university of groningen / faculty of science and engineering / mathematics and applied mathematics

Prime Polynomials over Finite Fields and Chebyshev's Bias

Bachelor's Project Mathematics

July 2017

Student: S. Taams

First supervisor: Prof. dr. J. Top

Second assessor: Dr. M.C. Kronberg

1 Abstract

This thesis serves as an introduction to number theory of polynomial rings over finite fields. We give several classic and modern proofs for the prime number theorem for polynomials. As an extension we prove the analogue of Dirichlet's theorem using Dirichlet L-series. We provide an asymptotic formula for the bias of the primes towards any residue class modulo some polynomial, called the Chebyshev's bias. Finally we give an asymptotic formula for the bias towards quadratic residues versus quadratic non-residues. Assuming the generalized Riemann hypothesis and the grand simplicity hypothesis Rubinstein and Sarnak proved in [RS94] that for integers this bias is always towards the non-residues. We prove a similar result, however the GSH can be falsified in specific cases. We provide examples where it fails and give an example where the bias is towards the squares.

2 Introduction

This thesis is concerned with the number of monic irreducible polynomials over a finite field $\mathbb{F}_q$. We can and will make this question formal in many different ways, the first of which is perhaps the most obvious and also has a very famous proof.

Theorem 2.1. *There are infinitely many monic irreducible polynomials in* $\mathbb{F}_q[T]$.

Proof. Assume there are finitely many monic irreducible polynomials $\{P_1, \cdots, P_n\}$. Then consider the polynomial $N = 1 + \prod_{i=1}^{n} P_i$, it cannot be irreducible, since it is monic and has bigger degree then any of the P_i. Also it cannot be a unit since $\deg(N) = \sum \deg P_i \geq \deg T = 1$ and the only units are those with degree 0. The only other option is that it is reducible. Because $\mathbb{F}_q[T]$ is a unique factorization domain, this means that for some unit u we can write $N = uP_1^{e_1} \cdots P_n^{e_n}$ with $e_n \in \mathbb{N}$. Finally this implies that for some P_i we have $P_i | 1 + \prod_{i=1}^{n} P_i$ i.e. $P_i | 1$. This is a contradiction and we conclude that there are in fact infinitely many prime numbers. ☺

This proof is an exact copy of Euclid's proof to show that there are infinitely many prime numbers! These two problems are so closely related because both the integers and the polynomial ring $\mathbb{F}_q[T]$ are a unique factorization domain, this of course means that being prime and being irreducible is the same thing. Moreover they are Euclidean domains, which lets us compare "size" of numbers and polynomials via there absolute value and degree respectively. It turns out this key similarity creates fascinating analogues far beyond this elementary proof.

The original question could be seen as an algebraic one, but we will not use much more than knowledge of what a unique factorisation ring is. Rather we will take an analytic perspective of these problems as the area of analysis lends itself perfectly for counting and analysing general behaviour. We will need techniques like logarithmic derivatives, comparing coefficients of power series, big O notation, little o notation. Furthermore we will use a few elementary number theoretical concepts like Möbius inversion and Euler products. These concepts are explained for example on Wikipedia or in the lecture notes [ES16]. We will not spend a lot of time explaining these concepts within this text, so it is recommended to have at least some idea of these things beforehand.

This is of course not all of the story, for the more initiated people polynomials over finite fields are intricately connected with algebraic geometry. The results from this thesis can, and maybe should, be interpreted from this viewpoint as well. However to keep this within the scope of a Bachelor's thesis most of this is omitted and we will at a few points have to trust on a result of Weil, the Riemann hypothesis for curves over finite fields. This is a little bit unfortunate but I hope the reader will not be to distracted by the few (but vitally important) instances where this is used.

Throughout the chapters we will state and prove three, each depending on the previous, main theorems about counting specific classes of irreducible polynomials. The first one will be an explicit formula for the number of monic irreducible polynomials of a fixed degree. This formula turns out to be very similar to the formula for the number of prime numbers up to a given size. For this we will show several proofs dating back to Gauss and Euler and two modern ones. Next we will investigate how these monic irreducibles (of a fixed degree) distribute themselves over the residue classes modulo some polynomial. For example we might ask what fraction of monic irreducible polynomials of degree 2 are of the form $x^2 + \alpha x + 1$, which is the same as looking at the residue class $1 \mod x$. As it turns out every residue class that can have more then one monic irreducible will have roughly the same amount as all the others. This is the direct analogue of Dirichlet's theorem for prime numbers. For Dirichlet's theorem we will follow the book [Ros02].

As it turns out the errors that we estimate for Dirichlet's theorem contain a lot of structure within them. In fact under certain circumstances there are residue classes that will always have more primes then some of the others, no matter the degree. This phenomenon was first observed by Chebyshev for the integers where he looked at the primes that are $1 \mod 4$ and $3 \mod 4$. If we look at all the primes that are less then n then it turns out that 3 is usually ahead, but every now and again 1 takes over again. Under some very likely hypotheses regarding zeros of the Dirichlet-L functions M. Rubinstein and P. Sarnak proved [RS94] that usually the quadratic residues are behind on the quadratic non-residues, however the quadratic residues take over the lead every now and again. This is a case where the analogy breaks down a little bit, because there are cases where the quadratic residues are usually ahead of the non-residues and also cases where the non-residues are ahead forever and never get taken over. The polynomial case was adapted in [Cha08] by closely following [RS94].

As one might expect this is only one of the many directions one can take when counting irreducible polynomials, many of the standard questions have been investigated. One of the hypotheses for prime numbers is the infamous hypothesis H. This conjecture is an extreme generalization of many number theoretical problems about the existence (and number) of primes in the image of polynomials. For example Dirichlet's theorem is a specific case in which we only look at a single degree 1 polynomial. However we know barely anything beyond this degree 1 case for integers. Another specific case is the existence of twin primes, for which there exists no proof in the integer case. Beyond Dirichlet's theorem and the recent results of Maynard 2013 on twin primes not much more is known. If we try to write an analogue to this conjecture in the polynomial rings, the validity of the conjecture depends crucially on how we state the theorem. This is worked out for example in [Pol06] and in a paper [CCG08] the first proving the theorem in a specific case and the second providing counter examples in a more general setting. The above questions can be phrased in the form "is this thing prime?". Another very standard type of number theory question would be "can we write this thing in the following

form?" The question of if we can write a number as the sum of 9 cubes is what got Hardy and Littlewood to invent the circle method and it is not surprising that proofs of these kind of theorems depend on an adaptation of the circle method. An example of a problem in this spirit is an analogue to the (weak) Goldbach conjecture [Hay66].

There are of course many more interesting problems to consider that can be found for example in the review paper [Rud15]. Another good starting point to read would be the PhD thesis [Pol08]. It should be stated that theorems over polynomial rings are usually easier to prove then their integer counterparts. From my personal experience this seems to flow from the fact that degree is a nicer notion of size then absolute value. A more experienced mathematician might say that it is because the L series for polynomials have finitely many zeros instead of the infinitely many of the integer case [Ros02]. Interestingly enough in the days of Gauss and Euler this meant that a lot of results where proven for polynomials before they where proven for integers. One of the motivations for studying polynomials rings could therefore be that they might be a stepping stone for attacking the more prestigious results within integers. However in recent years results are sometimes proven for integers and then the methods are later adapted to work for the polynomial case.

3 The prime number theorem

One of the most celebrated results in number theory is the prime number theorem. This theorem gives an asymptotic formula for the number of primes up to a given constant. As it turns out even for weak error terms this theorem is very hard to prove, and the best error terms all rely on the (unproven) Riemann hypothesis. However in our setting of polynomials we are more fortunate and very elementary proofs of the analogous result are known. We will proceed with stating our PNT and then we will give several different proofs, starting with some very elegant modern proofs and ending with the classical proofs by Gauss and Euler.

Definition 3.1. Let $\pi(q, n)$ denote the number of monic irreducible polynomials over $\mathbb{F}_q$ of degree n.

Note that this definition differs slightly from the normal prime counting function in that we count polynomials of degree equal to n rather than up to n.

Theorem 3.2 (PNT)**.** *We can count the number of monic irreducible polynomials as*

$$\pi(q, n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

This gives rise to the following result

Corollary 3.3. *An asymptotic relation for the number of monic irreducible polynomials is*

$$\pi(q, n) = \frac{q^n}{n} + \mathcal{O}\left(\frac{q^{n/2}}{n}\right).$$

Proof. This follows from doing some basic estimates

$$\begin{aligned} \left|\pi(q, n) - \frac{q^n}{n}\right| &= \left|\frac{1}{n} \sum_{\substack{d|n \\ d \geq 2}} \mu(d) q^{n/d}\right|; \\ &\leq \frac{1}{n} \sum_{\substack{d|n \\ d \geq 2}} q^{n/d}. \end{aligned}$$

Now we take out the term with $d = 2$ and there are at most n other terms all of size at most $\frac{q^3}{n}$.

$$\begin{aligned} &\leq \frac{q^{n/2}}{n} + q^{n/3}; \\ &= \mathcal{O}\left(\frac{q^{n/2}}{n}\right). \end{aligned}$$

☺

We briefly explain why this is considered to be the analogue of the prime number theorem. The total number of monic polynomials of degree n is given by $X = q^n$, so if we write the above formula as a density we get

$$\frac{q^n}{n} + \mathcal{O}\left(\frac{q^{n/2}}{n}\right) = \frac{X}{\log_q X} + \mathcal{O}\left(\frac{\sqrt{X}}{\log_q X}\right).$$

This looks very much like the density for primes within the integers.

The first proof of the PNT will rely on some algebraic properties of the field $\mathbb{F}_q$ and its extensions. It is taught in many introductory courses on finite fields.

