Résumé

Dans cette thèse, nous étudions les propriétés de divisibilité de l'ordre multiplicatif modulo des nombres premiers. En particulier, nous nous intéressons à leurs extensions aux suites de Lucas à valeurs entières ou polynomiales sur des corps finis. Cette étude prend ses origines dans les travaux de Hasse sur la densité de Dirichlet des premiers pour lesquels un entier fixé satisfait certaines conditions de divisibilité, modulo ces premiers. De plus, ces résultats sont reliés à la conjecture d'Artin sur les racines primitives et à la distribution des diviseurs premiers des suites récurrentes.

Pour les suites de Lucas, l'analogue de l'ordre multiplicatif est le rang d'apparition des premiers. Étudier la divisibilité de ce rang par un entier fixé généralise le problème posé par Hasse. Des formules explicites des densités sont connues pour les suites dont le polynôme caractéristique est réductible, et des travaux récents dus à Sanna traitent le cas irréductible pour certains entiers.

Dans le contexte des corps de fonctions globaux, nous étendons les résultats de Sanna aux suites de Lucas polynomiales. Nous présentons des formules explicites de la densité dans la plupart des cas, ainsi que des programmes SageMath pour calculer les différentes constantes rentrant en jeu. Cela rend les résultats complètement explicites.

Enfin, pour les suites de Lucas usuelles à valeurs entières, nous démontrons des formules explicites pour la densité asymptotique des premiers dont le rang d'apparition est divisible par un entier pair, sous certaines hypothèses. Comme dans le cas des corps de fonctions, nous présentons des programmes SageMath calculant explicitement les constantes utilisées.

Abstract

In this thesis, we study the divisibility properties of the multiplicative order modulo primes. In particular, we investigate their extensions to polynomial Lucas sequences over finite fields. This study has its origin in the work of Hasse on the Dirichlet density of primes for which a fixed integer satisfies some divisibility condition modulo these primes. Such results are naturally connected with Artin's conjecture on primitive roots and with the distribution of prime divisors in linear recurrences.

For Lucas sequences, the counterpart of the multiplicative order is the rank of appearance of prime numbers. Studying the divisibility of this rank by a fixed integer generalises Hasse's problem. Explicit formulas for the density are known for sequences with reducible characteristic polynomials, while recent results by Sanna cover the irreducible case for certain integers.

In the context of global function fields, we extend Sanna's results to polynomial Lucas sequences. We provide closed-form formulas for the density in most cases, along with SageMath computations for the constants that appear in these formulas. This makes our results explicit.

Finally, for classical Lucas sequences, we give a closed-form formula for the natural density of primes whose rank of appearance is divisible by even integers, under suitable assumptions. As in the function field case, we provide SageMath programs to explicitly compute our constants.

Remerciements / Acknowledgements

First and foremost, I would like to thank the referees, Florian Luca and Carlo Sanna, for their careful reading and insightful comments on my thesis, as well as Francesco Amoroso, Antonella Perucca, and Denis Simon, for agreeing to be part of my jury.

Me voici à la fin d'une grande aventure, pleine de rebondissements, qui m'a fait grandir tant sur le plan mathématique que sur le plan personnel. Pour cela, je ne peux que te remercier, Christian, pour m'avoir supporté au cours de ces trois années (et bien plus). Tu m'as toujours soutenu et aidé dans mes projets, et je t'en serai toujours reconnaissant.

Je tiens à remercier les membres de mon Comité de Suivi Individuel, Clément Coine et Christophe Delaunay, dont les conseils m'ont conduit à voyager, à rencontrer de nouvelles personnes et à saisir de nouvelles opportunités.

During the last year of my PhD, I was lucky enough to be invited by the Max Planck Institute for Mathematics for a duration of two months. It was an incredible journey, and for that I would like to thank all the staff members at the MPIM, as well as the many people I have met there. My deepest gratitude goes to Pieter Moree for taking me on as a mentee during my stay. Special thanks to Wadim Zudilin for trusting me to be a speaker at the PLeaSANT seminar.

J'ai aussi eu la chance d'être invité à plusieurs séminaires en France. Merci à mon amie Candice de m'avoir invité dans la ville rose pour un exposé. Un séjour qui n'a fait que renforcer mon amour pour la violette. Un grand merci à Julien pour son accueil au Laboratoire Paul-Painlevé, qui m'a fait confiance pour le séminaire Arithmétique. Un très bon (quoique trop court) moment passé avec les doctorants lillois. Je garde également un excellent souvenir de mon passage à l'Institut de Mathématiques de Bordeaux et tiens à remercier Elena et Léo pour leur accueil et leur gentillesse.

I would like to thank Paul Voutier for his kind words and for taking the time to write to me. Even though we have never met, your encouragement meant a lot to me.

I am grateful to Steven Miller for his help with accommodation in the United States ahead of the 21st International Fibonacci Conference, and for his quick email replies when I needed assistance with a paper submission.

I met many wonderful people during the Fibonacci Conference, but one encounter that stood out is with Federico, Gessica, and Giuliano. You welcomed me to Turin twice with open arms, where I met even more amazing people. It is always a pleasure spending time with the three of you.

Tous ces voyages et ces rencontres n'auraient pas été possibles sans l'aide du LMNO et de l'École Doctorale, qui ne m'ont jamais rien refusé. Plus particulièrement, merci à Anita et Carole pour leur aide lors des missions.

Je n'oublierai jamais tous les doctorants rencontrés au LMNO, et les copains qui s'y

ajoutent, avec qui j'ai partagé des moments formidables. Merci au trio du jeu de rôle, Édouard, Romain et bien sûr Dorian, avec qui j'ai vécu les aventures les plus folles tout en restant autour d'une table. Merci à Alexandre pour m'avoir fait reprendre goût à l'escalade, à Dounia, Francesco et Hugues qui nous ont vite rejoints, puis tous les autres que l'on a occasionnellement convertis. À Nhuan, my friend, pour ta bonne humeur et pour avoir été le plus beau gosse du laboratoire. Je boirai du lait, comme promis.

Merci à notre doyen Hugo, dont l'énergie est plus que contagieuse. Bravo Adrien pour l'article et pour tes victoires au ping (yearly winner, n'en déplaise à Francesco). Merci à Raquel pour son partage de la culture brésilienne, et pour m'avoir enseigné les bases du portugais.

Merci à Guillaume, ou Guy pour les intimes, qui ne refuse jamais une pause et qui m'épate en sortant des jeux de cartes de toutes ses poches. Et puis, comment parler de Guy sans mentionner son co-bureau, Victor. Un plaisir de te battre au ping, mais surtout merci d'être toujours ouvert à la discussion quand je passe à ton bureau.

J'ai passé trois années avec quelqu'un face à moi, Alexis. Au-delà d'être une très belle vue, tu as été une excellente compagnie. Avoir eu quelqu'un avec qui discuter de tout et de rien, avec qui découvrir ensemble les premières conférences et écoles d'été, a été une vraie chance.

À ceux avec qui j'ai passé de bons moments à Bayeux, au bar, au restaurant, lors de sessions de jeux de société, ou lors des pauses du midi : Adrien, Albert (et ses beaux pulls de Noël), Alioune, Charlotte, Daniel, Étienne, Ilaria, Jacques, Lorenzo, Manu, Neha, Njaka, et Thibault. Ces moments ont beaucoup compté pour moi.

Je souhaite bien sûr beaucoup de réussite aux nouveaux, que je ne connais pas encore tous très bien. Alix, Antonio, Marceau, Mélina, et Ryan, profitez bien de ces années.

Je remercie plus que tout mon ami de toujours, Hugo, qui m'a toujours soutenu du début à la fin de cette thèse. Je n'oublie évidemment pas Aurélien et Maxime, mes deux autres pirates. Je sais que je peux toujours compter sur vous trois.

Je termine par le plus important, merci à mes parents, ma famille et mes proches pour le soutien qu'ils m'ont apporté. Un gros bisou à mes sœurs Axelle et Gabrielle. Je dédie cette thèse à mes grands-parents, qui n'ont pas pu en voir son aboutissement, mais qui seraient fiers.

Contents

List of Symbols

We provide a list of the symbols that appear frequently in this thesis. They are given in the order with which they appear. The page of first appearance is indicated whenever more information about the symbol can be found at this page.

We first give some general notation. We use the letters d, n, N to denote integers and l, p for prime numbers. We let $\mathbb{Q}$ and $\mathbb{F}_q$ be the field of rational numbers and the finite field of q elements. The letter q stands for a power of the prime p. We use various classical functions such as exp, log, Li, and $\lfloor \cdot \rfloor$, that is, the exponential, the natural logarithm, the logarithmic integral, and the floor functions respectively. We write ω, τ, φ, ψ, and μ for the prime-omega function, the number of divisors function, Euler's totient function, Dedekind psi function, and the Möbius function, respectively. For integers $a, b \in \mathbb{Z}$, we write (a, b) and $[a, b]$, respectively, for the gcd and the lcm of a and b. Both the Landau notation $\mathcal{O}$ and the Vinogradov symbol $\ll$ are used.

d^∞	supernatural number
$U(a_1, a_2)$	Lucas sequence U with parameters $a_1, a_2 \in A$, page 9
$\mathrm{ord}_n(a)$	order of a mod n in $(\mathbb{Z}/n\mathbb{Z})^\times$
v_p	p-adic valuation
(a/p)	Legendre symbol of a modulo p
d_3	d_3-density, page 6
A	UFD, $\mathbb{F}_q[T]$ (Chapters 3 and 4) or $\mathbb{Z}$ (Chapter 5)
K	fraction field of A, $\mathbb{F}_q(T)$ (Chapters 3 and 4) or $\mathbb{Q}$ (Chapter 5)
$\bar{K}$	algebraic closure of the field K
ζ_n	primitive n-th root of unity in $\bar{K}$
a_1, a_2	non-zero elements of A
a, b	roots of $X^2 - a_1X + a_2$ in $\bar{K}$
Δ	discriminant of $X^2 - a_1X + a_2$
L	splitting field $K(a)$ of $X^2 - a_1X + a_2$
$\rho_U(P)$	rank of appearance of $P \in A$ in $U(a_1, a_2)$, page 11

$\iota_U(P)$	index of appearance of $P \in A$ in $U(a_1, a_2)$, page 12
$\mathcal{O}_L$	ring of integers of L, integral closure of A in L
γ	quotient a/b of the roots of $X^2 - a_1X + a_2$
NP	the norm $\lvert A/P \rvert$ of P
ϵ_P	-1 if P is inert in L and 1 if P splits completely, page 11
σ_L	the non-trivial automorphism of L/K
$(L/K, \mathfrak{p})$	Frobenius element associated with a prime ideal $\mathfrak{p} \in \mathcal{O}_L$
$\mathrm{ord}_{\mathfrak{p}}(\gamma)$	order of the reduction of γ modulo $\mathfrak{p}$ in $(\mathcal{O}_L/\mathfrak{p})^\times$
$R_q(\gamma, d)$	set of prime polynomials $P \in \mathbb{F}_q[T]$ such that $d \mid \rho_U(P)$, page 16
d_1	d_1-density, page 16
$\mathcal{P}_+$	set of prime polynomials $P \in \mathbb{F}_q[T]$
I_N	number of monic and irreducible polynomials of degree N over $\mathbb{F}_q$
$(L/K, P)$	Artin symbol associated with a prime $P \in K$
$[L : K]$	degree of the field extension L/K
g_L	genus of an algebraic function field L
∞	prime at infinity, prime of degree 1 in $L = K(a)$
v_∞	∞-adic valuation
L_∞	completion of L with respect to v_∞, page 18
$\tilde{x}$	monic part of $x \in L$, page 18
$\mathrm{sgn}(x)$	leading coefficient of x in L_∞, page 18
LK	compositum of two fields K and L
$L_{n,d}/K$	Kummer extension, page 20 (Chapter 3), page 92 (Chapter 5)
$\mathbb{F}_{n,d}$	constant field of $L_{n,d}$
$(K^\times)^n$	set of n-th powers in K
h	maximal power for γ, page 20 (Chapter 3), page 93 (Chapter 5)
μ	$\mathrm{sgn}(\gamma)$, sign of γ, page 20
$\mathrm{ord}_G(g)$	order of g in the finite group G
$\mathrm{ind}_G(g)$	index of g in the finite group G
$\mathbb{F}_L$	constant field of L
f	multiplicative order $\mathrm{ord}_d(q)$
$[\,\cdot\,]$	Iverson brackets, page 24
e_N^+	$(q^N - 1, d^\infty)/d$, where $d \mid q^N - 1$

$R_q^+(\gamma, d)$	set of primes in $R_q(\gamma, d)$ with $\epsilon_P = 1$, page 25
f_L	lcm of f and $[\mathbb{F}_L : \mathbb{F}_q]$
$f_{u,v}$	degree of $\mathbb{F}_{dv,uv}/\mathbb{F}_q$, page 27
$\delta_q^+(\gamma, d)$	d_3-density of $R_q^+(\gamma, d)$, page 28
$R_q^-(\gamma, d)$	set of primes in $R_q(\gamma, d)$ with $\epsilon_P = -1$, page 31
$\sigma_{u,v}$	special automorphism of $L_{dv,uv}/K$, page 32
e_N^-	$(q^N + 1, d^\infty)/d$, where $d \mid q^N + 1$
d'	$d/(d, 2^\infty)$, odd part of d
$\delta_q^-(\gamma, d)$	d_3-density of $R_q^-(\gamma, d)$, page 34
$N_{L/K}$	field norm of L/K
$\mathbf{b}(h)$	boolean function, page 47
$\bar{f}$	multiplicative order $\mathrm{ord}_{d(h,d^\infty)}(q)$
h_1	$(h, 2^\infty)$
$\mathcal{Q}(n)$	boolean function, page 59
Δ_L	absolute discriminant of a number field L
$\mathcal{Q}$	boolean function $[N_{L/K}(\gamma^{1/h_1}) = 1]$
$\mathcal{R}$	boolean function $[v_2(h) = 1$ and $\tilde{a}_2/\Delta \in (K^\times)^2]$
$\mathcal{R}_\gamma(d)$	set of primes $p \in \mathbb{Z}$ such that $d \mid \rho_U(p)$, page 91
$\delta_\gamma(d)$	natural density of $\mathcal{R}_\gamma(d)$
d_0	$d/(d, h)$
h_0	$h/(d, h)$
$\mathcal{R}_\gamma^\pm(d)$	set of primes $p \in \mathcal{R}_\gamma(d)$ such that $(\Delta/p) = \pm 1$, page 99
$\delta_\gamma^\pm(d)$	natural density of $\mathcal{R}_\gamma^\pm(d)$, page 99
K_1, K_2	fields $K_1 = \mathbb{Q}(\sqrt{c})$ and $K_2 = \mathbb{Q}(\sqrt{c/\Delta_L})$, page 101
Δ_1, Δ_2	absolute discriminants of K_1 and K_2
σ_0	special automorphism of $L(\zeta_n)/\mathbb{Q}$, page 103
$\mathcal{Q}_1, \mathcal{Q}_2$	boolean functions $[\sigma_i(\gamma^{1/2h_1}) = \gamma^{-1/2h_1}]$, page 103

Chapter 1

Introduction

1.1 Divisibility of the multiplicative order

In 1965 and 1966, Hasse published two papers [10,11] that were to become the first brick to a much broader problem. He considered a square-free positive integer a, a prime number l, and asked how many prime numbers p satisfy $l \mid \mathrm{ord}_p(a)$, where $\mathrm{ord}_p(a)$ is the order of the reduction of a modulo p in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. Call $N_a(l)$ the set of such primes. Hasse proved that $N_a(l)$ has a Dirichlet density equal to

$$\frac{17}{24} \quad \text{or} \quad \frac{l}{l^2-1},$$

depending on whether $l = 2$ and $|a| = 2$, or not respectively. To interpret these results, recall that the Dirichlet density measures the proportion of primes lying in a given subset. Thus, approximately 71% of all primes lie in $N_2(2)$, and about 66% in $N_3(2)$.

In a series of papers [38–42], Wiertelak studied in great detail the divisibility properties of $\mathrm{ord}_p(a)$, where $a \in \mathbb{Z} \setminus \{\pm 1, 0\}$. Most notably, he gave a complete answer to Hasse's original problem, replacing l by a positive integer d. Not only did he find a formula for the Dirichlet density $\delta_a(d)$ of $N_a(d)$, but he proved an asymptotic formula for the counting function $N_a(d,x) = N_a(d) \cap [1,x]$, where $x > 1$ is a real number. The following is a restatement of Wiertelak's theorem [40] given by Moree [21]:

Theorem 1.1. *Let $d \geq 1$ be an integer and $x > 1$. We have*

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

where ω is the prime-omega function and Li *is the logarithmic integral function.*

Moreover, the formulas Wiertelak gives show that $\delta_a(d)$ is always in $\mathbb{Q}_{>0}$. More recently,

Pappalardi [27] 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 [21], where a is replaced by a rational $g \in \mathbb{Q} \setminus \{\pm 1, 0\}$, using a similar method. Write $g = \pm g_0^h$, where $g_0 \in \mathbb{Q}_{>0}$ is not a power and $h \geq 1$ is an integer, and let d^∞ be a supernatural number, where the exponents in the prime decomposition of d^∞ are equal to $+\infty$. We have

$$\delta_g(d) = \frac{\epsilon_1}{d(h, d^\infty)} \prod_{p \mid d} \left(\frac{p^2}{p^2 - 1} \right), \tag{1.1}$$

where (h, d^∞) is the gcd of h and d^∞, and $\epsilon_1 \in \mathbb{Q}_{>0}$ is given explicitly by Moree. Other related questions answered by Wiertelak concern two sets of prime numbers: those for which $d \| \mathrm{ord}_p(a)$, and those with $(\mathrm{ord}_p(a), n) = d$, where $n \geq 1$. Note that $d \| \mathrm{ord}_p(a)$ means $v_l(d) = v_l(\mathrm{ord}_p(a))$ for all primes $l \mid d$, where v_l is the l-adic valuation.

The motivations behind Hasse's and Wiertelak's results come from the Artin's conjecture on primitive roots. Stated by Artin in 1927, the conjecture says that if a is an integer different from -1 and from a square, then there are infinitely many primes p for which a is a primitive root modulo p. That is, $\mathrm{ord}_p(a) = p-1$ for infinitely many primes. By studying the distribution of primes p for which $\mathrm{ord}_p(a)$ satisfies certain divisibility conditions, they gave a first quantitative understanding of how $\mathrm{ord}_p(a)$ behaves. See [22] for a survey on Artin's conjecture.

Another motivation is found in prime divisors of integer sequences. For a linear recursion $X = (x_n)_{n \geq 0} \subset \mathbb{Z}$, we say that a prime p divides X, denoted by $p \mid X$, if there exists $n \geq 0$ such that $p \mid x_n$. When X is a linear recurrence of order exactly 2, Ward [36] showed that there are infinitely many primes p such that $p \mid X$. This was later generalised by Stephens [32, 33], who proved, under the generalised Riemann hypothesis (GRH), that this set has a positive density for a certain kind of recurrent sequences of order 2. His work was extended by Moree and Stevenhagen [24] to all second-order recursions using a clever generalisation of Artin's conjecture on primitive roots. Although these results are conditional, there are examples of sequences for which the Dirichlet density can be found unconditionally. This is the case of sequences X defined by

$$x_n = a^n + b^n,$$

for all $n \geq 0$, where $a, b \in \mathbb{Z} \setminus \{\pm 1, 0\}$. The set of primes p dividing X is equal, up to possibly finitely many exceptions, to $N_g(2)$, where $g = a/b$, whose density is given by (1.1). They are not the only sequences that can be linked to the work of Hasse and Wiertelak.

For instance, if d is a prime number and X is defined by

$$x_n = \sum_{k=0}^{d-1} a^{nk} b^{n(d-1-k)} = \frac{a^{dn} - b^{dn}}{a^n - b^n}, \tag{1.2}$$

for all $n \geq 1$, then the associated prime density is $\delta_g(d)$. Here, note that X is a linear recursion of order d. This example gives us some insight on the case of higher-order recursions, for which much less is known about their prime divisors. Recent progress by Järviniemi [13] shows that, under the generalised Riemann hypothesis, higher-order recursions have a positive lower density of prime divisors.

1.2 Generalisation to Lucas sequences

The Fibonacci sequence is probably the best-known example of a second-order recurrence. It is denoted by F, and is defined by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. With it comes the sequence $L = (L_n)_{n \geq 0}$ of Lucas numbers, defined by the same recursion and initial terms $L_0 = 2$ and $L_1 = 1$. In 1985, Lagarias [16] proved that the set of primes p such that $p \mid L$ has density $2/3$. He made use of Hasse's method [10, 11] and the link with sequences of the form $a^n + 1$. This makes sense as

$$L_n = \phi^n + \bar{\phi}^n,$$

for all $n \geq 0$, where $\phi = (1 + \sqrt{5})/2$ is the golden ratio and $\bar{\phi}$ its quadratic conjugate. Naturally, we can ask what replaces the multiplicative order of a modulo p in this instance. We define the rank of appearance, $\rho_F(p)$, of p in F as the least positive integer n such that $p \mid F_n$. This is analogous to the multiplicative order. In particular, we have $p \mid L$ precisely when $2 \mid \rho_F(p)$. It is only natural that the divisibility problem for the multiplicative order extends to primes whose rank of appearance in F is divisible by a fixed integer $d \geq 2$. This has been studied by Cubre and Rouse [8], who obtained a complete formula for the Dirichlet density of such primes, namely

$$\frac{c(d)}{d} \prod_{p \mid d} \left(\frac{p^2}{p^2 - 1} \right),$$

where $c(d)$ is equal to 1, 5/4, or 1/2 if, respectively, $10 \nmid d$, $d \equiv 10 \pmod{20}$, or $20 \mid d$.

Given two non-zero integers $a_1, a_2 \in \mathbb{Z}$, we define the Lucas sequence $U = (U_n)_{n \geq 0}$ with parameters a_1 and a_2. It satisfies the initial conditions $U_0 = 0$, $U_1 = 1$, and

$$U_{n+2} = a_1 U_{n+1} - a_2 U_n,$$

for all $n \geq 0$. As for the Fibonacci sequence $F = U(1,-1)$, one defines the rank of appearance of a prime p in U, denoted by $\rho_U(p)$, as the least positive integer n such that $p \mid U_n$. Of course, we may ask whether the Dirichlet density of primes p for which $d \mid \rho_U(p)$, where $d \geq 2$, exists and can be found explicitly for all Lucas sequences. This turns out to be a direct generalisation of Hasse's original problem. Indeed, one has $\rho_U(p) = \mathrm{ord}_p(a/b)$ for sequences U such that

$$f(X) = X^2 - a_1 X + a_2 = (X-a)(X-b) \tag{1.3}$$

is reducible over $\mathbb{Z}$. In that case, the density is equal to $\delta_g(d)$, where $g = a/b$, which was explicited in (1.1). This generalisation to Lucas sequences allows us to replace $a, b \in \mathbb{Z}$ by quadratic conjugates $a, b \in L := \mathbb{Q}(\sqrt{\Delta})$, where $\Delta = a_1^2 - 4a_2$, whenever $f(X)$ is irreducible.

The case $d = 2$ has been studied in great detail by Moree and Stevenhagen [20,23]. They gave a complete description of the density values when the root a is a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{\Delta})$. Recently, Sanna [30] made an important contribution to this problem. Let Δ_0 be the square-free part of Δ. Assuming that d is odd and not divisible by 3 if $L \neq \mathbb{Q}(\zeta_3)$, where ζ_3 is a primitive third root of unity, he showed that the Dirichlet density of the primes p for which $d \mid \rho_U(p)$ exists and is equal to

$$\delta_U(d) = \frac{1}{d}\left(\frac{1}{(h, d^\infty)} + \eta_U(d)\right) \prod_{p \mid d} \left(\frac{p^2}{p^2-1}\right),$$

where $\eta_U(d) = 0$ if $\Delta > 0$, or $\Delta_0 \not\equiv 1 \pmod 4$, or $\Delta_0 \nmid d^\infty$, and

$$\eta_U(d) = \frac{(h, d^\infty)}{[(h, d^\infty), \Delta_0/(d, \Delta_0)]^2},$$

otherwise. Prior to Sanna's result, some progress had already been made in some other cases. In 2013, Ballot considered Lucas sequences such that L is equal to a cyclotomic field. That is, when Δ is minus a square, or minus three times a square. Using clever decompositions of U into products of other sequences, which are only feasible when L is cyclotomic, he found the value of $\delta_U(d)$ for $d \in \{2, 4\}$ and $d \in \{3, 6\}$, when $L = \mathbb{Q}(i)$ and $L = \mathbb{Q}(\zeta_3)$ respectively, where $i^2 = -1$. This was done under some fairly general hypotheses on the parameter a_2.

The motivation for studying prime divisors of sequences is natural, as it mimics the case mentioned in Section 1.1. Indeed, we can replace a and b in (1.2) by quadratic conjugates. The sequences obtained lie in $\mathbb{Z}$, and the density of their prime divisors is equal to $\delta_U(d)$, for d a prime number. This can actually be extended to composite integers, where the

density is obtained via the Möbius sum

$$1 - \sum_{u|d} \mu(u)\delta_U(u),$$

where μ is the Möbius function. Another question, which provides a second motivation, is whether there exists a generalisation of Artin's conjecture to Lucas sequences with an irreducible characteristic polynomial. In a series of papers, Laxton [18, 19] constructed a group $G(f)$, where elements are equivalence classes of sequences sharing the same characteristic polynomial f, defined as in (1.3). The group operation of $G(f)$ has the property of preserving prime divisibility. In the first paper, Laxton restated the Artin primitive root conjecture via quotients of $G(f)$ by certain normal subgroups. This allowed for a first generalisation to the irreducible case. From an arithmetic point of view, the Artin conjecture for Lucas sequences asserts that, if a/b is not a square, there are infinitely many primes p for which $\rho_U(p)$ is maximal, that is,

$$\rho_U(p) = p - \left(\frac{\Delta}{p}\right),$$

where (Δ/p) is the Legendre symbol of Δ modulo p. This links $\rho_U(p)$ to another behaviour of the multiplicative order. Indeed, as $\mathrm{ord}_p(a)$ divides $p-1$, the same is true for $\rho_U(p)$, which divides $p - (\Delta/p)$.

1.3 The function field case

There is a well-known 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. In this setting, the analogue of $\mathbb{Q}$ is the fraction field of A, that is, $K := \mathbb{F}_q(T)$. In Sections 1.1 and 1.2, we discussed the problem of the divisibility of the rank of appearance of Lucas sequences. It is natural to ask whether a similar investigation can be conducted for sequences defined over A.

In 2006 and 2007, Ballot [2, 3] considered the Lucas sequence $U = (U_n)_{n\geq 0} \subset A$ with parameters $a_1 = T + 1$ and $a_2 = T$. That is, the sequence defined by

$$U_n = \frac{T^n - 1}{T - 1},$$

for all $n \geq 0$. As in Section 1.2, we define $\rho_U(P)$ as the rank of a prime P in U, that is, P is a monic and irreducible polynomial in A. In his papers, Ballot computed the density of the set of primes P whose rank of appearance is divisible by a prime number. Some remarkable properties of this sequence even allowed him to prove his results using

an elementary method. Note that, in contrast to the classical case, Ballot did not use the Dirichlet density, but another density notion referred to as the d_3-density. Let $S \subset A$ be a set of primes and $S(N)$ be the number of $P \in S$ with polynomial degree N, $N \geq 1$. Then, the d_3-density of S is defined by

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

when the limit exists. In discussing the different notions of prime density over $\mathbb{F}_q(T)$, Ballot [4] showed evidence that the d_3-density is a close analogue to the natural density of positive integers. Moreover, the existence of a d_3-density for a set S, implies the existence of its Dirichlet density. In that case, their value is the same. This confirms the d_3-density as a stronger notion of density than the Dirichlet density.

To our knowledge, Ballot's papers are the only instance in the literature that study the divisibility problem of the rank of appearance in this context. We believe that this can be explained by Artin's conjecture on primitive roots being settled in the function field setting. Without this motivation, fewer weaker problems have been studied to get closer to the conjecture's validity. Let $a \in K \setminus \mathbb{F}_q$, a not an l-th power for all $l \mid q-1$. The conjecture states that there exist infinitely many primes $P \in A$ such that a is a primitive root modulo P, that is, a has order $q^N - 1$ in $(A/P)^\times$. It was first proven by Bilharz [6] under the generalised Riemann hypothesis for function fields, which was later proved by Weil [37]. In his proof, Bilharz shows that the set of primes P that have a as a primitive root has positive Dirichlet density. Another proof was given in 1994 by Pappalardi and Shparlinski [28] by estimating the number of primes $P \in A$ of degree $n \geq 1$ that satisfy the conjecture. More recently, Kim and Murty [15] managed to prove Artin's conjecture without using the generalised Riemann hypothesis for function fields.

1.4 Thesis outline

The main purpose of this thesis is to extend Sanna's results [30] to polynomial Lucas sequences over the finite field $\mathbb{F}_q$ of q elements. The idea is to adapt his method to the function field setting and find a closed-form formula for the d_3-density of primes $P \in A = \mathbb{F}_q[T]$ whose rank of appearance is divisible by a fixed integer $d \geq 1$. We do not restrict ourselves to odd integers, and aim for a general characterisation of the density values. This generalises Ballot's results [2, 3] to other Lucas sequences. However, unlike him, we are unable to prove a general result by elementary means. Additionally, one of our objectives is to make progress on the divisibility problem for classical Lucas sequence in $\mathbb{Z}$. We seek to find the Dirichlet density of prime numbers p whose rank of appearance is divisible by an

even integer $d \geq 1$ when $\mathbb{Q}(\sqrt{\Delta})$ is not a cyclotomic field, where Δ was defined in Section 1.2. This would leave only the cyclotomic cases to be studied. Throughout this thesis, we refer to these types of problems under a common name: *the order problem*.

In Chapter 2, we define Lucas sequences in rings of integers of global fields. This is where we make our first essential assumptions on Lucas sequences for the thesis. Moreover, we give various properties of the rank of appearance.

In the third chapter, we consider various notions of density that were defined and compared in a discussion by Ballot [4]. For each notion, we study the existence of the density of the set of primes $P \in A$ such that $d \mid \rho_U(P)$, where $\rho_U(p)$ is the rank of appearance of P in a given Lucas sequence $U \subset A$ and d is a positive integer. We show that the Dirichlet and d_3 densities always exists in Theorems 3.18 and 3.23, and that the others do not in Theorem 3.31. Doing so, we obtain a first formula for the d_3-density. This chapter includes many preliminaries on field extensions of $K = \mathbb{F}_q(T)$. In particular, we study constant field extensions and Kummer extensions. For the latter, we find an exact formula for the field degree of Kummer extensions of rank 1 over K.

Chapter 4 complements Chapter 3, in which we obtained a first formula for the d_3-density. This formula involves an infinite series, which, as such, is not easy to compute. If U has reducible characteristic polynomial, then Theorem 4.12 provides a nicer formula for the density. However, we had to make assumptions on the constant field of our Kummer extensions to prove it. If U has irreducible characteristic polynomial $f(X)$, then we are able to find a closed-form formula in almost all cases. The only cases left occur when the splitting field of $f(X)$ is $\mathbb{F}_{q^2}(T)$. This is the only case in which we adjoin a root of unity to K, which parallels the case left aside by Sanna [30] in his theorem. At the end of this chapter, we provide a few algorithms and their SageMath [35] implementations in order to compute all the constants defined throughout Chapters 3 and 4. This makes our results explicit.

In Chapter 5, we come back to classical Lucas sequences $U \subset \mathbb{Z}$. Recall that Δ is the discriminant of the characteristic polynomial of U. Under the assumption that $\mathbb{Q}(\sqrt{\Delta})$ is not a cyclotomic field, we derive a closed-form formula for the Dirichlet density of prime numbers p whose rank $\rho_U(p)$ is divisible by an even integer $d \geq 1$. We use the method of Chapter 4. Our results depend on various constants. Thus, as in the previous chapter, we provide algorithms to compute these constants, with their SageMath implementations.

Chapter 2

Lucas sequences in integer rings

This first chapter is an introduction to Lucas sequences. We reprove classical properties about those sequences that are already known over $\mathbb{Z}$. This thesis is about prime densities for primes in both $\mathbb{Z}$ and $\mathbb{F}_q[T]$, where $\mathbb{F}_q$ is the finite field of q elements. Therefore, we generalise those results to rings of integers of global fields.

Section 2.1 is dedicated to basic definitions of our setting and of Lucas sequences. This is a short section in which we prove various properties of those sequences via elementary methods.

In the second section, we study the rank of appearance of primes in a Lucas sequence. That is, for a fixed prime ideal P, the least integer $n \geq 1$ such that P divides the n-th term of the sequence. We prove classical properties of the rank known as the laws of appearance, and of repetition.

Throughout this chapter, the letter n denote a non-negative integer and the letter p zero or a prime number. We let A denote the ring of integers of a global field K with characteristic p. We write $\bar{K}$ for an algebraic closure of K and ζ_n for a primitive n-th root of unity in $\bar{K}$.

2.1 Definitions and first properties

Let $a_1, a_2 \in A$ be non-zero. We consider the polynomial $f(X) = X^2 - a_1X + a_2$ in $A[X]$ with roots $a, b \in \bar{K}$ and discriminant $\Delta := a_1^2 - 4a_2$.

Definition 2.1. *A Lucas sequence $U = (U_n)_{n\geq 1}$ with parameters $a_1, a_2 \in A$ is a second order linear recursion with initial terms $U_0 = 0$ and $U_1 = 1$, and with characteristic polynomial $f(X)$, that is, such that $U_{n+2} = a_1U_{n+1} - a_2U_n$ for all $n \geq 0$.*

However, we prefer writing Lucas sequences in their Binet formula. We have two cases.

If $a = b$, then $U_n = na^{n-1}$ for all $n \geq 0$, and otherwise, we have

$$U_n = \frac{a^n - b^n}{a - b},$$

for all $n \geq 0$. This is the latter form that will be of interest throughout this thesis. We distinguish two kinds of Lucas sequences: the degenerate and non-degenerate Lucas sequences. If $U_n = 0$ for some $n \geq 1$, then U is called degenerate. Therefore, a Lucas sequence that is non-zero for all $n \geq 1$ is non-degenerate. Let $L = K(a)$ be the splitting field of $f(X)$. The following lemma shows that degeneracy can be expressed as a relation between the roots of the characteristic polynomial:

Lemma 2.2. *A Lucas sequence U is degenerate if and only if we have $a = \zeta b$ for some root of unity $\zeta \in L$. ($\zeta \neq 1$ if $p = 0$.)*

Proof. If $a = b$, then $U_n = na^{n-1} \neq 0$ unless $p > 0$ and $p \mid n$. If $a \neq b$, then

$$U_n = 0 \iff \frac{a^n - b^n}{a - b} = 0 \iff \left(\frac{a}{b}\right)^n = 1 \iff a = \zeta b,$$

for some n-th root of unity $\zeta \in L$. □

We assume that U is a non-degenerate sequence for the rest of this chapter, as there is much more to say in this case. Moreover, in the following chapters, we study the divisibility by primes of Lucas sequences, since the degenerate case is straightforward.

Proposition 2.3 (Divisibility sequence)**.** *For all $m, n \geq 0$, we have $U_n \mid U_{mn}$.*

Proof. If $a = b$, then the result follows directly from $U_n = na^{n-1}$. Otherwise, we have

$$\frac{U_{mn}}{U_n} = \frac{a^{mn} - b^{mn}}{a^n - b^n}.$$

Let $a' = a^n$ and $b' = b^n$. We see that the above quotient is the m-th term of the Lucas sequence U' with parameters $a' + b'$ and $a'b'$. We only need to show that the parameters are in A. But we have $a'b' = (ab)^n = a_1^n$. Also, $a' + b' = a^n + b^n$ is the n-th term of the sequence $V = (V_n)_{n \geq 0}$ defined by $V_0 = 2$, $V_1 = a_1$, and

$$V_{n+2} = a_2 V_{n+2} - a_2 V_n,$$

for all $n \geq 0$. We see from the recursion that $V_n \in A$. □

2.2 The rank of appearance of primes

Let $P \in A$ be a prime ideal. In this section, we study the behaviour of primes in Lucas sequences. The object of interest is called the rank of appearance, or just the rank as a shorthand, and is defined in the following:

Definition 2.4. *The rank of appearance of P in U, denoted by $\rho_U(P)$, is the least positive integer $n \geq 1$ such that $P \mid U_n$, if it exists. Otherwise, we write $\rho_U(P) = +\infty$.*

Let $\mathcal{O}_L$ denote the ring of integers of L, i.e., the integral closure of A in L. The next lemma shows how the rank can be seen as the multiplicative order of $\gamma := a/b$ modulo some prime ideal of L. As a consequence, we find that the condition $P \nmid a_2$ is sufficient for the rank of P to exist. We let $NP = |A/P|$.

Lemma 2.5. *Let $P \nmid 2\Delta a_2$ be prime and $\mathfrak{p} \mid P$ be a prime ideal of $\mathcal{O}_L$. Then, $\rho_U(P)$ is equal to the multiplicative order of γ modulo $\mathfrak{p}$, and $\rho_U(P) \mid NP - \epsilon_P$, where*

$$\epsilon_P = \begin{cases} 1, & \text{if } P \text{ splits in } L; \\ -1, & \text{if } P \text{ is inert in } L. \end{cases}$$

Proof. We prove that $P \mid U_n$ if and only if $\gamma^n \equiv 1 \pmod{\mathfrak{p}}$, where $n \geq 1$. Note that reducing γ modulo $\mathfrak{p}$ makes sense as $P \nmid a_2$ ensures that $\mathfrak{p} \nmid ab$. Since $\mathfrak{p}$ is lying above P, we have $P \mid U_n$ only if $\mathfrak{p}$ divides

$$U_n = \frac{a^n - b^n}{a - b} = \frac{a^n - b^n}{\sqrt{\Delta}}.$$

This makes sense because $P \nmid \Delta$, and thus $\mathfrak{p} \nmid \Delta$ as well. Hence $a^n \equiv b^n \pmod{\mathfrak{p}}$, which is equivalent to $\gamma^n \equiv 1 \pmod{\mathfrak{p}}$. For the converse, we saw that $\gamma^n \equiv 1 \pmod{\mathfrak{p}}$ if and only if we have $\mathfrak{p} \mid U_n$. If $L = K$, or $L \neq K$ and P is inert, then the result follows directly. For the other primes, since L/K has degree two, we know it is Galois. We have $\mathfrak{p} \mid U_n$ if and only if $\sigma_L(\mathfrak{p}) \mid U_n$, where σ_L is the non-trivial automorphism of L/K. It follows that $P \mid U_n$ because $P\mathcal{O}_L = \mathfrak{p} \cap \sigma_L(\mathfrak{p})$. Finally, the result follows by minimality of the rank of appearance of P and of the order modulo $\mathfrak{p}$.

Now, for the second part of the lemma, we note that if $p \neq 2$, then a prime of K is ramified in L if and only if it divides 2Δ. (See [7, Lemma 5] for reference.) If $p = 2$, then for any prime $P \in A$, the residue field A/P has characteristic $p = 2$. We have

$$f(X) = X^2 - a_1X + a_2 \equiv (X + \alpha)^2 \pmod{P}$$

if and only if $a_2 \equiv \alpha^2 \pmod{P}$ and $a_1 \equiv 0 \pmod{P}$, by identifying the coefficients on both sides. This is equivalent to $a \equiv b \pmod{P}$, that is, $P \mid \Delta = (a - b)^2$. By the

Dedekind-Kummer theorem, it follows that $P \nmid 2\Delta$ ensures that P is unramified in L. Therefore, the Frobenius element $\sigma_{\mathfrak{p}} := (L/K, \mathfrak{p})$ corresponding to a prime $\mathfrak{p} \mid P$ exists. We have $\sigma_{\mathfrak{p}} = \mathrm{id}$ if $\epsilon_P = 1$, and $\sigma_{\mathfrak{p}} = \sigma_L$ otherwise. By definition, we have

$$\sigma_{\mathfrak{p}}(\gamma) = \gamma^{NP} \pmod{\mathfrak{p}} \quad \text{and} \quad \sigma_{\mathfrak{p}}(\gamma) = \gamma^{\epsilon_P}.$$

Hence $\gamma^{NP-\epsilon_P} \equiv 1 \pmod{\mathfrak{p}}$, that is, $P \mid U_{NP-\epsilon_P}$ by the above. The claim follows by the minimality of the multiplicative order. □

Corollary 2.6. *Let $P \nmid \Delta a_2$ be prime and $n \geq 1$. Then, $P \mid U_n$ if and only if $\rho_U(P) \mid n$.*

Proof. This is a direct consequence of Lemma 2.5 and the rank being the multiplicative order of γ modulo $\mathfrak{p} \mid P$. □

Definition 2.7. *The unique integer $\iota_U(P)$ such that $\rho_U(P) \cdot \iota_U(P) = NP - \epsilon_P$ is called the index of appearance of P in U.*

Lemma 2.8. *Let U and U' be non-degenerate Lucas sequences. Assume that γ is the quotient of the roots of both $f(X)$ and $f'(X)$, their respective characteristic polynomials. Then, there exists $c \in K^\times$ such that $U_n = c^{n-1}U'_n$ for all $n \geq 0$.*

Proof. Let $f(X) = X^2 - a_1X + a_2$ and $f'(X) = X^2 - A_1X + A_2$. We denote by $a, b \in L$ the roots of f, and $\alpha, \beta \in L$ those of f'. We have $\gamma = a/b = \alpha/\beta$, and

$$\gamma + \gamma^{-1} = \frac{a_1^2}{a_2} - 2 = \frac{A_1^2}{A_2} - 2.$$

The latter yields $a_2/A_2 = (a_1/A_1)^2$. The result follows with $c = a_1/A_1$. □

We end this chapter with a formula that links $\mathrm{ord}_{\mathfrak{p}}(\gamma)$ to $\mathrm{ord}_{\mathfrak{p}}(-\gamma)$, where $\mathrm{ord}_{\mathfrak{p}}(\gamma)$ is the order of the reduction of γ modulo $\mathfrak{p}$ in $(\mathcal{O}_L/\mathfrak{p})^\times$. In particular, by Lemma 2.5, it links $\rho_U(P)$ to $\mathrm{ord}_{\mathfrak{p}}(-\gamma)$. Although simple, this observation plays an important role in our work, as we will see at the beginning of Chapters 4 and 5. The same argument was used by Wiertelak [40].

Lemma 2.9. *Assume $p \neq 2$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_L$. We have*

$$\mathrm{ord}_{\mathfrak{p}}(\gamma) = \begin{cases} \mathrm{ord}_{\mathfrak{p}}(-\gamma)/2, & \text{if } 2 \nmid \mathrm{ord}_{\mathfrak{p}}(\gamma); \\ 2\mathrm{ord}_{\mathfrak{p}}(-\gamma), & \text{if } \mathrm{ord}_{\mathfrak{p}}(\gamma) \equiv 2 \pmod 4; \\ \mathrm{ord}_{\mathfrak{p}}(-\gamma), & \text{if } 4 \mid \mathrm{ord}_{\mathfrak{p}}(\gamma). \end{cases}$$

Proof. Let $\rho = \mathrm{ord}_{\mathfrak{p}}(\gamma)$. Then, since

$$(-\gamma)^\rho \equiv (-1)^\rho \pmod{\mathfrak{p}},$$

we see that $2\rho = \mathrm{ord}_{\mathfrak{p}}(-\gamma)$ if ρ is odd. If $\rho \equiv 2 \pmod 4$, then $(-\gamma)^{\rho/2} \equiv 1 \pmod{\mathfrak{p}}$. We claim that $\rho/2$ is the least integer $t \geq 1$ such that $(-\gamma)^{\rho/2} \equiv 1 \pmod{\mathfrak{p}}$. If it is not, then there exists $m < \rho/2$ such that $(-\gamma)^m$ is 1 modulo $\mathfrak{p}$, which implies that $\gamma^{2m} \equiv 1 \pmod{\mathfrak{p}}$, a contradiction. If $4 \mid \rho$, then $(-\gamma)^{\rho/2} = \gamma^{\rho/2} \equiv -1 \pmod{\mathfrak{p}}$. The result follows. □

Remark 2.10. *The order* $\mathrm{ord}_{\mathfrak{p}}(-\gamma)$ *corresponds to the rank of appearance* $\rho_U(P)$ *for the Lucas sequence* $U(\Delta, -a_2\Delta)$.

