JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Christian BALLOT

Counting monic irreducible polynomials P in $\mathbb{F}_q[X]$ for which order of $X \pmod P$ is odd

Tome 19, n° 1 (2007), p. 41-58.

<http://jtnb.cedram.org/item?id=JTNB_2007__19_1_41_0>

Journal de Théorie des Nombres de Bordeaux **19** (2007), 41-58

Counting monic irreducible polynomials P in $\mathbb{F}_q[X]$ for which order of $X \pmod P$ is odd

par Christian BALLOT

Résumé. Hasse démontra que les nombres premiers p pour lesquels l'ordre de 2 modulo p est impair ont une densité de Dirichlet égale à 7/24-ième. Dans cet article, nous parvenons à imiter la méthode de Hasse afin d'obtenir la densité de Dirichlet δ_q de l'ensemble des polynômes irréductibles et unitaires P de l'anneau $\mathbb{F}_q[X]$ pour lesquels l'ordre de $X \pmod P$ est impair. Puis nous présentons une seconde preuve, nouvelle, élémentaire et effective de ces densités. D'autres observations sont faites et des moyennes de densités sont calculées, notamment la moyenne des δ_p lorsque p parcourt l'ensemble des nombres premiers.

Abstract. Hasse showed the existence and computed the Dirichlet density of the set of primes p for which the order of $2 \pmod p$ is odd; it is 7/24. Here we mimic successfully Hasse's method to compute the density δ_q of monic irreducibles P in $\mathbb{F}_q[X]$ for which the order of $X \pmod P$ is odd. But on the way, we are also led to a new and elementary proof of these densities. More observations are made, and averages are considered, in particular, an average of the δ_p's as p varies through all rational primes.

1. Introduction

In a 1958 paper [Sier], Sierpinski considered the partition of the rational primes p into two sets: the primes for which the order of $2 \pmod p$ is odd and those for which this order is even. He asked what the relative size of these two sets was. A satisfying and complete answer to this question was found by Hasse [Ha] in the mid-sixties: the odds in favour of the order of 2 (mod p) being odd versus even are 7 to 17. That is, in the sense of Dirichlet, or of natural density, the order of 2 is odd for 7 out of 24 primes. In this paper, we investigate a similar question but in a new setting. Given a prime power q we consider the euclidean ring $\mathbb{F}_q[X]$ and ask for the proportion of primes P in $\mathbb{F}_q[X]$ for which the order of $X \pmod P$ is odd. Here a prime P is a monic irreducible polynomial of $\mathbb{F}_q[X]$. It will be seen that

Manuscrit reçu le 26 juillet 2005.

the answer depends heavily on q, but we will show among other results that the 7 to 17 odds are again the correct answer if and only if q is an odd power of a prime congruent to 3 (mod 8). For any other odd q's, these odds are lower than 7 to 17.

Besides the introduction the paper contains five sections. Section 2 is preliminary and is divided into four subsections. Section 2.1 introduces notation. Section 2.2 is devoted to brief remarks and definitions about Dirichlet and natural densities for primes in $\mathbb{Z}$ or in $\mathbb{F}_q[X]$. Section 2.3 contains the statements of three relevant analogues of classical theorems: the Kummer-Dedekind prime decomposition theorem, the Dirichlet and Kronecker Density Theorems. In Section 2.4 a technical proposition about the power of 2 dividing $q^n - 1$ is proven in a most elementary way. This result will be of frequent use.

The calculation à la Hasse of the density δ_q of primes P in $\mathbb{F}_q[X]$ such that X has odd order modulo P is carried out in Section 3. The method devised by Hasse to compute the density of rational primes p for which the order of a (mod p) is odd (where a is any integer, not just 2) proceeded by first calculating the sub-densities of such primes within the primes p having a fixed power of 2 dividing $p-1$. The method we employ here works similarly with sub-densities being computed within the primes P having a fixed power of 2 dividing their degrees. We will indicate why our method constitutes a proper generalization of the classical method of Hasse (see Remark 3.4).

Now the sub-density corresponding to primes of odd degree (i.e. primes whose degree is divisible by 2^0) obtained in Section 3 yields the *exact* proportion of primes P, within primes of degree $n \geq 3$, for each odd integer n, for which the order of X (mod P) is odd. This, we prove in Section 4 in an elementary manner. This observation and the idea, used to mimic the Hasse method in Section 3, of separating primes according to the 2-adic valuation of their degree, are put together to yield another proof of the existence and of the values of the densities computed in Section 3. This new proof, however, is elementary in that it does not use the Kummer-Dedekind, nor the Kronecker Density Theorems; the proof actually shows that our sets of primes have a natural density, via a notion of natural density that was shown to imply Dirichlet density in [Ba2]. Moreover, the proof is effective in that it shows how the natural density is being approached when considering only primes up to a given norm q^N. Section 4 also contains additional remarks, one of which, Remark 4.6, is of computational interest and presents numerical data for $q = 3$ and primes P of small degrees.

Section 5 contains two subsections. In the first one we return to the classical case to calculate, through a dual and average point of view, and given a "typical" integer a, the expected density of primes p such that a

has odd order $\pmod p$. Indeed the 7:17 odds found by Hasse for $a = 2$ is not typical. These odds are 1:2 for most integers a and in particular for a equal to any odd prime q. Loosely speaking we may say that having chosen a "random" pair of primes (q, p), the odds that the order of $q \pmod p$ be odd are 1 to 2. Thus, this statement made in "dual" form leads us to a short heuristic argument, less educated than the proof of Hasse, to account for the proven, yet still intriguing fact that the order of $q \pmod p$ is twice as often even than odd. In Section 5.2, we carry this point of view over to $\mathbb{F}_q[X]$ and, as a consequence, we show that the choice of X rather than that of another monic polynomial in $\mathbb{F}_q[X]$ is representative of the general expected odds.

That the densities δ_q computed in Section 3 vary a great deal with q, and that the point of view of Section 5 be successful, suggests we investigate the densities themselves "on average". In the classical setting this average is 1/3. What will the densities in our setting turn out to be on average? Thus, in Section 6, we define in reasonable manner density averages over δ_q's. We do so either as q varies through the same e^{th} power of primes p, or as q varies among all powers of the same prime p, or simply over all prime powers q. We show how to prove their existence and we compute their values. For instance, we define $\delta(-, e = 1)$, the average of the δ_p's over all rational primes, as $\lim_x \frac{1}{\pi(x)} \sum_{p \le x} \delta_p$. Various asymptotic averages over rational primes have recently been investigated. For instance the quantity $\frac{1}{x} \sum_{p \le x} \frac{\alpha(p-1)}{p-1}$, where $\alpha(p-1)$ is the average order of elements in $\mathbb{F}_p^*$, was studied in [Ga], or $\delta(a, d) = \frac{1}{\pi(x)} \sum_{p \le x} \delta(p; a, d)$, where $\delta(p; a, d)$ is the proportion of elements of $\mathbb{F}_p^*$ whose order is congruent to $a \pmod d$, was studied in [Mo2]. Note that taking $d = 2$ and $a = 1$ in the last example is akin to our problem. In fact, see Remark 4.5, finding $\delta(1, 2)$ is like averaging over rational p's the proportions of P's for which the order of $X \pmod P$ is odd among primes P in $\mathbb{F}_p[X]$ of degree 1. Instead, we may say that our $\delta(-, e = 1)$ is an average over rational p's of the proportions of such P's regardless of degree.