Proof. Consider the following polynomial

$$Q = \prod_{P:\deg(P)|n} P,$$

where the product is over all the monic irreducible polynomials. We know that the roots of P lie in $\mathbb{F}_{q^{\deg(P)}}$. Also note that any element of $\mathbb{F}_{q^n}$ has a minimal polynomial $f \in \mathbb{F}_q[X]$ with $\deg(f)|n$ and hence is a root of Q. Moreover Q is squarefree by construction, so any zero has multiplicity 1.

Now consider the polynomial

$$R = x^{q^n} - x$$

We see that all elements of $\mathbb{F}_{q^n}$ are a root of this polynomial, because the Frobenius map is $\mathbb{F}_{q^n}$-linear. Also there are q^n elements in $\mathbb{F}_{q^n}$ and q^n roots (with multiplicity) of $x^{q^n} - x$, so these must be all the roots. We conclude that Q and R have the same roots and they must be the same polynomial.

Now we will consider the degree of these polynomials.

$$\begin{aligned}\deg(R) &= \deg \prod_{P:\deg(P)|n} P;\\ q^n &= \sum_{P:\deg(P)|n} \deg(P);\\ &= \sum_{d|n} \pi(q,d)d.\end{aligned}$$

We then use Möbius inversion to conclude

$$\pi(q,n)n = \sum_{d|n} \mu(d) q^{n/d}.$$

This proves the result. ☺

In his thesis [Pol08] P. Pollack suggests an idea for a proof that he got from personal communication with A. Granville, we work out the details here. Similar to the previous proof it is based on computing the degrees of polynomials, but it does not need the theory of field extensions.

Proof. First we notice that

$$nq^n = \sum_{\substack{M \\ \deg(M)=n}} \deg(M),$$

where the sum is over all the monic polynomials. From the unique factorization of a polynomial $M = P_1^{a_1} \cdots P_k^{a_k}$ we see that

$$\deg(M) = \sum_{\substack{P,a \\ P^a|M}} \deg P.$$

Substituting this we obtain

$$nq^n = \sum_{\substack{M \\ \deg(M)=n}} \sum_{\substack{P,a \\ P^a|M}} \deg(P).$$

Since this is just a finite sum we can reverse the order of summation

$$nq^n = \sum_{\substack{P,a \\ a\deg(P)\leq n}} \sum_{\substack{M \\ \deg(M)=n-a\deg(P)}} \deg(P);$$

Then instead of summing over all the P we sum over their degrees d and keep track of how many there are.

$$\begin{aligned} &= \sum_{\substack{d,a \\ ad\leq n}} \pi(q,d)d \sum_{\substack{M \\ \deg(M)=n-ad}} 1; \\ &= \sum_{\substack{d,a \\ ad\leq n}} \pi(q,d)dq^{n-ad}. \end{aligned}$$

Now we divide both sides by q^n.

$$n = \sum_{\substack{d,a \\ ad\leq n}} \pi(q,d)dq^{-ad}.$$

This identity holds for all n, hence we can apply it to $n-1$ and subtract this from the above to obtain

$$\begin{aligned} 1 &= \sum_{\substack{d,a \\ ad=n}} \pi(q,d)dq^{-ad}; \\ q^n &= \sum_{\substack{d,a \\ ad=n}} \pi(q,d)d. \end{aligned}$$

And again applying Möbius inversion gives us the result.

☺

The following argument is due to C.F. Gauss and is probably the first proof of this result. It relies on a combinatorics like argument to count monic polynomials in terms of monic irreducible polynomials.

Proof. We can write every monic polynomial M of degree less than n as a product of α_1 degree 1 polynomials times α_2 degree 2 polynomials, etc. The number of possible monic polynomials is then given below, where the binomial coefficient is the number of ways to pick α_i things with replacement out of a collection with $\pi(q,i)$ elements, where ordering does not matter.

$$q^n = \sum_{\alpha_1+2\alpha_2+\cdots+k\alpha_k \leq n} \prod_{i=1}^{k} \binom{\pi(q,i)+\alpha_i-1}{\alpha_i}$$

We then consider the generating functions for both of these expressions.

$$1+qu+q^2u^2+\ldots = \prod_{j=1}^{\infty}(1+u^j+u^{2j}+\ldots)^{\pi(q,n)};$$
$$\frac{1}{1-qu} = \prod_{j=1}^{\infty}\left(\frac{1}{1-u^j}\right)^{\pi(q,n)}.$$

A standard trick to get the π our of the power is to apply log to the expression, and then differentiate with respect to u to get rid of the logs again. This is exactly what we will do. Applying $u\frac{d}{du}\log$ to both sides gives.

$$\frac{qu}{1-qu} = \sum_{j=1}^{\infty} j\pi(q,j)\frac{u^j}{1-u^j}$$

$$qu+q^2u^2+\ldots = \sum_{j=1}^{\infty} j\pi(q,j)\left(u^j+u^{2j}+\ldots\right)$$

Comparing the coefficients on both sides gives us the familiar formula.

$$q^n = \sum_{d|n} d\pi(q,d)$$

☺

The final proof is due to Euler and, as in the classical case, makes use of the zeta-function.

Definition 3.4. We define the zeta function as

$$\zeta_q(s) = \sum_{M} \frac{1}{|M|^s}.$$

Here the sum is over all the monic polynomials over $\mathbb{F}_q$ and $|M| = q^{\deg(M)}$.

The zeta function converges absolutely whenever $\Re(s) > 1$, because

$$\sum_M \left| \frac{1}{|M|^s} \right| = \sum_{d=0}^{\infty} \left| \frac{q^d}{q^{ds}} \right| = \sum_{d=0}^{\infty} q^{d(1-\Re(s))}.$$

Here we turn the sum into a sum over all the possible degrees.

Proof. Because the sum in $\zeta_q(s)$ converges absolutely for $\Re(s) > 1$ we can write it as an Euler product. Note that the proof of Euler products for polynomials is an exact copy of the regular one. This is because the proof only relies on the unique factorisation property, which both the integers and polynomials over finite fields satisfy.

$$\zeta_q(s) = \prod_P \frac{1}{1 - |P|^{-s}} = \prod_{d=1}^{\infty} \left(\frac{1}{1 - q^{-sd}} \right)^{\pi(q,d)}$$

We can also calculate it in a more straight forward way

$$\zeta_q(s) = \sum_{d=0}^{\infty} q^d \frac{1}{q^{ds}} = \frac{1}{1 - q^{1-s}}$$

Now substituting $u = q^{-s}$ gives us the generating functions of Gauss and the result follows accordingly. ☺

The proof by Euler lends itself to solve different counting problems as well. In [Ros02] Rosen shows how to count the number of square free polynomials and suggests this can be extended for k-th power free polynomials. We will show how to do this.

Definition 3.5. We define the k-th power free indicator function as

$$\delta_k(A) = \begin{cases} 0 & \text{if } P^k | A \text{ for some } P \\ 1 & \text{otherwise} \end{cases}$$

Theorem 3.6. *The number of k-th power free polynomials of degree n is equal to*

$$\sum_{f:\deg(f)=n} \delta_k(f) = q^n(1 - q^k) = \frac{q^n}{\zeta(k)}$$

Proof. Because $\delta_k(A)$ is multiplicative we get the following Euler product

$$\prod_P \left(\sum_{i=0}^{\infty} \frac{\delta_k(P^n)}{|P|^{sn}} \right) = \sum_A \frac{\delta_k(A)}{|A|^s}$$

Now using that $\delta_k(P^i) = 0$ for all $i \geq k$ and 1 otherwise, we get the following relation.

$$\begin{aligned}\prod_P \frac{1-|P|^{-ks}}{1-|P|^{-s}} &= \sum_A \frac{\delta_k(A)}{|A|^s} \\ \frac{\zeta(s)}{\zeta(ks)} &= \sum_{i=0}^{\infty} \left(\sum_{A:\deg(A)=i} \delta_k(A) \right) q^{-is} \\ \frac{1-qu^k}{1-qu} &= \sum_{i=0}^{\infty} \left(\sum_{A:\deg(A)=i} \delta_k(A) \right) u^i\end{aligned}$$

Here we again substitute $u = q^{-s}$ and compare coefficients to see

$$\sum_{A:\deg(A)=i} \delta_k(A) = q^i(1-q^{1-k}).$$

We have seen before that

$$\zeta(k) = \frac{1}{1-q^{1-k}}.$$

So the result follows.

☺

We can also explicitly calculate an analogue to the Mertens function $M(n) = \sum_{k=1}^{n} \mu(k)$, for which we will recycle the notation.

Definition 3.7. The polynomial Möbius function

$$\mu(M) = \begin{cases} 0 & \text{if } P^2|M \\ (-1)^{\#\{P|M\}} & \text{otherwise} \end{cases}$$

Definition 3.8. The Mertens function for Polynomials

$$M(n) = \sum_{M:\deg(M)=n} \mu(M)$$

Theorem 3.9. *We have that*

$$M(n) = \mathcal{O}(q)$$

Proof. Using that μ is a multiplicative function we get an Euler product again

$$\begin{aligned}\sum_A \frac{\mu(A)}{|A|^{-sn}} &= \prod_P \sum_{i=0}^{\infty} \frac{\mu(P^i)}{|P|^{-s}} \\ \sum_{i=0}^{\infty} M(i) q^{-si} &= \prod_P (1-|P|^s) \\ &= \frac{1}{\zeta(s)} \\ &= 1-q^{1-s}\end{aligned}$$

Substitute $u = q^{-s}$ to get

$$\sum_{i=0}^{\infty} M(i)u^i = 1 - qu$$

So we see that

$$M(n) = \begin{cases} 1 \text{ if } n = 0 \\ -q \text{ if } n = 1 \\ 0 \text{ if } n \geq 2 \end{cases}$$

In particular we get the result of the theorem. ☺

4 Dirichlet's Theorem

In the following chapter we will consider an analogue of Dirichlet's theorem or the prime number theorem for arithmetic progressions. The theorem answers questions similar to: "how many irreducible polynomials end in $X+1$." We will first make a few notions formal before giving the precise theorem.

