INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 7(2) (2007), #A04

AN ELEMENTARY METHOD TO COMPUTE PRIME DENSITIES IN $\mathbb{F}_Q[X]$

Christian Ballot
Department of Mathematics, Université de Caen, France
ballot@math.unicaen.edu

Received: 12/2/05, Accepted: 9/13/06

Abstract

Fixing a prime ℓ and a power q of a prime p, we compute the Dirichlet density of the set of primes P of $\mathbb{F}_q[X]$ defined by

$$\{P \in \mathbb{F}_q[X];\ \ell \text{ divides the order of } X \pmod P\}.$$

Our method is fully elementary in that it does not use any Kummer theory, or the Chebotarev Density Theorem in any form.

1. Introduction.

Throughout the paper ℓ denotes a fixed odd rational prime. The exponent of the largest power of ℓ dividing an integer n is written $\nu_\ell(n)$. We will also write $\ell^{\nu_\ell(n)}||n$.

A classical result states that if $a \in \mathbb{Z} \setminus \mathbb{Z}^\ell$ and $\rho_p(a)$ is the order of $a \pmod p$, then

$$\big\{p \text{ rational prime; } \ell \mid \rho_p(a)\big\} \text{ has a Dirichlet density equal to } \frac{\ell}{\ell^2-1}. \tag{1}$$

We refer to [**Ha**] and [**Ba1**], p. 32 for algebraic proofs of (1). But finer and more general results exist, in particular formulas for the asymptotic proportion of primes $p \le x$ such that $m \mid \rho_p(a)$ with error estimates valid for any $a \in \mathbb{Z}$ and any composite integer $m \ge 2$ ([**Od**], [**Wie**], [**Pa**]).

In this paper, we investigate an analogous question in the ring $\mathbb{F}_q[X]$, where q is a prime power p^e, where $e \ge 1$. We show that

$$\bar{\Omega} = \{P \text{ prime in } \mathbb{F}_q[X];\ \ell \mid \rho_P(X)\} \tag{2}$$

has Dirichlet density $\delta_{q,\ell} = \dfrac{1}{f}\left[1 - \dfrac{1}{\ell^{\alpha-1}(\ell+1)}\right]$, where $\rho_P(X)$ is the order of $X \pmod P$, f is the order of $q \pmod \ell$, and $\alpha = \nu_\ell(q^f-1)$. Here a prime P in $\mathbb{F}_q[X]$ is a monic irreducible

polynomial of the ring. Note, for the sake of curiosity, that if q is a primitive root (mod ℓ) and $\alpha = \nu_\ell(q^{\ell-1} - 1) = 1$, then $\delta_{q,\ell}$ satisfies, as in the classical case (1), $\delta_{q,\ell} = \dfrac{\ell}{\ell^2 - 1}$.

But the most interesting feature of the paper, in our view, is that, contrary to the classical case, these densities are computed via an elementary method. This method does not use any Kummer theory, nor any form of the Chebotarev Density Theorem. The case $\ell = 2$ was handled in [**Ba3**]. The main object in [**Ba3**] was to show that the method of Hasse could successfully be adapted to the ring $\mathbb{F}_q[X]$. We clearly could have used the Hasse-like method here, but our intention was to give visibility and clarity to a method that does not have an equivalent in the classical setting. The method uses an adapted notion of asymptotic density d, which, at least in the present context, plays a role similar to what is usually called natural density in $\mathbb{Z}$. This notion was introduced in [**Ba2**] and shown to imply Dirichlet density δ with $\delta = d$. It was also shown that some sets of primes in $\mathbb{F}_q[X]$ have Dirichlet density δ, but no density d. Because this elementary method is close to an actual counting "by degree" (see Theorems 9 and 10), it yields asymptotic formulas for the densities d with error terms of interest. We would like to point out that some strong versions of the Chebotarev Density Theorem in function fields also provide estimates per degree, but that these theorems, contrary to the prime number theorem in $\mathbb{F}_q[X]$, are difficult to prove (see [**Ro**], p. 125-6, for such a theorem and some commentaries). Note that we focused our attention on the case of the order of X (mod P) and of a prime ℓ, but it remains to be seen whether X could be replaced by some other element M of $\mathbb{F}_q[X]$ and ℓ by any composite integer m. At least we can show that the densities we obtained for $M = X$ are equal to what one would expect heuristically on average over all monic polynomials M in $\mathbb{F}_q[X]$ (follow the method of Section 5.2 in [**Ba3**]; in fact, this is a faster way of obtaining the density values we calculate here).

