Prime densities for generalized Lucas sequences

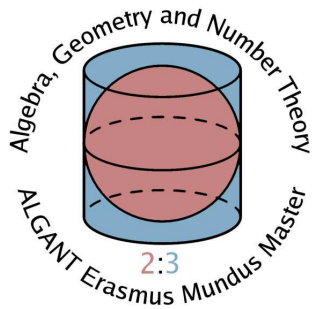
Ljujic, Z.

Željka Ljujić

Prime densities for generalized Lucas sequences

Master thesis, defended on June 26, 2007

Thesis advisor: Prof. Dr. P. Stevenhagen



Mathematisch Instituut, Universiteit Leiden

Contents

1 Introduction

For $X = \{x_n\}_{n=0}^{\infty}$ any integer sequence, we denote by D_X the set of all prime numbers p that divide some non-zero term of the sequence X. We will refer to the elements of the set D_X as the prime divisors of X.

Let S be a set of prime numbers. We define the natural density of S as

$$\delta(S) = \lim_{x \to \infty} \frac{|\{p \leq x \mid p \in S\}|}{|\{p \leq x \mid p \text{ prime }\}|}.$$

The question we are interested in is: when does $\delta(D_X)$ exist and when it exists, can we compute its exact value?

In this thesis, we only consider linearly recurrent sequences, i.e. sequences for which there exists $k \geq 1$, such that

$$x_{n+k} = \sum_{i=0}^{k-1} a_i x_{n+i} \quad \text{for } n \geq 0,$$

where $a_i \in \mathbb{Z}$, $a_0 \neq 0$. We call k the order of the recurrence. The polynomial $f(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_0 \in \mathbb{Z}[x]$ is the characteristic polynomial associated to the given recurrence relation. We assume that f is separable, such that we have

$$f(x) = \prod_{i=1}^{k} (x - \alpha_i) \in \overline{\mathbb{Q}}[x],$$

where $\alpha_i \neq \alpha_j$ for $i \neq j$. In this case, the terms of the sequence $X = \{x_n\}_{n=0}^{\infty}$ can be expressed as

$$x_n = \sum_{i=1}^{k} c_i \alpha_i^n \quad \text{for } n \geq 0.$$

From here, it easily follows, that for first order sequences the density question is trivial. On the other hand, for third order sequences the question is still an open problem, [10]. Hence, we will consider only second order linear recurrences.

Let the sequence X satisfy the recurrence relation

$$x_{n+2} = ax_{n+1} + bx_n,$$

where a, $b \in \mathbb{Z}$ and the characteristic polynomial is $f(x) = x^2 - ax - b \in \mathbb{Z}[x]$. We will assume that X does not satisfy a first order recurrence, so $b \neq 0$.

In the separable case, the terms of X can be expressed in the form

$$x_n = c\alpha^n + \overline{c\alpha}^n \quad \text{for } n \geq 0,$$

where α and $\overline{\alpha}$ are distinct roots of f. We denote by $q = \frac{\alpha}{\overline{\alpha}}$. Note that the "root quotient" q is defined only up to inversion. We call the sequence X non-degenerate if q is not a root of unity. It can easily be proved (see [9]) that in the case of degenerate sequences the set of prime divisors is finite or cofinite, so we will consider only non-degenerate cases.

Let p be a prime coprime to α and c. Then, we have the equivalence

$$p \text{ divides } x_n \Leftrightarrow \left(\frac{\alpha}{\overline{\alpha}}\right)^n = -\frac{\overline{c}}{c} \in (\mathcal{O}/p\mathcal{O})^*,$$

where $\mathcal{O}$ denotes the ring of integers of the field generated by the roots of f. Let us denote $r = -\frac{\overline{c}}{c}$. Note that, just as the root quotient, r is defined up to inversion. Then, for all but finitely many primes p, we obtain

$$p \text{ divides some term of } X \Leftrightarrow \langle r \rangle \subset \langle q \rangle \subset (\mathcal{O}/p\mathcal{O})^*.$$

Thus, we formulated the problem we are trying to solve without any reference to recurrent sequences. We consider the element r in the group $\mathbb{Q}(q)^*/\langle q \rangle$. One can easily see that in the non-degenerate case the field $\mathbb{Q}(q)$ coincides with $\mathbb{Q}(\alpha)$.

In the case of second order sequences, the key distinction is between the torsion and the non-torsion case. We refer to the case when r is a torsion element in the group $\mathbb{Q}(q)^*/\langle q \rangle$ as the torsion case of the problem, and the corresponding sequences are known as torsion sequences.

Depending on whether the polynomial f is reducible or irreducible over $\mathbb{Q}$, we consider a rational and a quadratic case. In the rational case $q \in \mathbb{Q}^*$, while in the quadratic case q is a quadratic integer of norm 1.

Ward [13] proved that any non-degenerate integer second order linear recurrent sequence has an infinite number of prime divisors.

Here, we consider the torsion case. "Generically", $(\mathbb{Q}(q)^*/\langle q \rangle)^{tor} = \{\pm 1\}$. More precisely, this occurs when $\mathbb{Q}(q)$ does not contain any roots of unity different than ± 1 and when q is not a power in $\mathbb{Q}(q)^*/\{\pm 1\}$. The case $r = 1$ is trivial, we have $\delta(D_X) = 1$. Hence, we assume $r = -1$ and consider the sequence

$$x_n = \alpha^n + \overline{\alpha}^n \quad \text{for } n \geq 0.$$

In the case $r = -1$, $q \in \mathbb{Q}^*$ it is possible to give an unconditional proof of the existence of the density. The main idea goes back to Hasse [4], who explicitly computed the density of certain non-degenerate integer second order linear recurring sequences with reducible characteristic polynomial.

More precisely, Sierpinski in [12] proposed the problem concerning the existence of the density of primes p for which the order of 2 modulo p is even. For a prime $p > 2$ this question is equivalent to the question when does p divide some term of the sequence $\{2^n + 1\}_{n=0}^{\infty}$. Note that this is exactly the case $r = -1$, $q = 2$. Hasse [4] found a method and used it to establish a more general result; he determined the density of prime divisors of the sequence $\{a^n + 1\}_{n=0}^{\infty}$, where a is a square-free integer.

We will describe Hasse's method briefly. Let us denote $X = \{a^n + 1\}_{n=0}^{\infty}$, for some square-free integer a. Let

$$S = \{p \mid \ p \text{ is an odd prime number } \}$$

and

$$D_X = \{p \in S \mid \ p \text{ divides some term of } X \ \}.$$

For a prime p, coprime to a, we have the equivalences

$$p \mid a^n + 1 \text{ for some } n \;\Leftrightarrow -1 \in \langle a \rangle \in \mathbb{F}_p^* \Leftrightarrow \text{order of } (a \bmod p) \text{ in } \mathbb{F}_p^* \text{ is even.}$$

We consider the subgroup $H \subset \mathbb{F}_p^*$ consisting of all elements of odd order. Its index equals 2^k, where $k = \mathrm{ord}_2(p-1)$. By Dirichlet's theorem, the probability that a prime p has $k = \mathrm{ord}_2(p-1)$ equals 2^{-k}. Next, if we consider non-square a, then, heuristically, for a prime p, such that $k = \mathrm{ord}_2(p-1)$, the probability that $a \in H$ is 2^{-k}. Hence, the density of primes for which $(a \bmod p)$ has odd order should equal

$$\sum_{k=1}^{\infty} \frac{1}{4^k} = \frac{1}{3}.$$

To make this heuristic argument into a proof, for fixed $k \in \mathbb{Z}_{\geq 0}$, we consider all prime numbers p, such that $2^k \| p-1$. We partition the set S into pairwise disjoint sets $S_k \subset S$ such that

$$S_k = \{p \in S |\ p \equiv 1 + 2^k \pmod{2^{k+1}}\}$$

and

$$S = \bigcup_{k=1}^{\infty} S_k.$$

Having the equivalence

$$p \in S_k \quad \Leftrightarrow \quad \begin{array}{l} p \text{ splits completely in the field } \mathbb{Q}(\zeta_{2^k}), \text{ but not in the} \\ \text{field } \mathbb{Q}(\zeta_{2^{k+1}}). \end{array}$$

and using the Chebotarev density theorem we obtain the densities $\delta(S_k) = 2^{-k}$, in accordance with Dirichlet's theorem.

We consider the sets

$$D_X^{(k)} = D_X \cap S_k.$$

Having the equivalence

$$a \in H \Leftrightarrow a \text{ is a } 2^k\text{th power in } \mathbb{F}_p^*,$$

if we denote

$$\overline{D}_X^{(k)} = S_k \setminus D_X^{(k)},$$

we obtain

$$p \in \overline{D}_X^{(k)} \quad \Leftrightarrow \quad \begin{array}{l} p \text{ splits completely in the field } \mathbb{Q}(\zeta_{2^k},\ \sqrt[2^k]{a}), \text{ but not in} \\ \text{the field } \mathbb{Q}(\zeta_{2^{k+1}},\ \sqrt[2^k]{a}). \end{array}$$

Again, using the Chebotarev density theorem we find the densities

$$\delta(\overline{D}_X^{(k)}) = \frac{1}{[\mathbb{Q}(\zeta_{2^k},\ \sqrt[2^k]{a}) : \mathbb{Q}]} - \frac{1}{[\mathbb{Q}(\zeta_{2^{k+1}},\ \sqrt[2^k]{a}) : \mathbb{Q}]} = 4^{-k} \text{ “generically”.}$$

Finally, from

$$\sum_{k=1}^{\infty} \delta(S_k^+) = \delta(S^+)$$

we conclude

$$\delta(D_X) = 1 - \sum_{k=1}^{\infty} \delta(\overline{D}_X^{(k)}).$$

Using Hasse's method, Ballot [1] completely determined the densities of the sets of prime divisors of the sequences $\{a^n + b^n\}_{n=0}^{\infty}$, for $a, b \in \mathbb{Z}_{\neq 0}$, $\frac{a}{b} \neq \{\pm 1\}$, which correspond to the case $r = -1$, $q \in \mathbb{Q}^*$.

Lagarias [6], observed that Hasse's method can be extended to certain second order linear recurrences with irreducible characteristic polynomials. In this case the computation is more involved and it is done in two stages depending on whether p splits or stays inert in the field $\mathbb{Q}(q)$.

In [8], P. Moree and P. Stevenhagen considered the Lucas sequence X_K associated with a real quadratic extension K, defined by

$$X_K = \{Tr_{K/\mathbb{Q}}(\varepsilon^n)\}_{n=0}^{\infty} = \{\varepsilon^n + \bar{\varepsilon}^n\}_{n=0}^{\infty},$$

where ε is a fundamental unit of K. They proved that the set of prime divisors of the sequence X_K has a natural density δ_K and determines it for each K.

Here, we extend this method to the "generalized Lucas sequences".

$$X_\alpha = \{Tr_{K/\mathbb{Q}}(\alpha^n)\}_{n=0}^{\infty} = \{\alpha^n + \bar{\alpha}^n\}_{n=0}^{\infty},$$

where α is any quadratic integer and K the corresponding quadratic field. We will prove our main theorem.