Definition 4.1. Two polynomials are said to be congruent modulo M or $A \equiv B \mod M$ whenever

$$A - B = FM$$

for some $F \in \mathbb{F}_q[X]$. We often write $A \equiv B(M)$ to save some space.

We see that we can restrict M to always be a monic polynomial, since congruence mod M is the same as congruence mod $x \cdot M$ for $x \in \mathbb{F}_q$. We denote the residue class of B as $[B] = \{A \in \mathbb{F}_q[X] : A \equiv B\}$. We will write $\mathbb{F}_q[X]/(M)$ for the set of congruence classes, which is a ring with the appropriate addition and multiplication.

Definition 4.2 (Greatest common divisor)**.** The greatest common divisor, or gcd, of A and B or (A, B) is the monic polynomial of largest degree that divides both A and B. We leave it undefined whenever $A = B = 0$.

The set of congruence classes that satisfy $(A, M) = 1$ is denoted by $(\mathbb{F}_q[X]/(M))^\times$, which is a group under multiplication. This is well defined since the gcd does not depend on which representative we chose for $[A]$. Indeed take $A \equiv B$ then $(A, M) = (A - FM, M) = (B, M)$.

Definition 4.3 (Euler phi)**.** The Euler phi function for polynomials $\Phi(M)$ is the number of residue classes $[A]$ modulo M that satisfy $(A, M) = 1$ i.e. $\#(\mathbb{F}_q/M\mathbb{F}_q)^\times$.

We are now ready to state Dirchlet's theorem.

Theorem 4.4 (Dirichlet's theorem)**.** *The number of monic irreducible polynomials P of degree n of the form $P \equiv A \mod M$ with $(A, M) = 1$, denoted by $\pi(m, A, M)$ is given by*

$$\pi(m, A, M) = \frac{1}{\Phi(M)} \frac{q^n}{n} + \mathcal{O}\left(\frac{q^{n/2}}{n}\right).$$

The restriction $(A, M) = 1$ is a natural one, since $(A, M) | FM + A$ for all F. This means there can be at most one such prime if $(A, M) \neq 1$ and therefore this is not a very interesting case. The theorem basically tells us that the rest of the irreducible polynomials show up in a certain residue class with probability $\frac{1}{\phi(M)}$. Just like you would expect if they were randomly distributed.

Before we can attempt to prove this we will have to develop some theory on Dirichlet characters and so called Dirichlet L-series. This is motivated by the fact that information about the irreducible polynomials was encoded in the zeta function. L-series are a generalization of the zeta function that also encode information about residue classes using so called Dirichlet characters.

Definition 4.5. A Dirichlet character modulo M is a function χ from $\mathbb{F}_q[X]$ to the complex numbers, satisfying

1. $\chi(A + BM) = \chi(A)$ for all A, B.
2. $\chi(A)\chi(B) = \chi(AB)$ for all A, B.
3. $\chi(A) = 0$ if and only if $(A, M) \neq 0$.

If we take $(\chi * \phi)(A) = \chi(A)\phi(A)$ and $\chi^{-1}(A) = \overline{\chi(A)}$ the characters mod M form a group. Also whenever $(A, M) = 1$ we can see that $A^n \equiv A$ for some n, then $\chi(A^n) = \chi(A)^n = \chi(A)$. This means that $|\chi(A)| \in \{0, 1\}$.

Dirichlet characters satisfy the following orthogonality relations.

Theorem 4.6. *Let χ_1 and χ_2 be two Dirichlet characters mod M,*

$$\frac{1}{\Phi(M)} \sum_{A \in \mathbb{F}_q[X]/(M)} \chi_1(A)\overline{\chi_2(A)} = \delta(\chi_1, \chi_2).$$

Let $(A, M) = (B, M) = 1$ then

$$\frac{1}{\Phi(M)} \sum_{\chi} \chi(A)\overline{\chi(B)} = \delta(A, B),$$

where the sum is over all the characters mod M.

Proof. The proof is left as an exercise for the reader. Hint: Whenever $\chi_1 \neq \chi_2$ multiply by $\chi_1(X)\overline{\chi_2(X)} \neq 1$ and use the group structure of $\mathbb{F}_q[X]/(M)$. ☺

Definition 4.7. The Dirichlet L-series of a character χ is

$$L(s, \chi) = \sum_{M} \frac{\chi(M)}{|M|^s},$$

where the sum is over all the monic irreducible polynomials.

Because $|\chi(M)| \leq 1$ we know this sum is dominated by $\zeta_q(s)$ and thus converges absolutely whenever $s > 1$. Since the L-series converges absolutely for $s > 1$ and χ is a multiplicative function we get the Euler product

$$L(s, \chi) = \prod_{P} \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1}. \tag{1}$$

For the trivial character modulo M,

$$\chi_0(A) = \begin{cases} 1 & \text{if } (A, M) = 1 \\ 0 & \text{otherwise} \end{cases},$$

this expression reduces to

$$\prod_{P|M}\left(1-\frac{1}{|P|^s}\right)\zeta_q(s). \tag{2}$$

Here we simply removed the factors in the Euler product of $\zeta_q(s)$ that correspond to $\chi_0(P)=0$.

Theorem 4.8. *For any non-trivial Dirichlet character mod M the L-series $L(s,\chi)$ is a polynomial in q^{-s}, with degree at most* $\deg(M)-1$.

Proof. We define the numbers

$$A(n,\chi)=\sum_{\substack{\text{monic } F\\ deg(F)=n}}\chi(F).$$

Then by substitution we get

$$L(s,\chi)=\sum_{n=0}^{\infty}A(n,\chi)\left(q^{-s}\right)^n.$$

Hence the theorem is equivalent to showing that $A(n,\chi)=0$ for all $n\geq\deg(M)$. We know that any polynomial with degree $n\geq\deg(M)$ can be uniquely written as $F=KM+R$ with $\deg(R)<\deg(M)$ and K a monic polynomial of degree $\deg(M)-\deg(F)$. Also for any K of appropriate degree every single R gives us a polynomial of degree n. (Note that this is not true if $M=0$, but this does not happen because of our assumption.) So the sum becomes

$$A(n,\chi)=\sum_{KM+R}\chi(KM+R)=\sum_K\sum_R\chi(R)=\sum_K 0=0.$$

Because R attains all the residue classes exactly once, the orthogonality relations applied to χ and χ_0 tell us that $\sum_R\chi(R)=\sum_R\chi(R)\overline{\chi_0(R)}=0$. ☺

Here is a quick lemma that will be useful for computing logarithmic derivatives.

Lemma 4.9.

$$u\frac{d}{du}\log\left(1-\alpha u\right)^{-1}=\sum_{k=1}^{\infty}\alpha^k x^k.$$

Proof. This follows from the differentiating the series for log.

$$\log(1-\alpha u)=-\sum_{k=1}^{\infty}\frac{\alpha^k u^k}{k}.$$

☺

We are now ready to prove Dirichlets theorem. Note the similarity between the role of L-series in this proof with that of the zeta function in the proof of the prime number theory.

Proof. From Theorem 4.8 we know that for $\chi \neq \chi_0$ we can write an L series as a polynomial in $q^{-s} = u$. We can then describe this polynomial via a product over its (inverse) roots. Note that $A(0, \chi) = \chi(1) = 1$, so 0 is not a root. Let $m = \deg(M)$.

$$L^*(u, \chi) = \sum_{k=1}^{m-1} a_k(\chi) u^k = \prod_{k=1}^{m-1} (1 - \alpha_k(\chi) u). \tag{3}$$

On the other hand we also know the Euler product for $L(s, \chi)$ as in equation 1. We will regroup the terms in this product depending on their degree, this will let us rewrite it in terms of u.

$$L(s, \chi) = \prod_{P \nmid M} \left(1 - \chi(P)|P|^{-s}\right)^{-1} = \prod_{d=1}^{\infty} \prod_{\substack{P \nmid M \\ \deg(P)=d}} \left(1 - \chi(P) q^{-ds}\right)^{-1}.$$

As promised we get an expression in $u = q^{-s}$.

$$L^*(u, \chi) = \prod_{d=1}^{\infty} \prod_{\substack{P \nmid M \\ \deg(P)=d}} \left(1 - \chi(P) u^d\right)^{-1}. \tag{4}$$

As we have done before we will consider the logarithmic derivatives of these two expressions and compare their coefficients which we will write as $c_n(\chi)$.

$$u \frac{d}{du} \log(L^*(u, \chi)) = \sum_{n=0}^{\infty} c_n(\chi) u^n.$$

First we consider the case of $\chi \neq \chi_0$, using equation 3 and lemma 4.9.

$$\begin{aligned} u \frac{d}{du} \log(L^*(u, \chi)) &= u \frac{d}{du} \log \left(\prod_{k=1}^{m-1} (1 - \alpha_k(\chi) u) \right); \\ &= \sum_{k=1}^{m-1} u \frac{d}{du} \log(1 - \alpha_k(\chi) u); \\ &= \sum_{k=1}^{m-1} \sum_{n=1}^{\infty} -\alpha_k(\chi)^n u^n; \\ &= \sum_{n=1}^{\infty} \sum_{k=1}^{m-1} -\alpha_k(\chi)^n u^n. \end{aligned}$$

We now read off the coefficients to be $c_n(\chi) = \sum_{k=1}^{m-1} -\alpha_k(\chi)^n$. In essence it follows from Weil's theorem that these inverse zeros all have absolute value $\sqrt{q}$ or 1, to fully understand this some prerequisites in algebraic geometry are necessary. A proof can be found in [Ros02]. Assuming this result this sum contributes $\mathcal{O}\left(q^{n/2}\right)$. A weaker result can also be proven that amounts to showing that the zeros of the L-series do not lie on the line with $\Re(s) = 1$. The proof of this is similar to standard proof of the same fact for L-series over the integers and can also be found in [Ros02].