Much work and progress has been done, since Sierpinski, to compute densities for rational primes defined in several ways that generalize the primes of the Sierpinski question. Thus, many densities for primes in $\mathbb{F}_q[X]$ are expected to be computable.

For instance, finding the density of primes P in $\mathbb{F}_q[X]$ with order of $X \pmod P$ even, as we did here, is the same as determining the density of primes dividing some term of the second order linear recurrence $(X^n + 1)_{n \ge 0}$. The Hasse method, as in the classical case, clearly generalizes to other special recurrences, such as the companion Chebyshev-like recurrence defined by $T_{n+2} = XT_{n+1} + T_n,\ n \ge 0$ with $T_0 = 2$ and $T_1 = X$ in $\mathbb{F}_q[X]$, q

odd. But would the elementary method of Section 4 also generalize to such a sequence T_n?

Also, if ℓ is any prime, not just 2, arguments analogous to those of Sections 3 or 4, yield the density of primes P in $\mathbb{F}_q[X]$ with order of $X \pmod P$ divisible by ℓ (see [Ba3]).

Acknowledgment. I thank the anonymous Referee who read this paper carefully and made sensible suggestions.

2. Preliminaries

2.1. Notation. We denote the exponent of the power of 2 dividing an integer n by $\nu_2(n)$. Equivalently, we will write $2^{\nu_2(n)}||n$ or say that $2^{\nu_2(n)}$ is the (exact) power of 2 *in* n.

Having fixed a rational prime p and an integer $e \geq 1$, we set $q = p^e$. A prime P in $\mathbb{F}_q[X]$ is a monic irreducible polynomial of the ring. The degree of a polynomial P is written $deg(P)$ and the size of the quotient ring $\mathbb{F}_q[X]/P$, i.e. the norm of P, is denoted by $|P|$. The field of fractions of the ring $\mathbb{F}_q[X]$ is denoted by K.

The symbol ζ_n denotes a *primitive* n-th root of unity in the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$.

We define for all integers $k \geq 0$ the sets $S_q(k)$ to be

$$\{P \in \mathbb{F}_q[X],\ P \text{ is prime and } 2^k||deg(P)\}.$$

2.2. Dirichlet and natural densities of sets of primes. Let S be a set of rational primes. Provided the limits exist, the *natural density* of S is defined as $d(S) = \lim_{N\to\infty} N^{-1} \sum_{n=1}^{N} \frac{\chi_S(p_n)}{1}$, where p_n is the n-th rational prime and χ_S is the characteristic function of S, while the *Dirichlet density* of S is $\delta(S) = \lim_{s\to 1^+} \frac{\sum_{p\in S} p^{-s}}{\sum_p p^{-s}}$.

It is well-known that a set S with a natural density d has a Dirichlet density $\delta = d$ ([Des], Chap. 8). However, a set of rational primes may have a Dirichlet density, but no natural density ([Ser], p. 76). The Chebotarev Density Theorem is usually stated with respect to Dirichlet density. However all Chebotarev sets of primes, i.e. sets to which the Chebotarev Density Theorem or one of its corollaries may be applied, all have a natural density ([Nar], Theorem 7.10*). The definition of natural density presents a computational advantage compared to that of Dirichlet in the sense that the approximants $N^{-1} \sum_{n=1}^{N} \chi_S(p_n)$ can be calculated using only a few primes to yield empirical evidence of the existence and the value of a density.

Definitions. A set S of primes in $\mathbb{F}_q[X]$ is said to have Dirichlet density δ if the limit below exists and

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

For a set S of primes in $\mathbb{F}_q[X]$, we define natural density by

$$d(S) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{S_n}{I_n}, \tag{2.1}$$

where S_n represents the number of primes in S of degree n and I_n is the number of primes of degree n in $\mathbb{F}_q[X]$, if the limit exists.

The reasons for defining $d(S)$ as in (2.1) are discussed abundantly in [Ba2] where (2.1) is compared to other definitions and shown to yield the best analogue to the classical notion. In particular, the relations between Dirichlet and natural densities are similar to that of the classical case. Also the N-th approximants $r_N = \frac{1}{N}\sum_{n=1}^{N} \frac{S_n}{I_n}$ can be computed to provide an empirical check to a density computed theoretically. In fact we do this in Remark 4.6.

2.3. Some relevant theorems : statement and reference.

Proposition 2.1. (A weak function field version of a classical Kummer-Dedekind Theorem) *Let α be an algebraic integer over K with minimal polynomial $M(Y) \in (\mathbb{F}_q[X])[Y]$ (that is $M(Y)$ is monic with coefficients in $\mathbb{F}_q[X]$) and P be a prime in $\mathbb{F}_q[X]$. Then there is a one-to-one correspondence between prime ideal factors $\mathcal{P}$ of the ideal generated by P in the ring of integers O_α of $K(\alpha)$ and monic irreducible factors $\mathcal{M}$ of M, and the correspondence is such that the degree of $O_\alpha/\mathcal{P}$ over $\mathbb{F}_q[X]/P$ matches the polynomial degree of $\mathcal{M}$.*

Proof. One may view this proposition as a particular instance of Proposition 25 of [Lan] with the Dedekind ring $A = \mathbb{F}_q[X]$. □

Theorem 2.2 (Dirichlet Density Theorem)**.** *Let B and M be two polynomials in $\mathbb{F}_q[X]$ with $deg(M) \geq 1$. Then the set of primes $\{P \in \mathbb{F}_q[X];\ P \equiv B \pmod{M}\}$ has Dirichlet density $\delta = 1/\Phi(M)$, where $\Phi(M)$ is the number of non-zero polynomials prime to M and of degree less than $deg(M)$.*

Proof. See [Ro], Theorem 4.7. □

Theorem 2.3 (Kronecker Density Theorem)**.** *Let L be a Galois extension of K of Galois group G. Then the set of primes in $\mathbb{F}_q[X]$ which split completely in L has Dirichlet density $1/|G|$.*

Proof. This is a special case of the Chebotarev Density Theorem (Theorem 9.13 of [Ro]). □

2.4. A useful lemma. Let p be an odd prime, e an integer ≥ 1 and $q = p^e$. We consider the pair of Lucas sequences $u_n = \frac{q^n-1}{q-1}$ and $v_n = q^n+1$ $(n \geq 0)$ with characteristic polynomial $X^2-(q+1)X+q$. As the reader may readily check we have the addition formula $2u_{m+n} = u_m v_n + u_n v_m$, $\forall m$ and $n \geq 0$, and its corollary, the so-called double-angle formula, $u_{2n} = u_n v_n$, $\forall n \geq 0$. In the next proposition, we write $x \sim y$ to mean that the powers of 2 dividing the integers x and y are the same.

