omega_\infty \equiv 1$. The conductor of ω will contain ∞ to the power 1 if χ' is nontrivial on F (in which case ω is ramified at ∞); otherwise, ∞ does not divide the conductor of ω (and ω is unramified at ∞).

We conclude that all of the α_i's appearing in (6) are either 0, roots of unity, or of absolute value $p^{1/2}$. Now consider the formal power series

$$T \frac{L'(\chi, T)}{L(\chi, T)} = \sum_{\ell \geq 1} \lambda_\ell T^\ell.$$

From (6), it follows that

$$\lambda_\ell = -\alpha_1^\ell - \alpha_2^\ell - \cdots - \alpha_{n-1}^\ell \text{ for all } \ell \geq 1. \tag{7}$$

But if we compute $TL'(\chi, T)/L(\chi, T)$ using the Euler product formula for $L(\chi, T)$ (see, e.g., [21, p. 196]), we obtain

$$\lambda_\ell = \sum_{\theta \in M_\ell} \chi(\theta) \Lambda(\theta). \tag{8}$$

Combining (7) and (8) with the fact the the α_i's are bounded by $p^{1/2}$ in absolute value, the proposition is proved. $\square$

We are now ready to prove Theorem 1. Let f be the given monic irreducible polynomial of degree n. For a multiplicative character χ on the finite field $F[X]/(f)$, let

$$J(\chi, \ell) = \sum_{\theta \in I_\ell} \ell \cdot \chi(\theta).$$

From Proposition 5 it follows that $J(\chi, \ell) = O(np^{\ell/2})$ if χ is nontrivial, and $J(\chi, \ell) = p^\ell + O(np^{\ell/2})$ otherwise.

For $\theta \in F[X]$ prime to f, let $\mathrm{ind}(\theta)$ be the discrete logarithm of $(\theta \bmod f)$ with respect to some arbitrary but fixed primitive root for $F[X]/(f)$. To apply Iwaniec's Shifted Sieve, we let $p^n - 1 = q_1^{e_1} \cdots q_r^{e_r}$ be the prime factorization of $p^n - 1$, and set $Q = q_1 \cdots q_r$. We put $\Gamma = I_\ell \backslash \{f\}$. Now for $\theta \in \Gamma$, put $U(\theta) = \mathrm{ind}(\theta)$, $W(\theta) = \ell$, and let S_d (for $d \mid Q$) and T be the corresponding sums.

To estimate S_d, let χ be a multiplicative character of order d on $F[X]/(f)$. Then we have

$$\begin{aligned} S_d &= \sum_{\substack{\theta \in \Gamma \\ \mathrm{ind}(\theta) \equiv 0 \pmod d}} \ell \\ &= \frac{1}{d} \sum_{\theta \in I_\ell} \sum_{i=0}^{d-1} \chi^i(\theta) \ell \\ &= \frac{1}{d} J(\chi^0, \ell) + \frac{1}{d} \sum_{i=1}^{d-1} J(\chi^i, \ell) \\ &= p^\ell / d + O(np^{\ell/2}). \end{aligned}$$

It then follows from Iwaniec's Shifted Sieve that

$$T = \sum_{\substack{\theta \in \Gamma \\ \gcd(\mathrm{ind}(\theta), Q) = 1}} \ell \geq c_1 p^\ell / (\log r + 1)^2 - c_2 r^2 p^{\ell/2} n.$$

We can force T to be positive by choosing ℓ so that $p^\ell > cr^4(\log r + 1)^4 n^2$, where c is a certain absolute constant. For such values of ℓ, Γ will contain a primitive root. This proves Theorem 1.

4. Dirichlet Characters in Algebraic Number Fields

In this section, we establish some notation and state some results concerning Dirichlet characters that will be used in subsequent sections.

