On the application of a generalization of Artin's primitive root conjecture in the theory of monoid rings

Spencer Chapman

Trinity University, Department of Mathematics

schapma3@trinity.edu

NCUR 2023 at UW EAU Claire

Introduction and Motivation

The focus of this research is to understand factorization in monoid rings, and how the properties of factorization tell us information about underlying structures.

Introduction and Motivation

The focus of this research is to understand factorization in monoid rings, and how the properties of factorization tell us information about underlying structures.

We will be discussing:

Introduction and Motivation

The focus of this research is to understand factorization in monoid rings, and how the properties of factorization tell us information about underlying structures.

We will be discussing:

- An introduction to monoid rings, along with examples of factorization within them

Introduction and Motivation

The focus of this research is to understand factorization in monoid rings, and how the properties of factorization tell us information about underlying structures.

We will be discussing:

- An introduction to monoid rings, along with examples of factorization within them
- Some results describing factorization

Introduction and Motivation

The focus of this research is to understand factorization in monoid rings, and how the properties of factorization tell us information about underlying structures.

We will be discussing:

- An introduction to monoid rings, along with examples of factorization within them
- Some results describing factorization, along with their immediate failure when attempting to generalize them

Introduction and Motivation

The focus of this research is to understand factorization in monoid rings, and how the properties of factorization tell us information about underlying structures.

We will be discussing:

- An introduction to monoid rings, along with examples of factorization within them
- Some results describing factorization, along with their immediate failure when attempting to generalize them
- A method of characterizing to what extend this "failure" occurs using collections of prime numbers

Introduction and Motivation

The focus of this research is to understand factorization in monoid rings, and how the properties of factorization tell us information about underlying structures.

We will be discussing:

- An introduction to monoid rings, along with examples of factorization within them
- Some results describing factorization, along with their immediate failure when attempting to generalize them
- A method of characterizing to what extend this "failure" occurs using collections of prime numbers
- Results about these collections, implied by Artin's Primitive Root Conjecture

Introduction and Motivation

The focus of this research is to understand factorization in monoid rings, and how the properties of factorization tell us information about underlying structures.

We will be discussing:

- An introduction to monoid rings, along with examples of factorization within them
- Some results describing factorization, along with their immediate failure when attempting to generalize them
- A method of characterizing to what extend this "failure" occurs using collections of prime numbers
- Results about these collections, implied by Artin's Primitive Root Conjecture
- A method of generating these primes relatively easily, and using these as justification for the conjecture

Building our toolbox:

We define the *Monoid Ring* $\mathbb{F}[X; M]$ as the set of formal sums of the form

$$\sum_{m \in M} a_m X^m,$$

where $a_m \in \mathbb{F}$ for each $m \in M$, and $a_m = 0$ for all but finitely many m, where $\mathbb{F}$ is a field, and M a commutative additive monoid.

Building our toolbox:

We define the *Monoid Ring* $\mathbb{F}[X; M]$ as the set of formal sums of the form

$$\sum_{m \in M} a_m X^m,$$

where $a_m \in \mathbb{F}$ for each $m \in M$, and $a_m = 0$ for all but finitely many m, where $\mathbb{F}$ is a field, and M a commutative additive monoid.

If $M = \mathbb{N}_0$, then our monoid ring is $\mathbb{F}[X]$, the set of "polynomials" with coefficients from $\mathbb{F}$ that we're familiar with. Changing $\mathbb{F}$ or M changes what these elements look like.

The set $\mathbb{F}[X; M]$ forms a ring under the "typical" polynomial addition and multiplication. Studying the factorization in various fields or rings can be valuable in understanding the behavior of these structures.

The set $\mathbb{F}[X;M]$ forms a ring under the "typical" polynomial addition and multiplication. Studying the factorization in various fields or rings can be valuable in understanding the behavior of these structures.

However, sometimes it can be interesting to vary what our exponents are. That is, to change our monoid M.

The set $\mathbb{F}[X; M]$ forms a ring under the "typical" polynomial addition and multiplication. Studying the factorization in various fields or rings can be valuable in understanding the behavior of these structures.

However, sometimes it can be interesting to vary what our exponents are. That is, to change our monoid M.

Let us consider the restriction $M = \mathbb{N}_0 \setminus \{1\}$; This restriction is very useful, in that the irreducibles of M are exacly the prime numbers. For our polynomials however, we completely lose linear terms. While $\mathbb{F}[X; M]$ is still a subring of $\mathbb{F}[X]$, its properties of factorization are entirely different.