Main Theorem. *The density of prime divisors of the generalized Lucas sequence X_α exists for every non-zero quadratic integer α for which $\alpha/\overline{\alpha}$ is not a root of unity and it is a rational number strictly between 0 and 1.*

Moreover, we will compute it for "generic" α, as well as for some special "non-generic" α's. At the end, we will give some numerical data obtained approximating the ratio

$$\frac{|\{p \leq x \mid p \in D_{X_\alpha}\}|}{|\{p \leq x \mid p \text{ prime }\}|}$$

for some α.

We begin presenting some theory necessary for understanding the proof of the main theorem.

2 Background Material

This is a short outline of the theory used in the main proof. Its only purpose is to recall the terminology and some well-known facts. We present the theory concentrating on the statements that are going to be useful for us in what follows and mainly without either proofs or particular references. In the section 2.1, we were mostly following the exposition given in [3] and [5], except for 2.1.4, where we were also using [7]. In the section 2.2 we followed [2], [11].

2.1 Number Fields

2.1.1 Galois Extensions

Let K be a number field and L a finite extension of K of degree n. We denote by $\mathcal{O}_K$, resp. $\mathcal{O}_L$ the ring of integers of K, resp. L. If $\mathfrak{p}$ is a prime ideal of K, then

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}...\mathfrak{P}_g^{e_g},$$

where the $\mathfrak{P}_i$'s are distinct primes of L lying above $\mathfrak{p}$. The integer e_i, also written as $e_{\mathfrak{P}_i|\mathfrak{p}}$, is called the ramification index of $\mathfrak{p}$ in $\mathfrak{P}_i$. For $\mathfrak{P}_i \mid \mathfrak{p}$, we consider the field extension $\mathcal{O}_L/\mathfrak{P}_i$ of $\mathcal{O}_K/\mathfrak{p}$. Its degree, written as f_i or $f_{\mathfrak{P}_i|\mathfrak{p}}$, is the inertial degree of $\mathfrak{p}$ in $\mathfrak{P}_i$. There exists a remarkable relation among the numbers e_i, f_i and n.

Theorem 2.1. *Let $K \subset L$ be number fields and let $\mathfrak{p}$ be a prime of K. If e_i, resp. f_i, $i = 1, ..., g$ are the ramification indices, resp. inertial degrees, then*

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

We say that prime $\mathfrak{p}$ of K is unramified in L if all e_i equal 1.

Theorem 2.2. *Let $K \subset L$ be an extension of number fields. Then a prime $\mathfrak{p}$ of K ramifies in L if and only if $\mathfrak{p}$ divides the discriminant of L over K.*

In particular, only finitely many primes are ramified.

Most of all the extensions $K \subset L$ we will deal with will be Galois extensions. In this case we have the following.

Theorem 2.3. *Let $K \subset L$ be Galois. If $\mathfrak{p}$ is a prime of K, then the Galois group $\mathrm{Gal}(L/K)$ acts transitively on the primes of L that are lying above $\mathfrak{p}$. If we write*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}...\mathfrak{P}_g^{e_g},$$

then $e_1 = ... = e_g = e$ and $f_1 = ... = f_g = f$. Also, $efg = n$.

Let L/K be a Galois extension. Then prime $\mathfrak{p}$ of K ramifies in L if $e > 1$, and is unramified if $e = 1$. If $\mathfrak{p}$ satisfies the stronger condition $e = f = 1$, we say that $\mathfrak{p}$ splits completely in L. In this case, $\mathfrak{p}$ is product of $n = [L : K]$ distinct primes $\mathfrak{P}_i$ in L.

Let $\mathfrak{P}$ be a prime of L. We define the decomposition group

$$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

and the inertia group

$$I_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\alpha) \equiv \alpha \,(\mathrm{mod}\ \mathfrak{P}) \text{ for all } \alpha \in \mathcal{O}_L\}.$$

Trivially, $I_{\mathfrak{P}} \subset D_{\mathfrak{P}}$. Also, $\mathcal{O}_L/\mathfrak{P}$ is a finite Galois extension of $\mathcal{O}_K/\mathfrak{p}$, where $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$. Let us denote $\widetilde{G} = \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$. Now, any $\sigma \in D_{\mathfrak{P}}$ induces an element $\tilde{\sigma} \in \widetilde{G}$. Thus the map $\sigma \mapsto \widetilde{\sigma}$ defines a homomorphism $D_{\mathfrak{P}} \to \tilde{G}$, whose kernel is exactly $I_{\mathfrak{P}}$.

Theorem 2.4. *Let $K \subset L$ be Galois. If $\mathfrak{p}$ is a prime of K and $\mathfrak{P}$ prime of L lying above $\mathfrak{p}$, then the homomorphism $D_{\mathfrak{P}} \to \widetilde{G}$ is surjective. Thus $D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \widetilde{G}$.*

It is not hard to see that $|\tilde{G}| = f_{\mathfrak{P}|\mathfrak{p}}$ and $|D_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}$. From here, $|I_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}}$. Hence, if $\mathfrak{P}$ is unramified in L, we have $D_{\mathfrak{P}} \cong \tilde{G}$.

The structure of the Galois group $\tilde{G}$ is well-known: if $\mathcal{O}_K/\mathfrak{p}$ has $q = N_{K/\mathbb{Q}}(\mathfrak{p})$ elements, then $\tilde{G}$ is a cyclic group with canonical generator given by the Frobenius automorphism $x \mapsto x^q$. Thus, if $\mathfrak{p}$ is unramified in L, there is is a unique $\sigma \in D_{\mathfrak{P}}$ that maps to the Frobenius element. Moreover, we have the following theorem

Theorem 2.5. *Let $K \subset L$ be Galois. Let $\mathfrak{p}$ be an unramified prime in K. If $\mathfrak{P}$ is a prime in L lying above $\mathfrak{p}$, then there is a unique element $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,*

$$\sigma_{\mathfrak{P}}(\alpha) \equiv \alpha^{N_{K/\mathbb{Q}}(\mathfrak{p})} \,(\mathrm{mod}\ \mathfrak{P}).$$

This automorphism $\sigma_{\mathfrak{P}}$ is called the Frobenius element of $\mathfrak{P}$ in $\mathrm{Gal}(L/K)$. From the last theorem, we can easily deduce following properties of the Frobenius element:

- If $\tau \in \mathrm{Gal}(L/K)$, then $\sigma_{\tau(\mathfrak{P})} = \tau \sigma_{\mathfrak{P}} \tau^{-1}$.
- The order of $\sigma_{\mathfrak{P}}$ is the inertial degree $f = f_{\mathfrak{P}|\mathfrak{p}}$.
- A prime $\mathfrak{p}$ splits completely in L if and only if $\sigma_{\mathfrak{P}} = 1$.

The Frobenius element restricts well to subfields: if $K \subset L$ and $L \subset M$ are Galois extensions of number fields, then $\sigma_{\mathcal{P}} \in \mathrm{Gal}(M/K)$ maps by restriction to $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$, where $\mathcal{P}$ is a prime of M, and $\mathfrak{P} = \mathcal{P} \cap \mathcal{O}_L$.

We define the Frobenius symbol of $\mathfrak{p}$ in L/K to be the conjugacy class $\{\sigma_{\mathfrak{P}} \mid \mathfrak{P}|\mathfrak{p}\}$ in $\mathrm{Gal}(L/K)$.

When $K \subset L$ is an abelian extension, the Frobenius element $\sigma_{\mathfrak{P}}$ depends only on the underlying prime $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. It follows that in the case $\mathrm{Gal}(L/K)$ abelian, we can denote the Frobenius element associated to $\mathfrak{P}$ simply by $\sigma_{\mathfrak{p}}$, independently of a choice of a prime $\mathfrak{P}$ lying above $\mathfrak{p}$.

2.1.2 Quadratic Fields

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. We say that K is a quadratic number field if $[K : \mathbb{Q}] = 2$. It can easily be showed that every quadratic number field can uniquely be written as $\mathbb{Q}(\sqrt{d})$, where d is a square-free integer.

Theorem 2.6. *If $d \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.*
If $d \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\frac{-1+\sqrt{d}}{2}]$.

Knowing how to find an explicit integral basis for $\mathcal{O}_K$, makes it easy to compute the discriminant of quadratic number fields. We have

Theorem 2.7. *Let Δ_K denote the discriminant of K. Then*

$$\Delta_K = \begin{cases} 4d & d \equiv 2, 3 \pmod 4, \\ d & d \equiv 1 \pmod 4. \end{cases}$$

Now, we want to determine how rational primes p split in $\mathcal{O}_K$.

Theorem 2.8. *Let K be a quadratic number field of discriminant d_K, and let the nontrivial automorphism of K be denoted $\alpha \mapsto \alpha'$. Let p be a prime number.*

(i) *If $(\frac{d}{p}) = 0$, then $p\mathcal{O}_K = \mathfrak{p}^2$, for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.*

(ii) *If $(\frac{d}{p}) = 1$, then $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}' = \{\gamma' \mid \gamma \in \mathfrak{p}\} \neq \mathfrak{p}$ are prime in $\mathcal{O}_K$.*

(iii) *If $(\frac{d}{p}) = -1$, then $p\mathcal{O}_K$ is prime in $\mathcal{O}_K$.*

In our proof of the main theorem, we will make use of the following lemma.

Lemma 2.9. *Let K be a quadratic field and $\alpha \in K \setminus \mathbb{Q}$. Then the extension $K(\sqrt{\alpha})$ is normal over $\mathbb{Q}$ if and only if $N(\alpha)$ is a square in K.*

Proof: The extension $K(\sqrt{\alpha})/\mathbb{Q}$ is normal if and only if $K(\sqrt{\alpha}) = K(\sqrt{\overline{\alpha}})$. By Kummer theory, this is equivalent to $\alpha \in \overline{\alpha} \cdot {K^*}^2$, which is equivalent to $\mathrm{N}(\alpha) = \alpha\overline{\alpha} \in {K^*}^2$. $\square$

2.1.3 Cyclotomic Fields

Let K be a number field and $n > 1$ be an integer. We consider the extension $L = K(\zeta_n)$, where ζ_n is a nth primitive root of unity. Clearly, L is a normal extension of K.

If $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(\zeta_n) = \zeta_n^k$, for some integer k, $(n, k) = 1$. The map $\sigma \mapsto k$ is a canonical map of $\mathrm{Gal}(L/K)$ into the group $(\mathbb{Z}/n\mathbb{Z})^*$. In particular, $[L : K] \leq \varphi(n)$.

Let us consider the extensions $\mathbb{Q}(\zeta_n)$.

Theorem 2.10. *The extension $\mathbb{Q}(\zeta_n)$ is a normal extension of $\mathbb{Q}$ of degree $\varphi(n)$; its Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is naturally isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$.*

Corollary 2.11. *For prime $p \nmid n$ the Frobenius element $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of p is given by $\sigma_p(\sum a_i\zeta_n) = \sum a_i\zeta_n^{ip}$, for $a_i \in \mathbb{Q}$.*

The next statements will concern the factorization of primes p in the extension $\mathbb{Q}(\zeta_n)$.

Theorem 2.12. *If p is a prime not dividing n then it is unramified in $\mathbb{Q}(\zeta_n)$ and its residue degree f_p is the least integer $f \geq 1$ such that $p^f \equiv 1 \pmod{n}$.*

Corollary 2.13. *If $p \nmid n$ is prime, then p splits completely in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ if and only if $p \equiv 1 \pmod{n}$.*

At the end, we state a lemma about quadratic subfields of $\mathbb{Q}(\zeta_{2^\infty})$.