Chapter 3

Existence of densities for the order problem

With the notation of Chapter 2, we let q be a power of the prime p. We write $K = \mathbb{F}_q(T)$ and $A = \mathbb{F}_q[T]$. Let U be a Lucas sequence with non-zero parameters $a_1, a_2 \in A$. This chapter is dedicated to the study of the rank of appearance $\rho_U(P)$ of primes $P \in A$, which are monic and irreducible polynomials over $\mathbb{F}_q$. More precisely, we ask what is the proportion of primes that have their rank divisible by a fixed integer?

This order problem has been studied by many authors in the classical case [1, 10, 11, 16, 20, 23, 30, 40]. However, it was only studied by Ballot [2, 3] in the function field setting, where he considered the Lucas sequence defined by

$$U_n = \frac{T^n - 1}{T - 1},$$

for all $n \geq 0$, and d a prime number. We aim to generalise his results in Chapters 3 and 4 to d a composite integer and U an arbitrary Lucas sequence.

Studying the rank of primes in Lucas sequences is of interest only if there are primes dividing U_n at some $n \geq 1$. Therefore, for U to truly be a polynomial sequence, we assume that a_1 and a_2 are not both constants in A. Throughout this chapter, we also assume that $\gamma = a/b$ is not a constant in $L = K(a)$. This ensures that U is *non-degenerate*, that is, U_n is non-zero for all $n \geq 1$. Note that $\gamma \notin \mathbb{F}_L := \bar{\mathbb{F}}_q \cap L$ is equivalent to a_1^2/a_2 not being a constant in $\mathbb{F}_q$. This is straightforward using that $\gamma + \gamma^{-1} = a_1^2/a_2 - 2$.

Let $d \geq 2$ be an integer. We study the set $R_q(\gamma, d)$ of primes $P \in A$ such that $\rho_U(P)$ exists and $d \mid \rho_U(P)$, and where P unramified in L. By Lemma 2.5 and its proof, the condition $P \nmid \Delta a_2$ is sufficient for $\rho_U(P)$ to exist and for P not to ramify in L. Therefore,

we define the set precisely as

$$R_q(\gamma, d) = \{P \in A \text{ prime} : P \nmid \Delta a_2 \text{ and } d \mid \rho_U(P)\}.$$

Note that the dependence on γ comes from Lemma 2.5, which states that $\rho_U(P)$ is the order of γ modulo any prime lying above P. However, there are many sequences associated with the same γ. To make sense of the definition of $R_q(\gamma, d)$, note from Lemma 2.8 that any two sequences U and U' associated with the same γ satisfy $U_n = c^{n-1}U'_n$ for all $n \geq 0$, for some $c \in K^\times$. It follows that the set of primes with $d \mid \rho_U(P)$ differs only by finitely many elements from the set of primes with $d \mid \rho_{U'}(P)$. Hence, they have the same density, equal to the density of $R_q(\gamma, d)$.

In addition, note that any $\gamma \in L$ with norm equal to 1 can be associated with a Lucas sequence. If $p \neq 2$ and $\gamma = (u+v\sqrt{\Delta})/d \in L$, for some $u, v, d \in A$, then γ can be associated with the Lucas sequence U with parameters $a_1 = 2(u + d)$ and $a_2 = 2d(u + d)$. The same is true in even characteristic if we consider $L = K(a)$, where a is a root of an irreducible polynomial $X^2 + A_1X + A_2$. If $\gamma = (u + av)/d$, then it can be associated with the Lucas sequence $U(A_1v, dA_1v)$. In this thesis, we take the point of view of Lucas sequences and the notation thereof.

Now, note that we are not directly studying $R_q(\gamma, d)$ itself, but rather two disjoint subsets $R_q^+(\gamma, d)$ and $R_q^-(\gamma, d)$. The subset $R_q^+(\gamma, d)$ is made of primes $P \in R_q(\gamma, d)$ that split completely in L, while $R_q^-(\gamma, d)$ is made of those that are inert in L.

To find the proportion of primes in $R_q^+(\gamma, d)$ and $R_q^-(\gamma, d)$, we use particular notions of prime density 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, where $N \geq 1$. 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

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

The number $\delta(S)$ is called the *Dirichlet density* of S and is the analogue of the Dirichlet density used for rational prime numbers. In a discussion about 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 follows from the classical asymptotic formula $I_n = q^n/n + \mathcal{O}(q^{n/2}/n)$ 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 $R_q(\gamma, d)$ 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 [27], Moree [21], and Sanna [30, 31], and on the elementary approach taken by Ballot [2, 3].

From the definition of the d_3-density, we see that we will need to estimate $R_q^{\pm}(\gamma, d, N)$, the number of primes in $R_q^{\pm}(\gamma, d)$ of degree N. The following analogue of the Chebotarev density theorem, see [9, Proposition 6.4.8], is our main tool for this chapter:

Theorem 3.1. *Let L/K be an extension of global function fields with Galois group G and respective constant fields $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$. Let $\mathcal{C} \subset G$ be a conjugacy class and k be a positive integer such that $\sigma|_{\mathbb{F}_{q^n}} = \tau^k|_{\mathbb{F}_{q^n}}$ for all $\sigma \in \mathcal{C}$, where τ is a Frobenius element of $\mathbb{F}_{q^n}/\mathbb{F}_q$. For all $N \geq 1$, we consider the counting function*

$$C_N(L/K, \mathcal{C}) = \#\{P \in \mathcal{P}_K : \deg(P) = N \text{ and } (L/K, P) = \mathcal{C}\},$$

where $\mathcal{P}_K$ denotes the set of primes of K unramified in L and $(L/K, P)$ denotes the Artin symbol of P. If $N \not\equiv k \pmod n$, then $C_N(L/K, \mathcal{C}) = 0$. If $N \equiv k \pmod n$, then

$$\left| C_N(L/K, \mathcal{C}) - \frac{\#\mathcal{C}}{m}\frac{q^N}{N} \right| \leq \frac{2\#\mathcal{C}}{mN}\left((m + g_L)q^{N/2} + m(2g_K + 1)q^{N/4} + g_L + dm\right),$$

where $m = [L : \mathbb{F}_{q^n}K]$ and $d = [K : \mathbb{F}_q(T)]$, and g_F denotes the genus of a field F.

Our first section is divided into three subsections. In Subsection 3.1.1, we prove necessary and sufficient conditions for $L(\gamma^{1/n})/L$ to be a constant field extension, where $n \geq 1$ and $\gamma \in L$. In the second subsection, we study Kummer extension of function fields. We

prove an exact formula for the degree of $L_{n,d} = L(\zeta_n, \gamma^{1/d})$, where $\zeta_n \in \bar{\mathbb{F}}_q$ is a primitive n-th root of unity and $d \mid n$ is a positive integer. Moreover, we give a bound of the genus of $L_{n,d}$ and conditions for the splitting of certain primes in $L_{n,d}$. In Subsection 3.1.3, we give a formula for the multiplicative order modulo integers.

In Section 3.2, we prove the existence of the d_3-density of $R_q^+(\gamma, d)$. We first study the number of primes in $R_q^+(\gamma, d)$ with fixed degree. We are able to apply Theorem 3.1 to obtain an asymptotic formula of the form

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

for some function f, and where $\delta_q^+(\gamma, d, N)$ is expressed in terms of degrees of Kummer extensions. Then, we prove our main result Theorem 3.18. The proof relies on a technique used by Ballot [2, 3] that consists on partitioning $\mathbb{N}$ into adequate disjoint arithmetic progressions. For all $n \geq 1$ in the same arithmetic progression, we find that $\delta_q^+(\gamma, d, N)$ is a constant independent of n, thus simplifying most calculations. The same is done in Section 3.3 for $R_q^-(\gamma, d)$ to find $\delta_q^-(\gamma, d, N)$. In both cases, we find a series representation of their density.

In Section 3.4, we prove that the d_1-density of $R_q(\gamma, d)$ only exists in the trivial cases. By the equivalence mentioned above, this also holds for the d_2-density.

3.1 Preliminary results

In the section, we prove preliminary results to the study of $R_q(\gamma, d)$. We first give a necessary and sufficient condition for an extension of the form $L(\gamma^{1/n})$ to be an extension of the field of constants of L. In the second subsection, we prove exact formulas for the degrees involving Kummer extensions $L_{n,d} := L(\zeta_n, \gamma^{1/d})$. Moreover, we show that the genus of $L_{n,d}$ is bounded above by a constant times a certain field degree. Finally, we evaluate the multiplicative order of $q \geq 2$ modulo some useful integers.

3.1.1 On constant field extensions

Recall that L/K is an algebraic extension of function fields which is either K or a quadratic extension of K. We fix $\infty \subset L$ a prime ideal of degree 1, i.e., such that $[\mathcal{O}_\infty/\infty : \mathbb{F}_L] = 1$, where $\mathcal{O}_\infty$ is the valuation ring of ∞ in L and $\mathbb{F}_L = L \cap \bar{\mathbb{F}}_q$. By [26, Theorem 2.2.9], the completion of L with respect to the valuation v_∞ is the field $L_\infty := \mathbb{F}_L((\pi))$ of Laurent series in π, a uniformizer of $\mathcal{O}_\infty$. Given $x \in L$, there exist $n_0 \in \mathbb{Z}$ and $(a_i)_{i \geq 0} \subset \mathbb{F}_L$ such that

$$x = \pi^{n_0} \sum_{i \geq 0} a_i \pi^i,$$

where x is seen as an element of L_∞. We say that x is *monic* when $a_0 = 1$. The *monic part* of x, denoted $\tilde{x}$, is defined by $\tilde{x} := a_0^{-1}x$. The coefficient a_0 is called the *sign* of x and acts as an analogue of the leading coefficient for polynomials. We denote it by $\mathrm{sgn}(x)$. We use this construction throughout the chapter, starting with the Theorem 3.3, which provides a necessary and sufficient condition for a radical extension of L to be a constant field extension. We first define the latter, as well as so-called geometric extensions.

Definition 3.2. *Let $K/\mathbb{F}_q$ be an algebraic function field and $L/\mathbb{F}_{q^n}$ be an extension of K, where $n \geq 1$. We say that L/K is*

(1) a constant field extension if $L = \mathbb{F}_{q^n}K$; or

(2) a geometric extension if $\bar{\mathbb{F}}_q \cap L = \bar{\mathbb{F}}_q \cap K$.

Note that an extension of function fields does not necessarily have to be constant or geometric.

Theorem 3.3. *Let $\gamma \in L^\times$. Then, the extension $L(\gamma^{1/n})/L$ is a constant field extension if and only if $\gamma = \mu b^n$ for some $\mu \in \mathbb{F}_L^\times$ and $b \in L^\times$.*

Proof. Let l be a prime. We first prove the result for $n = l^k$ by induction on $k \geq 1$. The base case is identical to the proof of [12, Lemma 3.3], so we may skip a few details.

Assume that $L(\gamma^{1/l})/L$ is a constant field extension. If $L(\gamma^{1/l}) = L$, then $\gamma = b^l$ for some $b \in L$. Next, if $L(\gamma^{1/l})$ is a proper extension of L, we let $M := L(\gamma^{1/l}) \cap \bar{\mathbb{F}}_q$. Thus, we have $M \neq L \cap \bar{\mathbb{F}}_q$ and $ML \subset L(\gamma^{1/l})$. Moreover, since $L(\gamma^{1/l})/L$ has prime degree l, we find that $L(\gamma^{1/l}) = ML$. An extension of finite fields is Galois, hence ML/L is Galois as well. In particular, the polynomial $X^l - \gamma$ splits completely in ML and, by Kummer theory, this shows that $L(\zeta_l) \subset ML$. Since $[L(\zeta_l) : L]$ divides both $l-1$ and l, we conclude that $L(\zeta_l) = L$. It follows that $\mathbb{F}_L := L \cap \bar{\mathbb{F}}_q$ contains an element ν that is not an l-th power. Therefore, $X^l - \nu$ is irreducible over L and $ML = L(\beta)$, where $\beta \in \bar{\mathbb{F}}_q$ is an l-th root of ν. The family $\{1, \beta, \ldots, \beta^{l-1}\}$ forms an L-basis of $L(\gamma^{1/l})$, and

$$\gamma^{1/l} = \sum_{i=0}^{l-1} b_i \beta^i,$$

for some $b_i \in L$. Consider $\sigma \in Gal(L(\gamma^{1/l})/L)$. By Kummer theory, $\sigma(\gamma^{1/l}) = \zeta_l^k \gamma^{1/l}$ for some $0 \leq k \leq l-1$. Similarly, we have $\sigma(\beta) = \zeta_l^m \beta$ for some $0 \leq m \leq l-1$. Hence

$$\sigma(\gamma^{1/l}) = \zeta_l^k \sum_{i=0}^{l-1} b_i \beta^i = \sigma\left(\sum_{i=0}^{l-1} b_i \beta^i\right) = \sum_{i=0}^{l-1} b_i \zeta_l^{mi} \beta_i.$$

By linear independence of $\{1, \beta, \ldots, \beta^{l-1}\}$, we obtain $b_i\zeta_l^k = b_i\zeta_l^{mi}$ for all $0 \le i \le l-1$. Since only one i satisfies $k \equiv mi \pmod{l}$, call it i_0, we conclude that $b_i = 0$ for all $i \neq i_0$. Therefore, we have $\gamma^{1/l} = b_{i_0}\beta^{i_0}$, that is, $\gamma = \mu b^l$, where $\mu = \beta^{i_0 l} = \nu^{i_0}$ and $b = b_{i_0}$.

Assume the result holds for some $k \ge 1$ and $L(\gamma^{1/l^{k+1}})/L$ is a constant field extension. Then, $L(\gamma^{1/l^k})/L$ is a constant field extension. Hence $\gamma = \mu b^{l^k}$ for some $\mu \in \mathbb{F}_L$ and $b \in L$, by the induction hypothesis. It follows that $\tilde{\gamma} = \tilde{b}^{l^k}$. Moreover, since $L(\gamma^{1/l^{k+1}})/L$ is a constant field extension, we see that this is also the case for $L(\tilde{\gamma}^{1/l^{k+1}}) = L(\tilde{b}^{1/l})$ over L. By the base case, there exists $u \in \mathbb{F}_L$ and $c \in L$ such that $\tilde{b} = uc^l$, that is, $\tilde{b} = \tilde{c}^l$ because $\tilde{b}$ is monic. Hence $\gamma = \lambda\tilde{\gamma} = \lambda\tilde{c}^{l^{k+1}}$ and the proof by induction is complete.

Now, write $n = q_1 \cdots q_s$ for some $s \ge 2$, where the q_i's are powers of distinct primes. By the above, we have

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

for some $b_i \in L^\times$ and $\mu_i \in \mathbb{F}_L^\times$. Since the q_i's are powers of distinct primes, we see that $\tilde{b}_1$ is a q_i-th power in L for all $1 \le i \le s$. Thus, $\tilde{\gamma} = b^n$ for some $b \in L^\times$. □

Note that this theorem can be generalised to finite algebraic extensions of $\mathbb{F}_q(T)$. For our purpose, only the quadratic case is needed.

3.1.2 On Kummer extensions

In this subsection, we prove an exact formula for the degree of $L_{n,d} := L(\zeta_n, \gamma^{1/d})$ over the field $\mathbb{F}_{n,d}K$, where $\mathbb{F}_{n,d} = \bar{\mathbb{F}}_q \cap L_{n,d}$ is the constant field of $L_{n,d}$, d, n are positive integers prime to p such that $d \mid n$, and ζ_n is a primitive n-th root of unity. Moreover, the genus of $L_{n,d}$ is showed to be bounded above by $[L_{n,d} : \mathbb{F}_{n,d}L]$ times a constant. Finally, we give properties of the Frobenius element of primes $\mathfrak{p} \in L_{n,d}$ lying above certain primes $P \in K$. We use the following theorem in order to compute the field degrees:

Theorem 3.4. *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 [17, Theorem 9.1]. □

Definition 3.5. *We write $\gamma = \mu\tilde{\gamma}_0^h$, where $\tilde{\gamma}_0 \in L$ is monic, $\mu = \operatorname{sgn}(\gamma) \in \mathbb{F}_L$ and h is the largest integer $t \ge 1$ such that $\tilde{\gamma}$ is an t-th power in L.*

Lemma 3.6. *The largest $v \mid d$ such that $L_{n,v}/L$ is a constant field extension is (d, h). Moreover, we have $\mathbb{F}_{n,d} = \mathbb{F}_L(\zeta_n, \mu^{1/(d,h)})$, where $\mathbb{F}_L := \bar{\mathbb{F}}_q \cap L$.*

Proof. Put $D = (d, h)$ and write $h = Dk$ for some $k \ge 1$. Then

$$L(\zeta_n, \gamma^{1/D}) = L(\zeta_n, \mu^{1/D}\tilde{\gamma}_0^k) = \mathbb{F}_L(\zeta_n, \mu^{1/D})L$$

is a constant field extension of L. Hence $D \mid v$. Indeed, otherwise there would be a prime power $l^\alpha \mid (d,h)$ such that $l^\alpha \nmid v$. Thus, $v' = [l^\alpha, v]$ is greater than v and divides d. However, we find that $L_{n,v'}$ is the compositum of L_{n,l^α} and $L_{n,v}$ over $L(\zeta_n)$, which are constant field extensions. It follows that $L_{u,v'}/L$ is a constant field extension, which contradicts the maximality of v. Let us now prove that $v = D$. By contradiction, assume there exists a prime l such that $lD \mid d$ and $L(\zeta_n, \gamma^{1/lD})/L$ is a constant field extension. Then $L(\gamma^{1/lD})/L$ is a constant field extension as well, and

$$\gamma = \omega c^{lD} = \mu \tilde{c}^{lD},$$

for some $\omega \in \mathbb{F}_L$ and $c \in L^\times$, by Theorem 3.3. Hence $\tilde{\gamma} = \tilde{c}^{lD}$, which, by maximality of h, yields that $lD \mid h$. A contradiction. □

Theorem 3.7. *Let $i = [\mathbb{F}_L : \mathbb{F}_q]$. We have*

$$[\mathbb{F}_{n,d} : \mathbb{F}_q] = \frac{i \cdot \mathrm{ord}_n(q^i) \cdot (d,h)}{(\mathrm{ind}_{\mathbb{F}_L(\zeta_n)^\times}(\mu), d, h)},$$

where $\mathrm{ind}_{\mathbb{F}_L(\zeta_n)^\times}(\mu)$ is the index of μ in the group $\mathbb{F}_q^\times$.

Proof. It is known that $[\mathbb{F}_L(\zeta_n) : \mathbb{F}_q] = i\mathrm{ord}_n(q^i)$. We write $u = \mathrm{ind}_{\mathbb{F}_L(\zeta_n)^\times}(\mu)$ and, by Lemma 3.6, we have

$$\mathbb{F}_{n,d} = \mathbb{F}_L(\zeta_n, \mu^{1/(d,h)}) = \mathbb{F}_L(\zeta_n, v^{1/u_0}),$$

where $u_0 = (d,h)/(d,h,u)$ and $v^{(d,h,u)} = \mu$. We claim that $u_0 = [\mathbb{F}_{n,d} : \mathbb{F}_L(\zeta_n)]$. Indeed, let us show that $X^{u_0} - v$ is irreducible over $\mathbb{F}_L(\zeta_n)$ using Theorem 3.4. Let $l \mid u_0$ be a prime. By contradiction, if $v = c^l$ for some $c \in \mathbb{F}_L(\zeta_n)$, then

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

Because $u_0 \mid q^{i\mathrm{ord}_n(q^i)} - 1$ and by the maximality of u, we obtain $l(d,h,u) \mid u$. This yields a contradiction since $l \mid u_0$. If $4 \mid u_0$ and $v = -4y^4$ for some $y \in \mathbb{F}_L(\zeta_n)$, then $v = (2iy^2)^2$. This is because $4 \mid u_0$ implies that $4 \mid q^{i\mathrm{ord}_n(q^i)} - 1$, so -1 is a square in $\mathbb{F}_L(\zeta_n)$. This contradicts what we proved in the above, and by Theorem 3.4, the polynomial $X^{u_0} - v$ is irreducible over $\mathbb{F}_L(\zeta_n)$. □

Theorem 3.8. *We have $[L_{n,d} : \mathbb{F}_{n,d}L] = d/(d,h)$.*

Proof. Put $d_0 = d/(d,h)$ and write $\gamma = b^{(d,h)}$ for some $b \in \mathbb{F}_{n,d}L$. The latter is possible because of Lemma 3.6. It suffices to show that $X^{d_0} - b$ is irreducible over $\mathbb{F}_{n,d}L$ using Theorem 3.4. By contradiction, if $b \in (\mathbb{F}_{n,d}L^\times)^l$ for some prime $l \mid d_0$, then $L(\gamma^{1/l(d,h)})/L$ is a constant field extension and $\gamma = uc^{l(d,h)}$, where $u \in \mathbb{F}_L$ and $c \in L$. Hence $\tilde{\gamma} = \tilde{c}^{l(d,h)}$

and $l(d,h) \mid h$, which contradicts the coprimality of d_0 and $h/(d,h)$. Finally, if $4 \mid d_0$ and if $b = -4x^4$ for some $x \in \mathbb{F}_{n,d}L$, then $b = (2\zeta_4 x^2)^2$ because $4 \mid d_0$ implies that $\zeta_4 \in \mathbb{F}_{n,d}$. We know from the above argument that $l = 2$ is not possible. □

Now, we prove a bound for the genus of $L_{n,d}/\mathbb{F}_{n,d}$. It will be used on the bound of Theorem 3.1, when applied to Kummer extensions, in order to get rid of the dependence in the degree $[L_{n,d} : \mathbb{F}_{n,d}K]$ in the upper bound.

Proposition 3.9. *Let $g_{n,d}$ be the genus of $L_{n,d}/\mathbb{F}_{n,d}$. Then, there exists a constant $c_0 > 0$, that only depends on γ and g_L, such that $g_{n,d} \leq c_0[L_{n,d} : \mathbb{F}_{n,d}L]$.*

Proof. Put $M := \mathbb{F}_{n,d}L$ and let g_M be the genus of $M/\mathbb{F}_{n,d}$. Note that $L_{n,d} = M(\alpha^{1/d_0})$, where $d_0 = d/(d,h) = [L_{n,d} : M]$ by Theorem 3.8, and $\alpha = v\tilde{\gamma}_0^{h_0}$, with $v \in \mathbb{F}_{n,d}$ a (d,h)-th root of μ and $h_0 = h/(d,h)$. Applying [34, Proposition 3.7.3] to $L_{n,d}$ and M yields

$$g_{n,d} = 1 + d_0\left(g_M - 1 + \frac{1}{2}\sum_{\substack{P \in \mathbb{P}_M \\ v_P(\alpha) \neq 0}} \left(1 - \frac{(v_P(\alpha), d_0)}{d_0}\right) \deg_M(P)\right),$$

where $\mathbb{P}_M$ is the set of primes of M and $\deg_M(P) = [\mathcal{O}_P/P : \mathbb{F}_{n,d}]$ is the degree of P, that is, the degree of its residue class field $\mathcal{O}_P/P$ over $\mathbb{F}_{n,d}$, where $\mathcal{O}_P$ denotes the valuation ring of P in M. Note that $v_P(\alpha) = 0$ if and only if $v_P(\tilde{\gamma}_0) = 0$ because v is a constant and $h_0 \geq 1$. Moreover, by [34, Theorem 3.6.3], we have $g_M = g_L$ the genus of $L/\mathbb{F}_q$. Thus,

$$g_{n,d} \leq d_0\left(g_L + \sum_{\substack{P \in \mathbb{P}_M \\ v_P(\tilde{\gamma}_0) \neq 0}} \frac{\deg_M(P)}{2}\right).$$

Let $\pi = P \cap L$, so that P is a prime lying above π in M. By [34, Theorem 3.6.3] again, we know that $\mathcal{O}_P/P$ is the compositum of $\mathcal{O}_\pi/\pi$ and $\mathbb{F}_{n,d}$. Hence

$$\deg_M(P) = [\mathcal{O}_P/P : \mathbb{F}_{n,d}] = \frac{[\mathcal{O}_P/P : \mathbb{F}_q]}{[\mathbb{F}_{n,d} : \mathbb{F}_q]} = \frac{[\mathcal{O}_\pi/\pi : \mathbb{F}_q]}{([\mathcal{O}_\pi/\pi : \mathbb{F}_q], [\mathbb{F}_{n,d} : \mathbb{F}_q])},$$

and we find that $\deg_M(P) \leq \deg_L(\pi)$. Since $\tilde{\gamma}_0 \in L$, we have $v_P(\tilde{\gamma}_0) = 0$ if and only if $v_\pi(\tilde{\gamma}_0) = 0$. Finally, because π splits into at most $\deg_L(\pi)$ primes in M, we obtain

$$\sum_{\substack{P \in \mathbb{P}_M \\ v_P(\tilde{\gamma}_0) \neq 0}} \frac{\deg_M(P)}{2} \leq \sum_{\substack{\pi \in \mathbb{P}_L \\ v_\pi(\tilde{\gamma}_0) \neq 0}} \sum_{\substack{P \in \mathbb{P}_M \\ P \mid \pi}} \frac{\deg_L(\pi)}{2} \leq \sum_{\substack{\pi \in \mathbb{P}_L \\ v_\pi(\tilde{\gamma}_0) \neq 0}} \frac{\deg_L(\pi)^2}{2},$$

and the result follows. □

Lemma 3.10. *Let $P \nmid \Delta a_2$ be a prime in K and $\mathfrak{p} \in L_{n,d}$ be a prime lying over P. We denote by $\sigma_\mathfrak{p}$ the Frobenius element $(L_{n,d}/K, \mathfrak{p})$. Then, we have*

$$NP \equiv \epsilon_P \pmod{n} \quad \textit{and} \quad d \mid \iota_U(P)$$

if and only if $\sigma_\mathfrak{p} = \mathrm{id}$ when $\epsilon_P = 1$, and otherwise

$$\sigma_\mathfrak{p}(\zeta_n) = \zeta_n^{-1} \quad \textit{and} \quad \sigma_\mathfrak{p}(\gamma^{1/d}) = \gamma^{-1/d}.$$

Proof. Assume that $NP \equiv \epsilon_P \pmod{n}$ and $d \mid \iota_U(P)$. Then, we have

$$\sigma_\mathfrak{p}(\zeta_n) \equiv \zeta_n^{NP} = \zeta_n^{\epsilon_P} \pmod{\mathfrak{p}}.$$

Since both sides are constants in $L_{n,d}$, we have equality. Next, let $\pi := \mathfrak{p} \cap \mathcal{O}_L$. On the one hand, we have $\sigma_\mathfrak{p}(\gamma) = (L/K, \pi)(\gamma) = \gamma^{\epsilon_P}$. Taking the d-th root on both sides, we obtain $\sigma_\mathfrak{p}(\gamma^{1/d}) = \zeta_d^k \gamma^{\epsilon_P/d}$ for some $k \in \mathbb{Z}$. On the other hand, we have

$$\sigma_\mathfrak{p}(\gamma^{1/d}) \equiv \gamma^{NP/d} \pmod{\mathfrak{p}}$$

by definition of the Frobenius element. Now, because $d \mid \iota_U(P)$, we know that $\rho_U(P)$ divides $(NP - \epsilon_P)/d$. Using Lemma 2.5, we obtain

$$\sigma_\mathfrak{p}(\gamma^{1/d}) \equiv \gamma^{(NP-\epsilon_P)/d} \cdot \gamma^{\epsilon_P/d} \equiv \gamma^{\epsilon_P/d} \pmod{\mathfrak{p}}$$

Hence $\zeta_d^k \gamma^{\epsilon_P/d} \equiv \gamma^{\epsilon_P/d} \pmod{\mathfrak{p}}$, and multiplying by $\gamma^{-\epsilon_P/d}$ yields $\zeta_d^k \equiv 1 \pmod{\mathfrak{p}}$. Now, because both sides are constants, we must have equality. Therefore, $\sigma_\mathfrak{p}$ is completely determined by the relations

$$\sigma_\mathfrak{p}(\zeta_n) = \zeta_n^{\epsilon_P} \quad \text{and} \quad \sigma_\mathfrak{p}(\gamma^{1/d}) = \gamma^{-1/d},$$

which completes this side of the equivalence.

For the converse, we have $\zeta_n^{\epsilon_P} \equiv \zeta_n^{NP} \pmod{\mathfrak{p}}$ by definition of the Frobenius element, so that $\zeta_n^{NP-\epsilon_P} = 1$. It follows directly that $NP \equiv \epsilon_P \pmod{n}$. Next, we have

$$\gamma^{(NP-\epsilon_P)/d} \equiv (\gamma^{1/d})^{NP} \gamma^{-\epsilon_P/d} = \sigma_\mathfrak{p}(\gamma^{1/d}) \gamma^{-\epsilon_P/d} = 1 \pmod{\mathfrak{p}},$$

which holds modulo π. Therefore, we have $\rho_U(P)$ divides $(NP - \epsilon_P)/d$ by Lemma 2.5, and we obtain $d \mid \iota_U(P)$. □

3.1.3 An arithmetic property of the multiplicative order

Let d, q be coprime integers. The first result of this subsection gives some basic arithmetic properties for numbers of the form $(q^N - 1, d^\infty)$. As a consequence, we prove a formula for $\mathrm{ord}_{dv}(q)$ that generalises the well-known formula

$$\mathrm{ord}_{l^k}(q) = \mathrm{ord}_l(q) \cdot \begin{cases} 1, & \text{if } 1 \le k \le \alpha; \\ l^{k-\alpha}, & \text{if } k > \alpha, \end{cases}$$

where $\alpha = v_l(q^{\mathrm{ord}_l(q)} - 1)$ and $l \ge 3$ is prime, and its analogue for $l = 2$. For every $m \ge 1$ such that $f := \mathrm{ord}_d(q)$ divides m, we define $\mathcal{P}(m)$ the proposition

$$\mathcal{P}(m): \quad 2 \| d, \quad q \equiv 3 \pmod 4 \quad \text{and} \quad 2 \nmid m, \tag{3.1}$$

Throughout this thesis, we use the Iverson brackets, defined for all propositions $\mathcal{P}$ by $[\mathcal{P}] = 1$ if $\mathcal{P}$ is true, and $[\mathcal{P}] = 0$ otherwise. The following lemma is enough to see that interesting things might happen when the proposition $\mathcal{P}(m)$ is true:

Lemma 3.11. *Let $m, n, q \ge 1$ be integers with $(d, q) = 1$ and $d \mid q^m - 1$. Then*

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

Proof. The map $d \mapsto (k, d^\infty)$, where k is a fixed integer, defines a 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 using $v_2(q^m + 1) = 1$ if $\mathcal{P}(m)$ is false. □

Lemma 3.12. *Let $q \ge 1$ be prime to d and $f = \mathrm{ord}_d(q)$. For all $v \mid d^\infty$, we have*

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

Proof. Assume $v_2(d) \ne 1$ and put $n = dv/(q^f - 1, dv)$. By Lemma 3.11, with $m = f$ and $n = n$, we have $dv \mid q^{fn} - 1$. Hence $n = tm$, where $m \ge 1$ and $t := \mathrm{ord}_{dv}(q)/f$. By Lemma

3.11 again, we have

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

so 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 $\mathrm{ord}_{2n}(q) = \mathrm{ord}_n(q)$. 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. □

3.2 The d_3-density of $R_q^+(\gamma, d)$

Throughout this section and the rest of this chapter, we write $e_N^+ = (q^N-1, d^\infty)/d$ for all $N \geq 1$ divisible by $f := \mathrm{ord}_q(d)$. Recall that $R_q^+(\gamma, d)$ is the set

$$R_q^+(\gamma, d) = \{P \in \mathcal{P}_+ : P \nmid \Delta a_2,\ d \mid \rho_U(P) \text{ and } \epsilon_P = 1\}.$$

In this chapter, we prove that $R_q^+(\gamma, d)$ has a d_3-density. Moreover, we obtain a formula for the density in the form of a series on the divisors of d^∞.

3.2.1 The proportion by degree

Given a natural number $N \geq 1$, we first study the function $R_q^+(\gamma, d, N)$ that counts the number of primes in in $R_q^+(\gamma, d)$ of degree N. By Lemma 2.5, we see that d must divide $q^N - 1$ for $R_q^+(\gamma, d, N)$ to be positive. Therefore, the order $f = \mathrm{ord}_d(q)$ must divide N. Note that $[\mathbb{F}_L : \mathbb{F}_q]$ must divide N as well. Indeed, when $L = K$ or L/K is geometric, we have $\mathbb{F}_L = \mathbb{F}_q$ and $[\mathbb{F}_L : \mathbb{F}_q] = 1$ trivially divides N. However, when $L = \mathbb{F}_{q^2}(T)$, by [29, Proposition 8.13], a prime $P \in K$ splits in L only if it has even order, i.e., $[\mathbb{F}_L : \mathbb{F}_q] \mid N$. Therefore, we consider positive $N \equiv 0 \pmod{f_L}$, where $f_L = [[\mathbb{F}_L : \mathbb{F}_q], f]$.

For a Galois extension M/K, we let $\{M\}$ denote the set of primes in K that completely split in M and $\{M\}_N$ the number of those primes that have degree N. In our first result, we write $R_q^+(\gamma, d, N)$ as a linear combination of functions $\{L_{n,d}\}_N$. It is an analogue of [21, Proposition 1] in the classical case.

Lemma 3.13. *For each $N \equiv 0 \pmod{f_L}$, we have*

$$R_q^+(\gamma, d, N) = \sum_{v \mid e_N^+} \sum_{u \mid d} \mu(u) \{L_{dv,uv}\}_N.$$

Proof. Let $S(N)$ be the set of monic irreducible polynomials in $R_q^+(\gamma, d)$ with degree N. Any prime $P \in S(N)$ satisfies

$$\deg(P) = N, \quad P \nmid \Delta a_2, \quad d \mid \rho_U(P), \quad \text{and} \quad \epsilon_P = 1.$$

Since $q^N - 1 = \rho_U(P)\iota_U(P)$, the condition $d \mid \rho_U(P)$ is equivalent to $d(\iota_U(P), d^\infty) \mid q^N - 1$, that is, there exists a unique $v \mid d^\infty$ such that

$$dv \mid q^N - 1, \quad v \mid \iota_U(P) \quad \text{and} \quad \left(\frac{\iota_U(P)}{v}, d\right) = 1. \tag{3.2}$$

The last condition in (3.2) is equivalent to $lv \nmid \iota_U(P)$ for all primes $l \mid d$. Hence, $S(N)$ is the disjoint union

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

where $S_{u,v}(N) = \{P \in S(N) : \ dv \mid q^N - 1 \text{ and } uv \mid \iota_U(P)\}$. Finally, the set $S_{u,v}(N)$ has cardinality $\{L_{dv,uv}\}_N$ by Lemma 3.10. The result follows by the inclusion-exclusion principle. □

Lemma 3.14. *If $[\mathbb{F}_{n,d} : \mathbb{F}_q] \nmid N$, then $\{L_{n,d}\}_N = 0$. Otherwise, there exists $c_1 > 0$, that only depends on γ and L, such that*

$$\left| \{L_{n,d}\}_N - \frac{q^N}{N} \frac{(d,h)}{[L : \mathbb{F}_L K]d} \right| \leq 2c_1 \cdot \frac{q^{N/2}}{N}.$$

Proof. It suffices to apply the Chebotarev density theorem, i.e., Theorem 3.1. The extension $L_{d,d}/K$ is Galois since it is the splitting field of $X^d - \gamma$ if $L = K$, and of

$$(X^d - \gamma)(X^d - \sigma_L(\gamma)),$$

otherwise, where σ_L is the non-trivial automorphism of L/K. They are separable polynomials because $p \nmid n$ and $\gamma \neq 0$. It follows that $L_{n,d}/K$ is Galois as well since $L_{n,d}/L_{d,d}$ is a constant field extension. We choose $\mathcal{C} = \{\mathrm{id}\}$ for the conjugacy class, as $P \in K$ splits completely in $L_{n,d}$ if and only if $(L_{n,d}/K, \mathfrak{p}) = \mathrm{id}$, where $\mathfrak{p} \in L_{n,d}$ is a prime above P. It

follows from Theorem 3.1 that $\{L_{n,d}\}_N = 0$ if $[\mathbb{F}_{n,d} : \mathbb{F}_q] \nmid N$, and that

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

for some $c_1 > 0$, otherwise. The constant c_1 is obtained using Proposition 3.9 and

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

valid for all $N \geq 1$. We have

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

where c_0 depends only on γ and L. The result follows using Theorem 3.8. □

For the rest of the chapter, we write $f_{u,v} = [\mathbb{F}_{dv,uv} : \mathbb{F}_q]$ for all $u \mid d$ and $v \mid d^\infty$. Combining Lemmas 3.13 and 3.14, we obtain the following theorem in which $f_{u,v}$ plays a crucial role:

Theorem 3.15. *For each positive $N \equiv 0 \pmod{f_L}$, we have*

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

where c_1 is the constant defined in Lemma 3.14 and

$$\delta_q^+(\gamma, d, N) = \frac{1}{[L : \mathbb{F}_L K]} \sum_{v \mid e_N^+} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{uv} [f_{u,v} \mid N].$$

Proof. Let $S_q^+(\gamma, d, N)$ denote the difference $R_q^+(\gamma, d, N) - \delta_q^+(\gamma, d, N) q^N / N$. Using Lemmas 3.13 and 3.14, we have

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

the sought result. □

3.2.2 The existence of the density

The proof of the existence and the computation of the d_3-density of $R_q^+(\gamma, d)$ requires to partition $\mathbb{N}$ into a countable union of distinct arithmetic progressions, following a method

of Ballot [3]. Recall that $f_L = [[\mathbb{F}_L : \mathbb{F}_q], f]$. We have

$$\mathbb{N} = \bigsqcup_{j=1}^{f_L-1} S_j \sqcup \bigsqcup_{w|d^\infty} \bigsqcup_{\substack{\alpha=1 \\ (\alpha,d)=1}}^{d} A_{w,\alpha}, \tag{3.3}$$

where $S_j = \{f_L n + j : n \geq 0\}$ and $A_{w,\alpha} = \{f_L w(\alpha + dn) : n \geq 0\}$. We have $\delta_q^+(\gamma, d, N) = 0$ for all $N \in S_j$. This is because $R_q^+(\gamma, d, N)$ is empty only if $f_L \nmid N$. For $N \in A_{w,\alpha}$, we have $e_N^+ = e_{f_L w}^+$ by Lemma 3.11, which is an integer that depends only on w. Moreover, we have $f_{u,v} \mid N$ if and only if $f_{u,v} \mid f_L w$. Indeed, by Theorem 3.7, we have $f_{u,v} = i\mathrm{ord}_{dv}(q^i)k_0$ for some $k_0 \mid d^\infty$, where $i = [\mathbb{F}_L : \mathbb{F}_q]$. By Lemma 3.12, we have $i\mathrm{ord}_{dv}(q^i) = f_L k_1$ for some $k_1 \mid d^\infty$. Hence $f_{u,v} = f_L k$, where $k \mid d^\infty$. We obtain

$$\delta_q^+(\gamma, d, N) = \frac{1}{[L : \mathbb{F}_L K]} \sum_{v | e_{f_L w}^+} \sum_{u|d} \frac{\mu(u)(uv, h)}{uv} \cdot [f_{u,v} \mid f_L w], \tag{3.4}$$

which is a constant that does not depend on n, nor α. We denote this quantity by δ_w^+, and define $\delta_q^+(\gamma, d)$ as

$$\delta_q^+(\gamma, d) = \frac{\varphi(d)}{d f_L} \sum_{w|d^\infty} \frac{\delta_w^+}{w}. \tag{3.5}$$

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

The following lemma displays two results that can be found in the literature. (See for instance the proofs of [21, Lemma 2] or [30, Lemma 6.3].) However, the proof is usually left to the reader. Here, we provide a short proof.

Lemma 3.16. *There exists $c_2 > 0$ such that for every $x \geq e^{2\omega(d)}$, we have*

$$\sum_{\substack{w|d^\infty \\ w \leq x}} 1 \leq c_2 \log(x)^{\omega(d)} \quad \text{and} \quad \sum_{\substack{w|d^\infty \\ w > x}} \frac{1}{w} \leq \frac{2c_2 \log(x)^{\omega(d)}}{x}.$$

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 prime divisors l of 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 $\log_l(x) + 1 \leq C_l \log(x)$. Then, we choose c_2 equal the product of the C_l's over all primes $l \leq e^2$. Next, we apply the Abel summation formula to the series on the right, so that $M_d(x)$ re-appears. We find

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

Call $I(x)$ the integral on the right-hand side of the above 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 3.17. *For every $N \geq e^{2\omega(d)}$, we have*

$$\left|\frac{1}{N}\sum_{n=1}^{N}\delta_q^+(\gamma,d,n) - \delta_q^+(\gamma,d)\right| \leq c_2\varphi(d)\left(1+\frac{2}{df_L}\right)\frac{\log(N)^{\omega(d)}}{N},$$

where c_2 is the absolute constant defined in Lemma 3.16.

Proof. From the partition of $\mathbb{N}$ given in (3.3), we have

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

where $A_{w,\alpha}(N) = \#A_{w,\alpha} \cap [1,N]$. Moreover, we used $\delta_q^+(\gamma,d,n) = 0$, if $n \in S_j$, and $\delta_q^+(\gamma,d,n) = \delta_w^+$, if $n \in A_{w,\alpha}$. Note that $w \leq N$ and

$$A_{w,\alpha}(N) = \left\lfloor \frac{N + f_L w(d-\alpha)}{df_L w} \right\rfloor,$$

which, by the properties of the floor function, satisfies

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

Therefore, on the one hand, we have

$$\begin{aligned} S_N &\geq \frac{\varphi(d)}{df_L}\sum_{\substack{w|d^\infty\\w\leq N}}\frac{\delta_w^+}{w} - \frac{\varphi(d)}{N}\sum_{\substack{w|d^\infty\\w\leq N}}\delta_w^+ \\ &= \delta_q^+(\gamma,d) - \frac{\varphi(d)}{N}\sum_{\substack{w|d^\infty\\w\leq N}}\delta_w^+ - \frac{\varphi(d)}{df_L}\sum_{\substack{w|d^\infty\\w>N}}\frac{\delta_w^+}{w}. \end{aligned}$$

and on the other hand,

$$\begin{aligned} S_N &\leq \frac{\varphi(d)}{df_L}\sum_{\substack{w|d^\infty\\w\leq N}}\frac{\delta_w^+}{dw} + \frac{\varphi(d)}{N}\sum_{\substack{w|d^\infty\\w\leq N}}\delta_w^+ \\ &= \delta_q^+(\gamma,d) + \frac{\varphi(d)}{N}\sum_{\substack{w|d^\infty\\w\leq N}}\delta_w^+ - \frac{\varphi(d)}{df_L}\sum_{\substack{w|d^\infty\\w>N}}\frac{\delta_w^+}{w}. \end{aligned}$$

Finally, we obtain

$$|S_N - \delta_q^+(\gamma,d)| \le \frac{\varphi(d)}{N}\sum_{\substack{w|d^\infty\\ w\le N}}\delta_w^+ + \frac{\varphi(d)}{df_L}\sum_{\substack{w|d^\infty\\ w>N}}\frac{\delta_w^+}{w} \le c_2\varphi(d)\left(1+\frac{2}{df_L}\right)\frac{\log(N)^{\omega(d)}}{N},$$

where we used that $\delta_w^+ \le 1$, and Lemma 3.16. □

We are now ready to prove the main result of this section, which is that $\delta_q^+(\gamma,d)$ is the d_3-density of $R_q^+(\gamma,d)$.

Theorem 3.18. *There exists a positive constant $c_3 > 0$, that may only depend on d, γ and g_L, such that*

$$\left|\frac{1}{N}\sum_{n=1}^{N}\frac{R_q^+(\gamma,d,n)}{q^n/n} - \delta_q^+(\gamma,d)\right| \le c_2\varphi(d)\left(1+\frac{2}{df_L}\right)\frac{\log(N)^{\omega(d)}}{N} + \frac{c_3}{N},$$

for all $N \ge e^{2\omega(d)}$, where c_2 is the constant defined in Lemma 3.16. In particular, $R_q^+(\gamma,d)$ has d_3-density equal to $\delta_q^+(\gamma,d)$.