For example, $X^2 - 1 = (X - 1)(X + 1)$ no longer holds!
Restricting the elements of M completely changes our factorization.

Our general question is: to what extent do "additive factorization" properties in M descend to multiplicative factorization properties in these "restricted" polynomials of $\mathbb{F}[X; M]$?

Our general question is: to what extent do "additive factorization" properties in M descend to multiplicative factorization properties in these "restricted" polynomials of $\mathbb{F}[X; M]$?

Let us consider the binomial $X^n - 1$.
In $\mathbb{Q}[X]$, we always have the following factorization:

$$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \cdots + X + 1).$$

Once we say $1 \notin M$ however, this no longer holds in $\mathbb{Q}[X; M]$.

Our general question is: to what extent do "additive factorization" properties in M descend to multiplicative factorization properties in these "restricted" polynomials of $\mathbb{F}[X; M]$?

Let us consider the binomial $X^n - 1$.
In $\mathbb{Q}[X]$, we always have the following factorization:

$$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \cdots + X + 1).$$

Once we say $1 \notin M$ however, this no longer holds in $\mathbb{Q}[X; M]$.

Is it perhaps that factorization of such a binomial changes form completely like when we vary our coefficient fields? Or is it that this binomial is now just irreducible?

We will need two more definitions:

- The *Characteristic* of $\mathbb{F}$: The smallest $n \in \mathbb{N}$ such that $n \cdot 1_{\mathbb{F}} = 0$. char($\mathbb{F}$) will either be prime, or zero if no such n exists.
- An element $\pi \in M$ is "indivisible" if $n \cdot \alpha = \pi$ with $n \in \mathbb{N}, \alpha \in M$ implies that $n = 1$ and $\alpha = \pi$.
  We say that such a number is an "additive irreducible" in M.

We will need two more definitions:

- The *Characteristic* of $\mathbb{F}$: The smallest $n \in \mathbb{N}$ such that $n \cdot 1_{\mathbb{F}} = 0$. char($\mathbb{F}$) will either be prime, or zero if no such n exists.
- An element $\pi \in M$ is "indivisible" if $n \cdot \alpha = \pi$ with $n \in \mathbb{N}, \alpha \in M$ implies that $n = 1$ and $\alpha = \pi$.
  We say that such a number is an "additive irreducible" in M.

Theorem (Kulosman, et. al.)

Suppose M is a submonoid of $\mathbb{Q}_0^+$. For any field $\mathbb{F}$ of characteristic zero, and any "indivisible" $\pi \in M$, the binomial $X^\pi - 1$ is irreducible in $\mathbb{F}[X; M]$.

We will need two more definitions:

- The *Characteristic* of $\mathbb{F}$: The smallest $n \in \mathbb{N}$ such that $n \cdot 1_{\mathbb{F}} = 0$. char($\mathbb{F}$) will either be prime, or zero if no such n exists.
- An element $\pi \in M$ is "indivisible" if $n \cdot \alpha = \pi$ with $n \in \mathbb{N}, \alpha \in M$ implies that $n = 1$ and $\alpha = \pi$.
  We say that such a number is an "additive irreducible" in M.

Theorem (Kulosman, et. al.)

Suppose M is a submonoid of $\mathbb{Q}_0^+$. For any field $\mathbb{F}$ of characteristic zero, and any "indivisible" $\pi \in M$, the binomial $X^\pi - 1$ is irreducible in $\mathbb{F}[X; M]$.

In an attempt to generalize these results, what happens if $\mathbb{F}$ has *positive* characteristic? In particular, what if $p \cdot 1_{\mathbb{F}} = 0$ for some prime p?

The simplest such case to consider is $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
Under the restriction of $M = \mathbb{N}_0 \setminus \{1\}$, Kulosman showed that

$$X^7 - 1 = (X^4 + X^3 + X^2 + 1)(X^3 + X^2 + 1) \quad \text{in } \mathbb{F}_2[X; M].$$

The simplest such case to consider is $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
Under the restriction of $M = \mathbb{N}_0 \setminus \{1\}$, Kulosman showed that

$$X^7 - 1 = (X^4 + X^3 + X^2 + 1)(X^3 + X^2 + 1) \quad \text{in } \mathbb{F}_2[X; M].$$

So, the previous theorem immediately fails in a very simple example of a prime characteristic field. Is this always the case?

