Artin's Conjecture for Polynomials Over Finite Fields

*Erik Jensen and M. Ram Murty**

1 Introduction

A classical conjecture of E. Artin[Ar] predicts that any integer $a \neq \pm 1$ or a perfect square is a primitive root (mod p) for infinitely many primes p. This conjecture is still open. In 1967, Hooley[H] proved the conjecture assuming the (as yet) unresolved generalized Riemann hypothesis for Dedekind zeta functions of certain number fields.

In 1983, R. Gupta and M.R. Murty[GM] made the first breakthrough by showing the following: given three prime numbers a, b, c, then at least one of the thirteen numbers

$$\{ac^2, a^3b^2, a^2b, b^3c, b^2c, a^2c^3, ab^3, a^3bc^c, bc^3, a^2b^3c, a^3c, ab^2c^3, abc\}$$

is a primitive root (mod p) for infinitely many primes p. This result has been further refined by R. Gupta, M.R. Murty, and V.K. Murty[GMM] to establish that at least one of the seven numbers

$$\{a, b, c, a^2b, ab^2, a^2c, ac^2\}$$

is a primitive root (mod p) for infinitely many primes p. Finally, Heath-Brown[HB] used the Chen-Iwaniec switching and a celebrated 1986 theorem of Bombieri, Friedlander, and Iwaniec[BFI] to derive the further refinement that at least one of $\{a, b, c\}$ is a primitive root for infinitely many primes p. The paper by Murty[M1] contains an overview of Artin's conjecture and its analogues for elliptic curves. (See also [M2]).

Although any undergraduate student can easily understand Artin's conjecture, to understand Hooley's results requires a strong background in both analytic and algebraic number theory, and thus is only possible at the senior or graduate level. The results of Gupta, M.R. Murty, V.K. Murty, and Heath-Brown require an even more formidable background in advanced sieve theory that is available only to the doctoral student or to the expert working in the field.

The purpose of this paper is twofold. Our first goal is to show that the sieve approach can be understood, at least conceptually, by the undergraduate student. Indeed, it was this kind of conceptual reasoning that led to the original breakthrough. Once our reasoning is in place, it is then just a matter of technical expertise to fine tune the argument to get a refined result.

The first author, an undergraduate, would like to thank the second author for giving him the opportunity of being a part of this research project. Research of the second author was partially supported by NSERC.

Our second goal is to study the analogue of Artin's conjecture for polynomials mod p. More precisely, fix a prime p and let $a(x)$ be a non-constant polynomial which is not equal to the square of a polynomial mod p. Are there infinitely many irreducible polynomials $p(x)$ such that $a(x)$ generates the residue classes of $(\mathbf{F}_p[x]/(p(x)))^*$?

In 1937, Bilharz[B], a student of E. Artin, answered this in the affirmative, by assuming the truth of the so-called Riemann hypothesis for curves. Then, in 1948, A. Weil proved the Riemann hypothesis for curves as a consequence of his rigorous treatment of algebraic geometry (see [L] for a proof). Thus, as it stands, even this "function field analogue" is not accessible to the undergraduate student.

In this paper, we will show that for $a(x) = x^m + c$, Artin's conjecture for $\mathbf{F}_p[x]$ can be established very easily and almost from first principles. The fact that the junior author co-authored this paper is proof enough that it is accessible to the undergraduate.

2 Sieve Theory and Artin's Conjecture

Understanding this section requires a familiarity with quadratic residues. We direct the reader to chapter 5, section 1 of Ireland and Rosen[IR].

Suppose that we want to prove that 2 is a primitive root (mod p) for infinitely many primes p. First, observe that if $(p-1) = 4q$, with q an odd prime, then 2 is a primitive root (mod p). To see this, suppose that 2 has order r. Then $r|(p-1)$. Hence, $r|4q$. Therefore, $r \in \{1, 2, 4, q, 2q, 4q\}$. Let's examine the separate cases. Clearly the case $r = 1$ is not possible. If $r = 2$, we have that $p|(2^2-1)$, which implies that $p = 3$. However, $p = 4q+1$, which is clearly ≥ 13. So, we see that $r \neq 2$. Similarly, if $r = 4$ we have that $p|(2^4 - 1)$, which implies that $p = 3$ or $p = 5$. However, we have seen that $p \geq 13$, so it is clear that $r \neq 4$. If $r = q$ or $r = 2q$, then

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Hence, 2 is a quadratic residue (mod p). Therefore,

$$p \equiv \pm 1 \pmod{8}.$$

However, it is easily seen that

$$p = 4q + 1 = 4(2k + 1) + 1 = 8k + 5 \equiv 5 \pmod{8}.$$

Hence, $r = 4q = (p - 1)$. It is at present unknown whether there are infinitely many primes p such that $(p - 1) = 4q$, with q prime. Heuristic reasoning[IR, ch. 2, §4] suggests that the number of such primes $p \leq x$ is asymptotic to $\frac{cx}{\log^2 x}$ as $x \to \infty$, for some constant $c > 0$. So, our attempt at a proof stalls here. However, if we continue along this line of thought, and use the ideas of sieve theory, we can prove that one of 2, 3, 5 is a primitive root for infinitely many primes p. First, though, we will pause to prove a lemma which will be useful later on.

