Partial zeta functions for $y - x^n$

Noah Bertram
Advised by Doug Haessig

May 17, 2021

Abstract

A partial zeta function is a type of generating function for the number of solutions to systems of polynomials over finite fields introduced by Wan [2] to generalize local zeta functions. Wan [3] proved, as in the case with local zeta functions, that partial zeta functions are rational functions over $\mathbb{Q}$. Here we examine examples of these partial zeta functions for low degree polynomials, then after noting their sporadic behavior relative to local zeta functions, we find the partial zeta function for the system of polynomials $y - x^n$, in the case when n does not divide the characteristic of the finite field.

1 Introduction

Generating functions are a powerful tool used in number theory to study sequences. Local zeta functions are a special type of generating function that give insight to certain kinds of numerical sequences, while also having connections with famous number theoretic functions such as the Riemann zeta function. Of interest, is a generalization of local zeta functions, which are known as partial zeta functions. While some properties of local zeta functions have been shown to generalize to partial zeta functions, we would like to understand how far this extension goes, and it is of interest to understand how well behaved partial zeta functions are, relative to local zeta functions. This paper intends to explore this avenue by computing, what at least were initially thought to be, simple examples of partial zeta functions.

2 Background

Fix $\mathbb{F}_q$ to be the finite field of q elements. Let X be a finite set of polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$. We define

$$N(m) = \#\{x \in \mathbb{F}_{q^m}^n \mid f(x) = 0, f \in X\},$$

that is, the number of points in $\mathbb{F}_{q^m}^n$ that are roots to all polynomials in X. We construct the following function in order to study $\{N(m)\}_{m=1}^{\infty}$:

$$z(T, X) = \exp\left(\sum_{m=1}^{\infty} \frac{N(m)}{m} T^m\right),$$

which is known as a *local zeta function*. These functions are thoroughly studied and well understood. It was proven by Dwork [1] that this is a rational function over $\mathbb{Q}$. This function will not be studied in this paper. Instead, we will study a generalization of it. Let $D = (d_1, d_2, \ldots, d_n)$ where $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 1}^n$. We define

$$N_D(m) = \{x \in \mathbb{F}_{q^{d_1 m}} \times \cdots \times \mathbb{F}_{q^{d_n m}} \mid f(x) = 0, f \in X\}.$$

As above, we construct the following function in order to study $\{N_D(m)\}_{m=1}^{\infty}$, first introduced in [2]:

$$z(T, X, D) = \exp\left(\sum_{m=1}^{\infty} \frac{N_D(m)}{m} T^m\right), \tag{1}$$

which we refer to as the *partial local zeta function of* X. One will notice that in the case that $D = (1, 1, \ldots, 1)$, the partial zeta function reduces to the local zeta function, hence its name. When both X and D are clear, we refer to $z(T, X, D)$ as $z(T)$ and $N_D(m)$ as $N(m)$. We now state an important fact concerning partial zeta functions. Fix X and D.

Theorem 2.1. *$z(T)$ is a rational function, over the rational numbers, in T [3].*

We would like to view the structure of these rational functions, and how much they differ from the case when $D = (1, \ldots, 1)$. For a primer, we find the partial zeta function for $X = ax + by + c$.

Linear. Let X be the singleton set containing a polynomial of the form $f(x,y) = ax + by + c \in \mathbb{F}_p[x,y]$, where $x \in \mathbb{F}_{p^{md_1}}$ and $y \in \mathbb{F}_{p^{md_2}}$, so that $D = (d_1, d_2)$. First for comparison, it is known that

$$z(T) = \frac{1}{1-pT},$$

when $D = (1,1)$. To compute the partial zeta function, we find explicitly the sequence $\{N(m)\}_{m=1}^{\infty}$, which means we need to find the number of pairs that are solutions to $f(x,y)$. To find a solution pair, it must be the case that $ax+by+c=0$. Since addition and multiplication are bijections in fields, we have for every x and y, $c = a(-x + a^{-1}z) + b(-y + b^{-1}w)$ for some z and w. Thus we can write

$$\begin{aligned} 0 = ax + by + c &= ax + by + a(-x + a^{-1}z) + b(-y + b^{-1}w) \\ &= a(x - x + a^{-1}z) + b(y - y + b^{-1}w) \\ &= aa^{-1}z + bb^{-1}w \\ &= z + w, \end{aligned}$$

so finding the number of solutions to $ax+by+c$ is equivalent to finding the number of solutions to $x + y = 0$. But from here it is clear that $x = -y$ are all solutions, but this only occurs when x and y are members of the same field. It is known that $\mathbb{F}_{p^{md_1}}$ shares $p^{\gcd(md_1, md_2)}$ elements with $\mathbb{F}_{p^{md_2}}$, hence $N(m) = p^{md}$, where we let $d = \gcd(d_1, d_2)$. This gives the zeta function

$$\begin{aligned} z(T) = \exp\left(\sum_{m=1}^{\infty} \frac{N(m)T^m}{m}\right) &= \exp\left(\sum_{m=1}^{\infty} \frac{p^{md}T^m}{m}\right) \\ &= \exp\left(-\log(1-p^dT)\right) \\ &= \frac{1}{1-p^dT}. \end{aligned}$$

This gives one of the most basic examples of a partial zeta function.

