DIVISIBILITY OF THE MULTIPLICATIVE ORDER MODULO MONIC IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

JOAQUIM CERA DA CONCEIÇÃO

ABSTRACT. We consider the set of monic irreducible polynomials P over a finite field $\mathbb{F}_q$ such that the multiplicative order modulo P of some a in $\mathbb{F}_q(T)$ is divisible by a fixed positive integer d. Call $R_q(a, d)$ this set. We show the existence or non-existence of the density of $R_q(a, d)$ for three distinct notions of density. In particular, the sets $R_q(a, d)$ have a Dirichlet density. Under some assumptions, we prove simple formulas for the density values.

CONTENTS

1. INTRODUCTION

Let $a \in \mathbb{Q} \setminus \{0, \pm 1\}$ and d be a positive integer. The proportion of rational prime numbers p such that d divides the multiplicative order of a modulo p has been widely studied. It was originally considered by Hasse [6, 7] in 1965 and 1966, with a a square-free integer and d a prime number, in order to find the natural density of the set of primes dividing the sequence $(1 + a^n + \cdots + a^{(d-1)n})_{n \geq 0}$ at some $n \geq 0$. The problem was completely solved when Wiertelak [16] proved the following theorem:

Theorem 1. *Let $N_a(d)$ be the set of prime numbers p such that d divides the multiplicative order of a modulo p and $N_a(d; x) = N_a(d) \cap [1, x]$. Then*

$$N_a(d; x) = \delta_a(d)\mathrm{Li}(x) + \mathcal{O}_{d,a}\left(\frac{x(\log\log x)^{\omega(d)+1}}{(\log x)^3}\right),$$

where the implied constant depends on d and a, Li *is the logarithmic integral func-tion, ω is the number of distinct-prime-divisor function, and $\delta_a(d) \in [0,1]$ is the natural density of $N_a(d)$.*

Moreover, Wiertelak gave a formula for $\delta_a(d)$ that shows that $\delta_a(d) \in \mathbb{Q}_{>0}$. More recently, Pappalardi [12] took a different approach to this problem and obtained another equivalent formula for the density. It was given in a more compact form by Moree [10], using a similar method. Note that in some cases, the set $N_a(d)$ is also related to sets of prime divisors of some linear integral sequences. See [1, Chapter 3] for the definition of such sequences and the computation of some of the densities.

There is an analogy between $\mathbb{Z}$ and the ring of polynomials $A = \mathbb{F}_q[T]$ with positive characteristic p. Both are euclidean rings in which prime numbers and monic irreducible polynomials are prime elements. The analogue of $\mathbb{Q}$ is the fraction field of A, that is, $K = \mathbb{F}_q(T)$. With the above problem in mind, it is natural to ask whether a similar investigation can be conducted for monic irreducible polynomials in A. This is the object of our paper. Let $a \in K^\times$ and d be a positive integer. We define $R_q(a,d)$ to be the set of primes $P \in A$ such that the multiplicative order of a in the group $(A/P)^\times$ is divisible by d. To our knowledge, the only instance of study of these sets are recent papers of Ballot [2, 3] in which the case $a = T$ and d a prime number is treated with elementary methods. To determine the proportion of such primes, we use prime densities on A. Let $S \subset A$ be a set of monic irreducible polynomials and $S(N)$ be the number of $P \in S$ with polynomial degree $N \geq 1$. The most common densities are the d_1 and δ densities defined, when they exists, by the limits

$$d_1(S) = \lim_{N \to +\infty} \frac{S(N)}{\mathcal{P}_+(N)} \quad \text{and} \quad \delta(S) = \lim_{s \to 1^+} \frac{\sum_{P \in S} NP^{-s}}{\sum_{P \in \mathcal{P}_+} NP^{-s}}.$$

The letter $\mathcal{P}_+$ denotes the set of monic irreducible polynomials in A and $NP = q^{\deg(P)}$ is the norm of P. The quantity $\mathcal{P}_+(N)$ is usually denoted I_N and is given by the sum

$$I_N = \frac{1}{N} \sum_{d|N} \mu(d) q^{N/d}.$$

The number $\delta(S)$ is called the *Dirichlet density* of S and is the analogue of the Dirichlet density used for rational prime numbers. However, in a discussion about prime densities on A, Ballot [4] defines five densities d_1, d_2, d_3, d_4 and δ, and con-cludes two things. Denoting by $\delta_1 \implies \delta_2$ the fact that any set of primes in A having a δ_1-density equal to d must have a δ_2-density equal to d, [4, Theorem A] states the following:

$$d_1 \iff d_2 \implies d_3 \implies d_4 \iff \delta.$$

Moreover, d_3 is not equivalent to d_2, nor d_4. In conclusion, there are three distinct densities to be considered. In this paper, we consider d_1, δ and the d_3-density defined by the limit

$$d_3(S) = \lim_{N \to +\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{S(n)}{I_n} = \lim_{N \to +\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{S(n)}{q^n/n},$$

when it exists. Note that the second equality comes from the well-known equiva-lence $I_n \sim q^n/n$ as n tends to infinity. Secondly, although there is some evidence

of d_1 being an analogue of the natural density commonly used on $\mathbb{N}$, Ballot concludes that d_3 seems to be a better candidate. Indeed, various sets of rational prime numbers that are known to have natural density have analogues in A that do not have d_1-density but have d_3-density. In this work, we prove that the set $R_q(a,d)$ does not usually have d_1-density, but always has d_3-density, thus confirming d_3 as a strong analogue of the natural density. Our work is based on the method used by Pappalardi [12] and Moree [10], and on the elementary approach taken by Ballot [2, 3].

In Section 2, we give definitions and results related to function fields that make up our main toolbox. An important tool is an analogue of the Chebotarev Density Theorem for global function fields. Another gives necessary and sufficient conditions for primes in a global function field K to completely split in a Galois extension L/K.

The idea is to describe $R_q(a,d)$ as a union of sets of primes that completely split in Kummer extensions of $K = \mathbb{F}_q(T)$, i.e., fields of the form $K(\zeta_n, a^{1/d})$, where d, n are positive integers such that $(n,p) = 1$ and $d \mid n$, $\zeta_n \in \bar{\mathbb{F}}_q$ is a primitive n-th root of unity and $a \in K^\times$. From this and the above-mentioned analogue of Chebotarev's Density Theorem, we obtain an asymptotic formula for $R_q(a,d,N) := R_q(a,d)(N)$ that involves degrees of Kummer extensions. Therefore, to make our formula simpler and to later compute a closed-form formula for the density, we need to determine the degree of Kummer extensions of K. In Section 3, we study the form an element $a \in K^\times$ may take when $K(a^{1/n})/K$ is a constant field extension, i.e., an extension of $\mathbb{F}_q$. These results are our primary tools for computing degrees of Kummer extensions in Section 4.

In Section 5, we show that $R_q(a,d,N)$ may be expressed in terms of the cardinality of sets of primes that completely split in some Kummer extensions of K. Applying the analogue of the Chebotarev Density Theorem, we find an asymptotic formula for $R_q(a,d,N)$ of the form

$$|R_q(a,d,N) - \delta_q(a,d,N) \cdot q^N/N| \ll f(N),$$

for some function f and where $\delta_q(a,d,N)$ is called the *proportion-density* of the quantity $R_q(a,d,N)$. (See Theorem 7.) We obtain a formula for $\delta_q(a,d,N)$ that involves degrees of Kummer extensions of K.

Section 6 is dedicated to preliminary results for the proofs of the main theorems. We prove a formula for the multiplicative order of an integer, and another for integers of the form $q^n - 1$, where n, q are integers. Moreover, we give a property of the degree of constant fields of some special Kummer extensions.

Our main results, Theorem 8 and Theorem 9, on the existence or non-existence of the d_1 and d_3-densities of $R_q(a,d)$ are proved in Section 7. The asymptotic formula given in Theorem 9 revolves around a technique used by Ballot that consists of partitioning $\mathbb{N}$ into adequate disjoint arithmetic progressions. For all $n \geq 1$ that belong in the same arithmetic progression, we find that $\delta_q(a,d,n)$ is a constant independent of n, thus simplifying most calculations.

Under some assumption on the degree of constant fields of some Kummer extensions, we prove in Section 8 that $d_3(R_q(a,d))$ can be written in a closed-form formula. (See Theorem 10.) We end our paper by giving sufficient conditions for this assumption to hold.

Throughout this paper, the letters l and p denote prime numbers, the letter q denotes a power of p, and the letters d, n and N denote positive integers with $d \mid n$

and $p \nmid n$. Given an integer d, we let d^∞ denote the *supernatural number*

$$d^\infty = \prod_{l \mid d} l^\infty.$$

This notation allows us to consider positive divisors v of d^∞, i.e., $v \mid d^t$ for some $t \geq 1$, and to use notation such as

$$(k, d^\infty) = \prod_{l \mid d} k^{v_l(k)},$$

where (a, b) denotes the gcd of a and b, and v_l denotes l-adic valuation. Note that $k \mapsto (k, d^\infty)$ is completely multiplicative, while $k \mapsto (k, d)$ is only multiplicative. We write $[a, b]$ for the lcm of two integers a and b. Given a field F, we denote by $(F^\times)^k$ the set of k-th powers in F and by $\bar{F}$ its algebraic closure. We write ω, τ, μ, φ and ψ to denote the number of distinct prime factors function, the number of divisors function, the Möbius function, Euler's totient function and Dedekind psi function, respectively. For a multiplicative group G and $g \in G$, we let $\mathrm{ord}_G(g)$ and $\mathrm{ind}_G(g)$ denote respectively the order and the index of g. Particular cases include the multiplicative group $G = (\mathbb{Z}/n\mathbb{Z})^\times$, for which we use the notation $\mathrm{ord}_n(g)$ and $\mathrm{ind}_n(g)$, and $G = (\mathbb{F}_q[T]/(P))^\times$, with the notation $\mathrm{ord}_P(g)$ and $\mathrm{ind}_P(g)$, where $n \geq 1$ and $P \in \mathbb{F}_q[T]$. We let the letters K and A denote respectively the rational function field $\mathbb{F}_q(T)$ and its integer ring $\mathbb{F}_q[T]$. For $f \in A$ non-zero, we let $\tilde{f}$ denote the monic part of f, that is, the unique monic polynomial in A such that $f = u\tilde{f}$ for some $u \in \mathbb{F}_q^\times$.