Lemma: *A natural number n cannot have more than $\frac{\log n}{\log 2}$ prime factors.*

Proof: Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}$, with $p_1, \ldots, p_l$ distinct primes. Then we see that

$$\log n = \sum_{i=1}^{l} \alpha_i \log p_i \geq l \log 2$$

and so clearly we have that

$$l \leq \frac{\log n}{\log 2}$$

and the lemma is proved. □

Ramanujan[R] observed that this estimate can be refined to

$$l = O\left(\frac{\log n}{\log \log n}\right)$$

in the following way: first, note that

$$\log n \geq \sum_{i=1}^{l} \log p_i \geq \sum_{i=1}^{l} \log q_i$$

where $2 = q_1 < q_2 < \cdots$ is the sequence of primes. Then, by the elementary Tchebychef theorem (see [IR, p. 25]), we obtain

$$\log n \geq cl \log l$$

for some constant $c > 0$. If $l \leq \frac{\log n}{\log \log n}$, then we are done, so assume that $l > \frac{\log n}{\log \log n}$. Then,

$$\log l > \log \log n - \log \log \log n$$

which gives

$$\log n \gg l \log \log n$$

as desired.

The seminal idea of Gupta and Murty was to use sieve theory to produce primes p such that $(p-1)$ has very few prime factors, thereby restricting the possibility for 2 to have order $< (p-1) \bmod p$. Indeed, sieve theory provides at least

$$\frac{cx}{\log^2 x}, \quad c > 0$$

primes $p \leq x$ such that $(p-1) = 2q$ or $(p-1) = 2q_1q_2$, with q, q_1, q_2 prime and $(2/p) = (3/p) = (5/p) = -1$. Moreover, one can arrange

$$q_2 > x^{\frac{1}{2}-\delta} > q_1 > x^{0.26} \quad \text{for some } \delta > 0.$$

If $(p-1) = 2q$, then as $(2/p) = -1$, we use the same reasoning as before and easily see that 2 has order $(p-1)$ mod p in this case. If $(p-1) = 2q_1q_2$, then the order of 2 (mod p) is either $2q_1$, $2q_2$, or $2q_1q_2$. If the order of 2 (mod p) is $2q_1$, then $p|(2^{2q_1}-1)$ and hence

$$p \left| \prod_{a<2x^{\frac{1}{2}-\delta}} (2^a - 1) \right. . \tag{1}$$

Using Lemma 1, we see that the number of primes $p \leq x$ satisfying (1) cannot exceed

$$\sum_{a<2x^{\frac{1}{2}-\delta}} a \leq 4x^{1-2\delta}.$$

Therefore, we have at least

$$\frac{cx}{\log^2 x} - 4x^{1-2\delta}$$

primes $p \leq x$ such that $(p-1) = 2q$ or $(p-1) = 2q_1q_2$ where the order of 2 (mod p) is either $2q_2$ or $(p-1)$.

Among these primes, let us consider the order of 3 (mod p). If the order is $2q_1$, then, as above, we have that

$$p \left| \prod_{a<2x^{\frac{1}{2}-\delta}} (3^a - 1) \right. ,$$

and the number of such primes cannot exceed

$$\sum_{a<2x^{\frac{1}{2}-\delta}} \left(\frac{\log 3}{\log 2}\right) a \leq \left(\frac{\log 3}{\log 2}\right) 4x^{1-2\delta}.$$

Similarly, the number of primes p for which the order of 5 (mod p) is $2q_1$ cannot exceed

$$\sum_{a<2x^{\frac{1}{2}-\delta}} \left(\frac{\log 5}{\log 2}\right) a \leq \left(\frac{\log 5}{\log 2}\right) 4x^{1-2\delta}.$$

Therefore, we have at least

$$\frac{cx}{\log^2 x} - O(x^{1-2\delta})$$

primes $p \leq x$ such that the order of 2, 3, and 5 (mod p) is one of $2q_2$ or $(p-1)$.