In Section 2, the abstract and simple frame of the method is being explained and translated into a theorem, Theorem 1. But framing the method in the abstract also facilitates the actual computing of the densities $\delta_{q,\ell}$, carried out in Section 3, where Theorem 1 will be referred to in the two instances $q \equiv 1$ (mod ℓ) and $q \not\equiv 1$ (mod ℓ). An amusing minor similarity to the Hasse method remains in that, technically, finding the density of $\bar{\Omega}$ (defined in (2)) is done by computing the density of its complementary set of primes Ω. Primes in $\mathbb{F}_q[X]$ are also polynomials and have roots. So we may count primes in Ω by counting their roots. Lemma 5 (and Lemma 6) explain how to do this counting transfer. Lemmas 7 and 8 are technical and ease up the writing of the main results, Theorems 9, 10, and 11. We added a short third section in which we compute the average of the densities $\delta_{p,\ell}$ over all rings $\mathbb{F}_p[X]$ as p varies through primes. This result, Theorem 12, is a mixed average over polynomial and rational primes and uses the classical Dirichlet Density Theorem.

The set of all primes in $\mathbb{F}_q[X]$ is denoted by I. If $S \subset I$, then S_n denotes the number of primes in S of degree n. We will use the formula $I_n = n^{-1} \sum_{d \,|\, n} \mu(d) q^{n/d}$, where μ is the Möbius function, and the equivalence $I_n \sim q^n/n$ known as the Prime Number Theorem for polynomials (PNT), both of which can be found in [**Ro**], Ch. 2, as well as the lower estimate

$nI_n \geq q^n - q/(q-1)q^{n/2} + q/(q-1)$ (see for instance Lemma 4.2 of [**Ba3**]).

2. The Elementary Method

Our method exploits a density result shown in [**Ba2**]. Namely, if S is a set of primes in $\mathbb{F}_q[X]$ and the limit

$$d = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{S_n}{I_n} \text{ exists,} \tag{3}$$

then S possesses a Dirichlet density

$$\delta = \lim_{s\to 1^+} \frac{\sum_{P\in S} |P|^{-s}}{\sum_P |P|^{-s}}, \quad \text{with } \delta = d.$$

The density defined in (3) was shown in [**Ba2**] to be a fair analogue to the classical notion of prime asymptotic density, which is also known to imply Dirichlet density for sets of primes in $\mathbb{Z}$. Our method to compute the limit d in (3), is based on finding approximations of the quotients S_n/I_n such that the discrepancies with their exact values have an average, over N, that tends to 0 as $N \to \infty$.

Theorem 1 Let S be a set of primes in $\mathbb{F}_q[X]$, and let K and τ be positive real numbers. Assume $\mathbb{N}$ is partitioned into a finite or countable union of disjoint arithmetic progressions $A_j = \{a_j + nd_j;\ n = 0, 1, 2, \dots\}$, where for each $j = 1, 2, 3, \dots$, $0 \leq a_j < d_j$, (a_j, d_j integral). Assume for each j there is a constant $c_j \in [0, 1]$ such that for any $n \in A_j$, we have

$$\left| \frac{S_n}{I_n} - c_j \right| \leq Kq^{-\tau n}. \tag{4}$$

Assume moreover that $\sum_{j\geq 1} c_j < \infty$. Then for any $N \geq 1$

$$\left| \frac{1}{N} \sum_{n=1}^{N} \frac{S_n}{I_n} - \sum_{j\geq 1} \frac{c_j}{d_j} \right| \leq \frac{C}{N},$$

where C may be chosen to be $\sum_{j\geq 1} c_j + K/(q^\tau - 1)$. In particular, S has a d-density and a Dirichlet density equal to $\sum_{j\geq 1} c_j/d_j$.

