JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Patrick MEISNER

On Incidences of φ and σ in the Function Field Setting

Tome 31, n° 2 (2019), p. 403-415.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2019__31_2_403_0>

Journal de Théorie des Nombres de Bordeaux **31** (2019), 403–415

On Incidences of φ and σ in the Function Field Setting

par Patrick MEISNER

Résumé. Erdős a conjecturé qu'il existe une infinité de nombres n et m tels que $\varphi(n) = \sigma(m)$, où φ est l'indicatrice d'Euler et σ est la fonction somme de diviseurs. Cette conjecture a été prouvée en 2010 par Ford, Luca et Pomerance. De façon analogue, on se demande s'il existe une infinité de polynômes F et G sur un corps fini $\mathbb{F}_q$ tels que $\varphi(F) = \sigma(G)$. On trouve que si $q \neq 2$ ou 3, c'est vrai seulement dans le cas trivial $F = G = 1$. De plus, on donne une caractérisation des solutions dans les cas $q = 2$ et 3. En particulier, on montre que si $q = 2$ ou 3, on a $\varphi(F) = \sigma(G)$ pour une infinité de polynômes.

Abstract. Erdős first conjectured that infinitely often we have $\varphi(n) = \sigma(m)$, where φ is the Euler totient function and σ is the sum of divisors function. This was proven true by Ford, Luca and Pomerance in 2010. We ask the analogous question of whether infinitely often we have $\varphi(F) = \sigma(G)$ where F and G are polynomials over some finite field $\mathbb{F}_q$. We find that when $q \neq 2$ or 3, then this can only trivially happen when $F = G = 1$. Moreover, we give a complete characterisation of the solutions in the case $q = 2$ or 3. In particular, we show that $\varphi(F) = \sigma(G)$ infinitely often when $q = 2$ or 3.

1. Introduction

1.1. Background. Erdős first conjectured in [6] that there should be infinitely many solutions to the equation $\varphi(n) = \sigma(m)$ where φ is the Euler totient function and σ is the sum of divisors function. This question is interesting in part because it is implied by the infinitude of two set sets of primes both of which are widely believed to be infinite: twin primes and Mersenne primes. Indeed, if we have a prime p such that $p+2$ is also prime then

$$\sigma(p) = p + 1 = \varphi(p + 2),$$

while if we have a Mersenne prime $2^n - 1$, then

$$\sigma(2^n - 1) = 2^n = \varphi(2^{n+1}).$$

Manuscrit reçu le 8 octobre 2018, accepté le 16 novembre 2018.

2010 *Mathematics Subject Classification.* 11N64.

Mots-clefs. Function Fields, Euler Totient Function, Primitive Divisors.

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 320755.

This conjecture was proved by Ford, Luca and Pomerance in [7]. Moreover, they showed that for some positive α, there are at least $\exp((\log\log x)^\alpha)$ common values less than x of φ and σ for large x. Under a uniform version of the prime k-tuples conjecture, Ford and Pollack [8] were able to show that the number of common values less than x of φ and σ is greater than $\frac{x}{(\log x)^{1+o(1)}}$, while in [9] they were able to prove unconditional upper bounds on the number of solutions.

1.2. Function Fields. In this paper, we are interested in the analogous question about function fields. That is, if $F, G \in \mathbb{F}_q[T]$ are polynomials over the finite field $\mathbb{F}_q$, then we define

$$\varphi(F) = \#(\mathbb{F}_q[T]/(F))^* = \prod_{P|F} |P|^{v_P(F)-1}(|P|-1) \tag{1.1}$$

$$\sigma(G) = \sum_{D|G} |D| \tag{1.2}$$

where for any polynomial $A \in \mathbb{F}_q[T]$, $|A| = q^{\deg(A)}$ and $v_P(A)$ is the largest natural number n such that $P^n|A$. Further, unless otherwise stated, when we consider ranging over divisors of a polynomial we always consider only *monic* divisors. Therefore, the P and D appearing in the definition of φ and σ are monic.

One thing of note is that, in the function field setting, the twin prime conjecture was proved by Bender and Pollack [4] in the large q limit for q odd (in fact, they just need q to grow sufficiently faster than n). Following this, Bary–Soroker [3] proved the full Hardy–Littlewood prime k-tuple conjecture in the large q limit for q odd and Carmon [5] proved it for q even. However, even with this big hammer it doesn't seem to help us prove the infinitude of solutions to $\varphi(F) = \sigma(G)$. Indeed, if we had a prime polynomial P such that $P+2$ was also prime, then

$$\begin{aligned}\sigma(P) &= |P| + 1 = q^{\deg(P)} + 1 \\ &\neq q^{\deg(P)} - 1 = q^{\deg(P+2)} - 1 \\ &= |P+2| - 1 = \varphi(P+2).\end{aligned}$$

The philosophy of the connection between the integers and function fields is that a true statement in one setting should have analogous true statement in the other. While the functions defined in (1.1) and (1.2) are the standard analogues in the function field setting we find that the analogous statements are almost never true.

