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 1
2. Known results 4
3. On constant field extensions 5
4. The degree of Kummer extensions of rational function fields 6
5. The proportion-density 7
6. More preliminary results 8
7. The main theorems 10
8. Closed-form for the d_3-density 14
References 15

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 [7, 8] 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 [19] 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*

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

2020 *Mathematics Subject Classification.* 11R44, 11T06, 11N37, 11R58.

Key words and phrases. Chebotarev density theorem, Dirichlet density, Kummer extension, finite field, global function field, monic irreducible polynomial, multiplicative order.

where the implied constant depends on d and a, Li *is the logarithmic integral function, 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 [13] 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 [12], 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, $N \geq 1$. The most common densities are the d_1 and δ densities defined, when they exist, 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 concludes 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 equivalence $I_n \sim q^n/n$ 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 [13] and Moree [12], and on the elementary approach taken by Ballot [2, 3].

Furthermore, this problem is closely related to Artin's primitive root conjecture over function fields. Let $a \in K \setminus \mathbb{F}_q$ not be an l-th power for all $l \mid q-1$. The conjecture states that there exist infinitely many $P \in \mathcal{P}_+$ such that a is a primitive root modulo P, that is, a has order $NP-1$ in $(A/P)^\times$. The conjecture has been widely studied in the function field setting. It was first proven by Bilharz [5] under the generalized Riemann hypothesis for function fields, which was later proved by Weil [18]. In his proof, Bilharz shows that the set $S(a)$ of primes P that have a as a primitive root has positive Dirichlet density. Another proof was given in 1994 by Pappalardi and Shparlinski [14] by estimating the number of $P \in \mathcal{P}_+$ of degree $n \geq 1$ that satisfy the conjecture. More recently, Kim and Murty [10] managed to prove Artin's conjecture without using the generalized Riemann hypothesis for function fields. Moreover, note that $S(T)$ has positive d_3-density. It was shown by Ballot [4] through a theorem of Shparlinski [15, Theorem 3]. Using Theorem 7 with $d = q^N - 1$ for all $N \geq 1$, we see that $d_3(S(a))$ can be estimated with [15, Theorem 3], or some variation of it, in a similar way, thus showing that $S(a)$ has positive d_3-density.

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 the *proportion-density* of $R_q(a,d,N)$. (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 $n, q \geq 1$ 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.)

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

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

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 $G = (\mathbb{Z}/n\mathbb{Z})^\times$, 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 [6, Proposition 6.4.8].) 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. 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

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

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 $P \in A$ such that $v_P(a) = 0$ splits completely in $K(\zeta_n, a^{1/d})$ if and only if*

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

Proof. It suffices to follow the proof of [16, 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 we can always split it in two such extensions. In this section, we give necessary and sufficient conditions for an algebraic extension $K(a^{1/n})/K$, $a \in K^\times$, to be 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. The "if" part is trivial. 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 see that $\tilde{b}_1 \in (K^\times)^{q_i}$ for all $1 \leq i \leq s$. 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 [9, Lemma 3.3]. 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 $a = \mu b^l$ by [9, Lemma 3.3]. 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. But $\tilde{b}$ and $\tilde{x}$ are both monic polynomials in the ring of integers of L, so 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 $a = \mu(b/g)^n$. □

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 $K = \mathbb{F}_q(T)$, i.e., 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 [11, Theorem 9.1]. □

Lemma 1. *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 be the index of μ in $\mathbb{F}_q(\zeta_n)^\times$, 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 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 $4 \mid q^{\mathrm{ord}_n(q)} - 1$. A contradiction. □

Lemma 2. *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, we have $\mathbb{F}_{n,d} = \mathbb{F}_q(\zeta_n, \lambda^{1/(d,h)})$.*

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

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

is 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

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

for some $\omega, \lambda \in \mathbb{F}_q^\times$ and $c \in K^\times$, by Theorem 4. Hence $\tilde{a} = \tilde{c}^{lD}$ and, by maximality of h, we find that $lD \mid h$. A contradiction to $lD \mid d$. □

Theorem 6. *Let $a \in K^\times$. We have $[K(\zeta_n, a^{1/d}) : \mathbb{F}_{n,d}K] = d/(d,h)$.*