3 Partial zeta functions for $y - x^n$

We try in some way to extend this approach to a broader family of polynomials. Consider, $X = \{y - x^n\}$, for $x \in \mathbb{F}_{p^{md_1}}$, $y \in \mathbb{F}_{p^{md_2}}$, and suppose that p does not divide n. Also let $\gcd(d_1, d_2) = d$ as above. We have the following helpful tool.

Proposition 3.1. *Let $X = \{y - x^n\}$ and $D = (d_1, d_2)$. Then we have that*

$$N_D(m) = \gcd(n, M_m)(p^{md} - 1) + 1, \tag{2}$$

where

$$M_m = \sum_{i=0}^{(d_1/d)-1} (p^{md})^i. \tag{3}$$

Proof. For $y = x^n$ to be satisfied, it must be that x^n lies in $\mathbb{F}_{p^{md_2}}$. Therefore the number of solutions to $y = x^n$ is the number of members of $\mathbb{F}_{p^{md_1}}$ that lie in both $\mathbb{F}_{p^{md_2}}$ and are nth powers. Let $q_1 = p^{md_1}$ and $q_2 = p^{md_2}$. It is known that $(\mathbb{F}_{q_1}^\times, \cdot)$ is cyclic of order $q_1 - 1$. So let α be a generator of $(\mathbb{F}_{q_1}^\times, \cdot)$ and consider β^n, where β is any arbitrary element. Then $\beta^n = (\alpha^k)^n = \alpha^{kn}$ for some non-negative integer k, so that $\beta^n \in \langle \alpha^n \rangle$. Conversely, α^{kn} for any non-negative integer k is an nth power of α^k. These facts imply that the set of nth powers is exactly $\langle \alpha^n \rangle$, which has size $\frac{q_1 - 1}{\gcd(q_1 - 1, n)}$.

Let $r = p^{md}$ and consider q_1 and q_2 as before. It is known that $\mathbb{F}_{q_1} \cap \mathbb{F}_{q_2} = \mathbb{F}_r$ which implies that $(\mathbb{F}_{q_1}^\times, \cdot) \cap (\mathbb{F}_{q_2}^\times, \cdot) = (\mathbb{F}_r^\times, \cdot)$, so that $(\mathbb{F}_r^\times, \cdot)$ is the only subgroup of order $r - 1$ in $(\mathbb{F}_{q_1}^\times, \cdot)$. Consider α again to be a generator of $(\mathbb{F}_{q_1}^\times, \cdot)$. Then $\alpha^k \in (\mathbb{F}_r^\times, \cdot)$ if and only if $\frac{q_1 - 1}{r - 1}$ divides k. Combining with the previous paragraph, $\alpha^{nk} \in (\mathbb{F}_r^\times, \cdot)$ if and only if $\frac{q_1 - 1}{r - 1}$ divides nk.

As is clear from the last paragraph, $r - 1$ divides $q_1 - 1$. This means that $p^{md} - 1$ divides $p^{md_1} - 1$. This fact is also made clear as

$$(p^{md} - 1) \sum_{i=0}^{(d_1/d)-1} (p^{md})^i = \sum_{i=0}^{(d_1/d)-1} (p^{md})^{i+1} - (p^{md})^i = (p^{md})^{d_1/d} - 1 = p^{md_1} - 1.$$

So let $M = \sum_{i=0}^{(d_1/d)-1} (p^{md})^i$. Then $\alpha^{nk} \in (\mathbb{F}_r^\times, \cdot)$ if and only if M divides nk. But now recall that the number of solutions to $y = x^n$ is the number of nth powers of $(\mathbb{F}_{q_1}^\times, \cdot)$ that lie in $(\mathbb{F}_r^\times, \cdot)$. For simplicity define the notation for $a, b \in \mathbb{Z}$ and a dividing b,

$$[a, b] = \{a, 2a, 3a, \ldots, b\}. \tag{4}$$

Now we can write

$$\begin{aligned} \{(x, y) \in \left(\mathbb{F}_{q_1}^\times, \cdot\right) \times \left(\mathbb{F}_{q_2}^\times, \cdot\right) : y = x^2\} &= \{\alpha^k : k \in [1, q_1 - 1], \alpha^{nk} \in \left(\mathbb{F}_r^\times, \cdot\right)\} \\ &= \{\alpha^k : k \in [1, q_1 - 1], M | nk\}. \end{aligned}$$

Therefore including $x = y = 0$,

$$\begin{aligned} N_D(m) &= \#\{k \in [1, q_1 - 1] : M \mid nk\} + 1 \\ &= \#\{k \in [n, n(p^{d_1 m} - 1)] : M \mid k\} + 1 \\ &= \#\{k \in [1, n(p^{d_1 m} - 1)] : M, n \mid k\} + 1 \\ &= \#\{k \in [M, n(p^{dm} - 1)M] : n \mid k\} + 1, \end{aligned} \tag{5}$$

where the last line uses the fact that $(p^{dm} - 1)M = p^{d_1 m} - 1$. Now any $Mk \in [M, n(p^{dm} - 1)M]$ is divided by n if and only if $n/\gcd(M, n)$ divides k. Thus

$$\begin{aligned} \{Mk : k \in [1, n(p^{dm} - 1)], n \mid Mk\} &= \left\{ Mk : k \in [1, n(p^{dm} - 1)], \frac{n}{\gcd(M, n)} \text{ divides } k \right\} \\ &= \left\{ \frac{nM}{\gcd(n, M)} k : k \in [1, \gcd(n, M)(p^{dm} - 1)] \right\}, \end{aligned}$$

which means that (5) becomes

$$\#\left\{ \frac{nM}{\gcd(n, M)} k : k \in [1, \gcd(n, M)(p^{dm} - 1)] \right\} + 1,$$

resulting in

$$N_D(m) = \gcd(n, M)(p^{dm} - 1) + 1,$$

completing the proof. □

It is important to note that M depends on m, so that $\gcd(n, M)$ is not a constant. We will see in a moment that this provides complications. But for comparison, it is not difficult to see that $N(m) = p^m$ when $D = (1, 1)$.