In the case that $\chi = \chi_0$ we use equation 2.

$$\begin{aligned} u\frac{d}{du}\log(L^*(u,\chi)) &= u\frac{d}{du}\log\left(\frac{1}{1-qu}\prod_{P|M}(1-u^{\deg P})\right); \\ &= u\frac{d}{du}\log(\frac{1}{1-qu}) + u\sum_{P|M}\frac{d}{du}\log(1-u^{\deg P}); \\ &= \sum_{k=1}^{\infty} q^n u^n + \sum_{P|M}\deg(P)\frac{u^{\deg(P)}}{u^{\deg(P)}-1}; \\ &= \sum_{k=1}^{\infty} q^n u^n + \sum_{P|M}\deg(P)\sum_{l=1}^{\infty} -u^{\deg(P)}. \end{aligned}$$

We see that the second sum contributes at most $\mathcal{O}(1)$ to any coefficient, since it is just a finite sum that does not depend on q or n. So we can summarize this by stating that $c_n(\chi_0) = q^n + \mathcal{O}(1)$ and $c_n(\chi \neq \chi_0) = \mathcal{O}\left(q^{n/2}\right)$.

Finally we will compute the logarithmic derivative using equation 4 and Lemma 4.9 again.

$$\begin{aligned} u\frac{d}{du}\log(L^*(u,\chi)) &= u\frac{d}{du}\log\left(\prod_{e=1}^{\infty}\prod_{\substack{P\nmid M \\ \deg(P)=e}}(1-\chi(P)u^e)^{-1}\right); \\ &= \sum_{e=1}^{\infty}\sum_{\substack{P\nmid M \\ \deg(P)=e}} u\frac{d}{du}\log\left(1-\chi(P)u^e\right)^{-1}. \end{aligned}$$

To evaluate the derivative we do the substitution $x = u^e$. This gives us $\frac{dx}{du} = eu^{e-1}$ and

$$u\frac{d}{du}\log\left(1-\chi(P)u^d\right)^{-1} = u\frac{dx}{du}\frac{d}{dx}\log\left(1-\chi(P)x\right)^{-1} = ex\frac{d}{dx}\log\left(1-\chi(P)x\right)^{-1}$$

And using Lemma 4.9 this becomes

$$e\sum_{n=1}^{\infty}\chi(P)^n x^n = e\sum_{n=1}^{\infty}\chi(P)^n u^{en}.$$

We substitute this in and reorder the terms to get the powers of u together.

$$\sum_{d=1}^{\infty} \sum_{\substack{P \nmid M \\ \deg(P)=d}} d \sum_{n=1}^{\infty} \chi(P)^n u^{dn} = \sum_{n=1}^{\infty} \sum_{d|n} \sum_{\substack{P \nmid M \\ \deg(P)=d}} d\chi(P)^{n/d} u^n.$$

We can now estimate the coefficients again.

$$c_n(\chi) = \sum_{d|n} \sum_{\substack{P \nmid M \\ \deg(P)=d}} d\chi(P)^{n/d} = n \sum_{\deg(P)=n} \chi(P) + \sum_{\substack{d|n \\ n \leq N/2}} d \sum_{\substack{P \nmid M \\ \deg(P)=d}} \chi(P)^{n/d}.$$

We know that $|\chi(P)| = \mathcal{O}(1)$ and by the PNT the last sum contains $\mathcal{O}\left(\frac{q^d}{d}\right)$ terms. So this becomes

$$n \sum_{\deg(P)=n} \chi(P) + \sum_{\substack{d|n \\ n \leq N/2}} \mathcal{O}\left(q^d\right) = n \sum_{\deg(P)=n} \chi(P) + \mathcal{O}\left(q^{n/2}\right) + \mathcal{O}\left(nq^{n/3}\right) = n \sum_{\deg(P)=n} \chi(P) + \mathcal{O}\left(q^{n/2}\right).$$

We now use this to compute

$$\sum_{\chi} \overline{\chi(A)} c_n(\chi) = n \sum_{\deg(P)=n} \sum_{\chi} \overline{\chi(A)} \chi(P) + \mathcal{O}\left(q^{n/2}\right) = n\Phi(M)\pi(n, M, A) + \mathcal{O}\left(q^{n/2}\right).$$

At the same time we have

$$\sum_{\chi} \overline{\chi(A)} c_n(\chi) = c_n(\chi_0) + \sum_{\chi \neq \chi_0} \overline{\chi(A)} c_n(\chi) = q^n + \mathcal{O}\left(q^{n/2}\right).$$

Combining these two expressions

$$\pi(n, M, A) = \frac{1}{\Phi(M)} \frac{q^n}{n} + \mathcal{O}\left(\frac{q^{n/2}}{n}\right).$$

☺

5 Chebyshev's bias

In this chapter we will investigate a phenomenon that was first observed by Chebyshev in a certain specific case. If we count the number of primes that are 1 mod 4 and 3 mod 4 then Dirichlet's theorem tells us that asymptotically both classes should contribute the same. However if we only count up to a small number, say 10000, then it turns out that there are always more prime numbers 3 mod 4 than 1 mod 4. A little bit after this 1 mod 4 takes the lead for a short while, but 3 mod 4 is clearly ahead most of the time. Such a bias can also be observed in the polynomial case for lots of different residue classes. This seemingly contradictory fact has since been explained and it turns out to have everything to do with the zeros of the L polynomials we have seen before and the fact that 3 mod 4 is a quadratic non-residue. Both the integer and polynomial results depend on the generalized Riemann hypothesis and grand simplicity hypothesis, both of which are far from being proved for the integers. However in our polynomial setting we have Weil's theorem, and in specific cases the grand simplicity hypothesis is provable and in other cases falsifiable. For a much completer but still accessible overview of the integer case I recommend the article [GM06]. In this chapter we will mainly follow the article [Cha08], working out the details and changing a few arguments along the way.

5.1 General asymptotic formula

The reason the bias does not contradict Dirichlet's theorem is that this bias is $\mathcal{O}\left(q^{n/2}\right)$, so it hides inside the error term of the theorem. In order to analyse this bias we will thus have to redo some of the analysis of the previous chapter and be more careful about our estimations of the error term. To start we define what we mean by the bias.

Definition 5.1. For a monic polynomial M, a residue class $A \mod M$ with $(A, M) = 1$, and a positive integer X we define the bias as

$$E_{M,A}(X) = \frac{X}{q^{X/2}} \sum_{N=1}^{X} \left(\Phi(M)\pi(N, M, A) - \pi(N)\right).$$

We can interpret the bias as the difference between the actual number of primes and the expected number of primes from Dirichlet's theorem.

Proposition 5.2. *The summand*

$$n\left(\Phi(M)\pi(n, M, A) - \pi(n)\right) = -\delta_{2|n} c(M, A) q^{n/2} - \sum_{\chi \neq \chi_0} \overline{\chi(A)} \sum_{k=1}^{\deg(M)-1} \alpha_k(\chi)^n + \mathcal{O}\left(q^{n/3}\right).$$

Here $\delta_{2|n} = 1$ when $2|n$ and 0 otherwise. As before $\alpha_k(\chi)$ denote the inverse roots of $L^*(u, \chi)$. The number

$$c(M, A) = -1 + \sum_{\substack{B^2 \equiv A \mod M \\ b \in (\mathbb{F}_q[T]/(M))^\times}} 1,$$

checks how many square roots $A \mod M$ has. It coincides with the Legendre symbol whenever M is irreducible.

Proof. Recall from the previous chapter that $c_n(\chi)$, the coefficients of $u\frac{d}{du}\log(L^*(u,\chi))$, are given by

$$c_n(\chi) = \sum_{d|n} d \sum_{\substack{P \nmid M \\ \deg(P)=d}} \chi(P)^{n/d}. \tag{5}$$

Also for $\chi \neq \chi_0$

$$c_n(\chi) = -\sum_{k=1}^{\deg(M)-1} \alpha_k(\chi)^n; \tag{6}$$

and

$$c_n(\chi_0) = q^n + \mathcal{O}(1). \tag{7}$$

Now we will again sum over all characters, but this time without doing any estimations. Using equation 5

$$\sum_{\chi} \overline{\chi(A)} c_n(\chi) = \sum_{d|n} d \sum_{\substack{P \nmid M \\ \deg(P)=d}} \sum_{\chi} \overline{\chi(A)} \chi(P)^{n/d}.$$

We introduce some notation to simplify this a bit,

$$\pi(d,k,M,A) := \#\{P | P^k \equiv A \mod M, \deg(P) = d\}.$$

This is a generalization of the normal prime counting function in the sense that $\pi(d,1,M,A) = \pi(d,M,A)$. It is then clear that using the orthogonality relations as before we get

$$\sum_{\chi} \overline{\chi(A)} c_n(\chi) = \sum_{d|n} d\Phi(M)\pi(d, n/d, M, A).$$

The term corresponding to $d = n$ gives a contribution of

$$n\Phi(M)\pi(n, M, A).$$

For the terms with $d < n/3$ we get at most

$$\frac{n}{3}\pi(n/3, 3, M, A) \leq \frac{n}{3}\pi(n/3) = \mathcal{O}\left(q^{n/3}\right).$$