We now show that there are infinitely many primes p such that one of 2, 3, 5 is a primitive root mod p. If not, then 2, 3, and 5 generate a subgroup of order $2q_2$ (mod p). Observe that

$$2q_2 = \frac{p-1}{q_1} < \frac{x}{x^{0.26}} = x^{0.74} = z.$$

Notice that if the numbers in the set

$$\{2^a 3^b 5^c,\ 0 \le a, b, c \le x^\alpha\}, \quad \alpha = 0.247$$

are all distinct, they generate a subgroup of size $x^{3\alpha}$. This is clearly a contradiction, since $3\alpha = 0.741 \Rightarrow x^{3\alpha} > z$. Hence, for some a, b, c and a', b', c', we have that

$$2^a 3^b 5^c \equiv 2^{a'} 3^{b'} 5^{c'} \pmod{p}$$

which implies that

$$2^{a-a'} 3^{b-b'} 5^{c-c'} \equiv 1 \pmod{p}.$$

Thus, p divides the numerator of

$$\prod_{0 \le |a|, |b|, |c| \le 2x^\alpha} (2^a 3^b 5^c - 1). \tag{2}$$

Observe that if e_i, $1 \le i \le r$ are integers then the numerator of

$$\prod_{i=1}^{r} p_i^{e_i} - 1$$

is

$$\prod_{e_i > 0} p_i^{e_i} - \prod_{e_i < 0} p_i^{-e_i}.$$

Thus, for a given triple a, b, c in the product from (2), the numerator can have at most $O(x^\alpha)$ prime factors.

The number of such primes is $O(x^{4\alpha})$, which is $o(\frac{x}{\log^2 x})$, since $4\alpha < 1$. Hence, one of 2, 3, or 5 is a primitive root (mod p) for these primes.

3 Sifting Function for Primitive Roots

In this section, we will use the Ramanujan sum and Theorem 272 from Hardy and Wright [HW, p. 238]. The Ramanujan sum is defined as:

$$c_d(j) = \sum_{\substack{1 \le k \le d \\ (k,d)=1}} e^{\frac{2\pi i k j}{d}}.$$

Theorem 272 states that

$$c_d(j) = \frac{\mu(\frac{d}{a})\phi(d)}{\phi(\frac{d}{a})}, \quad \text{where } a = (d, j).$$

With these tools at our disposal, we will prove the following lemma:

Lemma: *Let G be a cyclic group of order n. Let*

$$f(g) = \frac{\phi(n)}{n}\left\{1 + \sum_{\substack{d|n \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord } \chi = d} \chi(g)\right\}$$

where the inner sum runs over characters χ of G which are of order d. Then

$$f(g) = \begin{cases} 1, & \text{if } g \text{ generates } G \\ 0, & \text{otherwise.} \end{cases}$$

Proof: Let ε be a generator of G. Let $g = \varepsilon^j$. Then g generates G if and only if $(j, n) = 1$. Notice that if $\Psi(\varepsilon) = e^{\frac{2\pi i}{n}}$, then $\Psi^{\frac{n}{d}}$ is a character of order d. In fact, all of the characters of order d are given by $\Psi^{\frac{n}{d}k}$, where $(k, d) = 1$ and $1 \leq k \leq d$. Then

$$\begin{aligned} f(g) &= \frac{\phi(n)}{n}\left\{1 + \sum_{\substack{d|n \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord } \chi = d} \chi(g)\right\} \\ &= \frac{\phi(n)}{n}\left\{1 + \sum_{\substack{d|n \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\substack{1 \leq k \leq d \\ (k,d)=1}} \Psi^{\frac{n}{d}k}(\varepsilon^j)\right\} \\ &= \frac{\phi(n)}{n}\left\{1 + \sum_{\substack{d|n \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\substack{1 \leq k \leq d \\ (k,d)=1}} \Psi(\varepsilon)^{\frac{nkj}{d}}\right\} \\ &= \frac{\phi(n)}{n}\left\{1 + \sum_{\substack{d|n \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\substack{1 \leq k \leq d \\ (k,d)=1}} e^{\frac{2\pi i k j}{d}}\right\} \\ &= \frac{\phi(n)}{n}\left\{1 + \sum_{\substack{d|n \\ d>1}} \frac{\mu(d)}{\phi(d)} c_d(j)\right\} \end{aligned}$$