Theorem 1.1. *If $q = 2$ or 3 then there are infinitely many solutions to $\varphi(F) = \sigma(G)$ with $F, G \in \mathbb{F}_q[T]$ while if $q \neq 2$ or 3, the only solution is the trivial solution $F = G = 1$.*

This is a sharp contrast to the integer setting. Not only do we not get infinitely many solutions, for most q we do not get even one coincidental non-trivial one. A key ingredient for proving Theorem 1.1 for $q \neq 2,3$ is a result on primitive prime divisors of the sequence $\{a^n - b^n\}_{n\geq 1}$ (see Section 2.3 for more on this).

The proof to Theorem 1.1 for $q = 2,3$ can be done by construction. For every tuple of positive integers $\mathbf{v} = (v_0, v_1, \ldots, v_n)$, define

$$V_q(\mathbf{v}) = \left\{ (F,G) \in \mathbb{F}_q[T] : \begin{array}{c} G = \prod_{i=1}^n P_i^{v_i}, \ F = P_{n+1}, \\ \deg(P_k) = v_0 \prod_{i=1}^{k-1}(v_i+1) \end{array} \right\} \tag{1.3}$$

where the P_i are distinct prime polynomials.

Lemma 1.2. *If $(F,G) \in V_2(\mathbf{v})$ such that $v_0 = 1$ then $\varphi(F) = \sigma(G)$. While if $(F,G) \in V_3(\mathbf{v})$ with $v_0 = 2$, then $\varphi(TF) = \sigma(T(T+1)G)$.*

Clearly, the sets described in Lemma 1.2 are infinite. Therefore, this lemma implies Theorem 1.1 for $q = 2,3$. Moreover, the sets $V_q(\mathbf{v})$ together with some finite, exceptional sets generate all the solutions to $\varphi(F) = \sigma(G)$.

Theorem 1.3. *Suppose $q = 2$ or $q = 3$. Then there exists a finite set of tuples of polynomials $E_q \subset \mathbb{F}_q[T] \times \mathbb{F}_q[T]$ such that if $\varphi(F) = \sigma(G)$, then $F = \prod_{i=0}^n F_i$, $G = \prod_{i=0}^n G_i$ with $\gcd(F_i,F_j) = \gcd(G_i,G_j) = 1$, $i \neq j$, $(F_0,G_0) \in E_q$ and $(F_i,G_i) \in V_q(\mathbf{v}_i)$ for some $\mathbf{v}_i$ such that $v_{i,0}|6$ if $q = 2$ or $v_{i,0}|2$ if $q = 3$.*

Again, a main tool in proving this classification theorem is a result on primitive prime divisors of the sets $\{2^n - 1\}_{n\geq 1}$ and $\{3^n - 1\}_{n\geq 1}$.

In Section 4 we discuss the exceptional sets and the possible values of n and the $\mathbf{v}$'s. We get the following corollary.

Corollary 1.4. *With the same notation as in Theorem 1.3, if $q = 3$ then we must have $n \leq 2$. Moreover, all possible values of $\mathbf{v}_1, \mathbf{v}_2$ such that $v_{i,0}|2$ are possible.*

If $q = 2$, we must have $n \leq 3$. Moreover all possible values of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ such that $v_{i,0}|6$, $i = 1,2$ and $v_{3,0} = 1$ are possible except for $(2,2)$, $(2,2,1)$ and $(1,1,1)$.

Note that the three exceptions in the case $q = 2$ come from the fact that $\mathbb{F}_2$ is a very small field and hence only has two polynomials of degree 1 and only one polynomial of degree 2.

1.3. Other Formulations. One reason why we can not find solutions to $\phi(F) = \sigma(G)$ is because $\phi(F)$ will typically be divisible by a large power of $q - 1$ while it is difficult to enforce this condition on $\sigma(G)$. This is not an issue when $q = 2$ and has an easy fix when $q = 3$ with the observation that $3 + 1 = (3-1)^2$.

There is a natural way to reformulate σ that would incorporate powers of $q-1$. Namely, define

$$\sigma_{nm}(F) = \sum_{D|F}^{*} |D|$$

where * denotes the sum to be over not necessarily monic divisors of F. Moreover the nm in the subscript stands for non-monic and should not be confused with the standard notation σ_k, the sum of the k^{th} powers of divisors.

Then we have infinitely many solutions to $\varphi(F) = \sigma_{nm}(G)$ for $F, G \in \mathbb{F}_q[T]$, for any q. Indeed,

$$\sigma_{nm}(T^n) = \sum_{\alpha \in \mathbb{F}_q^*} \sum_{j=0}^{n} |\alpha T^j| = (q-1) \sum_{j=0}^{n} q^j = q^{n+1} - 1 = \varphi(P)$$

where P is any prime polynomial of degree $n+1$.