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 2 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. However, by Lemma 2, 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 $b \notin (\mathbb{F}_{n,d}K^\times)^l$. If $4 \mid d_0$, then the rest of the proof follows in the same way as the proof of Lemma 1. □

5. The proportion-density

Throughout this paper, we denote by $\mathcal{P}_+$ the set of monic irreducible polynomials in A, and by $R_q(a,d)$ the set of $P \in \mathcal{P}_+$ that satisfy $v_P(a) = 0$ and $d \mid \mathrm{ord}_P(a)$, where $a \in K^\times$ and $d \geq 1$ are fixed. For each $N \geq 1$, we consider the number of primes in $R_q(a,d)$ with degree N, denoted $R_q(a,d,N)$. We write $I_N = \mathcal{P}_+(N)$.

For $d = 1$, we trivially 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

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

Densities are easily computed here. We have $d_1(R_q(a,1)) = 1$ and it follows that the d_i's and the Dirichlet densities also exist and equal 1. The same goes for $R_q(a,\lambda)$ for which the densities are 1 or 0, whether $d \mid \mathrm{ord}_{\mathbb{F}_q^\times}(\lambda)$.

We assume that $d \geq 2$ and a is not a constant for the rest of this paper. Since $f := \mathrm{ord}_d(q) \nmid N$ implies that $R_q(a,d,N) = 0$, we only consider integers $N \equiv 0 \pmod f$. We put

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

Since K is fixed, 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 denote the number of primes in $\{L\}$ with degree N by $\{L\}_N$. We assume throughout the paper that $a = \lambda\tilde{a}$ and $\tilde{a} = b^h$, with the notation of the previous section.

Lemma 3. *For each positive $N \equiv 0 \pmod f$, we have*

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

Proof. We follow the proof of [12, Proposition 1]. Note in particular that the condition $p \leq x$ must be replaced by $\deg(P) = N$, and $p \equiv 1 \pmod{dv}$ by the condition $q^N \equiv 1 \pmod{dv}$. □

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 [17, Proposition 3.7.3] to $K_{n,d}$. □

Lemma 4. *There exists an absolute constant $c_1 > 0$ such that for each $N \geq 1$ such that $[\mathbb{F}_{n,d} : \mathbb{F}_q] \mid N$, we have*

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

Proof. We apply Theorem 2 to $\{K_{n,d}\}_N$. The error term is obtained using Proposition 1 and the bounds

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

valid for all $N \geq 1$. □

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,

$$f_{u,v} = \frac{\mathrm{ord}_{dv}(q)(uv, h)}{(\mathrm{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\lambda), uv, h)}, \tag{1}$$

by Lemmas 1 and 2.

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 constant defined in Lemma 4 and $\delta_q(a, d, N)$ is the proportion-density 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. We let $S_q(a, d, N) := R_q(a, d, N) - \delta_q(a, d, N) \cdot q^N/N$. By Lemmas 3 and 4, we have

$$|S_q(a, d, N)| \leq 2c_1 \cdot \frac{q^{N/2}}{N} \sum_{v \mid e_N} \sum_{u \mid d} |\mu(u)| = 2^{\omega(d)+1} c_1 \cdot \frac{\tau(e_N) q^{N/2}}{N},$$

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 5. *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. Thus, it suffices to prove the result for $(q^{mn} - 1, l^\infty)$, where $l \mid d$. By [3, Lemma 4] and [2, Proposition 2.4], and by replacing $\mathrm{ord}_l(q)$ by m and q by q^m respectively in the proofs, which is allowed since it only uses that $l \mid q^m - 1$, we obtain

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

The result follows by noting that if $\mathcal{P}$ is false, then $v_2(q^m + 1) = 1$. □

Lemma 6. *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. Assume $v_2(d) \neq 1$ and put $n = dv/(q^f - 1, dv)$. By Lemma 5, we see that $dv \mid (q^{fn} - 1, d^\infty)$. Hence $n = tm$, where $m \geq 1$ and $t := \mathrm{ord}_{dv}(q)/f$. By Lemma 5, we have