Notice that

$$\frac{\mu(1)}{\phi(1)} c_1(j) = 1.$$

We can use this fact to rewrite $f(g)$ more elegantly as

$$\frac{\phi(n)}{n}\left\{\sum_{d|n} \frac{\mu(d)}{\phi(d)} c_d(j)\right\}.$$

Now, we apply Theorem 272 to see that

$$\begin{aligned} f(g) &= \frac{\phi(n)}{n}\left\{\sum_{d|n}\frac{\mu(d)}{\phi(d)}\frac{\mu(\frac{d}{(d,j)})\phi(d)}{\phi(\frac{d}{(d,j)})}\right\} \\ &= \frac{\phi(n)}{n}\left\{\sum_{d|n}\frac{\mu(d)\mu(\frac{d}{(d,j)})}{\phi(\frac{d}{(d,j)})}\right\} \end{aligned}$$

Notice that

$$g = \varepsilon^j \text{ generates } G \Longrightarrow (j,n) = 1 \Longrightarrow (j,d) = 1 \ \forall\, d|n.$$

So, let g generate G. We now have that

$$f(g) = \frac{\phi(n)}{n}\sum_{d|n}\frac{\mu^2(d)}{\phi(d)}.$$

Since both μ and ϕ are multiplicative functions, then $\frac{\mu^2}{\phi}$ is also a multiplicative function. So, when g generates G, we have

$$\begin{aligned} f(g) &= \frac{\phi(n)}{n}\left(\prod_{p|n}\left(1+\frac{1}{p-1}\right)\right) \\ &= \frac{\phi(n)}{n}\left(\prod_{p|n}\frac{p}{p-1}\right) \\ &= \left(\prod_{p|n}\left(1-\frac{1}{p}\right)\right)\left(\prod_{p|n}\frac{p}{p-1}\right) \\ &= \left(\prod_{p|n}\frac{p-1}{p}\right)\left(\prod_{p|n}\frac{p}{p-1}\right) \\ &= 1 \end{aligned}$$

So, when g generates G, $f(g) = 1$.

Now, let's consider the case when g does not generate G. So, let $(j,n) = \delta, \delta > 1$. Then $n = \delta t$. Observe also that $(j,t) = 1$ and $(\delta,t) = 1$, since $\delta | j$. We look at

$$\frac{\phi(n)}{n}\left\{\sum_{d|n}\frac{\mu(d)\mu(\frac{d}{(d,j)})}{\phi(\frac{d}{(d,j)})}\right\}$$

Since $(\delta, t) = 1$ and $d|n$, we have that $d = (d, \delta)(d, t)$. Let $(d, \delta) = d_1$ and $(d, t) = d_2$ so that $d = d_1 d_2$. Now, we can rewrite the above expression as

$$\frac{\phi(n)}{n}\left\{\sum_{\substack{d_1|\delta \\ d_2|t}} \frac{\mu(d_1 d_2)\mu(\frac{d_1 d_2}{(d_1 d_2, j)})}{\phi(\frac{d_1 d_2}{(d_1 d_2, j)})}\right\}$$

Observe that since $(j, t) = 1$ and $(d, t) = d_2$, then $(d_2, j) = 1$, which implies that $(d_1 d_2, j) = (d_1, j)$. So, we can again rewrite the expression for $f(g)$ as

$$\frac{\phi(n)}{n}\left\{\sum_{\substack{d_1|\delta \\ d_2|t}} \frac{\mu(d_1 d_2)\mu(\frac{d_1 d_2}{(d_1, j)})}{\phi(\frac{d_1 d_2}{(d_1, j)})}\right\}$$

Using the facts that μ and ϕ are multiplicative, and that $(d_1, d_2) = 1$, we obtain

$$\begin{aligned} f(g) &= \frac{\phi(n)}{n}\left\{\sum_{\substack{d_1|\delta \\ d_2|t}} \frac{\mu(d_1)\mu(d_2)\mu(\frac{d_1}{(d_1, j)})\mu(d_2)}{\phi(\frac{d_1}{(d_1, j)})\phi(d_2)}\right\} \\ &= \frac{\phi(n)}{n}\left(\sum_{d_1|\delta} \frac{\mu(d_1)\mu(\frac{d_1}{(d_1, j)})}{\phi(\frac{d_1}{(d_1, j)})}\right)\left(\sum_{d_2|t} \frac{\mu^2(d_2)}{\phi(d_2)}\right) \\ &= \frac{\phi(n)}{n}\left(\sum_{d_1|\delta} \frac{\mu(d_1)\mu(\frac{d_1}{(d_1, j)})}{\phi(\frac{d_1}{(d_1, j)})}\right)\left(\frac{t}{\phi(t)}\right) \end{aligned}$$

But since $(j, n) = \delta$, and $(d, \delta) = d_1$, then $(d_1, j) = d_1$. So we have

$$\begin{aligned} f(g) &= \frac{\phi(n)}{n}\left(\sum_{d_1|\delta} \mu(d_1)\right)\frac{t}{\phi(t)} \\ &= 0, \quad \text{since } \delta > 1. \text{ (See [IR, p. 19])} \end{aligned}$$