Proof. First, we put

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

By Lemma 3.17, for all $N \ge e^{2\omega(d)}$, we have

$$|R_N - \delta_q^+(\gamma,d)| \le |R_N - S_N| + c_2\varphi(d)\left(1+\frac{2}{df_L}\right)\frac{\log(N)^{\omega(d)}}{N},$$

Let us bound $|R_N - S_N|$. By Theorem 3.15, and since $\delta_q^+(\gamma,d,n) = 0$ if $f_L \nmid n$, we have

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

By Lemma 3.11, we see that $e_n^+ \le 2^{v_2(q^{f_L}+1)}e_{f_L}^+ n/f_L$. This implies that the number of divisors of e_n^+ is at most $v_2(q^{f_L}+1)\tau(e_{f_L}^+)n/f_L$, using $\tau(m) \le m$ for all $m \ge 1$. Hence

$$|R_N - S_N| \le \frac{2^{\omega(d)+1}v_2(q^{f_L}+1)\tau(e_{f_L}^+)c_1}{Nf_L}\sum_{\substack{n=1\\ f_L|n}}^{N}nq^{-n/2} =: \frac{c}{Nf_L}\sum_{\substack{n=1\\ f_L|n}}^{N}nq^{-n/2}.$$

We obtain

$$|R_N - S_N| \leq \frac{c}{Nf_L} \sum_{\substack{n=1 \\ f_L | n}}^{+\infty} nq^{-n/2} = \frac{c}{N} \frac{q^{-f_L/2}}{(q^{-f_L/2}-1)^2} =: \frac{c_3}{N}.$$

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

Corollary 3.19. *The set $R_q^+(\gamma, d)$ has d_4 and Dirichlet density equal to $\delta_q^+(\gamma, d)$.*

Proof. Theorem 3.18 establishes the existence and the value of the d_3-density of $R_q^+(\gamma, d)$. The result follows from [4, Theorem A]. □

We successfully proved the existence of the d_3-density of $R_q^+(\gamma, d)$ for the non-trivial cases. However, the density $\delta_q^+(\gamma, d)$ is expressed via a series on all divisors of d^∞, which makes its computation difficult. We dedicate Chapter 4 to the search of a closed-form formula for the density, that is, an expression that requires only finitely many simple operations.

3.3 The d_3-density of $R_q^-(\gamma, d)$

In this section, we follow the same method as in the previous one to prove the existence of the d_3-density of

$$R_q^-(\gamma, d) = \{P \in \mathcal{P}_+ : P \nmid \Delta a_2,\ d \mid \rho_U(P) \text{ and } \epsilon_P = -1\}.$$

That is, we first study the function $R_q^-(\gamma, d, N)$ that counts the number of primes in $R_q^-(\gamma, d)$ that have degree N. Next, we partition $\mathbb{N}$ in a way that allows us to find the d_3-density expressed as a series.

Note that in many cases, the set $R_q^-(\gamma, d)$ is empty. For instance, when $L = K$, every prime $P \in K$ satisfies $\epsilon_P = 1$. Moreover, when $[L : K] = 2$, if there is no integer $k \geq 1$ such that $d \mid q^k + 1$, then $R_q^-(\gamma, d)$ is empty because d needs to divide $NP + 1 = q^{\deg(P)} + 1$ for all primes $P \in R_q^-(\gamma, d)$. Therefore, for the rest of the chapter, we assume $[L : K] = 2$ and the existence of k. Note that [5, Theorem 27, Section 2] provides necessary and sufficient condition for the existence of k. When it exists, we have $f = k = 1$ if $d = 2$, and $f = 2k$ otherwise. Now, we have only two cases to consider: $2 \mid f$ and $(d, q-1) \leq 2$, and $d = 2$. This comes from the following elementary lemma:

Lemma 3.20. *Assume $d \mid q^k + 1$ for some $k \geq 1$. Then, $R_q^-(\gamma, d)$ is not empty only if either $2 \mid f$ and $(d, q-1) \leq 2$, or $d = 2$.*

Proof. Let $P \in R_q^-(\gamma, d)$. Since $d \mid \rho_U(P)$, we have $d \mid NP + 1$ by Lemma 2.5. We first assume $d \geq 3$. We saw that $2 \mid f$ because of the existence of $k \geq 1$ such that $d \mid q^k + 1$. Now, let l be a prime that divides $(d, q-1)$. Then, l divides $NP+1$, which implies $l = 2$, since $(NP+1, q-1) \leq 2$. We write $(d, q-1) = 2^n$ for some $n \geq 0$. We trivially have $n \leq 1$ when $q \equiv 3 \pmod 4$ or $2 \mid q$. When $q \equiv 1 \pmod 4$, we have $v_2(NP+1) = 1$, and thus $v_2(d) \leq 1$ and $n = v_2(d)$. □

The case $d = 2$ turns out to be quite peculiar and is treated in a separate subsection. However, the method remains the same and, in both cases, we write $R_q^-(\gamma, d, N)$ as a linear combination of functions $C_N(L_{n,d}/K, \mathcal{C})$ defined in Theorem 3.1, where $d \mid n$. Here, we take $\mathcal{C}$ as the conjugacy class of a single element $\sigma \in Gal(L_{n,d}/K)$, when it exists, such that $\sigma(a) = b$, $\sigma(\zeta_n) = \zeta_n^{-1}$, and $\sigma(\gamma^{1/d}) = \gamma^{-1/d}$.

Lemma 3.21. *Assume that there exists $\sigma \in Gal(L_{n,d}/K)$ such that $\sigma(a) = b$, $\sigma(\zeta_n) = \zeta_n^{-1}$, and $\sigma(\gamma^{1/d}) = \gamma^{-1/d}$. Then, σ belongs to the center of $Gal(L_{n,d}/K)$.*

Proof. First, note that $L(\zeta_n)/K$ is an abelian extension. If $L = \mathbb{F}_{q^2}L$, then $L(\zeta_n)/K$ is a constant field extension, which is always cyclic. If L/K is geometric, then

$$Gal(L(\zeta_n)/K) \cong Gal(L/K) \times Gal(K(\zeta_n)/K),$$

by [17, Theorem 1.14] because $L \cap K(\zeta_n) = K$. But L/K is abelian since it is a quadratic extension, and $K(\zeta_n)$ is an extension of the field of constants. Hence $L(\zeta_n)/K$ is abelian. Now, we know that any automorphism $\sigma_1 \in Gal(L_{n,d}/K)$ is uniquely determined by the images of a, ζ_n, and $\gamma^{1/d}$. Therefore, we only need to check whether $\sigma_1\sigma\sigma_1^{-1}(x) = \sigma(x)$ for all $\sigma_1 \in Gal(L_{n,d}/K)$ and $x \in \{a, \zeta_n, \gamma^{1/d}\}$. By the above, we know that it is true for $x \in \{a, \zeta_n\}$ by restriction of σ and σ_1 to $L(\zeta_n)$. Finally, since $\sigma_1(\gamma)$ is equal to one of γ and γ^{-1}, we obtain $\sigma_1(\gamma^{1/d}) = \zeta_d^k\gamma^{\pm 1/d}$ for some $k \in \mathbb{Z}$. It is then easy to verify that σ and σ_1 commute. □

We proceed as in Section 3.2 by looking at the fields $L_{dv,uv}$, where $u \mid d$ and $v \mid d^\infty$. Again, we call $\sigma_{u,v}$ the automorphism of $L_{dv,uv}$ defined in Lemma 3.21, when it exists. That is, the automorphism such that $\sigma_{u,v}(a) = b$, $\sigma_{u,v}(\zeta_{dv}) = \zeta_{dv}^{-1}$, and $\sigma_{u,v}(\gamma^{1/uv}) = \gamma^{-1/uv}$. Finally, we write $e_N^- = (q^N + 1, d^\infty)/d$ for all $N \geq 1$ such that $d \mid q^N + 1$.

3.3.1 The case $2 \mid f$ and $(d, q-1) \leq 2$

Note that by our hypotheses, we have $d \mid q^N + 1$ if and only if $f \mid 2N$ and $f \nmid N$. Thus, we assume $N \equiv f/2 \pmod f$. Otherwise, $R_q^-(\gamma, d, N) = 0$.

Theorem 3.22. *For each positive $N \equiv f/2 \pmod f$, we have*

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

where $c_1 > 0$ is the constant defined in Lemma 3.14 and

$$\delta_q^-(\gamma, d, N) = \frac{1}{[L : \mathbb{F}_L K]} \sum_{v | e_N^-} \sum_{u | d} \frac{\mu(u)(uv, h)}{uv} \cdot \mathcal{B}_N(u, v),$$

with $\mathcal{B}_N(u, v) := [\sigma_{u,v}$ exists and $N \equiv f_{u,v}/2 \pmod{f_{u,v}}]$.

Proof. As in the proof of Lemma 3.13, we write $R_q^-(\gamma, d, N)$ as a double sum. Note that $\epsilon_P = 1$ should be replaced by $\epsilon_P = -1$, and $q^N - 1$ by $q^N + 1$. We obtain

$$R_q^-(\gamma, d, N) = \sum_{v | e_N^-} \sum_{u | d} \mu(u) S_{u,v}^-(N),$$

where $S_{u,v}^-(N)$ is the number of primes $P \nmid \Delta a_2$ in K of degree N such that $\epsilon_P = -1$, $dv \mid q^N + 1$, and $uv \mid \iota_U(P)$. By Lemma 3.10, this is equivalent to $(L_{dv,uv}/K, \mathfrak{p}) = \sigma_{u,v}$ for all primes $\mathfrak{p} \in L_{dv,uv}$ lying above P, when $\sigma_{u,v}$ exists. Hence $S_{u,v}^-(N)$ counts exactly the primes P whose Artin symbol satisfies $(L_{dv,uv}/K, P) = \{\sigma_{u,v}\}$, since the conjugacy class of $\sigma_{u,v}$ is the singleton $\{\sigma_{u,v}\}$ by Lemma 3.21. Therefore, with the notation of Theorem 3.1, we have $S_{u,v}^-(N) = C_N(L_{dv,uv}/K, \{\sigma_{u,v}\}) \cdot [\sigma_{u,v}$ exists$]$. We now want to apply Theorem 3.1 to $C_N(L_{dv,uv}/K, \{\sigma_{u,v}\})$ for all $u \mid d$ and $v \mid e_N^-$ whenever $\sigma_{u,v}$ exists. First, we determine $k \geq 1$ such that $\sigma_{u,v}|_{\mathbb{F}_{dv,uv}} = \tau^k|_{\mathbb{F}_{dv,uv}}$, where τ is the Frobenius automorphism of $\mathbb{F}_{dv,uv}/\mathbb{F}_q$. Since $\sigma_{u,v}^2 = \mathrm{id}$, the same is true for the restriction. Therefore, $\sigma_{u,v}|_{\mathbb{F}_{dv,uv}}$ is either the identity, or has order two. The relation $\sigma_{u,v}(\zeta_{dv}) = \zeta_{dv}^{-1}$ ensures that it has order two, because $d \geq 3$ and $\zeta_{dv} \neq \zeta_{dv}^{-1}$. We obtain

$$\tau^{2k}|_{\mathbb{F}_{dv,uv}} = \mathrm{id} \quad \text{and} \quad \tau^k|_{\mathbb{F}_{dv,uv}} \neq \mathrm{id},$$

which implies that $f_{u,v}/2$ is a good choice for k. By Theorem 3.1, we obtain

$$\left| C_N(L_{dv,uv}/K, \{\sigma_{u,v}\}) - \frac{1}{[L_{dv,uv} : \mathbb{F}_{dv,uv} K]} \frac{q^N}{N} \right| \leq 2c_1 \cdot \frac{q^{N/2}}{N}, \tag{3.6}$$

for all $N \equiv f_{u,v}/2 \pmod{f_{u,v}}$, where $c_1 > 0$ is the same constant as in Lemma 3.14. Otherwise, we have $C_N(L_{dv,uv}/K, \{\sigma_{u,v}\}) = 0$. Finally, we obtain

$$\left| R_q^-(\gamma, d, N) - \delta_q^-(\gamma, d, N) \cdot \frac{q^N}{N} \right| \leq 2c_1 \sum_{v | e_N^-} \sum_{u | d} |\mu(u)| \cdot \frac{q^N}{N},$$

where we used (3.6), Theorem 3.8 for the degree, and $\mathcal{B}_N(u,v) \leq 1$. The right-hand side is equal to $2^{\omega(d)+1} c_1 \tau(e_N^-) q^N/N$, the upper bound we sought. □

We compute the d_3-density by partitioning $\mathbb{N}$ in a convenient way. The partition we use is different from the one used in Section 3.2. We have $\mathbb{N} = A \sqcup B$, where A the set of positive integers $N \not\equiv f/2 \pmod f$ and

$$B = \bigsqcup_{w \mid d'^{\infty}} \bigsqcup_{\substack{\alpha=1 \\ (\alpha,[2,d])=1}}^{d} B_{w,\alpha}, \tag{3.7}$$

where $d' = d/(d, 2^\infty)$ and $B_{w,\alpha} = \{fw(\alpha + [2,d]n)/2 : n \geq 0\}$. We see that $\delta_q^-(\gamma, d, N) = 0$ for all $N \in A$ since $R_q^-(\gamma, d, N) = 0$ when $N \not\equiv f/2 \pmod f$. Moreover, we have

$$e_N^- = \frac{e_{2N}^+}{(q^N - 1, d^\infty)} = \frac{e_{fw}^+}{(q^N - 1, 2^\infty)},$$

for all $N \in B_{w,\alpha}$, by Lemma 3.11 and because $(q^N + 1, q^N - 1) \leq 2$. Since $v_2(N) = v_2(f)$ and because $2 \nmid w$, we have $(q^N - 1, 2^\infty) = (q^{fw} - 1, 2^\infty)$. Hence $e_N^- = e_{fw/2}^-$ for all $N \in B_{w,\alpha}$, which only depends on w. We obtain

$$\delta_q^-(\gamma, d, N) = \frac{1}{[L : \mathbb{F}_L K]} \sum_{v \mid e_{fw/2}^-} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{uv} \cdot \mathcal{B}_N(u, v),$$

for all $N \in B_{w,\alpha}$. The best-case scenario would be that $\delta_q^-(\gamma, d, N)$ only has a dependence on w, akin to its analogue $\delta_q^+(\gamma, d, N)$ in (3.4). Combining Theorem 3.7 and Lemma 3.12, we see that $f_{u,v} = fk$ for some $k \mid d^\infty$. Therefore, the congruence $N \equiv f_{u,v}/2 \pmod{f_{u,v}}$ is equivalent to $fw \equiv f_{u,v} \pmod{2f_{u,v}}$ for all $N \in B_{w,\alpha}$. Hence, we let

$$\delta_w^- = \frac{1}{[L : \mathbb{F}_L K]} \sum_{v \mid e_{fw/2}^-} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{uv} \cdot \mathcal{B}(u, v), \tag{3.8}$$

where $\mathcal{B}(u,v) = [\sigma_{u,v}$ exists and $fw \equiv f_{u,v} \pmod{2f_{u,v}}]$. We are now ready to prove the main theorem for this subsection, which states that

$$\delta_q^-(\gamma, d) := \frac{2\varphi(d)}{f[2,d]} \sum_{w \mid d'^{\infty}} \frac{\delta_w^-}{w} \tag{3.9}$$

is the d_3-density of $R_q^-(\gamma, d)$.

Theorem 3.23. *There exists $c_4 > 0$, that only depends on d, γ and g_L, such that*

$$\left|\frac{1}{N}\sum_{n=1}^{N}\frac{R_q^-(\gamma,d,n)}{q^n/n}-\delta_q^-(\gamma,d)\right| \le c_2\varphi(d)\left(1+\frac{4}{[2,d]f}\right)\frac{\log(N)^{\omega(d')}}{N}+\frac{c_4}{N},$$

for all $N \ge e^{2\omega(d')}$, where c_2 is the constant defined in Lemma 3.16. In particular, $R_q^-(\gamma,d)$ has d_3-density equal to $\delta_q^-(\gamma,d)$.

Proof. The proof is similar to the proofs of Lemma 3.17 and Theorem 3.18, so we may skip a few details. We define

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

We aim to bound $|R_N - S_N|$ and $|S_N - \delta_q^-(\gamma,d)|$. By Theorem 3.22, we have

$$|R_N - S_N| \le \frac{1}{N}\sum_{n=1}^{N}\left|\frac{R_q^-(\gamma,d,n)}{q^n/n}-\delta_q^-(\gamma,d,n)\right| \le \frac{2^{\omega(d)+1}c_1}{N}{\sum_{n=1}^{N}}'\tau(e_n^-)q^{-n/2},$$

where $\sum'$ indicates that indices are taken congruent to $f/2$ modulo f. By Lemma 3.11, we show that $e_n^- = e_{2n}^+/(q^n-1,d^\infty) = e_{f/2}^-(2n/f,d^\infty)$. Hence

$${\sum_{n=1}^{N}}'\tau(e_n^-)q^{-n/2} \le \tau(e_{f/2}^-){\sum_{n=1}^{N}}'\frac{2nq^{-n/2}}{f} = \tau(e_{f/2}^-)\sum_{k=0}^{\lfloor(2N-f)/2f\rfloor}(1+2k)q^{-(1+2k)f/4},$$

where we used that $\tau(e_n^-) \le \tau(e_{f/2}^-)2n/f$. Because $q^{-f/4} < 1$, we obtain

$$|R_N - S_N| \le \frac{2^{\omega(d)+1}c_1\tau(e_{f/2}^-)}{N}\sum_{n=1}^{+\infty}nq^{-fn/4} = \frac{2^{\omega(d)+1}c_1\tau(e_{f/2}^-)q^{-f/4}}{N(q^{-f/4}-1)^2} =: \frac{c_4}{N}.$$

We now turn our attention to $|S_N - \delta_q^-(\gamma,d)|$. Using (3.7), we have

$$S_N = \frac{1}{N}\sum_{n=1}^{N}\delta_q^-(\gamma,d,n) = \frac{1}{N}\sum_{\substack{w\mid d'^\infty\\ w\le N}}\sum_{\substack{\alpha=1\\(\alpha,[2,d])=1}}^{[2,d]}B_{w,\alpha}(N)\delta_w^-,$$

where $B_{w,\alpha}(N) = \#B_{w,\alpha}\cap[1,N]$, where we took into account that $\delta_q^-(\gamma,d,n) = 0$ for all $n \in A$. We have

$$B_{w,\alpha}(N) = \left\lfloor\frac{2N + fw([2,d]-\alpha)}{f[2,d]w}\right\rfloor,$$

and, similarly to the proof of Lemma 3.17, we find the upper bound

$$S_N \leq \delta_q^-(\gamma, d) + \frac{2\varphi([2,d])}{[2,d]f} \sum_{\substack{w \mid d'^\infty \\ w > N}} \frac{\delta_w^-}{w} + \frac{\varphi([2,d])}{N} \sum_{\substack{w \mid d'^\infty \\ w \leq N}} \delta_w^-,$$

and the lower bound

$$S_N \geq \delta_q^-(\gamma, d) - \frac{2\varphi([2,d])}{[2,d]f} \sum_{\substack{w \mid d'^\infty \\ w > N}} \frac{\delta_w^-}{w} - \frac{\varphi([2,d])}{N} \sum_{\substack{w \mid d'^\infty \\ w \leq N}} \delta_w^-.$$

By Lemma 3.16, and since $\varphi([2,d]) = \varphi(d)$ and $\delta_w^- \leq 1$, we obtain

$$\left|S_N - \delta_q^-(\gamma, d)\right| \leq \varphi(d) c_2 \left(1 + \frac{4}{[2,d]f}\right) \frac{\log(N)^{\omega(d')}}{N},$$

for all $N \geq e^{2\omega(d')}$. The inequality $|R_N - \delta_q^-(\gamma, d)| \leq |R_N - S_N| + |S_N - \delta_q^-(\gamma, d)|$ and our bounds yield the result. □

3.3.2 The case $d = 2$

We now assume that $d = 2$. Since $(d, q) = 1$, we may use the Legendre symbol (Δ/P) instead of the ϵ_P notation for all $P \in A$.

As mentioned before, this case is somewhat different. Indeed, the study of $R_q^-(\gamma, 2, N)$ has two cases: $q^N \equiv 1 \pmod 4$ and $q^N \equiv 3 \pmod 4$. In some special cases, we obtain that $R_q^-(\gamma, 2)$ has a positive d_1-density. However, any hope of having a similar result for the full set $R_q(\gamma, 2)$ will vanish in Section 3.4, where we prove that $R_q(\gamma, 2)$ does not have a d_1-density.

Lemma 3.24. *Let $u \in \mathbb{F}_q$ be the leading coefficient of a_2. Then, we have*

$$[\mathbb{F}_{2,2} : \mathbb{F}_q] = \begin{cases} 2, & \text{if } \mathbb{F}_L = \mathbb{F}_{q^2}, \text{ or } 2 \mid h \text{ and } u \notin (\mathbb{F}_q^\times)^2; \\ 1, & \text{otherwise.} \end{cases}$$

Proof. By Lemma 3.6, we have $\mathbb{F}_{2,2} = \mathbb{F}_L(\mu^{1/(2,h)})$. Moreover, because $\gamma = a^2/a_2$, we can write $\mu = \operatorname{sgn}(a)^2/u$. Then, we can replace μ by u to obtain $\mathbb{F}_{2,2} = \mathbb{F}_L(u^{1/(2,h)})$. Now, because $u \in \mathbb{F}_q$, it follows that $\mathbb{F}_{2,2} = \mathbb{F}_{q^2}$ if $\mathbb{F}_L = \mathbb{F}_{q^2}$. Otherwise, $\mathbb{F}_{2,2} = \mathbb{F}_q(u^{1/(2,h)})$ and the result follows trivially. □

Theorem 3.25. *Let $N \geq 1$ be such that $q^N \equiv 1 \pmod 4$. Then $R_q^-(\gamma, 2, N) = 0$ if $2 \mid N$*

and $\mathbb{F}_{2,2} = \mathbb{F}_{q^2}$. *Otherwise, we have*

$$\left| R_q^-(\gamma, 2, N) - \left(\frac{1}{[L : \mathbb{F}_L K]} - \frac{[\sigma_{2,1} \text{ exists}]}{[L_{2,2} : \mathbb{F}_{2,2} K]} \right) \cdot \frac{q^N}{N} \right| \leq 4c_1 \cdot \frac{q^{N/2}}{N},$$

where $c_1 > 0$ *is the constant of Lemma 3.14 and* $\sigma_{2,1}$ *was defined below Lemma 3.21. Moreover,* $\sigma_{2,1}$ *exists in the Galois group of* $L_{2,2}/K$ *if and only if* $2 \nmid h$, *or*

(1) $2 \mid h$, $\mathbb{F}_L = \mathbb{F}_q$ *and* $\mu \notin (\mathbb{F}_q^\times)^2$; *or*

(2) $\gamma \in (L^\times)^2$ *and* $\sigma_L(\gamma^{1/2}) = \gamma^{-1/2}$.

Proof. Let $P \in R_q^-(\gamma, 2)$ have degree N. Since $v_2(q^N + 1) = 1$, we have $2 \mid \rho_U(P)$ if and only if $2 \nmid \iota_U(P)$. By Lemma 3.10, we have

$$R_q^-(\gamma, 2, N) = C_N(L/K, \{\sigma_L\}) - C_N(L_{2,2}/K, \{\sigma_{2,1}\}) \cdot [\sigma_{2,1} \text{ exists}],$$

where the C_N functions were defined in Theorem 3.1.

First, we apply Theorem 3.1 to $C_N(L/K, \{\sigma_L\})$. We have $\sigma_L|_{\mathbb{F}_L} = \tau^k$, where τ is the Frobenius automorphism of $\mathbb{F}_{q^2}/\mathbb{F}_q$, and $k = 0$ if $\mathbb{F}_L = \mathbb{F}_q$, and $k = 1$ otherwise. By Theorem 3.1, we obtain $C_N(L/K, \{\sigma_L\}) = 0$ if $2 \mid N$ and $\mathbb{F}_L = \mathbb{F}_{q^2}$, and

$$\left| C_N(L/K, \{\sigma_L\}) - \frac{1}{[L : \mathbb{F}_L K]} \cdot \frac{q^N}{N} \right| \leq 2c_1 \cdot \frac{q^{N/2}}{N}, \tag{3.10}$$

otherwise, where $c_1 > 0$ is defined as in Lemma 3.14.

Next, we study $C_N(L_{2,2}/K, \{\sigma_{2,1}\})$. If $\sigma_{2,1}$ exists, then $\sigma_{2,1}|_{\mathbb{F}_{2,2}} = \tau^k$, where τ is the Frobenius automorphism of $\mathbb{F}_{2,2}/\mathbb{F}_q$, and $k = 0$ if $\mathbb{F}_{2,2} = \mathbb{F}_q$, and $k = 1$ otherwise. We used the definition of σ and Lemma 3.24. By Theorem 3.1, we obtain

$$\left| C_N(L_{2,2}/K, \{\sigma_{2,1}\}) - \frac{1}{[L_{2,2} : \mathbb{F}_{2,2} K]} \cdot \frac{q^N}{N} \right| \leq 2c_1 \cdot \frac{q^{N/2}}{N}, \tag{3.11}$$

for all positive $N \equiv k \pmod{[\mathbb{F}_{2,2} : \mathbb{F}_q]}$, and $C_N(L_{2,2}/K, \{\sigma_{2,1}\}) = 0$ otherwise. The result follows by putting (3.10) and (3.11) together.

Lastly, we prove the conditions for the existence of $\sigma_{2,1}$. Since $\sigma_{2,1}|_L = \sigma_L$, it suffices to find conditions for σ_L to be extended into the right automorphism. Assume $2 \nmid h$. Then, the polynomial $f(X) = X^2 - \gamma$ is irreducible over L. Since $L_{2,2} \cong L[X]/(f(X))$, we can extend σ_L into $\sigma_{2,1}$ if and only if $\sigma_L f$ annihilate $\gamma^{-1/2}$. This is the case, since $\sigma_L(\gamma) = \gamma^{-1}$. The same applies to the case $2 \mid h$, $\mathbb{F}_L = \mathbb{F}_q$ and μ is not a square in $\mathbb{F}_q$. Finally, assume γ is a square in L. Then $L_{2,2} = L$, and $\sigma_{2,1}$ exists if and only if $\sigma_{2,1} = \sigma_L$ and $\sigma_L(\gamma^{1/2}) = \gamma^{-1/2}$. □

As mentioned at the beginning of the subsection, we obtain a positive d_1-density in some cases. Assume $q \equiv 1 \pmod 4$ and $L_{2,2}/K$ is geometric. By Theorem 3.25, we have

$$\left| \frac{R_q^-(\gamma, 2, N)}{q^N/N} - \left(\frac{1}{2} - \frac{[\sigma_{2,1} \text{ exists}]}{2[L_{2,2} : L]} \right) \right| \leq 4c_1 q^{-N/2}, \tag{3.12}$$

for all $N \geq 1$. Letting N tend to infinity, we find that $R_q^-(\gamma, 2)$ as a d_1-density either equal to 0, 1/2, or 1/4. For the remaining cases, the following corollary provides the value of the d_3-density of $R_q^-(\gamma, 2)$ when $q \equiv 1 \pmod 4$:

Corollary 3.26. *Assume $q \equiv 1 \pmod 4$. Then, for all $N \geq 1$, we have*

$$\left| \frac{1}{N} \sum_{n=1}^{N} \frac{R_q^-(\gamma, 2, n)}{q^n/n} - \left(\frac{1}{2} - \frac{[\sigma_{2,1} \text{ exists}]}{2[L_{2,2} : L]} \right) \right| \leq \left(\frac{4c_1}{\sqrt{q} - 1} + \frac{3}{4} \right) \frac{1}{N}.$$

Necessary and sufficient conditions for the existence of $\sigma_{2,1}$ are given in Theorem 3.25.

Proof. If $\mathbb{F}_{2,2} = \mathbb{F}_q$, then $d_1(R_q^-(\gamma, 2))$ exists by the discussion above the corollary. Then, using (3.12), the bound for the d_3-density is given by

$$\frac{4c_1}{N} \sum_{n=1}^{N} q^{-n/2} \leq \frac{4c_1}{N} \sum_{n=1}^{+\infty} q^{-n/2} = \frac{4c_1}{(\sqrt{q} - 1)N}. \tag{3.13}$$

If $\mathbb{F}_{2,2} = \mathbb{F}_{q^2}$, then $R_q^-(\gamma, 2, N) = 0$ for all even $N \geq 1$, by Theorem 3.25. We have

$$S_N := \frac{1}{N} \sum_{\substack{n=1 \\ 2 \nmid n}}^{N} \left(\frac{1}{[L : \mathbb{F}_L K]} - \frac{[\sigma_{2,1} \text{ exists}]}{[L_{2,2} : \mathbb{F}_{2,2} K]} \right) = \frac{1}{2} \left(1 - \frac{[\sigma_{2,1} \text{ exists}]}{[L_{2,2} : L]} \right) + f(N),$$

where $f(N) \leq 3/4N$ for all $N \geq 1$. If R_N denotes the average of the $R_q^-(\gamma, 2, n)/(q^n/n)$ from $n = 1$ up to N, then

$$\left| R_N - \left(\frac{1}{2} - \frac{[\sigma_{2,1} \text{ exists}]}{2[L_{2,2} : L]} \right) \right| \leq |R_N - S_N| + \left| S_N - \left(\frac{1}{2} - \frac{[\sigma_{2,1} \text{ exists}]}{2[L_{2,2} : L]} \right) \right|$$

for all $N \geq 1$. We use the bound of (3.13) for $|R_N - S_N|$, and the bound $3/4N$ for the second term. □

Example 3.27. *Let $a_1 = a_2 = T$ and $q = 5$. We have $h = 1$, so that $L_{2,2} = L(\gamma^{1/2})$ has degree 4. By Corollary 3.26, we find that $\delta_5^-(\gamma, 2) = 1/4$. We computed*

$$\frac{1}{6} \sum_{n=1}^{6} \frac{R_5^-(\gamma, 2)}{5^n/n} \approx 0.251989,$$

which matches the theoretical value of $1/4$.

Lemma 3.28. *Let* $N \geq 1$ *be an odd integer and assume* $q \equiv 3 \pmod 4$. *We have*

$$\left| R_q^-(\gamma, 2, N) - \delta_q^-(\gamma, 2, N) \cdot \frac{q^N}{N} \right| \leq 4c_1 \cdot \frac{\tau(e_1^-) q^{N/2}}{N},$$

where $c_1 > 0$ *is the constant defined in Lemma 3.14 and*

$$\delta_q^-(\gamma, 2, N) = \frac{1}{[L : \mathbb{F}_L K]} \sum_{i=0}^{v_2(e_1^-)} \sum_{j=0}^{1} \frac{(-1)^j (2^{i+j}, h)}{2^{i+j}} \cdot \mathcal{B}_N(2^j, 2^i),$$

where $\mathcal{B}_N(2^j, 2^i)$, $i \geq 1$, *was defined in Theorem 3.22, and* $\mathcal{B}_N(2, 1) = [\sigma_{2,1}$ *exists*$]$ *and* $\mathcal{B}_N(1, 1) = 1$ *otherwise.*

Proof. As in the proof of Theorem 3.22, we show that

$$R_q^-(\gamma, 2, N) = \sum_{i=0}^{v_2(e_N^-)} \Big(C_N(i, 0) - C_N(i, 1) \Big), \tag{3.14}$$

where $C_N(i, j)$ is defined for all $1 \leq i \leq v_2(e_N^-)$ and $j \in \{0, 1\}$ by

$$C_N(i, j) = C_N(L_{2^{i+1}, 2^{i+j}}/K, \{\sigma_{2^j, 2^i}\}) \cdot [\sigma_{2^j, 2^i} \text{ exists}].$$

where $\sigma_{2^j, 2^i}$ was defined below Lemma 3.21. Because $2 \nmid N$ and $q \equiv 3 \pmod 4$, applying Lemma 3.11 to $v_2(q^{2N} - 1)$ and $v_2(q^N - 1)$ implies that $v_2(q^N + 1) = v_2(q + 1)$ for all odd integers N. Hence, we replace e_N^- by e_1^- in (3.14). We study the case $i \geq 1$. If $\sigma_{2^j, 2^i}$ exists, then it has order two by definition. It follows that its restriction to $\mathbb{F}_{2^{i+1}, 2^{i+j}}$ has order two because $\zeta_{2^{i+1}}$ is sent to $\zeta_{2^{i+1}}^{-1} \neq \zeta_{2^{i+1}}$. Hence $k = f_{2^j, 2^i}/2$ satisfies $\sigma_{2^j, 2^i}|_{\mathbb{F}_{2^{i+1}, 2^{i+j}}} = \tau^k$, where τ is the Frobenius of $\mathbb{F}_{2^{i+1}, 2^{i+j}}/\mathbb{F}_q$. By Lemma 3.21, $\sigma_{2^j, 2^i}$ belongs to the center of the Galois group. By the Chebotarev density theorem, i.e., Theorem 3.1, we find

$$\left| C_N(i, j) - \frac{(2^{i+j}, h)}{2^{i+j}[L : \mathbb{F}_L K]} \frac{q^N}{N} \right| \leq 2c_1 \cdot \frac{q^{N/2}}{N},$$

for all $N \equiv f_{2^j, 2^i}/2 \pmod{f_{2^j, 2^i}}$, where $c_1 > 0$ is the constant of Lemma 3.14. Otherwise, we have $C_N(i, j) = 0$. If $i = j = 0$, then $\sigma_{1,1} = \sigma_L$, the non-trivial automorphism of L/K, which always exists. Its restriction to $\mathbb{F}_L$ is either the identity element if $\mathbb{F}_L = \mathbb{F}_q$, and has order 2 otherwise. The integer

$$k = \begin{cases} 0, & \text{if } L/K \text{ is geometric;} \\ 1, & \text{otherwise,} \end{cases} \tag{3.15}$$

satisfies $\sigma_L|_{\mathbb{F}_L} = \tau^k$, where τ is the Frobenius of $\mathbb{F}_L/\mathbb{F}_q$. By Theorem 3.1, we have

$$\left| C_N(0,0) - \frac{1}{[L:\mathbb{F}_L K]} \frac{q^N}{N} \right| \leq 2c_1 \cdot \frac{q^{N/2}}{N},$$

for all odd $N \equiv k \pmod{[\mathbb{F}_L : \mathbb{F}_q]}$. By definition of k, we see that the bound holds for all odd $N \geq 1$. If $j = 1$, then $\sigma_{2,1}$ is entirely determined by the relations

$$\sigma_{2,1}(\sqrt{\Delta}) = -\sqrt{\Delta} \quad \text{and} \quad \sigma_{2,1}(\gamma^{1/2}) = \gamma^{-1/2}.$$

By Lemma 3.24, we know that $\mathbb{F}_{2,2}$ has degree at most 2 over $\mathbb{F}_q$. Therefore, we define k in a way similar to (3.15), so that Theorem 3.1 yields

$$\left| C_N(0,1) - \frac{(2,h)}{2[L:\mathbb{F}_L K]} \frac{q^N}{N} \right| \leq 2c_1 \cdot \frac{q^{N/2}}{N},$$

for all odd $N \geq 1$, using the same reasoning as before. The result follows from applying the bounds to (3.14). For the final bound, we follow the same path as in Theorem 3.22. □

Theorem 3.29. *Assume $q \equiv 3 \pmod 4$. For each $N \geq 1$, we have*

$$\left| \frac{1}{N} \sum_{n=1}^{N} \frac{R_q^-(\gamma, 2, n)}{q^n/n} - \delta_q^-(\gamma, 2) \right| \leq \left(\frac{8c_1 \tau(e_1^-)}{\sqrt{q} - 1} + \frac{7}{4} \right) \frac{1}{N},$$

where $c_1 > 0$ is the constant defined in Lemma 3.14 and

$$\delta_q^-(\gamma, 2) = \delta_0 + \frac{1}{2[L:\mathbb{F}_L K]} \sum_{i=0}^{v_2(e_1^-)} \sum_{j=0}^{1} \frac{(-1)^j (2^{i+j}, h)}{2^{i+j}} \cdot \mathcal{B}(2^j, 2^i),$$

where $\mathcal{B}(2^j, 2^i) = [\sigma_{2^j,2^i}$ exists and $2 \| f_{2^j,2^i}]$ if $i \geq 1$, $\mathcal{B}_N(2,1) = [\sigma_{2,1}$ exists$]$, $\mathcal{B}_N(1,1) = 1$, and $\delta_0 = 0$ if $\mathbb{F}_{2,2} = \mathbb{F}_{q^2}$, and otherwise,

$$\delta_0 = \frac{1}{4} - \frac{[\sigma_{2,1} \text{ exists}]}{4[L_{2,2} : L]}.$$

Necessary and sufficient conditions for the existence of $\sigma_{2,1}$ are given in Theorem 3.25.

Proof. As usual, we study the sum

$$R_N = \frac{1}{N} \sum_{n=1}^{N} \frac{R_q^-(\gamma, 2, n)}{q^n/n}.$$

We write $S_1(N)$ and $S_2(N)$ for the parts with odd and even indices respectively. From

Theorem 3.25, we see that $S_2(N) = 0$ if $\mathbb{F}_{2,2} = \mathbb{F}_{q^2}$. Otherwise, we have

$$\left| S_2(N) - \left(\frac{1}{4} - \frac{[\sigma_{2,1} \text{ exists}]}{4[L_{2,2} : L]} \right) \right| \leq \left(\frac{4c_1}{\sqrt{q}-1} + \frac{1}{4} \right) \frac{1}{N},$$

by following the proof of Corollary 3.26, and since

$$\frac{1}{N} \sum_{\substack{n=1 \\ 2|n}}^{N} \left(\frac{1}{2} - \frac{[\sigma_{2,1} \text{ exists}]}{2[L_{2,2} : L]} \right) = \left(\frac{1}{4} - \frac{[\sigma_{2,1} \text{ exists}]}{4[L_{2,2} : L]} \right) + f(N),$$

for some $f(N) \leq 1/4N$.

For the sum $S_1(N)$, we first prove that $B_n(2^j, 2^i)$, which was defined in Lemma 3.28, does not depend on n when $i \geq 1$. By Theorem 3.7 and Lemma 3.12, we have

$$f_{2^j,2^i} = \frac{2^{i+2}}{(q^2-1, 2^{i+1})} \cdot \frac{(2^{i+j}, h)}{(\text{ind}_{\mathbb{F}_L(\zeta_{2^{i+1}})}(\mu), 2^{i+j}, h)}.$$

We see that $f_{2^j,2^i} = 2^m$ for some $m \geq 1$. However, the condition $n \equiv f_{2^j,2^i}/2 \pmod{f_{2^j,2^i}}$, which appears in the expression of $B_n(2^j, 2^i)$ has to take into account the parity of n to hold. Since n is odd, this happens if and only if $2 \| f_{2^j,2^i}$. Hence

$$\mathcal{B}_n(2^j, 2^i) = [\sigma_{2^j,2^i} \text{exists and } 2 \| f_{2^j,2^i}] =: \mathcal{B}(2^j, 2^i),$$

for all odd $n \geq 1$. The expression of $\delta_q^-(\gamma, 2, n)$ in Lemma 3.28 does not have any dependence on n. We write $\delta^- := \delta_q^-(\gamma, 2, n)$. We find that

$$\left| S_1(N) - \frac{\delta^-}{2} \right| \leq \left(\frac{4c_1\tau(e_1^-)}{\sqrt{q}-1} + \frac{3\delta^-}{2} \right) \frac{1}{N},$$

for all $N \geq 1$, where we followed the method used for $S_2(N)$. Finally, since δ^- must be less than or equal to 1, we obtain

$$|R_N - \delta_q^-(\gamma, 2)| \leq \left| S_1(N) - \frac{\delta^-}{2} \right| + |S_2(N) - \delta_0| \leq \left(\frac{8c_1\tau(e_1^-)}{\sqrt{q}-1} + \frac{7}{4} \right) \frac{1}{N},$$

the result we sought. □

3.4 On the d_1 and d_2-densities

The purpose of this section is to prove that the d_1 and d_2-densities of $R_q(\gamma, d)$ do not exist except in some trivial cases. Because the d_1 and d_2-densities are equivalent, see [4, Theorem A], we will work with d_1 only. Let us consider the case $d = 1$. Since 1 always divides $\rho_U(P)$

for primes $P \nmid \Delta a_2$, we have

$$R_q(\gamma, 1, N) = I_N - a_N,$$

for all $N \geq 1$, where a_N counts primes P of degree N such that $P \mid \Delta a_2$. Note that a_N is zero for all, but a finite number of N's. Hence, as expected, the quotient $R_q(\gamma, 1, N)/I_N$ converges to 1 as $N \to +\infty$ and $d_1(R_q(\gamma, 1)) = 1$.

Another trivial case arises when γ is a constant in L, say $\zeta \in \mathbb{F}_L$. We have $a = \zeta b$, and by Lemma 2.2, this is equivalent to U being a degenerate Lucas sequence. In that case, the rank of any prime P in U is equal to $\mathrm{ord}_{\mathbb{F}_L^\times}(\zeta)$. We obtain

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

for all $N \geq 1$. We conclude that $d_1(R_q(\zeta, d))$ is either 1 or 0, depending on whether $d \mid \mathrm{ord}_{\mathbb{F}_L^\times}(\zeta)$ or not, respectively. Note that it includes Lucas sequences for which a_1^2/a_2 is a constant in K.

Lastly, when $p \mid d$, there is no prime $P \nmid \Delta a_2$ such that $d \mid \rho_U(P)$. This is because the rank of P divides $NP - \epsilon_P$, which is congruent to ± 1 modulo p. Hence, we have a d_1-density equal to 0 in that case.

We now tackle the general case. We need the following lemma on the multiplicativity of the function $[f_{u,v} \mid N]$ of the variable u, $u \mid d$, where $N \geq 1$ is an integer and $v \mid d^\infty$:

Lemma 3.30. *Let $N \geq 1$ be such that $f_{1,v} \mid N$. Then, the function $u \mapsto [f_{u,v} \mid N]$ is multiplicative for all $v \mid d^\infty$.*

Proof. It suffices to prove that $f_{u_1u_2,v} = [f_{u_1,v}, f_{u_2,v}]$ for coprime $u_1, u_2 \mid d$. Indeed, it will follow that $f_{u_1u_2,v} \mid N$ if and only if both $f_{u_1,v}$ and $f_{u_2,v}$ divide N. Recall that $\mu \in \mathbb{F}_L^\times$ is the sign of γ in L_∞ and $[\mathbb{F}_L : \mathbb{F}_q]$ is denoted by the letter i. We have

$$\mathrm{ind}_{\mathbb{F}_L(\zeta_{dv})^\times}(\mu) = \frac{q^r - 1}{m},$$

where $r = i \cdot \mathrm{ord}_{dv}(q^i)$ and $m = \mathrm{ord}_{\mathbb{F}_L(\zeta_{dv})^\times}(\mu) = \mathrm{ord}_{\mathbb{F}_L^\times}(\mu)$. 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 by Theorem 3.7, we obtain

$$f_{u,v} = \frac{r(uv, h)}{\left(\frac{q^r-1}{m}, uv, h\right)} = \frac{r(v, h)}{(v, H_r)} \cdot \frac{\left(u, \frac{h}{(v,h)}\right)}{\left(u, \frac{H_r}{(v,H_r)}\right)}, \tag{3.16}$$

for all $u \mid d$, where $H_r := (h, (q^r - 1)/m)$. It follows that

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

Since $u \mapsto (u, k)$ is a multiplicative function for a fixed integer k and $(u_1, u_2) = 1$, the lcm is equal to the product of the two numbers. Hence $[f_{u_1,v}, f_{u_2,v}] = f_{u_1 u_2, v}$. □

Theorem 3.31. *Assume $d \geq 2$, $p \nmid d$, and $\gamma \notin \mathbb{F}_L$. Then, the set $R_q(\gamma, d)$ does not have a d_1-density, nor a d_2-density.*

Proof. It suffices to show that the quotient

$$\frac{R_q(\gamma, d, N)}{q^N/N} = \frac{R_q^+(\gamma, d, N)}{q^N/N} + \frac{R_q^-(\gamma, d, N)}{q^N/N} \tag{3.17}$$

converges to different limits for disjoint subsequences. First, by Theorem 3.15, we have

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

for all positive $N \equiv 0 \pmod{f}$. By Lemma 3.11, we see that $\tau(e_N^+) = \mathcal{O}_d(N)$. Therefore, the quotient of $R_q^+(\gamma, d, N)$ by q^N/N in (3.17) has limit l if and only if $\delta_q^+(\gamma, d, N)$ has limit l, as $N \to +\infty$. By (3.4), for numbers of the form $N = f_L w(1 + nd)$, where $n \geq 0$ and $w \mid d^\infty$, we have

$$\delta_q^+(\gamma, d, N) = \frac{1}{[L : \mathbb{F}_L K]} \sum_{v \mid e^+_{f_L w}} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{uv} \cdot [f_{u,v} \mid f_L w] = \delta_w^+,$$

which only depends on w. Secondly, note that if $d \geq 3$, then $R_q^-(\gamma, d, N) = 0$ for all integers $N = f_L w(1 + nd)$. This is either because $N \not\equiv f/2 \pmod{f}$ if $2 \mid f$, or because of Lemma 3.20 otherwise. If $d = 2$, we may choose N to be even, so that

$$\lim_{N \to +\infty} \frac{R_q^-(\gamma, 2, N)}{q^N/N} = \frac{1}{[L_{2,2} : \mathbb{F}_{2,2} K]},$$

if $a_2 \notin (K^\times)^2$, or $R_q^-(\gamma, 2, N) = 0$ otherwise, by Theorem 3.25. What is important to notice is that the quotient of $R_q^-(\gamma, 2, N)$ by q^N/N has a limit $L \geq 0$ that does not depend on w in those cases.