Proposition 2.4. *For all integers $n \geq 0$ we have that i) u_{2n+1} is odd, and ii) $u_{2n} \sim n(q+1)$.*

Proof. First we prove i) by induction on n. If $n = 0$, then $u_{2n+1} = u_1 = 1$ is odd. Assuming u_{2n+1} is odd for some $n \geq 0$ then $u_{2n+3} = (q+1)u_{2n+2} - qu_{2n+1} \equiv -qu_{2n+1} \equiv 1 \pmod 2$ and we are done. We then prove ii) by induction on $\nu_2(n)$. And we prove the initial step $\nu_2(n) = 0$ itself by induction on the odd integers $n \geq 1$. For $n = 1$ we have $u_{2n} = u_2 = q+1 \sim n(q+1) = q+1$. Assume $u_{2n} \sim q+1$ for some odd n, then by the addition formula we have $2u_{2n+4} = u_{2n}v_4 + u_4 v_{2n}$. Now for any integer $k \geq 0$ the integer v_k is even and $v_{2k} = (q^2)^k + 1 \equiv 1^k + 1 \equiv 2 \pmod 4$ satisfies $v_{2k} \sim 2$. Hence $u_{2n}v_4 \sim 2(q+1)$ while $u_4 v_{2n} = u_2 v_2 v_{2n} \sim 2(q+1)v_2$ so the power of 2 in $u_4 v_{2n}$ is larger than the power of 2 in $u_{2n}v_4$. Therefore $u_{2n+4} \sim q+1$ and the case $\nu_2(n) = 0$ holds. So let us assume ii) is true for any n with $\nu_2(n) = k \geq 0$. Then if n is such that $\nu_2(n) = k+1$, write $n = 2m$. We have using the inductive hypothesis $u_{2n} = u_{4m} = u_{2m}v_{2m} \sim 2u_{2m} \sim 2m(q+1) \sim n(q+1)$. □

We restate Proposition 2.4 as a lemma in a form that will be of direct use throughout the paper.

Lemma 2.5. *Let $q = p^e$, where p is an odd prime and n an integer ≥ 1. Then*

$$\nu_2(q^n-1) = \begin{cases} \nu_2(q-1), & \text{if } n \text{ is odd,} \\ \nu_2(q^2-1) + \nu_2(n) - 1, & \text{if } n \text{ is even.} \end{cases}$$

Notation. We will denote by m the arithmetic function of $n \geq 1$ defined by $m(n) = \nu_2(q^n-1)$.

Remark 2.6. By Lemma 2.5, $m(n)$ depends only on $\nu_2(n)$.

3. Computation of δ_q via a method analogous to Hasse's

In the proofs of Theorems 3.1 and 3.2, whenever the argument of the function m is dropped, we mean $m(2^k)$.

Theorem 3.1. *For all integers $k \geq 0$ the sets $S_q(k)$ have a Dirichlet density $\delta(S_q(k))$ where*

$$\delta(S_q(k)) = \frac{1}{2^{k+1}}.$$

Proof. Given the prime p, our reckonings take place within a fixed algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. The sets $S_q(k),\ k = 0, 1, 2, \ldots$, partition the set I of primes of $\mathbb{F}_q[X]$. By Remark 2.6, the function $\nu_2(|P| - 1) = \nu_2(q^{\deg P} - 1)$ of the prime P depends only on k. In fact, for $P \in S_q(k)$, $\nu_2(|P| - 1) = m(2^k)$. And we have, for the ideal P, the equivalence

(3.1)

$$P \in S_q(k) \iff P \text{ splits completely in } K(\zeta_{2^m}),\ \text{but not in } K(\zeta_{2^{1+m}}).$$

Indeed, $P \in S_q(k)$ if and only if 2^m, but not 2^{m+1}, divides the order of the cyclic group $\left(\mathbb{F}_q[X]/P\right)^*$, or -1 is a 2^{m-1}-th power, but not a 2^m-th power in that cyclic group, or equivalently $Y^{2^{m-1}} + 1 = 0$ is solvable in $\mathbb{F}_q[X] \pmod P$, but $Y^{2^m} + 1 = 0$ is not solvable. So that, applying Prop. 2.1 yields (3.1). Now by the Kronecker Density Theorem

$$\delta(S_q(k)) = [K(\zeta_{2^m}) : K]^{-1} - [K(\zeta_{2^{1+m}}) : K]^{-1}. \tag{3.2}$$

But the dimension $[K(\zeta_{2^m}) : K]$ is also the degree of the extension $\mathbb{F}_q(\zeta_{2^m})$ over $\mathbb{F}_q$ (see Lemma 3.1.10 p. 64 of [Sti]).

Now the largest primitive 2^x-th root of unity, ζ_{2^x} in $\mathbb{F}_{q^{2^k}}$ corresponds to $x = m(2^k)$. Indeed $\mathbb{F}^*_{q^{2^k}}$ has order $q^{2^k} - 1$. And ζ_{2^m} is a primitive element of $\mathbb{F}_{q^{2^k}}/\mathbb{F}_q$ since a proper subfield of this extension (if any), i.e. any $\mathbb{F}_{q^{2^\ell}}$, $\ell < k$, has $m(2^\ell) < m(2^k)$ by Lemma 2.5. Therefore $\mathbb{F}_{q^{2^k}} = \mathbb{F}_q(\zeta_{2^{m(2^k)}})$ so that, by (3.2) and the remark that follows (3.2), we have $\delta(S_q(k)) = 2^{-k} - 2^{-k-1} = 2^{-k-1}$. □

Definition. Define $O_q(k)$ as $\{P \in S_q(k)$; order of $X \pmod P$ is odd$\}$ and O_q as $\bigcup_{k\geq 0} O_q(k)$. The complement of $O_q(k)$ in $S_q(k)$ is $E_q(k) = \{P \in S_q(k)$; order of $X \pmod P$ is even$\}$.

Theorem 3.2. *The sets $O_q(k)$ have a Dirichlet density $\delta(O_q(k))$ where*

$$\delta(O_q(k)) = 2^{-m(2^k)-k-1} = \begin{cases} 2^{-\nu_2(p-1)-1}, & \text{if } e \text{ is odd and } k = 0, \\ 2^{-\nu_2(p^2-1)-\nu_2(e)-2k}, & \text{otherwise.} \end{cases}$$

Proof. Let P be a prime of degree n in $S_q(k)$. Then to say that X has odd order $\pmod P$ means that $X^{\frac{|P|-1}{2^m}} \equiv 1 \pmod P$, or that there is a solution $Y \in \mathbb{F}_q[X]$ satisfying $Y^{2^m} - X \equiv 0 \pmod P$, or again by Prop. 2.1 that the ideal P splits completely in $L_k = K(\zeta_{2^m}, \sqrt[2^m]{X})$, but not completely in $L_k(\zeta_{2^{m+1}})$ since $P \in S_q(k)$. Now we have $[L_k : K] = [L_k : K(\zeta_{2^m})] \times [K(\zeta_{2^m}) : K] = 2^m \times [K(\zeta_{2^m}) : K]$, and by the proof of Theorem 3.1 we conclude that $[L_k : K] = 2^m \times 2^k$, and also that $L_k(\zeta_{2^{m+1}})$ is a quadratic extension of L_k. Hence, by the Kronecker Density Theorem, we get $\delta(O_q(k)) = 2^{-1} \times 2^{-m(2^k)-k}$. By Lemma 2.5, if $k = 0$ and e is odd, then $m(2^k) = \nu_2(q^n - 1) = \nu_2(q - 1) = \nu_2(p - 1)$ and otherwise

$m(2^k) = \nu_2(p^{ne}-1) = \nu_2(p^2-1) + \nu_2(ne) - 1 = \nu_2(p^2-1) + k + \nu_2(e) - 1$ so that $\delta(O_q(k))$ has the announced density. □

Remark. Because Dirichlet densities are finitely additive we deduce that $E_q(k)$ possesses such a density, namely $\delta(S_q(k)) - \delta(O_q(k))$.