A Dirichlet character modulo a positive integer m is a character on the group $(\mathbf{Z}/m\mathbf{Z})^*$, extended by zero to all integers. Let $x > 0$. For a positive integer k, let

$$\Lambda_0(k, x) = \begin{cases} (\log k)(1 - k/x) & \text{if } k \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

For a Dirichlet character χ mod m, let

$$J(\chi, x) = \sum_{k < x} \Lambda_0(k, x) \chi(k).$$

Montgomery [22, Chapter 13] establishes the following character sum estimate:

Proposition 9. *Assume the ERH. For a Dirichlet character χ mod m, and for $x > 0$, we have $J(\chi, x) = x/2 + O(x^{1/2} \log m)$ for $\chi = \chi_0$, and $J(\chi, x) = O(x^{1/2} \log m)$ otherwise.*

From these estimates, one can easily derive an upper bound of $O((\log p)^2)$ on the least prime that is a quadratic nonresidue (or residue) modulo a prime p. This was first proved by Ankeny [2]. The following simple variant of Ankeny's theorem will be useful.

Proposition 10. *Assume the ERH. Let p be an odd prime. Then there exists a prime $q = O((\log p)^2)$ with $q \equiv 1 \pmod 4$ such that q is a quadratic nonresidue (or residue) mod p.*

Proof. Consider the group $(\mathbf{Z}/4p\mathbf{Z})^*$, along with the subgroup G of index 2 consisting of all $k \equiv 1 \pmod 4$, and the subgroup $H = G^2$ of index 4. Then we have

$$\sum_{\substack{k<x \\ k \in G}} \Lambda_0(k, x) = \frac{1}{2} \sum_{k<x} \sum_{\chi} \chi(k) \Lambda_0(k, x),$$

where the sum on χ is over the two Dirichlet characters mod $4p$ that are 1 on G. By considering the principal character separately, and applying Proposition 9, we see that

$$\sum_{\substack{k<x \\ k \in G}} \Lambda_0(k, x) = x/4 + O(x^{1/2} \log p). \tag{11}$$

A similar argument shows that

$$\sum_{\substack{k<x \\ k \in H}} \Lambda_0(k, x) = x/8 + O(x^{1/2} \log p). \tag{12}$$

It is easy to see that (11) and (12) together imply the proposition. $\square$

Dirichlet characters are also defined in algebraic number fields. We first summarize the basic definitions (see Heilbronn [7, p. 204 ff.] for more background). K will denote a number field with ring of integers O. By Δ we will denote the absolute value of the discriminant of K and h the class number. For an integral ideal A, $N(A)$ denotes its norm, and for $\alpha \in K$, $N(\alpha)$ denotes its norm.

We let $\mathcal{I}$ denote the group of nonzero (fractional) ideals and $\mathcal{P}$ the subgroup of principal ideals. Let M be a given integral ideal. We let $\mathcal{I}_M$ denote the subgroup of ideals prime to M, and $\mathcal{P}_M$ denote the subgroup of principal ideals prime to M. An element $\alpha \in K$ is called *totally positive* if it is positive in all real embeddings of K in $\mathbf{C}$. (In our application, K will be a complex quadratic field, and so all nonzero elements of K are vacuously totally positive.) We let $\mathcal{P}_M^1$ denote the subgroup of $\mathcal{P}_M$ consisting of all principal ideals that are generated by an element a/b such that *(i)* $a, b \in O$, *(ii)* a, b prime to M, *(iii)* $a \equiv b \pmod{M}$, and *(iv)* a/b is totally positive.

One can show that $[\mathcal{I}_M : \mathcal{P}_M] = h$ and that $[\mathcal{P}_M : \mathcal{P}_M^1]$ is finite, so that in particular, $\mathcal{I}_M/\mathcal{P}_M^1$ is a finite abelian group. Let $H^{(M)}$ denote the character group of $\mathcal{I}_M/\mathcal{P}_M^1$. A function $\chi \in H^{(M)}$ is known as a Dirichlet character modulo M. As for ordinary Dirichlet characters, we extend χ by zero to all ideals.