Lemma 2.14. *The only quadratic subfields of $\mathbb{Q}(\zeta_{2^\infty})$ are the quadratic subfields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ of $\mathbb{Q}(\zeta_8)$.*

Proof: By construction of $\mathbb{Q}(\zeta_{2^\infty})$, it is enough to prove that the extensions $\mathbb{Q}(\zeta_{2^k})$ do not have any other quadratic subfields, where $k \geq 3$.

We have $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}) \cong (\mathbb{Z}/2^k\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$, so if $k \geq 3$ the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^k})/\mathbb{Q})$ has exactly 3 subgroups of index 2, hence $\mathbb{Q}(\zeta_{2^k})$ has exactly 3 quadratic subfields. This proves the lemma.

2.1.4 The Chebotarev Density Theorem

Let $K \subset L$ be be number fields and L Galois over K. To every unramified prime ideal $\mathfrak{P}$ we associate its Frobenius element $\sigma_{\mathfrak{P}}$. Conversely, we have that every element from $\mathrm{Gal}(L/K)$ is the Frobenius element for infinitely many prime ideals of L. More precisely, we have the following theorem

Theorem 2.15. *(Chebotarev Density Theorem). Let $K \subset L$ be Galois, and let $C \subset \mathrm{Gal}(L/K)$ be a conjugacy class. Then the set*

$$S = \{\mathfrak{p} \mid \mathfrak{p} \text{ a prime of } K, \mathfrak{p} \nmid \Delta_{L/K}, \sigma_{\mathfrak{p}} \in C\}$$

has density $\delta(S) = |C|/|\mathrm{Gal}(L/K)|$.

Here, by density we mean the natural density. If S is a set of primes of K, we define the natural density of S to be

$$\delta(S) = \lim_{x\to\infty} \frac{|\{\mathfrak{p} \mid N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathfrak{p} \in S\}|}{|\{\mathfrak{p} \mid N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathfrak{p} \text{ prime}\}|}$$

if this limit exists. In the case $K = \mathbb{Q}$, the set S is a set of prime numbers and

$$\delta(S) = \lim_{x\to\infty} \frac{|\{p \leq x \mid p \in S\}|}{|\{p \leq x \mid p \text{ prime }\}|}.$$

Hence, if the density $\delta(S)$ in the theorem is positive, we easily deduce that the set S has to be infinite.

Note that if the natural density exists then it is equal to the Dirichlet density, but the converse is not true; there are cases where the Dirichlet density exists but the natural density does not. Originally, the statement of the Chebotarev Density Theorem referred to the Dirichlet density, but it was shown later that it is valid for either notion of density.

In the case L/K is abelian, we have the following.

Corollary 2.16. *Let L be an abelian extension of K and $\sigma \in \mathrm{Gal}(L/K)$. Then the set*

$$S = \{\mathfrak{p} \mid \mathfrak{p} \text{ a prime of } K, \mathfrak{p} \nmid \Delta_{L/K}, \sigma_{\mathfrak{p}} = \sigma\}$$

has density $\delta(S) = 1/[L:K]$ and hence is infinite.

Applying the previous corollary to the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, we obtain a famous theorem of Dirichlet.

Corollary 2.17. *For any $a \in (\mathbb{Z}/n\mathbb{Z})$, the set $\{p \mid p \equiv a \pmod{n}\}$ has density $1/\varphi(n)$.*

At last, let us state and prove the lemma that it is going to be widely used in the proof of the main theorem.

Lemma 2.18. *Let S be a set of prime numbers and let us partition the set S into pairwise disjoint sets $S_k \subset S$, where $k \geq 1$ and $S = \bigcup_{k=1}^{\infty} S_k$. For $D \subset S$, we define $D_k = D \cap S_k$, for $k \geq 1$. Then $S = \bigcup_{k=1}^{\infty} S_k$ and $S \setminus D = \bigcup_{k=1}^{\infty}(S_k \setminus D_k)$. If the sets S_k, D_k and S, where $k \geq 1$, have a natural density, and*

$$\delta(S) = \sum_{k=1}^{\infty} \delta(S_k),$$

then sets D, $S \setminus D$ have densities, as well. Moreover

$$\delta(D) = \sum_{k=1}^{\infty} \delta(D_k)$$

and

$$\delta(S \setminus D) = \sum_{k=1}^{\infty} \delta(S_k \setminus D_k).$$

Proof: Having that the sets S_k and D_k, where $k \geq 1$, have natural densities we obtain that the sets $S_k \setminus D_k$, where $k \geq 1$, have density, and

$$\delta(S_k \setminus D_k) = \delta(S_k) - \delta(D_k).$$

Both D and $S \setminus D$ are countable disjoint unions of sets of primes having a natural density. Hence, it follows that D has lower density $\delta_-(D) \geq \sum_{k=1}^{\infty} \delta(D_k)$, and that $S \setminus D$ has lower density $\delta_-(S \setminus D) \geq \sum_{k=1}^{\infty} \delta(S_k \setminus D_k)$. These lower densities add up to $\delta(S)$, so in fact they are densities. Indeed,

$$\begin{aligned}\delta_-(D)+\delta_-(S\setminus D) &\leq \delta(S)\\ &= \textstyle\sum_{k=1}^{\infty}\delta(S_k)\\ &= \textstyle\sum_{k=1}^{\infty}(\delta(D_k)+\delta(S_k\setminus D_k))\\ &= \textstyle\sum_{k=1}^{\infty}\delta(D_k)+\sum_{k=1}^{\infty}\delta(S_k\setminus D_k)\\ &\leq \delta_-(D)+\delta_-(S\setminus D).\end{aligned}$$

Hence

$$\delta_-(D)+\delta_-(S\setminus D)=\delta(S),$$

and

$$\delta(D)=\delta_-(D)=\sum_{k=1}^{\infty}\delta(D_k),$$

$$\delta(S\setminus D)=\delta_-(S\setminus D)=\sum_{k=1}^{\infty}\delta(S_k\setminus D_k). \qquad \square$$

2.2 Kummer Extensions and Kummer Theory

Let K be a number field. For an integer $n>1$, we denote with ζ_n an nth primitive root of unity. We assume that $\zeta_n\in K$.

Let a be a non-zero element of K and let $L=K(\sqrt[n]{a})$ be the splitting field of x^n-a. We have a map

$$\mathrm{Gal}(L/K)\hookrightarrow\langle\zeta_n\rangle$$

$$\sigma\mapsto\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

Note that this is independent of the choice of $\sqrt[n]{a}$, since choices differ by a root of unity, which is already in K. Moreover, this is a group homomorphism, hence the extension L/K is abelian.

Theorem 2.19. *Let a be a non-zero element of K and $L=K(\sqrt[n]{a})$ the splitting field of the polynomial x^n-a. There is a group homomorphism of $Gal(L/K)$ into $\langle\zeta_n\rangle$, given by $\sigma\mapsto\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$. In particular, if a is of order n in K^*/K^{*n}, the Galois group is cyclic of order n.*

Kummer theory gives that, conversely, if L/K is cyclic of degree n, and $\zeta_n\in K$, then there exists $\alpha\in L$ such that $L=K(\alpha)$ and $\alpha^n\in K$.

More generally, there is a bijection

$$\{L:K\subset L\subset K^{\mathrm{ab}},\mathrm{Gal}(L/K)^n=1\}\leftrightarrow\{W:K^{*n}\subset W\subset K^*\}$$

between abelian extensions L of K of exponent dividing n and subgroups $W\subset K^*$ containing K^{*n}, defined by

$$W\longmapsto K(\sqrt[n]{W})$$

$$L^{*n} \cap K^* \longleftrightarrow L.$$

If L corresponds to W, then we have a perfect pairing

$$\mathrm{Gal}(L/K) \times W/K^{*n} \to \langle \zeta_n \rangle$$

$$(\sigma, a) \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

That is,

$$\mathrm{Gal}(L/K) \cong \mathrm{Hom}(W/K^{*n}, \langle \zeta_n \rangle).$$

This pairing is Galois equivariant, as for $\varphi \in \mathrm{Aut}(\overline{K})$ we have

$$(\sigma, a)^{\varphi} = (\varphi\sigma\varphi^{-1}, \varphi a),$$

for any $a \in W/K^{*n}$.

We conclude this section with the Schinzel's theorem.

Theorem 2.20 (Schinzel)**.** *For $a \in K^*$, the polynomial $x^n - a$ has abelian splitting field over K if and only if $a^w \in K^{*n}$, with $w = \sharp(\langle \zeta_n \rangle \cap K)$.*

3 Main Theorem

Let α be a quadratic integer and K the corresponding quadratic field. Here, by a quadratic integer we mean an algebraic number whose minimal polynomial over $\mathbb{Q}$ is of degree 2. The Lucas sequence associated with α is the integer sequence

$$X_\alpha = \{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^n)\}_{n=0}^{\infty} = \{\alpha^n + \bar{\alpha}^n\}_{n=0}^{\infty},$$

where $\bar{\alpha}$ stands for the conjugate of α. This sequence satisfies the second order linear recurrence

$$x_{n+2} = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)x_{n+1} - \mathrm{N}_{K/\mathbb{Q}}(\alpha)x_n \quad \text{for } n \geq 0.$$

We will consider only non-degenerate sequences, so we assume that $\alpha/\overline{\alpha}$ is not a root of unity. We are interested in the existence of the natural density δ_α of the set of primes dividing at least one term of the sequence X_α. In particular, we show that δ_α exists for every α and we compute it for "generic" α.

First, we will prove that the density δ_α^+ of the primes that split completely in K and divide some term of X_α and the density δ_α^- of the primes that are inert in K and divide some term of X_α exist. Since there are only finitely many primes that ramify in K, they do not have any influence on the density, so we are not considering them. Finally, $\delta_\alpha = \delta_\alpha^+ + \delta_\alpha^-$.

This chapter will be dedicated to the proof of the main theorem.

Theorem 3.1. *The density δ_α exists for every non-zero quadratic integer α for which $\alpha/\overline{\alpha}$ is not a root of unity and it is a positive rational number.*

Along this proof, we will assume that $K \not\subset \mathbb{Q}(\zeta_8)$. The case when K is the quadratic subfield of $\mathbb{Q}(\zeta_8)$ will be studied in section 4.1.

We write $K = \mathbb{Q}(\sqrt{d})$, where d is a squarefree integer. Let p be a prime number coprime to α. We have

$$p \text{ divides } x_n = \alpha^n + \bar{\alpha}^n \Leftrightarrow (\alpha/\overline{\alpha})^n = -1 \in (\mathcal{O}/p\mathcal{O})^*.$$

Let us denote $q = \alpha/\overline{\alpha}$. We assume $p \nmid 2d$. In the following lemma we obtain the characterization of primes p that divide some term of X_α in terms of the order of $q \in (\mathcal{O}/p\mathcal{O})^*$.