Now, it suffices to show that $\delta_{w_1}^+ \neq \delta_{w_2}^+$ for a good choice of w_1 and w_2 to prove the theorem. First, note that $f_v := f_{1,v}$ divides $f_{u,v}$ for all $u \mid d$. This is because $\mathbb{F}_{dv,v}$ is a

subfield of $\mathbb{F}_{dv,uv}$. Hence

$$\delta_w^+ = \frac{1}{[L:\mathbb{F}_L K]} \sum_{\substack{v \mid e^+_{f_L w} \\ f_v \mid f_L w}} \sum_{u \mid d} \frac{\mu(u)(uv,h)}{uv} \cdot [f_{u,v} \mid f_L w].$$

By Lemma 3.30, the function $u \mapsto \mu(u)(uv,h)[f_{u,v} \mid f_L w]/u(v,h)$ is multiplicative and

$$\delta_w^+ = \frac{1}{[L:\mathbb{F}_L K]} \sum_{\substack{v \mid e^+_{f_L w} \\ f_v \mid f_L w}} \frac{(v,h)}{v} \prod_{l \mid d} \left(1 - \frac{(lv,h)[f_{l,v} \mid f_L w]}{l(v,h)}\right).$$

Let $w_1, w_2 \mid d^\infty$ be such that $w_1 \mid w_2$ and $w_1 < w_2$. We have $e^+_{f_L w_1} \mid e^+_{f_L w_2}$ since $(q^n-1)_{n \geq 0}$ is a divisibility sequence. Therefore, we have

$$\delta_{w_2}^+ = \delta_{w_1}^+ + \frac{1}{[L:\mathbb{F}_L K]} {\sum_v}' \frac{(v,h)}{v} \prod_{l \mid d} \left(1 - \frac{(lv,h)[f_{l,v} \mid f_L w_2]}{l(v,h)}\right), \tag{3.18}$$

where $\sum'$ is taken over all $v \mid e^+_{f_L w_2}$ such that $v \nmid e^+_{f_L w_1}$ and $f_v \mid f_L w_2$. We show that the sum on the right-hand side of the equality is positive for a good choice of w_1 and w_2.

Assume that $d \geq 3$ and put $w_1 = \bar{f}_L(h, d^\infty)/f_L$, where $\bar{f}_L := [[\mathbb{F}_L : \mathbb{F}_q], \mathrm{ord}_{d(h,d^\infty)}(q)]$. Note that $w_1 \mid d^\infty$ because $\bar{f}_L = f_L m$ for some $m \mid d^\infty$, by Lemma 3.11. Next, we let l_0 be a prime that divides d such that $l_0 \geq 3$ if d has an odd prime. Let $k > v_{l_0}(e^+_{f_L w_1})$ be an integer and $w_2 = l_0^k w_1$. Thus, we have $e^+_{f_L w_2} = e^+_{f_L w_1} l_0^k \nu$, where ν is a power of 2, by Lemma 3.11. Now, if we put $v := (h, d^\infty) l_0^k$, we see that $v \mid e^+_{f_L w_2}$ and $v \nmid e^+_{f_L w_1}$. It remains to show that $f_v \mid f_L w_2$. With $i = [\mathbb{F}_L : \mathbb{F}_q]$, we have

$$f_v = \frac{i \mathrm{ord}_{dv}(q^i)(v,h)}{(\mathrm{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\mu), v, h)} = \frac{i \mathrm{ord}_{dv}(q^i)(h,d^\infty)}{(\mathrm{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\mu), h, d^\infty)},$$

which divides $i\mathrm{ord}_{dv}(q^i)(h,d^\infty) = (h,d^\infty)[i, \mathrm{ord}_{dv}(q)]$. By Lemma 3.12 with $d = d(h,d^\infty)$ and $v = l_0^k$, we have

$$\mathrm{ord}_{dv}(q) = \frac{\bar{f} d(h,d^\infty) l_0^k}{(q^{\bar{f}} - 1, d(h,d^\infty) l_0^k)} = \bar{f} l_0^k \cdot \left(\frac{q^{\bar{f}} - 1}{d(h,d^\infty)}, l_0^k\right)^{-1},$$

where $\bar{f} = \mathrm{ord}_{d(h,d^\infty)}(q)$. The factor 2 that is present in some cases of Lemma 3.12 does not appear here because l_0 is odd when $d \nmid 2^\infty$, and $[\mathcal{P}(\bar{f})] = 0$ when $d = 2^\alpha$, $\alpha \geq 2$. It

follows that $\mathrm{ord}_{dv}(q) \mid \bar{f} l_0^k$, so that

$$f_v \mid (h, d^\infty)[i, \bar{f} l_0^k] = (h, d^\infty) \cdot \begin{cases} \bar{f}_L l_0^k, & \text{if } d \nmid 2^\infty; \\ \bar{f} 2^k, & \text{otherwise,} \end{cases}$$

because $k \geq 1$. In both cases, we obtain $f_v \mid (h, d^\infty) \bar{f}_L l_0^k = f_L w_2$. Therefore, the general term in $v = (h, d^\infty) l_0^k$ does appears in (3.18) and is equal to

$$\frac{1}{l_0^k} \prod_{l \mid d} \left(1 - \frac{[f_{l,v} \mid f_L w_2]}{l}\right),$$

using that $(lv, h) = (v, h) = (h, d^\infty)$ for all $l \mid d$. Regardless of whether $f_{l,v} \mid f_L w_2$ or not, the general term is always positive and $\delta^+_{w_2} > \delta^+_{w_1}$. Finally, let $(x_n)_{n \geq 0}$ and $(y_n)_{n \geq 0}$ be defined by $x_n = f_L w_1 (1 + nd)$ and $y_n = f_L w_2 (1 + nd)$ for all $n \geq 0$. Then,

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

are subsequences of (3.17) that converges to $\delta^+_{w_1}$ and $\delta^+_{w_2}$ respectively, since $R^-_q(\gamma, d, N) = 0$ when $d \geq 3$ and $f \mid N$. The d_1-density of $R^+_q(\gamma, d)$ does not exist because $\delta^+_{w_1} \neq \delta^+_{w_2}$.

Assume that $d = 2$. The method is the same, but with $w_1 = 2\bar{f}_L (h, 2^\infty)/f_L$ to make sure that w_1 is even. We let $w_1 = 2^k w_1$, where $k > v_2(e^+_{f_L w_1})$. As in the $d \geq 3$ case, we see that $v = (h, 2^\infty) 2^k$ divides $e^+_{f_L w_2}$, but not $e^+_{f_L w_1}$. We use that $f_v \mid (h, 2^\infty) \cdot [i, \mathrm{ord}_{2v}(q)]$ again to show that $f_v \mid f_L w_2$. By Lemma 3.12, we have

$$\mathrm{ord}_{2v}(q) = \frac{2^{k + v_2(h) + 1} c \bar{f}}{(q^{c\bar{f}} - 1, 2^{k + v_2(h) + 1})},$$

where $c = 1 + [q \equiv 3 \pmod 4]$. We see that $\mathrm{ord}_{2v}(q) \mid 2^{k+1} \bar{f}$, so that f_v divides

$$(h, 2^\infty) \cdot [i, 2^{k+1} \bar{f}] = (h, 2^\infty) \cdot 2^{k+1} \bar{f}.$$

Thus, we obtain $f_v \mid 2^{k+1} \bar{f}_L (h, 2^\infty) = f_L w_2$. The rest of the proof follows the same path as the case $d \geq 3$, with the same subsequences. Note that this time, the quotient in (3.17) converges to $\delta^+_{w_1} + L$ and $\delta^+_{w_2} + L$ respectively, which are distinct. □

Chapter 4

Explicit results for the d_3-density

In this chapter, we compute closed-form formulas for the d_3-densities in the non-trivial cases. Indeed, we obtained formulas (3.5) and (3.9) that involve non-trivial boolean functions and an infinite series over divisors of d^∞. Our goal is to remove both dependencies when possible.

Recall that $\gamma = \mu\tilde{\gamma}_0^h$ for some $\mu \in \mathbb{F}_L$ and $\tilde{\gamma}_0 \in L$, $\tilde{\gamma}_0$ is monic in L_∞ and is not a power in L. This makes $h \geq 1$ maximal. When L/K is geometric, we have

$$N_{L/K}(\gamma) = \mu^2 N_{L/K}(\tilde{\gamma}_0)^h = 1.$$

Hence $\mu^2 = \lambda^h$ for some $\lambda \in \mathbb{F}_q$ and $\gamma = \pm\lambda^{h/(2,h)}\tilde{\gamma}_0^h$. For simplification, we would prefer γ to be an h-th power in L. Therefore, we define the boolean function

$$\mathbf{b}(h) = [\lambda^{h/(2,h)} \notin (\mathbb{F}_q^\times)^h \text{ and } -\lambda^{h/(2,h)} \notin (\mathbb{F}_q^\times)^h].$$

If $\mathbf{b}(h) = 0$, then γ or $-\gamma$ is an h-th power. The following theorem allows us to switch between γ and $-\gamma$ with no loss of generality:

Theorem 4.1. *For every $d \geq 2$, we have*

$$\delta_q(\gamma, d) = \begin{cases} \delta_q(-\gamma, 2d) + \delta_q(-\gamma, d/2) - \delta_q(-\gamma, d), & \text{if } 2\|d; \\ \delta_q(-\gamma, d), & \text{otherwise.} \end{cases}$$

Proof. By Lemmas 2.5 and 2.9, we have

$$\rho_U(P) = \begin{cases} \mathrm{ord}_\mathfrak{p}(-\gamma)/2, & \text{if } 2 \nmid \rho_U(P); \\ 2\mathrm{ord}_\mathfrak{p}(-\gamma), & \text{if } \rho_U(P) \equiv 2 \pmod 4; \\ \mathrm{ord}_\mathfrak{p}(-\gamma), & \text{if } 4 \mid \rho_U(P). \end{cases}$$

First, we have $\rho_U(P) = \mathrm{ord}_{\mathfrak{p}}(-\gamma)$ when $4 \mid d$ and $d \mid \rho_U(P)$. Moreover, when d is odd, we have $d \mid \rho_U(P)$ if and only if $d \mid \mathrm{ord}_{\mathfrak{p}}(-\gamma)$. Hence $R_q(\gamma, d) = R_q(-\gamma, d)$ and the result follows. Finally, when $2 \| d$, the set $R_q(\gamma, d)$ is the union of the sets

$$A_1 = \{P \in \mathcal{P}_+ : P \nmid a_2\Delta \text{ and } 2d \mid \rho_U(P)\},$$

and $A_2 = R_q(\gamma, d) \setminus A_1$. Any $P \in A_1$ satisfies $4 \mid \rho_U(P)$, so that $\rho_U(P) = \mathrm{ord}_{\mathfrak{p}}(-\gamma)$. Hence, we have $A_1 = R_q(-\gamma, 2d)$. For A_2, we see that any P in this set satisfies

$$d \mid \rho_U(P) \quad \text{and} \quad 2d \nmid \rho_U(P).$$

It follows that $\rho_U(P) = 2\mathrm{ord}_{\mathfrak{p}}(-\gamma)$, and $P \in A_2$ if and only if

$$d \mid 2\mathrm{ord}_{\mathfrak{p}}(-\gamma) \quad \text{and} \quad d \nmid \mathrm{ord}_{\mathfrak{p}}(-\gamma).$$

We find that $A_2 = R_q(-\gamma, d/2) \setminus R_q(-\gamma, d)$. The result follows by taking the d_3-density of these sets, which exists by our results in Sections 3.2 and 3.3. □

c

We saw in Remark 2.10, that $-\gamma$ is associated with the Lucas sequence $U(\Delta, -a_2\Delta)$. Thus, it makes sense to consider $\delta_q(-\gamma, d)$ and to use Theorem 4.1.

Next, we note that Corollary 3.26 actually provides density results for many other cases. Indeed, we have the following:

Theorem 4.2. *If $q \equiv 1 \pmod 4$, $2 \mid d$, and $a_2 \in (K^\times)^2$, then $\delta_q^-(\gamma, d) = 0$.*

Proof. Since $d \mid \rho_U(P)$ and $2 \mid d$, we see that $R_q^-(\gamma, d)$ is a subset of $R_q^-(\gamma, 2)$. Call x a square root of a_2 in K. By Corollary 3.26, we have

$$\delta_q^-(\gamma, d) \leq \delta_q^-(\gamma, 2) = \frac{1}{2} - \frac{[\sigma_{2,1} \text{ exists}]}{2[L_{2,2} : L]}.$$

Since $a_2 \in (K^\times)^2$, we have $L_{2,2} = L$. Moreover, by Theorem 3.25, the automorphism $\sigma_{2,1}$ exists if and only if $\sigma_L(\gamma^{1/2}) = \gamma^{-1/2}$. We have $N_{L/K}(\gamma^{1/2}) = N_{L/K}(a/x) = a_2/x^2 = 1$. Thus, we see that $\sigma_{2,1}$ exists and $\delta_q^-(\gamma, d) \leq 0$. □

For the rest of this chapter, we assume that $a_2 \notin (K^\times)^2$ when $q \equiv 1 \pmod 4$ and $2 \mid d$. For convenience, we do not state this assumption in the many results of this chapter that are related to the study of $R_q^-(\gamma, d)$. However, it will be restated at the beginning of the concerned sections, and when we summarise our results.

In the first section, we prove three important preliminary results, namely, Lemma 4.4, Lemma 4.5 and Lemma 4.6. The first one provides our main tool for the cases $\mathbf{b}(h) = 1$ and

$L = \mathbb{F}_{q^2}(T)$. The second and third are about expressing certain sums into Euler products. This simplifies many calculations for the obtention of the closed-form formulas.

In our second section, we find necessary and sufficient conditions for the automorphisms $\sigma_{u,v}$ defined in Section 3.3 to exist.

As a consequence of Theorem 4.1, we study the case $\mathbf{b}(h) = 0$ under the assumption that γ is an h-th power in Section 4.3. To prevent repetition, we treat the case $L = K$ in the same section. However, we are not able to obtain a closed-form formula in all cases when $L = K$, while no case is missing from the case $\mathbf{b}(h) = 0$. Recall that $R_q^-(\gamma, d)$ is not empty only if $d \nmid q^k + 1$ for some $k \geq 1$. Thus, we assume the existence of such integer k throughout this chapter. Under this assumption, Lemma 3.20 shows that only the cases $d = 2$, or $2 \mid f$ and $(d, q-1) \leq 2$ need to be treated.

In Section 4.4, we study the case $\mathbf{b}(h) = 1$. We add constants to L and K by adjoining the square root of λ. This allows for γ to be an h-th power in $\mathbb{F}_{q^2}L$. Then, we are able to link $\delta_{q^2}(\gamma, d)$ to $\delta_q(\gamma, d)$ using a result of Section 4.3. A few cases remain to obtain the full density, but they are free of most difficulties.

We look at the case $L = \mathbb{F}_{q^2}(T)$ in Section 4.5. As in the case $\mathbf{b}(h) = 1$, there is a connection between $\delta_{q^2}(\gamma, d)$ and $\delta_q(\gamma, d)$ that leaves only a few simple cases to work on. We are able to obtain an explicit formula for all γ, except for some very specific cases.

In the last section, we provide some algorithms to compute every constant that appear in the closed-form formulas. For instance, the first algorithm allows us to compute the constant h associated to γ for any given $a_1, a_2 \in A$ under our main hypotheses. Moreover, we compute $\mathbf{b}(h)$ and other constants yet to be defined.

4.1 Preliminary results

We first prove a result that will link $R_q(\gamma, d, N)$ to $R_{q^2}(\gamma, d, N)$ for all $N \geq 1$. This will be useful to write the d_3-density of $R_q(\gamma, d)$ in terms of $d_3(R_{q^2}(\gamma, d))$. Secondly, we prove a few formulas on sums and Euler products.

Lemma 4.3. *Let $P \in \mathcal{P}_+$ and $\mathfrak{p} \mid P$ be a prime in L. Then $\rho_U(P) = \rho_U(\mathfrak{p})$.*

Proof. There is nothing to do if P is inert in L. Assume that $P = \mathfrak{p}\sigma_L(\mathfrak{p})$, where σ_L is the non-trivial automorphism of L/K. If $P \mid U_n$ for some $n \geq 2$, then $\mathfrak{p} \mid U_n$ as well. Hence, we have $\rho_U(\mathfrak{p}) \mid \rho_U(P)$. For the converse, if $\mathfrak{p}$ divides some U_n, then $\sigma_L(\mathfrak{p})$ must divide U_n because $U_n \in K$. It follows that $P \mid U_n$ and $\rho_U(P) = \rho_U(\mathfrak{p})$. □

Lemma 4.4. *For all $N \geq 1$, we have*

$$R_{q^2}(\gamma, d, N) = 2R_q(\gamma, d, 2N) + \begin{cases} R_q(\gamma, d, N), & \text{if } 2 \nmid N; \\ 0, & \text{if } 2 \mid N. \end{cases}$$

Proof. Let $P \in \mathcal{P}_+$ be counted by $R_q(\gamma, d, 2N)$. Since $\deg(P) = 2N$ is even, we know from [29, Proposition 8.13] that P splits completely in $\mathbb{F}_{q^2}(T)$. Let $\mathfrak{p}$ be a prime lying above P in $\mathbb{F}_{q^2}(T)$. By Lemma 4.3 both $\mathfrak{p}$ and $\sigma_L(\mathfrak{p})$ are counted by $R^{\pm}_{q^2}(\gamma, d, N)$. Hence

$$R_{q^2}(\gamma, d, N) = 2R_q(\gamma, d, 2N) + S(N),$$

where $S(N)$ denotes the number of primes $\mathfrak{p}$ counted by $R_{q^2}(\gamma, d, N)$ such that $P = \mathfrak{p} \cap K$ is inert in $\mathbb{F}_{q^2}(T)$. By [29, Proposition 8.13], and since $\deg(P) = \deg(\mathfrak{p})$, we see that $S(N)$ is zero when $2 \mid N$. When $2 \nmid N$, we have $S(N) = R_q(\gamma, d, N)$ by Lemma 4.3 again. □

In the next lemma, we find a product formula for a sum which is a variation of a series computed by Sanna in the proof of [30, Lemma 5.4], which was already a generalisation of result of Moree, [21, Lemma 4]. We follow their method.

Lemma 4.5. *Let $d, e, h, m \geq 1$ be integers and define the sum*

$$S_{d,e,h}(m) = \sum_{\substack{v \mid (m, d^\infty) \\ e \mid v}} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{uv}.$$

Then, we have

$$S_{d,e,h}(m) = \begin{cases} \dfrac{(h, d^\infty)}{[e, (h, d^\infty)]} \displaystyle\prod_{l \mid d} \left(1 - \frac{l^{v_l([e,(h,d^\infty)])}}{l^{v_l(m)+1}}\right) & , \text{if } [e, (h, d^\infty)] \mid (m, d^\infty); \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Clearly, when $e \nmid (m, d^\infty)$, the outer sum is an empty sum, thus $S_{d,e,h}(m) = 0$. Hence, we assume $e \mid (m, d^\infty)$. The function defined by

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

is multiplicative. We use the Euler product formula on $S_{d,e,h}(m)$ to obtain

$$S_{d,e,h}(m) = \sum_{\substack{v \mid (m, d^\infty) \\ e \mid v}} \frac{(v, h)}{v} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{u(v, h)} = \sum_{\substack{v \mid (m, d^\infty) \\ e \mid v}} \frac{(v, h)}{v} \prod_{l \mid d} \left(1 - \frac{(lv, h)}{l(v, h)}\right).$$

We see that the product is non-zero if and only if $(h, d^\infty) \mid v$. Indeed, if $l \mid (h, d^\infty)$ is such that $v_l(v) < v_l(h)$, then $v_l(lv) \leq v_l(h)$ and $(lv, h) = l(v, h)$. We see that $S_{d,e,h}(m) = 0$ for all $m \geq 1$ such that $(h, d^\infty) \nmid m$. Therefore, when both e and (h, d^∞) divide (m, d^∞), that

is, when $e_0 := [e, (h, d^\infty)] \mid (m, d^\infty)$, we have

$$S_{d,e,h}(m) = \frac{\varphi(d)}{d} \sum_{\substack{v \mid (m,d^\infty) \\ e_0 \mid v}} \frac{(v,h)}{v} = \frac{\varphi(d)(h,d^\infty)}{de_0} \sum_{e_0 v \mid (m,d^\infty)} \frac{1}{v},$$

where we used that $(v,h) = (h,d^\infty)$ because $e_0 \mid v$. We apply the Euler product one last time to the sum to obtain

$$\sum_{e_0 v \mid m} \frac{1}{vv} = \prod_{e_0 l \mid (m,d^\infty)} \left(\sum_{r=0}^{v_l(m/e_0)} \frac{1}{l^r} \right) = \prod_{e_0 l \mid (m,d^\infty)} \left(\frac{1 - l^{-v_l(m/e_0)-1}}{1 - l^{-1}} \right).$$

Since $(m,d^\infty)/e_0$ divides d^∞, we may replace the index of the product by $l \mid d$. Indeed, the only instance it could be a problem is when $l \mid d$, but $l \nmid (m,d^\infty)/e_0$. However, we see that the general term in the product is equal to 1 in that case. The result follows by taking $(1 - l^{-1})^{-1}$ out of the product, which yields a factor of $d/\varphi(d)$. □

Lemma 4.6. *Let $\bar{f} = \mathrm{ord}_{d(h,d^\infty)}(q)$. We have*

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

Proof. Using $(dh, u^\infty) \leq (q^{\bar{f}} - 1, u^\infty)$, we obtain the inequality

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

which shows that the series is absolutely convergent. We may now interchange the sum symbols in the expression. We obtain

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

Let $S(u)$ denote the inner series. The function $\nu \mapsto \nu(\nu, u^\infty)$ is multiplicative, thus

$$S(u) = \prod_{l \mid d} \left(\sum_{r \geq 0} \frac{1}{l^{r(1+[l|u])}} \right) = \prod_{l \mid d} \left(1 - \frac{1}{l^{1+[l|u]}} \right)^{-1}.$$

Separating the primes $l \mid u$ from those that do not divide u, we obtain

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

where ψ is the Dedekind psi function. Finally, going back to $D(d)$, the result follows by using the Euler product formula on the remaining sum. □

4.2 Existence of the good automorphisms

In this section, we assume $[L : K] = 2$. We give necessary and sufficient conditions for the existence of $\sigma \in Gal(L_{n,d}/K)$ such that $\sigma(a) = b$, $\sigma(\zeta_n) = \zeta_n^{-1}$, and $\sigma(\gamma^{1/d}) = \gamma^{-1/d}$. The search for such conditions is justified by Theorems 3.22 and Lemma 3.28, which correlate these automorphisms to the primes counted by $R_q^-(\gamma, d, N)$. We construct σ step by step by extending an automorphism of $K(\zeta_n)$ to $L(\zeta_n)$, and then to $L_{n,d}$.

Lemma 4.7. *Assume $n \geq 3$. Then, there exists $\sigma \in Gal(L(\zeta_n)/K)$ such that $\sigma(a) = b$ and $\sigma(\zeta_n) = \zeta_n^{-1}$ if and only if*

(1) $(n, q-1) \leq 2$;

(2) $2 \mid \mathrm{ord}_n(q)$, if L/K is geometric;

(3) $2 \| \mathrm{ord}_n(q)$, if $L = \mathbb{F}_{q^2}(T)$.

Proof. Let us first construct $\sigma_0 \in Gal(K(\zeta_n)/K)$ such that $\sigma_0(\zeta_n) = \zeta_n^{-1}$. The minimal polynomial of ζ_n over $\mathbb{F}_q$ is given by

$$\Phi_n(X) = \prod_{i=0}^{\mathrm{ord}_n(q)-1} (X - \zeta_n^{q^i}).$$

For σ_0 to send ζ_n to ζ_n^{-1}, we need that $\zeta_n^{-1} = \zeta_n^{q^i}$ for some $0 \leq i \leq \mathrm{ord}_n(q) - 1$. Following the proof of Lemma 3.20, we see that $n \mid q^i + 1$ holds if and only if $(n, q-1) \leq 2$, in which case $\mathrm{ord}_n(q) = 2i$. If L/K is geometric, then $f(X) = X^2 - a_1 X + a_2$ remains the minimal polynomial of a over $K(\zeta_n)$. Therefore, because $L(\zeta_n) \cong K(\zeta_n)/(f(X))$, we can extend σ_0 in exactly two ways to $\sigma \in Gal(L(\zeta_n)/K)$ such that $\sigma|_{K(\zeta_n)} = \sigma_0$ and such that σ sends a to one of the root of $\sigma_0 f = f$. It suffices to choose the root b. If $L = \mathbb{F}_{q^2}(T)$, we proved that $2 \mid \mathrm{ord}_n(q)$, so $L(\zeta_n) = K(\zeta_n)$. Therefore, we see that σ_0 is the right automorphism if and only if $\sigma_0|_L \neq \mathrm{id}$. We write $M = L(\zeta_n)$ and let $H \lhd Gal(M/K)$ be the subgroup generated by σ_0. It is easy to see that the field

$$M^H = \{x \in M : \forall \sigma \in H, \sigma(x) = x\} = \{x \in M : \sigma_0(x) = x\}$$

is equal to $K(\zeta_n+\zeta_n^{-1})$, since $\sigma_0(\zeta_n+\zeta_n^{-1})=\zeta_n+\zeta_n^{-1}$ and because $X^2-(\zeta_n+\zeta_n^{-1})X+1$ is the minimal polynomial of ζ_n over M^H. Hence $\sigma_0|_L \neq \mathrm{id}$ if and only if $L \not\subset M^H$. We are dealing with constant field extensions of K, thus this is equivalent to $\mathbb{F}_{q^2} \not\subset \mathbb{F}_q(\zeta_n+\zeta_n^{-1})$, which happens if and only if $[M^H : K] = \mathrm{ord}_n(q)/2$ is odd. □

Note that the condition $(n, q-1) \leq 2$ makes sense as $R_q^-(\gamma, d)$ is empty for all $d \geq 3$ such that $(d, q-1) \leq 2$ by Lemma 3.20.

Theorem 4.8. *Let $n \geq 3$. There exists $\sigma \in Gal(L_{n,d}/K)$ such that $\sigma(a) = b$, $\sigma(\zeta_n) = \zeta_n^{-1}$, and $\sigma(\gamma^{1/d}) = \gamma^{-1/d}$ if and only if*

(1) $(n, q-1) \leq 2$;

(2) $2 \mid \mathrm{ord}_n(q)$ if L/K is geometric;

(3) $2 \| \mathrm{ord}_n(q)$, if $L = \mathbb{F}_{q^2}(T)$;

(4) and $\sigma_0(\gamma^{1/(d,h)}) = \gamma^{-1/(d,h)}$, where σ_0 is defined in Lemma 4.7.

Proof. By Lemma 4.7, there exists $\sigma_0 \in Gal(L(\zeta_n)/K)$ satisfying the first two properties if and only if *(1)* and one of *(2)* and *(3)* hold. It suffices to prove that σ_0 can be extended to the right automorphism if and only if *(4)* holds. Put $d_0 = d/(d,h)$. We claim that

$$f(X) = X^{d_0} - \omega$$

is the minimal polynomial of $\gamma^{1/d}$ over $L(\zeta_n)$, where ω is a (d,h)-th root of γ in $L(\zeta_n)$. First, since $\gamma = \mu\tilde{\gamma}_0^h$, we have $\omega = \mu^{1/(d,h)}\tilde{\gamma}_0^{h_0}$, where $h_0 = h/(d,h)$. Moreover, by [29, Proposition 8.13], we know that ∞ is inert and has degree 1 in $M := L(\zeta_n)$. Therefore, the completion of M with respect to v_∞ is given by $M_\infty = \mathbb{F}_L(\zeta_n)((\pi))$, where π is a uniformizer of ∞. It follows that $\tilde{\omega} = \tilde{\gamma}_0^{h_0} \in L$ because $\tilde{\gamma}_0 \in L_\infty \subset M_\infty$. We are now ready to prove the irreducibility of $f(X)$. Let $l \mid d_0$ be a prime, and assume that $\omega \in (M^\times)^l$. Then, we have $\tilde{\omega} \in (M^\times)^l$ as well. By Theorem 3.3, since $L(\tilde{\omega}^{1/l})$ is a constant field extension of L, we may write $\tilde{\omega} = ux^l$ for some $u \in \mathbb{F}_L$ and $x \in L$. Hence $\tilde{\gamma}_0^{h_0} = \tilde{x}^l$, and by the maximality of h, we obtain $l \mid h_0$. This contradicts $(d_0, h_0) = 1$. Now, if $\omega = -4y^4$ for some $y \in L(\zeta_n)$, it follows that $\tilde{\omega}$ is a square in L using the same method. This contradicts the above and, by Theorem 3.4, the polynomial $f(X)$ is irreducible over $\mathbb{F}_L(\zeta_n)$. Finally, since we have $L_{n,d} \cong L(\zeta_n)[X]/(f(X))$, we can extend σ_0 to the right automorphism σ if and only if $\gamma^{-1/d}$ is a root of $(\sigma_0 f)(X) = X^{d_0} - \sigma_0(\omega)$, that is, if and only if $\sigma_0(\omega) = \omega^{-1}$. □

We will later see that conditions *(2)* and *(3)* are easily satisfied in our calculations. However, the last condition is too weak at the moment to be used efficiently, as there is a dependence on n and d. In most cases, we will be able to reduce it to a simple

condition involving σ_L and the divisibility of d by a power of 2. Let $h_1 = (h, 2^\infty)$. The next proposition deals with the case L/K geometric and $q \not\equiv 1 \pmod 4$. The following lemma is useful to prove the proposition and other later results when $q \equiv 1 \pmod 4$:

Lemma 4.9. *Assume that L/K is geometric. Then, we have $\sigma_0(\gamma^{1/(d,h)}) = \gamma^{-1/(d,h)}$ if and only if $\sigma_0(\gamma^{1/\alpha}) = \gamma^{-1/\alpha}$, where $\alpha = (d, h, 2^\infty)$ and σ_0 is defined in Lemma 4.7.*

Proof. Let $D = (d, h)$, so that $\alpha = (D, 2^\infty)$. One way is trivial by taking the (D/α)-th power of both sides of $\sigma_0(\gamma^{1/D}) = \gamma^{-1/D}$. Assume that $\sigma_0(\gamma^{1/\alpha}) = \gamma^{-1/\alpha}$ and define

$$L' = \begin{cases} L, & \text{if } \mathbf{b}(h) = 0; \\ \mathbb{F}_{q^2}L, & \text{if } \mathbf{b}(h) = 1. \end{cases}$$

Then, we have $\sigma_0(\gamma^{1/D}) = \sigma_{L'}(\gamma^{1/D}) = \zeta_{D/\alpha}^k \gamma^{-1/D}$ for some $k \in \mathbb{Z}$ and $\zeta_{D/\alpha} \in L'$, where $\sigma_{L'} = \sigma_0|_{L'}$. Note that we know that $\gamma^{1/D} \in L'$ because it has the form $\gamma = \lambda^{h/(2,h)}\tilde{\gamma}_0^h$. Taking the α-th power in the equality, we see that

$$\sigma_L(\gamma^{\alpha/D}) = \zeta_{D/\alpha}^{\alpha k}\gamma^{-\alpha/D},$$

where $\gamma^{\alpha/D}$ now belongs to L. But $(D/\alpha, q-1) = 1$ by hypothesis, so $\zeta_{D/\alpha}^{\alpha k} = 1$. Now, since α and D/α are coprime, we have $\zeta_{D/\alpha}^k = 1$ as well, and the claim follows. □

Proposition 4.10. *Assume L/K geometric, $\mathbf{b}(h) = 0$, and $q \not\equiv 1 \pmod 4$. Then, condition (4) of Theorem 4.8 is equivalent to the following:*

(1) $h_1 \nmid d$; or

(2) $h_1 \mid d$ and $\sigma_L(\gamma^{1/h_1}) = \gamma^{-1/h_1}$.

Proof. Let $\alpha = (d, h, 2^\infty)$. By Lemma 4.9, we can replace condition *(4)* of Theorem 4.8 with $\sigma_0(\gamma^{1/\alpha}) = \gamma^{-1/\alpha}$. It suffices to show that the equality $\sigma_L(\gamma^{1/\alpha}) = \gamma^{-1/\alpha}$ holds if $h_1 \nmid d$. Since $\sigma_0(\gamma) = \gamma^{-1}$ and $\gamma^{1/\alpha} \in L$, we have

$$\sigma_0(\gamma^{1/2\alpha}) = \sigma_L(\gamma^{1/2\alpha}) = \zeta_{2\alpha}^i \gamma^{-1/2\alpha},$$

for some $i \in \mathbb{Z}$ and $\zeta_{2\alpha} \in L$. We have $(\alpha, q-1) \leq 2$, so that $\zeta_\alpha^i = \pm 1$. Squaring both sides, we obtain $\sigma_0(\gamma^{1/\alpha}) = \gamma^{-1/\alpha}$. □

One may ask where the assumption $q \not\equiv 1 \pmod 4$ was used. It turns out that the case $q \equiv 1 \pmod 4$ could be treated similarly, but we decided to hold on to that for now. In the following, we will show that even simpler conditions can be found under specific assumptions made in the various sections.

4.3 The case $L = K$ or $\mathbf{b}(h) = 0$

Throughout this section, we assume that $f_{u,v} = \mathrm{ord}_{dv}(q)$ for all $u \mid d$ and $v \mid d^\infty$. Note that this is always the case when L/K is geometric and $\mathbf{b}(h) = 0$. Indeed, since γ is an h-th power in L, so is its sign μ in $\mathbb{F}_q$. Therefore, we have

$$\mathrm{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\mu) = (q^{\mathrm{ord}_{dv}(q)} - 1, h) \cdot \mathrm{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\epsilon),$$

where $\epsilon^h = \mu$. Since (uv, h) divides the right-hand side, and by Theorem 3.7, we obtain

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

However, this may not always be the case when $L = K$. We provide sufficient condition for our assumption to hold at the end of the subsection. We first prove a closed-form formula for $\delta_q^+(\gamma, d)$, which holds if L/K is geometric and $\mathbf{b}(h) = 0$, or $L = K$. Then, we find a closed-form formula for $\delta_q^-(\gamma, d)$ in the geometric case, as $R_q^-(\gamma, d)$ is empty if $L = K$.

4.3.1 The formula for $\delta_q^+(\gamma, d)$

Let us now define $\eta : \mathbb{Z}_{>0}^2 \longrightarrow \mathbb{Z}_{>0}$ by $\eta(m, n) = 2^{v_2(q^{\bar{f}}+1)-1}$ if $\mathcal{P}(\bar{f})$ is true and $2 \mid (m, n)$, and by $\eta(m, n) = 1$ otherwise. Here, $\bar{f} = \mathrm{ord}_{d(h,d^\infty)}(q)$. Note that $m \mapsto \eta(m, n)$ is a multiplicative function for all $n \geq 1$.

Lemma 4.11. *Assume $f_{u,v} = \mathrm{ord}_{dv}(q)$ for all $u \mid d$ and $v \mid d^\infty$. For each $w \mid d^\infty$, we have*

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

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 on ν clearer.

Proof. Since $f_{u,v} = \mathrm{ord}_{dv}(q)$, and because $v \mid e_{fw}^+$ if and only if $\mathrm{ord}_{dv}(q) \mid fw$, we obtain from (3.4) that δ_w^+ becomes

$$\delta_w^+ = \frac{1}{[L : K]} \sum_{v \mid e_{fw}^+} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{uv} = \frac{S_{d,1,h}(e_{fw}^+)}{[L : K]},$$

where the sum $S_{d,1,h}(e^+_{fw})$ was defined in Lemma 4.5. We obtain

$$\delta^+_w = \frac{1}{[L:K]} \cdot \begin{cases} \prod_{l|d} \left(1 - \frac{l^{v_l(dh)}}{l^{v_l(q^{fw}-1)+1}}\right), & \text{if } (h, d^\infty) \mid e^+_{fw}; \\ 0, & \text{otherwise,} \end{cases}$$

from Lemma 4.5. However, we have $(h, d^\infty) \mid e^+_{fw}$ if and only if $\bar{f} \mid fw$. By Lemma 3.12, we have $\bar{f} = fk$ for some $k \mid d^\infty$, and it follows that $fw = \bar{f}\nu$ for some $\nu \mid d^\infty$. The function

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

is multiplicative and, by the Euler product formula, we have

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

We now apply Lemma 3.11 to $(q^{\bar{f}\nu} - 1, u^\infty)$ in the denominator of the general term of the sum, which is allowed since $u \mid q^{\bar{f}} - 1$. We obtain $(q^{\bar{f}\nu} - 1, u^\infty) = (q^{\bar{f}} - 1, u^\infty)(\nu, u^\infty)\eta(\nu, u)$, and the result follows. □

Theorem 4.12. *Assume that $f_{u,v} = \mathrm{ord}_{dv}(q)$ for all $u \mid d$ and $v \mid d^\infty$. Then, we have*

$$\delta^+_q(\gamma, d) = \frac{1}{\bar{f}[L:K]} \prod_{l|d} \left(1 - \frac{l^{v_l(dh)} C^{[l=2]\cdot[\mathcal{P}(\bar{f})]}}{(l+1)l^{v_l(q^{\bar{f}}-1)}}\right),$$

where $C = 3 \cdot 4^{-1} + 2^{-v_2(q^{\bar{f}}+1)-1}$.

Proof. By Lemma 4.11, we may only consider indices $w \mid d^\infty$ that satisfy $fw = \bar{f}\nu$, $\nu \mid d^\infty$, in the expression of $\delta^+_q(\gamma, d)$. We obtain

$$\delta^+_q(\gamma, d) = \frac{\varphi(d)}{d} \sum_{w|d^\infty} \frac{\delta_w}{fw} = \frac{\varphi(d)}{d} \sum_{\nu|d^\infty} \frac{\delta(\nu)}{\bar{f}\nu}.$$

If $2 \nmid d$ or $[\mathcal{P}(\bar{f})] = 0$, then $\eta(\nu, u)$ is equal to 1. We obtain

$$\delta^+_q(\gamma, d) = \frac{\varphi(d)D(d)}{d\bar{f}[L:K]},$$

and the result follows by Lemma 4.6, in which $D(d)$ was defined. If $2 \mid d$ and $[\mathcal{P}(\bar{f})] = 1$, then we may interchange the series and the sum in $\delta(\nu)$, by the argument used in the proof

of Lemma 4.6. We have

$$\delta_q^+(\gamma, d) = \frac{\varphi(d)}{d\bar{f}[L:K]} \sum_{u|d} \frac{\mu(u)(dh, u^\infty)}{u(q^{\bar{f}} - 1, u^\infty)} \sum_{\nu | d^\infty} \frac{1}{\nu(\nu, u^\infty)\eta(\nu, u)}.$$

Let $S(d, u)$ denote the inner series. We know that $\nu \mapsto \nu(\nu, u^\infty)\eta(\nu, u)$ is multiplicative. Thus, $d \mapsto S(d, u)$ is also multiplicative. Moreover, we have $\eta(\nu, u) = \eta(\mathrm{rad}(\nu), u)$, where rad is the radical of an integer function. Writing $d' = d/(d, 2^\infty)$, we obtain

$$S(d, u) = S(d', u) \cdot \left(1 + \sum_{r \geq 1} \frac{1}{2^{r(1+[2|u])}\eta(2, u)}\right),$$

Following the proof of Lemma 4.6, we show that $S(d', u) = S(d', u') = d'u'/\varphi(d')\psi(u')$. By the properties of the φ and ψ functions, we have

$$S(d, u) = \frac{3du}{4\varphi(d)\psi(u)} \left(1 - \frac{1}{3 \cdot 2^{v_2(q^{\bar{f}}+1)-1}}\right)^{[2|u]} = \frac{duC^{[2|u]}}{\varphi(d)\psi(u)}.$$

Replacing $S(d, u)$ by its new value in $\delta_q^+(\gamma, d)$, we find that

$$\delta_q^+(\gamma, d) = \frac{1}{\bar{f}[L:K]} \sum_{u|d} \frac{\mu(u)(dh, u^\infty)C^{[2|u]}}{\psi(u)(q^{\bar{f}} - 1, u^\infty)},$$

and the result follows by the Euler product formula. □

Note that Theorem 4.12 matches [2, Theorem 3.3] and [3, Theorem 11] that Ballot proved in the case $\gamma = T$ and, respectively, $d = 2$ and d an odd prime.

Example 4.13. *Let $a_1 = T$, $a_2 = 1$, $q = 3$, and $d = 20$. We have $h = 2$ and $\bar{f} = 4$. By Theorem 4.12, the density of $R_3^+(\gamma, 20)$ is equal to*

$$\delta_3^+(\gamma, 20) = \frac{1}{8} \cdot \left(1 - \frac{1}{6}\right)^2 = \frac{25}{288} = 0.086805\bar{5}.$$

We made the following computation:

$$\frac{1}{8} \sum_{n=1}^{8} \frac{R_3^+(\gamma, 20)}{3^n/n} \approx 0.085493,$$

which matches the value of $\delta_3^+(\gamma, 20)$. Moreover, since $20 \nmid 3^k + 1$ for every $k \geq 1$, it follows from Section 3.3 that $R_3^-(\gamma, 20)$ is empty. Hence $\delta_3(\gamma, 20) = 25/288$.

We successfully proved a closed-form formula for $\delta_q^+(\gamma, d)$. However, the assumption that the degree of $\mathbb{F}_{dv,uv}$ over $\mathbb{F}_q$ is equal to $\mathrm{ord}_{dv}(q)$ for all $v \mid d^\infty$ and $u \mid d$ was used.

We have seen that it always holds when L/K has degree two and $\mathbf{b}(h) = 0$. The following proposition provides sufficient conditions for this equality to hold.

Proposition 4.14. *Assume $L = K$, and either $(h, d) = 1$ or $(\mathrm{ord}_{\mathbb{F}_q^\times}(\mu), d) = 1$. Then, we have $f_{u,v} = \mathrm{ord}_{dv}(q)$ for all $u \mid d$ and $v \mid d^\infty$.*

Proof. By Theorem 3.7, we have

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

If $(d, h) = 1$, then $(uv, h) = 1$ and the result follows. If $(\mathrm{ord}_{\mathbb{F}_q^\times}(\mu), d) = 1$, then the order of μ in $\mathbb{F}_q(\zeta_{dv})^\times$ is equal to $\mathrm{ord}_{\mathbb{F}_q^\times}(\mu)$. Hence

$$\mathrm{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\mu) = \frac{q^{\mathrm{ord}_{dv}(q)} - 1}{\mathrm{ord}_{\mathbb{F}_q^\times}(\mu)}. \tag{4.1}$$

We see in (4.1) that uv divides $\mathrm{ind}_{\mathbb{F}_q(\zeta_{dv})^\times}(\mu)$. Indeed, $uv \mid dv$ and $(\mathrm{ord}_{\mathbb{F}_q^\times}(\mu), uv) = 1$ imply that $\mathrm{ord}_{\mathbb{F}_q^\times}(\mu) \cdot uv \mid q^{\mathrm{ord}_{dv}(q)} - 1$. □

However, Proposition 4.14 is not enough to cover all cases. For instance, it does not give any information about the density when $L = K$ and $(\mathrm{ord}_{\mathbb{F}_q^\times}(\mu), d, h) > 1$.

