UAB
Universitat Autònoma
de Barcelona

Bachelor Thesis

Euclidean proofs of the infinitude of primes in arithmetic progressions

Author:
Joan Arenillas i Cases

Supervisor:
Marc Masdeu

BSc in Mathematics
Department of Mathematics
Faculty of Sciences

June 25, 2025

What has been affirmed without proof
can also be denied without proof.

Euclid

Acknowledgements

I would like to thank everyone who supported me throughout the execution of this work. Especially and most importantly, to my supervisor, Marc Masdeu. His guidance, ideas, and numerous corrections have shaped and perfected the work you are reading now. I want to thank him for taking the time and effort to make sure I understood the material in this thesis, as well as helping me improve my mathematical writing skills. His expertise and advice have made me truly enjoy every step of this journey.

I also want to express my gratitude to my university colleagues and friends for their insights and plentiful comments on early versions of the thesis. Their availability to discuss diverse topics has been vital to keep me motivated until the submission of this work. A special mention goes to my friend Roger, who has been very helpful in this endeavour.

Finally, I want to thank Cristina for introducing me to the fascinating world of webpage programming. Her innovative ideas have inspired the interactive way in which some of the results are presented.

Thank you all for being part of this work.

Contents

1 Introduction

It is a natural question to ask whether there exist infinitely many prime numbers ending in 3. This can be translated into finding out if the arithmetic progression $10n + 3$ for $n \geqslant 0$ contains infinitely many primes. The first terms of this sequence are

$$3, 13, 23, 33, 43, 53, 63, 73, 83, \ldots$$

and indeed $3, 13, 23, 43, 53, 73$ and 83 are primes. Whether the list of such primes is infinite can be determined using Dirichlet Theorem [PS21], which guarantees that the above progression contains infinitely many primes since 10 and 3 are coprime. This theorem only requires the two integers defining the progression, say k and ℓ, to be relatively prime to ensure the existence of infinitely many primes in $kn + \ell$ for $n \geqslant 0$. The proof of this theorem involves studying advanced properties of L-functions and working with Dirichlet characters.

However, proving the weaker claim that there are infinitely many primes is very straightforward, as only basic divisibility properties are needed. Such is the simplicity that Euclid, around the year 300 BC, already proved this result [EucBC]. One can go a little further and —using a proof that very much resembles Euclid's idea— prove that there exist infinitely many primes of the form $6n + 5$ [HW60]. This can also be done with the progression $4n + 1$ and $4n + 3$ [Leb56]. Thus, it is again natural to ask in what progressions $kn + \ell$ a "Euclidean proof" can be found to show that infinitely many primes lie in them.

In 1912, Issai Schur proved that if $\ell^2 \equiv 1 \pmod{k}$, then infinitely many primes could be found following Euclid's idea [Sch12]. In 1988, M. Ram Murty made the term "Euclidean proof" precise and further proved that Schur's condition was the only case where a Euclidean proof could be established [RT08]. Therefore, Dirichlet Theorem cannot be fully proved *à la Euclid*. In fact, Schur and Murty show us that Euclidean proofs are rather restricted, being only available when $\ell^2 \equiv 1 \pmod{k}$. Although many proofs of Dirichlet Theorem only using elemental mathematics exist for specific progressions [GT02; Lin15; Sel49; Meš23], in this thesis we are only looking for proofs that mimic Euclid's model.

The objective of this thesis will be to understand every detail that leads to Schur and Murty's theorems. Once these results stand in their full form, we will use their ideas to build our own *automated proof generator*, which will consist of a code that returns a fully Euclidean proof of the infinitude of primes in $kn + \ell$. The values of k and ℓ will be supplied by the user, and a proof resembling that of Euclid will be automatically generated, specifically tailored for the given progression. Some cases have already been discussed by several authors. For instance, Paul T. Bateman gives Euclidean proofs for every ℓ satisfying $\ell^2 \equiv 1 \pmod{24}$ [BL65]. However, giving a complete and systematic method to construct Euclidean proofs for every arithmetic progression satisfying $\ell^2 \equiv 1 \pmod{k}$ is something new to the literature. Furthermore, we will take advantage of the results we prove in the way to obtain Schur's theorem to characterise some splitting properties of prime numbers in a subfield of the cyclotomic field of degree at most 2.

This document will be structured as follows. In Section 2 we will briefly discuss the basic notions needed to prove the main theorems. In Section 3 we will prove Schur and Murty's theorems in detail, also quantifying the number of Euclidean proofs available

out of every case allowed by Dirichlet Theorem. Furthermore, we will interpret the main results in this section to characterise the splitting of primes. In Section 4 we will use the ideas developed in the previous sections to build Euclidean proofs for every possible value of k and ℓ satisfying $\ell^2 \equiv 1 \pmod{k}$. Conclusions and further work will be described in Section 5.

2 Fundamental concepts

In this section we will present the basic results that will be needed in future sections. We shall start by introducing some terminology so we can conveniently translate arithmetic progressions into modular arithmetic. We will then define what a "Euclidean proof" is in light of the well-known theorems of Euclid and Dirichlet. Also, some basic but relevant properties and definitions related to polynomials will be given. This chapter will conclude with a compendium of Galois and Algebraic Number Theory results, which form the core of the central results in this work.

2.1 Arithmetic progressions

Our main goal is to find a special type of proof of the fact that there exist infinitely many primes in some arithmetic progressions, which are sequences $\{a_n\}_{n=0}^{\infty} \subset \mathbb{R}$, where the nth term is given by the formula

$$a_n = kn + \ell, \ n \geqslant 0, \tag{2.1}$$

for some $k, \ell \in \mathbb{R}$.

Hereafter, unless otherwise specified, we will always assume k and ℓ to be a pair of non-zero positive integers, since we are only interested in integer values of the sequence $\{a_n\}$. Observe that these two integers univocally identify the arithmetic progression $kn + \ell$, $n \geqslant 0$. We may additionally suppose that $k > \ell$.

Remark 2.1. Observe that requiring $0 < \ell < k$ is not restrictive:

- The cases where $k = 0$ or $\ell = 0$ have obviously no interest, since there is no hope to find infinitely many primes in such progressions.
- If k and ℓ are negative, one can multiply by -1 and obtain the same progression, with positive terms instead. We consider positive progressions since we are looking for primes of a certain form, which are positive numbers.
- If $k > 0$ and $\ell < 0$, consider the canonical representative $\bar{\ell} := \ell \bmod k$, which will be positive and less than k. Note that the progression $kn + \ell$ will have the same terms as $kn + \bar{\ell}$ for $n \geqslant 1$. This is really just a choice of writing: if, say, $k = 5$ and $\ell = -3$, the progression $5n - 3$ has the same terms as $5n + 2$ (except for the first one). Therefore, in this thesis we choose to write our progressions in the latter form.
- If $k < 0$ and $\ell > 0$, consider the progression $-kn - \ell$, which will have the same terms (but positive) and apply the previous point since now $k > 0$ and $\ell < 0$.
- Finally, if $k, \ell > 0$ but $k < \ell$, consider again the progression $kn + \bar{\ell}$ and note that $kn + \ell$ and $kn + \bar{\ell}$ will have the same terms for $n \geqslant 1$.