Proof. Let N be a large positive integer. Then $A_j \cap [1, N]$ contains n_j members where $n_j = N/d_j + \varepsilon_j$ for some $\varepsilon_j \in \mathbb{R}$ satisfying $|\varepsilon_j| \leq 1$. Then the sum $s_N = \sum_{n=1}^{N} S_n/I_n$ satisfies

$$\begin{aligned}
\sum_{j\geq 1} n_j c_j - K \sum_{n=1}^{N} q^{-\tau n} \ &\leq s_N \leq \textstyle\sum_{j\geq 1} n_j c_j + K \sum_{n=1}^{N} q^{-\tau n}, \ \text{ implying} \\
\left| s_N - N \sum_{j\geq 1} c_j/d_j \right| \ &\leq \textstyle\sum_{j\geq 1} c_j + Kq^{-\tau}/(1 - q^{-\tau}), \ \text{ so that} \\
\left| \frac{s_N}{N} - \sum_{j\geq 1} \frac{c_j}{d_j} \right| \ &\leq N^{-1} \left[\textstyle\sum_{j\geq 1} c_j + K/(q^\tau - 1) \right],
\end{aligned}$$

thereby proving the theorem. □

Remark 2. Theorem 1 remains true even if (4) is false for finitely many degrees n although one may have to choose a larger value for K.

In the ring $\mathbb{Z}$, the Dirichlet Density Theorem says that, for any $d \geq 2$, primes are equidistributed among linear forms $\{a+nd;\ n=1,2,\dots\}$ where a varies through all residue classes (mod d) that are coprime to d. In $\mathbb{F}_q[X]$, Theorem 1 allows us to state an analogue of the Dirichlet Theorem that takes into account the fact that there are primes of any norm. Indeed, for any $d \geq 2$, primes are equidistributed among the d subsets of primes of degree $a+nd$, $n=1,2,\dots$, when a varies from 0 to $d-1$. We state this result below.

Theorem 3 (Dirichlet Density Theorem for primes having degree in arithmetic progression) Let a and d be integers with $d \geq 1$. Then the set of primes in $\mathbb{F}_q[X]$ of degree in the arithmetic progression $a+nd$ has Dirichlet density $\dfrac{1}{d}$.

Proof. Apply Theorem 1, taking Remark 2 into account, with $A_j = \{j+nd;\ n=1,2,\dots\}$ for $j=0,1,\dots,d-1$ and $c_j = 0$ unless $j \equiv a \pmod{d}$, in which case $c_j = 1$. □

3. Application to Primes P such that $\ell \mid \rho_P(X)$

In the sequel, ℓ is an odd rational prime, q is a prime power p^e, where p and $e \geq 1$ are fixed, f denotes the order of q (mod ℓ) and $\alpha = \nu_\ell(q^f-1)$. We seek to apply Theorem 1 to the set Ω of primes defined by

$$\Omega = \{P \text{ prime in } \mathbb{F}_q[X];\ \ell \nmid \rho_P(X)\}.$$

We first recall a few facts from the theory of Lucas sequences (see [**Wil**], **4.3**). Consider the Lucas sequence of general term $u_n = \dfrac{q^n-1}{q-1}$. Then the least natural number $r \geq 1$ such that ℓ divides u_r is called the rank of ℓ in (u_n). With our hypotheses r is known to exist. Moreover, we have

$$\begin{aligned} \nu_\ell(u_n) &= 0, && \text{if } r \nmid n, && (5)\\ \nu_\ell(u_{mr}) &= \nu_\ell(u_r) + \nu_\ell(m), && \text{if } n = mr, \\ \text{so that} \qquad \nu_\ell(q^{mr}-1) &= \nu_\ell(q^r-1) + \nu_\ell(m). && && (6) \end{aligned}$$

Lemma 4 Assume $q = p^e$, where p be a prime distinct from ℓ. Then for any integer $n \geq 1$, we have

$$\nu_\ell(q^n-1) = 0, \ \text{ if } f \nmid n, \nu_\ell(q^f-1) + \nu_\ell(n), \ \text{ if } f \mid n.$$