2. KNOWN RESULTS

We use this section to state two important results for our work. The first theorem is a special case of a theorem that takes various forms in literature. It is usually referred to as the Chebotarev Density Theorem for global function fields. (See [5, Proposition 6.4.8] or, for the curve point of view, [11, Theorem 1].) It gives a bound on the number of primes in K of a fixed degree satisfying a certain property. Since there are finitely many primes of degree N, the name "density" is not the most accurate. We use the term *proportion-density* instead to refer to the "density" number described in the theorem. Throughout this paper, we denote by g_L the genus of a field L and by $\mathcal{P}_+$ the set of monic irreducible polynomials in A.

Theorem 2. *Let L/K be a Galois extension of global function fields and $\mathbb{F}_{q^n}$ be the constant field of L. Put $m := [L : \mathbb{F}_{q^n} K]$ and*

$$\pi(N) := \#\{P \in \mathcal{P}_+ : \deg(P) = N \text{ and } P \text{ splits completely in } L\}.$$

Then $\pi(N) = 0$ if $n \nmid N$, and otherwise, we have

$$\left| \pi(N) - \frac{q^N}{Nm} \right| \leq \frac{2}{Nm} \left((m + g_L)q^{N/2} + mq^{N/4} + g_L + m \right).$$

Proof. It is a special case of [5, Proposition 6.4.8].   □

The second result gives necessary and sufficient conditions for a prime to split completely in some Kummer extensions of K.

Theorem 3. *Let $n \geq 1$ be an integer with $p \nmid n$ and $a \in K^\times$. A prime P in A that satisfy $v_P(a) = 0$ splits completely in $K(\zeta_n, a^{1/d})$ if and only if the following holds:*

$$NP \equiv 1 \pmod{n} \quad \text{and} \quad a^{\frac{NP-1}{d}} \equiv 1 \pmod{P}.$$

Proof. It suffices to follow the proof of [13, Proposition 10.6]. □

3. ON CONSTANT FIELD EXTENSIONS

Let M/L be an algebraic extension of function fields. We say that M is a constant field extension of L if $M = (M \cap \bar{\mathbb{F}}_q)L$. Similarly, we say that M is a geometric extension of L if $M \neq L$ and $M \cap \bar{\mathbb{F}}_q = L \cap \bar{\mathbb{F}}_q$. Note that it is likely that M/L is neither a geometric nor a constant field extension, but in that case we can always split it in two such extensions. In this section, we give necessary and sufficient conditions for an algebraic extension $K(a^{1/n})/K$ to be a constant field extension, where $a \in K^\times$.

Lemma 1. *Let $a \in K^\times$ and $l \neq p$ be a prime. Then, $K(a^{1/l})/K$ is a constant field extension if and only if $a = \mu b^l$ for some $b \in K^\times$ and $\mu \in \mathbb{F}_q^\times$.*

Proof. By [8, Lemma 3.3], we have $K(a^{1/l})/K$ non-geometric if and only if $a = \mu b^l$ for some $b \in K^\times$ and $\mu \in \mathbb{F}_q^\times$. Since l is a prime, any non-geometric extension is a constant field extension. □

Theorem 4. *Let $a \in K^\times$. Then, $K(a^{1/n})/K$ is a constant field extension if and only if $a = \mu b^n$ for some $b \in K^\times$ and $\mu \in \mathbb{F}_q^\times$.*

Proof. If $a = \mu b^n$, then the result follows directly. For the converse, we start with the case $a \in A$. First assume that the result holds for prime powers and write $n = q_1 \cdots q_s$, where the q_i's are powers of distinct primes and $s \geq 2$. We have

$$a = \mu_1 b_1^{q_1} = \cdots = \mu_s b_s^{q_s} \quad \text{and} \quad \tilde{a} = \tilde{b}_1^{q_1} = \cdots = \tilde{b}_s^{q_s},$$

for some non-zero $b_i \in A$ and $\mu_i \in \mathbb{F}_q^\times$. Since the q_i's are powers of distinct primes, we obtain

$$\tilde{b}_1 \in \bigcap_{i=2}^{s} (K^\times)^{q_i},$$

thus $\tilde{a} = b^n$ for some non-zero $b \in A$, and $a = \mu\tilde{a} = \mu b^n$. Hence it suffices to prove the result for prime powers. Let l be a prime number and $k \geq 1$. We proceed by induction on $k \geq 1$ to show the statement holds for all $n = l^k$. The base case follows from Lemma 1. Assume the statement holds for some $k \geq 1$ and that $K(a^{1/l^{k+1}})/K$ is a constant field extension. In particular, $K(a^{1/l})/K$ a constant field extension and we may write $a = \mu b^l$ using Lemma 1. Let x be an l^{k+1}-th root of a in $L := K(a^{1/l^{k+1}})$. Then

$$\tilde{a} = \tilde{b}^l = \tilde{x}^{l^{k+1}},$$

and we obtain $\tilde{b} = \zeta_l \tilde{x}^{l^k}$ for some l-th root of unity ζ_l. Since $\tilde{b}$ and $\tilde{x}$ are both monic polynomials in the ring of integers of L, we find that $\zeta_l = 1$. Because $\tilde{x} \in L$, we find that $K(\tilde{b}^{1/l^k})$ is a subfield of L, thus $K(\tilde{b}^{1/l^k})/K$ is a constant field extension. By the induction hypothesis, we have $\tilde{b} = \lambda c^{l^k} = \tilde{c}^{l^k}$ for some $\lambda \in \mathbb{F}_q^\times$ and $c \in K^\times$. Hence $\tilde{a} = \tilde{b}^l = \tilde{c}^{l^{k+1}}$ and $a = \mu\tilde{c}^{l^{k+1}}$, where $\mu \in \mathbb{F}_q^\times$ is the leading coefficient of a. We successfully proved the result for $a \in A$. If $a = f/g \in K^\times$, then

$K(a^{1/n}) = K((fg^{n-1})^{1/n})$ and by the above, fg^{n-1} is of the form μb^n. Hence we have $a = \mu(b/g)^n$.   □

4. THE DEGREE OF KUMMER EXTENSIONS OF RATIONAL FUNCTION FIELDS

We extend the notation $\tilde{a}$ to rational functions $a = f/g \in K^\times$ by $\tilde{a} = \tilde{f}/\tilde{g}$. We denote by $\lambda \in \mathbb{F}_q^\times$ the unique constant such that $a = \lambda\tilde{a}$. Let h denote the largest integer $t \geq 1$ such that $\tilde{a} \in (K^\times)^t$. In this section, we study Kummer extensions of $K = \mathbb{F}_q(T)$, that is, fields of the form $K(\zeta_n, a^{1/d})$, where $\zeta_n \in \bar{\mathbb{F}}_q$ is a primitive n-th root of unity and $a \in K^\times$. We find formulas for the following field degrees:

$$[K(\zeta_n, a^{1/d}) : \mathbb{F}_{n,d}K] \quad \text{and} \quad [\mathbb{F}_{n,d} : \mathbb{F}_q],$$

where $\mathbb{F}_{n,d}$ denotes the constant field of $K(\zeta_n, a^{1/d})$. The key result we use is the following theorem on polynomials of the form $X^n - a$:

Theorem 5. *Let K be a field and $a \in K^\times$. Then $X^n - a$ is irreducible over K if and only if $a \notin (K^\times)^l$ for all $l \mid n$ and $a \notin -4(K^\times)^4$ if $4 \mid n$.*

Proof. See [9, Theorem 9.1].   □

Lemma 2. *Let $\mu \in \mathbb{F}_q^\times$. We have*

$$[\mathbb{F}_q(\zeta_n, \mu^{1/d}) : \mathbb{F}_q] = \frac{\mathrm{ord}_n(q)d}{(\mathrm{ind}_{\mathbb{F}_q(\zeta_n)^\times}(\mu), d)}.$$

Proof. It is known that $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \mathrm{ord}_n(q)$. Let $u = \mathrm{ind}_{\mathbb{F}_q(\zeta_n)^\times}(\mu)$ be the index of μ in $\mathbb{F}_q(\zeta_n)$, that is, the greatest positive divisor $t \mid q^{\mathrm{ord}_n(q)} - 1$ such that $\mu = x^t$ for some $x \in \mathbb{F}_q(\zeta_n)^\times$. We have

$$\mathbb{F}_q(\zeta_n, \mu^{1/d}) = \mathbb{F}_q(\zeta_n, v^{1/d_0}),$$

where $d_0 = d/(d, u)$ and $v^{(u,d)} = \mu$. We claim that d_0 is the degree of the extension $\mathbb{F}_q(\zeta_n, \mu^{1/d})/\mathbb{F}_q(\zeta_n)$. Indeed, let us show that $X^{d_0} - v$ is irreducible over $\mathbb{F}_q(\zeta_n)$ using Theorem 5. Let $l \mid d_0$ be a prime. By contradiction, if we have $v = c^l$ for some $c \in \mathbb{F}_q(\zeta_n)$, then

$$x^u = \mu = v^{(u,d)} = c^{l(u,d)}.$$

Because $d_0 \mid q^{\mathrm{ord}_n(q)} - 1$ and by the maximality of u, we must have $l(u,d) \mid u$. This yields a contradiction since $l \mid d_0$. Now, if $4 \mid d_0$, assume by contradiction that $v = -4y^4$ for some $y \in \mathbb{F}_q(\zeta_n)$. Then, since v is not a square in $\mathbb{F}_q(\zeta_n)$ by the above, we find that -1 is not a square in $\mathbb{F}_q(\zeta_n)$. Hence $4 \nmid q^{\mathrm{ord}_n(q)} - 1$, but $4 \mid d_0$ and $d_0 \mid n$ imply that $4 \mid q^{\mathrm{ord}_n(q)} - 1$. We find a contradiction. By Theorem 5, the polynomial $X^{d_0} - v$ is irreducible over $\mathbb{F}_q(\zeta_n)$ and the result follows.   □