Observe that, fixed k and ℓ, every term a_n in the sequence defined by Eq. (2.1) satisfies

$$a_n \equiv \ell \pmod{k}, \ n \geqslant 0.$$

Therefore, any prime p we may find in the sequence $\{a_n\}$ will also satisfy $p \equiv \ell \pmod{k}$. Since the integers k and ℓ univocally define the arithmetic progression $a_n = kn + \ell$, we

will be interested in finding certain proofs of the infinitude of primes (in the arithmetic progression) $\equiv \ell \pmod{k}$ or, equivalently, proofs of the existence of infinitely many primes in the congruence class ℓ mod k[1].

2.2 The Theorems of Euclid and Dirichlet

Euclid's theorem of the infinitude of primes [EucBC] plays a pivotal role in this thesis, as we are trying to mimic his proof and extend it to more cases. We should therefore state his Theorem and its proof.

Theorem 2.2 (Euclid). *There are infinitely many prime numbers.*

Proof. Suppose there are finitely many primes, say $p_1, p_2, \ldots, p_m$. Our goal is to show that there exists yet another prime not in our list to reach a contradiction. Thus, consider $Q := p_1 p_2 \cdots p_m + 1$. This number has at least one prime divisor, p, since $Q > 1$. If p was one of the p_i for $1 \leqslant i \leqslant m$, then p would divide $p_1 p_2 \cdots p_m$. Since p also divides Q, we deduce that p divides $Q - p_1 p_2 \cdots p_m = 1$, so p must equal 1, a contradiction (1 is not a prime). Therefore, p is a prime, and it cannot be in our list, which is a contradiction again. □

We are now interested in extending this model of proof to primes of a certain form. In particular, to primes that are $\equiv \ell \pmod{k}$. In other words, we want to prove *à la Euclid* that there exist infinitely many primes of the form $kn + \ell$, $n \geqslant 0$.

It is immediate to check that we need to impose some conditions over k and ℓ to have some possibility of success. For example, if $\gcd(k, \ell) = d > 1$, then $k = dk'$ and $\ell = d\ell'$, for some $k', \ell' \in \mathbb{Z}$. Suppose that p is a prime satisfying $p \equiv \ell \pmod{k}$. Then, $p \equiv \ell \pmod{d}$, but since d also divides ℓ, then $p \equiv 0 \pmod{d}$. Thus, d divides p, which necessarily means that $p = d$. Therefore, there is only one prime (if any) in the arithmetic progression $\equiv \ell \pmod{k}$ if $\gcd(k, \ell) > 1$. Imposing an extra constraint makes all the difference:

Theorem 2.3 (Dirichlet). *Suppose that k and ℓ are two fixed, non-zero integers. If $\gcd(k, \ell) = 1$, there exist infinitely many primes in the congruence class ℓ mod k.*

As we said in the introduction, the proof of this theorem was first given by Dirichlet in terms of L-functions. Although some other proofs that minimize the prerequisites are available [Sel49; Sha50a; Sha50b], proving this theorem is still far from straightforward. Therefore, we shall not give the proof here, but [PS21] is a good reference for it.

Remark 2.4. An even stronger result asserts that the density of primes in the congruence class ℓ mod k exists and equals $1/\varphi(k)$ (see [TH86]), where φ is Euler's totient function (this function counts the number of positive integers less than k relatively prime to k). In this thesis, Dirichlet's Theorem will only refer to Theorem 2.3, not to the stronger assertion about the density of such primes.

Thanks to Dirichlet's Theorem 2.3 we must look for infinitely many primes in arithmetic progressions that satisfy $\gcd(k, \ell) = 1$, which sets an extra condition over k and ℓ. From now on, we will always assume this condition to be true. In fact, for every $k > 2$, there are $\varphi(k) > 1$ congruence classes with infinitely many primes[2].

[1] If the context is clear, we will refer to the congruence class ℓ mod k as simply ℓ.

[2] In the cases $k = 1, 2$ the only congruence class with infinitely many primes is $\ell = 1$.

However, not every one of these $\varphi(k)$ progressions admits a proof that follows the spirit of Euclid's. In Section 3 we will establish that the condition $\gcd(k, \ell) = 1$ is not enough to find such proofs, the constraint $\ell^2 \equiv 1 \pmod{k}$ being also required. In fact, this last condition is stronger than the first one, since it implies that ℓ is an invertible element of $\mathbb{Z}/k\mathbb{Z}$, so ℓ belongs to $(\mathbb{Z}/k\mathbb{Z})^\times$, and thus $\gcd(k, \ell) = 1$.

Proving that a Euclidean proof can be found if and only if $\ell^2 \equiv 1 \pmod{k}$ will be the main technical achievement of this thesis. The progressions that satisfy this will obviously be a subset of those allowed by Dirichlet's Theorem 2.3. For any of this to make sense, however, we must precisely define what we mean by "Euclidean proof" of the infinitude of primes $\equiv \ell \pmod{k}$. We will first give an example of a proof that follows Euclid's idea in Theorem 2.2, so the definition we will give later is more natural.

Example 2.5. Suppose there are finitely many primes $\equiv 1 \pmod{3}$, say $p_1, p_2, \ldots, p_m$. Our goal is to show that there exists yet another prime $\equiv 1 \pmod{3}$ not in our list. For this goal, consider $Q := p_1 p_2 \cdots p_m$ and the polynomial $f(x) := x^2+3$. Now, $f(Q) = Q^2+3$ has at least one prime divisor, p, since it is greater than one. We then have that p divides $Q^2 + 3$.

Observe that $p \neq p_i$, $1 \leqslant i \leqslant m$: if $p = p_i$ for some i, then p would divide Q^2. Since p also divides $Q^2 + 3$, we get that p divides 3, so $p = p_i = 3$, which is a contradiction (3 is not $\equiv 1 \pmod{3}$). Therefore, p is a prime not in our list. We just need to show that $p \equiv 1 \pmod{3}$ to reach a contradiction and conclude the proof.

If p divides $Q^2 + 3$, then $Q^2 \equiv -3 \pmod{p}$. By the Legendre symbol, this means that $\left(\frac{-3}{p}\right) = 1$. Since $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$, we deduce that $\left(\frac{p}{3}\right) = 1$, which happens if and only if $p \equiv 1 \pmod{3}$ (see Theorem 6.4 in Section 6.1 in the Appendix). This gives us an infinitude of primes $\equiv 1 \pmod{3}$ provided we have one. Since 7 is a prime $\equiv 1 \pmod{3}$, the desired result is finally settled.

Observe that in the case of Theorem 2.2 we supposed there are finitely many primes, considered their product, Q, and also implicitly considered the polynomial $f(x) = x + 1$. We then developed a contradiction argument based on the value $f(Q)$. Similarly, for the previous example, we also considered the product Q and used the irreducible polynomial $f(x) = x^2+3$. We then showed that every prime divisor of $f(Q)$ is $\equiv 1 \pmod{3}$ and again reached a contradiction. To end the proof, we needed to find one prime $\equiv 1 \pmod{3}$.

To construct the proof in the general case, we first define the following concept. Let $f \in \mathbb{Z}[x]$ be a polynomial. We say that a prime number p is a *prime divisor* of f (or simply that p *divides* f) if there exists $m \in \mathbb{Z}$ such that p divides $f(m)$. The set of prime divisors of f is denoted by $\mathrm{Spl}_1(f)$. Now, in the general case, we will see that it is enough to find an irreducible polynomial such that all its prime divisors are $\equiv 1$ or $\ell \pmod{k}$ (except maybe *finitely* many)[3]. Therefore, we define:

Definition 2.6. The arithmetic progression $\equiv \ell \pmod{k}$ admits a *Euclidean polynomial* if there exists an irreducible polynomial $f \in \mathbb{Z}[x]$ such that all its prime divisors (except for finitely many) are either $\equiv 1$ or $\ell \pmod{k}$, with infinitely many of the latter kind occurring. We may also suppose that f is monic.