So, we have shown that

$$f(g) = \begin{cases} 1, & \text{if } g \text{ generates } G \\ 0, & \text{otherwise.} \end{cases}$$

□

4 Reformulation and Solution of the Problem

Let $\mathbf{F}_q$ be a finite field with $q = p^n$ elements. Consider the polynomial ring $\mathbf{F}_p[x]$. Let $a(x)$ be a polynomial in $\mathbf{F}_p[x]$. We would like to know the number of irreducible polynomials

$p(x) \in \mathbf{F}_p[x]$ such that $a(x)$ generates $(\mathbf{F}_p[x]/(p(x)))^*$. Recall that if $\deg p(x) = n$ then

$$\mathbf{F}_p[x]/(p(x)) \simeq \mathbf{F}_{p^n}$$

Moreover, $\mathbf{F}_{p^n}^*$ is cyclic of order $p^n - 1$. Also recall that the isomorphism $\mathbf{F}_p[x]/(p(x)) \simeq \mathbf{F}_{p^n}$ is given explicitly as follows: for $g(x) \in \mathbf{F}_p[x]$, we write

$$g(x) = p(x)q(x) + r(x), \quad \text{with } r(x) = 0 \text{ or } 0 \leq \deg r < \deg p = n.$$

Let $\theta \in \mathbf{F}_{p^n}$ be a root of $p(x)$. Then

$$g(\theta) = r(\theta) = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}, \ a_i \in \mathbf{F}_p$$

describes all the elements of $\mathbf{F}_{p^n}$. Thus, $a(x)$ generating $(\mathbf{F}_p[x]/(p(x)))^*$ is equivalent to $a(\theta)$ generating $\mathbf{F}_{p^n}^*$.

Hence, to count the number of irreducible $p(x)$ of degree n for which $a(x)$ is a generator is tantamount to counting the number of θ of degree n for which $a(\theta)$ generates $\mathbf{F}_{p^n}^*$. Indeed, since each $p(x)$ has n roots, we find

$$\begin{aligned}&\#\{p(x) \in \mathbf{F}_p[x] : p(x) \text{ irreducible, } \deg p = n, \ a(x) \text{ generates } (\mathbf{F}_p[x]/(p(x)))^*\} \\ &\quad = \frac{1}{n}\#\{\theta \in \mathbf{F}_{p^n} : \deg\theta = n, \ a(\theta) \text{ generates } \mathbf{F}_{p^n}^*\}\end{aligned}$$

We now apply the lemma of section 3 to see that the number in question is:

$$\begin{aligned}\frac{1}{n}\sum_{\substack{\theta\in\mathbf{F}_{p^n}\\ \deg\theta=n}} f(a(\theta)) &= \frac{1}{n}\sum_{\substack{\theta\in\mathbf{F}_{p^n}\\ \deg\theta=n}}\left(\frac{\phi(p^n-1)}{p^n-1}\left(1+\sum_{\substack{d\mid p^n-1\\ d>1}}\frac{\mu(d)}{\phi(d)}\sum_{\text{ord }\chi=d}\chi(a(\theta))\right)\right) \\ &= \frac{1}{n}\sum_{\substack{\theta\in\mathbf{F}_{p^n}\\ \deg\theta=n}}\left(\frac{\phi(p^n-1)}{p^n-1}+\frac{\phi(p^n-1)}{p^n-1}\sum_{\substack{d\mid p^n-1\\ d>1}}\frac{\mu(d)}{\phi(d)}\sum_{\text{ord }\chi=d}\chi(a(\theta))\right) \\ &= \frac{1}{n}\sum_{\substack{\theta\in\mathbf{F}_{p^n}\\ \deg\theta=n}}\frac{\phi(p^n-1)}{p^n-1}+\frac{1}{n}\sum_{\substack{\theta\in\mathbf{F}_{p^n}\\ \deg\theta=n}}\frac{\phi(p^n-1)}{p^n-1}\sum_{\substack{d\mid p^n-1\\ d>1}}\frac{\mu(d)}{\phi(d)} \\ &\quad \sum_{\text{ord }\chi=d}\chi(a(\theta))\end{aligned}$$

So, the contribution from the main term (the first term in the expression above) is

$$\frac{p^n - p^{n-1}}{n} \cdot \frac{\phi(p^n-1)}{p^n-1}.$$

and the error term is

$$\frac{\phi(p^n-1)}{n(p^n-1)}\sum_{\substack{d\mid p^n-1\\ d>1}}\frac{\mu(d)}{\phi(d)}\sum_{\text{ord }\chi=d}\sum_{\substack{\theta\in\mathbf{F}_{p^n}\\ \deg\theta=n}}\chi(a(\theta)).$$

We will show in the following sections that when $d > 1$, and $a(x)$ is of the form $x^m + c$, the sum

$$\left| \sum_{\substack{\theta \in \mathbf{F}_{p^n} \\ \deg \theta = n}} \chi(a(\theta)) \right| \leq m p^{\frac{n}{2}} \tag{3}$$

Hence, the contribution from the error term is $O(p^{\frac{n}{2}}\delta(p^n - 1))$, where $\delta(u)$ is the number of divisors of u.