Example 4.15. *Let $a_1 = 2T^2 + 1$, $a_2 = 2T^2$, and $q = 5$. We have $\gamma = 2T^2$, and it follows that $\mu = 2$ and $h = 2$. Since $\mathrm{ord}_{\mathbb{F}_5^\times}(2) = 4$, any even d satisfies $(\mathrm{ord}_{\mathbb{F}_q^\times}(\mu), d, h) > 1$. Applying the formula of Theorem 4.12 with $d = 2$ would give a d_3-density of $2/3$. However, our computations show that*

$$\frac{1}{6}\sum_{n=1}^{6} \frac{R_5(2T^2, 2, n)}{5^n/n} \approx 0.854677,$$

which deviates from the expected value of $2/3$. For $d = 21$, the formula of Theorem 4.12 applies, giving $\delta_3^+(\gamma, 21) = 77/576 = 0.133680\bar{5}$. We have

$$\frac{1}{6}\sum_{n=1}^{6} \frac{R_5(2T^2, 21, n)}{5^n/n} \approx 0.128165,$$

which is relatively close to the value of $\delta_3^+(\gamma, 21)$.

More numerical comparisons can be found in Appendix A.1. We experimented on various other sequences in the case $\mathbf{b}(h) = 0$. See Tables A.1, A.2, A.3, and A.4.

4.3.2 The density $\delta_q^-(\gamma, d)$ when $2 \mid f$ and $(d, q-1) \leq 2$

From now on, we assume that $L \neq K$ and $\mathbf{b}(h) = 0$. Recall our assumption that a_2 is not a square when $q \equiv 1 \pmod 4$ and $2 \mid d$. The closed-form formula for $\delta_q^-(\gamma, d)$ is obtained using the formula for δ_w^- found in Section 3.3, i.e.,

$$\delta_w^- = \frac{1}{[L:K]} \sum_{v \mid e^-_{fw/2}} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{uv} \cdot \mathcal{B}(u, v),$$

where $\mathcal{B}(u, v) = [\sigma_{u,v} \text{ exists}] \cdot [fw \equiv f_{u,v} \pmod{2f_{u,v}}]$. In our case, we have $[L : K] = 2$ and $f_{u,v} = \mathrm{ord}_{dv}(q)$. The condition that $fw \equiv f_{u,v} \pmod{2f_{u,v}}$ becomes equivalent to v dividing e^+_{2fw}, but not e^+_{fw}. Since $(d, q-1) \leq 2$, this is equivalent to $v \mid e^-_{fw/2}$. Therefore, we may rewrite δ_w^- as

$$\delta_w^- = \sum_{v \mid e^-_{fw/2}} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{2uv} \cdot [\sigma_{u,v} \text{ exists}].$$

This sum is close to $S_{d,1,h}(e^-_{fw/2})$. To simplify it, we need to discuss the existence of the $\sigma_{u,v}$ automorphism.

By Theorem 4.8 and Proposition 4.10, we see that $\sigma_{u,v}$ always exists in even characteristic because it is assumed that $p \nmid d$. Indeed, condition *(1)* of Proposition 4.10 is always satisfied for $h_1 \geq 2$. Otherwise, $h_1 = 1$ and $\sigma_L(\gamma^{1/h_1}) = \gamma^{-1/h_1}$ trivially holds. Let

$$\mathcal{Q}(n) = [h_1 \nmid n] + [h_1 \mid n \text{ and } \sigma_L(\gamma^{1/h_1}) = \gamma^{-1/h_1}], \tag{4.2}$$

for all $n \geq 1$. We saw the importance of this boolean function in Proposition 4.10. For instance, we have $\mathcal{Q}(uv) = 1$ if and only if $\sigma_{u,v}$ exists, when $q \equiv 3 \pmod 4$. The existence of $\sigma_{u,v}$ remains to be determined when $q \equiv 1 \pmod 4$. We have the following:

Lemma 4.16. *Assume that $q \equiv 1 \pmod 4$. Then, $\sigma_{u,v}$ exists if and only if $(dv, q-1) \leq 2$ and $2 \nmid (uv, h)$.*

Proof. We only need to work on the last condition of Theorem 4.8. Note that we already have $2 \mid \mathrm{ord}_{dv}(q)$ because f is even. Moreover, the first condition $(dv, q-1) \leq 2$ implies that $v_2(dv) \leq 1$ and $v_2(uv) \leq 1$. If $\alpha := (uv, h, 2^\infty) = 1$, then clearly $\sigma_0(\gamma^{1/\alpha}) = \gamma^{-1/\alpha}$ and condition *(4)* of Theorem 4.8 holds by Lemma 4.9. If $\alpha = 2$, we have $2 \mid h$, which is equivalent to a_2 being a square in L. This is because $\gamma = a^2/a_2$ is an h-th power in L when $\mathbf{b}(h) = 0$. We easily see that $a_2 \in (L^\times)^2$ if and only if one of a_2 and a_2/Δ is the square of an element in K, say x^2. In the latter case, we have

$$\sigma_0(\gamma^{1/\alpha}) = \sigma_L(\gamma^{1/2}) = \sigma_L(a/x\sqrt{\Delta}) = -b/x\sqrt{\Delta} = -\gamma^{-1/2}.$$

Thus, $\sigma_{u,v}$ does not exist. The case $a_2 \in (K^\times)^2$ can not happen by our assumption at the beginning of Subsection 4.3.2. □

Lemma 4.17. *Let $d' = d/(d, 2^\infty)$ and $w \mid d'^\infty$. Then $2\delta_w^- = S_{d',1,h}(e_{fw/2}^-) \cdot C_0(d,h)$, where*

$$C_0(d,h) = \begin{cases} 1, & \text{if } 2 \nmid d, \text{ or } q \equiv 1 \pmod 4 \text{ and } 2 \mid h; \\ 0, & \text{if } 2 \mid (d,h),\ q \equiv 3 \pmod 4 \text{ and } h_1 \nmid 2e_{f/2}^-; \\ 1 - \dfrac{2^{v_2(dh)}\mathcal{Q}}{2^{v_2(q^{f/2}+1)+1}}, & \text{otherwise,} \end{cases}$$

and where $\mathcal{Q} = [\sigma_L(\gamma^{1/h_1}) = \gamma^{-1/h_1}]$.

Proof. Let $w \mid d'^\infty$. Applying Proposition 4.10 and Lemma 4.16 to (3.8) yields

$$\delta_w^- = \sum_{v \mid e_{fw/2}^-} \sum_{u \mid d} \frac{\mu(u)(uv,h)}{2uv} \cdot \begin{cases} \mathcal{Q}(uv), & \text{if } q \equiv 3 \pmod 4; \\ 1, & \text{if } 2 \mid q; \\ [2 \nmid (uv,h)], & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

Note that we should have $[(dv, q-1) \le 2] \cdot [2 \nmid (uv,h)]$ for $q \equiv 1 \pmod 4$ in the above. However, since $dv \mid q^{fw/2}+1$, the condition $(dv, q-1) \le 2$ is necessarily satisfied. If $2 \nmid (d,h)$, then it follows directly that $2\delta_w^- = S_{d,1,h}(e_{fw/2}^-)$. When $2 \mid d$ and $2 \nmid h$, we write

$$2\delta_w^- = S_{d',1,h}(e_{fw/2}^-) \left(1 - \frac{2^{v_2(dh)}}{2^{v_2(q^{f/2}+1)+1}}\right),$$

since (h, d^∞) is odd, which allows us to take out the $l = 2$ factor out with no other assumption. Note also that $v_2(e_{fw/2}^-) = v_2(e_{f/2}^-)$ since $2 \nmid w$. For the rest of the proof, we assume $2 \mid (d,h)$.

Assume that $q \equiv 1 \pmod 4$. Then, we see that v is odd, so that $2 \mid (uv,h)$ if and only if $2 \mid (u,h)$. We obtain $[2 \nmid (uv,h)] = 1 - [2 \mid u]$, and the part in the expression of δ_w^- that corresponds to $[2 \mid u]$ is equal to

$$\sum_{v \mid e_{fw/2}^-} \sum_{\substack{u \mid d \\ 2 \mid u}} \frac{\mu(u)(uv,h)}{2uv} = -\sum_{v \mid e_{fw/2}^-} \sum_{u' \mid d'} \frac{\mu(u')(u'v,h)}{2u'v}.$$

We used $v_2(uv) = 1$, so that $(uv,h) = 2(u'v,h)$, where $u' = u/(u, 2^\infty)$. Thus, since $e_{fw/2}^-$ is odd, i.e., $e_{fw/2}^- \mid d'^\infty$, and by Lemma 4.5, we may write

$$2\delta_w^- = S_{d,1,h}(e_{fw/2}^-) + S_{d',1,h}(e_{fw/2}^-).$$

Moreover, since $2 \mid (d,h)$, the sum $S_{d,1,h}(e^-_{fw/2})$ must be equal to zero because $h_1 \nmid e^-_{fw/2}$. Hence, we obtain $\delta^-_w = S_{d',1,h}(e^-_{fw/2})/2$.

Assume that $q \equiv 3 \pmod 4$. We write

$$\delta^-_w = \sum_{v \mid e^-_{fw/2}} \frac{(v,h)}{2v} \sum_{u \mid d} \frac{\mu(u)(uv,h)\mathcal{Q}(uv)}{u(v,h)},$$

and, given $v \mid e^-_{fw/2}$, let $S(v)$ be the inner sum in the above expression. If $v_2(h) > v_2(2v)$, then $\mathcal{Q}(uv) = 1$ for all $u \mid d$, and thus

$$S(v) = \prod_{l \mid d} \left(1 - \frac{(lv,h)}{l(v,h)}\right) = 0,$$

because the $l = 2$ factor is equal to zero since $(2v,h) = 2(v,h)$. It follows that $\delta^+_w = 0$ when $h_1 \nmid 2e^-_{fw/2}$. We can replace $e^+_{fw/2}$ by $e^-_{f/2}$ since w is odd and $v_2(e^-_{fw/2}) = v_2(e^-_{f/2})$ using Lemma 3.11. Assume that $h_1 \mid 2e^-_{f/2}$. With the convention $0^0 = 1$, we have

$$2\delta^-_w = \mathcal{Q} S_{d,h_1,h}(e^-_{fw/2}) + \sum_{v \mid e^-_{fw/2}}{}' \sum_{u \mid d} \frac{\mu(u)(uv,h)\mathcal{Q}^{[2|u]}}{uv},$$

where $\sum'$ means that indices v are taken with 2-adic valuation equal to $v_2(h)-1$. Here, we used $\mathcal{Q}(uv) = \mathcal{Q}$ for all $u \mid d$ when $h_1 \mid v$. This yields the left summand in the above. For the sum on the right, we call it S_0, we used $\mathcal{Q}(v) = 1$ and $\mathcal{Q}(2v) = \mathcal{Q}$ when $v_2(2v) = v_2(h)$. We now work on S_0. We have

$$S_0 = \sum_{v \mid e^-_{fw/2}}{}' \frac{(v,h)}{v} \sum_{u \mid d} \frac{\mu(u)(uv,h)\mathcal{Q}^{[2|u]}}{u(v,h)} = \sum_{v \mid e^-_{fw/2}}{}' \frac{(v,h)S(v)}{v},$$

The general term of $S(v)$ defines a multiplicative function in u. Therefore, the Möbius sum $S(v)$ seen as a function $d \mapsto S(v) := S(v,d)$ is also multiplicative. We obtain

$$S(v,d) = S(v,d')S(v,2^{v_2(d)}) = S(v,d') \sum_{u \mid 2} \frac{\mu(u)(uv,h)\mathcal{Q}^{[2|u]}}{u(v,h)} = S(v,d')(1-\mathcal{Q}),$$

where we used $(2v,h) = 2(v,h)$ in the last equality. Replacing $S(v)$ in the expression of S_0, and using $(uv,h) = 2^{v_2(h)-1}(uv',h)$, where $v' = v/(v,2^\infty)$, we find that

$$S_0 = (1-\mathcal{Q}) \sum_{v \mid e^-_{fw/2}}{}' \sum_{u \mid d'} \frac{\mu(u)(uv,h)}{uv} = (1-\mathcal{Q}) \sum_{\substack{v \mid e^-_{fw/2} \\ 2 \nmid v}} \sum_{u \mid d'} \frac{\mu(u)(uv,h)}{uv}.$$

We obtain $2\delta_w^- = \mathcal{Q}S_{d,h_1,h}(e^-_{fw/2}) + (1-\mathcal{Q})S_{d',1,h}(e^-_{fw/2})$. Since $h_1 \mid (h, d^\infty)$, we see using the product form of $S_{d,h_1,h}(e^-_{fw/2})$ of Lemma 4.5 that $S_{d,h_1,h}(e^-_{fw/2}) = S_{d,1,h}(e^-_{fw/2})$. Hence, we can factor the products in the following way:

$$2\delta_w^- = \left(\mathcal{Q}\left(1 - \frac{2^{v_2(dh)}}{2^{v_2(q^{fw/2}+1)+1}}\right)[h_1 \mid e^-_{f/2}] + 1 - \mathcal{Q}\right) S_{d',1,h}(e^-_{fw/2}).$$

A quick computation shows that the first factor is equal to $1 - 2^{v_2(dh)}\mathcal{Q}/2^{v_2(q^{fw/2}+1)+1}$ whether h_1 divides $e^-_{f/2}$ or not. Finally, we use $v_2(q^{fw/2}+1) = v_2(q^{f/2}+1)$ by Lemma 3.11, since $2 \nmid w$. □

Lemma 4.18. *Let $f_0 = \mathrm{ord}_{d(h,d'^\infty)}(q)$ and assume $[\mathcal{P}(f)] = 0$. We have*

$$\bar{f} = f_0 \cdot \begin{cases} \dfrac{(h, 2^\infty)}{(e_f^+, h, 2^\infty)}, & \text{if } 2 \mid d; \\ 1, & \text{if } 2 \nmid d. \end{cases}$$

Proof. By Lemma 3.12, we have

$$\bar{f} = \frac{f_0 d(h, d^\infty)}{(q^{f_0} - 1, d(h, d^\infty))}.$$

We work on the denominator. If d is odd, then $d(h, d^\infty)$ divides $q^{f_0} - 1$ and the result follows. If $2 \mid d$, then

$$(q^{f_0} - 1, d(h, d^\infty)) = d(h, d'^\infty)\left(\frac{q^{f_0}-1}{d(h, d'^\infty)}, h, 2^\infty\right) = d(h, d'^\infty)(e^+_{f_0}, h, 2^\infty).$$

Since $v_2(f) = v_2(f_0)$ by Lemma 3.12, we can replace $e^+_{f_0}$ by e^+_f. □

Theorem 4.19. *If $q \equiv 1 \pmod 4$, $2 \mid d$ and a_2 is a square in K, then $\delta_q^-(\gamma, d) = 0$. Otherwise, we have*

$$\delta_q^-(\gamma, d) = \frac{C_0'(d,h)}{2\bar{f}} \prod_{l \mid d'} \left(1 - \frac{l^{v_l(dh)}}{(l+1)l^{v_l(q^{\bar{f}}-1)}}\right),$$

where, with the notation of Lemma 4.17, we define

$$C_0'(d,h) = C_0(d,h) \cdot \begin{cases} \dfrac{(h, 2^\infty)}{(e_f^+, h, 2^\infty)}, & \text{if } 2 \mid d; \\ 1, & \text{if } 2 \nmid d. \end{cases}$$

Proof. The first case is given by Theorem 4.2. Otherwise, we let $f_0 = \mathrm{ord}_{d(h,d'^\infty)}(q)$. By

Lemmas 4.17 and 4.5, we have

$$\delta_w^- = \frac{C_0(d,h)}{2} \cdot \begin{cases} \displaystyle\sum_{u \mid d'} \frac{\mu(u)(dh, u^\infty)}{u(q^{fw/2}+1, u^\infty)}, & \text{if } (h, d'^\infty) \mid e^-_{fw/2}; \\ 0, & \text{otherwise,} \end{cases}$$

where we expanded the product in $S_{d',e,h}(e^-_{fw/2})$ into a Möbius sum. On the one hand, we see that $(h, d'^\infty) \mid e^-_{fw/2}$ if and only if $fw \equiv f_0 \pmod{2f_0}$. By Lemma 3.12, the latter is equivalent to $fw = f_0\nu$ for some $\nu \mid d'^\infty$. On the other hand, we have

$$(q^{fw/2}+1, u^\infty) = (q^{f_0\nu}-1, u^\infty) = (q^{\bar{f}}-1, u^\infty)(\nu, u^\infty),$$

where we used $2 \nmid u$ for the first equality above, and Lemmas 3.11 and 4.18 for the second equality. Therefore, we obtain

$$\delta_w^- = \frac{C_0(d,h)}{2} \sum_{u \mid d'} \frac{\mu(u)(dh, u^\infty)}{u(q^{\bar{f}}-1, u^\infty)(\nu, u^\infty)} =: \frac{C_0(d,h)\delta(\nu)}{2},$$

if $fw = f_0\nu$ for some $\nu \mid d'^\infty$. By (3.9), we now have

$$\delta_q^-(\gamma, d) = \frac{2\varphi(d)}{[2,d]f} \sum_{w \mid d'^\infty} \frac{\delta_w^-}{w} = \frac{C_0(d,h)\varphi(d)}{f_0[2,d]} \sum_{\nu \mid d'^\infty} \frac{\delta(\nu)}{\nu}.$$

Expanding $\delta(\nu)$, the series becomes $D(d')$, defined in Lemma 4.6. This yields

$$\delta_q^-(\gamma, d) = \frac{C_0(d,h)\varphi(d)}{f_0[2,d]} \cdot \frac{d'}{\varphi(d')} \prod_{l \mid d'} \left(1 - \frac{l^{v_l(dh)}}{(l+1)l^{v_l(q^{\bar{f}}-1)}}\right).$$

Finally, we note that $d'/\varphi(d') = d/(2,d)\varphi(d)$ and that $d/[2,d](2,d) = 1/2$, so that

$$\frac{C_0(d,h)\varphi(d)}{f_0[2,d]} \cdot \frac{d'}{\varphi(d')} = \frac{C_0(d,h)}{2f_0}.$$

The result follows by Lemma 4.18, which applies because $2 \mid f$ ensures that $[\mathcal{P}(f)] = 0$. □

Example 4.20. *Let $a_1 = a_2 = T^2+1$, $q = 3$, and $d = 4$. Then, we have $h = 2$, $f = \bar{f} = 2$, and $\mathcal{Q} = 0$. By Theorem 4.19, we have*

$$\delta_3^-(\gamma, 4) = \frac{C_0'(4,2)}{4} = \frac{1}{4}.$$

Computations show that

$$\frac{1}{12}\sum_{n=1}^{12}\frac{R_3^-(\gamma,4)}{3^n/n}\approx 0.263888,$$

which is relatively close to the expected value.

4.3.3 When $d=2$

The density $\delta_q^-(\gamma,2)$ has already been explicited in Corollary 3.26 when $q\equiv 1 \pmod 4$. In this section, we focus on the case $q\equiv 3 \pmod 4$, where we have a closed-form formula by Theorem 3.29. However, the presence of the boolean $\mathcal{B}(2^j,2^i)=[\sigma_{2^j,2^i}$ exists and $2\|f_{2^j,2^i}]$ can make its computation difficult. In this section, we mostly work on the term

$$\sum_{i=0}^{v_2(e_1^-)}\sum_{j=0}^{1}\frac{(-1)^j(2^{i+j},h)}{2^{i+j}}\cdot\mathcal{B}(2^j,2^i), \tag{4.3}$$

that appears in the expression of $\delta_q^-(\gamma,2)$. The calculations are similar to those of the previous section for the case $q\equiv 3 \pmod 4$. We may skip a few details.

Theorem 4.21. *Assume $q\equiv 3 \pmod 4$. We have $\delta_q^-(\gamma,2)=\delta_0+\delta_1$, where δ_0 was defined in Theorem 3.29,*

$$\delta_1=\frac{1}{4}\cdot\begin{cases}0, & \text{if } h_1\nmid 2e_1^-;\\ 1-\dfrac{\mathcal{Q}h_1}{2^{v_2(q+1)}}, & \text{otherwise,}\end{cases}$$

and $\mathcal{Q}=[\sigma_L(\gamma^{1/h_1})=\gamma^{-1/h_1}]$.

Proof. Our initial goal is to simplify $\mathcal{B}(2^j,2^i)$ as much as can be. Applying Lemma 3.12 to $f_{2^j,2^i}=\mathrm{ord}_{2^{i+1}}(q)$, we find that $f_{2^j,2^i}=2$ for all $1\le i\le v_2(e_1^-)$. Hence

$$\mathcal{B}(2^j,2^i)=[\sigma_{2^j,2^i}\text{ exists}],$$

for $i\ge 1$, or $(i,j)=(0,1)$. By Proposition 4.10, we obtain $\mathcal{B}(2^j,2^i)=\mathcal{Q}(2^{i+j})$. Note that we recover the case $\mathcal{B}(1,1)=1$, since $\mathcal{Q}(1)=1$. We may rewrite (4.3) as

$$\delta:=\sum_{v\mid e_1^-}\sum_{u\mid 2}\frac{\mu(u)(uv,h)\mathcal{Q}(uv)}{uv}.$$

If $h_1\nmid 2v$, then $\mathcal{Q}(uv)=1$ for all $u\mid 2$, and the inner sum in δ is equal to 0. Therefore, the outer sum in the above expression of δ can be taken over $v\mid e_1^-$ such that $h_1\mid 2v$. In particular, we see that $\delta=S_{2,1,h}(e_1^-)=0$ if $h_1\nmid 2e_1^-$, by Lemma 4.5. We assume $h_1\mid 2e_1^-$

and separate δ into two sums

$$S_1 = \sum_{\substack{v \mid e_1^- \\ h_1 \mid v}} \sum_{u \mid 2} \frac{\mu(u)(uv,h)\mathcal{Q}(uv)}{uv} \quad \text{and} \quad S_2 = \mathcal{Q}(h_1/2) - \mathcal{Q}(h_1).$$

Note that S_1 can be zero if $h_1 \nmid e_1^-$. Moreover, S_2 corresponds to the general term of δ when $v = h_1/2$. We see that $S_2 = 1 - \mathcal{Q}$ by the definition of $\mathcal{Q}(n)$, and that $\mathcal{Q}(uv) = \mathcal{Q}$ for all values of u and v in S_1. Hence

$$\delta = S_{2,h_1,h}(e_1^-) + 1 - \mathcal{Q}.$$

We apply Lemma 4.5 and see that the formulas for $h_1 \mid e_1^-$ and $h_1 \nmid e_1^-$ coincide. □

Example 4.22. *Let $a_1 = T^2 + 1$, $a_2 = T + 1$ and $q = 3$. We have $h = 1$, thus $\mathcal{Q} = 1$. By Theorem 4.21, we have*

$$\delta_3^-(\gamma, 2) = \delta_0 + \frac{1}{4} \cdot \left(1 - \frac{1}{4}\right) = \frac{1}{8} + \frac{3}{16} = \frac{5}{16} = 0.3125.$$

We found $\delta_0 = 1/8$ from Theorem 3.29 because $L_{2,2} = L(\gamma^{1/2})$ is a geometric extension of degree 4 of K. Numerically, we obtain

$$\frac{1}{10} \sum_{n=1}^{10} \frac{R_3^-(\gamma, 2)}{3^n/n} \approx 0.323133.$$

The approximated value is relatively close to 5/16.

Note that the approximation error can be large, as we see in the above example or in Example 4.20. This is due to the exponential growth of the number of prime polynomials over $\mathbb{F}_q$, which restricts computations to the first few degrees n.

4.4 The case $\mathbf{b}(h) = 1$

We assume L/K is geometric of degree two and $\mathbf{b}(h) = 1$. For consistency with the other sections, and because Theorem 4.1 allows us to switch γ to $-\gamma$, we assume $\gamma = \lambda^{h/2}\tilde{\gamma}_0^h$. Before computing formulas for the densities, we note the following:

Lemma 4.23. *If $\mathbf{b}(h) = 1$, then $2 \mid h$ and $q \equiv 1 \pmod 4$.*

Proof. We prove the lemma by its contraposition. Clearly, $2 \nmid h$ implies that $\lambda^{h/(2,h)} = \lambda^h$. If $2 \mid q$, then every element of $\mathbb{F}_q$ is a power of 2, thus $\lambda^{h/2} \in (\mathbb{F}_q^\times)^h$. If $q \equiv 3 \pmod 4$, then for every $x \in \mathbb{F}_q$, exactly one of x and $-x$ is a square in $\mathbb{F}_q$. If λ is not a square in

$\mathbb{F}_q$, then $-\lambda$ must be a square. It follows that $-\lambda^{h/2}$ is a power of h if $2\|h$, and $\lambda^{h/2}$ is a power of h if $4 \mid h$. □

Therefore, throughout this section, we assume $2 \mid h$ and $q \equiv 1 \pmod 4$. Moreover, when dealing with results related to $R_q^-(\gamma, d)$, we assume a_2 is not a square in K if $2 \mid d$. The latter is again due to Theorem 4.2. We write

$$\frac{1}{N}\sum_{n=1}^{N}\frac{R_q(\gamma,d,n)}{q^n/n} = \frac{1}{N}\sum_{\substack{n=1\\2|n}}^{N}\frac{R_q(\gamma,d,n)}{q^n/n} + \frac{1}{N}\sum_{\substack{n=1\\2\nmid n}}^{N}\frac{R_q(\gamma,d,n)}{q^n/n}, \tag{4.4}$$

and call $S_{even}(N)$ and $S_{odd}(N)$ the sums on the right-hand side that run over even and odd integers respectively. Let $\mathbb{F}_{q^2}$ denote the extension of $\mathbb{F}_q$ obtained by adjoining a square root of λ. We consider the set $R_{q^2}(\gamma, d)$ of primes $P \in \mathbb{F}_{q^2}K$ whose rank $\rho_U(P)$ is divisible by d. Note that this makes sense as $U \subset A$. Using Lemma 4.4, we see that

$$S_{even}(N) = \frac{1}{N}\sum_{n=1}^{\lfloor N/2\rfloor}\left(\frac{R_{q^2}(\gamma,d,n) - R_q(\gamma,d,n)\cdot[2 \mid n]}{q^{2n}/n}\right).$$

Moreover, we have $0 \le R_q(\gamma, d, n) \le q^n/n$. Hence $R_q(\gamma, d, n) = \mathcal{O}(q^n/n)$, so that

$$S_{even}(N) = \frac{1}{N}\sum_{n=1}^{\lfloor N/2\rfloor}\frac{R_{q^2}(\gamma,d,n)}{q^{2n}/n} + \mathcal{O}\left(\frac{1}{N}\right).$$

It follows that $S_{even}(N)$ converges to $\delta_{q^2}(\gamma, d)/2$ as N tends to infinity. Moreover, we see that γ is an h-th power in $K' := \mathbb{F}_{q^2}(T)$, so that $\mathbf{b}(h) = 0$. This means the closed-form formulas of Section 4.3 can be used to compute $\delta_{q^2}(\gamma, d)$. We obtain the following:

Theorem 4.24. *If $\mathbf{b}(h) = 1$, then the d_3-density of $R_q(\gamma, d)$ is equal to*

$$\delta_q(\gamma,d) = \frac{\delta_{q^2}(\gamma,d)}{2} + \lim_{N\to+\infty} S_{odd}(N).$$

Proof. Note that the limit of $S_{odd}(N)$ exists, since the d_3-density of $R_q(\gamma, d)$ and $R_{q^2}(\gamma, d)$ exist by the results of Chapter 3. □

It remains to consider the limit of $S_{odd}(N)$. We split $S_{odd}(N)$ into two sums $S^+_{odd}(N)$ and $S^-_{odd}(N)$ respectively, using $R_q(\gamma, d, n) = R_q^+(\gamma, d, n) + R_q^-(\gamma, d, n)$. Note that Theorem 4.24 holds for $R_q^+(\gamma, d)$ and $R_q^-(\gamma, d)$ as well. In order to compute the two limits, we need a few preliminary results on the degree $f_{u,v}$ and on the existence of $\sigma_{u,v}$. By Lemma 3.6,

we have $\mathbb{F}_{dv,uv} = \mathbb{F}_q(\zeta_{dv}, \mu^{1/(uv,h)})$ and it follows that

$$f_{u,v} = \mathrm{ord}_{dv}(q) \cdot \begin{cases} 2, & \text{if } h_1 \mid uv \text{ and } 2 \nmid \mathrm{ord}_{dv}(q); \\ 1, & \text{otherwise,} \end{cases} \tag{4.5}$$

since $\mathbf{b}(h) = 1$ and $\mu = \lambda^{h/2}$. We use 4.5 to simplify the expressions of δ_w^+ and δ_w^- given in (3.4) and (3.8) respectively.

Moreover, we need to check the existence of $\sigma_{u,v}$ to simplify (3.8) further. Necessary and sufficient conditions are given in the following lemma:

Lemma 4.25. *Assume that $q \equiv 1 \pmod 4$ and $v_2(\mathrm{ord}_{dv}(q)) = 1$. Then, $\sigma_{u,v}$ exists if and only if $(dv, q-1) \leq 2$ and*

(1) $2 \nmid (uv, h)$, or

(2) $2 \mid uv$, $v_2(h) = 1$, and $\tilde{a}_2/\Delta \in (K^\times)^2$;

Proof. Let $\alpha = (uv, h, 2^\infty)$. We use the same method as in the proof of Lemma 4.16 for the case $\alpha = 1$. The only other case is $\alpha = 2$. We have $2 \mid h$ if and only if $\tilde{a}_2 \in (L^\times)^2$. This is because $\tilde{\gamma} = \tilde{a}^2/\tilde{a}_2$ is a square in L, which is not necessarily the case for γ since $\mathbf{b}(h) = 1$. If γ is a square, i.e., if $4 \mid h$, then a_2 is a square in L and we may use the method of Lemma 4.16. Thus, assume that γ is not a square, i.e., $v_2(h) = 1$. Only one of $\tilde{a}_2$ and $\tilde{a}_2/\Delta$ is a square in K, say x^2. Let $u = \mathrm{sgn}(a_2)$. If $\tilde{a}_2 = x^2$, then

$$\sigma_0(\gamma^{1/2}) = \sigma_0\left(\frac{a}{x\sqrt{u}}\right) = \frac{b}{x\sigma_0(\sqrt{u})},$$

where $\sqrt{u}$ is in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Hence $\sigma_0(\gamma^{1/2}) = \gamma^{-1/2}$ if and only if $\sigma_0(\sqrt{u}) = \sqrt{u}$. That is, we need $\mathbb{F}_{q^2}$ to be a subfield of $\mathbb{F}_q(\zeta_{dv} + \zeta_{dv}^{-1})$, the unique subfield M of $\mathbb{F}_{dv,uv} = \mathbb{F}_q(\zeta_{dv})$ such that $\sigma_0(y) = y$ for all $y \in M$, where the equality for $\mathbb{F}_{dv,uv}$ holds because $2 \mid \mathrm{ord}_{dv}(q)$. However, by assumption, we have

$$2 \nmid [\mathbb{F}_q(\zeta_{dv} + \zeta_{dv}^{-1}) : \mathbb{F}_q] = \frac{\mathrm{ord}_{dv}(q)}{2},$$

so that $\sigma_{u,v}$ does not exists. Finally, when $\tilde{a}_2/\Delta = x^2$, similar computations show that we have $\sigma_0(\gamma^{1/2}) = \gamma^{-1/2}$ if and only if $\sigma_0(\sqrt{u}) = -\sqrt{u}$. By the same reasoning as before, this is equivalent to $v_2(\mathrm{ord}_{dv}(q)) = 1$. □

We should note the presence of the assumption $v_2(\mathrm{ord}_{dv}(q)) = 1$. Recall that there are only two cases to study for $R_q^-(\gamma, d)$, namely $d = 2$, or $2 \mid f$ and $(d, q-1) \leq 2$. They appear only if there exists $k \geq 1$ such that $d \mid q^k + 1$. Otherwise, sets are empty and the

densities zero. We will see that there is no need to consider the case $4 \mid \mathrm{ord}_{dv}(q)$ in our calculations when $2 \mid f$.

4.4.1 The limit of $S^+_{odd}(N)$

This is the easiest case and the most straightforward. By Theorem 3.15, we have

$$S^+_{odd}(N) = \frac{1}{N}\sum_{\substack{n=1\\2\nmid n}}^{N} \frac{R^+_q(\gamma,d,n)}{q^n/n} = \frac{1}{N}{\sum_{n=1}^{N}}' \delta^+_q(\gamma,d,n) + \mathcal{O}_d\left(\frac{1}{N}\sum_{n=1}^{+\infty}\tau(e^+_n)q^{-n/2}\right)$$

for all $N \geq 1$, where $\sum'$ means that the sum is over all odd n divisible by f. Moreover, since $\tau(e^-_n) \ll n$, the error term is $\mathcal{O}_q(1/N)$ because the series converges. Thus, we see that $S^+_{odd}(N) = 0$ if $2 \mid f$. Hence, we assume f is odd. Let

$$S = \bigsqcup_{w \mid d^\infty} \bigsqcup_{\substack{\alpha=1\\(\alpha,d)=1}}^{d} A_{w,\alpha},$$

which is a subset of (3.3), where $A_{w,\alpha} = \{fw(\alpha + dn) : n \geq 0\}$. Then, we see that the set of indices taken by $\sum'$ is exactly the set

$$S \cap (2\mathbb{N}+1) = \bigsqcup_{w \mid d'^\infty} \bigsqcup_{\substack{\alpha=1\\(\alpha,[2,d])=1}}^{[2,d]} A'_{w,\alpha},$$

where $A'_{w,\alpha} = \{fw(\alpha + [2,d]n) : n \geq 0\}$. Using the method of the proof of Theorem 3.18, we show that

$$\lim_{N\to+\infty} S^+_{odd}(N) = \frac{\varphi(d)}{[2,d]f}\sum_{w \mid d'^\infty}\frac{\delta^+_w}{w}. \tag{4.6}$$

We find the following lemma:

Lemma 4.26. *Assume $v_2(f) = 0$. Then, we have $\delta^+_w = S_{d',1,h}(e^+_{fw})/2$.*

Proof. We first take a look at the expression of δ^+_w in (3.4), and at $\mathcal{B}(u,v) = [f_{u,v} \mid fw]$ in particular. Since fw is odd, by (4.5), we have

$$f_{u,v} \mid fw \iff f_{u,v} = \mathrm{ord}_{dv}(q) \text{ and } 2 \nmid \mathrm{ord}_{dv}(q).$$

Note that we have used $\mathrm{ord}_{dv}(q) \mid fw$ if and only if $v \mid e^+_{fw}$. We see that $f_{u,v} = \mathrm{ord}_{dv}(q)$ if and only if $h_1 \nmid uv$ by (4.5) again. By Lemma 3.12, and since $q \equiv 1 \pmod 4$, we have

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

In addition, we have $v \mid e^+_{fw}$ and $v_2(e^+_{fw}) = v_2(e^+_1)$ since fw is odd. It follows that $\mathrm{ord}_{dv}(q)$ is odd because $v_2(dv) \leq v_2(q^f - 1)$. Hence

$$\mathcal{B}(u, v) = [h_1 \nmid uv].$$

This is a better form of $\mathcal{B}(u, v)$. Indeed, we already see that $\mathcal{B}(u, v)$ is always 1 if d is odd. In that case, our lemma follows directly.

Assume $2 \mid d$. Since $\mathcal{B}(u, v) = 0$ if $h_1 \mid v$, we are only concerned with indices $v \mid e^+_{fw}$ such that $h_1 \nmid v$ in the first sum in (3.4). Let v be such an integer and put $k = v_2(h) - v_2(v)$. Then, the general term in v in (3.4) is

$$\sum_{u|d} \frac{\mu(u)(uv, h)}{uv} \cdot [2^k \nmid u].$$

Let us call $S(v)$ the sum in the above and assume that $k \geq 2$. Then, we have $[2^k \nmid u] = 1$ for all $u \mid d$ because of the Möbius function in $S(v)$. By proofs similar to the proof of Lemma 4.5, we write $S(v)$ as the product

$$S(v) = \frac{(v, h)}{v} \prod_{l|d} \left(1 - \frac{(lv, h)}{l(v, h)}\right).$$

The product is zero because of the factor $l = 2$. Indeed, we have $h_1 \nmid v$ and $(2v, h) = 2(v, h)$. Thus, we only need to study the case $k = 1$, that is, $v_2(2v) = v_2(h)$. We obtain

$$\delta^+_w = \sum_{v|(e^+_{fw}, d'^\infty)} \sum_{u|d'} \frac{\mu(u)(2^{v_2(h)-1}uv, h)}{2^{v_2(h)}uv} = \frac{S_{d',1,h}(e^+_{fw})}{2},$$

the result we sought. □

Theorem 4.27. *Assume $v_2(f) = 0$. Then, we have*

$$\lim_{N \to +\infty} S^+_{odd}(N) = \frac{C_1(d, h)}{4\bar{f}} \prod_{l|d'} \left(1 - \frac{l^{v_l(dh)}}{(l+1)l^{v_l(q^{\bar{f}}-1)}}\right),$$

where $C_1(d, h) = 1$ if $2 \nmid d$, and $C_1(d, h) = (h, 2^\infty)/(e^+_f, h, 2^\infty)$ otherwise.

Proof. The proof is similar to the proofs of Theorems 4.12 and 4.19, so we may skip a few details. By Lemmas 4.5 and 4.26, we have $\delta^+_w = 0$ if $f_0 \nmid fw$. Otherwise, let $\nu \mid d'^\infty$ be

such that $fw = f_0\nu$. Then, by expanding $S_{d',1,h}(e^+_{fw})$ into a Möbius sum, we obtain

$$\delta^+_w = \sum_{u|d'} \frac{\mu(u)(dh, u^\infty)}{2u(q^{f_0}-1, u^\infty)(\nu, u^\infty)} =: \frac{\delta(\nu)}{2},$$

where we used Lemma 3.11 to expand $(q^{fw}-1, u^\infty)$. Now, because $2 \nmid u$ and by Lemma 3.11, we have $(q^{f_0}-1, u^\infty) = (q^{\bar{f}}-1, u^\infty)$. The limit of $S^+_{odd}(N)$ is now equal to

$$\frac{\varphi(d)}{[2,d]f} \sum_{w|d'^\infty} \frac{\delta^+_w}{w} = \frac{\varphi(d)}{2[2,d]f_0} \sum_{w|d'^\infty} \frac{\delta(\nu)}{\nu} = \frac{\varphi(d)}{2[2,d]f_0} \cdot D(d'),$$

where $D(d')$ is given in Lemma 4.6. Since $q \equiv 1 \pmod 4$, we have $[\mathcal{P}(f)] = 0$. Thus, the result follows by applying Lemma 4.18, expanding $D(d')$, and using the simplifications used at the end of the proof of Theorem 4.19. □

We summarise our results for $S^+_{odd}(N)$ in the following theorem:

Theorem 4.28. *Assume* $\mathbf{b}(h) = 1$. *Then, we have*

$$\delta^+_q(\gamma, d) = \frac{\delta^+_{q^2}(\gamma, d)}{2} + [2 \nmid f] \cdot \frac{C_1(d,h)}{4\bar{f}} \prod_{l|d'} \left(1 - \frac{l^{v_l(dh)}}{(l+1)l^{v_l(q^{\bar{f}}-1)}}\right),$$

where $C_1(d,h)$ *is defined in Theorem 4.27.*

Proof. We use Theorems 4.24 and 4.27. □

Example 4.29. *Let* $a_1 = T$, $a_2 = 3(T^3+T^2+1)^2$, *and* $q = 5$. *Then, we have* $h = 2$, *and* $\mathbf{b}(h) = 1$, *where the latter holds because*

$$\gamma = 2\left(\frac{a}{T^3+T^2+1}\right)^2,$$

and neither of 2 *and* -2 *is a square in* $\mathbb{F}_5$. *We apply Theorem 4.28 with* $d = 2$ *and obtain*

$$\delta^+_5(\gamma, 2) = \frac{\delta^+_{25}(\gamma, 2)}{2} + \frac{1}{4} = \frac{5}{24} + \frac{1}{4} = \frac{11}{24} = 0.458\bar{3},$$

where we used Theorem 4.12 on $\delta^+_{25}(\gamma, 2)$. *Our computations show that*

$$\frac{1}{6}\sum_{n=1}^{6} \frac{R^+_5(\gamma, 2)}{5^n/n} \approx 0.455626,$$

which matches the expected value. In addition, since $q \equiv 1 \pmod 4$, *we find that* $R^-_5(\gamma, 2)$

has d_3-density equal to $1/4$ from Corollary 3.26. We have

$$\frac{1}{6}\sum_{n=1}^{6}\frac{R_5^-(\gamma,2)}{5^n/n}\approx 0.233333,$$

which also matches the expected value.

4.4.2 The limit of $S_{odd}^-(N)$

Recall our assumptions: $d \mid q^k+1$ for some $k\geq 1$, $q\equiv 1 \pmod 4$, and $a_2\notin (K^\times)^2$ if $2\mid d$. As usual, we deal with the cases $2\mid f$ and $(d,q-1)\leq 2$, and $d=2$ separately.

If $d=2$, then Corollary 3.26 already provides a formula for the density. Therefore, throughout this subsection, we assume $2\mid f$ and $(d,q-1)\leq 2$. By Theorem 3.23,

$$S_{odd}^-(N)=\frac{1}{N}\sum_{\substack{n=1\\2\nmid n}}^{N}\frac{R_q^-(\gamma,d,n)}{q^n/n}=\frac{1}{N}{\sum_{n=1}^{N}}'\delta_q^-(\gamma,d,n)+\mathcal{O}_{d,q}\left(\frac{1}{N}\right)$$

for all $N\geq 1$, where $\sum'$ means that the sum is over odd integers n congruent to $f/2$ modulo f. We see that $\sum'$ is empty if $4\mid f$. We obtain the following:

Theorem 4.30. *Assume $(d,q-1)\leq 2$ and $4\mid f$. Then, we have*

$$\delta_q^-(\gamma,d)=\frac{\delta_{q^2}^-(\gamma,d)}{2}.$$

Moreover, Theorem 4.12 provides a closed-form formula for $\delta_{q^2}^+(\gamma,d)$.

Proof. Theorem 4.12 can be applied because $\mathbf{b}(h)=0$ in $K'=\mathbb{F}_{q^2}(T)$. □

Assume that $v_2(f)=1$. Then, we see that $\mathrm{ord}_d(q^2)=1$. Hence, we have $\delta_{q^2}^-(\gamma,d)=0$ and we are left with

$$\lim_{N\to+\infty}S_{odd}(N)=\delta_q^-(\gamma,d).$$

Therefore, we only need to compute a closed-form formula of $\delta_q^-(\gamma,d)$ in the case $v_2(f)=1$. For the next result, we define

$$\mathcal{R}=[v_2(h)=1 \text{ and } \tilde{a}_2/\Delta\in(K^\times)^2].$$

This boolean function turns out to be useful in applying Lemma 4.25.

Lemma 4.31. *Assume $v_2(f) = 1$ and let $w \mid d'^{\infty}$. Then, we have*

$$\delta_w^- = \frac{S_{d',1,h}(e^-_{fw/2})}{2} \cdot \begin{cases} 1, & \text{if } 2 \nmid d \text{ or } \mathcal{R} = 0; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. The proof is similar to the proof of Lemma 4.17. Recall that

$$\delta_w^- = \sum_{v \mid e^-_{fw/2}} \sum_{u \mid d} \frac{\mu(u)(uv, h)}{2uv} \cdot \mathcal{B}(u, v),$$

where $\mathcal{B}(u, v) = [\sigma_{u,v} \text{ exists}] \cdot [fw \equiv f_{u,v} \pmod{2f_{u,v}}]$. By (4.5), we have $f_{u,v} = \mathrm{ord}_{dv}(q)$ for all $u \mid d$ and $v \mid d^{\infty}$. We saw at the beginning of Subsection 4.3.2 that

$$fw \equiv \mathrm{ord}_{dv}(q) \pmod{2\mathrm{ord}_{dv}(q)}$$

if and only if $v \mid e^-_{fw/2}$. Hence $\mathcal{B}(u, v) = [\sigma_{u,v} \text{ exists}]$. Note that $\mathcal{B}(u, v) = 1$ if $2 \nmid d$ and the result follows. Thus, we assume that d is even.