[3]Observe that the polynomial $f(x) = x^2 + 3$ we considered in the case $\equiv 1 \pmod{3}$ satisfies this condition.

We shall then say that there exists a *Euclidean proof* for the arithmetic progression $\equiv \ell \pmod{k}$ if the proof uses a Euclidean polynomial and the shape of its prime divisors to conclude there are infinitely many primes of this type. The procedure to reach this will be fully developed in Section 3.

There are other possible and interesting ways of proving specific examples of Dirichlet Theorem that also avoid its complexity and are not necessarily Euclidean. In [GT02; Lin15; Sel49; Meš23] many examples of such proofs can be found. We could call these other proofs *elementary*[4], rather than Euclidean. For instance, in [Sha93] infinitely many primes $\equiv 1 \pmod{p^n}$ are found (p is a prime and $n$lies in $\mathbb{N}$), but the scheme of the proof has nothing to do with our Definition 2.6. Instead, it uses the form of the prime divisors of $(2^{mp}-1)/(2^m-1)$ for some integer m.

Although Dirichlet's complexity can be overcome by many elemental methods for specific cases, in this thesis we are looking for a *general*, *elementary* and *Euclidean* method to obtain infinitely many primes $\equiv \ell \pmod{k}$.

2.3 Essential results

Some basic notation should be recalled before tackling the main results that will pave the way for those in Section 3. Let $k \geqslant 1$ be a fixed integer. We shall start by remembering that the multiplicative group of units of $\mathbb{Z}/k\mathbb{Z}$ is

$$G := (\mathbb{Z}/k\mathbb{Z})^\times = \{a \in \mathbb{Z}/k\mathbb{Z} : \gcd(k,a) = 1\},$$

and that the number of elements in G equals $\varphi(k)$. Since polynomials are at the core of Euclidean proofs, we will also outline some results and concepts regarding their prime divisors and roots, which will be later on important. The definiton of G enables us to define:

Definition 2.7. The *kth cyclotomic polynomial*, Φ_k, is defined by the formula

$$\Phi_k(x) := \prod_{a \in G} \left(x - e^{\frac{2\pi i a}{k}}\right) = \prod_{a \in G} (x - \zeta^a), \tag{2.2}$$

where we set $\zeta := e^{2\pi i/k}$. Observe that Φ_k is a monic polynomial.

It is obvious from Eq. (2.2) that the roots of Φ_k are all the kth primitive roots of unity and that $\deg(\Phi_k) = \varphi(k)$. Cyclotomic polynomials satisfy the following important relation, which is proved in [Rom07].

Lemma 2.8. *The following equality of polynomials holds:*

$$\prod_{d|k} \Phi_d(x) = x^k - 1. \tag{2.3}$$

Some results regarding the prime divisors of polynomials can already be established.

Lemma 2.9. *Let $f, r \in \mathbb{Z}[x]$. Then,* $\mathrm{Spl}_1(f \circ r) \subseteq \mathrm{Spl}_1(f)$.

[4]By *elementary* we refer to techniques that do not require advanced mathematics such as L-functions, but rather use undergraduate-level results.

Proof. Let p be a prime such that p belongs to $\mathrm{Spl}_1(f \circ r)$. This implies that there exists $a \in \mathbb{Z}$ such that p divides $f(r(a))$. Since $r(a)$ lies in $\mathbb{Z}$ because r belongs to $\mathbb{Z}[x]$, we have that p divides $f(b)$ with $b := r(a) \in \mathbb{Z}$, so p belongs to $\mathrm{Spl}_1(f)$. □

This enables us to prove the following result.

Proposition 2.10. *If $f \in \mathbb{Z}[x]$ is non-constant, the set $\mathrm{Spl}_1(f)$ is infinite.*

Proof. We can suppose that $f(0) = c \neq 0$. If $f(0) = 0$, exchange the polynomial f for $f \circ r$ with a suitable polynomial $r \in \mathbb{Z}[x]$ such that $f(r(0)) \neq 0$. Proving that $f \circ r$ has infinitely many prime divisors will automatically imply that f has infinitely many prime divisors since $\mathrm{Spl}_1(f \circ r) \subseteq \mathrm{Spl}_1(f)$ (see Lemma 2.9).

To begin with, there is obviously at least one prime divisor of f, since the case $f(x) = \pm 1$ only happens for a finite number of integer values of x. Next, suppose f has only a finite number of prime divisors, say $p_1, p_2, \ldots, p_t$, and let $Q := p_1 p_2 \cdots p_t$.

Since $f(0) = c \neq 0$ (changing f for $f \circ r$ if necessary), we have $f(Qcx) = cg(x)$ for some $g \in \mathbb{Z}[x]$ of the form $1 + c_1 x + c_2 x^2 + \cdots + c_d x^d$ (where $c_i \in \mathbb{Z}$ for every $1 \leqslant i \leqslant d$, and $d = \deg(f)$). Note that Q divides every c_i. This polynomial g must also have at least one prime divisor, say p, for the same reason as before. Therefore, p divides $g(m)$ for some $m \in \mathbb{Z}$, and this implies that p divides $f(Qcm)$. Since $m' := Qcm$ lies in $\mathbb{Z}$, it follows that p is a prime divisor of f. But p does not divide Q, since p dividing Q would mean that p divides c_i, for every $1 \leqslant i \leqslant d$ (recall that Q divides every c_i). This, together with the fact that p divides $g(m)$, would imply that p divides $g(m) - \sum_{i=1}^{d} c_i m^i = 1$, which means $p = 1$, a contradiction.

Now, p is a prime divisor of f, but p is not any of the primes $p_1, p_2, \ldots, p_t$, since we just proved that p does not divide $p_1 p_2 \cdots p_t = Q$. Thus, we found a new prime divisor of f not in our list, so one concludes that f has infinitely many prime divisors. □

The above proof is a detailed version of that in [RT08].

Remark 2.11. In Section 3 we will prove that every prime divisor of Φ_k is $\equiv 1 \pmod{k}$, except for finitely many, so, from Proposition 2.10, we deduce that Φ_k has infinitely many prime divisors $\equiv 1 \pmod{k}$. There is a result due to Trygve Nagell [RT08] that ensures that for any pair of non-constant polynomials f and g in $\mathbb{Z}[x]$, the set $\mathrm{Spl}_1(f) \cap \mathrm{Spl}_1(g)$ is infinite. This tells us that every non-constant polynomial has infinitely many prime divisors $\equiv 1 \pmod{k}$.

Let p be a prime and let $\mathbb{F}_p$ be the finite field with p elements. The following result also holds.

Proposition 2.12. *Fix a non-constant polynomial $f \in \mathbb{Z}[x]$ and let $\mathbb{F}$ be an extension field of $\mathbb{F}_p$. Also let $\overline{f} \in \mathbb{F}_p[x]$ be the reduction of $f \bmod p$. An element $a \in \mathbb{F}$ is a double root of $\overline{f}$ if and only if $f(a) \equiv 0 \pmod{p}$ and $f'(a) \equiv 0 \pmod{p}$.*

Proof. We shall always work in the field $\mathbb{F}_p$ to ease the notation. If f has a double root a, we can then write $f(x) = (x-a)^2 q(x)$ for some $q \in \mathbb{F}_p[x]$. It is then clear that $f(a) = 0$. Furthermore, using the formal derivative, $f'(x) = 2(x-a)q(x) + (x-a)^2 q'(x)$, which, at $x = a$, reduces to $f'(a) = 0$.