Lemma 3.2. *Let p and α be as above. Then*

$$p \textit{ divides some term of } X_\alpha \Leftrightarrow \textit{ the order of } q = \alpha/\overline{\alpha} \in (\mathcal{O}/p\mathcal{O})^* \textit{ is even }.$$

Proof: Since $N_{K/\mathbb{Q}}(q) = 1$ we obtain that

$$q \in \kappa_p = \ker[N : (\mathcal{O}/p\mathcal{O})^* \to \mathbb{F}_p^*].$$

In the split case the group $(\mathcal{O}/p\mathcal{O})^* \cong \mathbb{F}_p^* \times \mathbb{F}_p^*$ is a product of two cyclic groups of order $p-1$ and the norm map $N : (\mathcal{O}/p\mathcal{O})^* \to \mathbb{F}_p^*$ is given by multiplication, so κ_p is the cyclic subgroup of $(\mathcal{O}/p\mathcal{O})^*$ of order $p-1$. On the other hand, in

the inert case $(\mathcal{O}/p\mathcal{O})^* \cong \mathbb{F}_{p^2}^*$ is a cyclic group of order p^2-1 and the norm map $N : (\mathcal{O}/p\mathcal{O})^* \to \mathbb{F}_p^*$ raises all elements to the power $p+1$. Here, we have that κ_p is a cyclic group of order $p+1$. Summarizing, we obtain that κ_p is cyclic group of order $p-(\frac{d}{p})$. Thus -1 is the unique element of order 2 in the group κ_p. This ends the proof of the lemma.

We will continue with the proof of the theorem. Both in the split and in the inert case, we will describe the parity of the order of $q \in (\mathcal{O}/p\mathcal{O})^*$ in terms of the splitting behavior of a prime p in some infinite algebraic extension of $\mathbb{Q}$.

Split case. Let

$$S^+ = \{p \,|\, p \text{ is an odd prime number, coprime to } \alpha \text{ that splits completely in } K\}$$

and

$$D^+ = \{p \in S^+ |\ p \text{ divides some term of } X_\alpha\} \subset S^+.$$

If $p \in S^+$, we have $(\mathcal{O}/p\mathcal{O})^* \cong \mathbb{F}_p^* \times \mathbb{F}_p^*$, so $q \in (\mathcal{O}/p\mathcal{O})^*$ has odd order if and only if q is 2^kth power in $(\mathcal{O}/p\mathcal{O})^*$, where $p-1$ has exactly $k = \mathrm{ord}_2(p-1)$ factors 2. Writing the last condition as $p \equiv 1 + 2^k \pmod{2^{k+1}}$, this leads us to a partition of the set S^+ into pairwise disjoint sets $S_k^+ \subset S^+$ such that

$$S_k^+ = \{p \in S^+ |\ p \equiv 1 + 2^k \,(\mathrm{mod}\ 2^{k+1})\}$$

and

$$S^+ = \bigcup_{k=1}^{\infty} S_k^+.$$

Since p splits completely in K, the condition $p \equiv 1 \pmod{2^k}$ implies that p splits completely in the field $K(\zeta_{2^k})$, obtained by adjoining to K a primitive 2^k root of unity. On the other hand, condition that p is not congruent to 1 modulo 2^{k+1} implies that p does not split completely in the field $K(\zeta_{2^{k+1}})$, obtained by adjoining to K a primitive 2^{k+1} root of unity. Finally, having the equivalence

$$\begin{array}{ll} p \equiv 1 + 2^k \,(\mathrm{mod}\ 2^{k+1}) \text{ and splits} & \Leftrightarrow \quad p \text{ splits completely in } K(\zeta_{2^k}), \\ \text{completely in } K & \text{but not in } K(\zeta_{2^{k+1}}), \end{array}$$

and using the Chebotarev density theorem, we obtain that the natural density of S_k^+ inside the set of all primes is

$$\delta(S_k^+) = [K(\zeta_{2^k}) : \mathbb{Q}]^{-1} - [K(\zeta_{2^{k+1}}) : \mathbb{Q}]^{-1}.$$

Taking into account that the this sum is a telescopic sum, we obtain

$$\sum_{k=1}^{\infty} \delta(S_k^+) = [K : \mathbb{Q}]^{-1} = 1/2 = \delta(S^+).$$

Now, for $p \in S_k^+$, we have

the order of $q \in (\mathcal{O}/p\mathcal{O})^*$ is odd	$\Leftrightarrow$	q is a 2^kth power in $(\mathcal{O}/p\mathcal{O})^*$
	$\Leftrightarrow$	p splits completely in the field $K(\zeta_{2^k}, \sqrt[2^k]{q})$,

and finally

$p \in S_k^+$ does not divide some term of X_α	$\Leftrightarrow$	p splits completely in the field $K(\zeta_{2^k}, \sqrt[2^k]{q})$, but not in the field $K(\zeta_{2^{k+1}}, \sqrt[2^k]{q})$.

We denote

$$D_k^+ = D^+ \cap S_k^+.$$

Using the Chebotarev density theorem, we obtain that the complement of D_k^+ in S_k^+ has natural density

$$\delta(S_k^+ \setminus D_k^+) = [K(\zeta_{2^k}, \sqrt[2^k]{q}) : \mathbb{Q}]^{-1} - [K(\zeta_{2^{k+1}}, \sqrt[2^k]{q}) : \mathbb{Q}]^{-1}.$$

From here, we obtain that the set D_k^+ has a density as well. We have

$$D^+ = \bigcup_{k=1}^{\infty} D_k^+$$

and

$$S^+ \setminus D^+ = \bigcup_{k=1}^{\infty} (S_k^+ \setminus D_k^+).$$

By lemma 2.18,

$$\delta(D^+) = \sum_{k=1}^{\infty} \delta(D_k^+)$$

and

$$\delta(S^+ \setminus D^+) = \sum_{k=1}^{\infty} \delta(S_k^+ \setminus D_k^+).$$

Having

$$\delta_\alpha^+ = \delta(D^+) = \delta(S^+) - \delta(S^+ \setminus D^+) = \frac{1}{2} - \delta(S^+ \setminus D^+)$$

we conclude

$$\delta_\alpha^+ = \frac{1}{2} - \sum_{k=1}^{\infty} ([K(\zeta_{2^k}, \sqrt[2^k]{q}) : \mathbb{Q}]^{-1} - [K(\zeta_{2^{k+1}}, \sqrt[2^k]{q}) : \mathbb{Q}]^{-1}). \tag{1}$$

If we denote

$$F_k = K(\zeta_{2^k}, \sqrt[2^k]{q})$$

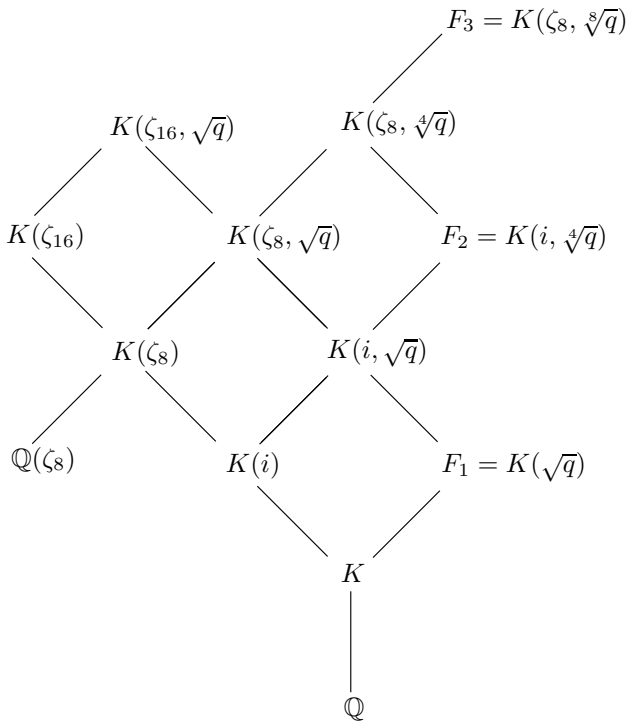
we obtain

$$\delta(S_k^+ \setminus D_k^+) = \begin{cases} \frac{1}{2}[F_k : \mathbb{Q}]^{-1} & \text{if } \zeta_{2^{k+1}} \notin F_k \\ 0 & \text{otherwise.} \end{cases}$$

We will prove that there exists $N \in \mathbb{Z}_{\geq 1}$ such that for all $k \geq N$, a primitive root of unity $\zeta_{2^{k+1}}$ generates a quadratic extension over F_k and $[F_{k+1} : F_k] = 4$. In particular, we obtain that for $k > N$, the extension $F_k = K(\zeta_{2^k}, \sqrt[2^k]{q})$ is nontrivial extension over $K(\zeta_{2^k})$, and this will be used later in the proof.

Having that $[K(\zeta_{2^k}) : \mathbb{Q}] = 2^k$ for all k, it is enough to consider the extension $F_k/K(\zeta_{2^k})$.

We have the diagram



For $k = 1$, we have

$$[F_1 : K] = 2 \Leftrightarrow q \notin K^{*2}.$$

If $k = 2$, by Kummer theory,

$$[F_2 : K(i)] = 4 \Leftrightarrow [K(i, \sqrt{q}) : K(i)] = 2,$$

and we obtain

$$[F_2 : K(i)] = 4 \Leftrightarrow q \notin \langle -1 \rangle \cdot K^{*2}.$$

Now, let $k = 3$. Again, applying Kummer theory,

$$[F_3 : K(\zeta_8)] = 8 \Leftrightarrow [K(\zeta_8, \sqrt{q}) : K(\zeta_8)] = 2.$$

On the other hand,

$$[K(\zeta_8, \sqrt{q}) : K(\zeta_8)] = 2 \Leftrightarrow [K(i, \sqrt{q}] : K(i)] = 2 \wedge K(\zeta_8) \neq K(i, \sqrt{q}).$$

The field $K(\zeta_8, \sqrt{q})$ is the compositum of the V_4 extensions $\mathbb{Q}(\zeta_8)$ and $K(\sqrt{q})$ of $\mathbb{Q}$, so the fields $K(\zeta_8)$ and $K(i, \sqrt{q})$ coincide if and only if one of the quadratic subfields $\mathbb{Q}(\sqrt{q} \pm 1/\sqrt{q})$ of $K(\sqrt{q})$ is equal to one of the three quadratic subfields of $\mathbb{Q}(\zeta_8)$. We have

$$[F_3 : K(\zeta_8)] = 8 \Leftrightarrow q \notin \langle -1 \rangle \cdot K^{*2} \wedge \mathrm{Tr}(q) \pm 2 \notin \langle -1, 2 \rangle \cdot \mathbb{Q}^{*2}.$$

Proposition 3.3. *If* $[F_3 : K(\zeta_8)] = 8$*, then* $[F_k : K(\zeta_{2^k})] = 2^k$*, for all* $k \geq 1$*.*

Proof: If $K(\zeta_8, \sqrt{q})$ is quadratic over $K(\zeta_8)$, then it is a V_4 extension over $K(i)$, so it is not equal to $K(\zeta_{16})$, which is C_4 extension over $K(i)$. From here, the proof easily follows by induction.

Thus, if for $1 \leq k \leq 3$, no "accident" happens, i.e. the extension F_k is of the maximal degree 4^k over $\mathbb{Q}$, then $[F_k : \mathbb{Q}] = 4^k$ for all $k \geq 1$.

Moreover, if only in the case $k = 3$ an "accident" happens, i.e. the extensions $\mathbb{Q}(\zeta_8)$ and $K(\sqrt{q})$ are not linearly disjoint over $\mathbb{Q}$, we have the following statement.