Lemma 3. *Let $a \in K^\times$. Then the greatest divisor v of d such that the extension $K(\zeta_n, a^{1/v})/K$ is a constant field extension is equal to (d, h). In particular, the constant field $\mathbb{F}_{n,d}$ of $K_{n,d}$ is equal to $\mathbb{F}_q(\zeta_n, \lambda^{1/(d,h)})$.*

Proof. We search for the maximal subfield M of $K(\zeta_n, a^{1/d})$ such that M/K is a constant field extension. We claim that $M = K(\zeta_n, a^{1/D})$, with $D = (d, h)$. Let us first show it is indeed a constant field extension of K. Write $h = Dk$ and $\tilde{a} = \tilde{b}^{Dk}$ for some $k \geq 1$ and $\tilde{b} \in K^\times$. We have

$$K(\zeta_n, a^{1/D}) = K(\zeta_n, \lambda^{1/D}\tilde{b}^k) = K(\zeta_n, \lambda^{1/D}) = \mathbb{F}_q(\zeta_n, \lambda^{1/D})K,$$

and we obtain a constant field extension of K. Next, we prove that D is maximal. By contradiction, assume there exists a prime l such that $lD \mid d$ and that $K(\zeta_n, a^{1/lD})$ is a constant field extension of K. Then, $K(a^{1/lD})/K$ is a constant field extension and, by Theorem 4, there exists $\omega, \lambda \in \mathbb{F}_q^\times$ and $c \in K^\times$ such that

$$a = \omega c^{lD} = \lambda \tilde{c}^{lD}.$$

Hence $\tilde{a} = \tilde{c}^{lD}$ and, by maximality of h, we find that $lD \mid h$. We obtain

$$l \mid \left(\frac{d}{(d,h)}, \frac{h}{(d,h)} \right) = 1,$$

which is a contradiction. Therefore, D is the maximal divisor $v \mid d$ such that $K(\zeta_n, a^{1/v})/K$ is a constant field extension and $\mathbb{F}_{n,d} = \mathbb{F}_q(\zeta_n, \lambda^{1/(d,h)})$. $\qquad\square$

Theorem 6. *Let $a \in K^\times$. We have*

$$[K(\zeta_n, a^{1/d}) : \mathbb{F}_{n,d}K] = \frac{d}{(d,h)}.$$

Proof. Put $d_0 = d/(d,h)$ and write $a = b^D$, where $D = (d,h)$ and $b \in \mathbb{F}_{n,d}K^\times$. The latter is possible since $a = \lambda \tilde{c}^D$ for some $c \in K^\times$, by Lemma 3 and Theorem 4. Thus $a = (\mu \tilde{c})^D$ with $\mu \in \mathbb{F}_{n,d}$ and $\mu^D = \lambda$. Using Theorem 5, we show that the polynomial $X^{d_0} - b$ is irreducible over $\mathbb{F}_{n,d}K^\times$. Let $l \mid d_0$ be a prime and assume by contradiction that $b = x^l$ for some $x \in \mathbb{F}_{n,d}K^\times$. Since $\mathbb{F}_{n,d}K$ is a rational function field and because $a \in A$, we find that $x \in \mathbb{F}_{n,d}[T]$. Then $\lambda = x_0^{lD}$, where $x_0 \in \mathbb{F}_{n,d}$ is the leading coefficient of x. But, by Lemma 3, D is the greatest positive integer $t \mid d$ such that λ is a t-th power in $\mathbb{F}_{n,d}^\times$. Hence we have a contradiction and $b \notin (\mathbb{F}_{n,d}K^\times)^l$. Now, if $4 \mid d_0$, then assume by contradiction that $b = -4x^4$ for some $x \in \mathbb{F}_{n,d}K^\times$. By the above, b is not a square in $\mathbb{F}_{n,d}K$, thus -1 is not a square in $\mathbb{F}_{n,d}K$. This yields that $4 \nmid \#\mathbb{F}_{n,d}^\times$. But $4 \mid d_0$ and $d_0 \mid \#\mathbb{F}_{n,d}^\times$, we have a contradiction. Hence $b \neq -4x^4$ and $X^{d_0} - b$ is irreducible over $\mathbb{F}_{n,d}K^\times$ by Theorem 5. $\qquad\square$

Corollary 1. *Let $a \in K^\times$. We have*

$$[K(\zeta_n, a^{1/d}) : K] = \frac{\mathrm{ord}_n(q)d}{(\mathrm{ind}_{\mathbb{F}_q(\zeta_n)^\times}(\lambda), d, h)}.$$

Proof. Using [13, Proposition 8.1], we have

$$[K(\zeta_n, a^{1/d}) : K] = [K(\zeta_n, a^{1/d}) : \mathbb{F}_{n,d}K][\mathbb{F}_{n,d}K : K]$$
$$= [K(\zeta_n, a^{1/d}) : \mathbb{F}_{n,d}K][\mathbb{F}_{n,d} : \mathbb{F}_q].$$

Then, it suffices to use the results of Lemmas 2 and 3, and Theorem 6. $\qquad\square$

5. The proportion-density

Throughout the rest of this paper, we denote by $R_q(a,d)$ the set

$$R_q(a,d) := \{P \in \mathcal{P}_+ : v_P(a) = 0 \text{ and } d \mid \mathrm{ord}_P(a)\},$$

where $a \in K^\times$ and $d \geq 1$ are fixed, and $\mathcal{P}_+$ is the set of monic irreducible polynomials in A. For each $N \geq 1$, we consider $R_q(a,d,N)$ the number of primes in

$R_q(a,d)$ with degree N. We denote by I_N the number of degree N polynomials in $\mathcal{P}_+$. It is well-known that

$$I_N = \frac{1}{N}\sum_{n|N}\mu(n)q^{N/n}.$$

Trivially, for $d = 1$, we have $R_q(a, 1, N) = I_N - a_N$, where a_N is the number of P of degree N such that $v_P(a) \neq 0$. Note that $a_N \neq 0$ for only finitely many N. Moreover, if $a = \lambda \in \mathbb{F}_q^\times$, then

$$R_q(\lambda, d, N) = \begin{cases} I_N, & \text{if } d \mid \operatorname{ord}_{\mathbb{F}_q^\times}(\lambda); \\ 0, & \text{otherwise.} \end{cases}$$

The densities in such particular cases are easily computed. First, the d_1-density of $R_q(a, d)$ is 1, and it follows that the d_i's and the Dirichlet densities of $R_q(a, 1)$ also exist and equal 1. Same goes for $R_q(a, \lambda)$ for which the densities are 1 or 0, whether $d \mid \operatorname{ord}_{\mathbb{F}_q^\times}(\lambda)$.

We assume that $d \geq 2$ and a is not a constant for the rest of this paper. A less obvious fact is that $\operatorname{ord}_d(q) \nmid N$ implies $R_q(a, d, N) = 0$. Indeed, to have $d \mid \operatorname{ord}_P(a)$ we must have $d \mid NP - 1 = q^N - 1$, that is, $\operatorname{ord}_d(q) \mid N$. Let $f := \operatorname{ord}_d(q)$. For all $N \equiv 0 \pmod{f}$, put

$$e_N(d) = e_N := \left(\frac{q^N - 1}{d}, d^\infty\right).$$

Since K is fixed throughout this paper, we denote by $\{L\}$ the set of primes in K that splits completely in L, where L/K is an algebraic extension. For each $N \geq 1$, we let $\{L\}_N$ denote the set of primes in $\{L\}$ with degree N. We consider the set $\mathcal{P}_+(a)$ of primes $P \in \mathcal{P}_+$ such that $v_P(a) = 0$. We assume throughout the paper that $a = \lambda\tilde{a}$ and $\tilde{a} = b^h$, with the notation of the previous section.