For the converse implication, we want to show that $(x-a)^2$ divides f in $\mathbb{F}_p[x]$. Since $f(a) = 0$, we have that $f(x) = (x-a)r(x)$ for some $r \in \mathbb{F}_p[x]$. Using the formal derivative

we get $f'(x) = r(x) + (x-a)r'(x)$, which, at $x = a$, reduces to $f'(a) = r(a)$. Since $f'(a)$ vanishes by hypothesis, we have that $r(a) = 0$, so we can also write $r(x) = (x-a)s(x)$ for some $s \in \mathbb{F}_p[x]$. Putting all together yields $f(x) = (x-a)r(x) = (x-a)^2 s(x)$. Hence, $(x-a)^2$ divides f. □

Finally, we also need to give an expression for the *discriminant* of a monic polynomial $f \in \mathbb{Z}[x]$, which we denote by $\Delta(f)$. Let $\deg(f) = d$ and let $\{r_1, r_2, \ldots, r_d\} \subset \mathbb{C}$ be the roots of f (not necessarily distinct). Then,

$$\Delta(f) = \prod_{i<j} (r_i - r_j)^2, \quad 1 \leqslant i, j \leqslant d. \tag{2.4}$$

2.4 Some Galois Theory

Galois Theory results will also be needed. Since our definition of Euclidean polynomial requires it to be irreducible (see Definition 2.6), we will find the following theorem particularly useful. The proofs of the next two results can be found in [Cox12, Chapter 6 and 7].

Theorem 2.13. *Let F be a field and let $f \in F[x]$ be a separable polynomial. Also let L be the splitting field of f. Then, the group $\mathrm{Gal}(L/F)$ is transitive on the roots of f if and only if f is irreducible over F.*

Consider now an arbitrary tower of field extensions $K/L/F$. Recall that if K/F is Galois, then K/L is automatically a Galois extension. A condition can be given so that L/F is also Galois.

Theorem 2.14. *Let $K/L/F$ be a tower of extensions where K/F is Galois. Suppose L is the fixed field of a subgroup H of $\mathrm{Gal}(K/F)$. Then, L/F is Galois if and only if H is normal on $\mathrm{Gal}(K/F)$.*

There is one particular field which will be relevant in this thesis. Again, fix an integer $k \geqslant 1$ and let ζ be a kth primitive root of unity (from now on, ζ will always denote a root of Φ_k). The field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is called the *kth cyclotomic field*. It is the smallest subfield of $\mathbb{C}$ containing ζ.

This extension is generated by the cyclotomic polynomial Φ_k. Indeed, since the cyclotomic polynomials are irreducible over $\mathbb{Q}$ (see [Cox12, Chapter 9]), we have that the cyclotomic field is generated via $\mathbb{Q}[x]/(\Phi_k)$, so $\mathbb{Q}(\zeta)$ is a finite field extension over $\mathbb{Q}$, with $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_k) = \varphi(k)$.

Now, since every kth root of unity is of the form ζ^j for some $j \in \mathbb{Z}$, it follows that $\mathbb{Q}(\zeta)$ contains every root of Φ_k (see Definition 2.7). Since we are working in characteristic 0, it follows that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension. The Galois group of this extension can be easily described thanks to the following proposition, proved in [Cox12, Chapter 9].

Proposition 2.15. *The group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/k\mathbb{Z})^\times$ via sending the morphism $\sigma_a : \zeta \mapsto \zeta^a$ of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to the residue class $a \bmod k$, for every $a \in (\mathbb{Z}/k\mathbb{Z})^\times$.*

In future sections we will extensively use this canonical isomorphism to identify some subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with the corresponding subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$.

2.5 Some Algebraic Number Theory

As we said in the introduction, Euclidean methods to show that the congruence class $\equiv \ell \pmod{k}$ contains infinitely many primes can only be found when $\ell^2 \equiv 1 \pmod{k}$. This requires proving two implications. Imagine we somehow have a Euclidean polynomial for the congruence class $\equiv \ell \pmod{k}$. In this situation, showing that $\ell^2 \equiv 1 \pmod{k}$ will be the hardest implication to settle. By "hard" we mean that some algebraic number theory will be needed. Therefore, we shall introduce some technical parlance and results, which we will take from Chapter 3 of [Mar87].

We say that a field extension K over $\mathbb{Q}$ is a *number field* if $[K : \mathbb{Q}]$ is finite. Now, fix a number field K with $[K : \mathbb{Q}] = n$. The set of all algebraic integers in K is denoted by $\mathcal{O}_K$. That is,

$$\mathcal{O}_K := \{\alpha \in K : \text{ exists a monic polynomial } h \in \mathbb{Z}[x], h \neq 0 \text{ and } h(\alpha) = 0\} \subseteq K.$$

This set is actually a ring, called the *ring of integers* of K. Moreover, $\mathcal{O}_K$ is a Dedekind domain, so every non-zero proper ideal factors uniquely (up to the order of the factors) into a product of prime ideals.

If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$, then the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is called a $\mathbb{Z}$-*power basis* of $\mathcal{O}_K$. In this case, the number field K is called a *monogenic* number field.

If $n = 2$ or K is a cyclotomic field, then $\mathcal{O}_K$ always admits a $\mathbb{Z}$-power basis. However, this is not always the case. There is an example due to Dedekind that shows that such a basis cannot always be found. For this purpose, Dedekind considered the number field $K := \mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^3 - x^2 - 2x - 8$ and showed that K is not monogenic (see page 30 of Dedekind's original article [Ded78]).

Now, given a prime p of $\mathbb{Z}$, consider the ideal of $\mathcal{O}_K$ defined by $p\mathcal{O}_K := \{px : x \in \mathcal{O}_K\}$. This ideal is not prime in general, but it breaks down uniquely as a product of prime ideals (up to the order of the factors). Precisely, suppose that the ideal $p\mathcal{O}_K$ factors in $\mathcal{O}_K$ like

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}, \tag{2.5}$$

where every $\mathfrak{p}_i$, $1 \leqslant i \leqslant g$, is a prime ideal of $\mathcal{O}_K$. The number $e_i \in \mathbb{N}$ is called the *ramification index* of $\mathfrak{p}_\mathfrak{i}$ over p. If $e_i > 1$ for any i, we say p is *ramified* in K. If every e_i equals 1, we say p is *unramified* in K. We also say that $\mathfrak{p}_i$ *divides* or *contains*[5] $p\mathcal{O}_K$.

We now have the following situation:

$$\begin{array}{ccccc} K & \supseteq & \mathcal{O}_K & \supseteq & p\mathcal{O}_K \\ | & & | & & | \\ \mathbb{Q} & \supseteq & \mathbb{Z} & \ni & p \end{array}$$

Observe that $\mathfrak{p}_i \cap \mathbb{Z} = p\mathbb{Z}$, since $\mathfrak{p}_i$ contains $p\mathcal{O}_K \supseteq \mathbb{Z}$, so it contains every multiple of p. Now, remember that in Dedekind domains, prime ideals are also maximal ideals. Therefore, for every $1 \leqslant i \leqslant g$, $\mathcal{O}_K/\mathfrak{p}_i$ is a field with characteristic p (for a proof of this fact, again see [Mar87, Chapter 3]), which is called the *residue field* of $\mathfrak{p}_i$. Since it is a field of characteristic p, it must be isomorphic to $\mathbb{F}_{p^n}$ for some integer $n \geqslant 1$. This integer

[5]This makes sense since the product of two ideals I and J in a general ring R always satisfies $IJ \subseteq I$ and $IJ \subseteq J$.

is called the *inertia degree* of $\mathfrak{p}_i$ over p, and it is denoted by $f_{K/\mathbb{Q}}(\mathfrak{p}_i|p)$ (or simply $f(\mathfrak{p}_i|p)$ or f_i if there is no ambiguity).