Since $q \equiv 1 \pmod 4$, we see that $dv \mid q^{fw/2} + 1$ implies that $2 \nmid v$ and $v_2(d) = 1$. By Lemma 4.25, we have $\mathcal{B}(u, v) = [2 \nmid u, \text{ or } 2 \mid u \text{ and } \mathcal{R} = 1]$. By the properties of the Iverson symbol on conjunctions and disjunctions, we find that

$$\mathcal{B}(u, v) = [2 \nmid u] + [2 \mid u] \cdot \mathcal{R}.$$

If $\mathcal{R} = 1$, then $B(u, v) = 1$ and $2\delta_w^- = S_{d,1,h}(e^-_{fw/2}) = 0$ because $e^-_{fw/2}$ is odd. If $\mathcal{R} = 0$, then the calculations in the proof of Lemma 4.17 show that $\delta_w^- = S_{d',1,h}(e^-_{fw/2})/2$. □

Theorem 4.32. *Assume $v_2(f) = 1$. We have*

$$\delta_q^-(\gamma, d) = \frac{C_2(d, h)}{2\bar{f}} \prod_{l \mid d'} \left(1 - \frac{l^{v_l(dh)}}{(l+1)l^{v_l(q^{\bar{f}}-1)}}\right),$$

where $C_2(d, h) = 0$ if $2 \mid d$ and $\mathcal{R} = 1$, and otherwise,

$$C_2(d, h) = \begin{cases} \dfrac{(h, 2^{\infty})}{(e_f^+, h, 2^{\infty})}, & \text{if } 2 \mid d; \\ 1, & \text{otherwise.} \end{cases}$$

Proof. As in the proofs of Theorems 4.12, 4.19, and 4.27, we show that

$$\delta_q^-(\gamma, d) = \frac{C_2(d, h)}{2f_0} \prod_{l \mid d'} \left(1 - \frac{l^{v_l(dh)}}{(l+1)l^{v_l(q^{\bar{f}}-1)}}\right),$$

where $f_0 = \mathrm{ord}_{d(h,d'\infty)}(q)$. Lastly, we write f_0 in terms of $\bar{f}$. This is done in Lemma 4.18, which can be applied because $2 \mid f$ implies that $[\mathcal{P}(f)] = 0$. □

We summarise our results in the following theorem:

Theorem 4.33. *Assume* $\mathbf{b}(h) = 1$. *If* $2 \mid d$ *and* a_2 *is a square in* K, *then* $\delta_q^-(\gamma, d) = 0$. *Otherwise, we have*

$$\delta_q^-(\gamma, d) = \frac{\delta_{q^2}^-(\gamma, d)}{2} + [2 \| f] \cdot \frac{C_2'(d,h)}{2\bar{f}} \prod_{l \mid d'} \left(1 - \frac{l^{v_l(dh)}}{(l+1)l^{v_l(q^{\bar{f}}-1)}}\right),$$

where $C_2'(d,h)$ *was defined in Theorem 4.32.*

Proof. We use Theorems 4.24 and 4.32. □

Example 4.34. *Let* $a_1 = T$, $a_2 = 3(T^3 + T^2 + 1)^2$, $q = 5$, *and* $d = 14$. *We have* $h = 2$, $\mathbf{b}(h) = 1$, *and* $f = 6$. *By Lemma 3.20, we have* $\delta_{25}^-(\gamma, 14) = 0$. *Hence*

$$\delta_5^-(\gamma, 14) = \frac{C_2(14,2)}{12} \cdot \left(1 - \frac{1}{8}\right) = \frac{7}{96} = 0.072916\overline{6}.$$

by Theorem 4.33. In comparison, we computed

$$\frac{1}{6} \sum_{n=1}^{6} \frac{R_5^-(\gamma, 14)}{5^n/n} \approx 0.070833,$$

which matches the value of $7/96$.

More experimentations with $U(T, 3(T^3+T^2+1)^2)$ can be found in Table A.5. See also Table A.6 for another example in the $\mathbf{b}(h) = 1$ case.

4.5 The case $L = \mathbb{F}_{q^2}(T)$

We assume $L = \mathbb{F}_{q^2}(T)$ and, when dealing with results concerning $R_q^-(\gamma, d)$, a_2 is not a square in K if $2 \mid d$ and $q \equiv 1 \pmod 4$. The latter assumption is due to Theorem 4.2. Throughout this subsection, we only consider elements $\gamma \in L$ that are monic, i.e., both numerator and denominator are monic. This will simplify most of our calculations, starting with the fact that $\gamma = \tilde{\gamma}_0^h$ is automatically an h-th power. The choice for this assumption is justified by the next theorem, which shows that γ is monic in most cases. We prove the following lemma first, which is an analogue of Theorem 3.3 for Artin-Schreier extensions:

Lemma 4.35. *Assume $p = 2$. Then, $K(a)/K$ is a proper constant field extension if and only if there exist $Q \in K$ and $c \in \mathbb{F}_q$ such that $X^2 + X + c$ is irreducible over $\mathbb{F}_q$ and*

$$a = a_1(Q + \alpha),$$

where α is a root of $X^2 + X + c$.

Proof. One way is trivial. Hence, we assume that $K(a)/K$ is a proper constant field extension. In even characteristic, any degree-two extension of $\mathbb{F}_q$ is generated by the roots of an irreducible polynomial

$$X^2 + X + c,$$

for some $c \in \mathbb{F}_q$. Call α one of its root, so that $K(a) = K(\alpha)$. Then, there exist $u, v \in K$ such that $\alpha = u + av$. Let $\sigma \in Gal(\mathbb{F}_{q^2}/\mathbb{F}_q)$ be the non-trivial automorphism, that is, it sends α onto $\alpha + 1$, the other root of $X^2 + X + c$. We have

$$\sigma(\alpha) = u + \sigma(a)v = \alpha + 1 = (u + 1) + av.$$

Moreover, since σ is non-trivial, it should send a to $b = a + a_1$. We find that

$$(u + a_1 v) + av = (u + 1) + av,$$

and, because $(1, a)$ is a K-basis of $K(a)$, we obtain $a_1 v = 1$. Hence $a = a_1(u + \alpha)$ and it suffices to put $Q = u$ to find the result. □

Theorem 4.36. *If $p = 2$, then $\operatorname{sgn}(\gamma) = 1$. If $p \geq 3$, we have*

(1) $\operatorname{sgn}(\gamma) = -1$, *if* $2\deg(a_1) < \deg(a_2)$;

(2) $\operatorname{sgn}(\gamma) = 1$, *if* $2\deg(a_1) = \deg(a_2)$ *and* $\operatorname{sgn}(a_1)^2 = 4 \cdot \operatorname{sgn}(a_2)$.

Note that $2\deg(a_1) > \deg(a_2)$ can not happen because $L \neq K$.

Proof. If $p = 2$, then $a = a_1(Q + \alpha)$, with the notation of Lemma 4.35. Since, by assumption, γ is not in $\mathbb{F}_{q^2}$ and

$$\gamma = \frac{Q + \alpha}{Q + \alpha + 1},$$

we see that $Q \notin \mathbb{F}_q$ and $\operatorname{sgn}(\gamma) = 1$. Assume that $p \geq 3$. By Theorem 3.3, we write $\Delta = u\delta^2$ for some $\delta \in A$ monic and $u \in \mathbb{F}_q$ not a square. First, we can not have $2\deg(a_1) > \deg(a_2)$ because $\Delta = a_1^2 - 4a_2$, so it would mean that u is the leading coefficient of a_1^2, which is a square. When $2\deg(a_1) < \deg(a_2)$, we have $\deg(\delta) = \deg(a_2)/2$ and

$$\operatorname{sgn}(a) = \operatorname{sgn}\left(\frac{a_1 + \delta\sqrt{u}}{2}\right) = \frac{\sqrt{u}}{2},$$

because $\deg(a_1) < \deg(\delta)$. Similarly, we obtain $\mathrm{sgn}(b) = -\sqrt{u}/2$ and $\mathrm{sgn}(\gamma) = -1$. Finally, if $2\deg(a_1) = \deg(a_2)$ and $\mathrm{sgn}(a_1)^2 = 4 \cdot \mathrm{sgn}(a_2)$, then $\deg(\delta) < \deg(a_1)$ and

$$\mathrm{sgn}(a) = \mathrm{sgn}\left(\frac{a_1 + \delta\sqrt{u}}{2}\right) = \frac{\mathrm{sgn}(a_1)}{2} = \mathrm{sgn}(b).$$

The result follows. □

Under the assumptions made in Theorem 4.36 and with Theorem 4.1, which allows to switch between γ and $-\gamma$, it makes sense to assume γ monic. However, the theorem does not hold in the case $2\deg(a_1) = \deg(a_2)$ and $\mathrm{sgn}(a_1)^2 \neq 4 \cdot \mathrm{sgn}(a_2)$. Indeed, if $q = 3$,

$$a_1 = T + 1 \quad \text{and} \quad a_2 = 2T^2 + 2T + 1,$$

then $\Delta = 2T^2$, and one can show that $\mathrm{sgn}(\gamma) = \sqrt{2} \in \mathbb{F}_9$. Therefore, although we deal with most cases here, there are unsolved remaining cases. The first consequences of this assumption are given in the following lemma:

Lemma 4.37. *Assume γ monic. Then, condition (4) of Theorem 4.8 is always satisfied, and we have $[\mathbb{F}_{n,d} : \mathbb{F}_q] = 2 \cdot \mathrm{ord}_n(q^2)$ for all $d \mid n$.*

Proof. Since γ is monic and because $\sigma_L(\gamma) = \gamma^{-1}$, we have

$$\sigma_0(\gamma^{1/(d,h)}) = \zeta_{(d,h)}^k \gamma^{-1/(d,h)} = \gamma^{-1/(d,h)}.$$

We know γ remains monic in $\mathbb{F}_{n,d}$ and that $\gamma^{1/(d,h)} = \tilde{\gamma}_0^{h/(d,h)}$ is monic as well. The same is true for $\sigma_0(\gamma)$ and $\sigma_0(\gamma^{1/(d,h)})$. Thus, the last condition in Theorem 4.8 is satisfied. Next, we use Theorem 3.7 to compute the degree. We have

$$\mathrm{ind}_{\mathbb{F}_{q^2}(\zeta_n)^\times}(\mu) = \mathrm{ind}_{\mathbb{F}_{q^2}(\zeta_n)^\times}(1) = q^{2\mathrm{ord}_n(q^2)} - 1,$$

which is divisible by (d, h), and the result follows. □

This lemma will be very helpful in our calculations, allowing for many simplifications. As in the previous section, we can show that

$$\delta_q(\gamma, d) = \frac{\delta_{q^2}(\gamma, d)}{2} + \lim_{N \to +\infty} S_{odd}(N), \tag{4.7}$$

where $S_{odd}(N)$ was defined in the same way as in Section 4.4. Note that the results of Chapter 3 imply that the limit exists because both $\delta_q(\gamma, d)$ and $\delta_{q^2}(\gamma, d)$ exist. Now, we know that a prime $P \in K$ splits in L if and only if $\deg(P)$ is even by [29, Proposition 8.13]. Therefore, we have $R_q(\gamma, d, n) = R_q^-(\gamma, d, n)$ for all odd $n \geq 1$. We obtain:

Theorem 4.38. *Assume $L = \mathbb{F}_{q^2}(T)$. Then, we have*

$$\delta_q^+(\gamma, d) = \frac{\delta_{q^2}^+(\gamma, d)}{2}.$$

If γ is monic, then Theorem 4.12 provides a closed-form formula for $\delta_{q^2}^+(\gamma, d)$.

Proof. See the above discussion for the equality. If γ is monic, then $[\mathbb{F}_{dv,uv} : \mathbb{F}_{q^2}]$ is equal to $\mathrm{ord}_{dv}(q^2)$ by Lemma 4.37. Thus, Theorem 4.12 applies □

Example 4.39. *Let $a_1 = 1$, $a_2 = T^2 + T + 1$, $q = 2$ and $d = 15$. We have*

$$f(X) = X^2 - a_1 X + a_2 = (X + T)^2 + (X + T) + 1,$$

thus the roots of f are $a = T + \alpha$ and $b = T + \alpha + 1$, where $\alpha \in \mathbb{F}_4$ satisfies $\alpha^2 + \alpha + 1 = 0$. We see that $\gamma = a/b$ is monic and $L = \mathbb{F}_{q^2}(T)$ by Lemma 4.35. Thus, we can apply Theorem 4.38. We find

$$\delta_2^+(\gamma, 15) = \frac{\delta_4^+(\gamma, 15)}{2} = \frac{1}{4}\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{6}\right) = \frac{5}{32} = 0.15625.$$

Numerically, we found

$$\frac{1}{8}\sum_{n=1}^{8} \frac{R_2^+(\gamma, 15)}{2^n/n} \approx 0.150000,$$

which matches the value. In addition, note that $15 \nmid 2^k + 1$ for all $k \geq 0$. Therefore, we have $\delta_2(\gamma, 15) = \delta_2^+(\gamma, 15) = 5/32$.

In the following, we address the case of $\delta_q^-(\gamma, d)$. We know that it is zero if $d \nmid q^k + 1$ for all $k \geq 1$. Otherwise, Lemma 3.20 shows that $S_{odd}(N) = 0$ for all $N \geq 1$ unless $2 \mid f$ and $(d, q - 1) \leq 2$, or $d = 2$.

When $d = 2$, by Corollary 3.26, we only need to address the case $q \equiv 3 \pmod 4$. Moreover, there is no need to consider the identity (4.7). Indeed, in the proof of Theorem 3.29, we actually show that

$$\delta_0 = \lim_{N \to +\infty} \frac{1}{N} \sum_{\substack{n=1 \\ 2 \mid n}}^{N} \frac{R_q^-(\gamma, 2, n)}{q^n/n},$$

where δ_0 is defined in the theorem, while the sum given by $\delta_q^-(\gamma, 2) - \delta_0$ corresponds to the limit of $S_{odd}(N)$. We have the following:

Theorem 4.40. *Assume $q \equiv 3 \pmod 4$ and γ is monic. Then, we have*

$$\delta_q^-(\gamma, 2) = \frac{1}{2} \cdot \begin{cases} 1 - \dfrac{h_1}{2^{v_2(q+1)}}, & \text{if } h_1 \mid e_1^-; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. First, note that the δ_0 constant defined in Theorem 3.29 is zero because L/K is not geometric, and thus neither is $L_{2,2}/K$. Next, by Lemma 4.37, we have

$$f_{2^j,2^i} = \frac{2\mathrm{ord}_{2^{i+1}}(q)}{(\mathrm{ord}_{2^{i+1}}(q), 2)} = \mathrm{ord}_{2^{i+1}}(q),$$

for all $i \geq 1$. Then, by Lemma 3.12, we obtain $f_{2^j,2^i} = 2$. Also, we see that $\sigma_{2^j,2^i}$ always exists if $i \geq 1$ or $(i, j) = (0, 1)$, since $(2^{i+1}, q-1) = 2$ and $2 \mid \mathrm{ord}_{2^{i+1}}(q)$, and by Lemma 4.37. Hence $\mathcal{B}(2^j, 2^i) = 1$ for all $i \geq 0$ and $j \in \{0, 1\}$, and

$$\delta_q^-(\gamma, 2) = \frac{1}{2} \sum_{i=0}^{v_2(e_1^-)} \sum_{j \in \{0,1\}} \frac{(-1)^j (2^{i+j}, h)}{2^{i+j}} = \frac{S_{2,1,h}(e_1^-)}{2},$$

by Theorem 3.29. The result follows by Lemma 4.5. □

Example 4.41. *Let $a_1 = 2T^2$, $a_2 = T^4 + (T+1)^2$, and $q = 3$. We see that $\Delta = -(T+1)^2$, thus $L = \mathbb{F}_9(T)$. Moreover, we have $h = 1$ and $\mathrm{sgn}(\gamma) = 1$, by Theorem 4.36. Therefore, we can apply Theorems 4.38 and 4.40. On the one hand, we have*

$$\delta_3^+(\gamma, 2) = \frac{1}{2}\left(1 - \frac{1}{12}\right) = \frac{11}{24} = 0.458333\bar{3},$$

and on the other hand, we have

$$\delta_3^-(\gamma, 2) = \frac{1}{2}\left(1 - \frac{1}{4}\right) = \frac{3}{8} = 0.375,$$

We computed

$$\frac{1}{8}\sum_{n=1}^{8} \frac{R_3^+(\gamma, 2)}{3^n/n} \approx 0.472107 \quad \text{and} \quad \frac{1}{8}\sum_{n=1}^{8} \frac{R_3^-(\gamma, 2)}{3^n/n} \approx 0.368990,$$

which matches the theoretical values.

We are done with the case $d = 2$. We already see that the assumption that γ is monic will simplify most calculations. Now, assume that $2 \mid f$ and $(d, q-1) \leq 2$. By Theorem

3.22, as in the previous section, we may write

$$S_{odd}(N) = \frac{1}{N}\sum_{\substack{n=1\\2\nmid n}}^{N} \frac{R_q^-(\gamma,d,n)}{q^n/n} = \frac{1}{N}\sum_{n=1}^{N}{}' \delta_q^-(\gamma,d,n) + \mathcal{O}_{d,q}\left(\frac{1}{N}\right), \tag{4.8}$$

for all $N \geq 1$, where $\sum'$ means that sum is over odd n's congruent to $f/2$ modulo f.

Theorem 4.42. *Assume $(d, q-1) \leq 2$ and $4 \mid f$. We have $\delta_q^-(\gamma, d) = 0$.*

Proof. The sum in the right-hand side of (4.8) is empty if $4 \mid f$. Thus, the limit of $S_{odd}(N)$ is zero. By (4.7), we are left with

$$\delta_q^-(\gamma,d) = \frac{\delta_{q^2}^-(\gamma,d)}{2},$$

However, in $K' = \mathbb{F}_{q^2}(T)$, we have $K'(a) = K'$. This means that $L' = K'$ and there is no prime P in K' with $\epsilon_P = -1$. Hence $R_{q^2}^-(\gamma, d)$ is empty. □

Next, if $v_2(f) = 1$, then $\mathrm{ord}_d(q^2) = 1$. It follows that $\delta_{q^2}^-(\gamma, d) = 0$ by Lemma 3.20. Therefore, from (4.7), we obtain

$$\lim_{N\to+\infty} S_{odd}(N) = \delta_q^-(\gamma,d).$$

Thus, there is no more trick we can use and we have to compute a closed-form of $\delta_q^-(\gamma, d)$ directly. Fortunately, the assumption $v_2(f) = 1$ simplifies many calculations.

Theorem 4.43. *Assume γ is monic, $(d, q-1) \leq 2$, and $v_2(f) = 1$. We have*

$$\delta_q^-(\gamma,d) = \frac{C_3(d,h)}{\bar{f}} \prod_{l\mid d'} \left(1 - \frac{l^{v_l(dh)}}{(l+1)l^{v_l(q^{\bar{f}}-1)}}\right),$$

where

$$C_3(d,h) = \begin{cases} 1, & \text{if } 2 \nmid d; \\ 1 - \dfrac{2^{v_2(dh)}}{2^{v_2(q+1)+1}}, & \text{if } 2 \mid d \text{ and } h_1 \mid e_{f/2}^-; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Recall from (3.9) and (3.8) that

$$\delta_q^-(\gamma,2) = \frac{\varphi(d)}{[2,d]f} \sum_{w\mid d'^\infty} \frac{\delta_w^-}{w} \quad \text{and} \quad \delta_w^- = \sum_{v\mid e_{fw/2}^-} \sum_{u\mid d} \frac{\mu(u)(uv,h)}{uv} \cdot \mathcal{B}(u,v).$$

We work on $\mathcal{B}(u,v)$ first. We have $(dv, q-1) \leq 2$ if $q \not\equiv 1 \pmod 4$. If $q \not\equiv 1 \pmod 4$, we see that $v_2(d) = 1$, and v is odd because $e^-_{fw/2}$ is. Hence $(dv, q-1) = 2$. Next, using Theorem 4.8 and Lemma 4.37, we find that $\sigma_{u,v}$ exists and

$$\mathcal{B}(u,v) = [fw \equiv \mathrm{ord}_{dv}(q) \pmod{2\mathrm{ord}_{dv}(q)}].$$

We saw at the beginning of Subsection 4.3.2 that this congruence is equivalent to the divisibility condition $v \mid e^-_{fw/2}$. It follows that $\mathcal{B}(u,v) = 1$ and $\delta^-_w = S_{d,1,h}(e^-_{fw/2})$. By Lemma 4.5, we have $\delta^-_w = 0$ if $(h, d^\infty) \nmid e^-_{fw/2}$ and otherwise, we have

$$\delta^-_w = \sum_{u \mid d} \frac{\mu(u)(dh, u^\infty)}{u(q^{fw/2}+1, u^\infty)}.$$

Note that the general term in δ^-_w is a multiplicative function in u, so $d \mapsto \delta^-_w =: \delta^-_w(d)$ is also multiplicative. Thus, we obtain

$$\delta^-_w(d) = \left(1 - \frac{2^{v_2(dh)}}{2^{v_2(q+1)+1}}\right)^{[2|d]} \delta^-_w(d'),$$

where we took into account that $v_2(e^-_{fw/2}) = v_2(e^-_{f/2}) = v_2(q+1) - v_2(d)$ is fixed. The latter implies that $\delta^-_q(\gamma, 2) = 0$ when $h_1 \nmid e^-_{f/2}$ and $2 \mid d$. Otherwise, let $\bar{f} = \mathrm{ord}_{d(h,d^\infty)}(q)$; it satisfies $v_2(\bar{f}) = v_2(f) = 1$, by Lemma 3.12. We have $(h, d^\infty) \mid e^-_{fw/2}$ if and only if there exists $\nu \mid d'^\infty$ such that $fw = \bar{f}\nu$. We obtain $\delta^-_w = S_{d',1,h}(e^-_{fw/2}) \cdot \epsilon_q(d,h)$, where

$$\epsilon_q(d,h) = \begin{cases} 1, & \text{if } 2 \nmid d; \\ 1 - \dfrac{2^{v_2(dh)}}{2^{v_2(q+1)+1}}, & \text{if } 2 \mid d \text{ and } h_1 \mid e^-_{f/2}. \end{cases}$$

Using the change of variables $fw = \bar{f}\nu$, expanding $S_{d',1,h}(e^-_{fw/2})$ into a Möbius sum, and applying Lemma 3.11 to $(q^{\bar{f}\nu/2}+1, u^\infty)$, we obtain

$$\delta^-_q(\gamma, d) = \frac{2\varphi(d)\epsilon_q(d,h)}{[2,d]\bar{f}} \sum_{\nu \mid d'^\infty} \sum_{u \mid d'} \frac{\mu(u)(dh, u^\infty)}{u(q^{\bar{f}}-1, u^\infty)\nu(\nu, u^\infty)}.$$

We apply Lemma 4.6, and the rest of the proof follows as in the proof of Theorem 4.19. □

We summarise our results for $d \geq 3$ in the following theorem:

Theorem 4.44. *Assume γ is monic, $2 \mid f$, and $(d, q-1) \leq 2$. If $v_2(f) = 1$, then*

$$\delta_q^-(\gamma, d) = \frac{C_3(d,h)}{\bar{f}} \prod_{l \mid d'} \left(1 - \frac{l^{v_l(dh)}}{(l+1)l^{v_l(q^{\bar{f}}-1)}}\right),$$

where $C_3(d,h)$ was defined in Theorem 4.43. Otherwise, if $4 \mid f$, then $\delta_q^-(\gamma, d) = 0$.

Proof. We use Theorem 4.43 and (4.7). □

Example 4.45. *Consider the sequence of Example 4.41 with $q = 3$ and $d = 14$. We have $h = 1$ and $f = \bar{f} = 6$. By Theorem 4.44, we have*

$$\delta_3^-(\gamma, 14) = \frac{C(14,1)}{6} \cdot \left(1 - \frac{1}{8}\right) = \frac{7}{64} = 0.109375.$$

Numerically, we found the following:

$$\frac{1}{12} \sum_{n=1}^{12} \frac{R_3^-(\gamma, 14)}{3^n/n} \approx 0.116224,$$

which is relatively close to our result. For further investigation, the values obtain numerically for $n = 9$, 10, and 11, are

$$0.154965, \quad 0.139468, \quad \textit{and} \quad 0.126789,$$

respectively. We see that it seems to slowly converge towards our result. Note that the degrees $n = 9$ and $n = 12$ are important. Indeed, they are multiples of $f/2 = 3$, and this is where we find new contributions to the density. See Table A.8 for more experimentations.

4.6 Algorithms and SageMath computations

In this section, we provide algorithms that find many of the constants that were defined in this chapter. We compute h, $\mathbf{b}(h)$, and $\sigma_L(\gamma^{1/h_1})$. By the results of Sections 4.3 and 4.5, the computation of such constants is difficult only when L/K is a geometric extension of degree 2. This will be our assumption throughout this section. We propose an implementation of every algorithm presented using SageMath 9.0 [35].

In the first subsection, we prove a simple algorithm to compute the constant h, not only in L, but in a given constant field extension of L as well. The latter will be useful in the next subsections. We use the Newton polygons of a certain family of polynomials over constant field extensions of K.

In the second subsection, we address the case of the boolean function $\mathcal{Q}$. The algorithm

simply computes successive square roots of γ, or $-\gamma$ in some cases, down to γ^{1/h_1}. Then, we find its image by σ_L easily.

4.6.1 The h and $\mathbf{b}(h)$ constants

Throughout this subsection, we let $M = \mathbb{F}_{q^m}L$ for some $m \geq 1$. To construct our first algorithm, recall that γ is an n-th power, $n \geq 2$, if and only if the polynomial $X^n - \gamma$ has a linear factor over M. This is equivalent to the polynomial

$$f_n(X) = (X^n - \gamma)(X^n - \sigma_L(\gamma)) = X^{2n} - uX^n + 1$$

having an irreducible factor of degree two over $\mathbb{F}_{q^m}K$, where we put $u := (a_1^2 - 2a_2)/a_2$ and σ_L for the non-trivial automorphism of $Gal(M/\mathbb{F}_{q^m}K)$. Indeed, we have

Theorem 4.46. *Let $n \geq 2$. We have $\gamma \in (M^\times)^n$ if and only if $f_n(X)$ has an irreducible factor of degree 2 over $\mathbb{F}_{q^m}(T)$.*

Proof. Let $\gamma = x^n$, where $x \in M$. Then $X^n - \gamma = (X - x)g(X)$ for some $g \in M[X]$, and

$$f_n(X) = (X - x)(X - \sigma_L(x)) \cdot h(X),$$

for some $h \in \mathbb{F}_{q^m}K[X]$. The polynomial $(X - x)(X - \sigma_L(x)) \in \mathbb{F}_{q^m}K[X]$ is irreducible, as $\gamma \notin \mathbb{F}_{q^m}K$ ensures that $x \notin \mathbb{F}_{q^m}K$. For the converse, if f_n has an irreducible factor of degree 2, say g, then it must split over M. Indeed, by contradiction, if g remains irreducible in $M[X]$, then it divides one of $X^n - \gamma$ and $X^n - \gamma^{-1}$. We assume that

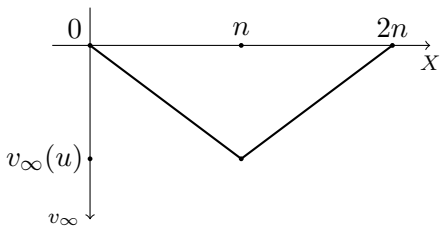
$$X^n - \gamma = g(X)h(X),$$

for some $h \in M[X]$. Then $X^n - \gamma^{-1} = g(X)(\sigma_L h)(X)$, where $\sigma_L g = g$ since $g \in \mathbb{F}_{q^m}K[X]$. Hence g divides both $X^n - \gamma$ and $X^n - \gamma^{-1}$, which are coprime because $\gamma \neq \gamma^{-1}$. This is a contradiction. Therefore, there exists $x \in M \setminus \mathbb{F}_{q^m}K$ such that $g(x) = 0$ and $x^n = \gamma$. □

We seek to determine for which integers $n \geq 2$ the polynomial $f_n(X)$ can be reducible. We draw the Newton polygons of f_n to show that there are only finitely many integers $n \geq 2$ to check. Those are divisors of $v(u)$ for a fixed valuation v of M.

Theorem 4.47. *We have $\gamma \in (M^\times)^n$ only if $n \mid \deg(u)$ if $2\deg(a_1) > \deg(a_2)$, and otherwise, there exists a prime $P \mid a_2$ in A such that $v_P(u) < 0$ and $n \mid v_P(u)$.*

Proof. Assume $2\deg(a_1) > \deg(a_2)$. Then, the Newton polygon of $f_n(X)$ with respect to the valuation $v_\infty = -\deg$ in M is the following:



If γ is an n-th power, then $f_n(X)$ is reducible by Theorem 4.46. On the Newton polygon, we see that non-constant factors of f_n have either $n/v_\infty(u)$, or $-n/v_\infty(u)$ as their slope. Since f_n is reducible, we should have non-trivial integer points on the two segments, where, by non-trivial, we mean different from $(0,0)$, $(n, v_\infty(u))$ and $(2n, 0)$. Such points exist only if $(v_\infty(u), n) > 1$, thus only if $n \mid \deg(u)$.

Assume $2\deg(a_1) \leq \deg(a_2)$. If $v_\mathfrak{p}(u) \geq 0$ for all primes $\mathfrak{p} \mid a_2$ in $\mathbb{F}_{q^m}[T]$, then $a_2 \mid a_1^2$ and $a_2 = \lambda a_1^2$ for some $\lambda \in \mathbb{F}_q^\times$ because $2\deg(a_1) \leq \deg(a_2)$. This is a contradiction to the non-degeneracy of U. Therefore, there exists a prime $\mathfrak{p} \mid a_2$ with $v_\mathfrak{p}(u) < 0$. We draw the Newton polygon with respect to the $\mathfrak{p}$-valuation to show that $n \mid v_\mathfrak{p}(u)$. Let $P = \mathfrak{p} \cap A$. Then, we find that $n \mid v_P(u)$ since $u \in K$ and $\mathbb{F}_{q^m}(T)$ is a constant field extension of K, hence unramified. □

Our first algorithm consists in computing a bound D for the powers of γ, whose existence is ensured by Theorem 4.47. Recall that $\gamma = \pm\lambda^{h/(2,h)}\tilde{\gamma}_0^h$. In particular, we see that γ is almost a full power of h. More importantly, only a constant is preventing γ from being an h-th power. Therefore, we may extend the field of constants of L to $\mathbb{F}_{q^m}$ for some $m \geq 1$, so that $\pm\lambda^{h/(2,h)} = x^h$, where $x \in \mathbb{F}_{q^m}$. It follows from Theorem 4.47 that D is a bound for our constant h.

Algorithm 1 Computation of a bound for h

Input: Non-zero polynomials $a_1, a_2 \in A$ with $a_1^2/a_2 \notin \mathbb{F}_q^\times$ and such that $X^2 - a_1X + a_2$ is irreducible over A.

Output: Integer $D \in \mathbb{Z}$ such that $h \mid D$.

```
u ← (a_1^2 − 2a_2)/a_2
D ← 2 deg(a_1) − deg(a_2)
if D ≤ 0 then                ▷ Looking for P with v_P(u) < 0 in case 2 deg(a_1) ≤ deg(a_2).
    for P | a_2 do
        D_P ← v_P(u)
        if D_P < 0 then
            D ← −D_P
            break
return D
```

In the next algorithm, we aim to compute both constants h and $\mathbf{b}(h)$. To compute h,

as mentioned above, we add constants to L so that γ is an h-th power in $M = \mathbb{F}_{q^m}L$. If D is odd, then γ is already an h-th power in L, so $m = 1$ and $\mathbf{b}(h) = 0$. If D is even and $p \neq 2$, we consider the field $\mathbb{F}_{q^m} = \mathbb{F}_{q^2}(\zeta_{2^{v_2(2D)}})$, where $m = 2\mathrm{ord}_{2^{v_2(2D)}}(q^2)$. We first consider $\mathbb{F}_{q^2}$ to make sure that $\lambda^{h/2}$ is an h-th power. The $2^{v_2(2D)}$-th roots of unity ensure that ± 1 is an h-th power. If $p = 2$, then $\gamma = \lambda^{h/2}\tilde{\gamma}_0^h$. Since every element of $\mathbb{F}_q$ is a square, we see that $\lambda^{h/2}$ is an h-th power, $m = 1$ and $\mathbf{b}(h) = 0$.

We check whether $f_n(X)$ has an irreducible factor of degree two in $\mathbb{F}_{q^m}(T)$ for all divisors $n \mid D$. By Theorem 4.46, the largest such n is equal to h. The method works similarly to compute $\mathbf{b}(h)$ when $2 \mid h$. Once we know the value of h, we check whether γ and $-\gamma$ are h_1-th powers in L. For that, we introduce another polynomial

$$g_n(X) = (X^n + \gamma)(X^n + \sigma_L(\gamma)) = X^{2n} + uX^n + 1.$$

There is only a change in the sign of u, so that Theorems 4.46 and 4.47 hold for g_n. Now, it suffices to check that f_{h_1} and g_{h_1} have an irreducible factor of degree two. If only one of them does, then $\mathbf{b}(h) = 0$. Moreover, if it is g_{h_1} that has an irreducible factor of degree two and not f_{h_1}, then we know γ should be switched to $-\gamma$. If none of them have such a factor, then $\mathbf{b}(h) = 1$.

Algorithm 2 Computation of h and $\mathbf{b}(h)$

Input: Non-zero polynomials $a_1, a_2 \in A$ with $a_1^2/a_2 \notin \mathbb{F}_q^\times$ such that $X^2 - a_1X + a_2$ is irreducible over A, and the bound D.

Output: The 3-tuple $(h, \mathbf{b}(h), e)$, where $e = -1$ when $\mathbf{b}(h) = 0$ and γ should be switched to $-\gamma$, and $e = 1$ otherwise.

$h, m, e \leftarrow 1$
if D is even **then** $m \leftarrow 2\mathrm{ord}_{2^{v_2(2D)}}(q^2)$
for $n \mid D$ **do** ▷ Divisors should be checked in increasing order.
    if $n \neq D$ and $f_{D/n}(X)$ has a prime factor of degree 2 in $\mathbb{F}_{q^m}(T)[X]$ **then**
        $h \leftarrow [h, D/n]$
if $f_{h_1}(X)$ has a prime factor of degree 2 in $\mathbb{F}_q(T)[X]$ **then**
    return $(h, 0, 1)$
if $g_{h_1}(X)$ has a prime factor of degree 2 in $\mathbb{F}_q(T)[X]$ **then**
    return $(h, 0, -1)$
return $(h, 1, 1)$.

We implemented Algorithms 1 and 2 using SageMath, and display our code below. First, we define $\mathbb{F}_q$, A, and $B := K[X]$:

[1]:
```
q=9
F.<a> = GF(q)
A.<T> = F[]
B.<X> = Frac(A)[]
```

The program below, **h_bound**, provides an implementation of Algorithm 1. Given two polynomials $a_1, a_2 \in A$, it returns an integer $D \in \mathbb{Z}$ such that $h \mid D$. As an example, we compute **h_bound**$(T, -1)$, which corresponds to the sequence of Fibonacci polynomials of characteristic polynomial $X^2 - TX - 1$.

[2]:
```
def h_bound(a_1,a_2):
    D = 2*A(a_1).degree()-A(a_2).degree()

    if D<=0:
        for p in prime_divisors(a_2):
            Dp = valuation(a_1^2-2*a_2,p)-valuation(a_2,p)
            if Dp<0:
                D = -Dp
                break

    return D

h_bound(T,-1)
```

[2]: 2

The next program, **h_constants**, provides an implementation of Algorithm 2. It takes two polynomials $a_1, a_2 \in A$ as an input and returns $[h, \mathbf{b}(h), e]$, where $e = -1$ if $\mathbf{b}(h) = 0$ and γ should be switched for $-\gamma$, and $e = 1$ otherwise.

In the first lines of the program, we define our setting. For instance, we define D by calling the **h_bound** function, then m is defined in the first `if` statement. The next lines define $\mathbb{F}_{q^m}$, $\mathbb{F}_{q^m}(T)[X]$, and u. The computation of h is done in the first `for` loop. The last part of the program focuses on computing $\mathbf{b}(h)$ as presented in Algorithm 2. Depending on whether the test holds for `f` or `g`, we can determine the value of e.

[3]:
```
def h_constants(a_1,a_2):
    D = h_bound(a_1,a_2)
    [h, m, b, e] = [1]*4
```

```
if D%2==0 and F.characteristic()!=2:
    v = valuation(2*D,2)
    m = 2*Mod(q^2,2^v).multiplicative_order()

G.<c> = F.extension(m)
R.<t> = G[]
K = Frac(R)
C.<x> = K[]

u = (a_1^2-2*a_2)/a_2

for n in divisors(D):
    d = D//n
    if h%d==0:
        continue
    f = x^(2*d)-K(u)*x^d+1
    for p, exp in f.factor():
        if p.degree()==2:
            h = lcm(h,d)
            break

if h%2==0 and q%4==1:
    w = valuation(h,2)
    f = X^(2^(w+1))-u*X^(2^w)+1
    g = f+2*u*X^(2^w)

    for p, exp in f.factor():
        if p.degree()==2:
            b = 0
            break

    if b==1 and F.characteristic()!=2:
        for p, exp in g.factor():
            if p.degree()==2:
                b = 0; e = -1
                break
```

```
    else: b = 0

    return [h,b,e]

%time h_constants(T,-1)
```

[3]: `[2, 0, 1]`

In the example computed above, with $a_1 = T$ and $a_2 = -1$, we obtain $h = 2$, $\mathbf{b}(h) = 0$ and $e = 1$ from **h_constants**. We check that this is valid. For the sequence of Fibonacci polynomials, we have $\gamma = -a^2$, where a is a root of $X^2 - TX - 1$, say

$$a = \frac{T + \sqrt{T^2 + 4}}{2}.$$

Since $q = 9$, we have $\gamma = (ia)^2$ for some $i \in \mathbb{F}_9$ such that $i^2 = -1$. It suffices to prove that ia is not an n-th power in $\bar{\mathbb{F}}_q L$. Following the method of Theorem 4.46, we show that

$$F_n(X) = (X^n - ia)(X^n - ib) = X^{2n} - iTX^n + 1$$

does not have an irreducible factor of degree 2 when $n \geq 2$. This is straightforward if we see $F_n(X)$ as a polynomial $F_n(X, T)$ in T. Indeed, we have

$$F_n(X, T) = -iX^n T + (X^{2n} + 1),$$

and the only way for $F_n(X)$ to be composite is for its coefficients $-iX^n$ and $X^n + 1$ to have a common factor. This is not the case, thus ia is at most a power of $n = 1$. We obtain $h = 2$. We easily see that $\mathbf{b}(h) = 0$ and $e = 1$ because γ is a power of 2.

4.6.2 The $\mathcal{Q}$ constant

In this second subsection, we present an algorithm computing $\mathcal{Q} = [\sigma_L(\gamma^{1/h_1}) = \gamma^{-1/h_1}]$. Note that the boolean $\mathcal{Q}$ is only needed when $\mathbf{b}(h) = 0$. Moreover, we assume the characteristic to be odd, because $\mathcal{Q}$ does not appear in the density formulas when $p = 2$. We assume h to be even in Algorithm 3. If h is odd, then we know that $\mathcal{Q} = 1$. Note that because $\sigma_L(\gamma^{1/h_1}) = \pm\gamma^{-1/h_1}$, we use $\mathcal{Q} = (\sigma_L(\gamma^{1/h_1}) \cdot \gamma^{1/h_1} + 1)/2$ in the algorithm.

Algorithm 3 Computation of $\mathcal{Q}$

Input: Non-zero polynomials $a_1, a_2 \in A$ with $a_1^2/a_2 \notin \mathbb{F}_q^\times$ and such that $X^2 - a_1X + a_2$ is irreducible over A, the constant h, and $e = -1$ when γ should be switched to $-\gamma$, or $e = 1$ otherwise.

Output: The constant $\mathcal{Q}$.

1: $r \leftarrow e\gamma$
2: **for** $1 \leq n \leq v_2(h)$ **do**
3: **if** r is a square in L **then**
4: $r \leftarrow \sqrt{r}$
5: $r \leftarrow \sqrt{-r}$
6: **return** $(\sigma_L(r) \cdot r + 1)/2$

As in Subsection 4.6.1, we implemented Algorithm 3 using SageMath. We use the same setting and the sequence of Fibonacci polynomials as an example.

[1]:
```
q=9
F.<a> = GF(q)
A.<T> = F[]
B.<X> = Frac(A)[]
```

The next program is a preliminary to the implementation of Algorithm 3. Indeed, SageMath does not have a built-in function for square roots in geometric extensions of the rational function field K. With Δ, x, $y \in K$ as inputs, the **sq_root** function returns a pair $u, v \in K$ such that $u + v\sqrt{\Delta}$ is a square root of $x + y\sqrt{\Delta}$ in L.

[2]:
```
def sq_root(Delta,x,y):
    N = x^2 - y^2*Delta

    if not N.is_square():
        return False

    n = N.sqrt()
    u = (x+n)/2
    v = (x-n)/2

    for z in [u,v]:
        if not z.is_square():
            continue
        a = z.sqrt()
```

```
        X = (x-n)/(2*Delta) if z==u else (x+n)/(2*Delta)
        if X.is_square():
            return [a, X.sqrt()]

    return False

sq_root(T^2+4, -(T^2+2)/2, -T/2)
```

[2]: `[(a + 1)*T, a + 1]`

In the above example, we computed a square root of γ for the sequence $U(T,-1)$ of Fibonacci polynomials. We have $\Delta = T^2+4$ and $\gamma = (ia)^2$, where $i^2 = -1$ and

$$a = \frac{T+\sqrt{\Delta}}{2} = 2T + 2\sqrt{\Delta}.$$

The letter `a` in the program is a primitive element of the extension $\mathbb{F}_9/\mathbb{F}_3$. In our case, it satisfies $\mathtt{a}^2 = \mathtt{a}+1$. One can easily check that $2i = \mathtt{a}+1$.

The final program of the section, **Q_boolean**, is an implementation of Algorithm 3, using **sq_root** to compute square roots. With inputs $a_1, a_2 \in A$ such that $\mathbf{b}(h) = 0$, the constant h, and e, it returns the values of $\mathcal{Q}$.

[3]:
```
def Q_boolean(a_1,a_2,h,e):
    v = valuation(h,2)
    Delta = a_1^2-4*a_2

    x = e*(a_1^2-2*a_2)/(2*a_2)
    y = e*a_1/(2*a_2)

    for n in range(1,v+1):
        r = sq_root(Delta,x,y)
        if r==False:
            r = sq_root(Delta,-x,-y)
        x = r[0]
        y = r[1]

    return (x^2-Delta*y^2+1)//2

Q_boolean(T,-1,2,1)
```

[3]: 1

In our example, we obtain $\mathcal{Q} = 1$. We can easily check this claim, since we know $h = 2$ and $\gamma^{1/2} = ia$. We have $\sigma_L(ia) = ib$, so that $\sigma_L(ia) \cdot ia = i^2 ab = -a_2 = 1$. Hence $\mathcal{Q} = 1$.

Chapter 5

The order problem in $\mathbb{Z}$

In this chapter, we study the order problem for Lucas sequences $U(a_1, a_2)$ with integer parameters $a_1, a_2 \in \mathbb{Z} \setminus \{0\}$. That is, can the density of prime numbers p whose rank of appearance $\rho_U(p)$ is divisible by a fixed integer $d \geq 1$ be found explicitly? We assume that U is non-degenerate, so that it makes sense to consider this problem. As mentioned in Chapter 3, this question has been study by many authors. There are two main results that stand out. One is a theorem of Wiertelak [40], that can be use to solve the reducible characteristic polynomial case. The second is a result of Sanna [30] that deals with the irreducible case under the assumption that d is odd and not divisible by 3 if $L := \mathbb{Q}(\sqrt{\Delta})$ has absolute discriminant $\Delta_L = -3$, where $\Delta = a_1^2 - 4a_2$.

The method used in Chapter 4 to compute densities, which consists in considering "good" booleans functions, can be applied to the number fields case. We are able to complete the work of Sanna for even integers d under the assumption that $\Delta_L \notin \{-4, -3\}$. The latter ensures that L is not a cyclotomic field, which comes with many problems regarding our methods. In the function field setting, the natural analogue is the constant field extension case discussed in Section 4.5. In fact, this is the only incomplete part of the irreducible characteristic polynomial case considered in this section, and also the only instance where roots of unity are adjoined to $\mathbb{F}_q(T)$.