We now define character sums as in [19]. Let Λ be the Von Mangoldt function for ideals, i.e., $\Lambda(A) = \log N(P)$ if A is the power of a prime ideal P, and $\Lambda(A) = 0$ otherwise. Now for $y > x > 1$ and $u > 0$, define $\hat{k}(u; x, y)$ as follows:

$$\hat{k}(u; x, y) = \begin{cases} 0 & \text{if } u > y^2, \\ u^{-1}\log(y^2/u) & \text{if } xy < u < y^2, \\ u^{-1}\log(u/x^2) & \text{if } x^2 < u < xy, \\ 0 & \text{if } u < x^2. \end{cases}$$

For convenience, we define

$$\Lambda_1(A, x, y) = \Lambda(A)N(A)^{-1}\hat{k}(N(A); x, y).$$

Finally, for a Dirichlet character χ, and $y > x > 1$, we define the character sum

$$I(\chi, x, y) = \sum_A \Lambda_1(A, x, y)\chi(A),$$

where A ranges over all nonzero integral ideals. Note that this is actually a finite sum, as it counts only prime-power ideals of norm less than y^2.

The following character sum estimates can be easily extracted from the proof of Theorem 1.2 in [19].

Proposition 13. *Assume the ERH. For a Dirichlet character χ mod M, and for $y > x > 1$, we have*

$$I(\chi, x, y) = (\log(y/x))^2 + O(x^{-1}\log(\Delta N(M))) + O(x^{-2}\log(y/x)\log(\Delta N(M))) \tag{14}$$

for $\chi = \chi_0$, and

$$I(\chi, x, y) = O(x^{-1}\log(\Delta N(M))) \tag{15}$$

for $\chi \neq \chi_0$.

5. Proof of Theorem 2

The prime p may, of course, be assumed to be odd. Let $p^2 - 1 = q_1^{e_1} \cdots q_r^{e_r}$, and $Q = q_1 \cdots q_r$.

First, we must find the least rational prime $\delta \equiv 1 \pmod 4$ such that $-\delta$ is a quadratic nonresidue modulo p. Assuming the ERH, the least such δ is $O((\log p)^2)$ by Proposition 10 (δ is a quadratic nonresidue if $p \equiv 1 \pmod 4$, and a quadratic residue otherwise).

Let $\omega = \sqrt{-\delta} \in \mathbf{C}$, and let $K = \mathbf{Q}(\omega)$. Then K is a number field with integers $O = \mathbf{Z}[\omega]$, and $\Delta = 4\delta$. As $\delta > 3$, the only units in O are ± 1. As a consequence of Minkowski's theorem, the class number h is $O(\Delta^{1/2} \log \Delta)$, which is $O((\log p)(\log\log p))$.

We shall represent $\mathrm{GF}(p^2)$ as $\mathrm{GF}(p)(\bar{\omega})$ where $\bar{\omega}$ is a root of $X^2 + \delta$ in $\mathrm{GF}(p^2)$. The map $\rho : O \to \mathrm{GF}(p^2)$ that sends $a + b\omega$ to $a + b\bar{\omega}$ is a surjective ring homomorphism with kernel (p).

We will show below that assuming the ERH, there exists $\alpha \in O$ with $N(\alpha) = O(r^4(\log r + 1)^4 h^2 (\log p)^2)$ such that $\rho(\alpha)$ is a primitive root in $\mathrm{GF}(p^2)$. It will then follow that there exist integers a, b such that $a + b\bar{\omega}$ is a primitive root for $\mathrm{GF}(p^2)$, where $|a| = O(r^2(\log r + 1)^2(\log p)^2(\log\log p))$ and $|b| = O(r^2(\log r + 1)^2(\log p)(\log\log p))$.

Consider the subgroup (± 1) of $\mathrm{GF}(p^2)^*$, and let η be the canonical homomorphism from $\mathrm{GF}(p^2)^*$ onto $G = \mathrm{GF}(p^2)^*/(\pm 1)$. Observe that G is a cyclic group of order $(p^2 - 1)/2$, and that since $4 \mid p^2 - 1$, $g \in \mathrm{GF}(p^2)^*$ is a generator if and only if $\eta(g) \in G$ is a generator. For a given element u of G, let $\mathrm{ind}(u)$ denote the discrete logarithm of u with respect to some arbitrary but fixed generator in G.