Example 3.1. Consider $X = \{y - x^2\}$. This means by the above proposition, $N(m) = \gcd(2, M)(p^{dm} - 1) + 1$. Now if d_1/d is odd, since $(p^{dm})^i$ is odd for any i and m when $p \neq 2$, we have that M is odd hence $\gcd(2, M) = 1$. In a similar manner, when d_1/d is even, we have that M is even hence $\gcd(2, M) = 2$. When $p = 2$, we have that M is always even so $\gcd(2, M) = 2$. Therefore

$\{\gcd(n, M)\}_{m=1}^{\infty}$ is constant. Thus

$$\begin{aligned} z(T) &= \exp\left(\sum_{m=1}^{\infty} \frac{N(m)}{m} T^m\right) = \exp\left(\sum_{m=1}^{\infty} \frac{\gcd(2, M)(p^{dm} - 1) + 1}{m} T^m\right) \\ &= \exp\left(\gcd(2, M)\left(\sum_{m=1}^{\infty} \frac{p^{dm} T^m}{m} - \sum_{m=1}^{\infty} \frac{T^m}{m}\right) + \sum_{m=1}^{\infty}\left(\frac{T^m}{m}\right)\right) \\ &= \exp\left(\gcd(2, M)\left(\log(1 - p^d T) - \log(1 - T)\right) + \log(1 - T)\right) \\ &= \exp\left(\log\left((1 - p^d T)^{-\gcd(2,M)}\right) + \log\left((1 - T)^{\gcd(2,M)}\right) - \log(1 - T)\right) \\ &= \frac{(1 - T)^{\gcd(2,M)}}{(1 - T)(1 - p^d T)^{\gcd(2,M)}} \end{aligned}$$

which means that

$$z(T) = \begin{cases} \frac{1}{1-p^d T} & \text{for } p, d_1/d \text{ odd} \\ \frac{1-T}{(1-p^d T)^2} & \text{for } p \text{ even or } d_1/d \text{ even.} \end{cases} \tag{6}$$

This is the first nontrivial result.

We can use this fact to find the zeta functions for all quadratic polynomials, at least if we assume that $p \neq 2$. So now let $X = \{y - ax^2 - bx - c\}$ where $a, b, c \in \mathbb{F}_p$. Now $y - ax^2 - bx - c$ has as many roots as $y - x^2 - bx - c$, and since $p \neq 2$, we can complete the square to get that

$$y - x^2 - bx - c = y - x^2 - bx - (2^{-1}b)^2 - c + 2^{-1}b^2 = y - c + 2^{-1}b^2 - (x + 2^{-1}b)^2,$$

which is easy to see since addition and multiplication are bijections, has the same number of roots as $y - x^2$. This generalizes the formulas above. Again, we can compare this with $z(T)$, which is not hard to see, is the same as the linear case.

The result for $n = 2$ is fairly nice. Let's go one step up to see if it is just as nice.

Example 3.2. Let $X = \{y - x^3\}$. As we know,

$$N(m) = \gcd(3, M_m)(p^{dm} - 1) + 1.$$

We now need to characterize all the possible sequences of $\{\gcd(3, M_m)\}_{m=1}^{\infty}$. We now show that $\{\gcd(3, M_m)\}_{m=1}^{\infty}$ takes one of four forms:

$$1, 1, 1, 1, 1, 1, 1, 1, \ldots \tag{7}$$

$$3, 3, 3, 3, 3, 3, 3, 3, \ldots \tag{8}$$

$$3, 1, 3, 1, 3, 1, 3, 1, \ldots \tag{9}$$

$$1, 3, 1, 3, 1, 3, 1, 3, \ldots. \tag{10}$$

Again for a reminder, $M = \sum_{i=0}^{d_1/d-1} \left(p^{md}\right)^i$, where $D = (d_1, d_2)$, $d = \gcd(d_1, d_2)$ and m varies through all natural numbers. First if $p = 3$, then clearly $M = 1 \mod 3$ so that $\gcd(3, M_m) = 1$ for all m giving us (7). Secondly, if $p = 1 \mod 3$, we have that

$$M \mod 3 = \sum_{i=0}^{(d_1/d)-1} \left(p^{md}\right)^i \mod 3 = \sum_{i=0}^{(d_1/d)-1} 1 \mod 3 = d_1/d \mod 3. \tag{11}$$

So if $d_1/d = 0 \mod 3$, we obtain (8) and if $d_1/d \neq 0 \mod 3$, we obtain (7).