Let $\mathcal{R}_\gamma(d)$ be the set of prime numbers whose rank of appearance in U is divisible by the integer $d \geq 1$, where $\gamma = a/b$ is the quotient of the roots of $X^2 - a_1X + a_2$, which we assume irreducible. Without loss of generality, we exclude the finitely many ramified primes $p \mid 2\Delta$. As seen at the beginning of Chapter 3 in the function field case, although many Lucas sequences share the same γ, their set $\mathcal{R}_\gamma(d)$ may differ by only finitely many primes. Therefore, for asymptotic density results, one can consider $\mathcal{R}_\gamma(d)$ for only one of these sequences. We denote by $\delta_\gamma(d)$ its natural density.

As in Chapter 4, we want to be able to switch between γ and $-\gamma$ at certain times. This will allow us to find density formulas in many more cases. Recall that $-\gamma$ can be

associated with the Lucas sequence $U(\Delta, -a_2\Delta)$ by Remark 2.10. Therefore, it makes sense to consider the set $\mathcal{R}_{-\gamma}(d)$ and to use $\delta_{-\gamma}(d)$ in the following theorem, which is an analogue of Theorem 4.1:

Theorem 5.1. *For every $d \geq 2$, we have*

$$\delta_\gamma(d) = \begin{cases} \delta_{-\gamma}(2d) + \delta_{-\gamma}(d/2) - \delta_{-\gamma}(d), & \text{if } 2\|d; \\ \delta_{-\gamma}(d), & \text{otherwise.} \end{cases}$$

Proof. The proof is the same as the proof of Theorem 4.1 in the function field case. □

In the first section, we prove various preliminary results on cyclotomic and Kummer extensions. Most notably, we study the existence of certain automorphisms in the Galois group of $L_{n,d} = L(\zeta_n, \gamma^{1/d})$ over $\mathbb{Q}$, and we compute the degree of $L_{n,d}/\mathbb{Q}$. Another important result is Lemma 5.8, an analogue of Lemma 4.5, that computes a closed-form formula for some special series.

In the second section, we briefly explain how the results of Sanna can be restated to prove the existence of $\delta_\gamma(d)$, the asymptotic density of $\mathcal{R}_\gamma(d)$.

We prove closed-form formulas for $\delta_\gamma(d)$ in the third section. Our formulas are written as linear combinations of the special series studied in Section 5.1.

In a final section, we display our algorithms and their SageMath [35] implementation. They are used to compute various boolean functions and field discriminants that appear in the density formulas.

5.1 Preliminary results

We study Kummer extensions $L_{n,d} = L(\zeta_n, \gamma^{1/d})$ of L, where $d, n \geq 1$, $d \mid n$, are integers, ζ_n is a primitive n-th root of unity, and $\Delta_L \notin \{-4, -3\}$. We start with a result on the behaviour of d-th powers in cyclotomic extensions of L. This generalises [30, Lemma 4.4] and is an analogue of [31, Lemma 4.8].

Lemma 5.2. *Let $\gamma \in L$ and $d \mid n$ be positive integers. Then, we have $\gamma \in L(\zeta_n)^d$ if and only if either $\gamma \in (L^\times)^d$ and d is odd, or $\gamma = \pm\delta^{d/2}$ for some $\delta \in L \cap (L(\zeta_n)^\times)^2$ and d is even.*

Proof. One way is trivial. Thus, we assume $\gamma = b^d$ for some $b \in L(\zeta_n)$. If $a = \gamma^{n/d} = b^n$, then $L(\zeta_n, a^{1/n}) = L(\zeta_n)$ is an abelian extension of L. By [14, Theorem 3.2, Chapter 8], we have $a_1^m = c^n$ for some $c \in L$, where $m = 1$, if $2 \nmid n$, and $m = 2$, otherwise. If $2 \nmid n$, then $\gamma^n = a^d = c^{dn}$ implies that $\gamma = \zeta_n c^d = c^d$ because the only n-th root of unity in L, which as discriminant $\Delta_L \notin \{-4, -3\}$, is $\zeta_n = 1$.

If $2 \mid n$, then $a^2 = c^n$. It follows that $a = \pm c^{n/2}$ and $\gamma^n = a^d = (\pm 1)^d c^{dn/2}$. We are done if $2 \mid d$, since we have

$$\gamma^n = c^{dn/2} \quad \text{and} \quad \gamma = \zeta_n^k c^{d/2} = \pm c^{d/2},$$

for some $k \in \mathbb{Z}$. If $2 \nmid d$, then $\gamma^n = \epsilon c^{dn/2}$ for some $\epsilon \in \{\pm 1\}$. We now have two cases. First, if $\epsilon = -1$, then we must have $v_2(n) = 1$, since -1 is not a square in L. Hence $dn/2$ is odd and $\gamma^n = (-c)^{dn/2}$. Moreover, $-c$ must be a square because $2 \mid n$. Therefore, there exists $k \in \mathbb{Z}$ and $x \in L$ such that

$$\gamma^n = (-c)^{dn/2} = x^{dn} \quad \text{and} \quad \gamma = \zeta_n^k x^d = \pm x^d = (\pm x)^d.$$

Lastly, if $\epsilon = 1$, we put $n' = n/(n, 2^\infty)$, so that $\gamma^{2n'} = \pm c^{n'd} = (\pm c)^{n'd}$ by the method of the above. Put $y = \pm c$. Then, we see that y must be a square in L because γ is raised to an even power, while $n'd$ is odd. It follows that $\gamma^{2n'} = x^{2n'd}$, and thus $\gamma = \pm x^d = (\pm x)^d$ for some $x \in L$. □

From now on, we consider $\gamma = a/b$ the quotient of the roots of $X^2 - a_1 X + a_2$, which we recall is irreducible.

Definition 5.3. *For all $u \in \{\pm 1\}$, we define $h(u)$ to be the largest integer $t \geq 1$ such that $u\gamma \in (L^\times)^t$. We call $h := \max(h(-1), h(1))$.*

We assume $h = h(1)$ throughout the rest of this section. When $h = h(-1)$, the results hold for $-\gamma$ instead. This will be helpful in Section 5.3. Note that $h(1)$ and $h(-1)$ may differ only by their 2-adic valuation. Also, if one of them is even, then the other must be odd. This is because -1 is not a square in L. Therefore, a necessary and sufficient condition for $h(1) > h(-1)$ to hold is that $\gamma \in (L^\times)^2$. We write $\gamma = \gamma_0^h$, where $\gamma_0 \in L$, and let $d_0 = d/(d, h)$ and $h_0 = h/(d, h)$.

Theorem 5.4. *The minimal polynomial of $\gamma^{1/d}$ over $L(\zeta_n)$ is*

(1) $X^{d_0} - \gamma_0^{h_0}$, if $2 \nmid d_0$ or $\gamma_0^{h_0} \notin (L(\zeta_n)^\times)^2$; or

(2) $X^{d_0/2} - \gamma_0^{h_0/2}$, otherwise.

Proof. Call $f(X)$ the minimal polynomial of $\gamma^{1/d}$. In both cases, we have $f(\gamma^{1/d}) = 0$, so that it suffices to show the irreducibility of f.

Assume $2 \nmid d_0$ or $\gamma_0^{h_0} \notin (L(\zeta_n)^\times)^2$. Let $l \mid d_0$ be an odd prime. By Lemma 5.2, we see that $\gamma_0^{h_0} \in (L(\zeta_n)^\times)^l$ if and only if $\gamma_0^{h_0} \in (L^\times)^l$. By the maximality of h, we have $l \mid h_0$, which contradicts $(d_0, h_0) = 1$. We are done if $2 \nmid d_0$ by Theorem 3.4. Next, assume $2 \mid d_0$ and $\gamma_0^{h_0}$ is not a square in $L(\zeta_n)$. By Theorem 3.4 again, it suffices to show that $\gamma_0^{h_0}$ is not

of the form $-4x^4$ for some $x \in L(\zeta_n)$ when $4 \mid d_0$. This is equivalent to $-\gamma_0^{h_0}/4 = \pm y^2$ for some $y \in L$, by Lemma 5.2. Hence

$$\gamma = \epsilon \cdot (2y)^{2(d,h)}, \quad \epsilon \in \{\pm 1\}.$$

If $\epsilon = 1$, then $2 \mid h_0$ and we have a contradiction to $(d_0, h_0) = 1$. If $\epsilon = -1$, then $-\gamma$ is a square. However, we saw that this is a sufficient condition to have $h(-1) > h(1)$. This is not possible since we assumed $h = h(1)$. Hence $\gamma_0^{h_0}$ is not of the form $-4x^4$ and $f(X)$ is irreducible by Theorem 3.4.

Assume $2 \mid d_0$ and $\gamma_0^{h_0} = z^2$, for some $z \in L(\zeta_n) \setminus L$. If $z = x^l$, where $x \in L(\zeta_n)$ and $l \mid d_0$ is an odd prime, then $\gamma_0^{h_0} \in L \cap (L(\zeta_n)^\times)^l$. By Lemma 5.2 and the same reasoning as the previous case, we show that this contradicts $(d_0, h_0) = 1$. Next, note that if $4 \mid d_0$ and $z = -4y^4$ in $L(\zeta_n)$, then $z = (2iy)^2$ because $4 \mid n$. Therefore, showing that z can not be a square is sufficient to prove the irreducibility of $f(X)$. By contradiction, if z is a square, then $\gamma_0^{h_0}$ is a 4-th power in $L(\zeta_n)$, which is equivalent to $\gamma_0^{h_0} = \pm\delta^2$, $\delta \in L$, by Lemma 5.2. We saw that this either contradicts $(d_0, h_0) = 1$, or $h = h(1)$. □

Lemma 5.5. *We have $\gamma_0^{h_0} \in (L(\zeta_n)^\times)^2$ if and only if $\gamma^{1/h_1} \in (L(\zeta_n)^\times)^2$.*

Proof. One way is trivial. Thus, assume that $\gamma^{1/h_1} = x^2$ for some $x \in L(\zeta_n)$. Moreover, we can write it as $x^2 = (\gamma_0^{h_0})^{(d,h')}$, where $h' = h/(h, 2^\infty)$. Then, there exists $u, v \in \mathbb{Z}$ such that $2u + (d, h')v = 1$ and

$$x^{2v} = (\gamma_0^{h_0})^{1-2u} = \gamma_0^{h_0} \cdot (\gamma_0^{h_0 u})^{-2}.$$

It follows that $\gamma_0^{h_0} = (x^v \gamma_0^{h_0 u})^2$. □

We now have all the tools to prove two results on Kummer extensions. We first find an explicit formula for the degree of $L_{n,d}/\mathbb{Q}$. Then, we give necessary and sufficient conditions for the existence of a $\sigma \in Gal(L_{n,d}/\mathbb{Q})$ such that $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$, $\sigma(\zeta_n) = \zeta_n^{-1}$ and $\sigma(\gamma^{1/d}) = \gamma^{-1/d}$. As in Chapter 3, this automorphism is used to compute the density of primes in $\mathcal{R}_\gamma(d)$ that are inert in L.

Theorem 5.6. *We have*

$$[L_{n,d} : \mathbb{Q}] = \frac{d\varphi(n)}{(d,h)} \cdot \begin{cases} \frac{1}{2}, & \text{if } \Delta_L \mid n,\ 2h_1 \mid d, \text{ and } \gamma^{1/2h_1} \in L(\zeta_n); \\ 2, & \text{if } \Delta_L \nmid n, \text{ and } 2h_1 \nmid d \text{ or } \gamma^{1/2h_1} \notin L(\zeta_n); \\ 1, & \text{otherwise.} \end{cases}$$

Proof. By [30, Lemma 4.5], we know that $[L(\zeta_n) : \mathbb{Q}] = \varphi(n) \cdot 2^{[\Delta_L \nmid n]}$. By Theorem 5.4

and Lemma 5.5, we see that

$$[L_{n,d} : L(\zeta_n)] = \frac{d}{(d,h)} \cdot \begin{cases} \frac{1}{2}, & \text{if } 2 \mid d_0 \text{ and } \gamma^{1/2h_1} \in L(\zeta_n); \\ 1, & \text{otherwise,} \end{cases}$$

where $d_0 = d/(d,h)$. The result is obtained using the multiplicativity of the degree and that $2 \mid d_0$ if and only if $2h_1 \mid d$. □

Theorem 5.7. *Let σ be an automorphism satisfying*

$$\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}, \quad \sigma(\zeta_n) = \zeta_n^{-1}, \quad \textit{and} \quad \sigma(\gamma^{1/d}) = \gamma^{-1/d}.$$

If $2h_1 \nmid d$ or $\gamma^{1/h_1} \notin (L(\zeta_n)^\times)^2$, then σ belongs to $Gal(L_{n,d}/\mathbb{Q})$ if and only if the two following conditions are satisfied:

(1) $\Delta < 0$ or $\Delta_L \nmid n$;

(2) $h_1 \nmid d$, or $h_1 \mid d$ and $N_{L/\mathbb{Q}}(\gamma^{1/h_1}) = 1$.

Otherwise, if $2h_1 \mid d$ and $\gamma^{1/h_1} \in (L(\zeta_n)^\times)^2$, then σ belongs to $Gal(L_{n,d}/\mathbb{Q})$ if and only if the two following conditions are satisfied:

(1) $\Delta < 0$ or $\Delta_L \nmid n$;

(2) $\sigma_0(\gamma^{1/2h_1}) = \gamma^{-1/2h_1}$,

where $\sigma_0 \in Gal(L(\zeta_n)/\mathbb{Q})$ satisfies $\sigma_0(\sqrt{\Delta}) = -\sqrt{\Delta}$ and $\sigma_0(\zeta_n) = \zeta_n^{-1}$.

Proof. The proof of [30, Lemma 4.2] shows that σ_0 exists if and only if $\Delta < 0$ or $\Delta_L \nmid n$. Since $\sigma|_{L(\zeta_n)} = \sigma_0$, it suffices to find necessary and sufficient conditions for σ_0 to be extended into σ. Let $\mu(X)$ be the minimal polynomial of $\gamma^{1/d}$ over $L(\zeta_n)$, which is given by Theorem 5.4.

First, we assume $2 \nmid d_0$ or $\gamma_0^{h_0/2} \notin L(\zeta_n)$. Hence $\mu(X) = X^{d_0} - \gamma_0^{h_0}$ by Theorem 5.4. Since $L_{n,d} \cong L(\zeta_n)[X]/(\mu(X))$, we can extend σ_0 in exactly d_0 ways by sending a root of μ to any root of $\sigma_0\mu$. Therefore, we need $\sigma_0\mu$ to annihilate $\gamma^{-1/d}$, or equivalently

$$(\sigma_0\mu)(X) = X^{d_0} - \sigma_0(\gamma_0^{h_0}) = X^{d_0} - \gamma_0^{-h_0}.$$

This happens if and only if $\sigma_0(\gamma_0^{h_0}) = \gamma_0^{-h_0}$. If $h_1 \nmid d$, then $\gamma_0^{h_0}$ is a square in L. Moreover, because $\sigma_L(\gamma) = \gamma^{-1}$, we have $\sigma_L(\gamma_0^{h_0/2}) = \pm\gamma_0^{-h_0/2}$. Hence $\sigma_0(\gamma_0^{h_0}) = \gamma_0^{-h_0}$ holds by squaring both sides. Thus, the equality $\sigma_0(\gamma_0^{h_0}) = \gamma_0^{-h_0}$ may not hold only if $h_1 \mid d$. In that case, we have $\sigma_0(\gamma_0^{h_0}) = \gamma_0^{-h_0}$ holds if and only if $\sigma_0(\gamma^{1/h_1}) = \gamma^{-1/h_1}$ does.

Next, assume $2 \mid d_0$ and $\gamma_0^{h_0/2} \in L(\zeta_n)$, so that $\mu(X) = X^{d_0/2} - \gamma_0^{h_0/2}$. By the same method as the previous case, we can extend σ_0 if and only if the equality $\sigma_0(\gamma_0^{h_0/2}) = \gamma_0^{-h_0/2}$ holds. Clearly, it implies that $\sigma_0(\gamma^{1/2h_1}) = \gamma^{-1/2h_1}$. For the converse, taking the (d, h')-th root on both sides, where $h' = h/(h, 2^\infty)$, we obtain

$$\sigma_0(\gamma^{1/2h_1(d,h')}) = \sigma_0(\gamma_0^{h_0/2}) = \zeta_{(d,h')}^k \gamma_0^{-h_0/2},$$

for some $k \in \mathbb{Z}$. Squaring both sides, we obtain $\sigma_L(\gamma_0^{h_0}) = \zeta_{(d,h')}^{2k} \gamma_0^{-h_0}$, which holds in L. Hence $\zeta_{(d,h')}^{2k} = 1$ and, because $2 \nmid (d, h')$, we have $\zeta_{(d,h')}^k = 1$ as well. The result follows using Lemma 5.5 on the condition $\gamma_0^{h_0} \in (L(\zeta_n)^\times)^2$. □

This last lemma is an analogue of Lemma 4.5. It generalises a formula given in the proof of [30, Lemma 5.4].

Lemma 5.8. *Let $d, e, h \geq 1$ and $\nu \geq 0$ be integers with $2 \mid d$. Then, we have*

$$\sum_{\substack{v \mid d^\infty \\ e \mid v}} \sum_{u \mid d} \frac{\mu(u)(uv, h)[2^\nu \mid uv]}{\varphi(dv)uv} = \frac{(h, d^\infty)\epsilon(d, e, \nu)}{d[(h, d^\infty), e, 2^\nu]^2} \cdot \prod_{p \mid d} \left(\frac{p^2}{p^2 - 1} \right), \tag{5.1}$$

where $\epsilon(d, e, \nu) = 0$ if $e \nmid d^\infty$, and

$$\epsilon(d, e, \nu) = 1 - \frac{3(h, 2^\infty)}{(h, 2^\nu)} \cdot [e \mid d^\infty \text{ and } 2^\nu \nmid e]$$

For the rest of this chapter, we write $S_{d,e,h}(\nu)$ for the double sum in equation (5.1) and $S_{d,e,h} = S_{d,e,h}(0)$ as a shorthand.

Proof. For $\nu = 0$, see the proof of [30, Lemma 5.4]. Assuming $\nu \geq 1$, we have

$$S_{d,e,h}(\nu) = S_{d,[e,2^\nu],h}(0) + {\sum_{v \mid d^\infty}}' \sum_{u \mid d} \frac{\mu(u)(uv, h)}{\varphi(dv)uv} \cdot [2^\nu \mid uv],$$

where $\sum'$ means that indices have 2-adic valuation equal to $\nu - 1$ and are divisible by e. The double sum is zero if $2^\nu \mid e$. Otherwise, note that $[2^\nu \mid uv] = [2 \mid u]$ and that $e \mid v$ if and only if $e' = e/(e, 2^\infty)$ divides v. Calling S the double sum, we obtain

$$S = \sum_{\substack{v \mid d'^\infty \\ e' \mid v}} \sum_{u \mid d'} \frac{-\mu(u)(2^\nu uv, h)}{4^{\nu-1}\varphi(dv)uv} = \frac{-(2^\nu, h)}{4^{\nu-1}} \cdot \frac{S_{d',e',h}(0)}{2^{v_2(d)}},$$

where we used that $\varphi(dv) = 2^{v_2(d)-1}\varphi(d'v)$. By the case $\nu = 0$, we obtain $S = 0$ if $e' \nmid d^\infty$,

and otherwise, we have

$$S = \frac{-(2^\nu, h)}{4^{\nu-1}} \cdot \frac{(h, d'^\infty)}{2^{v_2(d)} d'[(h, d'^\infty), e']^2} \cdot \prod_{p|d'} \left(\frac{p^2}{p^2-1}\right)$$
$$= \frac{-3 \cdot (2^\nu, h)}{4^\nu d} \cdot \frac{(h, d'^\infty)}{[(h, d'^\infty), e']^2} \cdot \prod_{p|d} \left(\frac{p^2}{p^2-1}\right).$$

Next, we use the identity $[(h, d'^\infty), e'] = [(h, d^\infty), e, 2^\nu](h, 2^\nu)/(h, 2^\infty)2^\nu$, which holds because $2^\nu \nmid e$ implies that $[e, 2^\nu] = 2^\nu e'$. Hence

$$S = \frac{-3(h, 2^\infty)(h, d^\infty)}{(h, 2^\nu)[(h, d^\infty), e, 2^\nu]^2} \cdot \prod_{p|d} \left(\frac{p^2}{p^2-1}\right),$$

and the result follows by expanding $S_{d,[e,2^\nu],h}(0)$. □

5.2 Existence of the density

In the statement of [30, Theorem 1.1], Sanna assumes d is odd and not divisible by 3 if $L = \mathbb{Q}(\sqrt{\Delta})$ has discriminant $\Delta_L = -3$. However, these restrictions are not used in the proofs of the existence of the density or of the upper bound. Indeed, [30, Lemma 5.1] is stated without them, and while they appear in the statement of [30, Lemma 5.3], the proof does not invoke them. The proof of the main theorem only relies on these lemmas and [30, Lemmas 5.2 and 5.4]. It is in the latter that the assumption on d is required to compute a closed-form formula of the density.

Let $x > 1$, and denote by $\mathcal{R}_\gamma(d, x)$ the number of primes $p \in \mathcal{R}_\gamma(d)$ with $p \leq x$. By modifying the proof [30, Lemma 5.2], Sanna's theorem can be restated in the following form, with no assumption on L, nor on d, and under our notation:

Theorem 5.9. *Let d be an integer. There exists an absolute constant $B > 0$, such that for every $x > \exp(Bd^{40})$, we have*

$$\mathcal{R}_\gamma(d; x) = \delta_\gamma(d)\mathrm{Li}(x) + \mathcal{O}_\gamma\left(\frac{d}{\varphi(d)} \cdot \frac{x(\log\log x)^{\omega(d)}}{(\log x)^{9/8}}\right),$$

where

$$\delta_\gamma(d) = \sum_{v|d^\infty} \sum_{u|d} \frac{\mu(u)(1 + [\sigma_{u,v} \text{ exists}])}{[L_{dv,uv} : \mathbb{Q}]},$$

and $\sigma_{u,v}$ satisfies $\sigma_{u,v}(\sqrt{\Delta}) = -\sqrt{\Delta}$, $\sigma_{u,v}(\zeta_{dv}) = \zeta_{dv}^{-1}$, and $\sigma_{u,v}(\gamma^{1/uv}) = \gamma^{-1/uv}$, if it exists in $Gal(L_{dv,uv}/\mathbb{Q})$.

Proof. As mentioned above, it suffices to follow the proof of [30, Theoreom 1.1]. We deal with a few technicalities that may change only the proof of [30, Lemma 5.2]. We apply the Chebotarev density theorem, [30, Theorem 3.5] to

$$\pi_{\gamma,dv,uv}(x) := \#\left\{p \le x : p \nmid 2\Delta a_2,\ p \equiv \left(\frac{\Delta}{p}\right) \pmod{n} \text{ and } d \mid \iota_U(p)\right\},$$

where $\iota_U(p)$ satisfies $\rho_U(p) \cdot \iota_U(p) = p - (\Delta/p)$. By [30, Lemma 4.2], we have

$$\pi_{\gamma,dv,uv}(x) = \pi_{L_{dv,uv}/\mathbb{Q},C}(x),$$

where $\pi_{L_{dv,uv}/\mathbb{Q},C}(x)$ counts the number of primes $p \le x$ unramified in $L_{dv,uv}$ and whose Artin symbol is contained in C, a union of conjugacy classes of the Galois group. Therefore, we can apply [30, Theorem 3.5] with $E = L_{dv,uv}$, $F = \mathbb{Q}$, and $C = \{\mathrm{id}\}$ if $\sigma_{u,v}$ does not exists, or $C = \{\mathrm{id}, \sigma_{u,v}\}$ otherwise. Let $n_{u,v} = [L_{dv,uv} : \mathbb{Q}]$ and $\Delta_{u,v}$ be the absolute discriminant of $L_{dv,uv}$. We obtain

$$\pi_{\gamma,dv,uv}(x) = \frac{1 + [\sigma_{u,v} \text{ exists}]}{n_{u,v}} \cdot \mathrm{Li}(x) + \mathcal{O}\left(2x \exp\left(-c_1\sqrt{\log(x)/n_{u,v}}\right)\right),$$

for every $x \ge \exp(c_2 \max(n_{u,v}(\log|\Delta_{u,v}|)^2, |\Delta_{u,v}|^{1/n_{u,v}}/n_{u,v}))$, where $c_1, c_2 > 0$ are absolute constants. To find the same result as in [30, Lemma 5.2], we make sure the bounds

$$|\Delta_{u,v}|^{1/n_{u,v}} \ll_U n^3 \quad \text{and} \quad \log|\Delta_{u,v}| \ll_U n^2 \log(n+1),$$

given in [30, Lemma 4.5], hold in the general case. The second is a consequence of first, so we may only prove that $|\Delta_{u,v}|^{1/n_{u,v}} \ll_U n^3$. The only change we have to make in Sanna's proof is in the computation of the norm

$$N_{L(\zeta_{dv})/\mathbb{Q}}(\Delta_{L_{dv,uv}/L(\zeta_{dv})}).$$

Without knowing the minimal polynomial of $\gamma^{1/uv}$ over $L(\zeta_{dv})$, we use the existence of an integer $s \ge 1$ such that $s\gamma \in \mathcal{O}_L$, so that

$$L_{dv,uv} = L(\zeta_{dv}, \gamma^{1/uv}) = L(\zeta_{dv}, (s^{uv}\gamma)^{1/uv}).$$

Then, by [7, Lemma 5], we find that $\Delta_{L_{dv,uv}/L(\zeta_{dv})}$ divides

$$(uv)^{uv-1} N_{L(\zeta_{dv})/\mathbb{Q}}(s^{uv}\gamma) = (uv)^{uv-1} N_{L/\mathbb{Q}}(s^{uv}\gamma) = (uv)^{uv-1} s^{2uv},$$

so that $\Delta_{L_{dv,uv}/L(\zeta_{dv})} \mid (sn)^\infty$. It follows that $N_{L(\zeta_{dv})/\mathbb{Q}}(\Delta_{L_{dv,uv}/L(\zeta_{dv})}) \mid (sn)^\infty$ as well.

From this, the rest of the proof can proceed as that of Sanna. □

5.3 Closed-form formulas

Assume $\Delta_L \notin \{-4, 3\}$ and $2 \mid d$. We prove a closed-form formula for the density of $\mathcal{R}_\gamma(d)$, which is given in Theorem 5.9 by

$$\delta_\gamma(d) = \sum_{v \mid d^\infty} \sum_{u \mid d} \frac{\mu(u)(1 + [\sigma_{u,v} \text{ exists}])}{[L_{dv,uv} : \mathbb{Q}]},$$

Similar to Chapters 3 and 4, we separate $\delta_\gamma(d)$ into $\delta_\gamma^+(d)$ and $\delta_\gamma^-(d)$ in accordance to the sum $1 + [\sigma_{u,v} \text{ exists}]$. We have

$$\delta_\gamma^+(d) = \sum_{v \mid d^\infty} \sum_{u \mid d} \frac{\mu(u)}{[L_{dv,uv} : \mathbb{Q}]} \quad \text{and} \quad \delta_\gamma^-(d) = \sum_{v \mid d^\infty} \sum_{u \mid d} \frac{\mu(u)[\sigma_{u,v} \text{ exists}]}{[L_{dv,uv} : \mathbb{Q}]}.$$

Note that $\delta_\gamma^+(d)$ corresponds to the density of $\mathcal{R}_\gamma^+(d)$, the set of primes p whose rank is divisible by d and with Legendre symbol $(\Delta/p) = 1$. For $\delta_\gamma^-(d)$, we have $(\Delta/p) = -1$ and we denote by $\mathcal{R}_\gamma^-(d)$ the corresponding set.

Now, let $\mathcal{Q} = [N_{L/\mathbb{Q}}(\gamma^{1/h_1}) = 1]$. We deal with the two cases $\mathcal{Q} = 0$ and $\mathcal{Q} = 1$ separately. In the $\mathcal{Q} = 0$ case, we are able to find a closed-form formula for $\delta_\gamma(d)$ without much trouble. However, when $\mathcal{Q} = 1$, calculations are much more dense.

5.3.1 The case $\mathcal{Q} = 0$

Assume that $\mathcal{Q} = 0$. We prove a closed-form formula for $\delta_\gamma^+(d)$ and $\delta_\gamma^-(d)$. Note that our assumption implies that $2 \mid h$ and $\Delta > 0$. Indeed, since $\mathcal{Q} = 0$ and $N_{L/\mathbb{Q}}(\gamma) = 1$, we must have $h_1 \geq 2$. Moreover, if $\gamma^{1/h_1} = u + v\sqrt{\Delta}$ for some $u, v \in \mathbb{Q}^\times$, then $\mathcal{Q} = 0$ implies that the norm of γ^{1/h_1} is equal to $u^2 - v^2\Delta = -1$. Hence $\Delta > 0$. These two facts are used to find the closed-form of $\delta_\gamma^-(d)$.

Theorem 5.10. *Assume $\mathcal{Q} = 0$ and let $e = \Delta_L/(d, \Delta_L)$. Then, we have*

$$\delta_\gamma^+(d) = \frac{1}{2d}\left(\frac{1}{(h, d^\infty)} + [e \mid d^\infty] \cdot \frac{(h, d^\infty)}{[(h, d^\infty), e]^2}\right) \prod_{p \mid d} \left(\frac{p^2}{p^2 - 1}\right).$$

Proof. Note that $\mathcal{Q} = 0$ implies that $N_{L/\mathbb{Q}}(\gamma^{1/h_1}) = -1$. Therefore, γ^{1/h_1} is not a square in $L(\zeta_n)$ because of Lemma [31, Lemma 4.6]. By Theorem 5.6, we obtain

$$[L_{dv,uv} : \mathbb{Q}] = \frac{\varphi(dv)uv}{(uv, h)} \cdot 2^{[\Delta_L \nmid dv]}. \tag{5.2}$$

Hence, using $\Delta_L \mid dv$ if and only if $e \mid v$, we have

$$\delta_\gamma^+(d) = \sum_{v \mid d^\infty} \sum_{u \mid d} \frac{\mu(u)(uv,h)}{\varphi(dv)uv} \cdot \frac{1}{2^{[e\nmid v]}} = \frac{S_{d,1,h} + S_{d,e,h}}{2},$$

Note that we used the identity $2^{-[e\nmid v]} = (1 + [e \mid v])/2$ in the last equality. The result follows by Lemma 5.8. □

Example 5.11. *Let $a_1 = 4$, $a_2 = 2$ and $d = 2$. We have $\Delta = \Delta_L = 8$, $e = 4$ and*

$$\gamma = \frac{a^2}{2} = \left(\frac{a}{\sqrt{2}}\right)^2 = \left(\frac{2+2\sqrt{2}}{\sqrt{2}}\right)^2 = (2+\sqrt{2})^2.$$

It follows that $\sigma_L(\gamma^{1/2}) = 2 - \sqrt{2} \neq \gamma^{-1/2}$. Hence $\mathcal{Q} = 0$ and $v_2(h) = 1$. Since $d = 2$, there is no need to know the full value of h. By Theorem 5.10, we obtain

$$\delta_\gamma^+(2) = \frac{1}{4} \cdot \left(\frac{1}{2} + \frac{1}{8}\right) \cdot \frac{4}{3} = \frac{5}{24} = 0.208\overline{3}.$$

Numerically, we computed $\mathcal{R}_\gamma^+(2, 10^6)/\pi(10^6) \approx 0.207482$, where π is the prime counting function, which matches the theoretical value.

Theorem 5.12. *Assume $\mathcal{Q} = 0$ and let $e = \Delta_L/(d, \Delta_L)$. Then, we have*

$$\delta_\gamma^-(d) = \frac{3}{2d}\left(\frac{1}{(h,d^\infty)} - [e \mid d^\infty \text{ and } h_1 \nmid e] \cdot \frac{(h,d^\infty)}{[(h,d^\infty),e]^2}\right) \prod_{p \mid d}\left(\frac{p^2}{p^2-1}\right).$$

Proof. Recall that $\mathcal{Q} = 0$ implies that $2 \mid h$ and $\Delta > 0$. By Theorem 5.7, we see that $\sigma_{u,v}$ exists if and only if $h_1 \nmid uv$ and $\Delta_L \nmid dv$. Therefore, using Theorem 5.6, we obtain

$$\delta_\gamma^-(d) = \sum_{v \mid d^\infty} \sum_{u \mid d} \frac{\mu(u)(uv,h)}{\varphi(dv)uv} \cdot \frac{[e \nmid v][h_1 \nmid uv]}{2^{[e\nmid v]}}.$$

We linearise $\delta_\gamma^-(d)$ using that

$$\frac{[e \nmid v][h_1 \nmid uv]}{2^{[e\nmid v]}} = \frac{1 - [h_1 \mid uv] - [e \mid v] + [e \mid v][h_1 \mid uv]}{2}.$$

With the notation of Lemma 5.8, we obtain

$$\delta_\gamma^-(d) = \frac{1}{2}\Big(S_{d,1,h} - S_{d,1,h}(\nu) - S_{d,e,h} + S_{d,e,h}(\nu)\Big),$$

where $\nu = v_2(h)$. By Lemma 5.8, and because $\nu = v_2(h)$, we see that $S_{d,1,h}(\nu) = -2S_{d,1,h}$.

Similarly, when $e \mid d^\infty$, we have $S_{d,e,h}(\nu) = \big(1 - 3 \cdot [h_1 \nmid e]\big) \cdot S_{d,e,h}$. Hence

$$\delta_\gamma^-(d) = \frac{3}{2}\bigg(S_{d,1,h} - [h_1 \nmid e] \cdot S_{d,e,h}\bigg),$$

and the result follows by expanding $S_{d,1,h}$ and $S_{d,e,h}$ into products with Lemma 5.8. □

Example 5.13. *We keep the same sequence as in Example 5.11 with $d = 2$ again. By Theorem 5.12, and because $h_1 = 2$ divides $e = 4$, we have*

$$\delta_\gamma^-(2) = \frac{3}{4} \cdot \left(\frac{1}{2} - 0\right) \cdot \frac{4}{3} = \frac{1}{2}.$$

Numerically, we have $\mathcal{R}_\gamma^-(2, 10^6)/\pi(10^6) \approx 0.500343$. This matches the value of $\delta_\gamma^-(2)$.

More numerical comparisons can be found in Appendix A.2 for various sequences. In particular, Table A.9 is dedicated to the sequence $U(4, 2)$ of Examples 5.11 and 5.13.

5.3.2 The case $\mathcal{Q} = 1$

From now on, we assume that $\mathcal{Q} = 1$. This makes calculations more difficult as we have to check whether γ^{1/h_1} is a square in $L(\zeta_n)$ in some cases. By [31, Lemma 4.6], we know that γ^{-1/h_1} is a square in $L(\zeta_n)$ if and only if one of $\sqrt{c}$ and $\sqrt{c/\Delta_L}$ belongs to $\mathbb{Q}(\zeta_n)$, where $c = (u-1)/2$ and $\gamma^{1/h_1} = u + v\sqrt{\Delta_L}$ for some $u, v \in \mathbb{Q}$.

For the rest of this chapter, we define $K_1 = \mathbb{Q}(\sqrt{c})$ and $K_2 = \mathbb{Q}(\sqrt{c/\Delta_L})$. Let us denote by Δ_1 and Δ_2 their respective absolute discriminants. Now, by [31, Lemma 4.1], we have $\gamma^{1/h_1} \in (L(\zeta_n)^\times)^2$ if and only if $\Delta_1 \mid n$ or $\Delta_2 \mid n$.

We prove that $\delta_\gamma^+(d)$ and $\delta_\gamma^-(d)$ can be written as linear combinations of sums $S_{d,e,h}(\nu)$, which are defined in Lemma 5.8 and have closed-form.

Theorem 5.14. *Assume $\mathcal{Q} = 1$. Let $\nu = v_2(h) + 1$ and*

$$e = \frac{|\Delta_L|}{(d, |\Delta_L|)} \quad \text{and} \quad e_i = \frac{|\Delta_i|}{(d, |\Delta_i|)},$$

for all $1 \le i \le 2$, and put $e_0 = 1$ and $e_3 = [e_1, e_2]$. Then, we have

$$\delta_\gamma^+(d) = \frac{1}{2}\sum_{i=0}^{3}(-1)^{[i=3]}\bigg(S_{d,e_i,h}(\nu^{[i>0]}) + S_{d,[e_i,e],h}(\nu^{[i>0]})\bigg).$$

Proof. First, let us define two booleans

$$\mathcal{P}_1(n, d) = [\Delta_L \mid n] \cdot [2h_1 \mid d] \cdot [\Delta_1 \mid n \text{ or } \Delta_2 \mid n],$$

and $\mathcal{P}_2(n,d) = [\Delta_L \nmid n] \cdot [2h_1 \nmid d \text{ or } \Delta_i \nmid n \text{ for all } 1 \le i \le 2]$. Then, using Theorem 5.6, we decompose $\delta_\gamma^+(d)$ in the following way:

$$\delta_\gamma^+(d) = S_{d,1,h} + S_1(d) - \frac{S_2(d)}{2},$$

where we have defined

$$S_i(d) = \sum_{v \mid d^\infty} \sum_{u \mid d} \frac{\mu(u)(uv,h)\mathcal{P}_i(dv,uv)}{\varphi(dv)uv}.$$

We compute S_1 and S_2 separately. Note that $e \mid v$ if and only if $\Delta_L \mid dv$, and the same holds for Δ_i and e_i. We use

$$\mathcal{P}_1(dv,uv) = [e \mid v] \cdot [2h_1 \mid uv] \cdot ([e_1 \mid v] + [e_2 \mid v] - [e_3 \mid v])$$

to write $S_1(d) = S_{d,[e,e_1],h}(\nu) + S_{d,[e,e_2],h}(\nu) - S_{d,[e,e_3],h}(\nu)$. Similarly, for $S_2(d)$, we use the following decomposition:

$$\mathcal{P}_2(dv,uv) = 1 - [e \mid v] - [2h_1 \mid uv][e_1 \mid v \text{ or } e_2 \mid v] + \mathcal{P}_1(dv,uv).$$

Using the latter and the same technique as for the computation of $S_1(d)$, we have

$$S_2(d) = S_{d,1,h} - S_{d,e,h} - \left(S_{d,e_1,h}(\nu) + S_{d,e_2,h}(\nu) - S_{d,e_3,h}(\nu)\right) + S_1(d),$$

Finally, going back to the density $\delta_\gamma^+(d)$, we obtain

$$\delta_\gamma^+(d) = \frac{1}{2}\left(S_{d,1,h} + S_{d,e,h} + S_1(d) + S_{d,e_1,h}(\nu) + S_{d,e_2,h}(\nu) - S_{d,e_3,h}(\nu)\right)$$

The result follows by expanding $S_1(d)$ and rearranging the terms. □

Example 5.15. *Let $a_1 = 5$, $a_2 = 1$ and $d = 4$. We have $\Delta = \Delta_L = e = 21$ and*

$$\gamma = \left(\frac{5+\sqrt{21}}{2}\right)^2.$$

Thus, $2 \mid h$. One can show that $\gamma^{1/2}$ is not a square in L, so that $h_1 = 2$. Since 2 is the only prime dividing d, there is no need to find the full value of h. We see that $\mathcal{Q} = 1$. Next, we have $c = (5/2-1)/2 = 3/4$, so that $K_1 = \mathbb{Q}(\sqrt{c}) = \mathbb{Q}(\sqrt{3})$ and $K_2 = \mathbb{Q}(\sqrt{7})$. Their discriminants are $\Delta_1 = 12$ and $\Delta_2 = 28$, and it follows that $e_1 = 3$ and $e_2 = 7$. By

Theorem 5.14 and Lemma 5.8, we have

$$\delta_\gamma^+(4) = \frac{S_{4,1,h}(0)}{2} = \frac{1}{12} \approx 0.08\bar{3}.$$

For comparison, we find $\mathcal{R}_\gamma^+(4, 10^6)/\pi(10^6) \approx 0.083467$ *in Table A.12.*

We now turn our attention to $\delta_\gamma^-(d)$. The automorphism defined in Theorem 5.7 exists if and only if $\Delta < 0$ or $\Delta_L \nmid n$, and

(1) $2h_1 \nmid d$ or $\gamma^{1/h_1} \notin (L(\zeta_n)^\times)^2$; or

(2) $2h_1 \mid d$, $\gamma^{1/h_1} \in (L(\zeta_n)^\times)^2$, and $\sigma_0(\gamma^{1/2h_1}) = \gamma^{-1/2h_1}$,

where $\sigma_0 \in Gal(L(\zeta_n)/L)$ is such that $\sigma_0(\sqrt{\Delta}) = -\sqrt{\Delta}$ and $\sigma_0(\zeta_n) = \zeta_n^{-1}$. However, we can make conditions (1) and (2) more precise, with less dependence on n. Indeed, recall that $\gamma^{1/h_1} \in (L(\zeta_n)^\times)^2$ if and only if there exists $1 \le i \le 2$ such that $\Delta_i \mid n$. It follows that the smallest cyclotomic fields containing $\gamma^{1/2h_1}$ are $\mathbb{Q}(\zeta_{|\Delta_1|})$ and $\mathbb{Q}(\zeta_{|\Delta_2|})$. With that in mind, we define $\sigma_i = \sigma_0|_{\mathbb{Q}(\zeta_{[\Delta_i|})}$ for all $1 \le i \le 2$. Conditions (1) and (2) become

(1) $2h_1 \nmid d$ or $\Delta_i \nmid n$ for all $1 \le i \le 2$;

(2) or $2h_1 \mid d$ and $\exists i \in \{1, 2\},\ \Delta_i \mid n$ and $\sigma_i(\gamma^{1/2h_1}) = \gamma^{-1/2h_1}$,

provided $\Delta < 0$ or $\Delta_L \nmid n$, so that the σ_i's exist. We define $\mathcal{Q}_i = [\sigma_i(\gamma^{1/2h_1}) = \gamma^{-1/2h_1}]$ for all $1 \le i \le 2$ when it is the case. Let us also define

$$\mathcal{P}_1(n, d) = [2h_1 \nmid d \text{ or } \forall i \in \{1, 2\},\ \Delta_i \nmid n], \tag{5.3}$$

which corresponds to condition (1), and

$$\mathcal{P}_2(n, d) = [2h_1 \mid d] \cdot [\exists i \in \{1, 2\},\ \Delta_i \mid n \text{ and } \mathcal{Q}_i = 1], \tag{5.4}$$

which corresponds to (2). Then, the expression $\big(\mathcal{P}_1(n, d) + \mathcal{P}_2(n, d)\big) \cdot [\Delta < 0 \text{ or } \Delta_L \nmid n]$ is equal to 1 if and only if σ exists. We now prove the final result of this section.

Theorem 5.16. *Assume* $\mathcal{Q} = 1$. *With the notation of Theorem 5.14, we have*

$$\delta_\gamma^-(d) = \frac{1}{2}\sum_{i=0}^{3}(-1)^{[3\nmid i]+\mathcal{Q}_i}\left(S_{d,e_i,h}(\nu^{[i>0]}) + (-1)^{[\Delta>0]}S_{d,[e_i,e],h}(\nu^{[i>0]})\right),$$

where $\mathcal{Q}_0 = 0$ *and* $\mathcal{Q}_3 = \mathcal{Q}_1\mathcal{Q}_2$.