Finally we compute the densities δ_q.

Theorem 3.3. *The Dirichlet density δ_q of the set O_q of primes P in $\mathbb{F}_q[X]$ for which the order of $X \pmod P$ is odd exists and is*

$$\delta_q = \begin{cases} 1, & \text{if } p = 2, \\ 2^{-\nu_2(p-1)-1} + 3^{-1} \cdot 2^{-\nu_2(p^2-1)}, & \text{if } e \text{ is odd}, \\ 3^{-1} \cdot 2^{-\nu_2(p^2-1)-\nu_2(e)+2}, & \text{if } e \text{ is even}. \end{cases}$$

Proof. If $p = 2$ then the cyclic group $(\mathbb{F}_q[X]/P)^*$ is of odd order $2^{e \deg P} - 1$. So every element has odd order, in particular X. Since X has odd order $\pmod P$ for any prime $P \in \mathbb{F}_q[X]$, we have $\delta_q = 1$. For odd p, we claim that δ_q exists and is the infinite sum $\sum_{k\geq 0} \delta(O_q(k))$ (Dirichlet densities are finitely additive and since $\sum_{k\geq 0} \delta(O_q(k))$ converges, the lower density is at least the sum of the series, but a similar reasoning holds for primes for which X has even order which is the complementary set). Thus for e odd, we have $\delta_q = 2^{-\nu_2(p-1)-1} + \sum_{k\geq 1} 2^{-\nu_2(p^2-1)-2k}$ and for e even we also get δ_q by summing a geometric series of common ratio $1/4$. □

Remark. It does not take long to check that for p not 2, δ_q is at most $\frac{1}{4} + \frac{1}{24} = \frac{7}{24}$ and that this upper bound is reached exactly for q an odd power of a prime $p \equiv 3 \pmod 8$ (as claimed in the introduction).

Remark 3.4. In the classical Hasse method, odd primes p are partitioned into sets $\mathcal{P}^j$, $j = 1, 2, 3, \ldots$, where $\mathcal{P}^j = \{p;\ \nu_2(p-1) = j\}$. Then for a fixed $j \geq 1$, necessary and sufficient splitting conditions on p in $\mathcal{P}^j$ are established for the order of $2 \pmod p$ to be odd, yielding for each j, as in Theorem 3.2 for each k, a sub-density d^j. To compute the density of O_q in the ring $\mathbb{F}_q[X]$ we computed the sub-densities of O_q within sets of primes P having a fixed power of 2 in their degree n. By Lemma 2.5, the power of 2 in $q^n - 1$ is a simple linear (or nearly linear with slope 1) function of the power of 2 in the degree n. But $q^n - 1 = |P| - 1$. Thus, our approach replaces the $p - 1$ of the Hasse method of the classical setting by $|P| - 1$, a rather close analogue.

4. An elementary calculation of the densities based on counting primes

For any integer $n \geq 1$, let F_n be the number of elements of odd order in the multiplicative group $\mathbb{F}_{q^n}^*$ and let G_n be the number of primitive elements of the extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ which have odd order in $\mathbb{F}_{q^n}^*$. Note that the

F_n elements of odd order in $\mathbb{F}_{q^n}^*$ form a subgroup of $\mathbb{F}_{q^n}^*$. We recall that the number I_n of primes $P \in \mathbb{F}_q[X]$ of degree n is given by the formula $I_n = \frac{1}{n}\sum_{d \mid n} \mu(d) q^{n/d}$, where μ is the Moebius function (see for instance [Ro], Chap. 2).

Lemma 4.1. *Let $\alpha \in \overline{\mathbb{F}}_q$ of degree n over $\mathbb{F}_q$ and let P denote the minimal polynomial of α over $\mathbb{F}_q$. Then*

α has odd order in the multiplicative group of the field $\mathbb{F}_q(\alpha)$ if and only if $P \in O_q$.

Proof. Since $\mathbb{F}_q(\alpha) \simeq \mathbb{F}_{q^n}$, α has odd order in $\mathbb{F}_{q^n}^*$ if and only if α is a root of $X^{F_n} - 1$ or equivalently P divides $X^{F_n} - 1$ in $\mathbb{F}_q[X]$, that is to say $P \in O_q$. □

Lemma 4.2. *For any prime power q and any integer $n \geq 2$, we have the double inequality*

$$q^n - \frac{q}{q-1} q^{n/2} < nI_n < q^n.$$

Proof. Not every element of $\mathbb{F}_{q^n}$ is a root of an irreducible polynomial of degree n, therefore $nI_n < |\mathbb{F}_{q^n}| = q^n$. Also

$$\begin{aligned} q^n - nI_n &= \Big| \sum_{1 < d \mid n} \mu(d) q^{n/d} \Big| \\ &\leq \sum_{k=1}^{n/2} q^k, \text{ since } \frac{n}{d} \leq \frac{n}{2}, \\ &< \frac{q}{q-1} q^{n/2}, \text{ implying the other inequality.} \end{aligned}$$

□

Theorem 4.3. *Assume $q = p^e$, p an odd prime and $e \geq 1$. Let Ω_n be the number of primes in O_q of degree n. Then the ratio Ω_n / I_n satisfies*

$$\begin{cases} \frac{\Omega_n}{I_n} = 2^{-m(n)}, & \text{if } n \text{ is odd} \geq 3, \\ 2^{-m(n)} - \frac{q}{2(q-1)} q^{-n/2} < \frac{\Omega_n}{I_n} < 2^{-m(n)} + \frac{q}{8(q-2)} q^{-n/2}, & \text{if } n \text{ is even,} \end{cases}$$

Proof. Since an element of a cyclic group of order x has odd order if and only if it belongs to the unique subgroup of order $2^{-\nu_2(x)} \cdot x$, we have $F_n = 2^{-\nu_2(q^n-1)} \cdot (q^n - 1) = 2^{-m(n)}(q^n - 1)$. To compute G_n observe that $F_n = \sum_{d \mid n} G_d$. So by the Moebius inversion formula we have $G_n = \sum_{d \mid n} \mu(d) F_{n/d}$. And by Lemma 4.1 we have $\Omega_n = G_n / n$.

Assume first that n is odd ≥ 3. Then any divisor d of n is odd and therefore $m(d) = m(1) = m(n)$ by Remark 2.6. Hence

$$G_n = 2^{-m(n)} \sum_{d \,|\, n} \mu(d)(q^{n/d} - 1)$$

$$= 2^{-m(n)} \sum_{d \,|\, n} \mu(d) q^{n/d} - 2^{-m(n)} \sum_{d \,|\, n} \mu(d), \tag{4.1}$$

yielding $G_n = 2^{-m(n)} \sum_{d \,|\, n} \mu(d) q^{n/d}$, since $n > 1$ implies $\sum_{d \,|\, n} \mu(d) = 0$. And $\Omega_n = G_n/n = 2^{-m(n)} I_n$ implies $\Omega_n / I_n = 2^{-m(n)}$.