Finally, when it exists, the $d = n/2$ term contributes

$$\frac{n}{2}\Phi(M)\pi(n/2, 2, M, A) = \frac{n}{2}\Phi(M) \sum_{\substack{P:\deg(P)=n/2 \\ P \equiv B(M) \\ B^2 \equiv A(M)}} 1 = \frac{n}{2}\Phi(M) \sum_{B^2 \equiv A(M)} \sum_{\substack{P:\deg(P)=n/2 \\ P \equiv B(M)}} 1.$$

Note that $(B, M) = 1 \Leftrightarrow (B^2, M) = 1$, so we can apply Dirichlet's theorem.

$$= \frac{n}{2}\Phi(M) \sum_{B^2 \equiv A(M)} \left(\frac{1}{\Phi(M)} \frac{q^{n/2}}{n/2} + \mathcal{O}\left(q^{n/4}\right) \right) = \delta_{2|N}(c(M,A)+1)q^{n/2} + \mathcal{O}\left(q^{n/4}\right).$$

Combining all the terms gives

$$\sum_{\chi} \overline{\chi(A)} c_n(\chi) = n\Phi(M)\pi(n, M, A) + \delta_{2|N}(c(M,A)+1)q^{n/2} + \mathcal{O}\left(q^{n/3}\right),$$

which we can rewrite using equation 6 and 7.

$$n\Phi(M)\pi(n, M, A) = -\sum_{\chi \neq \chi_0} \overline{\chi(A)} \sum_{k=1}^{\deg(M)-1} \alpha_k(\chi)^n + q^n - \delta_{2|N}(c(M,A)+1)q^{n/2} + \mathcal{O}\left(q^{n/3}\right).$$

We can see that by adding the extra term $n/2$ we get an error of order $q^{n/3}$, instead of $q^{n/2}$ like in the previous chapter. It is then also this term that is responsible for the bias. Finally redoing the estimates for $\pi(n)$,

$$n\pi(n) = \sum_{d|n} q^{n/d}\mu(d) = q^n - \delta_{2|n}q^{n/2} + \mathcal{O}\left(q^{n/3}\right).$$

Combining this with our other estimates cancels some terms

$$n(\Phi(M)\pi(n, M, A) - \pi(n)) = q^n - q^n - \delta_{2|n}(c(M,A)+1-1)q^{n/2} - \sum_{\chi \neq \chi_0} \overline{\chi(A)} \sum_{k=1}^{\deg(M)-1} \alpha_k(\chi)^n + \mathcal{O}\left(q^{n/3}\right).$$

Which proves the proposition. ☺

To turn these estimates of the summand into estimates for the entire sum we will need a lemma.

Lemma 5.3. *For any complex number β, with $|\beta| > 1$,*

$$\lim_{n\to\infty} \frac{n}{\beta^n} \left(\sum_{i=1}^{n} \frac{\beta^i}{i} \right) = \frac{\beta}{\beta - 1}$$

Proof. We first apply partial summation with arithmetic function $f(n) = \beta^n$ and smooth function $\phi(x) = \frac{1}{x}$.

$$\sum_{i=1}^{n} \beta^i \frac{1}{i} = \left(\sum_{i=1}^{n} \beta^i \right) \frac{1}{n} + \int_1^n \left(\sum_{i=1}^{[t]} \beta^i \right) \frac{1}{t^2} dt.$$

Recognizing the geometric series this gives

$$\frac{n}{\beta^n} \sum_{i=1}^{n} \beta^i \frac{1}{i} = \frac{\beta - \beta^{1-n}}{\beta - 1} + \frac{n}{\beta^n} \frac{\beta}{\beta - 1} \int_1^n \frac{\beta^{[t]} - 1}{t^2} dt.$$

Clearly

$$\frac{\beta-\beta^{1-n}}{\beta-1}\to\frac{\beta}{\beta-1}.$$

So we want the remaining terms to go to 0, firstly

$$\frac{n}{\beta^n}\frac{\beta}{\beta-1}\int_1^n\frac{-1}{t^2}dt=\frac{n}{\beta^n}\frac{\beta}{1-\beta}\to 0.$$

The harder part is the integral

$$\frac{n}{\beta^n}\frac{\beta}{\beta-1}\int_1^n\frac{\beta^{[t]}}{t^2}dt\le C\frac{n}{\beta^n}\int_1^n\frac{|\beta|^t}{t^2}dt.$$

We will use partial integration to estimate this integral.

$$\frac{n}{\beta^n}\int_1^n\frac{|\beta|^t}{t^2}dt=\frac{n}{\beta^n}\frac{1}{\log|\beta|}\left(|\beta|^n/n^2-|\beta|\right)+\frac{2}{\log|\beta|}\frac{n}{\beta^n}\int_1^n\frac{|\beta|^t}{t^3}dt.$$

Clearly

$$\frac{n}{\beta^n}\frac{1}{\log|\beta|}\left(|\beta|^n/n^2-|\beta|\right)\to 0.$$

and finally we split up the integral into two intervals.

$$\begin{aligned}\frac{n}{\beta^n}\int_1^n\frac{|\beta|^t}{t^3}dt&=\frac{n}{\beta^n}\int_1^{n/2}\frac{|\beta|^t}{t^3}dt+\frac{n}{\beta^n}\int_{n/2}^n\frac{|\beta|^t}{t^3}dt;\\&\le\frac{n}{\beta^n}|\beta|^{n/2}\int_1^{n/2}\frac{1}{t^3}dt+\frac{n}{\beta^n}|\beta|^n\int_{n/2}^n\frac{1}{t^3}dt;\\&\le\frac{n}{\beta^n}|\beta|^{n/2}\cdot c+\frac{n}{\beta^n}|\beta|^n\left(\frac{-2}{n^2}+\frac{-2}{(n/2)^2}\right)\to 0.\end{aligned}$$

This concludes the proof. ☺

The following theorem is the main result of this thesis and describes the bias directly in terms of the inverse roots of L-series.

Theorem 5.4. *Asymptotically as $X\to\infty$*

$$E_{M,A}(X)=-c(M,A)\mathcal{B}_q(X)-\sum_{\chi\neq\chi_0}\overline{\chi(A)}\sum_{\gamma_\chi}e^{i\theta(\gamma_\chi)X}\frac{\gamma_\chi}{\gamma_\chi-1}+o(1)$$

where $\mathcal{B}$ (for bias) denotes

$$\mathcal{B}_q(X)=\begin{cases}\sqrt{q}/(q-1) & \text{if } X \text{ is odd;}\\ q/(q-1) & \text{if } X \text{ is even.}\end{cases}$$

The sum over γ_χ is a sum over the inverse roots of $L^*(u,\chi)$, with $\gamma_\chi=\sqrt{q}e^{i\theta(\gamma_\chi)}$.

Proof. The proof will apply Lemma 5.3 several times to Proposition 5.2.

$$\begin{aligned} E_{M,A}(X) = &\frac{X}{q^{X/2}} \sum_{n=1}^{X} \delta_{2|n} c(M,A) \frac{q^{n/2}}{n} \\ &+ \frac{X}{q^{X/2}} \sum_{n=1}^{X} \frac{-\sum_{\chi \neq \chi_0} \overline{\chi(A)} \sum_{k=1}^{\deg(M)-1} \alpha_k(\chi)^n}{n} \\ &+ \frac{X}{q^{X/2}} \sum_{n=1}^{X} \frac{\mathcal{O}\left(q^{n/3}\right)}{n}. \end{aligned}$$

We will do the three sums separately, firstly

$$\frac{X}{q^{X/2}} \sum_{n=1}^{X} \frac{\mathcal{O}\left(q^{n/3}\right)}{n} \leq \frac{X}{q^{X/2}} X \mathcal{O}\left(q^{X/3}\right) = o(1).$$

Secondly if $X = 2Y$ is even,

$$\frac{X}{q^{X/2}} \sum_{n=1}^{X} \delta_{2|n} c(M,A) \frac{q^{n/2}}{n} = c(M,A) \frac{2Y}{q^Y} \sum_{n=1}^{Y} \frac{q^n}{2n} = c(M,A) \frac{q}{q-1} + o(1).$$

If $X = 2Y + 1$ is odd,

$$\frac{X}{q^{X/2}} \sum_{n=1}^{X} \delta_{2|n} c(M,A) \frac{q^{n/2}}{n} = c(M,A) \frac{1}{\sqrt{q}} \frac{2Y+1}{q^Y} \sum_{n=1}^{Y} \frac{q^n}{2n} = c(M,A) \frac{\sqrt{q}}{q-1} + o(1).$$

Recall that the inverse zeros of the Dirichlet L series all have absolute value 1 or $\sqrt{q}$. For the zeros with absolute value one we will get

$$\frac{X}{q^{X/2}} \sum_{n=1}^{X} \frac{\overline{\chi(A)} \alpha^n}{n} \leq \frac{X}{q^{X/2}} \sum_{n=1}^{X} \frac{1^n}{n} \leq \frac{X^2}{q^{X/2}} = o(1).$$

For the rest of the zeros we write $\alpha = \sqrt{q} e^{i\theta}$ to obtain

$$\frac{X}{q^{X/2}} \sum_{n=1}^{X} \frac{\overline{\chi(A)} \alpha^n}{n} = \overline{\chi(A)} e^{i\theta X} \frac{X}{\alpha^X} \sum_{n=1}^{X} \frac{\alpha^n}{n} = \overline{\chi(A)} e^{i\theta X} \frac{\alpha}{\alpha - 1} + o(1).$$

Combining all the terms gives the result.

☺

Looking at this formula we should not expect $\lim_{X \to \infty} E_{M,A}(X)$ to converge, because there are oscillating terms that do not go to 0. However, the average of $E_{M,A}(X)$ does converge.