The estimate in (3) is a consequence of A. Weil's celebrated work proving the analogue of the Riemann hypothesis for zeta functions over finite fields. However, one can also obtain this estimate in a more elementary manner using Gauss sums. In section 5, we recount some of the theory of Gauss sums over finite fields. Then, in section 6, we use that theory to obtain the estimate in (3).

Once we justify this estimate, it is clear that we have proven the function field analogue of Artin's conjecture in the special case where $a(x) = x^m + c$. To see this, notice that in our expression for the number of irreducible $p(x)$ of degree n such that $a(x)$ generates $(\mathbf{F}_p[x]/(p(x)))^*$, the contribution from the main term far outweighs the contribution from the error term.

5 Gauss Sums Over Finite Fields

In this section, we review some basic properties of Gauss sums over finite fields. All of this can be found in Davenport[D].

Let p be prime and consider the finite field $\mathbf{F}_{p^n}$. Let

$$e(\alpha) = \exp\left(\frac{2\pi i}{p} \mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(\alpha)\right), \quad \text{for } \alpha \in \mathbf{F}_{p^n}.$$

Let χ be a character of $\mathbf{F}_{p^n}^*$. The Gauss sum is defined as

$$\tau(\chi) = \sum_{\alpha \in \mathbf{F}_{p^n}^*} \chi(\alpha) e(\alpha)$$

Observe that for any $\eta \neq 0$,

$$\chi(\eta)\tau(\overline{\chi}) = \sum_{\alpha \in \mathbf{F}_{p^n}^*} \overline{\chi}(\alpha)\chi(\eta) e(\alpha)$$

If we make the change of variables $\alpha = \eta\beta$, we have that

$$\chi(\eta)\tau(\overline{\chi}) = \sum_{\beta \in \mathbf{F}_{p^n}^*} \chi(\beta) e(\eta\beta)$$

since $\overline{\chi}(\eta)\chi(\eta) = |\chi(\eta)|^2 = 1$ and as β ranges over elements of $\mathbf{F}_{p^n}^*$, so does $\eta\beta$.

Theorem: $|\tau(\chi)| = p^{n/2}$, *for all non-trivial characters* χ.

Proof: If $\chi \neq \chi_0$ (the principal character), then

$$|\tau(\chi)|^2 = \sum_{\alpha,\beta \in \mathbf{F}_{p^n}^*} \chi(\alpha)\overline{\chi}(\beta)e(\alpha - \beta)$$

We set $\alpha = \beta\gamma$. Then we have that

$$|\tau(\chi)|^2 = \sum_{\gamma,\beta \in \mathbf{F}_{p^n}^*} \chi(\gamma)e(\beta(\gamma - 1)).$$

Notice that if $w_1, \ldots, w_n$ is an $\mathbf{F}_p$-basis of $\mathbf{F}_{p^n}$, then

$$\begin{aligned}\sum_{\beta \in \mathbf{F}_{p^n}} e(\beta) &= \sum_{a_1,\ldots,a_n \in \mathbf{F}_p} e(a_1 w_1 + \cdots + a_n w_n) \\ &= \prod_{j=1}^{n} \left(\sum_{a_j \in \mathbf{F}_p} e(a_j w_j) \right).\end{aligned}$$

Since

$$\begin{aligned}\sum_{a_j \in \mathbf{F}_p} e(a_j w_j) &= \sum_{a_j=0}^{p-1} \exp\left(\frac{2\pi i a_j \mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(w_j)}{p}\right) \\ &= \begin{cases} p, & \text{if } \mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(w_j) = 0 \\ 0, & \text{otherwise.} \end{cases}\end{aligned}$$

we have that

$$\sum_{\beta \in \mathbf{F}_{p^n}} e(\beta) = \begin{cases} p^n, & \text{if } \mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(w_1) = \cdots = \mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(w_n) = 0 \\ 0, & \text{otherwise.} \end{cases}$$

In the first case, we deduce that

$$\mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(\eta) = 0 \quad \forall \eta \in \mathbf{F}_{p^n}.$$

In particular, if $1, \theta, \theta^2, \ldots, \theta^{n-1}$ is a basis, we find that

$$\begin{aligned}0 = a_{ij} &= \mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(\theta^{i+j}) \\ &= \sum_{k=1}^{n} \theta^{(k)i}\theta^{(k)j}\end{aligned}$$

and $\theta^{(1)}, \ldots, \theta^{(n)}$ are the conjugates of θ. The above equation can be rewritten as $\Omega\Omega^T = 0$, where $\Omega = (\theta^{(j)i})$ is a Vandermonde matrix. However, this is a contradiction since $\theta^{(1)}, \ldots, \theta^{(n)}$ are all distinct, which implies that $\det \Omega \neq 0$.