Therefore, $f(\mathfrak{p}_i|p) := [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$, and, in view of this, one can define the *absolute norm* of the nonzero ideal $\mathfrak{p}_\mathfrak{i}$ by $\mathrm{N}(\mathfrak{p}_\mathfrak{i}) := p^{f_i}$. In the specific case where $K/\mathbb{Q}$ is a normal extension (thus automatically Galois), we have the following result:

Proposition 2.16. *If $K/\mathbb{Q}$ is a normal extension, then there exists a unique $e \in \mathbb{N}$ such that $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^e$, and every inertia degree f_i is the same for $1 \leqslant i \leqslant g$ (we then simply write the inertia degree as f). Moreover, $e \cdot f \cdot g = [K : \mathbb{Q}]$.*

In all, when we express $p\mathcal{O}_K$ as in Eq. (2.5), we refer to the data provided by the ramification indices, the inertia degrees and the natural number g as the "shape" of the factorization of $p\mathcal{O}_K$.

There are some quantities attached to every number field that describe it. One of these quantities is called the *discriminant* of K, and it regulates which primes ramify in K. Let $b_1, \ldots, b_n$ be an integral basis of $\mathcal{O}_K$, and let $\{\sigma_1, \ldots, \sigma_n\}$ be the set of injective ring homomorphisms from K to $\mathbb{C}$. The *discriminant* of a number field K, $\Delta(K)$, is defined by $\Delta(K) := (\det(\sigma_i(b_j)_{i,j}))^2$, for $1 \leqslant i, j \leqslant n$.

The notion of discriminant can be extended to $\mathcal{O}_K$. In this case, $\Delta(\mathcal{O}_K)$ is defined to be the discriminant of K. Also, if $K = \mathbb{Q}(\alpha)$ for some α in $\mathcal{O}_K$, and we let h denote the minimal polynomial of α, we then have that $\Delta(\mathbb{Z}[\alpha])$ coincides with the discriminant of h. If K is monogenic with $\mathcal{O}_K = \mathbb{Z}[\beta]$ for some $\beta \in \mathcal{O}_K$, then $\Delta(K)$ also coincides with the discriminant of the minimal polynomial of β.

Remark. We have so far worked with field extensions over $\mathbb{Q}$. The same results hold for *relative extensions* over a fixed, arbitrary number field. This requires replacing $\mathbb{Q}$ with a number field F and $\mathbb{Z}$ with $\mathcal{O}_F$. Also, p would now be a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$.

In the same lines, one can also define the *relative discriminant* of an extension K/F, which is denoted by $\Delta(K/F)$. It is an ideal of $\mathcal{O}_F$ and controls what primes of F ramify in K.

We will now learn that the shape of $p\mathcal{O}_K$ can be studied via the factorization of a certain polynomial. Suppose a monic polynomial $\overline{h} \in \mathbb{F}_p[x]$ factors into monic irreducible factors $\overline{h_i} \in \mathbb{F}_p[x]$ like

$$\overline{h} = \overline{h_1}^{e_1} \overline{h_2}^{e_2} \cdots \overline{h_g}^{e_g},$$

for some natural numbers g and e_i. We also refer to the quantity g, the exponents e_i and the degrees of each $\overline{h_i}$ as the "shape" of the factorization of the polynomial $\overline{h}$ in $\mathbb{F}_p[x]$. There exists a criterion by Dedekind that allows to work out the shape of the factorization of $p\mathcal{O}_K$ via the shape of the factorization in $\mathbb{F}_p[x]$ of a certain polynomial with integer coefficients. The criterion holds for all but finitely many primes, and is proved in detail in [Mar87, Chapter 3]. It reads:

Theorem 2.17 (Dedekind Criterion). *Let α belong to $\mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$. Let $h \in \mathbb{Z}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Also, let p be a prime not dividing $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, and let $\overline{h}$ be the reduction of $h \bmod p$. Then, there exists an integer $g \geqslant 1$, some prime ideals $\mathfrak{p}_i \subseteq \mathcal{O}_K$ and some ramification indices e_i such that*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g} \quad \textit{if and only if} \quad h \equiv \overline{h_1}^{e_1} \overline{h_2}^{e_2} \cdots \overline{h_g}^{e_g} \pmod{p},$$

where every $\overline{h_i}$ is a distinct monic irreducible factor of h in $\mathbb{F}_p[x]$. Moreover, there is an isomorphism of residue fields $\mathbb{F}_p[x]/(\overline{h_i}) \cong \mathcal{O}_K/\mathfrak{p}_i$ defined by sending $x \mapsto \alpha \pmod{\mathfrak{p}_i}$, for every $1 \leqslant i \leqslant g$.

The above theorem tells us that $f(\mathfrak{p}_i|p) = \deg(\overline{h_i})$, and that there is a bijection between every prime ideal $\mathfrak{p}_i$ and each irreducible factor $\overline{h_i}$ such that $\mathrm{N}(\mathfrak{p}_\mathfrak{i}) = p^{\deg(\overline{h_i})}$. Moreover, since $\Delta(\mathbb{Z}[\alpha]) = \Delta(h) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2\Delta(\mathcal{O}_K)$ holds, it is enough to check that p^2 does not divide $\Delta(h)$ for Dedekind Criterion to work for p. The following result can be deduced from the previous theorem.

Corollary 2.18. *Consider the field extension K/F. A prime ideal $\mathfrak{p}$ of F ramifies in K if and only if $\mathfrak{p}$ divides $\Delta(K/F)$.*

Remark 2.19. Since $\Delta(K/F) \neq 0$, only finitely many prime ideals of F ramify in K.

For the following two results we temporarily write the kth cyclotomic field as $\mathbb{Q}(\zeta_k)$, and we let p be a prime and n a positive integer. The proof of the upcoming two results can be found in [Was96, Chapter 2].

Proposition 2.20. *The discriminant of the number field $\mathbb{Q}(\zeta_{p^n})$ is $\pm p^{p^{n-1}(pn-n-1)}$, where the sign is negative if $p = 2$ and $n = 2$ or if $p \equiv 3 \pmod 4$. The sign is otherwise positive.*

For the next result, first observe that $\Delta(\Phi_k) = \Delta(\mathbb{Q}(\zeta_k))$, because $\mathbb{Q}(\zeta_k)$ is monogenic since its ring of integers is $\mathbb{Z}[\zeta_k]$.

Proposition 2.21. *If p divides $\Delta(\Phi_k)$, then p also divides k.*

Proof. A prime number p divides $\Delta(\Phi_k) = \Delta(\mathbb{Q}(\zeta_k))$ if and only if p ramifies in $\mathbb{Q}(\zeta_k)$ (see Corollary 2.18). Thus, we are reduced to prove that the fact that p ramifies in $\mathbb{Q}(\zeta_k)$ implies that p divides k. Equivalently, we will show that if p does not divide k, then p does not ramify in $\mathbb{Q}(\zeta_k)$.