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

and we find that $m = (m, d^\infty)$ divides $(q^f - 1, d^\infty)/(q^f - 1, dv)$. But the latter is coprime to n, which yields that $m = 1$. Next, assume that $2 \parallel d$ 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 $\mathrm{ord}_{dv}(q) = \mathrm{ord}_{dv/2}(q)$ and we conclude using what we proved in the above. When $2 \mid v$, put $D = 2d$ and $u = v/2$ 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. We have $\mathrm{ord}_D(q) = [\mathrm{ord}_4(q), \mathrm{ord}_{d/2}(q)] = [\mathrm{ord}_4(q), f]$ because $2^2 \| D$, 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. □

Remark 1. *We know that $f_{u,v} = \mathrm{ord}_{dv}(q)k_0$ for some $k_0 \mid d^\infty$ by (1). Hence Lemma 6 shows that $f_{u,v} = fk$ for some $k \mid d^\infty$.*

Lemma 7. *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. We want to show that $[f_{u_1u_2,v} \mid N] = [f_{u_1,v} \mid N] \cdot [f_{u_2,v} \mid N]$ for coprime $u_1, u_2 \mid d$, or equivalently, $f_{u_1u_2,v} = [f_{u_1,v}, f_{u_2,v}]$. Let $r = \operatorname{ord}_{dv}(q)$ and $m = \operatorname{ord}_{\mathbb{F}_q^\times}(\lambda)$. We see that $\operatorname{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\lambda) = (q^r-1)/m$ because $\lambda \in \mathbb{F}_q^\times$. Moreover, we note that

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

for all $u \mid d$. From the above and Lemmas 1 and 2, we obtain

$$f_{u,v} = \frac{r(uv,h)}{\left(\frac{q^r-1}{m}, uv, h\right)} = \frac{r(v,h)}{(v,H_r)} \cdot \frac{\left(u, \frac{h}{(v,h)}\right)}{\left(u, \frac{H_r}{(v,H_r)}\right)}, \tag{2}$$

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 the product of the two numbers. Moreover, recall that $u \mapsto (u,k)$ is a multiplicative function for all fixed integers k. Therefore, using (2), we find that $[f_{u_1,v}, f_{u_2,v}] = f_{u_1u_2,v}$. □

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, if $f \geq 2$. 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. *If $f \geq 2$, then 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

$$\frac{R_q(a,d,N)N}{q^N} \tag{3}$$

does not exist. We proceed to show that (3) converges to different limits for distinct subsequences. 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 $n \geq 0$. Let $(y_n)_{n\geq 0}$ be the sequence defined by $y_n = \bar{f}(h,d^\infty)(dn+1)$ for all $n \geq 0$. By Theorem 7, we have

$$\left|\frac{R_q(a,d,y_n)y_n}{q^{y_n}} - \delta_q(a,d,y_n)\right| \leq 2^{\omega(d)+1}c_1\tau(e_{y_n})q^{-y_n/2}, \tag{4}$$

and by Lemma 5, we see that $e_{y_n} = e_{\bar{f}}(h,d^\infty)\nu$, with $\nu \mid 2^\infty$, making e_{y_n} a constant, say E, that does not depend on n. In particular, $\tau(e_{y_n})$ is also a constant and the right hand side of (4) converges to 0 as $n \to +\infty$. Hence the limit of (3), where we substituted N for y_n, is the limit of $\delta_q(a,d,y_n)$. By Theorems 6 and 7,

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

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. 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

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

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 7. Therefore, we have

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

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

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

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 that $(lv,h) = v$, we find the general term to be

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

which is non-zero, whether $f_{l,v} \mid \bar{f}(h,d^\infty)$ or not. We obtain that (3) converges to 0 and $\delta > 0$ for distinct subsequences. Hence, the set $R_q(a,d)$ has no d_1-density, and thus no d_2-density by [4, Proposition 1.8]. □

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

$$\mathbb{N} = \bigsqcup_{j=1}^{f-1} S_j \sqcup \bigsqcup_{w \mid d^\infty} \bigsqcup_{\substack{\alpha=1 \\ (\alpha,d)=1}}^{d} A_{w,\alpha}, \tag{5}$$

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

$$\delta_q(a,d,N) = \sum_{v \mid e_{fw}} \sum_{u \mid d} \frac{\mu(u)(uv,h)}{uv} \cdot [f_{u,v} \mid fw] \tag{6}$$

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

$$\delta_q(a,d) = \frac{\varphi(d)}{df} \sum_{w|d^\infty} \frac{\delta_w}{w}. \tag{7}$$

We show that $\delta_q(a,d)$ is the d_3-density of the set $R_q(a,d)$.