Now suppose that $p = 2 \mod 3$. This means that even powers of p are congruent to $1 \mod 3$ and odd powers of p are congrugent to $2 \mod 3$. Therefore if d is even, the same reasoning in (11) applies to give us (8) when $d_1/d = 0 \mod 3$ and (7) if $d_1/d \neq 0 \mod 3$. Now if d is odd, then we have that when m is odd,

$$M \mod 3 = \sum_{i=0}^{(d_1/d)-1} \left(p^{md}\right)^i \mod 3 = \sum_{\substack{i=0 \\ i \text{ even}}}^{(d_1/d)-1} 1 + \sum_{\substack{i=0 \\ i \text{ odd}}}^{(d_1/d)-1} 2 \mod 3, \tag{12}$$

which means that $M = 0 \mod 3$ if d_1/d is even and $M \neq 0 \mod 3$ if d_1/d is odd. Clearly if m is even we have that $M = d_1/d \mod 3$. This means when d_1/d is even and $d_1/d = 0 \mod 3$ we obtain (8) and when d_1/d is odd and $d_1/d \neq 0 \mod 3$ we obtain (7). Now consider when d_1/d is even and $d_1/d \neq 0 \mod 3$. When m is even we have that $M \neq 0 \mod 3$ and when m is odd we have that $M = 0 \mod 3$. This produces (9). Lastly if d_1/d is odd and $d_1/d = 0 \mod 3$, we have that $M \neq 0 \mod 3$ when m is odd and $M = 0 \mod 3$ when m is even, which produces (10). This completes our classification $\{\gcd(3, M)\}_{m=1}^{\infty}$.

From this classification, we can produce zeta functions for $y - x^3$. Let's go one at a time. Consider the sequence (7), that is,

$$1, 1, 1, 1, 1, 1, 1, 1, \ldots. \tag{7}$$

This means that, using the results at the beginning of this section,

$$N(m) = 1(p^{md} - 1) + 1 = p^{md}.$$

Therefore,

$$z(T) = \exp\left(\sum_{m=1}^{\infty} N(m)\frac{T^m}{m}\right) = \exp\left(\sum_{m=1}^{\infty} \frac{(p^d T)^m}{m}\right) = \exp\left(-\log\left(1 - p^d T\right)\right)$$
$$= \frac{1}{1 - p^d T}. \tag{13}$$

This is of course the most simple zeta function for $y - x^3$. Now consider (8), which is

$$3, 3, 3, 3, 3, 3, 3, 3, \ldots. \tag{8}$$

Again using the result stated at the beginning of this section, we have that

$$N(m) = 3(p^{md} - 1) + 1 = 3p^{md} - 3 + 1 = 3p^{md} - 2.$$

Thus,

$$\begin{aligned} z(T) = \exp\left(\sum_{m=1}^{\infty} N(m)\frac{T^m}{m}\right) &= \exp\left(\sum_{m=1}^{\infty}(3p^{md} - 2)\frac{T^m}{m}\right) \\ &= \exp\left(3\sum_{m=1}^{\infty}\frac{\left(p^d T\right)^m}{m} - 2\sum_{m=1}^{\infty}\frac{T^m}{m}\right) \\ &= \exp\left(-3\log\left(1 - p^d T\right) + 2\log\left(1 - T\right)\right) \\ &= \frac{(1-T)^2}{\left(1 - p^d T\right)^3}. \end{aligned} \tag{14}$$

From here on out, things get a bit more tricky. Consider first (9), which is

$$3, 1, 3, 1, 3, 1, 3, 1, \ldots. \tag{9}$$

To solve this problem, we split up the sum. We get that

$$z(T) = \exp\left(\sum_{m=1}^{\infty} N(m)\frac{T^m}{m}\right) = \exp\left(\sum_{m\geq 1,\text{even}} (p^{md})\frac{T^m}{m} + \sum_{m\geq 1,\text{odd}} \left(3p^{md} - 2\right)\frac{T^m}{m}\right). \tag{15}$$

Let's compute both

$$\sum_{m\geq 1,\text{even}} \frac{T^m}{m} \qquad (16) \qquad \text{and} \qquad \sum_{m\geq 1,\text{odd}} \frac{T^m}{m}. \qquad (17)$$

For (16), note that

$$\frac{1+(-1)^m}{2} = \begin{cases} 1 & m \text{ even} \\ 0 & m \text{ odd.} \end{cases}$$

This means we can write (16) as

$$\sum_{m\geq 1,\text{even}} \frac{T^m}{m} = \sum_{m=1}^{\infty} \frac{(1+(-1)^m)}{2}\frac{T^m}{m} = \frac{1}{2}\left(\sum_{m=1}^{\infty}\frac{T^m}{m} + \sum_{m=1}^{\infty}\frac{(-T)^m}{m}\right) \qquad (18)$$

$$= \frac{1}{2}\left(-\log(1-T) - \log(1+T)\right) \qquad (19)$$

$$= -\frac{1}{2}\log((1-T)(1+T)). \qquad (20)$$

For (17), we can argue similarly. We have that

$$\frac{1-(-1)^m}{2} = \begin{cases} 0 & m \text{ even} \\ 1 & m \text{ odd} \end{cases}$$

so

$$\sum_{m\geq 1,\text{odd}} \frac{T^m}{m} = \sum_{m=1}^{\infty} \frac{(1-(-1)^m)}{2}\frac{T^m}{m} = \frac{1}{2}\left(\sum_{m=1}^{\infty}\frac{T^m}{m} - \sum_{m=1}^{\infty}\frac{(-T)^m}{m}\right) \qquad (21)$$