Lemma 4. *For each positive $N \equiv 0 \pmod{f}$, we have*

$$R_q(a, d, N) = \sum_{v|e_N}\sum_{u|d}\mu(u)\{K_{dv,uv}\}_N,$$

Proof. Let $S(N)$ be the set of monic irreducible polynomials in $R_q(a, d)$ that have degree N. A prime $P \in S(N)$ satisfies

$$\deg(P) = N, \quad d \mid \operatorname{ord}_P(a) \quad \text{and} \quad v_P(a) = 0.$$

Since $q^N - 1 = \operatorname{ord}_P(a)\operatorname{ind}_P(a)$, the condition $d \mid \operatorname{ord}_P(a)$ is equivalent to $d \cdot (\operatorname{ind}_P(a), d^\infty) \mid q^N - 1$, that is, there exists a unique $v \mid d^\infty$ such that

$$dv \mid q^N - 1, \quad v \mid \operatorname{ind}_P(a) \quad \text{and} \quad \left(\frac{\operatorname{ind}_P(a)}{v}, d\right) = 1. \tag{1}$$

The last condition in (1) is equivalent to $lv \nmid \operatorname{ind}_P(a)$ for all primes $l \mid d$. Hence

$$S(N) = \bigsqcup_{v|e_N}\left(S_{1,v}(N) \setminus \bigcup_{l|d}S_{l,v}(N)\right),$$

where $S_{u,v}(N) = \{P \in \mathcal{P}_+(a) : \deg(P) = N, \; dv \mid q^N - 1 \text{ and } uv \mid \operatorname{ind}_P(a)\}$. By Theorem 3, we find that the set $S_{u,v}(N)$ is exactly the set $\{K_{dv,uv}\}_N$. The result follows by the inclusion-exclusion principle. $\qquad\square$

Proposition 1. *There exists $c_0 > 0$, that only depends on a, such that*

$$g_{K_{n,d}} \leq c_0 \cdot [K_{n,d} : \mathbb{F}_{n,d}K].$$

Proof. It suffices to apply [15, Proposition 3.7.3] to $K_{n,d}$. □

Lemma 5. *For each $N \geq 1$ such that $[\mathbb{F}_{n,d} : \mathbb{F}_q] \mid N$, we have*

$$\left| \{K_{n,d}\}_N - \frac{q^N}{N} \frac{1}{[K_{n,d} : \mathbb{F}_{n,d}K]} \right| \leq 2c_1 \cdot \frac{q^{N/2}}{N},$$

with c_1 the absolute constant

$$c_1 = \frac{1}{\sqrt[4]{q}} + \left(1 + \frac{1}{\sqrt{q}} \right)(c_0 + 1),$$

where c_0 is the constant from Proposition 1.

Proof. By Theorem 2, the quantity

$$\left| \{K_{n,d}\}_N - \frac{q^N}{N} \frac{1}{[K_{n,d} : \mathbb{F}_{n,d}K]} \right|$$

is bounded above, for all N divisible by $[\mathbb{F}_{n,d} : \mathbb{F}_q]$, by

$$f(N) = \frac{2}{Nm_{n,d}} \left((m_{n,d} + g_{K_{n,d}})q^{N/2} + m_{n,d}q^{N/4} + g_{K_{n,d}} + m_{n,d} \right),$$

where $m_{n,d} = [K_{n,d} : \mathbb{F}_{n,d}K]$. The result follows by the trivial bounds

$$\frac{1}{N} \leq \frac{1}{\sqrt{q}} \frac{q^{N/2}}{N} \quad \text{and} \quad \frac{q^{N/4}}{N} \leq \frac{1}{\sqrt[4]{q}} \frac{q^{N/2}}{N},$$

and the bound given in Proposition 1, where all three hold for $N \geq 1$. □

Let $\mathcal{P}$ be a proposition. Throughout the rest of the paper, we use the Iverson symbol defined by $[\mathcal{P}] = 1$ if $\mathcal{P}$ is true, and $[\mathcal{P}] = 0$ otherwise. For integers $v \mid d^\infty$ and $u \mid d$, we let $f_{u,v} = [\mathbb{F}_{dv,uv} : \mathbb{F}_q]$, that is,

$$f_{u,v} = \frac{\operatorname{ord}_{dv}(q)(uv, h)}{(\operatorname{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\lambda), uv, h)}, \tag{2}$$

by Lemmas 2 and 3.

Theorem 7. *For each positive $N \equiv 0 \pmod{f}$, we have*

$$\left| R_q(a, d, N) - \frac{q^N}{N} \cdot \delta_q(a, d, N) \right| \leq 2^{\omega(d)+1} c_1 \cdot \frac{\tau(e_N)q^{N/2}}{N},$$

where c_1 is the absolute constant defined in Lemma 5 and $\delta_q(a, d, N)$ is defined by

$$\delta_q(a, d, N) = \sum_{v \mid e_N} \sum_{u \mid d} \frac{\mu(u)[f_{u,v} \mid N]}{[K_{dv,uv} : \mathbb{F}_{dv,uv}K]}.$$

Proof. Let $S_q(a, d, N)$ be the difference

$$S_q(a, d, N) = R_q(a, d, N) - \frac{q^N}{N} \cdot \delta_q(a, d, N).$$

By Lemmas 4 and 5, we have

$$
|S_q(a, d, N)| = \left| \sum_{v \mid e_N} \sum_{u \mid d} \mu(u) \left(\{K_{dv,uv}\}_N - \frac{q^N}{N} \frac{[f_{u,v} \mid N]}{[K_{dv,uv} : \mathbb{F}_{dv,uv} K]} \right) \right|
$$

$$
\leq 2c_1 \cdot \frac{q^{N/2}}{N} \sum_{v \mid e_N} \sum_{u \mid d} |\mu(u)|
$$

$$
= 2c_1 \cdot \frac{\tau(e_N) q^{N/2}}{N} \cdot \prod_{l \mid d} (1 + 1)
$$

$$
= 2^{\omega(d)+1} c_1 \cdot \frac{\tau(e_N) q^{N/2}}{N},
$$

the sought result.   □

6. More preliminary results

We show in this section three preliminary results to the study of the d_1 and d_3-densities of $R_q(a, d)$. Our first result gives basic arithmetic properties of certain numbers of the form $(q^N - 1, d^\infty)$. As a consequence, we prove a formula for $\mathrm{ord}_{dv}(q)$ that generalizes a well-known formula for $\mathrm{ord}_{l^k}(q)$, with $k \geq 1$. Finally, we prove that, under the hypothesis $f_{1,v} \mid N$, the Iverson symbol $[f_{u,v} \mid N]$ defines a multiplicative function in the variable u. We use the letter $\mathcal{P}$ to denote the proposition

$$
\mathcal{P}: \quad 2 \| d, \quad q \equiv 3 \pmod{4} \quad \text{and} \quad 2 \nmid f.
$$

The following lemma is enough to see that interesting things might happen when $\mathcal{P}$ is true:

Lemma 6. *Let* $m, n, q \geq 1$ *be integers with* $(d, q) = 1$ *and* $d \mid q^m - 1$. *Then*

$$
(q^{mn} - 1, d^\infty) = (q^m - 1, d^\infty)(n, d^\infty) \cdot \begin{cases} 2^{v_2(q^m+1)-1}, & \text{if } [\mathcal{P}] = 1 \text{ and } 2 \mid n; \\ 1, & \text{otherwise.} \end{cases}
$$

Proof. The map $d \mapsto (k, d^\infty)$, where k is a fixed integer, defines a completely multiplicative function. We obtain the product formula

$$
(q^{mn} - 1, d^\infty) = \prod_{l \mid d} (q^{mn} - 1, l^\infty). \tag{3}
$$

Therefore, it is enough to prove the result for all primes $l \mid d$. By [3, Lemma 4], and by replacing $\mathrm{ord}_l(q)$ by m in the proof, which is allowed since it only uses that $l \mid q^m - 1$, we obtain

$$
v_l(q^{mn} - 1) = v_l(q^m - 1) + v_l(n),
$$

for all $l \geq 3$ and $n \geq 1$, thus $(q^{mn} - 1, l^\infty) = (q^m - 1, l^\infty)(n, l^\infty)$. For $l = 2$, so in particular $2 \mid d$, we have

$$
v_2\left(\frac{q^{mn} - 1}{q^m - 1} \right) = v_2(n) + \begin{cases} v_2(q^m + 1) - 1, & \text{if } 2 \mid n; \\ 0, & \text{otherwise,} \end{cases}
$$

by [2, Proposition 2.4] and replacing q by q^m in the proof. We find

$$
(q^{mn} - 1, 2^\infty) = (q^m - 1, 2^\infty)(n, 2^\infty) \cdot \begin{cases} 2^{v_2(q^m+1)-1} & \text{if } 2 \mid n; \\ 1, & \text{otherwise.} \end{cases}
$$

The result follows by applying the formulas we obtained to (3) and noting that if $\mathcal{P}$ is false, then $v_2(q^m + 1) = 1$. $\qquad\square$

Lemma 7. *Let $q \geq 1$ be an integer prime to d and $f = \mathrm{ord}_d(q)$. Then, for all $v \mid d^\infty$, we have*

$$\mathrm{ord}_{dv}(q) = fdv \cdot \begin{cases} \dfrac{2}{(q^{2f} - 1, dv)}, & \text{if } [\mathcal{P}] = 1 \text{ and } 2 \mid v; \\ \dfrac{1}{(q^f - 1, dv)}, & \text{otherwise.} \end{cases}$$

Proof. We first assume $v_2(d) \neq 1$ and put $n = dv/(q^f - 1, dv)$. By Lemma 6, we have

$$(q^{fn} - 1, d^\infty) = (q^f - 1, d^\infty)(n, d^\infty) = (q^f - 1, d^\infty) \cdot \frac{dv}{(q^f - 1, dv)},$$

which is a number divisible by dv. If we let $t = \mathrm{ord}_{dv}(q)/f$, then $n = tm$ for some $m \geq 1$, and

$$dv \mid (q^{ft} - 1, d^\infty) = (q^f - 1, d^\infty) \cdot \frac{dv}{(q^f - 1, dv)(m, d^\infty)}.$$