Lemma 8. *There exists an absolute constant $c_2 > 0$ such that for every $x \geq e^{2\omega(d)}$, we have*

$$\sum_{\substack{w|d^\infty \\ w\leq x}} 1 \leq c_2 \log(x)^{\omega(d)} \quad \textit{and} \quad \sum_{\substack{w|d^\infty \\ w> x}} \frac{1}{w} \leq \frac{3c_2 \log(x)^{\omega(d)}}{x}.$$

Proof. Let $M_d(x)$ denote the sum on the left. We see that $M_d(x)$ is bounded above by the product of $\log_l(x)+1$ for all $l \mid d$. We have $\log_l(x)+1 \leq \log(x)$ for all primes $e^2 \leq l \leq x$. If $l \leq e^2$, then there exists a constant $C_l > 0$ such that $\log_l(x)+1 \leq C_l \log(x)$. The result follows by choosing c_2 as the product of the C_l's for all primes $l \leq e^2$. Next, we apply Abel summation formula to the series on the right so that $M_d(x)$ appears in the expression. We find

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

Call $I(x)$ the integral on the right-hand side of the inequality. For $x \geq e^{2\omega(d)}$, we see that $I(x) - 2\log(x)^{\omega(d)}/x$ is an increasing function that converges to 0 as x tends to infinity. Hence $I(x) \leq 2\log(x)^{\omega(d)}/x$ and the result follows. □

Lemma 9. *For every $N \geq e^{2\omega(d)}$, we have*

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

where c_2 is the absolute constant defined in Lemma 8.

Proof. From the partition of $\mathbb{N}$ given in (5), 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 $w \leq N$ and

$$\#A_{w,\alpha}(N) = \bigg\lfloor \frac{N + fw(d-\alpha)}{fdw} \bigg\rfloor,$$

thus, we obtain

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

By definition of the floor function, on the one hand, we have

$$S_N \geq \frac{\varphi(d)}{N} \sum_{\substack{w \mid d^\infty \\ w \leq N}} \delta_w \left(\frac{N}{fdw} - 1 \right) = \delta_q(a,d) - \frac{\varphi(d)}{N} \sum_{\substack{w \mid d^\infty \\ w \leq N}} \delta_w - \frac{\varphi(d)}{fd} \sum_{\substack{w \mid d^\infty \\ w > N}} \frac{\delta_w}{w}.$$

and on the other hand,

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

We obtain

$$|S_N - \delta_q(a,d)| \leq \frac{\varphi(d)}{N} \sum_{\substack{w \mid d^\infty \\ w \leq N}} \delta_w + \frac{\varphi(d)}{fd} \sum_{\substack{w \mid d^\infty \\ w > N}} \frac{\delta_w}{w} \leq c_2 \varphi(d) \left(1 + \frac{3}{fd} \right) \frac{\log(N)^{\omega(d)}}{N},$$

where we used that $\delta_w \leq 1$, and Lemma 8. □

Theorem 9. *There exists an absolute constant $c_3 > 0$ such that*

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

for all $N \geq e^{2\omega(d)}$, where c_2 is the absolute constant defined in Lemma 8. 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

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

for all $N \geq e^{2\omega(d)}$, by Lemma 9. Let us now bound the term $|R_N - S_N|$. Using Theorem 7, and since $R_q(a,d,n) = \delta_q(a,d,n) = 0$ if $f \nmid n$, we have

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

By Lemma 5, $e_n \leq 2^{v_2(q^f+1)} e_f n/f$. Hence $\tau(e_n) \leq v_2(q^f+1)\tau(e_f)n/f$, and

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

Since $q^{-1/2} < 1$, we obtain

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

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 $\delta_q(a,d)$. □

Corollary 1. *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]. □

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 $f_{u,v} = \mathrm{ord}_{dv}(q)$ 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 $2 \nmid (m,n)$ and by $\eta(m,n) = 2^{v_2(q^{\bar{f}}+1)-1}$ otherwise. Note that $m \mapsto \eta(m,n)$ is a multiplicative function for all $n \geq 1$.