Proposition 3.4. *If* $q \notin \langle -1 \rangle \cdot K^{*2}$*, but* $[F_3 : K(\zeta_8)] = 4$*, then* $[F_k : K(\zeta_{2^k})] = 2^{k-1}$*, for all* $k \geq 3$*.*

Proof: If $K(\zeta_8, \sqrt[4]{q}) = K(\zeta_{16})$, then $x^4 - q$ has an abelian splitting field over K which is, by Schinzel's theorem, equivalent to $q^2 \in K^4$, i.e. $q \in \langle -1 \rangle \cdot K^2$. □

Now, we can consider the general case. We write $q = \pm q_0^{2^s}$, where $s \in \mathbb{Z}_{\geq 0}$ and $q_0 \notin \langle -1 \rangle \cdot K^{*2}$. Then, if $q = q_0^{2^s}$, for $k \leq s$, the extension $F_k / K(\zeta_2^k)$ is trivial. On the other hand, for $q = -q_0^{2^s}$, we obtain $[F_k : K(\zeta_{2^k})] = 2$, if $k \leq s$. In the case $k \geq s+1$, the extensions $K(\zeta_2^k, \sqrt[2^k]{q}) / K(\zeta_{2^k})$ and $K(\zeta_2^k, \sqrt[2^k]{-q}) / K(\zeta_{2^k})$ have the same degree. Using propositions 3.3 and 3.4, we obtain the following.

Theorem 3.5. *If* $q = \pm q_0^{2^s}$*, where* $s \in \mathbb{Z}_{\geq 0}$ *and* $q_0 \notin \langle -1 \rangle \cdot K^{*2}$*, then for* $k \geq \max\{3, s+1\}$

$$[F_k : \mathbb{Q}] = \begin{cases} 2^{2k-s} & \text{if } Tr(q_0) \pm 2 \notin \langle -1, 2 \rangle \cdot \mathbb{Q}^{*2}, \\ 2^{2k-1-s} & \text{if } Tr(q_0) \pm 2 \in \langle -1, 2 \rangle \cdot \mathbb{Q}^{*2}. \end{cases}$$

It easily follows, that if $k \geq N = \max\{3, s+1\}$, then

$$[F_{k+1} : F_k] = 4,$$

and

$$[F_k(\zeta_{2^{k+1}}) : F_k] = 2.$$

Hence, using (1), we obtain

$$\delta_\alpha^+ = \frac{1}{2} - \Big(\sum_{k=1}^{N} \delta(S_k^+ \setminus D_k^+) + \frac{1}{2} \sum_{k=N}^{\infty} \frac{1}{2^{2k-m}}\Big),$$

where

$$m = \begin{cases} s & \text{if } \mathrm{Tr}(q_0) \pm 2 \notin \langle -1, 2 \rangle \cdot \mathbb{Q}^{*2}, \\ s-1 & \text{if } \mathrm{Tr}(q_0) \pm 2 \in \langle -1, 2 \rangle \cdot \mathbb{Q}^{*2}. \end{cases}$$

Thus $\delta_\alpha^+ \in \mathbb{Q}$.

To prove that $\delta_\alpha^+ > 0$, it is enough to prove that for some $k \in \mathbb{Z}_{\geq 1}$, $\delta(D_k^+) > 0$. Having, $\delta(D_k^+) = \delta(S_k^+) - \delta(S_k^+ \setminus D_k^+)$, for $k > N$, we obtain

$$\delta(D_k^+) = \frac{1}{2}[K(\zeta_{2^k}) : \mathbb{Q}]^{-1}(1 - \frac{1}{2^{k-m}}) = \frac{1}{2^{k+1}}(1 - \frac{1}{2^{k-m}}),$$

and since $k - m > 0$, we obtain $\delta(D_k^+) > 0$, and moreover $\delta_\alpha^+ > 0$.

On the other hand, $\delta_\alpha^+ < \frac{1}{2}$, since for $k \geq N$, the density

$$\delta(S_k^+ \setminus D_k^+) = \frac{1}{2^{2k-m+1}} > 0.$$

Inert case. Let p be an odd prime that is inert in $K/\mathbb{Q}$. Then, p is coprime to α and $q \in (\mathcal{O}/p\mathcal{O})^*$. Let

$$S^- = \{p \mid p \text{ odd prime inert in } K\}$$

and

$$D^- = \{p \in S^- \mid p \text{ divides some term of } X_\alpha\} \subset S^-.$$

Suppose first that $p \equiv 1 \pmod 4$. We denote

$$S_1^- = \{p \in S^- \mid p \equiv 1 \pmod 4\}$$

and

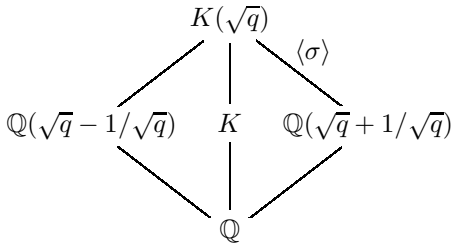
$$D_1^- = D^- \cap S_1^-.$$

We easily obtain $\delta(S_1^-) = \frac{1}{4}$.

Having that $N_{K/\mathbb{Q}}(q) = 1$, we obtain $q^{p+1} = 1 \in (\mathcal{O}/p\mathcal{O})^*$. Since κ_p is a subgroup of the cyclic group $(\mathcal{O}/p\mathcal{O})^*$ of index $p-1$, all the elements in κ_p are $p-1$th powers. In particular, $q = x^2 \in (\mathcal{O}/p\mathcal{O})^*$. Then $N(x) = x^{p+1} = q^{\frac{p+1}{2}} = \pm 1 \in (\mathcal{O}/p\mathcal{O})^*$, where N is the norm map $N : (\mathcal{O}/p\mathcal{O})^* \to \mathbb{F}_p^*$. As $\frac{p+1}{2}$ is odd, we have the equivalence

$$\text{the order of } q \text{ is odd} \Leftrightarrow N(x) = 1.$$

Let us consider the extension $K(\sqrt{q})/\mathbb{Q}$. Since $N_{K/\mathbb{Q}}(q) = 1$, by lemma 2.9, this extension is normal, hence Galois. Moreover, it is abelian. If $\sigma_p \in \mathrm{Gal}(K(\sqrt{q})/\mathbb{Q})$ is the Frobenius element of p, restricting it to the field K, we obtain the Frobenius element of p in the abelian group $\mathrm{Gal}(K/\mathbb{Q})$. We have the diagram



Note that this diagram may collapse, in the case $\sqrt{q} \in K$. Otherwise it is V_4.

Using that

$$\sigma_p \mid_K = id \Leftrightarrow \text{ } p \text{ splits completely in } K,$$

we obtain the equivalence

p is inert in $K/\mathbb{Q}$	$\Leftrightarrow$	the Frobenius element σ_p of p in the abelian group $\mathrm{Gal}(K(\sqrt{q})/\mathbb{Q})$ is such that $\sigma_p \mid_K \neq id$.

For inert p, the equivalence

$$N(x) = 1 \Leftrightarrow \sigma_p(\sqrt{q}) = (\sqrt{q})^{-1}$$

shows that the condition $\mathrm{N}(x) = 1$ determines σ_p uniquely. Hence, if $p \equiv 1 \pmod 4$ is a prime that is inert in $K/\mathbb{Q}$, we have

p is does not divide some term of X_α	$\Leftrightarrow$	the Frobenius element σ_p of p in the abelian group $\mathrm{Gal}(K(\sqrt{q})/\mathbb{Q})$ is the unique element σ such that $\sigma(\sqrt{q}) = (\sqrt{q})^{-1}$.

If the fields K, $\mathbb{Q}(\sqrt{q} - 1/\sqrt{q})$, $\mathbb{Q}(\sqrt{q} + 1/\sqrt{q})$ are linearly disjoint over $\mathbb{Q}$, i.e. q is not a square in K, then for prime $p \equiv 1 \pmod 4$ we have

$$\sigma_p = \sigma \Leftrightarrow p \text{ splits in } \mathbb{Q}(\sqrt{q} + 1/\sqrt{q})/\mathbb{Q} \text{ and is inert in } \mathbb{Q}(\sqrt{q} - 1/\sqrt{q})/\mathbb{Q}.$$

Hence we have to consider the case when one of the fields $\mathbb{Q}(\sqrt{q}+1/\sqrt{q})$, $\mathbb{Q}(\sqrt{q}-1/\sqrt{q})$ equals $\mathbb{Q}(\sqrt{-1})$ separately.

For $\mathbb{Q}(\sqrt{q} - 1/\sqrt{q}) = \mathbb{Q}(\sqrt{-1})$, no prime $p \equiv 1 \pmod 4$ is inert in $\mathbb{Q}(\sqrt{q} - 1/\sqrt{q})/\mathbb{Q}$, so the density $\delta(S_1^- \setminus D_1^-) = 0$.

If $\mathbb{Q}(\sqrt{q} + 1/\sqrt{q}) = \mathbb{Q}(\sqrt{-1})$, every prime $p \equiv 1 \pmod 4$ splits in $\mathbb{Q}(\sqrt{q} + 1/\sqrt{q})/\mathbb{Q}$, so the density $\delta(S_1^- \setminus D_1^-) = \frac{1}{4}$.

In the case K, $\mathbb{Q}(\sqrt{q} - 1/\sqrt{q})$, $\mathbb{Q}(\sqrt{q} + 1/\sqrt{q}) \neq \mathbb{Q}(\sqrt{-1})$, using the Chebotarev density theorem, we deduce

$$\delta(S_1^- \setminus D_1^-) = \frac{1}{2} \cdot \frac{1}{[K(\sqrt{q}) : \mathbb{Q}]} = \begin{cases} \frac{1}{4} & \text{if } q \text{ is a square in } K, \\ \frac{1}{8} & \text{otherwise,} \end{cases}$$

where $\frac{1}{2}$ arises from the density of primes $p \equiv 1 \pmod 4$.

Next, we assume $p \equiv 3 \pmod 4$ and we follow the argument similarly to the split case.

If $p \in S^-$, we have that $q \in (\mathcal{O}/p\mathcal{O})^*$ has odd order if and only if q is a 2^lth power in $(\mathcal{O}/p\mathcal{O})^*$, where $p^2 - 1$ has exactly $l = \mathrm{ord}_2(p^2 - 1)$ factors 2. The condition $p \equiv 3 \pmod 4$ implies $\mathrm{ord}_2(p - 1) = 1$, so $l = \mathrm{ord}_2(p + 1) + 1 \geq 2$.

Using the equivalence $k = \mathrm{ord}_2(p+1) \Leftrightarrow p \equiv -1 + 2^k \pmod{2^{k+1}}$ we partition the set S^- as

$$S^- = \bigcup_{k=1}^{\infty} S_k^-,$$

where

$$S_k^- = \{p \in S^- |\ p \equiv -1 + 2^k \,(\mathrm{mod}\ 2^{k+1})\}.$$

We denote

$$D_k^- = D^- \cap S_k^-.$$

Note, that the case $k = 1$ is the case $p \equiv 1\,(\mathrm{mod}\ 4)$, so we only consider the case $k \geq 2$.