Set $k = \prod_i q_i^{n_i}$, for some primes q_i and some integer exponents $n_i > 0$ and note that $\mathbb{Q}(\zeta_k)$ is the compositum of the fields $\mathbb{Q}(\zeta_{q_i^{n_i}})$. Suppose p does not divide k, so $p \neq q_i$ for every i. Then p is unramified in each $\mathbb{Q}(\zeta_{q_i^{n_i}})$, since p does not divide the discriminant of $\mathbb{Q}(\zeta_{q_i^{n_i}})$ (see Proposition 2.20). Therefore, p does not ramify in the compositum, which is $\mathbb{Q}(\zeta_k)$. □

If $p \neq 2$, then the converse of the previous proposition is also true: if p divides k, then $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_k)$. Since $p \neq 2$, p ramifies in $\mathbb{Q}(\zeta_p) \supsetneq \mathbb{Q}$ (because it divides $\Delta(\mathbb{Q}(\zeta_p))$), so we deduce that p ramifies in $\mathbb{Q}(\zeta_k)$. Thus, p divides $\Delta(\mathbb{Q}(\zeta_k)) = \Delta(\Phi_k)$. However, if we take $p = 2$ and $k = 6$, then p divides k, but p does not divide $\Delta(\Phi_6) = -3$.

2.6 Notation for Murty Theorem

With the definitions and results we have given so far we can introduce some notation that will easen the proof of Murty Theorem [RT08]. The notation we follow here is due to Keith Conrad, who gives a detailed version of Murty's theorem in [Con10].

Let $h \in \mathbb{Z}[x]$ be a monic polynomial and let p be a prime divisor of h. Recall that in Section 2.2 we set

$$\mathrm{Spl}_1(h) := \{p : p \text{ is a prime divisor of } h\} = \{p : h \bmod p \text{ has a linear factor in } \mathbb{Z}/p\mathbb{Z}[x]\}.$$

Giving a rule to determine which primes belong to $\mathrm{Spl}_1(h)$ is the so-called "reciprocity problem", and any possible answer to it is a "reciprocity law". A helpful reference regarding this topic is [Wym72].

These reciprocity laws exist for generating polynomials of quadratic extensions and cyclotomic extensions. For example, the well-known *Quadratic Reciprocity Law* (see Theorem 6.4 in Section 6.1 in the Appendix) determines when an irreducible monic polynomial $h(x) = x^2 + b$ with b in $\mathbb{Z}$ splits into linear factors when reduced mod p. That is, this law determines $\mathrm{Spl}_1(h)$ when $\deg(h) = 2$. For example, the QRL enables us to give an easy description of the set $\mathrm{Spl}_1(\Phi_4) = \mathrm{Spl}_1(x^2+1)$. Indeed, let p be a prime divisor of Φ_4, so $n^2 + 1 \equiv 0 \pmod{p}$, for some $n \in \mathbb{Z}$. This tells us that -1 is a quadratic residue mod p, for every prime divisor of Φ_4 different from 2, so $\left(\frac{-1}{p}\right) = 1$ for $p \neq 2$. By the supplemental laws of the QRL (again, see Section 6.1), we deduce that $p \equiv 1 \pmod{4}$, so finally $\mathrm{Spl}_1(\Phi_4) = \{p : p \equiv 1 \pmod{4}\} \cup \{2\}$.

However, $\mathrm{Spl}_1(h)$ for $h(x) = x^5 - x + 1$ has no easy description. Nevertheless, in this thesis —taking advantage of the results that lead to Euclidean proofs— we will give an explicit reciprocity law for a special type of polynomials, which had not been previously considered in the literature. Suppose $L := \mathbb{Q}(\eta)$ for some $\eta \in \mathbb{Q}(\zeta)$ and $[\mathbb{Q}(\zeta) : L] \leqslant 2$. We will effectively give a characterisation of $\mathrm{Spl}_1(h)$, where h is the minimal polynomial of η over $\mathbb{Q}$. In fact, the reciprocity law for the cyclotomic case $[\mathbb{Q}(\zeta) : L] = 1$ is already known [Wym72].

Now fix an arbitrary number field K over $\mathbb{Q}$. Similarly to the set $\mathrm{Spl}_1(h)$, one may define the set $\mathrm{Spl}_1(K)$ as

$$\mathrm{Spl}_1(K) := \{p : \text{some } \mathfrak{p} \text{ dividing } p\mathcal{O}_K \text{ in } K \text{ has } f_{K/\mathbb{Q}}(\mathfrak{p}|p) = 1\}.$$

Thus, in the notation of Eq. (2.5), $\mathrm{Spl}_1(K)$ is the set of primes such that the corresponding factorization in prime ideals of $\mathcal{O}_K$ includes a prime ideal $\mathfrak{p}_i$ with $\mathrm{N}(\mathfrak{p}_i) = p$, for some $1 \leqslant i \leqslant g$. As Keith Conrad summarises in [Con10], "p lies in $\mathrm{Spl}_1(h)$ when h has a root mod p, while p lies in $\mathrm{Spl}_1(K)$ when p has a prime ideal factor in K whose residue field is $\mathbb{Z}/p\mathbb{Z}$".

Again, any rule that determines what primes lie in $\mathrm{Spl}_1(K)$ is called a reciprocity law. For instance, $\mathrm{Spl}_1(\mathbb{Q}(i))$ can be easily calculated using Dedekind Criterion (Theorem 2.17) with $\alpha = i$ and $h = \Phi_4$, which is the minimal polynomial of the algebraic element i. Observe that $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, so Dedekind Criterion holds for every prime. Thus, to calculate $\mathrm{Spl}_1(\mathbb{Q}(i))$ we need to work out for what primes p the reduction of $\Phi_4(x) = x^2 + 1$ mod p produces a linear factor in $\mathbb{F}_p[x]$ (since the degrees of the irreducible factors correspond to the inertia degrees)[6]. But this will happen exactly when p lies in $\mathrm{Spl}_1(h)$, so finally $\mathrm{Spl}_1(\mathbb{Q}(i)) = \{p : p \equiv 1 \pmod{4}\} \cup \{2\}$.

Following this idea, in this thesis we will also give a characterisation of $\mathrm{Spl}_1(L)$, for L lying below $\mathbb{Q}(\zeta)$ of degree at most 2.

Now that we have a better understanding of the sets $\mathrm{Spl}_1(h)$ and $\mathrm{Spl}_1(K)$, we can introduce two more sets, which will play a crucial role in the proof of Murty's theorem. As usual, fix an integer $k \geqslant 1$. We define

$$S_1(k, h) := \{b \bmod k : p \equiv b \pmod{k} \text{ for infinitely many } p \in \mathrm{Spl}_1(h)\}$$

[6]In fact, since $\mathbb{Q}(i)/\mathbb{Q}$ is Galois, if Φ_4 has a linear factor (mod p), every factor of Φ_4 mod p will be linear.

and

$$S_1(k,K) := \{b \bmod k : p \equiv b \pmod{k} \text{ for infinitely many } p \in \mathrm{Spl}_1(K)\}.$$

Observe that the elements of the above (finite) sets are congruence classes mod k. Moreover, they are subsets of $(\mathbb{Z}/k\mathbb{Z})^\times$, since $\gcd(k,b) = 1$, for otherwise the condition of existing infinitely many primes $\equiv b \pmod{k}$ would not be met.

Remark 2.22. These sets are of particular interest since they give a simple description of Euclidean polynomials. Using again Dedekind Criterion, if h is irreducible over $\mathbb{Q}$, and θ is a root of h, $\mathrm{Spl}_1(h)$ and $\mathrm{Spl}_1(\mathbb{Q}(\theta))$ are the same, except maybe in a finite number of cases arising if $\mathbb{Z}(\theta)$ is not the ring of integers of $\mathbb{Q}(\theta)$. However, $S_1(k,h)$ and $S_1(k,\mathbb{Q}(\theta))$ do coincide without exceptions.