So, we have that

$$\sum_{\beta \in \mathbf{F}_{p^n}} e(\beta) = 0.$$

Now, if $\gamma \neq 1$, then

$$\sum_{\beta \in \mathbf{F}_{p^n}^*} e(\beta(\gamma - 1)) = -1.$$

If $\gamma = 1$, then

$$\sum_{\beta \in \mathbf{F}_{p^n}^*} e(\beta(\gamma - 1)) = p^n - 1.$$

Thus we have that

$$\begin{aligned} |\tau(\chi)|^2 &= p^n - 1 + (-1) \sum_{\substack{\gamma \neq 1 \\ \gamma \in \mathbf{F}_{p^n}^*}} \chi(\gamma) \\ &= (p^n - 1) + (-1)(-1), \quad \text{since } \chi \text{ is non-trivial} \\ &= p^n \end{aligned}$$

So we have shown that $|\tau(\chi)| = p^{\frac{n}{2}}$, for all non-trivial characters χ. □

6 Estimation

We will estimate

$$\sum_{\theta \in \mathbf{F}_{p^n}} \chi(a(\theta))$$

when $a(x) = x^m + c$. For this purpose, we can rewrite the above as

$$\sum_{\theta \in \mathbf{F}_{p^n}} \chi(\theta^m + c).$$

If $(m, p^n - 1) = 1$, then $\theta \mapsto \theta^m$ is an isomorphism, and the sum becomes

$$\sum_{\theta \in \mathbf{F}_{p^n}} \chi(\theta + c) = 0.$$

If $(m, p^n - 1) = t > 1$, then write $m = ts$. Then, $(s, p^n - 1) = 1$, and by the same reasoning,

$$\sum_{\theta \in \mathbf{F}_{p^n}} \chi(\theta^m + c) = \sum_{\theta \in \mathbf{F}_{p^n}} \chi(\theta^t + c). \tag{4}$$

Since $t|(p^n-1)$, let Ψ be a character of $\mathbf{F}_{p^n}^*$ of order t. Then

$$\frac{1}{t}\sum_{i=0}^{t-1}\Psi^i(\alpha)=\begin{cases}1, & \text{if } \alpha=\theta^t \text{ for some } \theta\\ 0, & \text{otherwise.}\end{cases}$$

Putting this in expression (4) gives

$$\begin{aligned}\sum_{\theta\in\mathbf{F}_{p^n}}\chi(\theta^t+c) &= t\sum_{\alpha\in\mathbf{F}_{p^n}}\chi(\alpha+c)\,\frac{1}{t}\sum_{i=0}^{t-1}\Psi^i(\alpha)\\ &= \sum_{i=0}^{t-1}\sum_{\alpha\in\mathbf{F}_{p^n}}\chi(\alpha+c)\Psi^i(\alpha)\end{aligned}$$

Now, we use Gauss sums to replace $\chi(\alpha+c)$ as follows:

$$\chi(\alpha+c)=\frac{1}{\tau(\overline{\chi})}\sum_{\beta\in\mathbf{F}_{p^n}^*}\overline{\chi}(\beta)e(\beta(\alpha+c)).$$

Thus interpreting $\chi(0)$ as zero, we have

$$\begin{aligned}\sum_{\alpha\in\mathbf{F}_{p^n}}\Psi^i(\alpha)\chi(\alpha+c) &= \frac{1}{\tau(\overline{\chi})}\sum_{\alpha\in\mathbf{F}_{p^n}}\Psi^i(\alpha)\sum_{\beta\in\mathbf{F}_{p^n}}\overline{\chi}(\beta)e(\beta(\alpha+c))\\ &= \frac{1}{\tau(\overline{\chi})}\sum_{\beta\in\mathbf{F}_{p^n}}\overline{\chi}(\beta)e(\beta c)\overbrace{\sum_{\alpha\in\mathbf{F}_{p^n}}\Psi^i(\alpha)e(\beta\alpha)}^{\text{also a Gauss sum}}\\ &= \frac{1}{\tau(\overline{\chi})}\sum_{\beta\in\mathbf{F}_{p^n}}\overline{\chi}(\beta)e(\beta c)\overline{\Psi}^i(\beta)\tau(\Psi^i)\\ &= \frac{\tau(\Psi^i)}{\tau(\overline{\chi})}\sum_{\beta\in\mathbf{F}_{p^n}}\overline{\chi}(\beta)\overline{\Psi}^i(\beta)e(\beta c)\end{aligned}$$