However, it is generally accepted that the sum of monic divisors is the correct analogue in the function field setting as monic polynomials correspond to positive integers.

Since we are looking at analogues of sums of divisors, another natural choice would be to do just that: sum the divisors. Thus, we can consider the new function

$$\widetilde{\sigma}(F) = \sum_{D|F} D.$$

Now, to consider incidences to $\widetilde{\sigma}$ and φ, it is clear we must modify φ slightly in order for this question to make sense. Thus we define

$$\widetilde{\varphi}(F) = \prod_{P|F} P^{v_P(F)-1}(P-1).$$

That is, we just remove the norm function in the definition of the usual φ.

Theorem 1.5. *The number of solutions to $\widetilde{\varphi}(F) = \widetilde{\sigma}(G)$ for $F, G \in \mathbb{F}_q[T]$ with $\deg(F) = \deg(G) = n$ is $\gg \frac{q^n}{n^2}$ as q tends to infinity.*

Proof. The Hardy–Littlewood Theorem for function fields ([3, 4, 5]) states that as q tends to infinity, the number of primes P of a fixed degree n such that $P+2$ is also prime is $\gg \frac{q^n}{n^2}$ as q tends to infinity. Now, it is easy to see that $\widetilde{\sigma}(P) = \widetilde{\varphi}(P+2)$. □

As we mentioned above, Ford and Pollack [8] showed that under a uniform Hardy–Littlewood conjecture they can show that the number of solutions to $\varphi(n) = \sigma(m)$ with n, m less than x is at least $\frac{x}{(\log x)^{1+o(1)}}$. Now, Bary–Soroker [3] and Carmon [5] give us a uniform Hardy–Littlewood conjecture in the large q limit. So it is likely possible to adapt Ford and Pollack's methods to the function field setting and prove, unconditionally, that there are at least $\frac{q^n}{n^{1+o(1)}}$ solutions to $\widetilde{\varphi}(F) = \widetilde{\sigma}(G)$.

We note that in the special case $q = 2$, we get that $\widetilde{\varphi}(P) = \widetilde{\sigma}(P)$ for all primes P. Therefore, we get that the number of solutions in $\mathbb{F}_2[T]$ with $\deg(F) = \deg(G) = n$ will be greater than $\frac{1}{2}2^n$, as $F = G$, with F square-free will always give a solution. It would be interesting to determine if for any other q we get a positive proportion of solutions to $\widetilde{\phi}(F) = \widetilde{\sigma}(G)$ with $\deg(F) = \deg(G) = n$ as n tends to infinity.

Acknowledgements. I would like to thank Jake Chinis for initially asking me this question and for useful conversations at the early stages. I would also like to thank Zeev Rudnick for pointing me to the work of Zsigmondy and Andrés Jaramillo Puentes for suggesting computation tools that helped with enumerating the exceptional sets. Finally, I would like to thank the anonymous referee for useful comments and details on the history of primitive prime divisors.

2. Proof of Theorem 1.1

2.1. Proof of Lemma 1.2.

Proof of Lemma 1.2. Let $(F, G) \in V_2(\mathbf{v})$ for some $\mathbf{v}$ such that $v_0 = 1$. Then

$$\begin{aligned}
\sigma(G) &= \prod_{i=1}^{n}(|P_i|^{v_i} + |P_i|^{v_i-1} + \cdots + |P_i| + 1) = \prod_{i=1}^{n} \frac{|P_i|^{v_i+1} - 1}{|P_i| - 1} \\
&= \prod_{i=1}^{n} \frac{2^{\prod_{j=1}^{i}(v_j+1)} - 1}{2^{\prod_{j=1}^{i-1}(v_j+1)} - 1} \\
&= 2^{\prod_{j=1}^{n}(v_j+1)} - 1 = \varphi(F)
\end{aligned}$$

Let $(F, G) \in V_3(\mathbf{v})$ for some $\mathbf{v}$ such that $v_0 = 2$. First, we note that since $v_0 = 2$ all the primes dividing F and G have degree greater than or equal to 2. In particular, $\gcd(F, T) = \gcd(G, T(T+1)) = 1$. Therefore

$$\begin{aligned}
\sigma(T(T+1)G) &= (3+1)^2 \prod_{i=1}^{n}(|P_i|^{v_i} + |P_i|^{v_i-1} + \cdots + |P_i| + 1) \\
&= 16 \prod_{i=1}^{n} \frac{|P_i|^{v_i+1} - 1}{|P_i| - 1} = 16 \prod_{i=1}^{n} \frac{3^{2\prod_{j=1}^{i}(v_j+1)} - 1}{3^{2\prod_{j=1}^{i-1}(v_j+1)} - 1} \\
&= 16 \frac{3^{2\prod_{j=1}^{n}(v_j+1)} - 1}{3^2 - 1} \\
&= 2(3^{2\prod_{j=1}^{n}(v_j+1)} - 1) = \varphi(TF)
\end{aligned}$$

□

2.2. Preliminary Lemma. Before we continue with the proof of Theorem 1.1 we have a preliminary lemma that reduces our search down significantly.