Proof. Assume first that $q \equiv 1 \pmod{\ell}$. Then $f = 1$ and we need to show that

$$\nu_\ell(q^n-1) = \nu_\ell(q-1) + \nu_\ell(n). \tag{7}$$

We have $\dfrac{q^n-1}{q-1} = \sum_{k=0}^{n-1} q^k \equiv n \pmod{\ell}$. Therefore $r = \ell$. Hence (7) follows from (5) if $\ell \nmid n$. For $n = m\ell$, we write $q \equiv 1 + \lambda\ell \pmod{\ell^2}$ for some λ, $0 \le \lambda \le \ell - 1$. Hence, $u_\ell = \sum_{k=0}^{\ell-1} q^k \equiv \ell + \lambda\ell \sum_{k=1}^{\ell-1} k \equiv \ell \pmod{\ell^2}$, which implies $\nu_\ell(q^\ell - 1) = \nu_\ell(q-1) + 1 = \alpha + 1$. And by (6) we have $\nu_\ell(q^{m\ell} - 1) = \nu_\ell(q^\ell - 1) + \nu_\ell(m) = \alpha + 1 + \nu_\ell(m) = \alpha + \nu_\ell(m\ell)$, and (7) follows.

Assume now that $q \not\equiv 1 \pmod{\ell}$. Then $r = f$. And by (5) and (6) respectively we get

$$\nu_\ell\left(\frac{q^n-1}{q-1}\right) = \nu_\ell(q^n - 1) = 0, \text{ if } f \nmid n, \alpha + \nu_\ell(n), \text{ if } f \mid n,$$

since $(f, \ell) = 1$ implies $\nu_\ell(n) = \nu_\ell(m)$. □

Rather than counting primes P in Ω, we may, instead, count the roots of these primes P. The next two lemmas use this idea to yield an expression for Ω_n that will make Ω_n comparable to I_n. In turn this will allow us to use Theorem 1.

Let F_n be the number of elements in the multiplicative group $\mathbb{F}_{q^n}^*$ of $\mathbb{F}_{q^n}$ with order prime to ℓ. Note that these elements form a subgroup of $\mathbb{F}_{q^n}^*$.

Lemma 5 Let γ be algebraic of degree n over $\mathbb{F}_q$ and P denote its minimal polynomial over $\mathbb{F}_q$. Then, the order of γ in the multiplicative group of $\mathbb{F}_q(\gamma)$ is prime to ℓ if and only if P is in Ω.

Proof. Since $\mathbb{F}_q(\gamma) \simeq \mathbb{F}_{q^n}$, the order of γ in $\mathbb{F}_{q^n}^*$ is prime to ℓ if and only if γ is a root of $X^{F_n} - 1$, which holds if and only if P divides $X^{F_n} - 1$ in $\mathbb{F}_q[X]$. But that means $P \in \Omega$. □

Define G_n to be the number of elements $\gamma \in \mathbb{F}_{q^n}^*$ of order prime to ℓ such that $\mathbb{F}_q(\gamma) = \mathbb{F}_{q^n}$.

Lemma 6 We have $F_n = (q^n - 1)\ell^{-\nu_\ell(q^n-1)}$, $G_n = \sum_{d \mid n} \mu(d) F_{n/d}$, and $\Omega_n = G_n/n$.

Proof. Since $\mathbb{F}_{q^n}^*$ is cyclic of order $q^n - 1$, we see that F_n is indeed the largest divisor of $q^n - 1$ prime to ℓ. Now $F_n = \sum_{d \mid n} G_d$, so the Möbius inversion formula yields the claimed expression for G_n. That $\Omega_n = G_n/n$ is a direct consequence of Lemma 5. □

Lemma 7 Suppose $n = \ell^k n'$, where $(n', \ell) = 1$ and $k \ge 1$. Consider a sum $S = \sum_{d \mid n} \mu(d)\omega_d$, where the ω_d's are real numbers whose values depend only on $\nu_\ell(d)$. Then either $S = \omega_1 - \omega_\ell$, if $n = \ell^k$, or 0, otherwise.