Proof. By (5.3) and (5.4), we may write $\delta_\gamma^-(d) = S_1(d) + S_2(d)$, where

$$S_i(d) = \sum_{v|d^\infty}\sum_{u|d}\frac{\mu(u)\mathcal{P}_i(dv, uv)}{[L_{dv,uv} : \mathbb{Q}]} \cdot [\Delta < 0 \text{ or } \Delta_L \nmid dv],$$

for all $i \in \{1,2\}$. We start with $S_1(d)$. Assuming $\mathcal{P}_1(dv,uv)=1$, we have

$$\frac{1}{[L_{dv,uv}:\mathbb{Q}]} = \frac{(uv,h)}{\varphi(dv)uv}\cdot\left(\frac{1}{2}\right)^{[\Delta_L \nmid dv]} = \frac{(uv,h)}{2\varphi(dv)uv}\cdot\big(1+[e \mid v]\big),$$

by Theorem 5.6 and using that $\Delta_L \mid dv$ if and only if $e = |\Delta_L|/(d,|\Delta_L|)$ divides v. Replacing in $S_1(d)$, we obtain a general term of

$$\frac{\mu(u)(uv,h)}{2\varphi(dv)uv}\cdot\big(1+[e \mid v]\big)\cdot\mathcal{P}_1(dv,uv)\cdot[\Delta<0 \text{ or } e\nmid v]$$

First, note that $\big(1+[e \mid v]\big)\cdot[\Delta<0 \text{ or } e\nmid v] = 1+(-1)^{[\Delta>0]}[e \mid v]$. Next, we use the inclusion-exclusion principle to write

$$\begin{aligned}\mathcal{P}_1(dv,uv) &= 1-[2h_1 \mid uv \text{ and } \exists i\in\{1,2\},\ \Delta_i \mid dv]\\ &= \sum_{i=1}^{3}(-1)^{[3\nmid i]}\cdot[2h_1 \mid uv \text{ and } e_i \mid v].\end{aligned}$$

Expanding the product $\big(1+(-1)^{[\Delta>0]}[e \mid v]\big)\cdot\mathcal{P}_2(dv,uv)$ in $S_1(d)$, we obtain

$$S_1(d) = \frac{1}{2}\sum_{i=1}^{3}(-1)^{[3\nmid i]}\left(S_{d,e_i,h}(\nu^{[i>0]}) + (-1)^{[\Delta>0]}S_{d,[e_i,e],h}(\nu^{[i>0]})\right).$$

We now turn our attention to $S_2(d)$. Assuming $\mathcal{P}_1(dv,uv)$, we have

$$\frac{1}{[L_{dv,uv}:\mathbb{Q}]} = \frac{(uv,h)}{\varphi(dv)uv}\cdot\big(1+[e \mid v]\big),$$

by Theorem 5.6. Again, we use $\big(1+[e \mid v]\big)\cdot[\Delta<0 \text{ or } e\nmid v] = 1+(-1)^{[\Delta>0]}[e \mid v]$ and

$$\mathcal{P}_2(dv,uv) = \sum_{i=1}^{3}(-1)^{[3|i]}\mathcal{Q}_i\cdot[2h_1 \mid uv \text{ and } e_i \mid v],$$

to obtain

$$S_2(d) = \sum_{i=1}^{3}(-1)^{[3|i]}\mathcal{Q}_i\left(S_{d,e_i,h}(\nu^{[i>0]}) + (-1)^{[\Delta>0]}S_{d,[e_i,e],h}(\nu^{[i>0]})\right).$$

Finally, we add $S_2(d)$ to $S_1(d)$ and use the identity

$$\frac{(-1)^{[3\nmid i]}}{2} + (-1)^{[3|i]}\mathcal{Q}_i = \frac{(-1)^{[3\nmid i]+\mathcal{Q}_i}}{2}$$

on indices $i \in \{1,2,3\}$, which coincides with the case $i = 0$, to find the result. □

Example 5.17. *With the sequence of Example 5.15 and $d = 4$. None of e, e_1, or e_2 divide d^∞, so there is no need to compute $\mathcal{Q}_1$ and $\mathcal{Q}_2$. By Theorem 5.16 and Lemma 5.8, we have*

$$\delta_\gamma^-(4) = \frac{S_{4,1,h}(0)}{2} = \frac{1}{12} = 0.08\overline{3}.$$

Our computations in Table A.12 show that $\mathcal{R}_\gamma^-(4, 10^6)/\pi(10^6) \approx 0.083326$.

In conclusion, we proved four theorems that computes a closed-form formula of the density of $\mathcal{R}_\gamma(d)$ when d is even and $\Delta_L \notin \{-4, -3\}$. Together with Sanna's results, the only cases left to consider are $L = \mathbb{Q}(i)$ and $2 \mid d$, and $L = \mathbb{Q}(\zeta_3)$ and $(d, 6) > 1$.

5.4 Algorithms and SageMath computations

In this section, we provide an algorithm, as well as its implementation in SageMath 9.0 [35], that computes $\mathcal{Q}, \mathcal{Q}_1$ and $\mathcal{Q}_2$, and the discriminants Δ_1 and Δ_2, defined in Section 5.3.

In contrast to the previous chapter, we do not provide an algorithm to compute the constant h. However, we display below a SageMath program, called **h_constant**, that computes it. The method used in the program was kindly shared by Sanna in an e-mail communication with him. Thus, we would like to thank him.

We use that $\gamma = a^2/a_2$ is an S-unit, where S is the set of prime ideals $\mathfrak{p}$ in $\mathcal{O}_L$ that divide a_2. That is, γ belongs to the set

$$\mathcal{O}_{L,S}^\times = \{x \in L : v_\mathfrak{p}(x) = 0 \text{ for all } \mathfrak{p} \notin S\}.$$

By Dirichlet's S-unit theorem, [25, Corollary 11.7], we know that $\mathcal{O}_{L,S}^\times$ is a finitely generated abelian group. Let $e \in \{\pm 1\}$. We write $e\gamma$ as a product of generators of $\mathcal{O}_{L,S}^\times$, so that the gcd of the exponents is equal to $h(e)$. We easily check which of $h(1)$ and $h(-1)$ is maximal by checking whether a_2 is a square in L. This amounts to checking if one of a_2 and a_2/Δ is a square in $\mathbb{Q}$.

Given an input of $a_1, a_2 \in \mathbb{Z}$ such that L is not cyclotomic, **h_constant** returns $[h, e]$, where $e = -1$ if $2 \mid h$ and γ should be switched for $-\gamma$, and $e = 1$ otherwise.

[1]:
```
def h_constant(a_1,a_2):
    if (a_1^2-4*a_2).is_square(): return False

    s=1
    if is_square(-a_2) or is_square(-a_2/(a_1^2-4*a_2)): s=-1
```

```
    x = polygen(QQ)
    K.<a> = NumberField(x^2-a_1*x+a_2)

    S = K.ideal(a_2).prime_factors()
    S_unit_group = UnitGroup(K, S=tuple(S))

    g = a^2/(s*a_2)

    return [gcd(S_unit_group(g).exponents()),s]

h_constant(1,-1)
```

```
[1]: [2, -1]
```

With the Fibonacci sequence $U(1,-1)$ as an example, we see that $h = 2$ and $e = -1$ in our computation. This makes sense, as $\gamma = -\phi^2$ is not a square, while $-\gamma$ is, where ϕ is the golden ratio.

Algorithm 4 Computation of $\mathcal{Q}$, $\mathcal{Q}_1$, $\mathcal{Q}_2$, Δ_1 and Δ_2

Input: Non-zero integers $a_1, a_2 \in \mathbb{Z}$ such that L is not $\mathbb{Q}$, nor a cyclotomic field.

Output: The 3-tuple $(\mathcal{Q}, L_1, L_2)$, where $L_i = -1$ if $\mathcal{Q} = 0$, $L_i = [\mathcal{Q}_i, \Delta_i]$ if $\mathcal{Q} = 1$ and σ_i exists, and $L_i = [-1, \Delta_i]$ otherwise.

$h,\ e \leftarrow$ **h_constant**(a_1, a_2)
$r \leftarrow (e\gamma)^{1/h_1} \in L$
if $N_{L/\mathbb{Q}}(r) = -1$ **then**
    return $(0, -1, -1)$
Find $u, v \in \mathbb{Q}$ such that $r = u + v\sqrt{\Delta_L}$
$c \leftarrow (u-1)/2$
$K_1,\ K_2 \leftarrow \mathbb{Q}(\sqrt{c}),\ \mathbb{Q}(\sqrt{c/\Delta_L})$
$\Delta_1,\ \Delta_2 \leftarrow \mathrm{Disc}_{\mathbb{Q}}(K_1),\ \mathrm{Disc}_{\mathbb{Q}}(K_1)$
for $1 \leq i \leq 2$ **do**
    $L_i \leftarrow [0, \Delta_i]$
    if $\Delta > 0$ and $\Delta_L \nmid \Delta_i$ **then** ▷ Checks the existence of σ_i in $Gal(L(\zeta_{|\Delta_i|})/\mathbb{Q})$.
        $L_i \leftarrow [-1, \Delta_i]$
    else
        for $\sigma \in Gal(L(\zeta_{|\Delta_i|})/\mathbb{Q})$ **do**
            if $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$ and $\sigma(\zeta_{|\Delta_i|}) = \zeta_{|\Delta_i|}^{-1}$ and $\sigma_i(\gamma^{1/2h_1}) = \gamma^{-1/2h_1}$ **then**
                $L_i \leftarrow [1, \Delta_i]$
return $(1, L_1, L_2)$

We are now ready to implement Algorithm 4 in SageMath. First, notice how the automorphism σ_i that we look for in the Galois group of $L(\zeta_{|\Delta_i|})$ is an element of order two. Thus, instead of checking every elements of the Galois group, we only check those with order 2. To do so, we implemented **elements_of_order2** that takes an multiplicative abelian group G as an input, and returns the set of elements of order 2 in G.

[2]:
```
from itertools import product

def elements_of_order2(G):
    Id = G.identity()
    V = [(g,g.order()) for g in G.gens()]

    subgroups = []
    for g, n in V:
        if n%2==0:
            subgroups.append([Id,g**(n//2)])
```

```
        else:
            subgroups.append([Id])

    res = []
    for vect in product(*subgroups):
        h = Id
        for coord in vect:
            h*=coord
        if h!=Id:
            res.append(h)

    return res

G = AbelianGroup([4,6])

elements_of_order2(G)
```

[2]:
```
[f1^3, f0^2, f0^2*f1^3]
```

In our example, we define G the multiplicative abelian group isomorphic to $C_4 \times C_6$, where C_n is a multiplicative cyclic group of order $n \geq 1$. The elements `f0` and `f1` are the generators of G.

[3]:
```
def Q_booleans(a_1,a_2):
    Delta = a_1^2-4*a_2
    if Delta.is_square(): return False

    x = polygen(QQ)
    f = x^2-a_1*x+a_2
    K.<a> = NumberField(f)

    h, s = h_constant(a_1,a_2)
    r = a^2/(s*a_2)
    v = valuation(h,2)

    for n in range(1, v+1):
        if r.is_square(): r = r.sqrt()
        else: r = (-r).sqrt()
```

```
N = (r.norm()+1)/2
if N==0: return [0, -1, -1]

R = r.list()
c = (R[0]+R[1]*(a_1/2)-1)/2

Delta_L = squarefree_part(a_1^2-4*a_2)
if not Mod(Delta_L,4)==1: Delta_L = 4*Delta_L

roots = f.roots(QQbar, multiplicities=False)
a_in_QQbar = roots[0]

U = [squarefree_part(c), squarefree_part(c/Delta_L)]
res = [N]

for Delta_i in U:
    if not Mod(Delta_i,4)==1: Delta_i = 4*Delta_i

    if Delta>0 and Delta_i%abs(Delta_L)==0:
        res.append([-1, Delta_i])
    else:
        C = CyclotomicField(abs(Delta_i))
        M.<zeta> = K.composite_fields(C, preserve_embedding=True)[0]

        K_roots_in_M = f.roots(M, multiplicities=False)
        a_in_M = K_roots_in_M[0]
        b_in_M = K_roots_in_M[1]

        phi = C.polynomial()
        C_roots_in_M = phi.roots(M, multiplicities=False)
        zeta_in_M = C_roots_in_M[0]

        phi_K = K.hom([a_in_M], M)
        u = phi_K(r).sqrt()

        for tau in elements_of_order2(M.galois_group()):
```

```
                if tau(a_in_M)==b_in_M and tau(zeta_in_M)==zeta_in_M^(-1):
                    res.append([(u*tau(u)+1)/2, Delta_i])
                    break

    return res

Q_booleans(1,-1)
```

[3]: `[0, -1, -1]`

We see that **Q_booleans** returns $\mathcal{Q} = 0$ for the Fibonacci sequence. Indeed, recall that $\gamma = -\phi^2$ and $h = 2$. If we switch to $-\gamma$, we find

$$\sigma_L(\sqrt{-\gamma}) = \sigma_L(\phi) = 1 - \phi,$$

which is not equal to ϕ^{-1}. This matches the output.

Appendix

In the first two appendices, we provide numerical evidence of the closed-form formulas proved in Chapters 4 and 5. We display the SageMath [35] programs used for our computations, all are written using SageMath 9.0.

In Appendix A.3, we provides reference tables that summarise which of the main theorems of Chapter 4 apply in each case. They serve as guides to identify the appropriate closed-form formula for the density under the given conditions.

A.1 Numerical data in the function field case

In this section, we demonstrate Theorems 4.12 and the many theorems for the closed-form formula of $\delta_q^-(\gamma, d)$, through SageMath experimentations. We start by presenting the SageMath programs used. We first define the setting.

[1]:
```
q=9
F.<a> = GF(q)
A.<T> = F[]
```

With the **Lucas** program, we compute the n-th term of the Lucas sequence $U(a_1, a_2)$, where $a_1, a_2 \in A$, using the companion matrix method.

[2]:
```
def Lucas(a_1,a_2,n):
    if n<2: return n
    M = matrix([[0,1],[-a_2,a_1]])
    return (M^n)[0,1]
```

The next two programs are preliminaries to the main program. The first function, **irreducible_polynomials**, returns the Python generator that yields monic and irreducible polynomials of degree n over $\mathbb{F}_q$. The second, **num_irred_polynomials**, returns the number of such polynomials.

[3]:
```
def irreducible_polynomials(n):
    T_powers = [T^i for i in range(0,n)]

    irreds_1 = [T+i for i in F]
    if n==1:
        for p in irreds_1: yield p

    irreds_2 = [T^2+i for i in A.polynomials(max_degree=1) if (T^2+i).
↪is_irreducible()]

    if n==2:
        for p in irreds_2: yield p

    for coeffs in cartesian_product([F]*n):
        f = T^n
        for i in range(n):
            f+=coeffs[i]*T_powers[i]

        if any(f%g==0 for g in irreds_1+irreds_2):
            continue

        if f.is_irreducible():
            yield f

def num_irred_polynomials(n):
    return sum(moebius(d)*q^(n//d) for d in divisors(n))//n
```

The function **lucas_rank_mod** takes as an input two non-zero polynomials $a_1, a_2 \in A$ such that $U(a_1, a_2)$ is non-degenerate (see Lemma 2.2), a positive integer d, and a prime polynomial P. The program returns the boolean $[d \mid \rho_U(P)]$ and ϵ_P, where the latter was defined in Lemma 2.5.

[4]:
```
def lucas_rank_mod(a_1,a_2,d,p):
    p_degree = p.degree()
    Delta = a_1^2-4*a_2
    f = Mod(q,d).multiplicative_order()

    if Delta.mod(p)==0: return [False,0]
```

```
    if p_degree%f not in [0,f/2]: return [False,0]

    R = F['T'].quotient(p, 'x')
    x = R.gen()

    B.<y> = R[]

    epsilon_p = -1
    if F.characteristic()!=2:
        norm, var = R(1), R(Delta)
        for i in range(p_degree):
            norm*=var
            var = var**q
        if F(norm.lift())**((q-1)//2)==1: epsilon_p = 1
    elif not B(y^2-a_1*y+a_2).is_irreducible(): epsilon_p = 1

    N = q^p_degree - epsilon_p

    a_1_mod = R(a_1)
    a_2_mod = R(a_2)

    rank = 1
    for n in divisors(N):
        if Lucas(a_1_mod,a_2_mod,n)==0:
            rank = n
            break

    return [rank%d==0,epsilon_p]

lucas_rank_mod(T,-1,2,T+1)
```

[4]: [True, 1]

Here, using the Fibonacci polynomial $U(T,-1)$ as an example, we find that $P = T+1$ has rank $\rho_U(P)$ divisible by 2 and $\epsilon_P = 1$. The first 5 terms of the sequences are

$$0,\ 1,\ T,\ T^2+1,\ T^3-T.$$

We see that P divides $U_4 = T^3 - T$, but none of the preceding terms. Hence $\rho_U(P) = 4$. Now, since we are in odd characteristic, we have ϵ_P is equal to the Legendre symbol (Δ/P), where $\Delta = T^2 + 1$. We have

$$\left(\frac{\Delta}{P}\right) \equiv \Delta^{(NP-1)/2} \equiv (-1)^4 \equiv 1 \pmod{P},$$

so that $\epsilon_P = 1$. Therefore, we see that **lucas_rank_mod** returns the right values.

Our final program is called **d3_densities**. Given $a_1, a_2 \in A$ such that $U(a_1, a_2)$ is non-degenerate and integers $d, N \geq 1$, the function returns the values of

$$\frac{1}{N}\sum_{n=1}^{N} \frac{R_q^+(\gamma, d, n)}{q^n/n} \quad \text{and} \quad \frac{1}{N}\sum_{n=1}^{N} \frac{R_q^-(\gamma, d, n)}{q^n/n},$$

where γ is the quotient of the root of the characteristic polynomial of the Lucas sequence. Note that experimentations with **d3_densities** can be slow and tedious due to the exponential growth of the number of irreducible polynomials of degree n over $\mathbb{F}_q$,

[5]:
```
def d3_densities(a_1,a_2,d,N):
    if Mod(d,F.characteristic())==0: return 0

    res_plus = 0
    res_minus = 0

    L = [num_irred_polynomials(n) for n in range(1,N+1)]
    f = Mod(q,d).multiplicative_order()

    if Mod(f,2)==0 and (q^(f//2)+1)%d==0 and gcd(d,q-1)<3:
        f = f//2

    for n in range(f,N+1,f):
        nb = 0
        for l in irreducible_polynomials(n):
            u, v  = lucas_rank_mod(a_1,a_2,d,l)
            if v==1:
                res_plus+=u/L[n-1]
            else:
                res_minus+=u/L[n-1]
```

```
    return [res_plus*1./N, res_minus*1./N]

%time d3_densities(T,-1,2,4)
```

```
CPU times: user 23 s, sys: 35.5 ms, total: 23 s
Wall time: 23 s
```

```
[5]: [0.405478395061728, 0.000000000000000]
```

In the above example, we find some approximated values of $\delta_9^+(\gamma, 2)$ and $\delta_9^-(\gamma, 2)$ for the sequence of Fibonacci polynomials over $\mathbb{F}_9$. Since $a_2 = -1$ is a square in $\mathbb{F}_9$, we see that $\delta_9^-(2) = 0$ by Theorem 4.2, which matches the computation. Next, in Section 4.6, we saw that $h = 2$, γ is a square, and $\mathcal{Q} = 0$. Hence, we apply Theorem 4.12 and find

$$\delta_9^+(\gamma, 2) = \frac{5}{12} = 0.41\bar{6}.$$

This matches the computation as well.

In what follows, we use tables to compare the values of $\delta_q^+(\gamma, d)$ and $\delta_q^-(\gamma, d)$ with experimental values obtained via our SageMath computations. The numerical and experimental values respectively appear in the "num." and "exp." columns. Since the number of polynomials of degree n is asymptotically equivalent to q^n/n, we restrict ourselves to small values of q. For each q, we are able to go up to a certain degree N, which is indicated below the tables.

More information about the sequences tested can be found after their table. For instance, the value of h, $\mathbf{b}(h)$, and $\mathcal{Q}$. When it is needed, they are computed using the programs in Section 4.6.

d	$\delta_q^+(\gamma, d)$	num.	exp.	$\delta_q^-(\gamma, d)$	num.	exp.	$\delta_q(\gamma, d)$
2	5/12	0.416666	0.374341	1/4	0.251989	0.251989	2/3
4	1/3	0.333333	0.319328	0	0.000000	0.000000	1/3
6	11/64	0.171875	0.167273	3/32	0.093750	0.098611	17/64
21	77/1152	0.066840	0.063565	77/1152	0.066840	0.066666	77/576

Table A.1: The sequence $U(T, T)$ with $q = 5$

The sequence $U(T, T)$, with $q = 5$, comes with the constants: $h = 1$, $\mathbf{b}(h) = 0$, $\mathcal{Q} = 1$, and there is no need to switch to $-\gamma$. Computations are done up to degree $N = 6$.

d	$\delta_q^+(\gamma,d)$	num.	exp.	$\delta_q^-(\gamma,d)$	num.	exp.	$\delta_q(\gamma,d)$
2	1/6	0.166666	0.141057	1/4	0.250000	0.236111	5/12
4	1/12	0.083333	0.075388	0	0.000000	0.000000	1/12
10	25/288	0.086805	0.082029	0	0.000000	0.000000	25/288
14	7/144	0.048611	0.044042	7/96	0.072916	0.077380	35/288

Table A.2: The sequence $U(T+1,T^4)$ with $q=3$

The sequence $U(T+1,T^4)$, with $q=3$, comes with: $h=4$, $\mathbf{b}(h)=0$, $\mathcal{Q}=0$, and there is no need to switch to $-\gamma$. Computations are done up to degree $N=12$.

d	$\delta_q^+(\gamma,d)$	num.	exp.	$\delta_q^-(\gamma,d)$	num.	exp.	$\delta_q(\gamma,d)$
3	1/16	0.062500	0.055638	1/16	0.062500	0.078869	1/8
5	5/48	0.104166	0.094444	5/48	0.104166	0.161616	5/24
7	7/48	0.145833	0.150238	0	0.000000	0.000000	7/48
15	5/192	0.026041	0.022636	0	0.000000	0.000000	5/192

Table A.3: The sequence $U(T+1,T^3)$ with $q=2$

The sequence $U(T+1,T^3)$, with $q=2$, comes with: $h=3$, $\mathbf{b}(h)=0$, $\mathcal{Q}=1$, and there is no need to switch to $-\gamma$. Computations are done up to degree $N=12$.

d	$\delta_q^+(\gamma,d)$	num.	exp.	$\delta_q^-(\gamma,d)$	num.	exp.	$\delta_q(\gamma,d)$
2	11/24	0.458333	0.444530	1/4	0.250000	0.261904	17/24
4	5/24	0.208333	0.191125	1/4	0.250000	0.261904	11/24
6	23/64	0.359375	0.342146	0	0.000000	0.000000	23/64
8	1/6	0.166666	0.136218	1/4	0.250000	0.261904	5/12

Table A.4: The sequence $U(T,-1)$ with $q=7$

The sequence $U(T,-1)$, with $q=7$, comes with: $h=2$, $\mathbf{b}(h)=0$, $\mathcal{Q}=0$ and we should switch to $-\gamma$. Computations are done up to degree $N=6$.

d	$\delta_q^+(\gamma,d)$	num.	exp.	$\delta_q^-(\gamma,d)$	num.	exp.	$\delta_q(\gamma,d)$
2	11/24	0.458333	0.455626	1/4	0.250000	0.233333	17/24
4	5/12	0.416666	0.411543	0	0.000000	0.000000	5/24
14	77/1152	0.066840	0.052906	7/96	0.072916	0.708333	161/1152
18	5/96	0.052083	0.040310	1/16	0.062500	0.062500	11/96

Table A.5: The sequence $U(T, 3(T^3+T^2+1)^2)$ with $q=5$

The sequence $U(T, 3(T^3+T^2+1)^2)$, with $q=5$, comes with: $h=2$, $\mathbf{b}(h)=1$, and there is no need to switch to $-\gamma$. Computations are done up to degree $N=6$.

d	$\delta_q^+(\gamma,d)$	num.	exp.	$\delta_q^-(\gamma,d)$	num.	exp.	$\delta_q(\gamma,d)$
2	11/24	0.458333	0.415671	1/4	0.250000	0.270645	17/24
13	13/112	0.116071	0.076666	13/112	0.116071	0.177519	13/56
14	77/1152	0.066840	0.054069	0	0.000000	0.000000	77/1152
18	5/96	0.052083	0.042054	0	0.000000	0.000000	5/96

Table A.6: The sequence $U(3T^2-1, 3T^2-1)$ with $q=5$

The sequence $U(3T^2-1, 3T^2-1)$, with $q=5$, comes with: $h=2$, $\mathbf{b}(h)=1$, and there is no need to switch to $-\gamma$. Computations are done up to degree $N=6$.

In Table A.6, some values do not seem to match. There are two main reasons. First, for $d=13$, we have $\bar{f}=4$. From Chapter 3, new contributions to $\delta_5^+(\gamma,13)$ appear only at degrees divisible by $\bar{f}$. At $N=6$, we are between two contributions and the approximation weakens. Testing up to $N=8$ gives $\delta_5^+(\gamma,13)=0.432753$, which is closer to the expected value. The second reason is that we can not take N large enough for a good approximation. This is particularly the case for $d=18$, for which we have $\bar{f}=6$, since we can not reach the next contribution at $N=12$. The same happens in Table A.5.

d	$\delta_q^+(\gamma,d)$	num.	exp.	$\delta_q^-(\gamma,d)$	num.	exp.	$\delta_q(\gamma,d)$
3	3/8	0.375000	0.361327	3/8	0.375000	0.372023	3/4
5	5/24	0.208333	0.186318	0	0.000000	0.000000	5/24
7	7/48	0.145833	0.144969	0	0.000000	0.000000	7/48
9	1/8	0.125000	0.102017	1/8	0.125000	0.157738	1/4

Table A.7: The sequence $U(T, T^6+T^3+T^2)$ with $q=2$

The sequence $U(T, T^6 + T^3 + T^2)$, with $q = 2$, comes with: $h = 1$, $L = \mathbb{F}_4(T)$, and there is no need to switch to $-\gamma$. Computations are done up to degree $N = 12$.

d	$\delta_q^+(\gamma, d)$	num.	exp.	$\delta_q^-(\gamma, d)$	num.	exp.	$\delta_q(\gamma, d)$
2	11/24	0.458333	0.472107	3/8	0.375000	0.368990	323/384
4	5/12	0.416666	0.441584	1/4	0.250000	0.258012	2/3
10	115/576	0.199652	0.204783	0	0.000000	0.000000	115/576
14	77/576	0.133680	0.098060	7/64	0.109375	0.093750	35/144

Table A.8: The sequence $U(2T^2, T^4 + (T+1)^2)$ with $q = 3$

The sequence $U(2T^2, T^4 + (T+1)^2)$, with $q = 3$, comes with: $h = 1$, $L = \mathbb{F}_9(T)$, and there is no need to switch to $-\gamma$. Computations are done up to degree $N = 8$.

A.2 Numerical data in the classical case

In this section, we provide numerical evidence of Theorems 5.10, 5.12, 5.14, and 5.16. We start by presenting the SageMath programs used.

Our first program computes the n-th term of the Lucas sequence $U(a_1, a_2)$ using the companion matrix method.

[1]:
```
def Lucas(a_1,a_2,n):
    if n<2: return n
    M = matrix([[0,1],[-a_2,a_1]])
    return (M^n)[0,1]
```

The program **lucas_rank_mod** takes as an input two non-zero integers $a_1, a_2 \in \mathbb{Z}$ such that $U(a_1, a_2)$ is non-degenerate (see Lemma 2.2), a positive integer d, and a prime number p. The program returns the boolean $[d \mid \rho_U(p)]$ and the legendre symbol (Δ/p), where $\Delta = a_1^2 - 4a_2$. Note that there is an exception for $p = 2$, for which we return 0 instead of the legendre symbol. This is important in the main program, as we choose to ignore the even prime in our experimentations.

[2]:
```
def lucas_rank_mod(a_1,a_2,d,p):
    if p==2: return [a_2%2!=0 and (2 + a_1%2)%d==0, 0]

    Delta = a_1^2-4*a_2
    legendre = legendre_symbol(Delta,p)
```

```
    N = p - legendre

    if N%d!=0 or a_2%p==0: return [False,0]

    a_1_mod = Mod(a_1,p)
    a_2_mod = Mod(a_2,p)

    rank = 1
    for n in divisors(N):
        if Lucas(a_1_mod,a_2_mod,n)==0:
            rank = n
            break

    return [rank%d==0, legendre]

lucas_rank_mod(1,-1,2,7)
```

[2]: `[True, -1]`

With inputs $U(1,-1)$, $d=2$, and $p=7$, we obtain [`True`, -1] from **lucas_rank_mod**. In other words, 2 divides $\rho_U(7)=8$, and $(\Delta/7)=(5/7)=-1$, which is valid.

[3]:
```
def densities(a_1,a_2,d,x):
    res_plus = 0
    res_minus = 0

    Delta = a_1^2-4*a_2
    Nb_of_primes = prime_pi(x)

    for p in prime_range(3,x+1):
        u, v = lucas_rank_mod(a_1,a_2,d,p)
        if v==1:
            res_plus+=u

        if v==-1:
            res_minus+=u
```

```
    return [res_plus*1./Nb_of_primes, res_minus*1./Nb_of_primes]

%time densities(1,-1,2,10^6)
```

```
CPU times: user 2min 19s, sys: 51.4 ms, total: 2min 19s
Wall time: 2min 19s
```

```
[3]: [0.416749471324110, 0.250019108767102]
```

In the example, we obtain an approximation of $\delta_\gamma^+(2)$ and $\delta_\gamma^-(2)$ for the Fibonacci sequence $U(1,-1)$. We may compute the density values. Note that $\gamma = -\phi^2$ and $h = 2$. By Theorem 5.1, we have

$$\delta_\gamma^+(2) = \delta_{-\gamma}^+(4) + \delta_{-\gamma}^+(1) - \delta_{-\gamma}^+(2).$$

Since $\delta_{-\gamma}^+(1)$ is the density of primes that split completely in $\mathbb{Q}(\sqrt{5})$, we have $\delta_{-\gamma}^+(1) = 1/2$. Next, one can verify that $\mathcal{Q} = 0$, since $(-\gamma)^{1/2}$ has norm -1. Thus, by Theorem 5.10,

$$\delta_{-\gamma}^+(4) = \frac{1}{12} \quad \text{and} \quad \delta_{-\gamma}^+(2) = \frac{1}{6}.$$

It follows that $\delta_\gamma^+(2) = 5/12 = 0.41\bar{6}$. The same method yields $\delta_\gamma^-(2) = 1/4 = 0.25$. We see that the density values match the experimentation. Other comparisons for the Fibonacci sequence can be found in Table A.10.

In the following tables, we compare the values of $\delta_\gamma^+(d)$ and $\delta_\gamma^-(d)$ with experimental values obtained via our SageMath computations. The numerical and experimental values respectively appear in the "num." and "exp." columns. We test primes up to 10^6.

More information about the sequences tested can be found below their table. For instance, the value of h, $\mathcal{Q}$, Δ_L, and various other constants that are defined in our main theorems. They are computed using the programs in Section 5.4.

d	$\delta_\gamma^+(d)$	num.	exp.	$\delta_\gamma^-(d)$	num.	exp.	$\delta_\gamma(d)$
2	5/24	0.208333	0.207482	1/2	0.500000	0.500343	17/24
4	1/6	0.166666	0.166399	1/4	0.250000	0.250363	5/12
6	5/64	0.078125	0.078231	3/16	0.187500	0.187278	17/64
14	35/1152	0.030381	0.030268	7/96	0.072916	0.073084	119/1152
24	1/32	0.031250	0.031287	0	0.000000	0.000000	1/32
42	35/3072	0.011393	0.011325	7/256	0.027343	0.027669	119/3072

Table A.9: The sequence $U(4, 2)$

The sequence $U(4, 2)$ of Table A.9 comes with: $h = 2$, $\Delta_L = 8$ and $\mathcal{Q} = 0$. There is no need to switch γ to $-\gamma$. We apply Theorems 5.10 and 5.12.

d	$\delta_\gamma^+(d)$	num.	exp.	$\delta_\gamma^-(d)$	num.	exp.	$\delta_\gamma(d)$
2	5/12	0.416666	0.416749	1/4	0.250000	0.250019	2/3
4	1/12	0.083333	0.083021	1/4	0.250000	0.250019	1/3
6	5/32	0.156250	0.156462	3/32	0.093750	0.094002	1/4
10	25/144	0.173611	0.174373	0	0.000000	0.000000	25/144
20	5/144	0.034722	0.035083	0	0.000000	0.000000	5/144
30	25/384	0.065104	0.065619	0	0.000000	0.000000	25/384

Table A.10: The sequence $U(1, -1)$

The Fibonacci sequence $U(1, -1)$ of Table A.10 comes with: $h = 2$, $\Delta_L = 5$ and $\mathcal{Q} = 0$. Since $a_2 = -1$, we should switch γ to $-\gamma$. We apply Theorems 5.10, 5.12, and 5.1.

d	$\delta_\gamma^+(d)$	num.	exp.	$\delta_\gamma^-(d)$	num.	exp.	$\delta_\gamma(d)$
2	1/6	0.166666	0.165774	1/2	0.500000	0.500471	2/3
4	1/12	0.083333	0.083021	1/4	0.250000	0.250019	1/3
6	1/48	0.020833	0.020662	3/48	0.062500	0.062332	1/12
10	5/72	0.069444	0.068995	0	0.000000	0.000000	5/72
18	1/144	0.006944	0.006879	3/144	0.020833	0.020892	1/36
30	5/576	0.008680	0.008713	0	0.000000	0.000000	5/576

Table A.11: The sequence $U(10, 5)$

The sequence $U(10,5)$ of Table A.11 comes with: $h=6$, $\Delta_L=5$ and $\mathcal{Q}=0$. There is no need to switch γ to $-\gamma$. We apply Theorems 5.10 and 5.12.

d	$\delta_\gamma^+(d)$	num.	exp.	$\delta_\gamma^-(d)$	num.	exp.	$\delta_\gamma(d)$
2	1/6	0.166666	0.166602	1/6	0.166666	0.167227	1/3
4	1/12	0.083333	0.083467	1/12	0.083333	0.083326	1/6
6	1/32	0.031250	0.031414	3/32	0.093750	0.093607	1/8
10	5/144	0.034722	0.035045	5/144	0.034722	0.034446	5/72
14	7/576	0.012152	0.011949	7/576	0.012152	0.012344	7/288
42	7/768	0.009114	0.009095	0	0.000000	0.000000	7/768

Table A.12: The sequence $U(5,1)$

The sequence $U(5,1)$ of Table A.12 comes with the constants: $h=2$, $\Delta_L=21$, $\mathcal{Q}=1$, $\mathcal{Q}_1=0$, $\Delta_1=12$, $\mathcal{Q}_2=1$, and $\Delta_2=28$. There is no need to switch γ to $-\gamma$. We apply Theorems 5.14 and 5.16.

d	$\delta_\gamma^+(d)$	num.	exp.	$\delta_\gamma^-(d)$	num.	exp.	$\delta_\gamma(d)$
2	1/3	0.333333	0.332632	1/3	0.333333	0.334135	2/3
4	1/6	0.166666	0.166488	1/6	0.166666	0.167392	1/3
6	1/16	0.062500	0.062574	3/16	0.187500	0.187151	1/4
12	1/32	0.031250	0.031746	3/32	0.093750	0.094040	1/8
26	13/252	0.051587	0.051529	0	0.000000	0.000000	13/252
78	13/1344	0.009672	0.009554	0	0.000000	0.000000	13/1344

Table A.13: The sequence $U(1,-3)$

The sequence $U(1,-3)$ of Table A.13 comes with the constants: $h=1$, $\Delta_L=13$, $\mathcal{Q}=1$, $\mathcal{Q}_1=0$, $\Delta_1=-3$, $\mathcal{Q}_2=0$, and $\Delta_2=-39$. Note that $\mathcal{Q}_2=0$ since the automorphism σ_2 itself does not exist. This is because $\Delta_L \mid \Delta_2$. There is no need to switch γ to $-\gamma$. We apply Theorems 5.14 and 5.16.

d	$\delta_\gamma^+(d)$	num.	exp.	$\delta_\gamma^-(d)$	num.	exp.	$\delta_\gamma(d)$
2	1/12	0.083333	0.082881	1/12	0.083333	0.083607	1/6
4	1/24	0.041666	0.041466	1/24	0.041666	0.042077	1/12
6	1/64	0.015625	0.015363	1/64	0.015625	0.015694	1/32
10	5/576	0.008680	0.008611	5/576	0.008680	0.008790	5/288
22	11/1440	0.007638	0.007783	11/1440	0.007638	0.007732	11/720
30	5/768	0.006510	0.006675	5/768	0.006510	0.006573	5/384

Table A.14: The sequence $U(7, 16)$

The sequence $U(7, 16)$ of Table A.14 comes with the constants: $h = 4$, $\Delta_L = -15$, $\mathcal{Q} = 1$, $\mathcal{Q}_1 = 1$, $\Delta_1 = -24$, $\mathcal{Q}_2 = 1$, and $\Delta_2 = -40$. There is no need to switch γ to $-\gamma$. We apply Theorems 5.14 and 5.16.

A.3 Reference tables of density formulas

In this appendix, we display three tables that helps find the right theorem in order to compute a closed-form formula of $\delta_q^+(\gamma, d)$ and $\delta_q^-(\gamma, d)$. Each table represents, in order, one of the three assumptions: $q \equiv 1 \pmod 4$, $2 \mid q$, and $q \equiv 3 \pmod 4$. Note that we do not mention the possible switch between γ and $-\gamma$ in the tables. If there is a need to switch, then one should use Theorem 4.1 first, and then our tables.

In each cell, we either reference the theorem to use or, in trivial cases, we write the density values directly. If the mention `n/a` appears, then the case in question does not happen. We consider four columns, the first being for $\delta_q^+(\gamma, d)$. The next three columns deal with $\delta_q^-(\gamma, d)$ in the cases $2 \mid f$ and $(d, q-1) \leq 2$, $d = 2$, and otherwise. We use "o/w" as an abbreviation for "otherwise".

Throughout this section, we assume that L/K is a degree-two extension. If $L = K$, then $R_q^-(\gamma, d)$ is empty and the density of $\delta_q^+(\gamma, d)$ is obtained via Theorem 4.12. In addition, we also assume $d \mid q^k + 1$ for some $k \geq 1$ in the three columns that consider the case of $R_q^-(\gamma, d)$, as it is empty otherwise.

	$\delta_q^+(\gamma, d)$	$d = 2$	$2 \mid f$ and $(d, q-1) \leq 2$	o/w
$\mathbf{b}(h) = 0$	Theorem 4.12	Corollary 3.26	Theorem 4.19	0
$\mathbf{b}(h) = 1$	Theorem 4.28	Corollary 3.26	Theorem 4.33	0
$L = \mathbb{F}_{q^2}(T)$	Theorem 4.38	Corollary 3.26	Theorem 4.44	0

Table A.15: The case $q \equiv 1 \pmod 4$

	$\delta_q^+(\gamma, d)$	$d = 2$	$2 \mid f$ and $(d, q-1) \leq 2$	o/w
$\mathbf{b}(h) = 0$	Theorem 4.12	0	Theorem 4.19	0
$\mathbf{b}(h) = 1$	`n/a`	`n/a`	`n/a`	`n/a`
$L = \mathbb{F}_{q^2}(T)$	Theorem 4.38	0	Theorem 4.44	0

Table A.16: The case $2 \mid q$

	$\delta_q^+(\gamma, d)$	$d = 2$	$2 \mid f$ and $(d, q-1) \leq 2$	o/w
$\mathbf{b}(h) = 0$	Theorem 4.12	Theorem 4.21	Theorem 4.19	0
$\mathbf{b}(h) = 1$	`n/a`	`n/a`	`n/a`	`n/a`
$L = \mathbb{F}_{q^2}(T)$	Theorem 4.38	Theorem 4.40	Theorem 4.44	0

Table A.17: The case $q \equiv 3 \pmod 4$

Bibliography

[1] C. Ballot. Density of prime divisors of linear recurrences. *Mem. Amer. Math. Soc.*, 115(551):viii+102, 1995.

[2] C. Ballot. Counting monic irreducible polynomials P in $\mathbb{F}_q[X]$ for which order of X (mod P) is odd. *J. Théor. Nombres Bordeaux*, 19(1):41–58, 2007.

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

[4] C. Ballot. Competing prime asymptotic densities in $\mathbb{F}_q[X]$: a discussion. *Enseign. Math. (2)*, 54(3-4):303–327, 2008.

[5] C. Ballot and H. C. Williams. *The Lucas sequences—theory and applications*, volume 8 of *CMS/CAIMS Books in Mathematics*. Springer, Cham, [2023] ©2023.

[6] H. Bilharz. Primdivisoren mit vorgegebener Primitivwurzel. *Math. Ann.*, 114(1):476–492, 1937.

[7] B. J. Birch. Cyclotomic fields and Kummer extensions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 85–93. Academic Press, London, 1967.

[8] P. Cubre and J. Rouse. Divisibility properties of the Fibonacci entry point. *Proc. Amer. Math. Soc.*, 142(11):3771–3785, 2014.

[9] M. D. Fried and M. Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[10] 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. Ann.*, 162:74–76, 1965/66.

[11] 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. Ann.*, 166:19–23, 1966.

[12] L. Hochfilzer and E. Waxman. On Artin's primitive root conjecture for function fields over $\mathbb{F}_q$. *Q. J. Math.*, 75(3):1181–1200, 2024.

[13] Olli Järviniemi. Positive lower density for prime divisors of generic linear recurrences. *Math. Proc. Cambridge Philos. Soc.*, 175(3):467–478, 2023.

[14] G. Karpilovsky. *Topics in field theory*, volume 155 of *North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam, 1989. Notas de Matemática, 124. [Mathematical Notes].

[15] S. Kim and M. Ram Murty. Artin's primitive root conjecture for function fields revisited. *Finite Fields Appl.*, 67:101713, 15, 2020.

[16] J. C. Lagarias. The set of primes dividing the Lucas numbers has density 2/3. *Pacific J. Math.*, 118(2):449–461, 1985.

[17] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[18] R. R. Laxton. On groups of linear recurrences. I. *Duke Math. J.*, 36:721–736, 1969.

[19] R. R. Laxton. On groups of linear recurrences. II. Elements of finite order. *Pacific J. Math.*, 32:173–179, 1970.

[20] P. Moree. On the prime density of Lucas sequences. *J. Théor. Nombres Bordeaux*, 8(2):449–459, 1996.

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

[22] P. Moree. Artin's primitive root conjecture—a survey. *Integers*, 12(6):1305–1416, 2012.

[23] P. Moree and P. Stevenhagen. Prime divisors of Lucas sequences. *Acta Arith.*, 82(4):403–410, 1997.

[24] P. Moree and P. Stevenhagen. A two-variable Artin conjecture. *J. Number Theory*, 85(2):291–304, 2000.

[25] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[26] M. Papikian. *Drinfeld modules*, volume 296 of *Graduate Texts in Mathematics*. Springer, Cham, [2023] ©2023.

[27] F. Pappalardi. Square free values of the order function. *New York J. Math.*, 9:331–344, 2003.

[28] F. Pappalardi and I. Shparlinski. On Artin's conjecture over function fields. *Finite Fields Appl.*, 1(4):399–404, 1995.

[29] M. Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[30] C. Sanna. On the divisibility of the rank of appearance of a Lucas sequence. *Int. J. Number Theory*, 18(10):2145–2156, 2022.

[31] C. Sanna. On the index of appearance of a Lucas sequence. *Ramanujan J.*, 63(4):1199–1223, 2024.

[32] P. J. Stephens. Prime divisors of second-order linear recurrences. I. *J. Number Theory*, 8(3):313–332, 1976.

[33] P. J. Stephens. Prime divisors of second order linear recurrences. II. *J. Number Theory*, 8(3):333–345, 1976.

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

[35] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. `https://www.sagemath.org`.

[36] M. Ward. Prime divisors of second order recurring sequences. *Duke Math. J.*, 21:607–614, 1954.

[37] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*, volume 7 (1945) of *Publications de l'Institut de Mathématiques de l'Université de Strasbourg [Publications of the Mathematical Institute of the University of Strasbourg]*. Hermann & Cie, Paris, 1948. Actualités Scientifiques et Industrielles, No. 1041. [Current Scientific and Industrial Topics].

[38] K. Wiertelak. On the density of some sets of primes. I. *Acta Arith.*, 34(3):183–196, 1977/78.

[39] K. Wiertelak. On the density of some sets of primes. II. *Acta Arith.*, 34(3):197–210, 1977/78.

[40] K. Wiertelak. On the density of some sets of primes. IV. *Acta Arith.*, 43(2):177–190, 1984.

[41] K. Wiertelak. On the density of some sets of primes p, for which $(\mathrm{ord}_p\, b, n) = d$. *Funct. Approx. Comment. Math.*, 21:69–73, 1992.

[42] K. Wiertelak. On the density of some sets of primes p, for which $n \mid \mathrm{ord}_p a$. *Funct. Approx. Comment. Math.*, 28:237–241, 2000. Dedicated to Włodzimierz Staś on the occasion of his 75th birthday.