Lemma 2.1. *Suppose $\varphi(F) = \sigma(G)$ then F must be square-free. Moreover, if $q \neq 2$, then the number of prime divisors of F must be even.*

Proof. We can rewrite $\varphi(F)$ as a sum of divisors in the following way:

$$\varphi(F) = \sum_{D|F} \mu(F/D)|D|.$$

Then we notice that $\varphi(F) \equiv \mu(F) \mod q$. Moreover, we note that $\sigma(G) \equiv 1 \mod q$. Hence, if $\varphi(F) = \sigma(G)$, we must have $\mu(F) \equiv 1 \mod q$. The result then follows. □

2.3. Key Proposition. For any sequence $U_1, U_2, \ldots, U_n, \ldots$, we will say that U_n has a primitive prime divisor if there exists a prime, p, such that $p|U_n$ but $p \nmid U_m$ for all $m < n$. A major tool in this paper is the following result on primitive prime divisors of a class of sequences.

Theorem 2.2. *For any $a > b$ positive, coprime integers all the elements of the sequence*

$$\{a - b, a^2 - b^2, \ldots, a^n - b^n, \ldots\}$$

have a primitive prime divisor unless $a = 2$, $b = 1$ and $n = 6$ or $a + b$ is a power of 2 and $n = 2$.

This was first proved by Bang in [2] in the case $b = 1$ and then proved in general by Zsigmondy [10]. Later Artin [1] gave a different proof of this.

We will use this theorem to show that unless $a = 2$ or 3, an element in the set multiplicatively generated by $\{a - 1, a^2 - 1, \ldots\}$ will have a unique decomposition. This will be instrumental in proving the absence of solutions when $q \neq 2, 3$.

First, recall that a multiset is a set of not necessarily distinct objects $\{x_1, \ldots, x_n\}$. The multiplicity of an object x is the number of $x_i = x$, with the multiplicity being 0 if x does not appear in the multiset. We say two multisets $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$ are equal if each object occurs with the same multiplicity.

Proposition 2.3. *Let a be any integer greater than 1, $(n_1, \ldots, n_t)$ and $(m_1, \ldots, m_s)$ any tuples of positive integers such that*

$$\prod_{i=1}^{t} (a^{n_i} - 1) = \prod_{j=1}^{s} (a^{m_j} - 1).$$

Then if $a = 2$, we must have $\{n_i : n_i \nmid 6\} = \{m_j : m_j \nmid 6\}$ as multisets; if $a = 3$, we must have $\{n_i : n_i \nmid 2\} = \{m_j : m_j \nmid 2\}$ as multisets; if $a \neq 2, 3$, we must have $\{n_1, \ldots, n_t\} = \{m_1, \ldots, m_s\}$ as multisets.

Proof. We will begin in the case where $a \neq 2, 2^m - 1$. Then by Theorem 2.2, we get that there always exists a prime, p, that divides $a^n - 1$ but does not divide $a^m - 1$ for all such $m < n$. Define p_n as the smallest such prime. Denote

$$N_0 := N = \prod_{i=1}^{t} (a^{n_i} - 1) = \prod_{j=1}^{s} (a^{m_j} - 1).$$

Let k be largest such that $p_k | N$. Then we must have that $a^k - 1 | N$. Indeed, if there were some $\ell > k$ such that $a^\ell - 1 | N$, then $p_\ell | N$ contradicting the maximality of k. Moreover, if all the $n_i, m_j < k$, then we could not have $p_k | N$ as $p_k \nmid a^m - 1$ for all $m < k$. By the same reasoning we see that

$$N_1 := \frac{N}{(a^k - 1)^{v_{p_k}(N)/v_{p_k}(a^k - 1)}} \in \mathbb{Z}$$

and $p_k \nmid N_1$. Here, we again use the notation $v_p(m)$ to denote the largest number n such that $p^n | m$. Hence, we need that

$$|\{i : n_i = k\}| = |\{j : m_j = k\}| = v_{p_k}(N)/v_{p_k}(a^k - 1).$$

Repeating the same process with N_1 multiple times we get that for any ℓ, we must have

$$|\{i : n_i = \ell\}| = |\{j : m_j = \ell\}| = v_{p_\ell}(N)/v_{p_\ell}(a^\ell - 1)$$

and thus $\{n_1, \ldots, n_t\} = \{m_1, \ldots, m_s\}$ as multisets.