Now, we define $\tau : \mathcal{P}_p \to G$ as follows. For $A \in \mathcal{P}_p$, choose a, b in O prime to p such that $A = (a/b)$, and define $\tau(A) = \eta(\rho(a)/\rho(b))$. It is easy to show that this definition is independent of the choice of a and b, and that τ is a surjective group homomorphism with kernel $\mathcal{P}_p^1$.

It will suffice to show the existence of an integral ideal $A \in \mathcal{P}_p$ of small norm such that $\gcd(\mathrm{ind}(\tau(A)), Q) = 1$. Let $y > x > 1$ be fixed (their values will be determined later). Using the notation of Iwaniec's Shifted Sieve, we let $\Gamma = \mathcal{P}_p$, and for $A \in \mathcal{P}_p$, let $U(A) = \mathrm{ind}(\tau(A))$ and $W(A) = \Lambda_1(A, x, y)$. Let S_d (for $d \mid Q$) and T be the corresponding sums.

To estimate S_d, let $\mathcal{J}_d$ be the pre-image of G^d under τ, where G^d is the subgroup of d-th powers in G. Then $\mathcal{J}_d$ is a subgroup of index d in $\mathcal{P}_p$ containing $\mathcal{P}_p^1$. Let H_d denote the subgroup of the character group $H^{(p)}$ that is 1 on the subgroup $\mathcal{J}_d/\mathcal{P}_p^1$ of $\mathcal{I}_p/\mathcal{P}_p^1$. Then H_d is a group of order hd, and for any $A \in \mathcal{I}_p$,

$$\sum_{\chi \in H_d} \chi(A) = \begin{cases} hd & \text{if } A \in \mathcal{J}_d \\ 0 & \text{otherwise.} \end{cases}$$

It follows from this, and the bound (15), that

$$\begin{aligned} S_d &= \frac{1}{hd} \sum_{\chi \in H_d} I(\chi, x, y) \\ &= \frac{I(\chi_0, x, y)}{hd} + O(x^{-1} \log(\Delta N(p))). \end{aligned}$$

It then follows from Iwaniec's Shifted Sieve that

$$T \geq \frac{c_1 I(\chi_0, x, y)}{h(\log r + 1)^2} - c_2 r^2 x^{-1} \log(\Delta N(p)).$$

We now choose x and y to ensure that $T > 0$. From the bound (14), for an appropriately large constant c, $x = cr^2(\log r + 1)^2 h \log(\Delta N(p))$ and $y = 2x$ will do the job. Since $\log(\Delta N(p)) = O(\log p)$, this implies the existence of an ideal A of norm less than $y^2 = O(r^4(\log r + 1)^4 h^2 (\log p)^2)$ such that $A \in \mathcal{P}_p$ and $\tau(A)$ is a generator for G.

6. Proof of Theorem 3

For integer k, let $\mathrm{ind}(k)$ denote the discrete logarithm of k mod p with respect to some fixed primitive root. Let Q denote the product of the distinct primes dividing $p - 1$. For a given x, one applies Iwaniec's Shifted Sieve using $\Gamma = \{k : 1 < k < x,\ p \not| k\}$, and for $k \in \Gamma$, $U(k) = \mathrm{ind}(k)$ and $W(k) = \Lambda_0(k, x)$. The proof then follows the same general line of reasoning as the proofs of Theorems 1 and 2: one first uses Proposition 9 to obtain an estimate for the sum S_d, and then applies Iwaniec's Shifted Sieve to get a lower bound on T in terms of x. We omit the details.

References

[1] L. M. Adleman and H. W. Lenstra Jr. Finding irreducible polynomials over finite fields. In *18th Annual ACM Symposium on Theory of Computing*, pages 350–355, 1986.

[2] N. C. Ankeny. The least quadratic nonresidue. *Ann. of Math.*, 55:65–72, 1952.

[3] E. Bach and J. von zur Gathen. Deterministic factorization of polynomials over special finite fields. Technical Report 799, Computer Sciences Department, University of Wisconsin–Madison, 1988.

[4] Z. I. Borevich and I. R. Shafarevich. *Number Theory.* Academic Press, 1966.

[5] D. A. Burgess. Character sums and primitive roots in finite fields. *Proc. London Math. Soc.*, 3(17):11–25, 1967.