$$= \frac{1}{2}\left(-\log(1-T) + \log(1+T)\right) \qquad (22)$$

$$= \frac{1}{2}\log\left(\frac{1+T}{1-T}\right). \qquad (23)$$

We can now apply these results to (15) to get that

$$\begin{aligned} z(T) &= \exp\left(\sum_{m\geq 1,\text{even}} (p^{md})\frac{T^m}{m} + \sum_{m\geq 1,\text{odd}} \left(3p^{md}-2\right)\frac{T^m}{m}\right) \\ &= \exp\left(-\frac{1}{2}\log((1-p^dT)(1+p^dT)) + \frac{3}{2}\log\left(\frac{1+p^dT}{1-p^dT}\right) - \log\left(\frac{1+T}{1-T}\right)\right) \\ &= \frac{(1+p^dT)^{3/2}(1-T)}{(1-p^dT)^{1/2}(1+p^dT)^{1/2}(1-p^dT)^{3/2}(1+T)} \\ &= \frac{(1+p^dT)(1-T)}{(1-p^dT)^2(1+T)}. \end{aligned} \tag{24}$$

We have a very similar result when we consider (10)

$$1, 3, 1, 3, 1, 3, 1, 3, \ldots. \tag{10}$$

We have that

$$\begin{aligned} z(T) &= \exp\left(\sum_{m\geq 1,\text{even}} \left(3p^{md}-2\right)\frac{T^m}{m} + \sum_{m\geq 1,\text{odd}} (p^{md})\frac{T^m}{m}\right) \\ &= \exp\left(-\frac{3}{2}\log((1-p^dT)(1+p^dT)) + \log((1-T)(1+T) - \frac{1}{2}\log\left(\frac{1+p^dT}{1-p^dT}\right)\right) \\ &= \frac{(1-p^dT)^{1/2}(1-T)(1+T)}{(1-p^dT)^{3/2}(1+p^dT)^{3/2}(1+p^dT)^{1/2}} \\ &= \frac{(1-T)(1+T)}{(1-p^dT)(1+p^dT)^2}. \end{aligned} \tag{25}$$

Again because $N(m) = p^m$ when $D = (1, 1)$, we have that $z(T) = \frac{1}{1-pT}$. It should now be apparent that there is a stark contrast in the possible functions between the local zeta function and the generalization here, despite the polynomial being the same.

Based on the complexity of the last example, we forgo attempting solutions with lower ordered terms. The techniques used here can simply not support counting such polynomials. Recall we already know for $X = \{y - x^n\}$ that $N(m) = \gcd(n, M_m)(p^{md} - 1) + 1$, where $M_m = \sum_{i=0}^{(d_1/d)-1} \left(p^{md}\right)^i$. The following lemma will be of much use in determining properties of these partial zeta functions.

Lemma 3.2. *The sequence* $\{\gcd(n, M_m)\}_{m=1}^{\infty}$ *has period* $\varphi(n)$.

Proof. Write $m = \ell\varphi(n) + r$, where r is some remainder less than $\varphi(n)$. We have that

$$\sum_{i=0}^{k} \left(p^{md}\right)^i = \sum_{i=0}^{k} \left(p^{d(\ell\varphi(n)+r)}\right)^i = \sum_{i=0}^{k} \left(p^{d\ell\varphi(n)}p^{dr}\right)^i, \tag{26}$$

for which

$$\sum_{i=0}^{k} \left(p^{d\ell\varphi(n)}p^{dr}\right)^i = \sum_{i=0}^{k} \left(p^{dr}\right)^i \mod n, \tag{27}$$

by Euler's generalization of Fermat's little theorem. This says that $M_m = M_{m \bmod \varphi(n)} \mod n$. Since $\gcd(a, b) = \gcd(a, b \mod a)$ for any integers a, b, our result follows. □

Using this lemma, we can break up the infinite series contained in the zeta function's definition much in the same way that we proceeded in the case of $y - x^3$. At this point, we can write,

$$\begin{aligned} z(T) &= \exp\left(\sum_{m=1}^{\infty} N(m)\frac{T^m}{m}\right) \\ &= \exp\left(\sum_{m=1}^{\infty} \gcd(n, M_m)(p^{md} - 1)\frac{T^m}{m} + \frac{T^m}{m}\right) \qquad (28) \\ &= \exp\left(\sum_{i=1}^{\varphi(n)} \sum_{\substack{m\sim i \\ m\geq 1}} \gcd(n, M_i)(p^{md} - 1)\frac{T^m}{m} + \frac{T^m}{m}\right) \\ &= \exp\left(\sum_{i=1}^{\varphi(n)} \gcd(n, M_i) \sum_{\substack{m\sim i \\ m\geq 1}} \frac{\left(p^d T\right)^m}{m} - \frac{T^m}{m}\right)/(1 - T), \qquad (29) \end{aligned}$$

where we define $a \sim b$ to be $a = b \bmod \varphi(n)$. It is now natural to determine the sum

$$\sum_{\substack{m\sim i \\ m\geq 1}} \frac{T^m}{m}. \tag{30}$$

We explain our first approach.

Dirichlet Character. We attempt to employ a method to rewrite the above series. Let ℓ be a positive integer. A Dirichlet character modulo ℓ is a complex valued function χ on the set of positive integers for which the following properties hold:

1. $\chi(k+\ell) = \chi(k)$, for all $k = 1, 2, 3, \ldots$
2. $\chi(ab) = \chi(a)\chi(b)$, for all $a, b = 1, 2, 3, \ldots$
3. $\chi(a) \neq 0$ if and only if ℓ and a are relatively prime.