Theorem 5.5. *For any M, A the limit*

$$\lim_{n\to\infty}\frac{1}{n}\sum_{X=1}^{n}E(M,A)(X) = -c(M,A)\frac{\sqrt{q}+q}{2(q-1)} - \sum_{\chi\in I}\overline{\chi(A)}\frac{\sqrt{q}}{\sqrt{q-1}}$$

Here I is the set (with multiplicity) of all characters mod M that have $\sqrt{q}$ as an inverse root.

This theorem justifies thinking of $-c(M,A)$ as the cause of the bias, since often I is empty. For example when $\deg(M) \le 4$ it is empty, since there are no degree 3 polynomials with integer coefficients that have $\sqrt{q}$ as an inverse root twice. (The real roots of the polynomial $L^*(u,\chi)$ always have even multiplicity.) Note that if this limit is negative this does not mean that in the limit the squares always get less primes then they deserve. The bias might be very negative every time it is negative and only a little bit positive whenever it is positive. This way the average can be negative even though the bias is positive most of the time.

Proof. Because of Theorem 5.4 it suffices to compute the limits

$$\lim_{n\to\infty}\frac{1}{n}\sum_{X=1}^{n}\mathcal{B}_q(X);$$

$$\lim_{n\to\infty}\frac{1}{n}\sum_{X=1}^{n}o(1);$$

$$\lim_{n\to\infty}\frac{1}{n}\sum_{X=1}^{n}e^{i\theta(\gamma_\chi)X}.$$

For the first one we will group the neighbours.

$$\lim_{n\to\infty}\frac{1}{n}\sum_{X=1}^{n}\mathcal{B}_q(X) = \lim_{n\to\infty}\frac{1}{n}\sum_{X=1}^{[n/2]}\frac{\sqrt{q}+q}{q-1} + \frac{1}{n}(1-\delta_{2|n})\frac{\sqrt{q}}{q-1} \to \frac{\sqrt{q}+q}{2(q-1)}$$

For the second limit, we recall that $f(X) = o(1)$ implies that for every $\epsilon > 0$ there exists an N such that for all $X > N$, $|f(X)| \le \epsilon$. Now take any $\epsilon > 0$

$$\lim_{n\to\infty}\left|\frac{1}{n}\sum_{X=1}^{n}o(1)\right| \le \lim_{n\to\infty}\frac{1}{n}\left(\sum_{X=1}^{N}f(X) + \sum_{X=N+1}^{n}\epsilon\right) = \lim_{n\to\infty}\frac{K}{n} + \frac{n-N}{n}\epsilon \to \epsilon.$$

Hence the limit exists and must be equal to 0. Finally we recognize a geometric series whenever $e^{i\theta(\gamma_\chi)} \neq 1$.

$$\lim_{n\to\infty}\left|\frac{1}{n}\sum_{X=1}^{n}e^{i\theta(\gamma_\chi)X}\right| = \lim_{n\to\infty}\frac{1}{n}\left|\frac{1-e^{i\theta(\gamma_\chi)n}}{1-e^{i\theta(\gamma_\chi)}}\right| \le \lim_{n\to\infty}\frac{1}{n}\left|\frac{2}{1-e^{i\theta(\gamma_\chi)}}\right| = 0.$$

If $e^{i\theta(\gamma_\chi)} = 1$ i.e. $\gamma_\chi = \sqrt{q}$, then of course

$$\lim_{n\to\infty} \frac{1}{n} \sum_{X=1}^{n} e^{i\theta(\gamma_\chi)X} = 1.$$

Combining everything gives the result.

☺

5.2 Quadratic residues

We have seen above that the main cause of the bias is how many square roots A mod M has. In view of this observation we will focus our attention to irreducible modulus M and split the residues into two different groups, depending on if they are a square or not.

$$a(n) = \#\{P|\chi_{\text{quad}}(P) = 1, \deg(P) = n\}$$

$$b(n) = \#\{P|\chi_{\text{quad}}(P) = -1, \deg(P) = n\}$$

Where χ_{quad} is the real quadratic character mod M, i.e.

$$\chi_{\text{quad}}(F) = \begin{cases} 1 & \text{if } F \text{ is a square modulo } M \\ -1 & \text{if } F \text{ is not a square modulo } M \\ 0 & \text{if } M|F \end{cases}$$

This is equal to $c(M, A)$ whenever M is irreducible.

Proposition 5.6. *With a, b as above we have*

$$n(a(n) - b(n)) = -\sum_{k=1}^{\deg(M)-1} \alpha_k(\chi_{quad})^n - \delta_{2|n} q^{N/2} + \mathcal{O}\left(q^{n/3}\right).$$

In the paper [Cha08] this is proven by comparing coefficients of the logarithmic derivatives of certain products of L-series. However it is also suggested that this may be proven using our previous Proposition 5.2, which is what we will work out here.

Proof. By definition of a and b,

$$\begin{aligned} n(a(n) - b(n)) &= n\left(\sum_{\chi_{\text{quad}}(A)=1} \pi(n, M, A) - \sum_{\chi_{\text{quad}}(A)=-1} \pi(n, M, A)\right); \\ &= \frac{1}{\Phi(M)} \sum_{A} \chi_{\text{quad}}(A) n \Phi(M) \pi(n, M, A), \end{aligned}$$

where the sums are over all the residue classes $A \mod M$. Since exactly half of these are quadratic residues we can add nothing

$$= \frac{1}{\Phi(M)} \sum_{A} \chi_{\text{quad}}(A) n \left(\Phi(M)\pi(n, M, A) - \pi(n)\right).$$

Now we apply Proposition 5.2,

$$= -\frac{1}{\Phi(M)}\sum_{A}\chi_{\text{quad}}(A)^2\delta_{2|X}q^{n/2} - \frac{1}{\Phi(M)}\sum_{A}\chi_{\text{quad}}(A)\sum_{\chi}\overline{\chi(A)}\sum_{k=1}^{\deg(M)-1}\alpha_k(\chi)^n + \mathcal{O}\left(q^{n/3}\right).$$

Simplifying using the orthogonality relations and $\chi_{\text{quad}}^2 = \chi_0$,

$$= -\delta_{2|X}q^{n/2} - \sum_{k=1}^{\deg(M)-1}\alpha_k(\chi_{\text{quad}})^n + \mathcal{O}\left(q^{n/3}\right).$$

☺

Similar to before we define

Definition 5.7. For a monic irreducible M, the bias towards quadratic non-residues is

$$E_{M,\text{quad}}(X) := \frac{X}{q^{X/2}}\sum_{n=1}^{X}(a(n) - b(n)).$$

And we get the analogue of theorem 5.4.

Theorem 5.8. *Enumerate the inverse zeros of $L^*(\chi_{quad}, u)$ with absolute value $\sqrt{q}$ as $\gamma_1, \overline{\gamma_1}, \cdots, \gamma_k, \overline{\gamma_k}$. Asymptotically as $X \to \infty$,*

$$E_{M,quad}(X) = -\mathcal{B}_q(X) - 2\sum_{j=1}^{k}\Re\left(e^{i\theta_j X}\frac{\gamma_j}{\gamma_j - 1}\right) + o(1).$$

Proof. Of course all the complex roots γ_i have a partner $\overline{\gamma_i}$. The fact that all the purely real roots also come in pairs is a result from algebraic geometry and we refer to Proposition 6.4 from [Cha08]. We observe

$$e^{i\theta_j X}\frac{\gamma_j}{\gamma_j - 1} + e^{-i\theta_j X}\frac{\overline{\gamma_j}}{\overline{\gamma_j} - 1} = 2\Re\left(e^{i\theta_j X}\frac{\gamma_j}{\gamma_j - 1}\right).$$

Now the proof is just an exact repeat of the proof of theorem 5.4. ☺

From here on we will try to answer the question of how often $E_{M,\text{quad}}(X) < 0$, i.e. how often the non-square primes are ahead of the square primes. In [Cha08] this is done in more generality, which requires a second course in measure theory. We will focus on the simpler cases $\deg(M) \leq 4$. This will allow us to tackle it without much more then knowledge of the Lebesgue measure.

Corollary 5.9. *If $\deg(M) \leq 2$, the quadratic non-residues almost always dominate the quadratic residues.*

Proof. If $\deg(M) = 2$ we can see from [Cha08, chapter 6] that the corresponding $L^*(\chi_{\text{quad}}, u)$, has no roots with absolute value $\sqrt{q}$. This means that the expression from Theorem 5.8 simplifies to

$$E_{M,\text{quad}}(X) = -\mathcal{B}_q(X) + o(1).$$

Now for all large enough X the function $o(1)$, will be smaller then $\mathcal{B}_q(X)$ and hence the expression will be negative for all large X. ☺

Next we will consider the case of degree $3, 4$. Again from [Cha08] we know that there are exactly two zeros of $L*(\chi_{\text{quad}}, u)$ with absolute value $\sqrt{q}$, denote them $\gamma, \overline{\gamma}$. If this root has $\theta(\gamma)$ a rational multiple of π, then $E_{M,\text{quad}}(X)$ is periodic (up to a small error) and we only have to compute the first few terms in order to know how it behaves everywhere. We explain what to do if $\theta(\gamma)$ is not a rational multiple of π.

Theorem 5.10. *For a monic irreducible polynomial M of degree 3 or 4. With $\theta(\gamma)$ not a rational multiple of π*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{X=1}^{N} \text{sign}\left(E_{M,quad}(X)\right) = \frac{\cos^{-1}\left(\frac{q}{2q-2}\left|\frac{\gamma-1}{\gamma}\right|\right) + \cos^{-1}\left(\frac{\sqrt{q}}{2q-2}\left|\frac{\gamma-1}{\gamma}\right|\right)}{2\pi} < \frac{1}{2}$$

Here $\text{sign}(x)$ *is* 1 *if* $x > 0$ *and* 0 *if* $x \leq 0$.