We find that (m, d^∞) divides $(q^f - 1, d^\infty)/(q^f - 1, dv)$. But

$$v_l\left(\frac{(q^f - 1, d^\infty)}{(q^f - 1, dv)}\right) = v_l\left(\frac{q^f - 1}{(q^f - 1, dv)}\right),$$

for all $l \mid d$. Hence, the coprimality of n and $(q^f - 1)/(q^f - 1, dv)$ implies that (m, d^∞) must be equal to 1 because $(m, d^\infty) \mid n$. The smallest $m \geq 1$ satisfying this condition is $m = 1$, thus $n = t$. Next, assume that $2 \| d$ and note that for any odd integer $n \geq 1$, we have $\mathrm{ord}_{2n}(q) = \mathrm{ord}_n(q)$. Therefore, when $2 \nmid v$, we have

$$\mathrm{ord}_{dv}(q) = \mathrm{ord}_{dv/2}(q) = \frac{fdv}{2(q^f - 1, dv/2)} = \frac{fdv}{(q^f - 1, dv)},$$

by what we proved in the above. When $2 \mid v$, put $D = 2d$ and $u = v/2 \mid D^\infty$ so that

$$\mathrm{ord}_{dv}(q) = \mathrm{ord}_{Du}(q) = \frac{\mathrm{ord}_D(q)dv}{(q^{\mathrm{ord}_D(q)} - 1, dv)},$$

by the above again. Since $2^2 \| D$, we have

$$\mathrm{ord}_D(q) = [\mathrm{ord}_4(q), \mathrm{ord}_{d/2}(q)] = [\mathrm{ord}_4(q), f]$$

and we conclude using that $\mathrm{ord}_4(q)$ equals 1 or 2, whether $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$ respectively. $\qquad\square$

Remark 1. *As a consequence of Lemma 7, we see that the numbers $f_{u,v}$ are of the form $f_{u,v} = fk$, where $k \mid d^\infty$. Indeed, we know that $f_{u,v} = \mathrm{ord}_{dv}(q)k_0$ for some $k_0 \mid d^\infty$ from (2). It then suffices to use Lemma 7 on the $\mathrm{ord}_{dv}(q)$ factor. This will come in handy in following sections.*

Lemma 8. *Let $N \geq 1$ be such that $f_{1,v} \mid N$. The function $u \mapsto [f_{u,v} \mid N]$ is multiplicative for all $v \mid d^\infty$.*

Proof. Let $u_1, u_2 \mid d$ be coprime. We want to show that

$$[f_{u_1 u_2, v} \mid N] = [f_{u_1, v} \mid N] \cdot [f_{u_2, v} \mid N],$$

or equivalently, $f_{u_1 u_2, v} = [f_{u_1, v}, f_{u_2, v}]$. Let $r = \operatorname{ord}_{dv}(q)$ and $m = \operatorname{ord}_{\mathbb{F}_q^\times}(\lambda)$. We see that

$$\operatorname{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\lambda) = \frac{q^r - 1}{\operatorname{ord}_{\mathbb{F}_q(\zeta_{dv})^\times}(\lambda)} = \frac{q^r - 1}{m},$$

since $\lambda \in \mathbb{F}_q^\times$. Moreover, we note that

$$(uv, h) = (v, h) \left(\frac{uv}{(v,h)}, \frac{h}{(v,h)} \right) = (u, v) \left(u, \frac{h}{(v,h)} \right),$$

for all $u \mid d$. From the above and Lemmas 2 and 3, we obtain

$$f_{u,v} = \frac{r(uv, h)}{\left(\frac{q^r - 1}{m}, uv, h \right)} = \frac{r(v, h)}{(v, H_r)} \cdot \frac{\left(u, \frac{h}{(v,h)} \right)}{\left(u, \frac{H_r}{(v, H_r)} \right)}, \tag{4}$$

for all $u \mid d$, where $H_r = (h, (q^r - 1)/m)$. Now, we find

$$[f_{u_1, v}, f_{u_2, v}] = \frac{r(v, h)}{(v, H_r)} \cdot \left[\frac{\left(u_1, \frac{h}{(v,h)} \right)}{\left(u_1, \frac{H_r}{(v, H_r)} \right)}, \frac{\left(u_2, \frac{h}{(v,h)} \right)}{\left(u_2, \frac{H_r}{(v, H_r)} \right)} \right].$$

Since $(u_1, u_2) = 1$, the lcm is just the product of the two numbers. Moreover, recall that $u \mapsto (u, k)$ is a multiplicative function for all fixed integers k. Therefore, using (4), we have

$$[f_{u_1, v}, f_{u_2, v}] = \frac{r(v, h)}{(v, H_r)} \cdot \frac{\left(u_1 u_2, \frac{h}{(v,h)} \right)}{\left(u_1 u_2, \frac{H_r}{(v, H_r)} \right)} = f_{u_1 u_2, v},$$

and the result follows. $\qquad\square$

7. The main theorems

In this section, we prove that the set $R_q(a, d)$ does not have d_1-density, and thus no d_2-density by equivalence. However, we show that the d_3-density exists and we find a formula for it. From now on, we denote by $\bar{f}$ the order of q modulo $d(h, d^\infty)$.

Theorem 8. *The set $R_q(a, d)$ has no d_1-density, nor d_2-density.*

Proof. It suffices to show that the limit, as N tends to infinity, of

$$\frac{R_q(a, d, N)N}{q^N} \tag{5}$$

does not exist. We proceed to show that (5) converges to different limits for distinct subsequences of integers. First, let $(x_n)_{n \geq 1}$ be an increasing sequence of integers N not divisible by f. By the discussion at the beginning of Section 5, we have $R_q(a, d, x_n) = 0$ for all $n \geq 0$, which converges to 0. Let $(y_n)_{n \geq 0}$ be the sequence defined by $y_n = \bar{f}(h, d^\infty)(dn + 1)$ for all integers $n \geq 0$. By Theorem 7, we have

$$\left| \frac{R_q(a, d, y_n)y_n}{q^{y_n}} - \delta_q(a, d, y_n) \right| \leq 2^{\omega(d)+1} c_1 \tau(e_{y_n}) q^{-y_n/2}, \tag{6}$$

and by Lemma 6, we have

$$e_{y_n} = \left(\frac{q^{y_n} - 1}{d}, d^\infty\right) = \left(\frac{q^{\bar{f}} - 1}{d}, d^\infty\right)(h, d^\infty)\nu,$$

for some $\nu \mid 2^\infty$. We see that e_{y_n} is a constant, say E, that does not depend on n. In particular, $\tau(e_{y_n})$ is also a constant and we see that the right hand side of (6) converges to 0 as $n \to +\infty$. Hence the limit of (5), where we substituted N for y_n, is the limit of $\delta_q(a, d, y_n)$. By Theorems 6 and 7,

$$\delta_q(a, d, y_n) = \sum_{v|e_{y_n}} \sum_{u|d} \frac{\mu(u)(uv, h)}{uv} \cdot [f_{u,v} \mid y_n]$$

$$= \sum_{v|E} \sum_{u|d} \frac{\mu(u)(uv, h)}{uv} \cdot [f_{u,v} \mid \bar{f}(h, d^\infty)],$$

where we used that $e_{y_n} = E$ and that $f_{u,v} \mid y_n$ if and only if $f_{u,v} \mid \bar{f}(h, d^\infty)$. The latter follows from Remark 1. It follows that $\delta_q(a, d, y_n)$ is a constant that does not depend on n, say δ. It suffices to show that $\delta \neq 0$ to complete the proof. Since $\mathbb{F}_{dv,v}$ is a subfield of $\mathbb{F}_{dv,uv}$, we find that $f_v := f_{1,v}$ divides $f_{u,v}$ for all $u \mid d$. We may write

$$\delta = \sum_{\substack{v|E \\ f_v|\bar{f}(h,d^\infty)}} \sum_{u|d} \frac{\mu(u)(uv, h)}{uv} \cdot [f_{u,v} \mid \bar{f}(h, d^\infty)].$$

For all $v \mid E$ such that $f_v \mid \bar{f}(h, d^\infty)$, the function

$$u \mapsto \frac{\mu(u)(uv, h)}{u(v, h)} \cdot [f_{u,v} \mid \bar{f}(h, d^\infty)]$$

is multiplicative by Lemma 8. Therefore, we have

$$\delta = \sum_{\substack{v|E \\ f_v|\bar{f}(h,d^\infty)}} \frac{(v, h)}{v} \sum_{u|d} \frac{\mu(u)(uv, h)}{u(v, h)} \cdot [f_{u,v} \mid \bar{f}(h, d^\infty)]$$

$$= \sum_{\substack{v|E \\ f_v|\bar{f}(h,d^\infty)}} \frac{(v, h)}{v} \prod_{l|d} \left(1 - \frac{(lv, h)}{l(v, h)} \cdot [f_{l,v} \mid \bar{f}(h, d^\infty)]\right),$$

where we used the Euler product formula. We see that δ is non-negative as each general term is. Hence it suffices to show that there is one non-zero term. We claim that the term in $v = (h, d^\infty)$ is positive. First, let us show that we have $f_v \mid \bar{f}(h, d^\infty)$. Note that $(v, h) = v$, so that

$$f_{(h,d^\infty)} = \frac{\operatorname{ord}_{dv}(q)(v, h)}{(\operatorname{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\lambda), v, h)} = \frac{\bar{f}(h, d^\infty)}{(\operatorname{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\lambda), h, d^\infty)}.$$

We find that $f_{(h,d^\infty)} \mid \bar{f}(h, d^\infty)$ and the term in $v = (h, d^\infty)$ appears in the sum. Using again that $(v, h) = v$, and also that $(lv, h) = v$, we find the general term to be

$$\frac{(h, d^\infty)}{v} \prod_{l|d} \left(1 - \frac{[f_{l,v} \mid \bar{f}(h, d^\infty)]}{l}\right),$$

which is non-zero, whether $f_{l,v} \mid \bar{f}(h, d^\infty)$ or not. We obtain that

$$\frac{R_q(a, d, x_n)x_n}{q^{x_n}} \quad \text{and} \quad \frac{R_q(a, d, y_n)y_n}{q^{y_n}}$$

converge to 0 and $\delta > 0$ respectively. Hence the limit of (5) as $N \to +\infty$ does not exist. The set $R_q(a, d)$ has no d_1-density, and thus no d_2-density by [4, Proposition 1.8]. $\square$