It happens to be the case that for any Dirichlet character modulo ℓ, χ, that $\chi(a)$ either is 0 or is an ℓ-th root of unity. Furthermore, there are $\varphi(\ell)$ Dirichlet characters modulo ℓ which form a group isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^*$ under pointwise multiplication. That is, for two characters modulo ℓ, χ_1 and χ_2, we define $\chi_1\chi_2$ on the set of natural numbers by $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$ and in fact $\chi_1\chi_2$ is a Dirichlet character modulo ℓ. The use of these characters comes in an orthogonality condition expressed by them:

Let a, b be natural numbers. Then

$$\sum_{\chi \bmod \ell} \chi(a)\overline{\chi(b)} = \begin{cases} \varphi(\ell) & \text{if } a = b \bmod \ell,\ a \text{ and } \ell \text{ are relatively prime,} \\ 0 & \text{otherwise,} \end{cases}$$

where the sum runs over all characters modulo ℓ, and $\varphi(\ell)$ is the order of $(\mathbb{Z}/\ell\mathbb{Z})^*$. We can insert this orthogonality condition into (30) as follows:

$$\sum_{\substack{m \sim i \\ m \geq 1}} \frac{T^m}{m} = \sum_{m \geq 1} \left(\sum_{\chi \bmod \varphi(n)} \chi(i)\overline{\chi(m)} \right) \frac{T^m}{m} = \sum_{\chi \bmod \varphi(n)} \chi(i) \sum_{m \geq 1} \overline{\chi(m)} \frac{T^m}{m}. \tag{31}$$

It is clear that this makes progress on (30). There is one more fact that is useful about Dirichlet charachters. Fix a Dirichlet character mod ℓ, χ, and let $g(\chi, m) = \sum_{j=1}^{\ell} \chi(j)\zeta^{mj}$, where m is a natural number and ζ is a primitive ℓ-th root of unity. It turns out for some characters the following is true:

$$\chi(m) = \frac{1}{g(\overline{\chi}, 1)} \sum_{j=1}^{\ell} \overline{\chi(j)}\zeta^{mj}. \tag{32}$$

If we were to insert this into (31), we would get that

$$\sum_{\chi \bmod \varphi(n)} \chi(i) \sum_{m\geq 1} \overline{\chi(m)} \frac{T^m}{m} = \sum_{\chi \bmod \varphi(n)} \chi(i) \sum_{m\geq 1} \frac{1}{g(\chi,1)} \sum_{j=1}^{\ell} \zeta^{mj} \frac{T^m}{m} \tag{33}$$

$$= \sum_{\chi \bmod \varphi(n)} \frac{\chi(i)}{g(\chi,1)} \sum_{j=1}^{\ell} \sum_{m\geq 1} \frac{\left(\zeta^j T\right)^m}{m}. \tag{34}$$

This has a few complications as we found out. The orthogonality condition would only apply if i and $\varphi(n)$ were relatively prime, but this can be remedied by factoring out their greatest common divisor, though it provides a messier formula. The formulation overall is very complicated. But the biggest complication would be that (31) only holds for what we call primitive characters modulo ℓ. A primitive character modulo ℓ is a character whose smallest period is ℓ. In the case where χ is imprimitive, that is not primitive, $g(\overline{\chi}, 1)$ can sometimes be 0 so (31) cannot possibly hold. For this idea to work, (31) would need to hold for all characters modulo ℓ. We were able to produce a much more simple method using a well known fact.

Roots of unity. We now attempt to employ a similar method as the method involving Dirichlet characters, and take inspiration from the technique used to find the series $\sum_{m\geq 1,\text{odd}} \frac{T^m}{m}$.

Lemma 3.3. *Let ζ be a primitive ℓ-th root of unity. Then*

$$\sum_{j=1}^{\ell} \zeta^{(m-i)j} = \begin{cases} \ell & \text{if } m = i \bmod \ell \\ 0 & \text{otherwise.} \end{cases} \tag{35}$$

Proof. Taking m' to be $m - i$ and inserting this into (35), we see it suffices to show (35) when $i = 0$. We have that

$$(x-1)\sum_{j=0}^{\ell-1} x^j = \sum_{j=0}^{\ell-1} x^j - x^{j+1} = x^\ell - 1,$$

so dividing by $x - 1$ we arrive at

$$\sum_{j=1}^{\ell} x^j = \frac{x^\ell - 1}{x - 1}. \tag{36}$$

Now the ℓ-th roots of unity are exactly the roots of $x^\ell - 1$ so the roots of $x^\ell - 1$ that are not 1 are the roots of the left hand side. We arrive at the desired result when we insert ζ^m in for (36) noting that ζ^m is 1 when $m = 0 \mod \ell$ and ζ^m is an ℓ-th root of unity not 1 when $m \neq 0 \mod \ell$. $\square$

Its application to (30) should be obvious given our previous discussion. Let ζ be a primitive $\varphi(n)$-th root of unity. Then

$$\begin{aligned}\sum_{\substack{m\sim i\\ m\geq 1}} \frac{T^m}{m} = \sum_{m\geq 1}\left(\frac{1}{\varphi(n)}\sum_{j=1}^{\varphi(n)}\zeta^{(m-i)j}\right)\frac{T^m}{m} &= \frac{1}{\varphi(n)}\sum_{j=1}^{\varphi(n)}\sum_{m\geq 1}\zeta^{(m-i)j}\frac{T^m}{m}\\ &= \sum_{m\geq 1}\left(\frac{1}{\varphi(n)}\sum_{j=1}^{\varphi(n)}\zeta^{(m-i)j}\right)\frac{T^m}{m}\\ &= \frac{1}{\varphi(n)}\sum_{j=1}^{\varphi(n)}\zeta^{-ij}\sum_{m\geq 1}\frac{(\zeta^j T)^m}{m}\\ &= -\frac{1}{\varphi(n)}\sum_{j=1}^{\varphi(n)}\zeta^{-ij}\log(1-\zeta^j T).\end{aligned} \tag{37}$$