Now, if $a = 2^m - 1$, again by Theorem 2.2, we can define p_n in the same way as long as $n \neq 1, 2$ and, repeating the same process, we would find that for all $\ell \neq 1, 2$, we would get that

$$|\{i : n_i = \ell\}| = |\{j : m_j = \ell\}| = v_{p_\ell}(N)/v_{p_\ell}(a^\ell - 1).$$

In particular, we have shown that $\{n_i : n_i \nmid 2\} = \{m_j : m_j \nmid 2\}$ as multisets which finishes the case for $a = 3$.

We have reduced the question down to the case where all the n_i, m_j are either 1 or 2. Let c_ℓ, d_ℓ be the number of n_i, m_j that equal ℓ, respectively. Then we would need

$$(a - 1)^{c_1} (a^2 - 1)^{c_2} = (a - 1)^{d_1} (a^2 - 1)^{d_2}.$$

Now, since $a = 2^m - 1$, we get

$$\begin{aligned}(a - 1)^{c_1} (a^2 - 1)^{c_2} &= 2^{c_1 + (m+1)c_2} (2^{m-1} - 1)^{c_1 + c_2} \\ &= 2^{d_1 + (m+1)d_2} (2^{m-1} - 1)^{d_1 + d_2} = (a - 1)^{d_1} (a^2 - 1)^{d_2}.\end{aligned}$$

Therefore, as long as $m \neq 2$ (or $a \neq 3$), we get that

$$c_1 + (m + 1)c_2 = d_1 + (m + 1)d_2 \qquad c_1 + c_2 = d_1 + d_2$$

whence $c_1 = d_1$ and $c_2 = d_2$ and $\{n_1, \ldots, n_t\} = \{m_1, \ldots, m_s\}$ as multisets.

Finally, when $a = 2$, using the same method, Theorem 2.2 as well as the observation that the primes of $2^6 - 1$ come from $2^2 - 1$ and $2^3 - 1$ tells us that as long as $\ell \neq 1, 2, 3, 6$, we get that

$$|\{i : n_i = \ell\}| = |\{j : m_j = \ell\}| = v_{p_\ell}(N)/v_{p_\ell}(a^\ell - 1).$$

This concludes the proof. □

2.4. Proof of Theorem 1.1.

Proof of Theorem 1.1. We already proved the case where $q = 2, 3$ in Section 2.1. Therefore, let $q \neq 2, 3$, and suppose that $\varphi(F) = \sigma(G)$. Then, by Lemma 2.1, F must be square-free with an even number of prime divisors. Therefore,

$$\varphi(F) = \prod_{P|F} (|P| - 1) = \prod_{P|F} (q^{\deg(P)} - 1).$$

On the other hand if we write $G = \prod P^{v_P}$, then we would have

$$\sigma(G) = \prod_{P|G} \sigma(P^{v_p}) = \prod_{P|G} (|P|^{v_p} + |P|^{v_p - 1} + \cdots + |P| + 1)$$
$$= \prod_{P|G} \frac{|P|^{v_p+1} - 1}{|P| - 1} = \prod_{P|G} \frac{q^{(v_p+1)\deg(P)} - 1}{q^{\deg(P)} - 1}.$$

Since $\varphi(F) = \sigma(G)$, we would then need

$$\prod_{P|F} (q^{\deg(P)} - 1) \prod_{P|G} (q^{\deg(P)} - 1) = \prod_{P|G} (q^{(v_p+1)\deg(P)} - 1).$$

By Proposition 2.3, we get

$$\{\deg(P) : P|F\} \cup \{\deg(P) : P|G\} = \{(v_p + 1)\deg(P) : P|G\}$$

as multisets. However, we see that the left hand side set has a size greater than or equal the right hand side with equality if and only if $\{\deg(P) : P|F\}$ is empty. That is, if and only if $F = 1$. Then we would have $\sigma(G) = \varphi(1) = 1$ and hence $G = 1$, as well. □

3. Characterising the Solutions

We will now characterise all the solutions to $\varphi(F) = \sigma(G)$ when $q = 2$ or 3 thus proving Theorem 1.3.

Let $d_2 = 6$ and $d_3 = 2$ and define

$$\widetilde{E}_q = \{(F_0, G_0) \in \mathbb{F}_q[T] : P|F_0 \implies \deg(P)|d_q \quad \text{and } P^v||G_0 \implies (v + 1)\deg(P)|d_q\}$$

where we use the convention that $P^v||G_0$ indicates that $P^v|G_0$ but $P^{v+1} \nmid G_0$. Clearly $\widetilde{E}_q$ is finite and we will show that $E_q \subset \widetilde{E}_q$.