Proof. Because the Möbius function is non-zero only for squarefree integers, we have $S = \sum_{\ell \nmid d} \mu(d)\omega_d + \sum_{\ell \| d} \mu(d)\omega_d = \omega_1 \sum_{d \mid n'} \mu(d) - \omega_\ell \sum_{d \mid n'} \mu(d) = \omega_1 - \omega_\ell$, if $n = \ell^k$, or 0, otherwise. □

Lemma 8 Let n be an integer ≥ 2 and let D_n be any set of positive divisors of n. Then the sum $S_{D_n} = \sum_{d \in D_n} \mu(d) q^{n/d}$ is, in absolute value, less than $2q^n$.

Proof. We have $S_{D_n} \le q^n + R_n$, where $R_n = S_{D_n \setminus \{1\}}$. But $|R_n| \le \sum_{k=1}^{n/2} q^k \le q^{n/2+1} \le q^n$ and the result follows. □

Theorem 9 Assume $q = p^e$ is congruent to 1 (mod ℓ). Let $n \ge 2$ be an integer. Then we have

$$\frac{\Omega_n}{I_n} = \ell^{-\alpha}, \quad \text{if } \nu_\ell(n) = 0, \left|\frac{\Omega_n}{I_n} - \ell^{-\alpha-\nu_\ell(n)}\right| \le Kq^{-\tau n}, \quad \text{if } \nu_\ell(n) \ge 1,$$

where $\tau = 1 - \dfrac{1}{\ell}$ and K is a constant depending on q and ℓ that can be effectively computed.

Proof. By Lemma 6 we have $G_n = \sum_{d \mid n} \mu(d) F_{n/d}$. If $\nu_\ell(n) = 0$, then for any d dividing n, $\nu_\ell(n/d) = 0$ and by Lemma 4, $\nu_\ell(q^{n/d} - 1) = \nu_\ell(q^f - 1) = \nu_\ell(q - 1) = \alpha$. So $G_n = \ell^{-\alpha} \sum_{d \mid n} \mu(d) q^{n/d} - \ell^{-\alpha} \sum_{d \mid n} \mu(d) = \ell^{-\alpha} \sum_{d \mid n} \mu(d) q^{n/d}$, since $n \ge 2$. Thus $G_n/n = \ell^{-\alpha} I_n$ so that the ratio Ω_n/I_n is exactly $\ell^{-\alpha}$.

For $\nu_\ell(n) \ge 1$, write $n' = n\ell^{-\nu_\ell(n)}$, $g = q^{\ell^{\nu_\ell(n)-1}}$, $m = \alpha + \nu_\ell(n)$, and $S = \sum_{d \mid n} \mu(d)\omega_d$ with $\omega_d = \ell^{-\nu_\ell(q^{n/d}-1)}$. Then $G_n = \sum_{d \mid n} \mu(d)\omega_d q^{n/d} - S = \ell^{-m} \sum_{\nu_\ell(d)=0} \mu(d) q^{n/d} + \ell^{-(m-1)} \sum_{\nu_\ell(d)=1} \mu(d) q^{n/d} - S = \ell^{-m} \sum_{d \mid n} \mu(d) q^{n/d} + \dfrac{\ell-1}{\ell^m} \displaystyle\sum_{\nu_\ell(d)=1} \mu(d) q^{n/d} - S = \ell^{-m} n I_n - \dfrac{\ell-1}{\ell^m} \displaystyle\sum_{d \mid n'} \mu(d) g^{n'/d} - S$. By Lemma 7, S is either 0 (if $n' > 1$) or $\omega_1 - \omega_\ell = (1-\ell)/\ell^m$ (if $n' = 1$), while $\sum_{d \mid n'} \mu(d) g^{n'/d}$ is dominated by $g^{n'}$. Therefore $0 \le \ell^{-m} n I_n - G_n \le (\ell-1)\ell^{-m} g^{n'} \le q^{n/\ell}$. Hence, because $I_n \sim q^n/n$ and $nI_n \ge q^n - q/(q-1)q^{n/2} + q/(q-1)$, there is a constant $K = K(q,\ell) > 1$, effectively computable, such that for any n with $\nu_\ell(n) \ge 1$,

$$\left|\Omega_n/I_n - \ell^{-m}\right| \le Kq^{-\tau n} \text{ with } \tau = 1 - \frac{1}{\ell}.$$

□

Theorem 10 Assume q is not congruent to 1 (mod ℓ) so that f, the order of q (mod ℓ), exceeds 1. Assume $n \ge 2$ is an integer. Then we have

$$\frac{\Omega_n}{I_n} = 1, \quad \text{if } f \nmid n, \left|\frac{\Omega_n}{I_n} - \ell^{-\alpha-\nu_\ell(n)}\right| \le Kq^{-\tau n}, \text{if } f \mid n,$$

where $\alpha = \nu_\ell(q^f - 1)$, $\tau = 1 - 1/p_1$, p_1 is the least prime factor of f, and K is a constant depending on q and ℓ which can be effectively computed.