[6] L. Carlitz. Distribution of primitive roots in a finite field. *Quart. J. Math.*, 4:4–10, 1953.

[7] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic Number Theory.* Academic Press, 1967.

[8] A. L. Chistov. Polynomial time construction of a finite field. In *Abstracts of Lectures at 7th All-Union Conference in Mathematical Logic, Novosibirsk*, page 196, 1984. In Russian.

[9] H. Davenport. On primitive roots in finite fields. *Quart. J. Math. (Oxford)*, 8:308–312, 1937.

[10] H. Davenport and D. J. Lewis. Character sums and primitive roots in finite fields. *Rend. Circ. Mat. Palermo*, 12:129–136, 1963.

[11] S. A. Evdokimov. Factoring a solvable polynomial over a finite field and Generalized Riemann Hypothesis. *Zapiski Nauchn. Semin. Leningr. Otdel. Matem. Inst. Acad. Sci. USSR*, 176:104–117, 1989. In Russian.

[12] J. B. Friedlander. A note on primitive roots in finite fields. *Mathematika*, 19:112–114, 1972.

[13] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, fifth edition, 1984.

[14] J. G. Hinz. Character sums and primitive roots in algebraic number fields. *Monatshefte für Mathematik*, 95(4):275–286, 1983.

[15] M. A. Huang. Riemann hypothesis and finding roots over finite fields. In *17th Annual ACM Symposium on Theory of Computing*, pages 121–130, 1985.

[16] H. Iwaniec. On the error term in the linear sieve. *Acta Arith.*, 19:1–30, 1971.

[17] H. Iwaniec. On the problem of Jacobsthal. *Demonstratio Mathematica*, 11:225–231, 1978.

[18] A. A. Karacuba. Character sums and primitive roots in finite fields. *Soviet. Math. Dokl.*, 9:755–757, 1968.

[19] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Inv. math.*, 54:271–296, 1979.

[20] H. W. Lenstra. Finding isomorphisms between finite fields. *Math. Comp.*, 56, 1991. To appear.

[21] R. Lidl and H. Niederreiter. *Finite Fields.* Addison-Wesley, 1983.

[22] H. L. Montgomery. *Topics in Multiplicative Number Theory (Lecture Notes in Mathematics No. 227).* Springer-Verlag, 1971.

[23] L. Rónyai. Factoring polynomials over finite fields. *J. Algorithms*, 9:391–400, 1988.

[24] L. Rónyai. Factoring polynomials modulo special primes. *Combinatorica*, 9(2):199–206, 1989.

[25] L. Rónyai. Galois groups and factoring polynomials over finite fields. In *30th Annual Symposium on Foundations of Computer Science*, pages 99–104, 1989.

[26] I. A. Semaev. Construction of irreducible polynomials over finite fields with linearly independent roots. *Mat. Sbornik*, 135:520–532, 1988. In Russian; English translation in *Math. USSR–Sbornik*, 63(2):507–519, 1989.

[27] V. Shoup. A theorem on factoring polynomials over finite fields. Technical Report 866, Computer Sciences Department, University of Wisconsin–Madison, 1989. To appear in *Inform. Process. Lett.* as "Smoothness and factoring polynomials over finite fields".

[28] V. Shoup. New algorithms for finding irreducible polynomials over finite fields. *Math. Comp.*, 54(189):435–447, 1990.

[29] V. Shoup. On the deterministic complexity of factoring polynomials over finite fields. *Inform. Process. Lett.*, 33(5):261–267, 1990.

[30] I. E. Shparlinsky. On primitive elements in finite fields and on elliptic curves. *Mat. Sbornik*, 181(9):1196–1206, 1990. In Russian.

[31] J. von zur Gathen. Factoring polynomials and primitive elements for special primes. *Theoret. Comput. Sci.*, 52:77–89, 1987.

[32] Y. Wang. On the least primitive root of a prime. *Scientia Sinica*, 10(1):1–14, 1961.

[33] A. Weil. *Basic Number Theory*. Springer-Verlag, third edition, 1974.