Thus, observing Definition 2.6 and Remark 2.11, a Euclidean polynomial for the progression $\equiv \ell \pmod{k}$ is any monic, irreducible polynomial $h \in \mathbb{Z}[x]$ such that $S_1(k,h) = \{1,\ell\}$ (writing ℓ instead of $\ell \bmod k$). Equivalently, h will be a Euclidean polynomial for the progression $\equiv \ell \pmod{k}$ if, for any root $\theta \in \mathbb{C}$ of h, we have that $S_1(k,\mathbb{Q}(\theta)) = \{1,\ell\}$.

2.7 Chebotarev Density Theorem

The key step to prove Murty's theorem will be Chebotarev Density Theorem. This result is even deeper than Dirichlet Theorem, and it constitutes a cornerstone in modern algebraic number theory. In order to understand its statement, we must first introduce some concepts and results (proved in detail in [Mar87]).

Let K and F be number fields, and assume K/F is an abelian extension. Also assume that K is a normal extension of F, so K/F is automatically Galois. Now set $G := \mathrm{Gal}(K/F)$ and let $\mathcal{O}_K$ and $\mathcal{O}_F$ denote the corresponding rings of integers. Also, denote by $\mathrm{Cl}(\sigma) = \{\tau\sigma\tau^{-1} : \tau \in G\}$ the conjugacy class of $\sigma \in G$.

Now, fix a prime $\mathfrak{p}$ of $\mathcal{O}_F$, so that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, for some prime p. For each prime $\mathfrak{q}$ of $\mathcal{O}_K$ lying over[7] $\mathfrak{p}$, we define the following two subgroups of G:

Definition 2.23. The *decomposition group* is defined by:

$$\begin{aligned} D_\mathfrak{q} &:= \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\} \\ &= \{\sigma \in G : \sigma(\alpha) \equiv 0 \pmod{\mathfrak{q}} \text{ if and only if } \alpha \equiv 0 \pmod{\mathfrak{q}}, \forall \alpha \in \mathcal{O}_K\}. \end{aligned}$$

The *inertia group* is defined by:

$$I_\mathfrak{q} := \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}, \forall \alpha \in \mathcal{O}_K\}.$$

From the definition, $I_\mathfrak{q}$ lies in $D_\mathfrak{q}$. In principle, $D_\mathfrak{q}$ and $I_\mathfrak{q}$ depend on $\mathfrak{p}$ and on the choice of $\mathfrak{q}$ lying over $\mathfrak{p}$. If $\mathfrak{q}'$ is another prime ideal of $\mathcal{O}_K$ lying over $\mathfrak{p}$, then $D_\mathfrak{q}$ and $D_{\mathfrak{q}'}$ (resp. $I_\mathfrak{q}$ and $I_{\mathfrak{q}'}$) are conjugate in G via any $\sigma \in G$ sending $\mathfrak{q}$ to $\mathfrak{q}'$. However, since K/F is abelian, every conjugacy class only contains one element, so $D_\mathfrak{q}$ and $I_\mathfrak{q}$ do not depend on the choice of $\mathfrak{q}$[8].

[7] By this we mean any prime ideal $\mathfrak{q} \subseteq \mathcal{O}_K$ such that $\mathfrak{q} \cap \mathcal{O}_F = \mathfrak{p}$.

[8] We will however not drop the subscript for clarity.

Any $\sigma \in G$ is an automorphism of the field K, so $\sigma(\mathcal{O}_K) \subseteq \mathcal{O}_K$. Now, if we additionally suppose that σ lies in $D_\mathfrak{q} \subseteq G$, then σ fixes $\mathfrak{q}$ and hence induces a well-defined automorphism σ^* of the field $\kappa(\mathfrak{q}) := \mathcal{O}_K/\mathfrak{q}$. Indeed, for each $\sigma \in D_\mathfrak{q}$, we define

$$\begin{aligned} \sigma^* : \kappa(\mathfrak{q}) &\longrightarrow \kappa(\mathfrak{q}) \\ [\alpha] &\longmapsto [\sigma(\alpha)] \\ [\alpha + t] &\longmapsto [\sigma(\alpha) + \sigma(t)] = [\sigma(\alpha)] + t \end{aligned}$$

for $\alpha \in \mathcal{O}_K$ and $t \in \mathfrak{q}$. Also write $\kappa(\mathfrak{p}) := \mathcal{O}_F/\mathfrak{p}$. Since σ also fixes $\mathcal{O}_F$ (because σ lies in G), it can be proved that σ^* belongs to $G^* := \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$, so we have a group homomorphism π between $D_\mathfrak{q}$ and G^*. Moreover, this homomorphism is surjective, and its kernel is:

$$\ker(\pi) = \{\sigma \in D_\mathfrak{q} : \sigma^* = \mathrm{id}\} = \{\sigma \in D_\mathfrak{q} : \sigma(\alpha+\mathfrak{q}) = \sigma(\alpha)+\sigma(\mathfrak{q}) = \alpha+\mathfrak{q},\ \forall \alpha \in \mathcal{O}_K\} = I_\mathfrak{q}, \tag{2.6}$$

from which we deduce that $I_\mathfrak{q}$ is a normal subgroup of G. Therefore, we have the following exact[9] sequence in $I_\mathfrak{q}$, $D_\mathfrak{q}$ and G^*:

$$\{1\} \longrightarrow I_\mathfrak{q} \hookrightarrow D_\mathfrak{q} \xrightarrow{\pi} G^* \longrightarrow \{1\}.$$

Assume now that $\mathfrak{p}$ is unramified in K (equivalently, $\mathfrak{p}$ does not divide $\Delta(K/F)$ because of Corollary 2.18). One can show that $\mathfrak{p}$ ramifies in K if and only if $I_\mathfrak{q} \neq \{1\}$. Therefore, if $\mathfrak{p}$ is unramified in K, $I_\mathfrak{q}$ is trivial, and we have that π is in fact an isomorphism from Eq. (2.6). Observe that $\kappa(\mathfrak{q})$ is a finite field extension of $\kappa(\mathfrak{p})$ with characteristic p. Therefore, the group G^* is cyclic, with a special generator descending from $D_\mathfrak{q}$:

Definition 2.24. The generator of G^* is denoted by $\mathrm{Frob}_\mathfrak{p}^*$, so $\langle \mathrm{Frob}_\mathfrak{p}^* \rangle = G^*$. If $\mathfrak{p}$ is unramified in K, the automorphism $\pi^{-1}(\mathrm{Frob}_\mathfrak{p}^*) \in D_\mathfrak{q}$ is well-defined, and we call it the *Frobenius automorphism* of $\mathfrak{q}$ over $\mathfrak{p}$ and we denote it by $\mathrm{Frob}_\mathfrak{p}$.