Proof. Assume $f \nmid n$. Then by Lemma 4, $\ell \nmid q^n - 1$. But $q^n - 1$ is the order of the cyclic group $(\mathbb{F}_q[X]/P)^*$ for any prime P of degree n. Thus, the order of X (mod P) can only be prime to ℓ, and $\Omega_n = I_n$.

Assume now that $f \mid n$. As in the proof of Theorem 9, we first obtain that

$$G_n = \sum_{d \mid n} \mu(d) q^{n/d} \ell^{-\nu_\ell(q^{n/d}-1)} - S. \tag{8}$$

We then split the sum over $d \mid n$ in (8) into three disjoint subsums S_1, S_2 and S_3 according to whether $f \nmid \frac{n}{d}$, $f \mid \frac{n}{d}$ with $\ell \nmid d$, and $f \mid \frac{n}{d}$ with $\ell^1 || d$, respectively. Hence by Lemma 4, we have, putting $k = \nu_\ell(n)$,

$$\begin{aligned}
S_1 &= \sum_{f \nmid \frac{n}{d}} \mu(d) q^{n/d} = \frac{1}{\ell^{\alpha+k}} S_1 + \frac{\ell^{\alpha+k}-1}{\ell^{\alpha+k}} S_1, \\
S_2 &= \frac{1}{\ell^{\alpha+k}} \sum \mu(d) q^{n/d}, \qquad \Big(\text{ summing over } d\text{'s with } f \mid \frac{n}{d} \text{ and } \ell \nmid d \Big) \\
S_3 &= \frac{\ell}{\ell^{\alpha+k}} \sum \mu(d) q^{n/d}, \qquad \Big(\text{ summing over } d\text{'s with } f \mid \frac{n}{d} \text{ and } \ell^1 || d \Big).
\end{aligned}$$

Therefore,

$$G_n = \frac{1}{\ell^{\alpha+k}} \sum_{d \mid n} \mu(d) q^{n/d} + \frac{\ell-1}{\ell^{\alpha+k}} \sum_{f \mid \frac{n}{d},\ \ell^1 || d} \mu(d) q^{n/d} + \frac{\ell^{\alpha+k}-1}{\ell^{\alpha+k}} S_1 - S. \tag{9}$$

The second term in (9) is $-\frac{\ell-1}{\ell^{\alpha+k}} \sum_{d \in D_{n/\ell}} \mu(d) q^{\frac{n/\ell}{d}}$, where $D_{n/\ell}$ is a set of divisors of n/ℓ. Hence by Lemma 8, this sum is less than $2(\ell-1)\ell^{-\alpha-k} q^{n/\ell}$.

We now consider S_1. If $f \nmid n/d$ and $f \mid n$, then the g.c.d. $(f, d) > 1$. So if p_1 is the least prime factor of f, then $n/d \le n/p_1$. Therefore, by Lemma 8, S_1 is less than $2q^{n/p_1}$. The theorem follows by dividing (9) by nI_n and having $nI_n \sim q^n$ and $nI_n \ge q^n - q/(q-1)q^{n/2} + q/(q-1)$ as in Theorem 9. □

Theorem 11 Let ℓ be an odd prime. Consider the ring $\mathbb{F}_q[X]$, where $q = p^e$ and p is a prime distinct from ℓ. Then the Dirichlet density $\bar{\delta} = \bar{\delta}_{q,\ell}$ of primes $P \in \mathbb{F}_q[X]$ such that the order of $X \pmod P$ is prime to ℓ, is

$$1 - \frac{1}{f} + \frac{1}{\ell^{\alpha-1}(\ell+1)} \frac{1}{f},$$

where f is the order of $q \pmod \ell$ and $\alpha = \nu_\ell(q^f - 1)$.