The simplest such case to consider is $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
Under the restriction of $M = \mathbb{N}_0 \setminus \{1\}$, Kulosman showed that

$$X^7 - 1 = (X^4 + X^3 + X^2 + 1)(X^3 + X^2 + 1) \quad \text{in } \mathbb{F}_2[X; M].$$

So, the previous theorem immediately fails in a very simple example of a prime characteristic field. Is this always the case?

We want to know when $X^q - 1$, with q prime, is irreducible in $\mathbb{F}_p[X; M]$, where $\mathbb{F}_{|} = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$, and $M = \mathbb{N}_0 \setminus \{1\}$.

Will it be that $X^q - 1$ always factors in $\mathbb{F}_p[X; M]$? How can we quantify the exceptions to the previous theorem?

Current Work

Definition

Let $E(p) = \{q \text{ prime} \mid X^q - 1 \text{ factors in } \mathbb{F}_p[X; M]\}$ be the set of *exceptional primes* for p.

This set quantifies the *failure* of the previous theorem in a field of characteristic p.

Current Work

Definition

Let $E(p) = \{q \text{ prime} \mid X^q - 1 \text{ factors in } \mathbb{F}_p[X; M]\}$ be the set of *exceptional primes* for p.

This set quantifies the *failure* of the previous theorem in a field of characteristic p.

Current Work

Definition

Let $E(p) = \{q \text{ prime} \mid X^q - 1 \text{ factors in } \mathbb{F}_p[X; M]\}$ be the set of *exceptional primes* for p.

This set quantifies the *failure* of the previous theorem in a field of characteristic p.

Conjecture

The set $E(p)$ is nonempty for all primes p.

Current Work

Definition

Let $E(p) = \{q \text{ prime} \mid X^q - 1 \text{ factors in } \mathbb{F}_p[X; M]\}$ be the set of *exceptional primes* for p.

This set quantifies the *failure* of the previous theorem in a field of characteristic p.

Conjecture

The set $E(p)$ is nonempty for all primes p.

Theorem (Daileda)

Assume the Generalized Riemann Hypothesis.
Then $E(p)$ is infinite for all p.

In particular, in terms of Artin's Primitive Root Conjecture, which is true under GRH, the sets $E(2)$ and $E(3)$ can be completely described as follows:

$$E(2) = \{q \neq 2 \mid [(\mathbb{Z}/q\mathbb{Z})^{\times} : \langle 2 \rangle] > 1\}$$

In particular, in terms of Artin's Primitive Root Conjecture, which is true under GRH, the sets $E(2)$ and $E(3)$ can be completely described as follows:

$$E(2) = \{q \neq 2 \mid [(\mathbb{Z}/q\mathbb{Z})^\times : \langle 2 \rangle] > 1\}$$

That is, $E(2)$ is the set of all primes not equal to 2, where the powers of 2 mod q do not yield all of $(\mathbb{Z}/q\mathbb{Z})^\times$. The same may be said for $E(3)$.

In particular, in terms of Artin's Primitive Root Conjecture, which is true under GRH, the sets $E(2)$ and $E(3)$ can be completely described as follows:

$$E(2) = \{q \neq 2 \mid [(\mathbb{Z}/q\mathbb{Z})^\times : \langle 2 \rangle] > 1\}$$

That is, $E(2)$ is the set of all primes not equal to 2, where the powers of 2 mod q do not yield all of $(\mathbb{Z}/q\mathbb{Z})^\times$. The same may be said for $E(3)$.

Under GRH, the set

$$E_2(p) = \{q \in E(p) \mid [(\mathbb{Z}/q\mathbb{Z})^\times : \langle p \rangle] = 2\}$$

is infinite, implying that $E(p)$ is infinite and in turn, nonempty.

The Problem:

From the previous descriptions,

$$E(2) = \{7, 17, 23, 31, 41, 43, 47, 71, 73, 79, 89, 97, \ldots\},$$

$$E(3) = \{11, 13, 23, 37, 41, 47, 59, 61, 67, 71, 73, 83, 97, \ldots\}.$$

The sets $E(2)$ and $E(3)$ are well understood.
However, this isn't a silver bullet;

The Problem:

From the previous descriptions,

$$E(2) = \{7, 17, 23, 31, 41, 43, 47, 71, 73, 79, 89, 97, \ldots\},$$

$$E(3) = \{11, 13, 23, 37, 41, 47, 59, 61, 67, 71, 73, 83, 97, \ldots\}.$$

The sets $E(2)$ and $E(3)$ are well understood.
However, this isn't a silver bullet;

$$\text{For } p \geq 5, E_2(p) \neq E(p).$$

Only some primes of $E(p)$ with $p \geq 5$ have been described. These few were enough to yield the previous theorem, but we are interested in what *exactly* is inside $E(p)$.