We consider the Frobenius element σ_p of an unramified prime p in the abelian group $\mathrm{Gal}(K(\zeta_{2^{k+1}})/\mathbb{Q})$. Reasoning as in the case $p \equiv 1\,(\mathrm{mod}\ 4)$ we obtain the equivalence

$$\begin{array}{lcl} p \text{ inert in } K/\mathbb{Q} & \Leftrightarrow & \text{the Frobenius element } \sigma_p \text{ of } p \text{ in the abelian} \\ & & \text{group } \mathrm{Gal}(K(\zeta_{2^{k+1}})/\mathbb{Q}) \text{ is such that } \sigma_p\,|_K \neq id. \end{array}$$

For $p \equiv -1 + 2^k \pmod{2^{k+1}}$, we have $\sigma(\zeta_{2^{k+1}}) = \zeta_{2^{k+1}}^{-1+2^k}$. This completely determines σ_p for $p \in S_k^-$, and we obtain the equivalence

$$\begin{array}{lcl} p \in S_k^- & \Leftrightarrow & \text{the Frobenius element } \sigma_p \text{ of } p \text{ in the abelian group} \\ & & \mathrm{Gal}(K(\zeta_{2^{k+1}})/\mathbb{Q}) \text{ is the unique element } \sigma \text{ such that} \\ & & \sigma|_K \neq id \text{ and } \sigma(\zeta_{2^{k+1}}) = \zeta_{2^{k+1}}^{-1+2^k}. \end{array} \qquad (2)$$

Using the Chebotarev density theorem we obtain that S_k^- has natural density

$$\delta(S_k^-) = [K(\zeta_{2^{k+1}}) : \mathbb{Q}]^{-1} = \frac{1}{2^{k+1}}, \quad \text{for all } k \geq 2.$$

Let $B_k \subset K(\zeta_{2^{k+1}})$ be the subfield fixed by σ. Since the order of σ in $\mathrm{Gal}(K(\zeta_{2^{k+1}})/\mathbb{Q})$ is 2, we obtain that $K(\zeta_{2^{k+1}})$ is a quadratic extension of B_k and, since $q \notin B_k$, we have $K(\zeta_{2^{k+1}}) = B_k(q)$. The construction of B_k yields

$$p \in S_k^- \Leftrightarrow p \text{ splits completely in } B_k, \text{ but not in } K(\zeta_{2^{k+1}})$$

and the fact that primes in S_k^- are inert in $K/\mathbb{Q}$ then implies that their extensions in B_k are inert in $B_k(q)$. More precisely, we have the equivalence

$$\begin{array}{lcl} p \in S_k^- & \Leftrightarrow & p \text{ splits completely in } B_k \text{ and has extensions in } B_k \\ & & \text{that are inert in } K(\zeta_{2^{k+1}}) = B_k(q). \end{array}$$

We have

$$\begin{array}{lcl} \text{the order of } q \in (\mathcal{O}/p\mathcal{O})^* \text{ is odd} & \Leftrightarrow & q \text{ is a } 2^{k+1}\text{th power in} \\ & & (\mathcal{O}/p\mathcal{O})^*. \end{array}$$

We have already proved that there exists an integer $N \in \mathbb{Z}_{\geq 1}$, such that for $k \geq N$, an element $\sqrt[2^{k+1}]{q}$ generates a nontrivial extension over $K(\zeta_{2^{k+1}})$. Let $q = q_0^{2^s}$, where $s \in \mathbb{Z}_{\geq 0}$ and $q_0 \notin \langle -1 \rangle \cdot K^{*2}$. Then, as we have $k+1$ rather then k here, $N = \max\{2, s+1\}$. Moreover, for $k \geq N$ we have

$$\mathrm{Gal}(K(\zeta_{2^{k+1}}, \sqrt[2^{k+1}]{q})/K(\zeta_{2^{k+1}})) \cong \mathbb{Z}/2^n\mathbb{Z},$$

where

$$n = \begin{cases} k+1-s & \text{if } \mathrm{Tr}(q_0) \pm 2 \notin \langle -1, 2 \rangle \cdot \mathbb{Q}^{*2}, \\ k-s & \text{if } \mathrm{Tr}(q_0) \pm 2 \in \langle -1, 2 \rangle \cdot \mathbb{Q}^{*2}. \end{cases}$$

Let $k \geq N$. For $p \in S_k^-$ and $\mathfrak{p} \subset \mathcal{O}_{K(\zeta_{2^{k+1}})}$ such that $\mathfrak{p} \mid p$, the fields $\mathcal{O}_{K(\zeta_{2^{k+1}})}/\mathfrak{p}\mathcal{O}_{K(\zeta_{2^{k+1}})}$ and $\mathcal{O}_K/p\mathcal{O}_K$ are fields of p^2 elements, so we obtain

the order of $q \in (\mathcal{O}/p\mathcal{O})^*$ is odd	$\Leftrightarrow$	the extensions of $p \in S_k^-$ in $K(\zeta_{2^{k+1}})$ split completely in $K(\zeta_{2^{k+1}}, \sqrt[2^{k+1}]{q})$

and finally

$p \in S_k^-$ does not divide some term of X_α	$\Leftrightarrow$	p splits completely in $B_k/\mathbb{Q}$ and has extensions in B_k that are inert in $B_k(q)/B_k$ and split completely in $K(\zeta_{2^{k+1}}, \sqrt[2^{k+1}]{q})/B_k(q)$.

Let us denote $F_k = K(\zeta_{2^{k+1}}, \sqrt[2^{k+1}]{q})$. Note that there is a slight difference in the definition of F_k between this and the split case. We want to translate the last condition in terms of Frobenius symbol of p in $\mathrm{Gal}(F_k/\mathbb{Q})$. Since $F_k/\mathbb{Q}$ is not an abelian extension, the Frobenius symbol of p will be unique only up to conjugacy. We have

$p \in S_k^-$ does not divide some term of X_α	$\Leftrightarrow$	the Frobenius symbol of p in $\mathrm{Gal}(F_k/\mathbb{Q})$ is an element of order 2 in the normal subgroup $\mathrm{Gal}(F_k/B_k)$, that does not lie in the normal subgroup $\mathrm{Gal}(F_k/B_k(q))$.

Note that the condition on the Frobenius symbol of p does not depend on the choice inside the conjugacy class.

If n_k denotes the number of such elements and we denote

$$D_k^- = D^- \cap S_k^-,$$

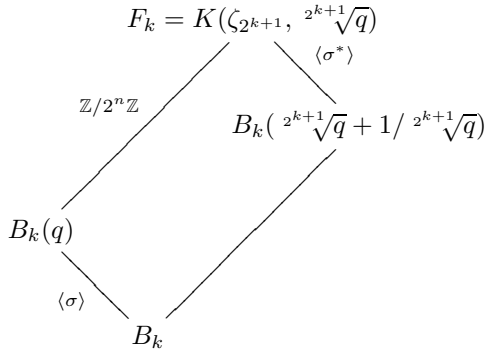
The Chebotarev density theorem implies

$$\delta(S_k^- \setminus D_k^-) = \frac{n_k}{[F_k : \mathbb{Q}]}.$$

We can extend σ to an element $\sigma^* \in \mathrm{Gal}(F_k/B_k)$ of order 2 by putting

$$\sigma^*(\sqrt[2^{k+1}]{q}) = 1/\sqrt[2^{k+1}]{q},$$

as shown in the diagram



The automorphism σ^* acts by inversion on $\langle q\rangle$, and by raising to the $-1+2^k$th power on $\langle\zeta_{2^{k+1}}\rangle$.

We obtain

$$\mathrm{Gal}(F_k/B_k) \cong \mathrm{Gal}(F_k/B_k(q)) \rtimes \langle\sigma^*\rangle \cong \mathbb{Z}/2^n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z},$$

and the action of σ^* on $\mathrm{Gal}(F_k/B_k(q))$ follows from the Galois equivariance of the Kummer pairing

$$\mathrm{Gal}(F_k/B_k(q)) \times \langle q\rangle \to \langle\zeta_{2^{k+1}}.\rangle$$

For σ^* acts on $\mathrm{Gal}(F_k/B_k(q))$ by raising to some power x, and

$$x \times -1 = -1 + 2^k,$$

we obtain that σ^* acts on $\mathrm{Gal}(F_k/B_k(q))$ by raising to the $1-2^k$th power.

Let φ be a generator of $\mathrm{Gal}(F_k/B_k(q))$. We are searching for the elements $(\varphi^r, \sigma^*) \in \mathrm{Gal}(F_k/B_k)$ of order 2, where $r \in \{0, 2^n - 1\}$. So, we have

$$\begin{array}{lcl}
(\varphi^r, \sigma^*) \text{ has order } 2 & \Leftrightarrow & \varphi^r\sigma^*\varphi^r\sigma^* = id \\
& \Leftrightarrow & \varphi^{r(2^k-2)} = id \\
& \Leftrightarrow & 2^n \mid r(2^k-2) \\
& \Leftrightarrow & r = 0 \vee r = 2^{n-1}.
\end{array}$$

This yields $n_k = 2$ for all $k \geq N$.

Having

$$\delta(S_1^-) + \sum_{k\geq 2}^{\infty} \delta(S_k^-) = \frac{1}{4} + \sum_{k\geq 2}^{\infty} \frac{1}{2^{k+1}} = \frac{1}{2} = \delta(S^-),$$

we can use lemma 2.18, so we obtain

$$\delta_\alpha^- = \frac{1}{2} - (\sum_{k=1}^{N} \delta(S_k^- \setminus D_k^-) + \sum_{k=N}^{\infty} \frac{n_k}{[F_k : \mathbb{Q}]}) = \frac{1}{2} - (\sum_{k=1}^{N} \delta(S_k^- \setminus D_k^-) + \sum_{k=N}^{\infty} \frac{2}{2^{k+1+n}}).$$

As the last term is a geometric series, we obtain $\delta_\alpha^- \in \mathbb{Q}$ and $\delta_\alpha \in \mathbb{Q}$. Moreover, we have that for $k \geq N$,

$$\delta(S_k^- \setminus D_k^-) = \frac{2}{2^{k+1+n}} > 0,$$

so $\delta_\alpha^- < \frac{1}{2}$ and $0 < \delta_\alpha < 1$. $\square$

4 Explicit computations

4.1 The case $K \subset \mathbb{Q}(\zeta_8)$

In this section, we will point out the changes that have to be made in order to extend the proof of the main theorem to the case $K \subset \mathbb{Q}(\zeta_8)$.

Split case. Here, we will modify the proof of the existence of $N \in \mathbb{Z}_{\geq 1}$ such that $[F_{k+1} : F_k] = 4$, for all $k \geq N$.

Let $K = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$. Then, for $K(i) = K$, we have

$$[F_2 : K(i)] = 4 \Leftrightarrow q \notin K^{*2}.$$

If $k = 3$, we obtain

$$[F_3 : K(\zeta_8)] = 8 \Leftrightarrow q \notin \langle i \rangle \cdot K^{*2}$$

Now, proposition 3.3 remains true and we obtain the following theorem.