Assume now that n is even. Then

$$G_n = \sum_{d \,|\, n} \mu(d) F_{n/d} = \sum_{d \,|\, n} \mu(d) 2^{-m(n/d)} q^{n/d} - \sum_{d \,|\, n} \mu(d) 2^{-m(n/d)}$$

$$\geq 2^{-m(n)} q^n - 2^{-m(n/2)} q^{n/2} + \sum_{d \,|\, n,\, d \geq 3} \mu(d) 2^{-m(n/d)} q^{n/d} - 1/2,$$

since $0 \leq \sum_{d \,|\, n} \mu(d) 2^{-m(n/d)} \leq 1/2$. Indeed,

$$\sum_{d \,|\, n} \mu(d) 2^{-m(n/d)} = \sum_{d \,|\, 2l+1} \mu(d) 2^{-m(1)} - \sum_{d \,|\, 2l+1} \mu(d) 2^{-m(2)}$$

$$= \begin{cases} 0, & \text{if } l \geq 1, \\ 2^{-m(1)} - 2^{-m(2)}, & \text{if } l = 0, \end{cases}$$

where $2l + 1 = 2^{-\nu_2(n)} n$. But $0 < 2^{-m(1)} - 2^{-m(2)} < 2^{-m(1)} \leq 1/2$.

Proceeding as in Lemma 4.2, we get for n even

$$\xi(n) \doteq \Big| \sum_{d \,|\, n,\, d \geq 3} \mu(d) 2^{-m(n/d)} q^{n/d} \Big| \leq \frac{1}{2(q-1)} q^{n/2} - \frac{1}{2}.$$

One can check directly the above inequality for $n = 2$ and 4, whereas for $n \geq 6$ observe that

$$\xi(n) \leq \frac{1}{2} \sum_{k=1}^{n/3} q^k \leq \frac{q^{n/3+1} - q}{2(q-1)} \leq \frac{q^{n/2}}{2(q-1)} - \frac{1}{2}.$$

Hence, using $-2^{-m(n/2)} \geq -1/2$, we have

$$G_n \geq 2^{-m(n)} q^n - 2^{-m(n/2)} q^{n/2} - \left(\frac{q^{n/2}}{2(q-1)} - \frac{1}{2} \right) - \frac{1}{2}$$

$$\geq 2^{-m(n)} q^n - \frac{q}{2(q-1)} q^{n/2}.$$

On the other hand, $G_n \le 2^{-m(n)}q^n - \zeta(n)$, where $\zeta(n) \doteq 2^{-m(n/2)}q^{n/2} - \sum_{d \,|\, n,\, d\ge 3} \mu(d)2^{-m(n/d)}q^{n/d}$. But

$$\begin{aligned}\zeta(n) &> 2^{-m(n/2)}q^{n/2} - \sum_{d \,|\, n,\, d\ge 6} \mu(d)2^{-m(n/d)}q^{n/d} \\ &\ge 2^{-m(n/2)}q^{n/2} - 2^{-m(n/2)} \sum_{k=1}^{n/6} q^k, \text{ which is } > 0,\end{aligned}$$

since $q^{n/2} > \sum_{k=1}^{n/6} q^k$ for $n \ge 6$, and where, in the above, we used $\mu(3) = \mu(5) < 0$, $\mu(d) = 0$, if $4 \mid d$, and $2^{-m(n/2)} > 2^{-m(n)}$. Therefore $G_n < 2^{-m(n)}q^n$.

Using the previous inequalities on G_n and Lemma 4.2 we get

$$\frac{2^{-m(n)}q^n - \frac{q}{2(q-1)}q^{n/2}}{q^n} < \frac{\Omega_n}{I_n} = \frac{G_n}{nI_n} < \frac{2^{-m(n)}q^n}{q^n - \frac{q}{q-1}q^{n/2}},$$

or

$$\begin{aligned}2^{-m(n)} - \frac{q}{2(q-1)}q^{-n/2} < \frac{\Omega_n}{I_n} &< 2^{-m(n)}\left(1 - \frac{q}{q-1}q^{-n/2}\right)^{-1} \\ &< 2^{-m(n)}\left(1 + \frac{q}{q-2}q^{-n/2}\right),\end{aligned}$$

where the rightmost inequality above is obtained by writing $1/(1-x) = 1 + x + x \cdot x/(1-x)$ with $x = \frac{q}{q-1}q^{-n/2}$ and having $\frac{x}{1-x} \le \frac{1/(q-1)}{1-1/(q-1)} = \frac{1}{q-2}$, since $q^{n/2} \ge q$. We get the announced estimate by noting that n even implies $m(n) \ge 3$, so that $\Omega_n/I_n < 2^{-m(n)} + \frac{q}{8(q-2)}q^{-n/2}$. □

We state a fact mentioned in our introduction as a corollary of Theorem 4.3.

Corollary 4.4. *The relative density ratio $\delta(O_q(k))/\delta(S_q(k))$ when $k = 0$ is more than a density since it is the exact proportion of primes in O_q within the set of primes of a given odd degree $n \ge 3$, i.e. $\delta(O_q(0))/\delta(S_q(0)) = \Omega_n/I_n$, for any odd $n \ge 3$.*

Proof. By Theorem 4.3 the ratio $\frac{\Omega_n}{I_n} = 2^{-m(n)}$ which by looking at Theorems 3.1 and 3.2 is the ratio $\delta(O_q(k=0))/\delta(S_q(k=0))$. □

Remark 4.5. For $n = 1$, $\sum_{d \,|\, n} \mu(d) = 1$, so by (3.1) we get $G_1 = 2^{-m(1)}(I_1 - 1) = 2^{-m(1)}(q-1)$, instead of $2^{-m(1)}q$. That we get $q-1$ instead of q comes from the fact that there are only $q-1$ primes of degree 1 for which the order of $X \pmod P$ is defined, namely $P = X - a$, for $a \in \mathbb{F}_q^*$. The ratio Ω_1/I_1 is again $2^{-m(1)}$ provided one only considers these $q-1$

primes. Indeed, $X \equiv a \pmod{X-a}$ implies the order of $X \pmod{X-a}$ is the order of a in $\mathbb{F}_q^*$. This order is odd if and only if a belongs to the subgroup of $\mathbb{F}_q^*$ of order $2^{-\nu_2(q-1)} \cdot (q-1) = 2^{-m(1)}(q-1)$ (a trivial case of Lemma 4.1). Thus, $\Omega_1/I_1 = 2^{-m(1)}(q-1)/q = 2^{-m(1)} - q^{-1}2^{-m(1)}$.

Remark 4.6. The numerical table below gives for $q = 3$ and each degree n from 1 to 11 the values of I_n, Ω_n and r_n, where Ω_n is the number of primes in O_3 of degree n and r_n is the n-th approximant to $d_3 = \delta_3$. See §1.2 for the definition of the r_n's. They are given here with 4 decimal places of accuracy.

n	1	2	3	4	5	6	7	8	9	10	11
I_n	3	3	8	18	48	116	312	810	2184	5880	16104
Ω_n	1	0	4	1	24	13	156	25	1092	726	8052
r_n	.3333	.1666	.2777	.2222	.2777	.2506	.2859	.2540	.2813	.2655	.2868

The Ω_n's can be obtained by asking some mathematical software to factor $X^t - 1 \pmod 3$ for various t's. But they can be computed directly by observing that if X has odd order modulo a prime P of degree n, then P must be a factor of some $X^m - 1$, where m is a factor of F_n, the largest odd factor in $q^n - 1$. One only considers those factors m for which the order of $q \pmod m$ is n. For in that case, the m-th cyclotomic polynomial $\Phi_m(X)$ factors into $\varphi(m)/n$ primes in Ω_n, where φ is Euler's totient function. As an example consider $q = 3$ and $n = 8$. Then $3^8 - 1 = 2^5 \times 5 \times 41$. So F_8 is 5×41. Since 3 has order 8 modulo 5×41 and modulo 41, there are $(4 \cdot 40)/8 + 40/8 = 25$ primes of degree 8 for which X has odd order.