So, what else is in $E(p)$?

The Project

The goal of this project was to construct an algorithm to generate the elements of $E(p)$ for any given prime p.

Maple was chosen for the programming because the availability of relatively quick factoring makes work a bit easier.

To restate:
Given primes $p \neq q$, define a function that returns true if $X^q - 1$ factors in $\mathbb{F}_p[X; M]$, and false otherwise. We then iterate this function over a set of primes to generate $E(p)$.

To restate:
Given primes $p \neq q$, define a function that returns true if $X^q - 1$ factors in $\mathbb{F}_p[X; M]$, and false otherwise. We then iterate this function over a set of primes to generate $E(p)$.

The first approach that I considered was just brute-forcing the generation; Given a binomial $X^q - 1$, assume there exists a factorization

$$X^q - 1 = (a_m X^m + \cdots + a_1 X^2 + a_0)(b_n X^n + \cdots + b_1 X^2 + b_0),$$

with $a_i, b_j \in \mathbb{F}_p$, and $m, n \in \mathbb{N}$ such that $q = m + n$.

We would then iterate through every sequence of a_i, b_j since $\mathbb{F}_P$ is finite, and then compute the products until one equals $X^q - 1$.

To restate:
Given primes $p \neq q$, define a function that returns true if $X^q - 1$ factors in $\mathbb{F}_p[X; M]$, and false otherwise. We then iterate this function over a set of primes to generate $E(p)$.

The first approach that I considered was just brute-forcing the generation; Given a binomial $X^q - 1$, assume there exists a factorization

$$X^q - 1 = (a_m X^m + \cdots + a_1 X^2 + a_0)(b_n X^n + \cdots + b_1 X^2 + b_0),$$

with $a_i, b_j \in \mathbb{F}_p$, and $m, n \in \mathbb{N}$ such that $q = m + n$.

We would then iterate through every sequence of a_i, b_j since $\mathbb{F}_P$ is finite, and then compute the products until one equals $X^q - 1$.

However, this proved to be way too daunting after just a few iterations, so this idea was scraped. Is there a way to simplify the work we need?

The Solution

Recall the trivial factorization in $\mathbb{Q}[X]$:

The Solution

Recall the trivial factorization in $\mathbb{Q}[X]$:

$$X^q - 1 = (X-1)(X^{q-1} + X^{q-2} + \cdots + X + 1).$$

The Solution

Recall the trivial factorization in $\mathbb{Q}[X]$:

$$X^q - 1 = (X-1)(X^{q-1} + X^{q-2} + \cdots + X + 1).$$

This factorization no longer holds in $\mathbb{Q}[X;M]$, much less in $\mathbb{F}_p[X;M]$. The righthand term is known as the *qth Cyclotomic Polynomial*, and is often denoted by Φ_q.

The Solution

Recall the trivial factorization in $\mathbb{Q}[X]$:

$$X^q - 1 = (X - 1)(X^{q-1} + X^{q-2} + \cdots + X + 1).$$

This factorization no longer holds in $\mathbb{Q}[X;M]$, much less in $\mathbb{F}_p[X;M]$. The righthand term is known as the *qth Cyclotomic Polynomial*, and is often denoted by Φ_q.

The cyclotomic polynomials are monic polynomials, and are irreducible over $\mathbb{Z}$ and $\mathbb{Q}$. However, Φ_q is not irreducible over a finite field.

In fact, over a finite field $\mathbb{F}_p$, Φ_q factorizes into $\varphi(q)/d$ irreducible polynomials, each of degree d, where $\varphi(d)$ is Euler's totient function, and d is the order of p modulo q.

In fact, over a finite field $\mathbb{F}_p$, Φ_q factorizes into $\varphi(q)/d$ irreducible polynomials, each of degree d, where $\varphi(d)$ is Euler's totient function, and d is the order of p modulo q.

If any such factor of Φ_q has no linear term, it follows that $X^q - 1$ factors in $\mathbb{F}_p[X; M]$.