Theorem 4.1. *If $q = i^k q_0^{2^s}$, where $s \in \mathbb{Z}_{\geq 0}$ and $q_0 \notin \langle i \rangle \cdot K^{*2}$, then for $k \geq N = \max\{3, s+2\}$*

$$[F_k : \mathbb{Q}] = 2^{2k-1-s}.$$

Thus,

$$\delta_\alpha^+ = \frac{1}{2} - (\sum_{k=1}^{N} \delta(S_k^+ \setminus D_k^+) + \frac{1}{2} \sum_{k=N}^{\infty} \frac{1}{2^{2k-1-s}}),$$

and, if $k \geq N$,

$$\delta(D_k^+) = \frac{1}{2}[K(\zeta_{2^k}) : \mathbb{Q}]^{-1}(1 - \frac{1}{2^{k-1-s}}) = \frac{1}{2^k}(1 - \frac{1}{2^{k-1-s}}).$$

In the case $K = \mathbb{Q}(\sqrt{\pm 2})$, the only difference is the case $k = 3$, since $K(\zeta_8) = K(i)$. We have

$$[F_3 : K(\zeta_8)] = 8 \Leftrightarrow q \notin \langle -1 \rangle \cdot K^{*2}.$$

Instead of proposition 3.3, we obtain the following statement.

Proposition 4.2. *If $q \notin \langle -1 \rangle \cdot K^{*2}$, then $[F_k : K(\zeta_{2^k})] = 2^k$, for all $k \geq 1$.*

The proof follows the same argument, only we consider extensions over K, instead over $K(i)$.
Hence, the theorem.

Theorem 4.3. *If $q = \pm q_0^{2^s}$, where $s \in \mathbb{Z}_{\geq 0}$ and $q_0 \notin \langle -1 \rangle \cdot K^{*2}$, then for $k \geq N = \max\{3, s+1\}$*

$$[F_k : \mathbb{Q}] = 2^{2k-1-s}.$$

We obtain

$$\delta_\alpha^+ = \frac{1}{2} - (\sum_{k=1}^{N} \delta(S_k^+ \setminus D_k^+) + \frac{1}{2} \sum_{k=N}^{\infty} \frac{1}{2^{2k-1-s}}),$$

and for $k \geq N$

$$\delta(D_k^+) = \frac{1}{2^k}(1 - \frac{1}{2^{k-1-s}}).$$

In both cases, we have $\delta_\alpha^+ \in \mathbb{Q}$ and $0 < \delta_\alpha^+ < \frac{1}{2}$.

Inert case. First, we assume $p \equiv 1 \pmod 4$.

Here, the only problem that can arise is the case $K = \mathbb{Q}(\sqrt{-1})$, since then there are no inert primes that are congruent to 1 modulo 4. Thus, then we have $\delta(S_1^-) = \delta(S_1^- \setminus D_1^-) = 0$.

Now, suppose $p \equiv 3 \pmod 4$.

First, we can observe that in the equivalence (2) from the proof of the main theorem, if p is an odd prime, its Frobenius element σ_p in the abelian group $\mathrm{Gal}(K(\zeta_{2^{k+1}})/\mathbb{Q})$ =$\mathrm{Gal}(\mathbb{Q}(\zeta_{2^{k+1}})/\mathbb{Q})$ is given by $\sigma_p(\zeta_{2^{k+1}}) = \zeta_{2^{k+1}}^p$. If $p \in S_k^-$, then σ_p is the unique element σ such that $\sigma(\zeta_{2^{k+1}}) = \zeta_{2^{k+1}}^{-1+2^k}$. For some k, the condition $\sigma \mid_K \neq id$ may not be satisfied and we have $S_k^- = \emptyset$.

Next, to use lemma 2.18, we need

$$\delta(S_1^-) + \sum_{k\geq 2}^{\infty} \delta(S_k^-) = \frac{1}{2} = \delta(S^-).$$

For $K = \mathbb{Q}(\sqrt{-1})$, all primes $p \equiv 3 \pmod 4$ are inert in $K/\mathbb{Q}$. We have

$$\delta(S_k^-) = [K(\zeta_{2^{k+1}}) : \mathbb{Q}]^{-1} = \frac{1}{2^k} \quad \text{for all } k \geq 2,$$

and $S_1^- = \emptyset$, so

$$\delta(S_1^-) + \sum_{k\geq 2}^{\infty} \delta(S_k^-) = \sum_{k\geq 2}^{\infty} \frac{1}{2^k} = \frac{1}{2} = \delta(S^-).$$

Let $K = \mathbb{Q}(\sqrt{2})$. For $k = 2$, $p \equiv 3 \pmod 8$, so p is inert in $K/\mathbb{Q}$. For $k \geq 3$, $p \equiv 7 \pmod 8$, so p splits in $K/\mathbb{Q}$. We obtain

$$\delta(S_2^-) = [\mathbb{Q}(\zeta_8) : \mathbb{Q}]^{-1} = \frac{1}{4}$$

and

$$S_k^- = \emptyset \quad \text{for all } k \geq 3,$$

so

$$\delta(S_k^-) = \delta(S_k^- \setminus D_k^-) = 0 \quad \text{for all } k \geq 3.$$

We have

$$\delta(S_1^-) + \sum_{k\geq 2}^{\infty} \delta(S_k^-) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2} = \delta(S^-).$$

Let $K = \mathbb{Q}(\sqrt{-2})$. For $k = 2$, $p \equiv 3 \pmod 8$, so p splits in $K/\mathbb{Q}$. For $k \geq 3$, $p \equiv 7 \pmod 8$, so p is inert in $K/\mathbb{Q}$. We obtain

$$S_2^- = \emptyset,$$

so

$$\delta(S_2^-) = \delta(S_2^- \setminus D_2^-) = 0,$$

and

$$\delta(S_k^-) = [K(\zeta_{2^{k+1}}) : \mathbb{Q}]^{-1} = \frac{1}{2^k} \quad \text{for all } k \geq 3.$$

We have

$$\delta(S_1^-) + \sum_{k\geq 3}^{\infty} \delta(S_k^-) = \frac{1}{4} + \sum_{k\geq 3}^{\infty} \frac{1}{2^k} = \frac{1}{2} = \delta(S^-).$$

Summarizing, we conclude that if $K = \mathbb{Q}(\sqrt{2})$, we have

$$\delta_\alpha^- = \frac{1}{2} - (\sum_{k=1}^{2} \delta(S_k^- \setminus D_k^-)),$$

and otherwise

$$\delta_\alpha^- = \frac{1}{2} - (\sum_{k=1}^{N} \delta(S_k^- \setminus D_k^-) + \sum_{k=N}^{\infty} \frac{2}{2^{2k+1-s}}).$$

Whence, $\delta_\alpha \in \mathbb{Q}_{>0}$.

4.2 Generic case

Let us define generic case as the case where no "anomalies" happen. By this, we mean that the extension $F_k = K(\zeta_{2^k}, \sqrt[2^k]{q})/\mathbb{Q}$ has maximal degree for every k, i.e. to have the following diagram

$$\begin{array}{c} F_k = K(\zeta_{2^k}, \sqrt[2^k]{q}) \\ \Big| \, 2^k \\ K(\zeta_{2^k}) \\ \Big| \, 2 \\ \mathbb{Q}(\zeta_{2^k}) \\ \Big| \, 2^{k-1} \\ \mathbb{Q} \end{array}$$

Proposition (3.3) implies that if F_k has maximal degree for $1 \leq k \leq 3$, then the degree will remain maximal for every k. Hence, the definition.

Definition 4.4. *A non-zero quadratic integer α is said to be generic if the following conditions are satisfied:*

(i) The corresponding quadratic field $K = \mathbb{Q}(\alpha) \not\subset \mathbb{Q}(\zeta_8)$.

(ii) $q \notin \langle -1 \rangle \cdot K^{*2}$.

(iii) $\mathbb{Q}(\sqrt{q} - 1/\sqrt{q})$, $\mathbb{Q}(\sqrt{q} + 1/\sqrt{q}) \not\subset \mathbb{Q}(\zeta_8)$.

The conditions (ii) and (iii) in the definition above can be replaced by equivalent conditions on $\mathrm{N}(\alpha)$ and $\mathrm{Tr}(q)$, and we obtain the following theorem.

Theorem 4.5. *A non-zero quadratic integer α is generic if and only if following conditions are satisfied:*

(i) *The corresponding quadratic field $K = \mathbb{Q}(\alpha) \neq \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$,$\mathbb{Q}(\sqrt{-2})$.*

(ii) $\mathrm{N}(\alpha) \notin \langle -1, d \rangle \cdot \mathbb{Q}^{*2}$, *where d is the discriminant of the field K over $\mathbb{Q}$.*

(iii) $\mathrm{Tr}(q) \pm 2 \notin \langle -1, 2 \rangle \cdot \mathbb{Q}^{*2}$.

Proof: By lemma 2.14 condition (i) is equivalent to condition $K \not\subset \mathbb{Q}(\zeta_8)$ in definition 4.4.

Next, having $q = \frac{\alpha}{\overline{\alpha}} = \frac{\alpha^2}{\mathrm{N}(\alpha)}$, we obtain that $q \notin \langle -1 \rangle \cdot K^{*2}$ if and only if $\mathrm{N}(\alpha) \notin \langle -1 \rangle \cdot K^{*2}$, which is equivalent to $\mathrm{N}(\alpha) \notin \langle -1, d \rangle \cdot \mathbb{Q}^{*2}$.

Now, let us consider the extensions $\mathbb{Q}(\sqrt{q} - 1/\sqrt{q})$, $\mathbb{Q}(\sqrt{q} + 1/\sqrt{q})$. We have $\mathbb{Q}(\sqrt{q} \pm 1/\sqrt{q}) = \mathbb{Q}(\sqrt{\mathrm{Tr}(q) \pm 2})$. Hence, the condition (ii) in definition 4.4 is equivalent to the condition $\mathrm{Tr}(q) \pm 2 \notin \langle -1, 2 \rangle \cdot \mathbb{Q}^{*2}$. $\square$

Theorem 4.6. *In the generic case we have $\delta_\alpha^+ = \delta_\alpha^- = \frac{1}{3}$.*

Proof: **Split case**. In this case, $[F_k : \mathbb{Q}] = 4^k$, for all k. Having that q is not a square in $K(\zeta_{2^k})$, for any k, we obtain that $[F_k(\zeta_{2^{k+1}}) : F_k(\zeta_{2^k})] = 2$, for all k, and we conclude

$$\delta_\alpha^+ = \frac{1}{2} - \frac{1}{2} \sum_{k=1}^{\infty} \frac{1}{4^k} = \frac{1}{3}.$$

Inert case. Let p be an odd prime that is inert in $K/\mathbb{Q}$.

If $p \equiv 1 \pmod 4$ we have

$$\delta(S_1 \setminus D_1) = \frac{1}{2} \cdot \frac{1}{[K(\sqrt{q}) : \mathbb{Q}]} = \frac{1}{8}.$$

Next, for $p \equiv 3 \pmod 4$ we have

$$\delta(S_k^- \setminus D_k^-) = \frac{2}{[F_k : \mathbb{Q}]}, \quad \text{for all } k \geq 2,$$

where $[F_k : \mathbb{Q}] = 4^{k+1}$. We conclude

$$\delta_\alpha^- = \frac{1}{2} - (\frac{1}{8} + \sum_{k=2}^{\infty} \frac{2}{4^{k+1}}) = \frac{1}{3}. \qquad \square$$

4.3 Extension to some non-generic cases

Although it is hard to state and prove a general result, for a given quadratic integer α, we can compute the density δ_α following the proof of the main theorem. Here, we will compute the density in the case when α satisfies conditions (ii), (iii), but not (i) in definition 4.4.