If $F=\prod_{i=1}^n P_i$ and $G=\prod_{i=1}^m Q_i^{v_i}$ such that $\varphi(F)=\sigma(G)$ then, as in the proof of Theorem 1.1, we get

$$\prod_{i=1}^n \left(q^{\deg(P_i)}-1\right)\prod_{i=1}^m \left(q^{\deg(Q_i)}-1\right)=\prod_{i=1}^m \left(q^{(v_i+1)\deg(Q_i)}-1\right).$$

Applying Proposition 2.3 we need that

$$\{\deg(P_i):\deg(P_i)\nmid d_q\}\cup\{\deg(Q_i):\deg(Q_i)\nmid d_q\} \\ =\{(v_i+1)\deg(Q_i):(v_i+1)\deg(Q_i)\nmid d_q\}$$

as multisets.

We see that $\{\deg(Q_i):\deg(Q_i)\nmid d_q\}=\{(v_i+1)\deg(Q_i):(v_i+1)\times\deg(Q_i)\nmid d_q\}$ as multisets if and only if both sets are empty. Thus, if $\{\deg(P_i):\deg(P_i)\nmid d_q\}$ is empty, then all three sets are empty and we get $(F,G)\in\widetilde{E}_q$.

Hence, without loss of generality, assume $\deg(P_n)\nmid d_q$. Then there exists a Q_{i_1} such that $\deg(P_n)=(v_{i_1}+1)\deg(Q_{i_1})$. If $\deg(Q_{i_1})\nmid d_q$, then there exists a Q_{i_2} such that $\deg(Q_{i_1})=(v_{i_2}+1)\deg(Q_{i_2})$. We continue this process until we find a Q_{i_k} such that $\deg(Q_{i_k})|d_q$. Relabel $Q_{i_j}=Q_{n,k-j+1}$ and $v_{i_j}=v_{n,k-j+1}$, so that we get

$$\deg(P_n)=\deg(Q_{n,1})\prod_{j=1}^k(v_{n,j}+1)\qquad \deg(Q_{n,i})=\deg(Q_{n,1})\prod_{j=1}^{i-1}(v_{n,j}+1).$$

That is, we find that $(P_n,\prod_{i=1}^k Q_{n,i}^{v_{n,i}})\in V_q(\mathbf{v})$ for some $\mathbf{v}$ such that $v_0=\deg(Q_{n,1})|d_q$.

Repeating this process for all the P_j such that $\deg(P_j)\nmid d_q$ we get our result with E_q some subset of $\widetilde{E}_q$.

4. The Exceptional Sets

Let $F=\prod_{i=0}^n F_i$, $G=\prod_{i=0}^n G_i$ such that $(F_0,G_0)\in\widetilde{E}_q$, $\gcd(F_i,F_j)=\gcd(G_i,G_j)=1$, $(F_i,G_i)\in V_q(\mathbf{v}_i)$ for some $\mathbf{v}_i=(v_{i,0},v_{i,1},\ldots,v_{i,n_i})$ with $v_{i,0}|d_q$ and $\varphi(F)=\sigma(G)$. In this section we will discuss what elements of $\widetilde{E}_q$ can appear in E_q as well as the possible values for n and the $\mathbf{v}_i$.

We have that

$$\sigma(G)=\prod_{P|G_0}\frac{q^{(v_P+1)\deg(P)}-1}{q^{\deg(P)}-1}\prod_{i=1}^n\frac{q^{v_{i,0}\prod_{j=1}^{n_i}(v_{i,j}+1)}-1}{q^{v_{i,0}}-1}$$

and

$$\varphi(F)=\prod_{P|F_0}\left(q^{\deg(P)}-1\right)\prod_{i=1}^n\left(q^{v_{i,0}\prod_{j=1}^{n_i}(v_{i,j}+1)}-1\right).$$

Hence, we need

$$\prod_{P|F_0}\left(q^{\deg(P)}-1\right)\prod_{P|G_0}\left(q^{\deg(P)}-1\right)\prod_{i=1}^{n}(q^{v_{i,0}}-1) = \prod_{P|G_0}\left(q^{(v_P+1)\deg(P)}-1\right). \tag{4.1}$$

Notice that the degrees of the polynomials on the left hand side of (4.1) all divide d_q. Therefore, we must have that $(v_P+1)\deg(P)|d_q$ for all $P|G_0$ as well as otherwise we would necessarily have a prime dividing the right hand side of (4.1) that does not divide the left hand side, by Theorem 2.2.

For ease of notation, we will denote

$$\omega_d(F) = \#\{P|F : \deg(P) = d\}, \tag{4.2}$$

$$\omega_{d,i}(F) = \#\{P|F : \deg(P) = d, v_P = i\} \tag{4.3}$$

and

$$\pi_q(d) = \#\{P \in \mathbb{F}_q[T] : \deg(P) = d\}. \tag{4.4}$$

Then we can rewrite (4.1) in terms of linear equations in the ω_d and $\omega_{d,i}$ of F_0, G_0, G where $d|d_q$. Moreover, we have the obvious inequality $\omega_{d,i}(F) \leq \omega_d(F) \leq \pi_q(d)$.