Consequently, the set $\{P \in \mathbb{F}_q[X] : \ \ell \text{ divides the order of } X \pmod P\}$ has Dirichlet density

$$\delta = \delta_{q,\ell} = \frac{1}{f}\left[1 - \frac{1}{\ell^{\alpha-1}(\ell+1)}\right].$$

Proof. First we assume $q \equiv 1 \pmod{\ell}$. Note that $\mathbb{N}$ is the disjoint union of the arithmetic progressions $A_{k,\lambda}$, for $k \geq 0$ and $1 \leq \lambda \leq \ell - 1$, where $A_{k,\lambda} = \{\lambda\ell^k + n\ell^{k+1};\ n = 0, 1, 2, \dots\}$. By Theorem 10 we may use Theorem 1 with $\tau = 1 - 1/\ell$ and $c_{k,\lambda} = 1/\ell^{\alpha+k}$ and conclude that Ω has a Dirichlet density $\bar{\delta}$ equal to

$$\sum_{k\geq 0}\sum_{\lambda=1}^{\ell-1} \frac{c_{k,\lambda}}{\ell^{k+1}} = \frac{\ell-1}{\ell^{\alpha+1}} \sum_{k\geq 0} \frac{1}{\ell^{2k}} = \frac{1}{\ell^{\alpha-1}} \frac{1}{\ell+1}.$$

Note that this formula matches the density formula claimed since here $f = 1$.

Assume now that $q \not\equiv 1 \pmod{\ell}$. Consider the arithmetic progressions $A_j = \{j + fn;\ n = 0, 1, 2, \dots\}$ for $j = 1, 2, \dots, f-1$, and $B_{k,\lambda}$ consisting of the integers n defined by

$$n \equiv 0 \pmod{f} \quad \text{and} \quad n \equiv \lambda\ell^k \pmod{\ell^{k+1}},$$

for $k \geq 0$ and $1 \leq \lambda \leq \ell - 1$. Note that $B_{k,\lambda}$ is an arithmetic progression of common difference $f\ell^{k+1}$. Then by Theorem 10 we may apply Theorem 1 with constants $c_j = 1$ and $b_{k,\lambda} = \ell^{-(\alpha+k)}$ and $\tau = 1 - 1/p_1$ so that Ω has Dirichlet density

$$\bar{\delta} = \sum_{j=1}^{f-1} \frac{1}{f} + \sum_{k\geq 0}\sum_{\lambda=1}^{\ell-1} \frac{1}{f\ell^{k+1}\ell^{\alpha+k}},$$

yielding the claimed density. □

Remark. For $\ell = 3$ and $q = 5$, we calculated $\dfrac{1}{10}\displaystyle\sum_{n=1}^{10} \Omega_n/I_n$ to be

$$\frac{1}{10}\left[1 + \frac{1}{5} + 1 + \frac{1}{3} + 1 + \frac{67}{645} + 1 + \frac{1}{3} + 1 + \frac{1}{3} \cdot \frac{3127}{3129}\right] \simeq 0.630,$$

where we counted $I_1 = 4$ discarding the prime X, since the order of $X \pmod{X}$ has no meaning. This value for $n = 10$ already compares well to the asymptotic density $5/8 = 0.625$ of Ω.

4. An Average Density Theorem

Here the odd rational prime ℓ is fixed and q varies through the rational primes p. Note that the Dirichlet densities $\delta_{p,\ell}$ of the sets $\{P \in \mathbb{F}_p[X];\ \ell \mid \rho_P(X)\}$ in various $\mathbb{F}_p[X]$ depend only on the parameters f and α. So let us write $d_{f,\alpha,\ell} = \dfrac{1}{f}\left[1 - \dfrac{1}{\ell^{\alpha-1}(\ell+1)}\right]$. Because the parameters f and α fluctuate much from prime to prime, we wish to compute the average δ_ℓ over all primes p of the $\delta_{p,\ell}$'s, i.e. the quantity $\lim_N N^{-1}\sum_{n=1}^{N} \delta_{p_n,\ell}$, where p_n is the n-th prime.