Theorem 4.7. *Let α and K be as above. If $K \subset \mathbb{Q}(\zeta_{2^\infty})$, $q = \alpha/\overline{\alpha}$ is not a square in $K(\zeta_{2^\infty})$ and $\mathbb{Q}(\sqrt{q}-1/\sqrt{q})$, $\mathbb{Q}(\sqrt{q}+1/\sqrt{q}) \not\subset \mathbb{Q}(\zeta_8)$ then the densities are as follows.*

	$d=-1$	$d=2$	$d=-2$
$\delta_\alpha+$	5/12	17/48	17/48
δ_α^-	5/12	5/16	17/48
δ_α	5/6	2/3	17/24

Proof: **Split case**. If $k \geq 3$, we have

$$\delta(S_k^+ \setminus D_k^+) = \frac{1}{2}[F_k : \mathbb{Q}]^{-1} = \frac{1}{4^k}.$$

If $K = \mathbb{Q}(\sqrt{-1})$, no prime $p \equiv 3 \pmod 4$ splits in K, so

$$S_1^+ = \emptyset$$

and

$$\delta(S_1^+ \setminus D_1^+) = 0.$$

For $k \geq 2$, we have $[F_k(\zeta_{2^{k+1}}) : F_k] = 2$, hence

$$\delta(S_k^+ \setminus D_k^+) = \frac{1}{2}[F_k : \mathbb{Q}] = \frac{1}{4^k}.$$

Finally,

$$\delta_\alpha^+ = \frac{5}{12}.$$

For $K = \mathbb{Q}(\sqrt{\pm 2})$, $[F_1(\zeta_4) : F_1] = 2$, while $[F_2(\zeta_4) : F_2] = 1$. We conclude

$$\delta_\alpha^+ = \frac{1}{2} - (\frac{1}{8} + \sum_{k=3}^{\infty} \frac{1}{4^k}) = \frac{17}{48}.$$

Inert case. If $k \geq 2$, we have

$$[F_k : \mathbb{Q}] = 2^{2k+1}.$$

For $K = \mathbb{Q}(\sqrt{-1})$, no prime $p \equiv 1 \pmod 4$ is inert in $K/\mathbb{Q}$, so

$$S_1^- = \emptyset,$$

and

$$\delta(S_1^- \setminus D_1^-) = 0.$$

If $k \geq 2$,

$$\delta(S_k^- \setminus D_k^-) = \frac{2}{[F_k : \mathbb{Q}]},$$

thus

$$\delta_\alpha^- = \frac{1}{2} - \sum_{k=2}^{\infty} \frac{1}{4^k} = \frac{5}{12}.$$

For $K = \mathbb{Q}(\sqrt{\pm 2})$,

$$\delta(S_1^- \setminus D_1^-) = \frac{1}{2} \cdot \frac{1}{[K(\sqrt{q}) : \mathbb{Q}]} = \frac{1}{8}.$$

If $K = \mathbb{Q}(\sqrt{2})$, we have

$$\delta(S_2^- \setminus D_2^-) = \frac{2}{[F_2 : \mathbb{Q}]}$$

and

$$\delta(S_k^- \setminus D_k^-) = 0 \quad \text{for all } k \geq 3,$$

as

$$S_k^- = \emptyset \quad \text{for all } k \geq 3.$$

Hence

$$\delta_\alpha^- = \frac{1}{2} - (\frac{1}{8} + \frac{1}{16}) = \frac{5}{16}.$$

For $K = \mathbb{Q}(\sqrt{-2})$, we obtain

$$S_2^- = \emptyset,$$

so

$$\delta(S_2^- \setminus D_2^-) = 0,$$

and

$$\delta(S_k^- \setminus D_k^-) = \frac{2}{[F_k : \mathbb{Q}]} \quad \text{for all } k \geq 3.$$

Hence

$$\delta_\alpha^- = \frac{1}{2} - (\frac{1}{8} + \sum_{k=3}^{\infty} \frac{1}{2^{2k}}) = \frac{17}{48}. \qquad \square$$

4.4 Numerical data

In this section we will present some results obtained numerically, implementing in GP/PARI an algorithm that computes the ratio

$$\frac{|\{p \leq x \mid p \in D_{X_\alpha}\}|}{|\{p \leq x \mid p \text{ prime }\}|},$$

for some non-zero quadratic integer α and $x \in \mathbb{R}_{>0}$. All the results exposed in table 1 were obtained for $x = 50000$, that is $|\{p \leq x \mid p \text{ prime }\}| = 5133$. For

a given α, the columns δ^+_{num}, δ^-_{num} represent the result obtained numerically, while the columns δ^+_α, δ^-_α indicate the value given by our theory.

The first three entries are examples of generic α. The following three are examples of α that satisfies conditions (ii),(iii), but not (i) in definition (4.4), so densities are as in theorem 4.7.

Next, let $\alpha = 1+\sqrt{2}$. Since $K = \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$, α is non-generic. Moreover, from $\mathrm{N}(\alpha) = -1$, we have $q = \alpha/\overline{\alpha} \in \langle -1\rangle \cdot K^{*2}$, while $\mathrm{Tr}(q) = -6$ implies $\mathbb{Q}(\sqrt{q} + 1/\sqrt{q}) = \mathbb{Q}(\sqrt{-1})$. Thus, α does not satisfies any condition of the generic case. Since α is a fundamental unit of K, we have $\delta_\alpha = \frac{17}{24}$, by [8].

In the case $\alpha = 1 + 4\sqrt{-3} = (2 + \sqrt{-3})^2$, we have $q = (\frac{1+4\sqrt{-3}}{7})^2$, where $q_0 = \frac{1+4\sqrt{-3}}{7} \notin \langle -1\rangle \cdot K^{*2}$. Having that $\mathrm{Tr}(q_0) \pm 2 \notin \langle -1, 2\rangle \cdot K^{*2}$, we obtain that for $k \geq 1$, a primitive root of unity $\zeta_{2^{k+1}}$ generates a quadratic extension over F_k and that $[F_k : \mathbb{Q}] = 2^{2k-1}$. Thus, $\delta^+_\alpha = \frac{1}{6}$.

In the inert case, if $k = 1$ the density $\delta(S^-_1 \setminus D^-_1) = \frac{1}{4}$, for q is a square in K. If $k \geq 2$, the extension $F_k/K(\zeta_{2^{k+1}})$ is of degree , and we obtain $\delta^-_\alpha = \frac{1}{6}$, so $\delta_\alpha = \frac{1}{3}$.

If $\alpha = \frac{7}{2}+\frac{3}{2}\sqrt{-7} = -\sqrt{-7}(\frac{1+\sqrt{-7}}{2})^2$, we have $q = -(\frac{\pi_2}{\overline{\pi_2}})^2$, where $\pi_2 = \frac{1+\sqrt{-7}}{2}$ and $q_0 = \frac{\pi_2}{\overline{\pi_2}} \notin \langle -1\rangle \cdot K^{*2}$. Hence, $s = 1$ and $\mathrm{Tr}(q_0) - 2 = -\frac{1}{2} \in \langle -1, 2\rangle \cdot K^{*2}$. If $k \geq 3$, we obtain that $\zeta_{2^{k+1}} \notin F_k$, and $[F_k : \mathbb{Q}] = 2^{2k-2}$. For $k = 1$, the extensions $K(\sqrt{q})$ and $K(\zeta_4)$ coincide, so $\delta(S^+_1 \setminus D^+_1) = 0$. In the case $k = 2$, we can see that $[F_2(\zeta_8) : F_2] = 2$ and $[F_2 : \mathbb{Q}] = \frac{1}{4}$, thus $\delta(S^+_2 \setminus D^+_2) = \frac{1}{8}$, and $\delta^+_\alpha = \frac{1}{3}$.

Let us consider the inert case. If $k = 1$, then $\delta(S^-_1 \setminus D^-_1) = 0$, for $\mathrm{Tr}(q_0) - 2 =\in \langle -1, 2\rangle \cdot K^{*2}$ implies $\mathbb{Q}(\sqrt{q} + 1/\sqrt{q}) = \mathbb{Q}(\sqrt{-1})$. For $k \geq 2$, we have $[F_k : K(\zeta_{2^k}] > 1$, so $\delta(S^-_k \setminus D^-_k) = \frac{2}{2^{2k}}$. Thus $\delta_\alpha - = \frac{1}{3}$.

α	δ^+_{num}	δ^-_{num}	δ^+_α	δ^-_α
$3+2\sqrt{5}$	0.327489	0.336061	$\frac{1}{3} \approx 0.333333$	$\frac{1}{3} \approx 0.333333$
$2+\sqrt{7}$	0.333918	0.332749	$\frac{1}{3} \approx 0.333333$	$\frac{1}{3} \approx 0.333333$
$4+\sqrt{-5}$	0.329437	0.335476	$\frac{1}{3} \approx 0.333333$	$\frac{1}{3} \approx 0.333333$
$2+3\sqrt{-1}$	0.413209	0.418664	$\frac{5}{12} \approx 0.416667$	$\frac{5}{12} \approx 0.416667$
$3+\sqrt{2}$	0.349893	0.312877	$\frac{17}{48} \approx 0.354167$	$\frac{5}{16} \approx 0.3125$
$7+3\sqrt{-2}$	0.351451	0.360803	$\frac{17}{48} \approx 0.354167$	$\frac{17}{48} \approx 0.354167$
$1+\sqrt{2}$	0.456263	0.252289	$\frac{11}{24} \approx 0.458333$	$\frac{1}{4} \approx 0.25$
$1+4\sqrt{-3}$	0.166764	0.166569	$\frac{1}{6} \approx 0.166667$	$\frac{1}{6} \approx 0.166667$
$\frac{7}{2}+\frac{3}{2}\sqrt{-7}$	0.332359	0.330411	$\frac{1}{3} \approx 0.333333$	$\frac{1}{3} \approx 0.333333$

Table 1: Numerical Data

References

[1] C. Ballot, Density of prime divisors of linear recurrences, Mem. Amer. Math. Soc. 551 (1995).

[2] J. W. S. Cassels, A. Fröhlich, Algebraic number theory, Academic press, 1967.

[3] D. A. Cox, Primes of the form $x^2 + ny^2$, John Wiley & Sons, Inc, 1989.

[4] H. Hasse, Über die Dichte der Primzhalen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist, Math. Ann. 166 (1996), 19-23.

[5] K. Ireland, M. Rosen, A classical introduction to modern number theory, Springer-Verlag, 1990.

[6] J. C. Lagarias, The set of primes dividing the Lucas number has density 2/3, Pacific J. Math. 118 (1985), 449-461.

[7] H.W. Lenstra, The Chebotarev Density Theorem, http://websites.math.leidenuniv.nl/algebra/ Lenstra-Chebotarev.pdf

[8] P. Moree, P. Stevenhagen, Prime divisors of Lucas sequences, Acta Arith. 82 (1997), 403-410.

[9] P. Ribenboim, The book of prime number records, Springer- Verlag, 1988

[10] J. Roskam, Prime divisors of linear reccurent sequences, J. Th. Nombres Bordeaux 13(1) (2001), 303-314.

[11] P. Stevenhagen, Class Field Theory, http://websites.math.leidenuniv.nl/algebra/cft.pdf

[12] W. Sierpinski, Sur une décomposition des nombres premiers en deux classes, Collect. Math. 10 (1958), 81-83.

[13] M. Ward, Prime divisors of second order recurring sequences, Duke Math. J., 21 (1954), 607-614.