It is of interest to see how the successive r_n's approach the asymptotic density $\delta_3 = 7/24$ which is about 0.2917.

Using Theorem 4.3 and the remarks about natural and Dirichlet densities made in §2.2, we give a purely elementary proof of Theorem 3.3. By "elementary", we mean not using the Kummer-Dedekind Theorem, nor the Kronecker Density Theorem. This is a major difference from the classical case. In fact, the method we follow yields an effective theorem in which we precise how the sequence of approximants (r_n) converges to the natural density d_q.

Theorem 4.7. *For any $N \geq 1$, we have, uniformly for any odd prime power $q = p^e$, $e \geq 1$,*

$$|r_N - \delta_q| < \frac{3}{4N},$$

where r_N is the N-th approximant $N^{-1}\sum_{n=1}^{N} \Omega_n/I_n$, δ_q is the Dirichlet density $\sum_{k\geq 0} 2^{-k-1-m(2^k)}$ of the set O_q found in Theorems 3.2 and 3.3. In particular, O_q has a natural density $d_q = \lim_N r_N$ equal to δ_q.

Proof. We show that the set of primes O_q possesses a natural density $d_q = \sum_{k\geq 0} 2^{-k-1}2^{-m(2^k)}$. It then follows that O_q has Dirichlet density $\delta(O_q) =$

d_q. Since $d_q = lim_N N^{-1} \sum_{n=1}^{N} \Omega_n/I_n$, if the limit exists, we consider a sum $S_N = \sum_{n=1}^{N} \Omega_n/I_n$. Because Ω_n/I_n depends essentially on $k = \nu_2(n)$, we need to estimate the number of integers n between 1 and N of the form $2^k(2l+1)$ for a fixed $k \geq 0$. Solving for l the inequality $2^k(2l+1) \leq N$ yields $0 \leq l \leq \frac{N-2^k}{2^{k+1}}$. Thus there are $\left\lfloor \frac{N+2^k}{2^{k+1}} \right\rfloor$ integers n with $\nu_2(n) = k$ between 1 and N. But using Theorem 4.3 which, in particular, for n even implies that $|\Omega_n/I_n - 2^{-m(n)}| < .5q(q-1)^{-1}q^{-n/2}$ and the end of Remark 4.5, we get

$$S_N = \sum_{k\geq 0} \left\lfloor \frac{N+2^k}{2^{k+1}} \right\rfloor 2^{-m(2^k)} + C_N, \tag{4.2}$$

where $|C_N| \leq .5q(q-1)^{-1} \sum_{n \text{ even} \leq N} q^{-n/2} - 2^{-m(1)}q^{-1}$.

Note that $-\frac{1}{2} \leq \frac{N}{2^{k+1}} - \left\lfloor \frac{N+2^k}{2^{k+1}} \right\rfloor < \frac{1}{2}$ so that replacing the integer value expressions $\left\lfloor \frac{N+2^k}{2^{k+1}} \right\rfloor$ in (4.2) by $2^{-k-1}N$ causes an error on S_N no greater than $2^{-1} \sum_{k\geq 0} 2^{-m(2^k)}$. Thus $S_N = N \sum_{k\geq 0} 2^{-k-1} 2^{-m(2^k)} + E_N$, where

$$|E_N| \leq 2^{-1} \sum_{k\geq 0} 2^{-m(2^k)} + .5q/(q-1) \sum_{n \text{ even} \leq N} q^{-n/2} - 2^{-m(1)}q^{-1}.$$

But $.5q/(q-1) \sum_{n \text{ even} \leq N} q^{-n/2} \leq \frac{q}{2(q-1)} \frac{q^{-1}}{1-q^{-1}} = .5q(q-1)^{-2}$ and

$2^{-1} \sum_{k\geq 0} 2^{-m(2^k)} = 2^{-1}\big(2^{-m(1)} + \sum_{k\geq 1} 2^{-m(2^k)}\big) = 2^{-1-m(1)} + 2^{-m(2)}$. Therefore,

$$\begin{aligned} |E_N| &\leq .5q(q-1)^{-2} + [2^{-1-\nu_2(q-1)} + 2^{-\nu_2(q^2-1)}] - 2^{-\nu_2(q-1)}q^{-1} \\ &< \frac{3}{8} + \left[\frac{1}{4} + \frac{1}{8}\right] - 0 = \frac{6}{8}. \end{aligned} \tag{4.3}$$

Dividing $S_N = N \sum_{k\geq 0} 2^{-k-1} 2^{-m(2^k)} + E_N$ through by N yields the theorem. □

Remark 4.8. The bound on $|E_N|$ given in (4.3) is better than 3/4 for most q's.

5. The classical 1:2 odds revisited and why the choice of X is a representative choice

Definition. (Arithmetic density of a set of monic polynomials) The arithmetic (or natural) density of a set $A \subset \mathbb{N}$ is defined, if it exists, as $d(A) = \lim_{N\to\infty} N^{-1}A_N$, where A_N is the number of natural integers in A and $\leq N$. Note that $d(A) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{\chi_A(n)}{1}$, where χ_A is the characteristic function of A. Analogously, we propose to define, if it exists, the

arithmetic density of a set S of monic polynomials in $\mathbb{F}_q[X]$ as the limit $d(S) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \frac{S(n)}{q^n}$, where $S(n)$ is the number of elements of S of degree n. Here q^n stands for the number of monic polynomials in $\mathbb{F}_q[X]$ of degree n, or of norm q^n.

5.1. A heuristic for the expected odds in the classical case. We start by recalling a fact which is familiar to people in the field of Lucas sequences: For "most" Lucas sequences $U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, the density of primes p with odd rank $r(p)$ in (U_n) is $\frac{1}{3}$ (see [Ba1, Lag, Lax, Mo1] and [M-S]). Here α and β are the roots of a quadratic $X^2 - aX + b \in \mathbb{Z}[X]$. The rank $r(p)$ is the least integer $r \geq 1$ such that $p \mid U_r$; it always exists if $p \nmid 2b$. Although with the existing results in the area this fact could be turned into an explicit theorem, our intention is merely to provide an informal argument aimed at *understanding*. Why do primes first divide (U_n) twice more often at even indices?