Now take (37) and apply it to (29), and letting $\delta_i = \gcd(n, M_i)$, to obtain

$$
\begin{aligned}
z(T) &= \exp\left(\sum_{i=1}^{\varphi(n)} \delta_i \sum_{\substack{m\sim i \\ m\geq 1}} \frac{(p^d T)^m}{m} - \frac{T^m}{m}\right) /(1-T) \\
&= \exp\left(\sum_{i=1}^{\varphi(n)} \frac{\delta_i}{\varphi(n)} \sum_{j=1}^{\varphi(n)} \zeta^{-ij} \left(\log(1-\zeta^j T) - \log(1-\zeta^j p^d T)\right)\right) /(1-T) \\
&= \exp\left(\frac{1}{\varphi(n)} \sum_{i=1}^{\varphi(n)} \delta_i \sum_{j=1}^{\varphi(n)} \zeta^{-ij} \log\left(\frac{1-\zeta^j T}{1-\zeta^j p^d T}\right)\right) /(1-T) \qquad (38) \\
&= \exp\left(\log \prod_{j=1}^{\varphi(n)} \left(\frac{1-\zeta^j T}{1-\zeta^j p^d T}\right)^{S_j/\varphi(n)}\right) /(1-T) \\
&= \prod_{j=1}^{\varphi(n)} \left(\frac{1-\zeta^j T}{1-\zeta^j p^d T}\right)^{S_j/\varphi(n)} \frac{1}{1-T}, \qquad (39)
\end{aligned}
$$

where

$$
S_j = \sum_{i=1}^{\varphi(n)} \delta_i \zeta^{-ij}, \qquad (40)
$$

which we refer to as the j-th divisor sum, is obtained by swapping the summation indices in (38) and bringing the coefficient of the log to a power inside. We now can see the rational-like structure of the partial zeta function. Now we employ Wan's result of rationality of partial zeta functions to say more [3]. We know that $z(T) \in \mathbb{Q}(T)$ which means that

$$
z(T) = \prod_{j=1}^{\varphi(n)} \left(\frac{1-\zeta^j T}{1-\zeta^j p^d T}\right)^{S_j/\varphi(n)} \cdot \frac{1}{1-T} \in \mathbb{Q}(T). \qquad (41)
$$

This means that $z(T) = r(T)/s(T)$ where $r(T), s(T) \in \mathbb{Q}[T]$. Therefore $r(T)$ has a root at x only if $z(T)$ has a root at x and $s(T)$ has a root at x only if $z(T)$ has a pole at x. Hence

$$
\frac{r(T)}{s(T)} = \prod_{j=1}^{\varphi(n)} \frac{(1-\zeta^j T)^{k_j}}{(1-\zeta^j p^d T)^{k'_j}} \cdot \frac{1}{1-T} = \prod_{j=1}^{\varphi(n)} \left(\frac{1-\zeta^j T}{1-\zeta^j p^d T}\right)^{S_j/\varphi(n)} \cdot \frac{1}{1-T}, \qquad (42)
$$

where k_j, k'_j are integers for all j, so in particular for $1 \leq \ell\varphi(n)$,

$$\prod_{j\neq\ell}^{\varphi(n)} \frac{(1-\zeta^j T)^{k_j}}{(1-\zeta^j p^d T)^{k'_j}} \frac{1}{1-T} = \frac{(1-\zeta^\ell p^d T)^{k'_\ell}}{(1-\zeta^\ell T)^{k_\ell}} \frac{r(T)}{s(T)} = \frac{(1-\zeta^\ell p^d T)^{k'_\ell}}{(1-\zeta^\ell T)^{k_\ell}} z(T). \quad (43)$$

Therefore since the left hand side has no reciprocal roots or poles at ζ^ℓ and $\zeta^\ell p^d$, it must be the case that $z(T)$ has no such reciprocal poles or roots, hence $k_\ell = S_\ell/\varphi(n) = k'_\ell$. This says that $S_j \in \mathbb{Z}$ and is divisible by $\varphi(n)$ for all j.

We can say some more using Galois theory. We can write

$$\begin{aligned} z(T) &= \prod_{j=1}^{\varphi(n)} \left(\frac{1-\zeta^j T}{1-\zeta^j p^d T}\right)^{S_j/\varphi(n)} \cdot \frac{1}{1-T} \\ &= \prod_{q|\varphi(n)} \prod_{o(j)=q} \left(\frac{1-\zeta^j T}{1-\zeta^j p^d T}\right)^{S_j/\varphi(n)} \cdot \frac{1}{1-T} \end{aligned}$$

where $o(j)$ is the additive order of j mod $\varphi(n)$. We have for any automorphism σ of $\mathbb{Q}(T)(\zeta)$ over $\mathbb{Q}(T)$ that

$$\sigma(z(T)) = \prod_{q|\varphi(n)} \prod_{o(j)=q} \left(\frac{1-\sigma(\zeta^j) T}{1-\sigma(\zeta^j) p^d T}\right)^{S_j/\varphi(n)} \cdot \frac{1}{1-T}.$$