4.1. $q = 3$. We will begin with the case $q = 3$ as it is simpler.

Using the fact that $d_q = 2$, and our observation that $(v_P+1)\deg(P)|d_q$ for all $P|G_0$, we see that G_0 must be a product of linear primes with exponent 1. In particular, we see that $\omega_{1,1}(G_0) = \omega_1(G_0)$.

Now, noting that $(3-1) = 2$ and $(3^2-1) = 2^3$, we can rewrite (4.1) as

$$2^{\omega_1(F_0)+\omega_1(G)+3(\omega_2(F_0)+\omega_2(G))} = 2^{3\omega_1(G_0)}. \tag{4.5}$$

Thus we need to find the solutions to

$$\omega_1(F_0) + \omega_1(G) + 3(\omega_2(F_0) + \omega_2(G)) = 3\omega_1(G_0)$$

under the constraints that

$$\omega_1(F_0), \omega_1(G) \leq \pi_3(1) = 3 \quad \omega_2(F_0), \omega_2(G) \leq \pi_3(2) = 3 \quad \omega_1(G_0) \leq \omega_1(G).$$

Manually going through all the possible solutions, we find that the tuple $(\omega_1(F_0), \omega_1(G_0), \omega_1(G), \omega_2(F_0), \omega_2(G))$ must be one of

$$(0,0,0,0,0), (2,1,1,0,0), (1,1,2,0,0), (0,1,3,0,0), (1,2,2,1,0),$$
$$(1,2,2,0,1), (3,2,3,0,0), (0,2,3,1,0), (0,2,3,0,1), (0,3,3,0,2),$$
$$(0,3,3,1,1), (0,3,3,2,0), (3,3,3,0,1), (3,3,3,1,0).$$

We summarize the information in the following table. E_3 is the set of tuples (F_0, G_0) such that F_0 and G_0 are in the same row. We recall that G_0

is always a product of linear primes, so the Q's appearing in the G_0 column will always be linear primes. Further, the third column shows the value of n while the last column gives restrictions on the possible $\mathbf{v}$ values that can occur with $\emptyset$ indicating that $n = 0$ and there would be no $V_3(\mathbf{v})$ part.

F_0	G_0	n	$\mathbf{v}$
1	1	0	$\emptyset$
$P_1P_2, \deg(P_i) = 1$	Q	0	$\emptyset$
$P_1P_2, \deg(P_i) = i$	Q_1Q_2	0	$\emptyset$
$P_1P_2, \deg(P_i) = 2$	$T(T+1)(T+2)$	0	$\emptyset$
$T(T+1)(T+2)P, \deg(P) = 2$	$T(T+1)(T+2)$	0	$\emptyset$
$P, \deg(P) = 1$	Q	1	$v_0 = 1$
$P, \deg(P) = 2$	Q_1Q_2	1	$v_0 = 1$
$T(T+1)(T+2)$	Q_1Q_2	1	$v_0 = 1$
$P, \deg(P) = 1$	Q_1Q_2	1	$v_0 = 2$
$P, \deg(P) = 2$	$T(T+1)(T+2)$	1	$v_0 = 2$
$T(T+1)(T+2)$	$T(T+1)(T+2)$	1	$v_0 = 2$
1	Q	2	$v_{1,0} = v_{2,0} = 1$
1	Q_1Q_2	2	$v_{1,0} = 1, v_{2,0} = 2$
1	$T(T+1)(T+2)$	2	$v_{1,0} = v_{2,0} = 2$

Observing this table proves Corollary 1.4 for $q = 3$.

4.2. $q = 2$. Following the same method as for $q = 3$, we can use the observation $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^6 - 1 = 3^2 \cdot 7$ to get that a solution to (4.1) corresponds to a solution to the system of equations

$$\begin{aligned}\omega_2(F_0) + \omega_2(G) + 2\omega_6(F_0) + 2\omega_6(G) \\ = \omega_{1,1}(G_0) + 2\omega_{1,5}(G_0) + 2\omega_{2,2}(G_0) + 2\omega_{3,1}(G_0)\end{aligned}$$

$$\begin{aligned}\omega_3(F_0) + \omega_3(G) + \omega_6(F_0) + \omega_6(G) \\ = \omega_{1,2}(G_0) + \omega_{1,5}(G_0) + \omega_{2,2}(G_0) + \omega_{3,1}(G_0)\end{aligned}$$

subject to the constraints that

$$\omega_2(F_0), \omega_2(G) \leq \pi_2(2) = 1 \qquad \omega_3(F_0), \omega_3(G) \leq \pi_2(3) = 2$$
$$\omega_6(F_0), \omega_6(G) \leq \pi_2(6) = 9 \qquad \omega_{1,1}(G_0) + \omega_{1,2}(G_0) + \omega_{1,5}(G_0) \leq \pi_2(1) = 2$$
$$\omega_{2,2}(G_0) \leq \omega_2(G) \qquad \omega_{3,1}(G_0) \leq \omega_3(G).$$