That is, if the followings holds:

$$\Phi_q(X) = f(X) \cdot (\cdots + aX^2 + b),$$

with $f(X)$ any monic polynomial in $\mathbb{F}_p[X]$, then $q \in E(p)$.

This leads us to the following algorithm:

Algorithm (Pseudocode)

Given q prime:

1. Compute all factors of Φ_q
2. Test which factors have no linear terms:
    1. If there exists a factor with no linear term, $q \in E(p)$
    2. Else, $q \notin E(p)$

Algorithm (Pseudocode)

Given q prime:

1. Compute all factors of Φ_q
2. Test which factors have no linear terms:
   1. If there exists a factor with no linear term, $q \in E(p)$
   2. Else, $q \notin E(p)$

To construct an array of factors of Φ_q, we define

```
local F := (Factors(NumberTheory:-Phi(q,X)) mod p)[2];
```

The function **Factors(a)** returns a list of the form $[u, [[f_1, e_1], \ldots, [f_n, e_n]]]$ such that $a = uf_1^{e_1} \cdots f_n^{e_n}$, with each $f[i]$ an irreducible polynomial.

So we have the factors of Φ_q, now we need to compute all possible products of them.

Recall that in a finite field, Φ_q factorizes into $\varphi(q)/d$ irreducible polynomials, each with degree d. So, each term in our list of factors will have multiplicity of one.

This is analogous to an Φ_q being a square-free integer, and calculating each divisor of the integer.

$$\begin{aligned} 106590 &= 2^1 \cdot 3^1 \cdot 5^1 \cdot 11^1 \cdot 17^1 \cdot 19^1 \\ 1045 &= 2^0 \cdot 3^0 \cdot 5^1 \cdot 11^1 \cdot 17^0 \cdot 19^1 \end{aligned}$$

Recall that in a finite field, Φ_q factorizes into $\varphi(q)/d$ irreducible polynomials, each with degree d. So, each term in our list of factors will have multiplicity of one.

This is analogous to an Φ_q being a square-free integer, and calculating each divisor of the integer.

$$106590 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 11^1 \cdot 17^1 \cdot 19^1$$
$$1045 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 11^1 \cdot 17^0 \cdot 19^1$$

As such, to calculate the products, we then iterate through all binary sequences of length $\varphi(q)/d$, take each term in F, and put it to the power of the corresponding digit in the binary sequence.

For example, if we have the sequence 001101, we would then compute

$$T := f_1^0 f_2^0 f_3^1 f_4^1 f_5^0 f_6^1.$$

First, we will pull out only the factors of Φ_q and disregard the exponents:

```
for i from 1 to r do F[i] := F[i][1]; end do;
```

First, we will pull out only the factors of Φ_q and disregard the exponents:

```
for i from 1 to r do F[i] := F[i][1]; end do;
```

Then, given an integer j, we convert it to a binary sequence of length r by

```
local b := map2(nprintf,cat("%0",r,"d"),convert(j,binary));
```

First, we will pull out only the factors of Φ_q and disregard the exponents:

```
for i from 1 to r do F[i] := F[i][1]; end do;
```

Then, given an integer j, we convert it to a binary sequence of length r by

```
local b := map2(nprintf,cat("%0",r,"d"),convert(j,binary));
```

Next we take this sequence b, and create a list E of its digits:

```
local E := map(parse,StringTools:-Explode(convert(b,string)));
```

First, we will pull out only the factors of Φ_q and disregard the exponents:

```
for i from 1 to r do F[i] := F[i][1]; end do;
```

Then, given an integer j, we convert it to a binary sequence of length r by

```
local b := map2(nprintf,cat("%0",r,"d"),convert(j,binary));
```

Next we take this sequence b, and create a list E of its digits:

```
local E := map(parse,StringTools:-Explode(convert(b,string)));
```

Fr this list, put each factor to the power the corresponding digit in the list, and multiply the factors together:

First, we will pull out only the factors of Φ_q and disregard the exponents:

```
for i from 1 to r do F[i] := F[i][1]; end do;
```

Then, given an integer j, we convert it to a binary sequence of length r by

```
local b := map2(nprintf,cat("%0",r,"d"),convert(j,binary));
```

Next we take this sequence b, and create a list E of its digits:

```
local E := map(parse,StringTools:-Explode(convert(b,string)));
```

Fr this list, put each factor to the power the corresponding digit in the list, and multiply the factors together:

```
for k from 1 to s do T := T * (F[k]^E[k]); end do;
```

Lastly, we take the resulting term T, and check for linear terms:

```
if evalb(coeff(T,X,1) mod p = 0) then return 1 fi;
```

Putting these steps in a for-loop for each binary sequence b up to $2^r - 1$ will accurately check if q is exceptional.