Observe that

$$\tau(\overline{\chi})\chi(n)=\sum_{\alpha\in\mathbf{F}_{p^n}}\overline{\chi}(\alpha)e(\alpha n).$$

So we have that

$$\sum_{\alpha\in\mathbf{F}_{p^n}}\Psi^i(\alpha)\chi(\alpha+c)=\frac{\tau(\Psi^i)}{\tau(\overline{\chi})}\tau(\overline{\chi\Psi^i})\chi(c).$$

Now, since $\chi, \overline{\chi}, \Psi^i, \overline{\Psi}^i$ are non-trivial characters, we apply the theorem of section 5 to see that

$$\left|\sum_{\alpha\in\mathbf{F}_{p^n}} \Psi^i(\alpha)\chi(\alpha+c)\right| = p^{n/2}.$$

Now, we conclude by showing that when $(m, p^n-1) = t > 1$

$$\begin{aligned}\left|\sum_{\theta\in\mathbf{F}_{p^n}} \chi(\theta^m+c)\right| &= \left|\sum_{\theta\in\mathbf{F}_{p^n}} \chi(\theta^t+c)\right| \\ &= \left|\sum_{i=0}^{t-1}\sum_{\alpha\in\mathbf{F}_{p^n}} \Psi^i(\alpha)\chi(\alpha+c)\right| \\ &\le \sum_{i=0}^{t-1}\left|\sum_{\alpha\in\mathbf{F}_{p^n}} \Psi^i(\alpha)\chi(\alpha+c)\right| \\ &\le \sum_{i=0}^{t-1} p^{\frac{n}{2}} \\ &\le mp^{\frac{n}{2}}.\end{aligned}$$

Thus, for all m and c, we have that

$$\left|\sum_{\theta\in\mathbf{F}_{p^n}} \chi(\theta^m+c)\right| \le mp^{\frac{n}{2}}.$$

References

[1] E. Artin, *Collected Papers.* Addison-Wesley, 1965.

[2] H. Bilharz, Primdivisoren mit vorgeberger Primitivwurzel. *Math. Annalen* **114** (1937), 476–492.

[3] E. Bombieri, Friedlander, J. and Iwaniec, H., Primes in arithmetic progressions to large moduli. *Acta Math.* **370** (1986), 203–251.

[4] H. Davenport, On Primitive Roots in Finite Fields. *Quart. J. Math.* (2) **8** (1937), 308–312. (See also *Collected Papers*, vol. 4, p. 1557–1561.)

[5] R. Gupta and Ram Murty, M., A remark on Artin's conjecture. *Invent. Math.* **101** (1990), 225–235.

[6] R. Gupta, Ram Murty, M. and Kumar Murty, V., The Euclidean algorithm for S-integers. In *Number Theory*, 189–201 (H. Kisilevsky and J. Labute, eds.). (Canadian Mathematical Society Conference Proceedings 7) (1987).

[7] C. Hooley, On Artin's conjecture. *J. Reine. Angew. Math.* **225** (1967), 209–220.

[8] D.R. Heath-Brown, Artin's conjecture for primitive roots. *Quart. J. Math. Oxford* (2) **37** (1986), 27–38.

[9] G.H. Hardy and Wright, E.M., *An Introduction to the Theory of Numbers*, 5th ed. Oxford University Press, 1979.

[10] K. Ireland and Rosen, M., *A Classical Introduction to Modern Number Theory.* Springer-Verlag, 1982.

[11] D. Lorenzini, *An Invitation to Arithmetic Geometry*, vol. 9. Graduate Studies in Mathematics, American Math Society, 1996, pp. 354–360.

[12] M. Ram Murty, Artin's conjecture and elliptic analogues. In *Sieve Methods, Exponential Sums, and their Applications in Number Theory*, 325–344. (G.R.H. Greaves, G. Harman, and M.N. Huxley, eds.). Cambridge University Press, 1996.

[13] M. Ram Murty, Artin's conjecture for primitive roots. *Math. Intelligencer* **10** (1988), 59–67.

Department of Mathematics
Queen's University
Kingston, Ontario
K7L 3N6, Canada
E-Mail: murty@mast.queensu.ca