Let us only consider Lucas sequences of the type $\frac{a^n - 1}{a - 1}$ where $a \in \mathbb{Z}$. Here $r(p)$ is the order of $a \pmod p$. And assume for simplicity that a is a positive integer. Let δ_a denote the density of primes p for which order of $a \pmod p$ is odd. From Theorem 3.1.3 of [Ba1] one can deduce that for any $a \in A$, $\delta_a = \frac{1}{3}$, where $A = \{a \in \mathbb{Z}_{\geq 1};\ a = 2^d \cdot m,\ \text{where } d \geq 0 \text{ and } m \text{ is a non-square odd integer}\}$. Since the arithmetic density of A is one, we get that $\lim_{N\to\infty} \frac{1}{N} \sum_{a=1}^{N} \delta_a = \frac{1}{3}$. This is a proof, but it required the knowledge of the existence and the value of the δ_a's. Let us now compute the average order of $a \pmod p$ from a dual point of view. Instead of fixing an a and counting primes for which a has odd order, let us fix a prime p and evaluate the proportion $\alpha(p)$, in terms of arithmetic density, of positive integers a having odd order $\pmod p$. In computing $\alpha(p)$, we discard integers a divisible by p. For $j \geq 1$, let $\mathcal{P}^j$ be the set $\{p \text{ prime } ;\ \nu_2(p-1) = j\}$. If $p \in \mathcal{P}^j$, then an integer a prime to p has odd order $\pmod p$ if and only if a is in the unique subgroup of order $\frac{p-1}{2^j}$ of $(\mathbb{Z}/p)^*$. Hence $\alpha(p) = \frac{1}{2^j}$. So it is never $\frac{1}{3}$. But what about the average over all p's? By the Dirichlet Density Theorem each $\mathcal{P}^j$ possesses a density $\delta(\mathcal{P}^j) = \frac{1}{2^j}$, so it seems reasonable[1] to assign to each possible value of $\alpha(p)$ a weight equal to the "probability" that p be in $\mathcal{P}^j$, i.e. $\delta(\mathcal{P}^j)$. Then this average is

$$\sum_{j\geq 1} \delta(\mathcal{P}^j) \cdot \frac{1}{2^j} = \sum_{j\geq 1} \frac{1}{4^j} = \frac{1}{4} \cdot \frac{1}{1 - 1/4} = \frac{1}{3}\ !$$

Remark. Had we considered the proportion $\beta(p)$, in terms of Dirichlet density, of *primes* q for which order of $q \pmod p$ is odd, rather than the proportion $\alpha(p)$ of positive integers a, then the Dirichlet Density Theorem

[1] And it can be proved. See the argument used in the proof of Theorem 6.1

would have given $\beta(p) = \alpha(p)$ and therefore we would have obtained an expected probability of $\frac{1}{3}$ again.

5.2. Expected odds in $\mathbb{F}_q[X]$. Let P be a prime of $\mathbb{F}_q[X]$ of degree d. Let $R \in \mathbb{F}_q[X]$ be of degree $< d$. Then $\mathcal{A} = \{M \in \mathbb{F}_q[X];\ M \text{ is monic and } M \equiv R \pmod P\}$ has an arithmetic density. Indeed suppose n is any integer $\geq d$. Then M of degree n belongs to $\mathcal{A}$ if and only if $M = R + \Lambda P$ with Λ a monic polynomial of degree $n - d$. Hence $d(\mathcal{A}) = \frac{q^{n-d}}{q^n} = \frac{1}{|P|}$.

To emulate what we did in **5.1** let $\alpha(P)$ be the proportion, in terms of arithmetic density, of monic polynomials M in $\mathbb{F}_q[X]$ for which the order of $M \pmod P$ is odd. In evaluating $\alpha(P)$ we discard those M divisible by P. Hence there are $|P| - 1$ disjoint sets of arithmetic density $1/|P|$ corresponding to the $|P| - 1$ classes in $(\mathbb{F}_q[X]/P)^*$. Exactly $\frac{|P|-1}{2^{\nu_2(|P|-1)}}$ have odd order $\pmod P$. Hence $\alpha(P) = 1/2^{\nu_2(|P|-1)}$.

As noticed in Section 3 the function $\alpha(P)$ is constant on $S_q(k)$. Thus as above we write that the average of the $\alpha(P)$ as P varies through the primes of $\mathbb{F}_q[X]$ is

$$\sum_{k\geq 0} \delta(S_q(k)) \cdot \alpha(P \in S_q(k)) = \sum_{k\geq 0} \frac{1}{2^{k+1}} \cdot \frac{1}{2^{m(k)}} = \sum_{k\geq 0} \delta(O_q(k)) = \delta_q! \tag{5.1}$$

Thus the polynomial X, unlike the prime 2 of Sierpinski, behaves like a typical polynomial.

Remark. By the Dirichlet Density Theorem the set $\{Q \in \mathbb{F}_q[X];\ Q \text{ prime and } Q \equiv R \pmod P\}$, where R is a representative of a class in $(\mathbb{F}_q[X]/P)^*$, has a density $= \frac{1}{\Phi(P)} = \frac{1}{q^d-1}$. Thus the sum in (5.1) can be interpreted as the "probability" that, given P and $Q \in \mathbb{F}_q[X]$, the order of $Q \pmod P$ be odd.

6. Density averages

Definition. In this Section we write $\delta(p, e)$ for the density δ_q, where $q = p^e$. Let $p_1 = 3, p_2 = 5, \ldots, p_n, \ldots$ denote the odd rational primes in their natural increasing order. Since a density $\delta(p_n, e)$ is associated to each prime power p_n^e, we define most naturally the average $\delta(-, e)$ of the densities $\delta(p, e)$ over all primes p by the limit $\lim_{N\to\infty} N^{-1} \sum_{n=1}^{N} \delta(p_n, e)$ if it exists. Similarly we define $\delta(p, -)$ to be $\lim_E E^{-1} \sum_{e=1}^{E} \delta(p, e)$, and the average over all $q's$, $\delta(-, -)$, as $\lim_N N^{-2} \sum_{n=1}^{N} \sum_{e=1}^{N} \delta(p_n, e)$, if these limits exist.

Theorem 6.1. *The average densities defined above all exist and are given, for odd p, by the formulas*

$$\delta(-,e) = \begin{cases} \frac{7}{36}, & \text{if } e \text{ is odd,} \\ 2^{-\nu_2(e)} \cdot \frac{4}{36}, & \text{if } e \text{ is even,} \end{cases}$$

$$\delta(p,-) = 36^{-1}[9 \cdot 2^{-\nu_2(p-1)} + 14 \cdot 2^{-\nu_2(p^2-1)}]$$

and

$$\delta(-,-) = \frac{5^2}{6^3} = \frac{4+\frac{1}{6}}{36}.$$

Proof. We only prove the formula for $\delta(-,e)$, since the other cases can be computed in similar fashion. Note in passing that both limits

$$\lim_N N^{-1} \sum_{n=1}^{N} \delta(p_n,-) \quad \text{and} \quad \lim_E E^{-1} \sum_{e=1}^{E} \delta(-,e)$$

turn out to also be equal to $\delta(-,-)$. So assume e to be a fixed integer ≥ 1.