Putting this all together, we have the following code:

```
> isExceptional := proc (q,p)
      local F := (Factors(NumberTheory:-Phi(q,X)) mod p)[2];
      local r := nops(F);
      local i := 1;
      for i from 1 to r do F[i] := F[i][1]; end do;
      local j := 1;
      for j from 1 to 2^r - 1 do
          local b := map2(nprintf,cat("%0",r,"d"),convert(j,binary));
          local E := map(parse,StringTools:-Explode(convert(b,string)));
          local s := nops(E);
          local k := 1;
          local T:= 1;
          for k from 1 to s do T := T * (F[k]^E[k]); end do;
          T := expand(T);
          if evalb(coeff(T,X,1) mod p = 0) then return 1 fi;
      end do;
      return 0;
  end proc;
```

Then by simply running this procedure through a for-loop of primes, we have $E(p)$.

```
Exceptionals := proc(p,n)
    local P:={};
    for i from 2 to n do
        if isprime(i) then
            if evalb(isExceptional(i,p) = 1) then
                P := P union {i};
            end if;
        end if;
    end do;
return P;
end proc;
```

By this algorithm, here are a few exceptionals less than 100:

$> E2 := Exceptionals(2, 100)$

$$E2 := \{7, 17, 23, 31, 41, 43, 47, 71, 73, 79, 89, 97\}$$

$> E3 := Exceptionals(2, 100)$

$$E3 := \{7, 17, 23, 31, 41, 43, 47, 71, 73, 79, 89, 97\}$$

$> E2 := Exceptionals(2, 100)$

$$E2 := \{7, 17, 23, 31, 41, 43, 47, 71, 73, 79, 89, 97\}$$

$> E3 := Exceptionals(3, 100)$

$$E3 := \{11, 13, 23, 37, 41, 47, 59, 61, 67, 71, 73, 83, 97\}$$

$> E5 := Exceptionals(5, 100)$

$$E5 := \{13, 19, 31, 41, 59, 61, 67, 71, 79\}$$

$> E7 := Exceptionals(7, 100)$

$$E7 := \{19, 29, 37, 43, 83\}$$

$> E11 := Exceptionals(11, 100)$

$$E11 := \{19, 37, 43, 61, 89\}$$

$> E13 := Exceptionals(13, 100)$

$$E13 := \{53, 61\}$$

Figure: Exceptional Primes Generated By Maple

Continued Work

Notice the scarcity of Exceptionals as we increase the size of our coefficient field. From Dr. Daileda's Theorem, not only is each $E(p)$ infinite, but the subset $E_2(p) \subseteq E(p)$ has a *theoretical* density $a(p)$, defined by

$$d(E_2(p)) = a(p) = \frac{3}{4}\left(\frac{2p-1}{p^2-p-1}\right) A \neq 0,$$

where A is Artin's constant. This density implies that $E(p)$ is infinite if Artin's Conjecture holds.

Continued Work

Empirical evidence seems to suggest that our theoretical density is indeed true. Tabulating these densities also reveals some interesting phenomenon.

Table 1: Approximate and conjectural densities of $E_2(p)$

p	$\pi_p(10^6)/\pi(10^6)$	$a(p)$
2	0.28143	0.28046
3	0.30052	0.28046
5	0.13815	0.13285
7	0.09112	0.08892
11	0.05461	0.05403
13	0.04635	0.04523
17	0.03448	0.03415
19	0.03076	0.03043
23	0.02563	0.02499
29	0.01949	0.01971

Thank you!

References

1. R. C. Daileda, *On the Irreducibility of* $X^q - 1$ *in Monoid Rings with Positive Characteristic*, preprint, https://arxiv.org/abs/2112.09080

Contact me or my advisor!

1. Spencer Chapman, Undergraduate, schapma3@trinity.edu
2. Dr. Ryan Daileda, Associate Professor, rdaileda@trinity.edu

Special Thanks to Trinity University for research funding, and to UW EAU Claire and NCUR for hosting us!