The proof of the existence and the computation of the d_3-density of $R_q(a, d)$ requires to partition $\mathbb{N}$ into a countable union of distinct arithmetic progressions, following a method of Ballot [3]. We have

$$\mathbb{N} = \bigsqcup_{j=1}^{f-1} S_j \sqcup \bigsqcup_{w \mid d^\infty} \bigsqcup_{\substack{\alpha=1 \\ (\alpha,d)=1}}^{d} A_{w,\alpha}, \tag{7}$$

where $S_j = \{fn + j : n \geq 0\}$ and $A_{w,\alpha} = \{fw(\alpha + dn) : n \geq 0\}$. Note that for $N \in S_j$, we have $\delta_q(a, d, N) = 0$ by the discussion at the beginning of Section 5. For $N = fw(dn + \alpha) \in A_{w,\alpha}$, we have

$$e_N = \left(\frac{q^{fw} - 1}{d}, d^\infty \right) = e_{fw},$$

by Lemma 6. Hence e_N is a constant that only depends on w. Moreover, we have $f_{u,v} \mid N$ if and only if $f_{u,v} \mid fw$, by Remark 1. We obtain

$$\delta_q(a, d, N) = \sum_{v \mid e_N} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{uv} \cdot [f_{u,v} \mid N]$$

$$= \sum_{v \mid e_{fw}} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{uv} \cdot [f_{u,v} \mid fw], \tag{8}$$

which is a constant that does not depend on n, nor α. We denote this quantity by δ_w. Moreover, we denote by $\delta_q(a, d)$ the sum

$$\delta_q(a, d) = \frac{\varphi(d)}{df} \sum_{w \mid d^\infty} \frac{\delta_w}{w}.$$

We show that $\delta_q(a, d)$ is the d_3-density of the set $R_q(a, d)$. The following lemma is an already known result that we found in various papers [10, 14] without a proof or a reference to a proof. Since it is not a long nor difficult result to prove, we find it preferable to give a proof.

Lemma 9. *There exists an absolute and effective constant $c_2 > 0$ such that*

$$M_d(x) := \#\{w \leq x : w \mid d^\infty\} \leq c_2 \log(x)^{\omega(d)},$$

for all $x \geq 2$.

Proof. If l is a prime divisor of d, then $l^k \leq x$ if and only if $k \leq \log_l x$. Thus,

$$M_d(x) = \sum_{\substack{w \mid d^\infty \\ w \leq x}} 1 \leq \prod_{l \mid d} (\log_l(x) + 1).$$

Note that if $x \geq e^2$, then for all primes $l \geq e^2$ we have $\log_l(x) + 1 \leq \log(x)$. Therefore, for only finitely many primes l we have $\log_l(x) + 1 \leq C_l \log(x)$ for all

$x \geq 2$, for some absolute constant $C_l > 0$. The result follows by choosing c_2 as the product of the C_l's for all primes $l \leq e^2$. $\qquad\square$

The next result can be found in a paper of Sanna [14]. However, the bound given is in $\log(x)^{\omega(d)+1}/x$ for all $x \geq e^{\omega(d)}$. With a slight change in the proof, we find a bound in $\log(x)^{\omega(d)}/x$ for all $x \geq e^{2\omega(d)}$.

Lemma 10. *For every $x \geq e^{2\omega(d)}$, we have*

$$\sum_{\substack{w|d^\infty \\ w>x}} \frac{1}{w} \leq 3c_2 \cdot \frac{\log(x)^{\omega(d)}}{x},$$

where $c_2 > 0$ is the absolute constant defined in Lemma 9.

Proof. Since $d \geq 2$, we have $x \geq e^{2\omega(d)} \geq 2$ and $M_d(t) \leq c_2 \log(t)^{\omega(d)}$ for every $t \geq x$, by Lemma 9. From this inequality and by Abel's summation formula, we have

$$\sum_{\substack{w|d^\infty \\ w>x}} \frac{1}{w} = \frac{M_d(x)}{x} + \int_x^{+\infty} \frac{M_d(t)}{t^2}dt \leq c_2\left(\frac{\log(x)^{\omega(d)}}{x} + \int_x^{+\infty} \frac{\log(t)^{\omega(d)}}{t^2}dt\right).$$

Let $g : [e^{2\omega(d)}, +\infty) \to \mathbb{R}$ be the function defined by

$$g(x) = \int_x^{+\infty} \frac{\log(t)^{\omega(d)}}{t^2}dt - \frac{2\log(x)^{\omega(d)}}{x},$$

By the Fundamental Theorem of Calculus, we obtain the derivative

$$g'(x) = -\frac{\log(x)^{\omega(d)}}{x^2} - 2 \cdot \frac{\omega(d)\log(x)^{\omega(d)-1} - \log(x)^{\omega(d)}}{x^2}$$
$$= \frac{\log(x)^{\omega(d)}}{x^2} - \frac{2\omega(d)\log(x)^{\omega(d)-1}}{x^2}.$$

It follows from $x \geq e^{2\omega(d)}$ that g' is non-negative, thus g is an increasing function. Moreover, f converges to 0 as x tends to infinity. Hence $g(x) \leq 0$ for every $x \in [e^{2\omega(d)}, +\infty)$, and the result follows. $\qquad\square$

Lemma 11. *For every $N \geq e^{2\omega(d)}$, we have*

$$\left|\frac{1}{N}\sum_{n=1}^N \delta_q(a,d,n) - \delta_q(a,d)\right| \leq \varphi(d)\left(1 + \frac{3c_2}{fd}\right)\frac{\log(N)^{\omega(d)}}{N},$$

where c_2 is the constant defined in Lemma 9.

Proof. From the partition of $\mathbb{N}$ given in (7), we have

$$S_N := \frac{1}{N}\sum_{n=1}^N \delta_q(a,d,n) = \frac{1}{N}\sum_{w|d^\infty}\sum_{\substack{\alpha=1 \\ (\alpha,d)=1}}^d \sum_{n \in A_{w,\alpha}(N)} \delta_w,$$

where $A_{w,\alpha}(N) = A_{w,\alpha} \cap [\![1,N]\!]$, and using that $\delta_q(a,d,n) = 0$ if $n \in S_j$, and that $\delta_q(a,d,n) = \delta_w$ if $n \in A_{w,\alpha}$. Note that w is be bounded above by N and

$$\#A_w(N) = \#\{1 \leq fw(\alpha+dn) \leq N : n \geq 0\} = \left\lfloor \frac{N + fw(d-\alpha)}{fdw} \right\rfloor,$$

thus, we obtain

$$S_N = \frac{1}{N} \sum_{\substack{w|d^\infty \\ w \leq N}} \sum_{\substack{\alpha=1 \\ (\alpha,d)=1}}^{d} \left\lfloor \frac{N + fw(d-\alpha)}{fdw} \right\rfloor \delta_w.$$

By the properties of the floor function, we have

$$\frac{N}{fdw} - 1 \leq \#A_{w,\alpha}(N) \leq \frac{N}{fdw} + 1.$$

Therefore, on the one hand, we have

$$S_N \geq \frac{\varphi(d)}{fd} \sum_{\substack{w|d^\infty \\ w \leq N}} \frac{\delta_w}{w} - \frac{\varphi(d)}{N} \sum_{\substack{w|d^\infty \\ w \leq N}} \delta_w$$

$$= \delta_q(a,d) - \frac{\varphi(d)}{N} \sum_{\substack{w|d^\infty \\ w \leq N}} \delta_w - \frac{\varphi(d)}{fd} \sum_{\substack{w|d^\infty \\ w > N}} \frac{\delta_w}{w}.$$

and on the other hand,

$$S_N \leq \frac{\varphi(d)}{fd} \sum_{\substack{w|d^\infty \\ w \leq N}} \frac{\delta_w}{dw} + \frac{\varphi(d)}{N} \sum_{\substack{w|d^\infty \\ w \leq N}} \delta_w$$

$$= \delta_q(a,d) + \frac{\varphi(d)}{N} \sum_{\substack{w|d^\infty \\ w \leq N}} \delta_w - \frac{\varphi(d)}{fd} \sum_{\substack{w|d^\infty \\ w > N}} \frac{\delta_w}{w}$$

$$\leq \delta_q(a,d) + \frac{\varphi(d)}{N} \sum_{\substack{w|d^\infty \\ w \leq N}} \delta_w + \frac{\varphi(d)}{fd} \sum_{\substack{w|d^\infty \\ w > N}} \frac{\delta_w}{w}.$$

We obtain

$$|S_N - \delta_q(a,d)| \leq \frac{\varphi(d)}{N} \sum_{\substack{w|d^\infty \\ w \leq N}} \delta_w + \frac{\varphi(d)}{fd} \sum_{\substack{w|d^\infty \\ w > N}} \frac{\delta_w}{w}.$$

By Lemma 9 and since $\delta_w \leq 1$, we find

$$\frac{\varphi(d)}{N} \sum_{\substack{w|d^\infty \\ w \leq N}} \delta_w \leq c_2 \varphi(d) \cdot \frac{\log{(N)}^{\omega(d)}}{N},$$

for all $N \geq 2$, where c_2 is the constant defined in the lemma. By Lemma 10, we have

$$\frac{\varphi(d)}{fd} \sum_{\substack{w|d^\infty \\ w > N}} \frac{\delta_w}{w} \leq \frac{3c_2 \varphi(d)}{fd} \cdot \frac{\log{(N)}^{\omega(d)}}{N},$$

for all $N \geq e^{2\omega(d)}$. $\qquad\qquad\square$

Theorem 9. *There exists an absolute constant $c_2 > 0$ such that*

$$\left| \frac{1}{N} \sum_{n=1}^{N} \frac{R_q(a,d,n)}{q^n/n} - \delta_q(a,d) \right| \leq \varphi(d) \left(1 + \frac{3c_2}{fd} \right) \frac{\log{(N)}^{\omega(d)}}{N} + \frac{c_3}{N},$$

for all $N \geq e^{2\omega(d)}$, *with* $c_3 = 2^{\omega(d)+1} c_1 \tau(e_f) v_2(q^f + 1) \cdot q^{-f/2}(q^{-f/2} - 1)^{-2}$ *and where* c_1 *is defined in Lemma 5. In particular,* $R_q(a, d)$ *has* d_3*-density equal to* $\delta_q(a, d)$.