Proof. We write $\frac{\gamma}{\gamma-1}$ in polar form $\left|\frac{\gamma}{\gamma-1}\right| e^{i\omega}$ and observe

$$\Re\left(e^{i\theta X}\frac{\gamma}{\gamma-1}\right) = \Re\left(e^{i\theta X}\left|\frac{\gamma}{\gamma-1}\right| e^{i\omega}\right) = \left|\frac{\gamma}{\gamma-1}\right| \cos\left(\theta X + \omega\right).$$

It then follows that

$$\text{sign}\left(E_{M,\text{quad}}(X)\right) = \begin{cases} 1 & \text{if } -\cos\left(\theta X+\omega\right) > \frac{\mathcal{B}_q(X)}{2}\left|\frac{\gamma-1}{\gamma}\right| + o(1) \\ 0 & \text{if } -\cos\left(\theta X+\omega\right) \leq \frac{\mathcal{B}_q(X)}{2}\left|\frac{\gamma-1}{\gamma}\right| + o(1) \end{cases}$$

By continuity of $\cos^{-1}$, for every $\epsilon > 0$, we can find a $\delta > 0$ such that:

$$b_{X,-\epsilon} = \cos^{-1}\left(\frac{\mathcal{B}_q(X)}{2}\left|\frac{\gamma-1}{\gamma}\right|\right) - \epsilon \leq \cos^{-1}\left(\frac{\mathcal{B}_q(X)}{2}\left|\frac{\gamma-1}{\gamma}\right| + \delta\right);$$

$$b_{X,+\epsilon} = \cos^{-1}\left(\frac{\mathcal{B}_q(X)}{2}\left|\frac{\gamma-1}{\gamma}\right|\right) + \epsilon \leq \cos^{-1}\left(\frac{\mathcal{B}_q(X)}{2}\left|\frac{\gamma-1}{\gamma}\right| - \delta\right).$$

These values are the boundary where the sign of $E_{M,\text{quad}}(X)$ switches with a small error. We define $\cos^{-1}(x) = 0$ whenever $x \geq 1$, to be consistent with this property. Next we define

$$I_{X,big} = [-b_{X,+\epsilon}, b_{X,+\epsilon}] \subset \mathbb{R}/\mathbb{Z};$$
$$I_{X,small} = (-b_{X,-\epsilon}, b_{X,-\epsilon}) \subset \mathbb{R}/\mathbb{Z}.$$

Take any $\epsilon > 0$ and take a δ such as above, then find a Y such that $o(1) < \delta$ for all $X \geq Y$. Now these intervals satisfy

$$\operatorname{sign}\left(E_{M,\mathrm{quad}}(X)\right) = 1 \Rightarrow \theta X + \omega + \pi \in I_{X,big}$$

and

$$\theta X + \omega + \pi \in I_{X,small} \Rightarrow \operatorname{sign}\left(E_{M,\mathrm{quad}}(X)\right) = 1$$

for all large $X \geq Y$. Using this we can bound the limit in terms of these intervals.

$$\begin{aligned}\lim_{N\to\infty} \frac{1}{N} \sum_{X=1}^{N} \operatorname{sign}\left(E_{M,\mathrm{quad}}(X)\right) &\geq \lim_{N\to\infty} \frac{K_Y}{N} + \frac{1}{N} \sum_{X=Y}^{N} \mathbb{1}_{I_{X,small}}\left(\theta X + \omega + \pi\right); \\ &= \lim_{N\to\infty} \frac{1}{N} \sum_{X=Y}^{N} \mathbb{1}_{I_{X,small}}\left(\theta X + \omega + \pi\right).\end{aligned}$$

The corresponding upper bound is

$$\lim_{N\to\infty} \frac{1}{N} \sum_{X=1}^{N} \operatorname{sign}\left(E_{M,\mathrm{quad}}(X)\right) \leq \lim_{N\to\infty} \frac{1}{N} \sum_{X=Y}^{N} \mathbb{1}_{I_{X,big}}\left(\theta X + \omega + \pi\right).$$

Now we observe that the final summand only depends on the parity of X, because we have removed the $o(1)$ function by just estimating it as $\pm\epsilon$. We can thus write the lower bound as

$$\lim_{N\to\infty} \frac{1}{N} \sum_{X=1}^{[N/2]} \mathbb{1}_{I_{1,small}}\left(\theta X + \omega + \pi\right) + \mathbb{1}_{I_{2,small}}\left(\theta X + \omega + \pi\right).$$

Here we have added finitely many terms at the start and maybe one at the end, but these are divided by N and thus converge to 0. We then apply the equidistribution theorem [HW08, Section 23.10], which says that whenever θ is irrational

$$\lim_{N\to\infty} \sum_{X=1}^{N} \mathbb{1}_I(\theta X) = \mu\left(I\right)$$

Here $\mu(I) = \tilde{\mu}(I)/2\pi$ where $\tilde{\mu}$ is the Lebesgue measure. In our case

$$\frac{\mu(I_{1,small}) + \mu(I_{2,small})}{2} = \frac{\cos^{-1}\left(\frac{q}{2q-2}\left|\frac{\gamma-1}{\gamma}\right|\right) + \cos^{-1}\left(\frac{\sqrt{q}}{2q-2}\left|\frac{\gamma-1}{\gamma}\right|\right) - 2\epsilon}{2\pi}$$

Which gives

$$\lim_{N\to\infty} \frac{1}{N} \sum_{X=1}^{N} \operatorname{sign}\left(E_{M,\mathrm{quad}}(X)\right) \geq \frac{\cos^{-1}\left(\frac{q}{2q-2}\left|\frac{\gamma-1}{\gamma}\right|\right) + \cos^{-1}\left(\frac{\sqrt{q}}{2q-2}\left|\frac{\gamma-1}{\gamma}\right|\right)}{2\pi} - \frac{\epsilon}{\pi}$$

And the lower bound follows similarly

$$\lim_{N\to\infty}\frac{1}{N}\sum_{X=1}^{N}\operatorname{sign}\left(E_{M,\mathrm{quad}}(X)\right)\leq\frac{\cos^{-1}\left(\frac{q}{2q-2}\left|\frac{\gamma-1}{\gamma}\right|\right)+\cos^{-1}\left(\frac{\sqrt{q}}{2q-2}\left|\frac{\gamma-1}{\gamma}\right|\right)}{2\pi}+\frac{\epsilon}{\pi}$$

Since this is true for all $\epsilon>0$ we get

$$\lim_{N\to\infty}\frac{1}{N}\sum_{X=1}^{N}\operatorname{sign}\left(E_{M,\mathrm{quad}}(X)\right)=\frac{\cos^{-1}\left(\frac{q}{2q-2}\left|\frac{\gamma-1}{\gamma}\right|\right)+\cos^{-1}\left(\frac{\sqrt{q}}{2q-2}\left|\frac{\gamma-1}{\gamma}\right|\right)}{2\pi}.$$

Finally since $\cos^{-1}$ of a positive number is strictly smaller then $\pi/2$ we get

$$\lim_{N\to\infty}\frac{1}{N}\sum_{X=1}^{N}\operatorname{sign}\left(E_{M,\mathrm{quad}}(X)\right)<\frac{\pi/2+\pi/2}{2\pi}=\frac{1}{2}.$$

Which concludes the proof. ☺

We have just seen that also in the case of two inverse zeros the quadratic non-residues dominate the quadratic residues. However this only works under the hypothesis that it is not a rational multiple of π. In general the same can be said in the case of higher degrees, but with the hypothesis that all the inverse zeros are linearly independent over $\mathbb{Q}$, that is linear combinations may also not be a rational multiple of π. The proof of this is mostly just a technical extension of the ideas in the previous proof and is worked out in [Cha08]. It is also very important to notice that the result is not generally true whenever the inverse zeros are rational multiples of π, this is because if we try to do the above analysis again the equidistribution theorem fails. We will look at examples of this and the other situations in the next chapter.

5.3 Numerical data

We end by showing some actual examples of the above behaviour. Most of these polynomials turn out to satisfy the conditions of theorem 5.10, and whenever the roots did have rational angles, the bias was usually towards the non-squares regardless, so finding examples of these cases is not hard. This should not come as a surprise, as usually "normal" polynomials do not have roots with rational angles. Also when the roots have a rational angle it is still very rare for them to overcome the negative term that is always present in the formula 5.8. To find the other examples we try to find q, a, b such that the minimal polynomial f of $\sqrt{q}e^{2\pi i\frac{a}{b}}$ with small degree. The reciprocal polynomial f^* then has this number as its inverse root and several more which are easily calculated. We can then use 5.8 to figure out if these roots will give a bias towards the squares. Once we have found a candidate in this way we can just search all the irreducible polynomials and calculate $L^*(u,\chi_{\mathrm{quad}})$ using formula 4.8, untill we find one with $L^*(u,\chi_{\mathrm{quad}})=f^*$. To speed this up we can use the symmetry of

Table 1: $M = T^2 + 1$

X	$E_{M,\mathrm{quad}}(X)$
1	-0.378
2	-1.714
3	-0.972
4	-1.469
5	-0.694
6	-1.294
7	-0.571
8	-1.246

$L^*(u, \chi_{\mathrm{quad}}) = \sum_{i=1}^{d} \alpha_i u^i$, namely that $\alpha_{d-i} = q^{d-i}\alpha_i$ for all $0 \leq i \lfloor d/2 \rfloor$. Up to $\deg(f) = 6, q = 9$, this is still doable on any machine with a couple of minutes of computation time. See also [Cha08] for some different examples.