Let $\mathcal{P}^u = \{p;\ \nu_2(p-1) = u\}$ and $\mathcal{P}^v_+ = \{p;\ \nu_2(p+1) = v\}$ for u and v integers ≥ 1. By the Dirichlet Density Theorem for primes in arithmetic progressions, we have $\delta(\mathcal{P}^u) = 2^{-u}$ and $\delta(\mathcal{P}^v_+) = 2^{-v}$, since for example $p \in \mathcal{P}^u \iff p \equiv 1 + 2^u \pmod{2^{u+1}}$ and $\varphi(2^{u+1}) = 2^u$. The constant values of $\delta(p,e)$ on each $\mathcal{P}^u$, $u \geq 2$, and on each $\mathcal{P}^v_+$, $v \geq 2$, are denoted respectively by δ^u and δ^v_+. Since primes in arithmetic progressions have a natural density d equal to their Dirichlet density ([Pra], Chap. 5), we have $d(\mathcal{P}^u) = 2^{-u}$ and $d(\mathcal{P}^v_+) = 2^{-v}$.

Theorem 3.3 gives the values of δ^u and δ^v_+ for $u \geq 2$ and $v \geq 2$. We claim that the contribution of primes $p \equiv 1 \pmod 4$ to $\delta(-,e)$ is $\sum_{u\geq 2} \delta(\mathcal{P}^u) \cdot \delta^u$. For instance if e is odd, it is $\sum_{u\geq 2} 2^{-u} \cdot 3^{-1} 2^{-u+1} = \frac{1}{18}$. And the contribution of primes $p \equiv -1 \pmod 4$ is $\sum_{v\geq 2} \delta(\mathcal{P}^v_+)\delta^v_+$. For e odd, it is $\sum_{v\geq 2} 2^{-v} \cdot (4^{-1} + 3^{-1}2^{-1-v}) = \frac{5}{36}$. Hence, for e odd, $\delta(-,e) = \frac{2}{36} + \frac{5}{36}$.

To prove the above claim, let $M_N = \frac{1}{N}\sum_{n=1}^{N} \delta(p_n,e)$ be the average of the $\delta(p,e)$'s over the first N odd primes. First we show that $\liminf M_N \geq l$ and then that $l \geq \limsup M_N$, where $l = \sum_{u\geq 2} \delta(\mathcal{P}^u)\delta^u + \sum_{v\geq 2} \delta(\mathcal{P}^v_+)\delta^v_+$. Let $\mathcal{P}^u(N)$ and $\mathcal{P}^v_+(N)$ be the number of indices n, $1 \leq n \leq N$, such that $p_n \in \mathcal{P}^u$ and respectively $p_n \in \mathcal{P}^v_+$. Since $M_N = \sum_{u\geq 2} \frac{\mathcal{P}^u(N)}{N}\delta^u + \sum_{v\geq 2} \frac{\mathcal{P}^v_+(N)}{N}\delta^v_+ \geq M_N(U,V)$, $\forall U \geq 2$, $V \geq 2$, where

$$M_N(U,V) = \sum_{u=2}^{U} \frac{\mathcal{P}^u(N)}{N}\delta^u + \sum_{v=2}^{V} \frac{\mathcal{P}^v_+(N)}{N}\delta^v_+,$$

we get as $N \to \infty$, $\liminf M_N \geq \sum_{u=2}^{U} d(\mathcal{P}^u)\delta^u + \sum_{v=2}^{V} d(\mathcal{P}_+^v)\delta_+^v$, for any U and any $V \geq 2$. Letting U and V go to ∞, the last inequality yields $\liminf M_N \geq l$.

On the other hand for any U and $V \geq 2$,

$$\begin{aligned} M_N &= M_N(U,V) + \frac{1}{N}\Big[\sum_{u>U} \mathcal{P}^u(N)\delta^u + \sum_{v>V} \mathcal{P}_+^v(N)\delta_+^v\Big] \\ &\leq M_N(U,V) + \frac{1}{N}\sum_{u>U} \mathcal{P}^u(N) + \frac{1}{N}\sum_{v>V} \mathcal{P}_+^v(N). \end{aligned}$$

Now $\lim_N \frac{1}{N}\sum_{u>U} \mathcal{P}^u(N) = d(\{p;\ p \equiv 1 \pmod{2^{U+1}}\}) = 2^{-U}$ and $\lim_N \frac{1}{N}\sum_{v>V} \mathcal{P}_+^v(N) = d(\{p;\ p \equiv -1 \pmod{2^{V+1}}\}) = 2^{-V}$. Hence, $\forall \epsilon > 0$, for any U, V and N large enough we have $M_N \leq M_N(U,V) + \epsilon$. As $N \to \infty$, we get $\limsup M_N \leq \sum_{u=2}^{U} \delta(\mathcal{P}^u)\delta^u + \sum_{v=2}^{V} \delta(\mathcal{P}_+^v)\delta_+^v + \epsilon$, which as $U, V \to \infty$ yields $\limsup M_N \leq l + \epsilon$. □

Example. The average over all primes p of the densities δ_{p4} is only $\frac{1}{36}$.

Remark. No average density $\delta(-,e)$, $\delta(p,-)$ or $\delta(-,-)$ is ever equal to any δ_q, q a prime power, contrary to the $1/3$ average, in the classical setting, of the densities of the sets $T_p = \{\ell$ rational prime; order of $p \pmod{\ell}$ is odd$\}$ as p varies through rational primes.

References

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

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

[Ba3] C. Ballot, *An elementary method to compute prime densities in $\mathbb{F}_q[X]$*. To appear in Integers.

[Des] R. Descombes, *Éléments de théorie des nombres*. Presses Universitaires de France (1986).

[Ga] J. von zur Gathen et als, *Average order in cyclic groups*. J. Theor. Nombres Bordx, vol. **16**, Nu. 1, (2004), 107–123.

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

[Lag] J. C. Lagarias, *The set of primes dividing the Lucas Numbers has density 2/3*. Pacific J. Math., vol. **118**, Nu. 2 (1985), 449–461 and "Errata", vol. **162** (1994), 393–396.

[Lan] S. Lang, *Algebraic Number Theory*. Springer-Verlag, 1986.

[Lax] R. R. Laxton, *Arithmetic Properties of Linear Recurrences*. Computers and Number Theory (A.O.L. Atkin and B.J. Birch, Eds.), Academic Press, New York, 1971, 119–124.

[Mo1] P. Moree, *On the prime density of Lucas sequences*. J. Theor. Nombres Bordx, vol. **8**, Nu. 2, (1996), 449–459.

[Mo2] P. Moree, *On the average number of elements in a finite field with order or index in a prescribed residue class*. Finite fields Appl., vol. **10**, Nu. 3, (2004), 438–463.

[M-S] P. Moree & P. Stevenhagen, *Prime divisors of Lucas sequences*. Acta Arithm., vol. **82**, Nu. 4, (1997), 403–410.

[Nar] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*. PWN - Polish Scientific Publishers, 1974.

[Pra] K. Prachar, *Primzahlverteilung*. Springer-Verlag, 1957.

[Ro] M. Rosen, *Number Theory in Function Fields*. Springer-Verlag, Graduate texts in mathematics **210**, 2002.
[Ser] J. P. Serre, *A course in Arithmetic*. Springer-Verlag, 1973.
[Sier] W. Sierpinski, *Sur une décomposition des nombres premiers en deux classes*. Collect. Math., vol. **10**, (1958), 81–83.
[Sti] H. Stichtenoth, *Algebraic Function Fields and Codes*. Springer-Verlag, 1993.

Christian Ballot
Département de Mathématiques,
Université de Caen, Campus 2,
14032 Caen Cedex, France
E-mail: ballot@math.unicaen.fr