Proof. First, we put

$$R_N = \frac{1}{N} \sum_{n=1}^{N} \frac{R_q(a, d, n)}{q^n / n} \quad \text{and} \quad S_N = \frac{1}{N} \sum_{n=1}^{N} \delta_q(a, d, n).$$

We have

$$
\begin{aligned}
|R_N - \delta_q(a, d)| &= |R_N - S_N + S_N - \delta_q(a, d)| \\
&\leq |R_N - S_N| + |S_N - \delta_q(a, d)| \\
&\leq |R_N - S_N| + \varphi(d)\left(1 + \frac{3c_2}{fd}\right) \frac{\log(N)^{\omega(d)}}{N},
\end{aligned}
$$

for all $N \geq e^{2\omega(d)}$, by Lemma 11. Let us now bound the term $|R_N - S_N|$. Using Lemma 7, and since $R_q(a, d, n) = \delta_q(a, d, n) = 0$ if $f \nmid n$, we have

$$|R_N - S_N| \leq \frac{1}{N} \sum_{\substack{n=1 \\ f|n}}^{N} \left| \frac{R_q(a, d, n)}{q^n / n} - \delta_q(a, d, n) \right| \leq \frac{2^{\omega(d)+1} c_1}{N} \sum_{\substack{n=1 \\ f|n}}^{N} \tau(e_n) q^{-n/2}.$$

By Lemma 6, we know that

$$e_n \leq 2^{v_2(q^f+1)-1}\left(\frac{q^f - 1}{d}, d^\infty\right)(n/f, d^\infty) \leq \frac{2^{v_2(q^f+1)} e_f n}{f}.$$

Hence $\tau(e_n) \leq v_2(q^f + 1)\tau(e_f)n/f$. We find

$$|R_N - S_N| \leq \frac{2^{\omega(d)+1} v_2(q^f + 1) c_1 \tau(e_f)}{Nf} \sum_{\substack{n=1 \\ f|n}}^{N} n q^{-n/2} := \frac{c}{Nf} \sum_{\substack{n=1 \\ f|n}}^{N} n q^{-n/2}.$$

Now, using the well-known equality

$$\sum_{n=1}^{+\infty} n x^n = \frac{x}{(x - 1)^2},$$

valid for $|x| < 1$, we obtain

$$|R_N - S_N| \leq \frac{c}{Nf} \sum_{\substack{n=1 \\ f|n}}^{+\infty} n q^{-n/2} = \frac{c}{Nf} \sum_{m=0}^{+\infty} fm q^{-fm/2} = \frac{c}{N} \frac{q^{-f/2}}{(q^{-f/2} - 1)^2} = \frac{c_3}{N}.$$

This completes the proof of the bound. Letting N tend to infinity shows that the set $R_q(a, d)$ has d_3-density equal to $\delta_q(a, d)$. $\qquad\square$

Corollary 2. *The set* $R_q(a, d)$ *has* d_4 *and Dirichlet density equal to* $\delta_q(a, d)$.

Proof. Theorem 9 establishes the existence and the value of the d_3-density of $R_q(a, d)$. The result follows from [4, Theorem A]. $\qquad\square$

8. Closed-form for the d_3-density

We proved in Section 7 that $\delta_q(a, d)$ is the d_3-density of $R_q(a, d)$. However, this constant is defined via a series, meaning that there are infinitely many operations to carry out in order to compute it. We show in this section, under the assumption $f_{u,v} = \operatorname{ord}_{dv}(q)$ for all $u \mid d$ and $v \mid d^\infty$, that $\delta_q(a, d)$ can be written in a closed-form formula, that is, a formula that requires only finitely many simple operations.

We define a function $\eta : \mathbb{N}^2 \longrightarrow \mathbb{N}$ by $\eta(m, n) = 1$ if $2 \nmid (n, d)$ and by $\eta(m, n) = 2^{v_2(q^{\bar{f}}+1)-1}$ otherwise. Note that $m \mapsto \eta(m, \cdot)$ is a multiplicative function. Indeed, if $m_1, m_2 \geq 1$ are coprime integers, then

$$\eta(m_1 m_2, n) = \begin{cases} 2^{v_2(q^{\bar{f}}+1)-1}, & \text{if } 2 \mid (m_1 m_2, n); \\ 1, & \text{otherwise.} \end{cases}$$

If $2 \mid (m_1 m_2, n)$, then only one of m_1 and m_2 is even, say m_1. Hence we have $\eta(m_1 m_2, n) = 2^{v_2(q^{\bar{f}}+1)-1} = \eta(m_1, n)\eta(m_2, n)$. For the case $2 \nmid (m_1 m_2, n)$, the function η is always equal to 1, so the multiplicativity trivially holds.

Proposition 2. *Assume that $f_{u,v} = \operatorname{ord}_{dv}(q)$ for all $u \mid d$ and $v \mid d^\infty$. For each $w \mid d^\infty$, we have*

$$\delta_w = \begin{cases} \displaystyle\sum_{u \mid d} \frac{\mu(u)(dh, u^\infty)}{u(q^{\bar{f}} - 1, u^\infty)(\nu, u^\infty)\eta(\nu, u)}, & \text{if } fw = \bar{f}\nu, \ \nu \mid d^\infty; \\ 0, & \text{otherwise.} \end{cases}$$

If $fw = \bar{f}\nu$, we may denote δ_w by $\delta(\nu)$ when it is written in the above form to make the dependence in ν more obvious.

Proof. Since $f_{u,v} = \operatorname{ord}_{dv}(q)$, and $v \mid e_{fw}$ if and only if $\operatorname{ord}_{dv}(q) \mid fw$, we find from (8) that δ_w becomes

$$\delta_w = \sum_{v \mid fw} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{uv}.$$

Using that the map

$$u \mapsto \frac{\mu(u)(uv, h)}{u(v, h)}$$

defines a multiplicative function, we use the Euler product formula to obtain

$$\delta_w = \sum_{v \mid e_{fw}} \frac{(v, h)}{v} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{u(v, h)} = \sum_{v \mid e_{fw}} \frac{(v, h)}{v} \prod_{l \mid d} \left(1 - \frac{(lv, h)}{l(v, h)}\right).$$

For all $l \mid d$, we have $(lv, h) = l(v, h)$ if and only if $v_l(v) < v_l(h)$. Hence δ_w is non-zero if and only if $(h, d^\infty) \mid e_{fw}$, or equivalently, $\bar{f} \mid fw$. Assume that $fw = \bar{f}\nu$ for some $\nu \mid d^\infty$. We have

$$\delta_w = \sum_{\substack{v \mid e_{fw} \\ (h, d^\infty) \mid v}} \frac{(v, h)}{v} \prod_{l \mid d} \left(1 - \frac{1}{l}\right) = \frac{\varphi(d)}{d} \sum_{\substack{v \mid e_{fw} \\ (h, d^\infty) \mid v}} \frac{(v, h)}{v}.$$

Since $v \mapsto (v, h)/v$ is multiplicative, we again use the Euler product formula on the sum and find

$$\sum_{\substack{v \mid e_{fw} \\ (h, d^\infty) \mid v}} \frac{(v, h)}{v} = \prod_{l \mid d} \sum_{r = v_l(h)}^{v_l(e_{\bar{f}\nu})} \frac{l^{v_l(h)}}{l^r}$$

$$= \prod_{l \mid d} \left(\frac{1 - l^{v_l(h) - v_l(e_{\bar{f}\nu}) - 1}}{1 - l^{-1}} \right)$$

$$= \frac{d}{\varphi(d)} \prod_{l \mid d} \left(1 - \frac{l^{v_l(dh)}}{l^{v_l(q^{\bar{f}\nu} - 1) + 1}} \right).$$

We obtain

$$\delta(\nu) = \prod_{l \mid d} \left(1 - \frac{l^{v_l(dh)}}{l^{v_l(q^{\bar{f}\nu} - 1) + 1}} \right),$$

where $\bar{f}\nu = fw$. Let g be the function defined by

$$g : u \mapsto \frac{\mu(u)(dh, u^\infty)}{u(q^{\bar{f}\nu} - 1, u^\infty)},$$

for all $u \geq 1$. Then, g is multiplicative and by the Euler product formula, we have

$$\sum_{u \mid d} \frac{\mu(u)(dh, u^\infty)}{u(q^{\bar{f}\nu} - 1, u^\infty)} = \prod_{l \mid d} \left(1 - \frac{l^{v_l(dh)}}{l^{v_l(q^{\bar{f}\nu} - 1) + 1}} \right) = \delta(\nu).$$

We now apply Lemma 6 to $(q^{\bar{f}\nu} - 1, u^\infty)$ in the denominator of the general term of the sum, which is allowed since $u \mid q^{\bar{f}} - 1$. The result follows. $\qquad \square$