Proposition 2. *Assume that $f_{u,v} = \mathrm{ord}_{dv}(q)$ 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. The proof being quite similar to the proof of [12, Lemma 4], we may skip a few details. Since $v \mid e_{fw}$ if and only if $\mathrm{ord}_{dv}(q) \mid fw$, and because $f_{u,v} = \mathrm{ord}_{dv}(q)$, we find from (6) that

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

where we used the Euler product formula on the inner sum. Note that the product is non-zero if and only if $(h, d^\infty) \mid e_{fw}$, or equivalently, $\bar{f} \mid fw$. Assume $fw = \bar{f}\nu$ for some $\nu \mid d^\infty$. Then, the product is equal to $\varphi(d)/d$. We use the Euler product formula twice on the remaining sum to obtain

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

Finally, we apply Lemma 5 to $(q^{\bar{f}\nu}-1, u^\infty)$ in the general term of the sum, which is allowed since $u \mid q^{\bar{f}} - 1$, to obtain $\delta_w = \delta(\nu)$. □

Theorem 10. *Put $C = 3 \cdot 4^{-1} + 2^{-v_2(q^{\bar{f}}+1)-1}$. Assume that $f_{u,v} = \mathrm{ord}_{dv}(q)$ 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 (7) of $\delta_q(a,d)$. We obtain

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

Since the series is absolutely convergent, we may interchange the sum in $\delta(\nu)$ and the series. We find

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

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. By the Euler product formula, we have

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

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

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

Writing $u' = u/(u,2)$, we have

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

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

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

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

Note that Theorem 10 coincides with [2, Theorem 3.3] and [3, Theorem 11] 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 that $\delta_q(a,d)$ can be written in a closed form in Section 8. However, the latter was done under the assumption that $[\mathbb{F}_{dv,uv} : \mathbb{F}_q]$ is equal to $\mathrm{ord}_{dv}(q)$ for all $v \mid d^\infty$ and $u \mid d$. It is quite easy to prove that this condition holds when $(d,h) = 1$ or $(d,m) = 1$, where $m = \mathrm{ord}_{\mathbb{F}_q^\times}(\lambda)$. However, this 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] H. Bilharz, Primdivisoren mit vorgegebener Primitivwurzel, Math. Ann., **114** (1937), 476–492.
[6] M. D. Fried and M. Jarden, Field Arithmetic, Ergeb. Math. Grenzgeb. (3), **11**, Springer-Verlag, HeidelBerg, 2008.
[7] 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.
[8] 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.
[9] L. Hochfilzer and E. Waxman, On Artin's primitive root conjecture for function fields over $\mathbb{F}_q$, Q. J. Math. **75** (2024), no. 3, 1181–1200.
[10] S. Kim and M. R. Murty, Artin's primitive root conjecture for function fields revisited, Finite Fields Appl., **67** (2020), 101713.
[11] S. Lang, Algebra, Graduate Texts in Mathematics, **211**, Springer-Verlag, 2002.
[12] P. Moree, On primes p for which d divides $\mathrm{ord}_p(g)$, Funct. Approx. Comment. Math. **33** (2005), 85–95.
[13] F. Pappalardi, Square-free values of the order function, New York J. Math., **9** (2003), 331–344.
[14] F. Pappalardi and I. Shparlinski, On Artin's conjecture over function fields, Finite Fields Appl. 1 (1995), 399–404.
[15] I. E. Shparlinski, Some arithmetic properties of recurrence sequences, Math. Notes, **47** (1990), 612–617; translated from Mat. Zametki, **47** (1990), 124–131.
[16] M. Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, (2002).
[17] H. Stichtenoth, Algebraic Function Fields and Codes, Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.
[18] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Actualités Sci. Ind., no. 1041, Publ. Inst. Math. Univ. Strasbourg, **7** (1945), Hermann et Cie., Paris, 1948.
[19] 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