Example 1. We start with the simplest case, where the degree of $M \leq 2$. Take

$$M = T^2 + 1 \in \mathbb{F}_7[T].$$

We expect $E_{M,\mathrm{quad}}(2X) = -\frac{7}{6} + \mathrm{o}\,(1) \approx -1.143$ and $E_{M,\mathrm{quad}}(2X+1) = -\frac{\sqrt{7}}{6} + \mathrm{o}\,(1) \approx -0.441$. We compute the first few values numerically in table 1. We see that the numbers seem to follow the prescribed pattern fairly well. It is worth mentioning that in general we should not expect the formula to work for small numbers (or any finite set), since the formula only tells us something about the limit.

Example 2. Next we consider an example where we can apply theorem 5.10. Take the irreducible polynomial defined in $\mathbb{F}_3[T]$

$$M = T^4 + T^2 + T + 1.$$

Then using formula 4.8 we find that the L-series is

$$L^*(u, \chi_{\mathrm{quad}}) = -3u^3 + u^2 + u + 1.$$

This is just a third degree polynomial so it is not hard to find the inverse roots

$$\alpha_1 = 1 \quad \alpha_2 = -1 + i\sqrt{2} \quad \alpha_3 = -1 - i\sqrt{2}.$$

So we are only concerned with

$$\gamma = -1 + i\sqrt{2} = \sqrt{3}e^{i(\pi - \arctan(\sqrt{2}))}.$$

The fact that $\arctan(\sqrt{2})$ is not a rational multiple of π is non-trivial. In [Cal06, Section 6] there is a complete list of square roots that are the tangent of a

rational multiple of π. Since $\sqrt{2}$ is not in this list we know that $\frac{\arctan(\sqrt{2}))}{\pi}$ must be irrational. We therefore expect $E_{M,\mathrm{quad}}(X)$ to be positive about

$$\frac{\cos^{-1}\left(\frac{3}{4}\left|\frac{-2+i\sqrt{2}}{-1+i\sqrt{2}}\right|\right)+\cos^{-1}\left(\frac{\sqrt{3}}{4}\left|\frac{-2+i\sqrt{2}}{-1+i\sqrt{2}}\right|\right)}{2\pi}=\frac{\cos^{-1}\left(\frac{3\sqrt{2}}{4}\right)+\cos^{-1}\left(\frac{\sqrt{6}}{4}\right)}{2\pi}\approx 0.145\ldots$$

of the time. Checking this numerically we find the numbers in table 2. So we

Table 2: $M = T^4 + T^2 + T + 1$

X	$E_{M,\mathrm{quad}}(X)$
1	0.577
2	0
3	-2.309
4	-1.778
5	-1.283
6	-3.556
7	-0.599
8	-1.778
9	-2.438
10	-0.576
11	-1.307
12	-2.733
13	0.268
14	-2.215
15	-1.750

see that for this small sample $2/15 \approx 1.33\ldots$ of the numbers are positive, which is already quite close to the limiting expectation.

Example 3. This is an example where there is no bias at all. Take the polynomial

$$M = T^4 + 5T^2 + 5T + 5 \in \mathbb{F}_7[T].$$

Again using formula 4.8 we get

$$L^*(u, \chi_{\mathrm{quad}}) = -7u^3 + 7u^2 - u + 1 = (1-u)(1-i\sqrt{7}u)(1+i\sqrt{7}u).$$

We then use formula 5.8 and also compute the values numerically in table 3. So we predict that the squares and non-squares are both ahead half of the time. We can see that also for small numbers this is the case.

Example 4. Now we give an example where we cannot apply 5.10, but we still observe a bias towards the non-squares. Take

$$M = T^3 - T + 1 \in \mathbb{F}_9[T].$$

Table 3: $M = T^4 + 5T^2 + 5T + 5$

X	Predicted $E_{M,\text{quad}}(X)$	Actual $E_{M,\text{quad}}(X)$
1	-1.1024	-0.378
2	0.5833	0.571
3	0.2205	0.324
4	-2.9167	-2.939
5	-1.1024	-1.388
6	0.5833	0.350
7	0.2205	0.154
8	-2.9167	-2.932

Then using formula 4.8 we get

$$L^*(u, \chi_{\text{quad}}) = 9u^2 - 3u + 1 = \left(1 - 3e^{2\pi i \frac{1}{6}}\right)\left(1 - 3e^{2\pi i \frac{5}{6}}\right).$$

We then apply formula 5.8 as in the previous example and compute the actual values numerically in table 4. We see that as predicted $\frac{2}{3}$ of the times the

Table 4: $M = T^3 - T + 1$

X	Predicted $E_{M,\text{quad}}(X)$	Actual $E_{M,\text{quad}}(X)$
1	-2.0893	-1.000
2	-0.6964	-0.667
3	1.7679	1.667
4	0.5893	0.741
5	-0.8036	-0.679
6	-3.2679	-3.267

non-squares are ahead and the actual values are quite close.

Example 5. We end by giving a rare example where we do observe a bias towards the squares. Take $\alpha \in \mathbb{F}_9$, such that $\alpha^2 = \alpha + 1$. Then we have the polynomial

$$M = T^7 + 2T^6 + \alpha^3 T^5 + \alpha^3 T^4 + T^3 + \alpha^5 T^2 + 2T + 2 \in \mathbb{F}_9[T].$$

Then once again using 4.8 we get

$$L^*(u, \chi_{\text{quad}}) = 729u^6 + 243u^5 + 81u^4 + 27u^3 + 9u^2 + 3u + 1,$$

which we recognize as

$$\left(1 - 3e^{2\pi i \frac{2}{14}}u\right)\left(1 - 3e^{2\pi i \frac{4}{14}}u\right)\left(1 - 3e^{2\pi i \frac{6}{14}}u\right)\left(1 - 3e^{2\pi i \frac{8}{14}}u\right)\left(1 - 3e^{2\pi i \frac{10}{14}}u\right)\left(1 - 3e^{2\pi i \frac{12}{14}}u\right)$$

This will give us 14 different cases depending on $X \mod 14$. We compute these using formula 5.8 in table 5. And we can see that the squares are ahead exactly $\frac{9}{14} > \frac{1}{2}$ of the time.

Table 5: $M = T^7 + 2T^6 + \alpha^3 T^5 + \alpha^3 T^4 + T^3 + \alpha^5 T^2 + 2T + 2$

$X \mod 14$	Predicted $E_{M,\text{quad}}(X)$
1	-1.2094
2	-0.4031
3	0.8656
4	0.2885
5	1.0962
6	0.3654
7	-5.8782
8	-1.9594
9	0.3469
10	0.1156
11	1.0385
12	0.3462
13	1.1154
14	-6.6282

6 Discussion

We have shown a variety of proofs for the prime number theorem for polynomials of finite fields. Doing this showed the similarity in results with the integer prime number theorem, while also showing that the proofs are simpler. We then extended the techniques of zeta functions and Euler products to give a proof of Dirichlet's theorem following [Ros02]. The error terms in this theorem depend crucially on the absolute value of the inverse roots of L-series, which can be derived from Weil's theorem. This derivation is not part of the thesis and would be interesting to investigate further.

More careful analysis of the error terms following [Cha08] reveal the Chebyshev's bias, showing that the error term is not zero on average. We then give some formulas for the asymptotic behaviour of this bias depending on the roots of L-series. From this formula we then derive a formula for the specific case where we split up the residue classes into squares and non-squares. This expresion only depends on the single L-series $L^*(u, \chi_{\text{quad}})$, which allows us to give a method of computing the bias for any irreducible modulus of degree ≤ 4. We then show some new examples of all the cases, bias towards squares, no bias and bias towards non-squares. The cases ≥ 5 are considered in [Cha08], but apart from existence no explicit approach is given as to calculating the bias there. The case of a bias towards squares is very rare and can only happen when the angles of the roots are linearly dependent over $\mathbb{Q}$, so it might be possible to classify all the cases in which it does. A heuristic approach to finding examples of this case is given, but it is not at all clear if there are infinitely many or if this approach will even find them.

References

[Cal06] J Calcut. Rationality and the tangent function. *preprint*, 2006. `http://www2.oberlin.edu/faculty/jcalcut/tanpap.pdf`, Accesed: 2017-07-01.

[CCG08] Brian Conrad, Keith Conrad, and Robert Gross. Prime specialization in genus 0. *Transactions of the American Mathematical Society*, 360(6):2867–2908, 2008.

[Cha08] Byungchul Cha. Chebyshevs bias in function fields. *Compositio Mathematica*, 144(6):1351–1374, 2008.

[ES16] Jan-Hendrik Evertse and Efthymios Sofos. Analytic number theory, Fall 2016. `http://pub.math.leidenuniv.nl/~evertsejh/ant.shtml`.

[GM06] Andrew Granville and Greg Martin. Prime number races. *The American Mathematical Monthly*, 113(1):1–33, 2006.

[Hay66] David Hayes. The expression of a polynomial as a sum of three irreducibles. *Acta Arithmetica*, 11(4):461–488, 1966.

[HW08] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 2008.

[Pol06] Paul Pollack. An explicit approach to the hypothesis h for polynomials over a finite fields. *In Proceedings of the Anatomy of Integers Conference, Montréal*, 2006.

[Pol08] Paul Pollack. *Prime polynomials over finite fields*. PhD thesis, Dartmouth College, 2008.

[Ros02] Micheal Rosen. *Number Theory in Function Fields*. Springer, 2002.

[RS94] Michael Rubinstein and Peter Sarnak. Chebyshev's bias. *Experimental Mathematics*, 3(3):173–197, 1994.

[Rud15] Zeev Rudnick. Some problems in analytic number theory for polynomials over a finite field. *arXiv preprint arXiv:1501.01769*, 2015.