Theorem 10. *Put $C = 3 \cdot 4^{-1} + 2^{-v_2(q^{\bar{f}} + 1)}$. Assume that $f_{u,v} = \operatorname{ord}_{dv}(q)$ for all $u \mid d$ and $v \mid d^\infty$. Then, we have*

$$\delta_q(a, d) = \frac{1}{\bar{f}} \prod_{l \mid d} \left(1 - \frac{l^{v_l(dh)} C^{[l=2]}}{(l+1) l^{v_l(q^{\bar{f}} - 1)}} \right).$$

Proof. By Proposition 2, we may only consider the indices $w \mid d^\infty$ that satisfy $fw = \bar{f}\nu$ for some $\nu \mid d^\infty$ in the expression of $\delta_q(a, d)$. We obtain

$$\delta_q(a, d) = \frac{\varphi(d)}{d} \sum_{w \mid d^\infty} \frac{\delta_w}{fw} = \frac{\varphi(d)}{d} \sum_{\nu \mid d^\infty} \frac{\delta(\nu)}{\bar{f}\nu}.$$

Using that $(dh, u^\infty) \leq (q^{\bar{f}} - 1, u^\infty)$, because $\bar{f} = \operatorname{ord}_{d(h, d^\infty)}(q)$, the inequality

$$\sum_{\nu \mid d^\infty} \sum_{u \mid d} \left| \frac{\mu(u)(dh, u^\infty)}{u\nu(\nu, u^\infty)(q^{\bar{f}} - 1, u^\infty)\eta(\nu, u)} \right| \leq \sum_{\nu \mid d^\infty} \sum_{u \mid d} \frac{1}{\nu} = \frac{\tau(d)\varphi(d)}{d}$$

shows that we have absolute converge of the series. Hence we can interchange the sum symbol in $\delta(\nu)$ and the series. We have

$$\delta_q(a, d) = \frac{\varphi(d)}{d} \sum_{u \mid d} \frac{\mu(u)(dh, u^\infty)}{u(q^{\bar{f}} - 1, u^\infty)} \sum_{\nu \mid d^\infty} \frac{1}{\nu(\nu, u^\infty)\eta(\nu, u)}.$$

Let $S(u)$ be the inner series. For all $u \in \mathbb{N}$, the function $\nu \mapsto \nu(\nu, u^\infty)\eta(\nu, u)$ is multiplicative. Moreover, we have $\eta(\nu, u) = \eta(\mathrm{rad}(\nu), u)$, where rad is the radical of an integer function. Therefore

$$S(u) = \sum_{\nu \mid d^\infty} \frac{1}{\nu(\nu, u^\infty)\eta(\nu, u)} = \prod_{l \mid d} \sum_{r=0}^{+\infty} \frac{1}{l^{r(1+[l\mid u])}\eta(l^r, u)}$$

$$= \prod_{l \mid d} \left(1 + \sum_{r=1}^{+\infty} \frac{1}{l^{r(1+[l\mid u])}\eta(l, u)} \right)$$

$$= \prod_{l \mid d} \left(1 + \frac{1}{\eta(l, u)(l^{1+[l\mid u]} - 1)} \right).$$

Since $\eta(l, u) = 1$ when $l \neq 2$ or $l \nmid u$, we have

$$S(u) = \prod_{\substack{l \mid d \\ l \nmid u}} \left(1 + \frac{1}{l - 1} \right) \prod_{l \mid u} \left(1 + \frac{2^{-[l=2](v_2(q^{\bar{f}}-1)-1)}}{l^2 - 1} \right).$$

Let us first look at the case $2 \nmid u$. We have

$$S(u) = \prod_{\substack{l \mid d \\ l \nmid u}} \left(\frac{l}{l - 1} \right) \prod_{l \mid u} \left(\frac{l^2}{l^2 - 1} \right) = \prod_{l \mid d} \left(\frac{l}{l - 1} \right) \prod_{l \mid u} \left(\frac{l}{l + 1} \right) = \frac{du}{\varphi(d)\psi(u)}.$$

If $2 \mid u$, then, writing $u = 2u'$, we find

$$S(u) = \prod_{\substack{l \mid d \\ l \nmid u}} \left(\frac{l}{l - 1} \right) \prod_{l \mid u'} \left(\frac{l^2}{l^2 - 1} \right) \cdot \left(1 + \frac{1}{2^{v_2(q^{\bar{f}}-1)-1}} \right)$$

$$= \prod_{\substack{l \mid d \\ l \nmid u}} \left(\frac{l}{l - 1} \right) \prod_{l \mid u} \left(\frac{l^2}{l^2 - 1} \right) \cdot \frac{3}{4} \left(1 + \frac{1}{2^{v_2(q^{\bar{f}}-1)-1}} \right)$$

$$= \frac{duC}{\varphi(d)\psi(u)}.$$

Therefore, going back to $\delta_q(a, d)$, we obtain

$$\delta_q(a, d) = \frac{1}{\bar{f}} \sum_{u \mid d} \frac{\mu(u)(dh, u^\infty)C^{[2\mid u]}}{(q^{\bar{f}} - 1, u^\infty)\psi(u)}.$$

The general term of the sum defines a multiplicative function in the variable u, thus the result follows from the Euler product formula. $\qquad\square$

Remark 2. *Note that Theorem 10 coincides with* [2, Theorem 3.3] *and* [3, Theorem 11] *that Ballot proved in the case $a = T$ and, respectively, $d = 2$ and d an odd prime.*

In conclusion, we proved that the set $R_q(a, d)$ has d_3-density $\delta_q(a, d)$ in Section 7 and we were able to write $\delta_q(a, d)$ in a closed-form in Section 8. However, the latter was done under the assumption that the degree of the field $\mathbb{F}_{dv,uv}$ over $\mathbb{F}_q$ is equal to $\mathrm{ord}_{dv}(q)$ for all $v \mid d^\infty$ and $u \mid d$. We conclude this paper with a lemma that gives sufficient conditions for this equality to hold.

Proposition 3. *If either $(d, h) = 1$ or $(d, m) = 1$, then*

$$[\mathbb{F}_{dv,uv} : \mathbb{F}_q] = \mathrm{ord}_{dv}(q),$$

for all $v \mid d^\infty$ and $u \mid d$.

Proof. By Lemma 2, we have that

$$[\mathbb{F}_{dv,uv} : \mathbb{F}_q] = \frac{\mathrm{ord}_{dv}(q)(uv, h)}{(\mathrm{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\lambda), uv, h)}.$$

If $(d, h) = 1$, then $(uv, h) = 1$ and the result follows. If $(d, m) = 1$, we use that the order of λ in $\mathbb{F}_q(\zeta_{dv})^\times$ is still equal to m, the order of λ in $\mathbb{F}_q^\times$. Hence

$$\mathrm{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\lambda) = \frac{q^{\mathrm{ord}_{dv}(q)} - 1}{m}. \tag{9}$$

We see in (9) that uv divides $\mathrm{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\lambda)$. Indeed, this is because $uv \mid dv$ and $(uv, m) = 1$ imply that $uvm \mid q^{\mathrm{ord}_{dv}(q)} - 1$. $\qquad\square$

However, our result is not enough to cover all cases. For instance, it does not give any information about the density when $(d, h, m) > 1$.

References

[1] C. Ballot, Density of prime divisors of linear recurrences, *Mem. Amer. Math. Soc.*, **115** (1995).

[2] C. Ballot, Counting monic irreducible polynomials P in $\mathbb{F}_q[X]$ for which order of $X \pmod P$ is odd, J. Theor. Nombres Bordeaux, **19** (2007), no. 1, 41–58.

[3] C. Ballot, An elementary method to compute prime densities in $\mathbb{F}_q[X]$, Combinatorial number theory, 71–80, de Greyter, Berlin, 2007.

[4] C. Ballot, Competing prime asymptotic densities in $\mathbb{F}_q[X]$: A discussion, Enseign. Math. (2), **54**, (2008).

[5] M. D. Fried and M. Jarden, *Field Arithmetic*, Ergeb. Math. Grenzgeb. (3), **11**, Springer-Verlag, HeidelBerg, 2008.

[6] H. H. Hasse, Über die Dichte der Primzhalen, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordhung mod p ist., *Math. Annalen.*, **166** (1966), 19–23.

[7] H. H. Hasse, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung mod.p ist., *Math. Annalen.*, **162** (1965), 74–76.

[8] L. Hochfilzer & E. Waxman, *On Artin's primitive root conjecture for function fields over $\mathbb{F}_q$*.

[9] S. Lang, *Algebra*, Graduate Texts in Mathematics, *211*, Springer-Verlag, 2002.

[10] P. Moree, On primes p for which d divides $\mathrm{ord}_p(g)$, Funct. Approx. Comment. Math. **33** (2005), 85–95.

[11] V. K. Murty and J. Scherk, Effective versions of the Chebotarev Density Theorem for function fields, C. R. Acard. Sci. Paris Sér. I Math. **319** (1994), no. 6, 523–528.

[12] F. Pappalardi, Square-free values of the order function, *New York J. Math.*, **9** (2003), 331–344.

[13] M. Rosen, *Number theory in function fields*, Springer Verlag (Graduate texts in mathematics; 210), (2002).

[14] C. Sanna, On the divisibility of the rank of appearance of a Lucas sequence, *Int. J. Number Theory*, **18** (2022), 2145–2156.

[15] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, 1993.

[16] K. Wiertelak, On the density of some sets of primes. IV, *Acta Arith.*, **43** (1984), 177–190.

Normandie Université, UNICAEN, CNRS, LMNO, 14000 Caen, France
Email address: joaquim.cera-daconceicao@unicaen.fr
URL: https://jceradaconceicao.github.io