Theorem 12 The average of the Dirichlet densities $\delta_{p,\ell}$, over all primes p, exists and equals

$$\delta_\ell = \frac{1}{\ell-1}\left(1-\frac{\ell}{(\ell+1)^2}\right)\sum_{f \,\big|\, \ell-1}\frac{\varphi(f)}{f},$$

where φ is the Euler totient function.

Proof. Let $\mathcal{P}_{f,\alpha}$ be the set of primes p with parameters f and α. This set has a Dirichlet density. Indeed, $p \in \mathcal{P}_{f,\alpha}$ if and only if $p^f \equiv 1 \pmod{\ell^\alpha}$ but $p^f \not\equiv 1 \pmod{\ell^{\alpha+1}}$. Now $p^f \equiv 1 \pmod{\ell^\alpha}$ if and only if p belongs to one of the $\varphi(f)$ residue classes in $(\mathbb{Z}/\ell^\alpha)^*$ of order f. By the Dirichlet Density Theorem such primes have density $\varphi(f)/\varphi(\ell^\alpha)$. Therefore, the Dirichlet density $\delta(\mathcal{P}_{f,\alpha})$ of $\mathcal{P}_{f,\alpha}$ is

$$\delta(\mathcal{P}_{f,\alpha}) = \frac{\varphi(f)}{\ell^\alpha - \ell^{\alpha-1}} - \frac{\varphi(f)}{\ell^{\alpha+1} - \ell^\alpha} = \frac{\varphi(f)}{\ell^\alpha},$$

since primes p such that $p^f \equiv 1 \pmod{\ell^{\alpha+1}}$ form a subset of $\{p;\ p^f \equiv 1 \pmod{\ell^\alpha}\}$. By the same argument as used in [**Ba3**], Theorem 5, we may assert that the average δ_ℓ exists and is equal to

$$\delta_\ell = \sum_{f \,\big|\, \ell-1}\sum_{\alpha\geq 1}\delta(\mathcal{P}_{f,\alpha})d_{f,\alpha,\ell} = \sum_{f \,\big|\, \ell-1}\sum_{\alpha\geq 1}\frac{\varphi(f)}{\ell^\alpha}d_{f,\alpha,\ell} = \sum_{f \,\big|\, \ell-1}\frac{\varphi(f)}{f}\sum_{\alpha\geq 1}\left(\frac{1}{\ell^\alpha} - \frac{1}{\ell+1}\frac{1}{\ell^{2\alpha-1}}\right),$$

which yields the value claimed in the statement of the theorem. □

Examples. For $\ell = 3$, we have $\delta_\ell = 39/64$, significantly less than δ_2 computed in [**Ba3**] which is $29/36$. For a prime $\ell = 2m+1$, where m is prime, $\delta_\ell = 3\dfrac{\ell-2}{(\ell-1)^2}\left(1-\dfrac{\ell}{(\ell+1)^2}\right)$.

References

[**Ba1**] C. Ballot, *Density of prime divisors of linear recurrences*, Memoirs of the A.M.S., vol. 115, **551** (1995).

[**Ba2**] C. Ballot, *Competing prime asymptotic densities in* $\mathbb{F}_q[X]$. *A discussion*, submitted preprint.

[**Ba3**] C. Ballot, *Counting monic irreducible polynomials* P *in* $\mathbb{F}_q[X]$ *for which order of* X (*mod* P) *is odd*, to appear in the Proceedings of the Journées Arithmétiques of Marseille of July 1995.

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

[**Pa**] F. Pappalardi, *Squarefree values of the order function*, New York J. Math. **9** (2003), 331–344.

[**Od**] R. W. K. Odoni, *A conjecture of Krishnamurty on decimal periods and some allied problems*, J. Number Theory **13** (1981), 303–319.

[**Ro**] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag (Graduate texts in mathematics; 210), (2002).

[**Wie**] K. Wiertelak, *On the density of some sets of primes p for which* $n \mid ord_p a$, Funct. Approx. Comment. Math. **28** (2000), 237-241.

[**Wil**] H. C. Williams, *Édouard Lucas and primality testing*, Wiley, Canadian Math. Soc. Series of Monographs and Advanced Texts (1998).