Again, we can manually find all the solutions to the above equations. We find that after observing all possible solutions we always have $n \leq 3$. Further, if $n = 0$ then there is no $\mathbf{v}$; if $n = 1$ then we can find a solution for all $\mathbf{v}$ such that $v_1 | 6$; if $n = 2$, we can find a solution for all $\mathbf{v}_1, \mathbf{v}_2$ such that $v_{1,0}, v_{2,0} | 6$ except for $(v_{1,0}, v_{2,0}) = (2, 2)$; if $n = 3$, then we can find a solution for all $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ such that $v_{1,0}, v_{2,0} | 6, v_{3,0} = 1$ except for

$(v_{1,0}, v_{2,0}, v_{3,0}) = (1,1,1)$ or $(2,2,1)$. We do not write down all the possible solutions as there are too many cases and it is not enlightening to do so. However, in the table below we give an example for each possible case. For ease of notation, we will denote P_i, Q_j as primes such that $\deg(P_i) = i$ and $\deg(Q_j) = j$.

F_0	G_0	n	$\mathbf{v}$
1	1	0	$\emptyset$
1	1	1	$v_0 = 1$
P_2	Q_3	1	$v_0 = 2$
P_2	Q_2^2	1	$v_0 = 3$
P_2	$Q_2^2 Q_3$	1	$v_0 = 6$
1	1	2	$v_{1,0} = 1, v_{2,0} = 1$
P_2	Q_3	2	$v_{1,0} = 1, v_{2,0} = 2$
P_2	Q_2^2	2	$v_{1,0} = 1, v_{2,0} = 3$
P_2	$Q_2^2 Q_3$	2	$v_{1,0} = 1, v_{2,0} = 6$
P_2	$Q_1^2 Q_3$	2	$v_{1,0} = 2, v_{2,0} = 3$
P_2	$Q_1^2 Q_{3,1} Q_{3,2}$	2	$v_{1,0} = 2, v_{2,0} = 6$
P_2	$Q_1^2 Q_2^2$	2	$v_{1,0} = 3, v_{2,0} = 3$
P_2	$Q_1^5 Q_2^2$	2	$v_{1,0} = 3, v_{2,0} = 6$
P_2	$Q_1^5 Q_2^2 Q_3$	2	$v_{1,0} = 6, v_{2,0} = 6$

For examples with $n = 3$, $F = F_0F_1F_2F_3$, $G = G_0G_1G_2G_3$, let $(F_3, G_3) \in V_2(\mathbf{v}_3)$ with $v_{3,0} = 1$ and $(F_0F_1F_2, G_0G_1G_2)$ one of the examples above with $n = 2$.

Even though all our examples have F_0 either 1 or a prime of degree 2 this is not always the case. For example, in the case that $n = 1$ and $v_0 = 6$ we can choose

$$F_0 = P_2P_6 \qquad G_0 = Q_1^5 Q_2^2 Q_3.$$

References

[1] E. ARTIN, "The orders of the linear groups", *Commun. Pure Appl. Math.* **8** (1955), p. 355-365.

[2] A. S. BANG, "Taltheoretiske undersøgelser", *Tidsskrift for mathematik* **4** (1886), p. 70-80.

[3] L. BARY-SOROKER, "Hardy–Littlewood tuple conjecture over large finite fields", *Int. Math. Res. Not.* **2014** (2014), no. 2, p. 568-575.

[4] A. O. BENDER & P. POLLACK, "On quantitative analogues of the Goldbach and twin prime conjectures over $\mathbb{F}_q[t]$", `https://arxiv.org/abs/0912.1702`, 2009.

[5] D. CARMON, "The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field in characteristic 2", *Philos. Trans. A, R. Soc. Lond.* **373** (2015), no. 2040, article ID 20140311 (14 pages).

[6] P. ERDŐS, "Remarks on number theory II. Some problems on the σ function", *Acta Arith.* **5** (1959), p. 171-177.

[7] K. FORD, F. LUCA & C. POMERANCE, "Common values of the arithmetic functions ϕ and σ", *Bull. Lond. Math. Soc.* **42** (2010), no. 3, p. 478-488.

[8] K. FORD & P. POLLACK, "On common values of $\varphi(n)$ and $\sigma(m)$. I", *Acta Math. Hung.* **133** (2011), no. 3, p. 251-271.

[9] ———, "On common values of $\phi(n)$ and $\sigma(m)$, II", *Algebra Number Theory* **6** (2012), no. 8, p. 1669-1696.

[10] K. Zsigmondy, "Zur theorie der Potenzreste", *Monatsh. f. Math.* **3** (1892), p. 265-284.

Patrick Meisner
Tel Aviv University, Israel
E-mail: pfmeisner@gmail.com