Because the conjugates of primitive q-th roots of unity over $\mathbb{Q}$ are all other primitive $\mathbb{Q}$-th roots of unity we can rewrite the inside product in the following way:

$$\prod_{o(j)=q} \left(\frac{1-\sigma(\zeta^j) T}{1-\sigma(\zeta^j) p^d T}\right)^{S_j/\varphi(n)} = \prod_{o(j)=q} \left(\frac{1-\zeta^{j_\sigma} T}{1-\zeta^{j_\sigma} p^d T}\right)^{S_j/\varphi(n)},$$

where j_σ is the number in $\mathbb{Z}/\varphi(n)\mathbb{Z}$ with additive order q such that $\sigma(\zeta^j) = \zeta^{j_\sigma}$. This fact also implies that there is an automorphism σ for which $j_\sigma = j'$ for any j and j' having additive orders q mod $\varphi(n)$. Therefore $S_{j'} = S_j$ for all j, j' with additive order q mod $\varphi(n)$, otherwise $\sigma(z(T))$ would have roots with multiplicities different from $z(T)$. This cannot happen since $\sigma(z(T)) = z(T)$ because $z(T) \in \mathbb{Q}(T)$ due to Wan [3].

Now define $S_q = S_j$ for j such that $o(j) = q$, which we can do since we just showed they are all equal. This allows us to write further that

$$\begin{aligned} z(T) &= \prod_{q|\varphi(n)} \prod_{o(j)=q} \left(\frac{1-\zeta^j T}{1-\zeta^j p^d T} \right)^{S_j/\varphi(n)} \cdot \frac{1}{1-T} \\ &= \prod_{q|\varphi(n)} \prod_{o(j)=q} \left(\frac{1-\zeta^j T}{1-\zeta^j p^d T} \right)^{S_q/\varphi(n)} \cdot \frac{1}{1-T} \\ &= \prod_{q|\varphi(n)} \left(\prod_{o(j)=q} \frac{1-\zeta^j T}{1-\zeta^j p^d T} \right)^{S_q/\varphi(n)} \cdot \frac{1}{1-T} \\ &= \prod_{q|\varphi(n)} \left(\frac{\Phi_q(T)}{\Phi_q(p^d T)} \right)^{S_q/\varphi(n)} \cdot \frac{1}{1-T}, \end{aligned} \tag{44}$$

where Φ_q is the q-th cyclotomic polynomial.

4 Conjectures and future work

There is one main conjecture, which concerns the sequence $\{M_m\}_{m=1}^{\varphi(n)}$.

Conjecture 4.1. *Consider the sequence* $\{\delta_m\}_{m=1}^{\varphi(n)}$ *where* $\delta_m = \gcd(n, M_m)$ *and* $M_m = \sum_{i=0}^{\ell} (p^{md})^i$. *Then if* $\gcd(\varphi(n), m) = \gcd(\varphi(n), m')$, *then* $\delta_m = \delta_{m'}$.

To see why this is helpful, and possibly true, recall that the order of m in $\mathbb{Z}/\varphi(n)\mathbb{Z}$ is $\frac{\varphi(n)}{\gcd(\varphi(n),m)}$, so if $\gcd(\varphi(n), m) = \gcd(\varphi(n), m')$, then their additive orders mod $\varphi(n)$ will be the same. Applything this to the first divisor sum, we see that this would mean the coefficients of the $\varphi(n)$-th roots of unity would be the same for those that are the same primitive roots. More generally, this would allow us to write

$$\begin{aligned} S_j = \sum_{m=1}^{\varphi(n)} \delta_m \zeta^{-mj} = \sum_{q|\varphi(n)} \sum_{o(m)=q} \delta_m \zeta^{-mj} &= \sum_{q|\varphi(n)} \delta_{(q)} \sum_{o(m)=q} (\zeta^m)^j \\ &= \sum_{q|\varphi(n)} \delta_{(q)} c_q(j), \end{aligned}$$

where $\delta_{(q)}$ is the (conjectured) equal coefficient for all elements order q mod $\varphi(n)$, and $c_q(j)$ is defined as Ramanujan's sum, the sum of the primitive q-th roots of unity to the j-th powers, which is known to take on only integer values.

From here it can also be shown that $S_j = S_{j'}$ whenever j and j' have the same additive over mod $\varphi(n)$. This would allow us to show that the divisor sums are integers, and potentially that they are divisible by $\varphi(n)$. If this is the case, then we could also arrive at (44) without appealing to Wan's result [3].

Any future work would attempt to prove this conjecture. Another avenue would be to consider $X = \{y^{n'} - x^n\}$ for n' a positive integer. This is not expected to provide much more difficulty than when $X = \{y - x^n\}$, but rather a simple extension. Additionally, it would be proper to understand the $X = \{y - x^n\}$ case when p divides n, but this is also not expected to be difficult. These cases would completely exhaust the technique employed in this paper, so future work to understand partial zeta functions would require a completely new technique.

References

[1] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *American Journal of Mathematics*, 82(3):631–648, 1960.

[2] Daqing Wan. Partial zeta functions of algebraic varieties over finite fields. *Finite Fields and Their Applications*, 7(1):238–251, 2001.

[3] Daqing Wan. Rationality of partial zeta functions. *Indagationes Mathematicae*, 14(2):285–292, 2003.