By noting that the finite group G^* is generated by the automorphism $x \mapsto x^{\mathrm{N}(\mathfrak{p})}$, $x \in \kappa(\mathfrak{q})$, one deduces that $\mathrm{Frob}_\mathfrak{p}$ is the unique automorphism of G with the following defining property for every $\alpha \in \mathcal{O}_K$:

$$\mathrm{Frob}_\mathfrak{p}(\alpha) \equiv \alpha^{\mathrm{N}(\mathfrak{p})} \pmod{\mathfrak{q}}.$$

Remark 2.25. In principle, $\mathrm{Frob}_\mathfrak{p}$ would also depend on the prime ideal $\mathfrak{q}$ lying above $\mathfrak{p}$, so we would instead write $\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}}$. In general, if we consider a different $\mathfrak{q}'$ lying above $\mathfrak{p}$, the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}'}$ attached to it would be conjugate to $\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}}$. Therefore, the Frobenius element is not well-defined as an element but rather as a conjugacy class. However, since we chose K/F to be abelian, the conjugacy classes only contain one element and $\mathrm{Frob}_\mathfrak{p}$ is a unique, well-defined element of $D_\mathfrak{q} \subseteq G$, which does not depend on the choice of $\mathfrak{q}$.

Before tackling Chebotarev Density Theorem, we first need to introduce a numerical measure of sets of prime ideals called the *Dirichlet density*.

[9] A sequence of maps $\cdots \to A \xrightarrow{f} B \xrightarrow{g} C \to \cdots$ is *exact* in B if $\mathrm{Im}(f) = \ker(g)$.

A set of prime ideals S in a number field K has *Dirichlet density* $d(S)$ if the limit

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s}}{-\log(s-1)} = d(S) \tag{2.7}$$

exists. If it does not exist, we may always define the *lower Dirichlet density* (resp. *upper Dirichlet density*) using the limit inferior (resp. limit superior).

The Dirichlet density is a finitely additive measure and, from Eq. (2.7), one has that $0 \leqslant d \leqslant 1$. The definition of this density is different from the more usual *natural density*. See Section 6.2 in the Appendix to understand where Eq. (2.7) comes from and the relation between the natural and Dirichlet density. To advance towards Chebotarev's theorem, we need the following result.

Lemma 2.26. *Let S be the set of primes $\mathfrak{p}$ lying above some prime p with $f_{F/\mathbb{Q}}(\mathfrak{p}|p) \geqslant 2$. Then, the Dirichlet density $d(S)$ is zero.*

Proof. For $d(S)$ to be zero, it is enough to prove that $\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s}$ converges (absolutely) at $s = 1$, since $\lim_{s\to 1^+} \log(s-1) = \infty$ (observe Eq. (2.7)). Let $f := f_{F/\mathbb{Q}}(\mathfrak{p}|p) \geqslant 2$, let T be the set of primes arising from $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for $\mathfrak{p} \in S$, and let Π be the set of all primes. Additionally, consider a normal closure M of F, which is a finite and normal extension of $\mathbb{Q}$. The number of prime ideals in the factorization of $p\mathcal{O}_M$ is bounded by some $g \leqslant [M:\mathbb{Q}]/2 < \infty$, for every p (because of Proposition 2.16). Since $\mathrm{N}(\mathfrak{p}) = p^f$, at $s = 1$ we have:

$$\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-1} = \sum_{\mathfrak{p}\in S} p^{-f} \leqslant \sum_{\mathfrak{p}\in S} p^{-2} \leqslant \frac{[M:\mathbb{Q}]}{2} \sum_{p\in\Pi} \frac{1}{p^2} \leqslant \frac{[M:\mathbb{Q}]}{2} \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty.$$

□

Remark 2.27. This tells us that the set of primes $\mathfrak{p}$ lying above a certain prime p with $f_{F/\mathbb{Q}}(\mathfrak{p}|p) = 1$ has Dirichlet density equal to one.

The Dirichlet density has the following property.

Lemma 2.28. *Let A be a set with $d(A) = 1$ and let B be a set with $d(B) = \delta > 0$. Then, $d(A \cap B) > 0$.*

Proof. Remember that the inclusion-exclusion principle holds for the Dirichlet density d since it is a finitely additive measure. A direct consequence of this fact is that $d(A \cup B) = d(A) + d(B) - d(A \cap B)$. Now, since always $d(A \cup B) \leqslant 1$, we have that

$$d(A) + d(B) - d(A \cap B) \leqslant 1,$$

which yields $d(A) + d(B) - 1 \leqslant d(A \cap B)$. Since $d(A) + d(B) = 1 + \delta > 1$, then $d(A \cap B) \geqslant d(A) + d(B) - 1 > 1 - 1 = 0$. □

Remark 2.29. From the above result we deduce that $A \cap B$ is infinite, observing Eq. (2.7).

Now that we have the notion of density, it is now natural to ask if a fixed element of G corresponds to a Frobenius automorphism over a prime ideal $\mathfrak{p}$. This question is answered using the Chebotarev Density Theorem, which is formulated in terms of Dirichlet density. In the general case where K/F is not necessarily abelian we have:

Theorem 2.30 (Chebotarev Density Theorem). *Let $C \subset G$ be a fixed conjugacy class. Then, the set*

$$S := \{\mathfrak{p} : \mathfrak{p} \text{ a prime ideal of } F, \mathfrak{p} \text{ unramified in } K,\ \mathrm{Cl}(\mathrm{Frob}_{\mathfrak{p}}) = C\}$$

has Dirichlet density $d(S) = \#C/\#G > 0$, so there exist infinitely many such prime ideals.

The proof of this theorem goes beyond the scope of this thesis, so it will be skipped here, but can be found in [SL96]. If the extension K/F is abelian, then each conjugacy class only contains one element, the automorphism $\mathrm{Frob}_{\mathfrak{p}}$ is well-defined and Theorem 2.30 reads:

Corollary 2.31. *Suppose that K/F is abelian, and fix $\sigma \in G$. Then, the set*

$$S := \{\mathfrak{p} : \mathfrak{p} \text{ a prime ideal of } F, \mathfrak{p} \text{ unramified in } K,\ \mathrm{Frob}_{\mathfrak{p}} = \sigma\}$$

has Dirichlet density $d(S) = 1/\#G > 0$, so there exist infinitely many such prime ideals.

3 The scope of Euclidean proofs

Our goal is to show that one can find Euclidean proofs of the infinitude of primes $\equiv \ell \pmod{k}$ if and only if $\ell^2 \equiv 1 \pmod{k}$. This section will primarily be an expanded and upgraded version of the main propositions and theorems in [RT08] and [Con10].

Let us fix the notation. In this section, k and ℓ will again denote a fixed pair of non-zero positive integers, which will univocally identify the arithmetic progression $kn + \ell$, $n \geqslant 0$, that is, integers $\equiv \ell \pmod{k}$. We will always suppose that they are relatively prime to satisfy Dirichlet Theorem 2.3 and we may additionally suppose that $k > \ell$ and $k \neq 1, 2$.

Remark 3.1. The cases $k = 1, 2$ are highly degenerate, and a Euclidean proof can be easily established (see Section 6.4 in the Appendix).

3.1 Schur Theorem

We will start by proving that one can find a Euclidean proof of the infinitude of primes $\equiv \ell \pmod{k}$ if $\ell^2 \equiv 1 \pmod{k}$, following Schur's proof detailed in [RT08]. Let ζ be a kth primitive root of unity (take $\zeta = e^{2\pi i/k}$) and let $K := \mathbb{Q}(\zeta)$. We know because of Proposition 2.15 that $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/k\mathbb{Z})^\times = G$, the group of coprime residue classes modulo k. Thus, the number of elements in G is $\varphi(k)$ and we may identify the field automorphism $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$ sending $\zeta \mapsto \zeta^i$ with the integer $i \in G$.

Consider the subgroup $H := \{1, \ell\} \leqslant G$, where for now we may suppose $\ell \not\equiv 1 \pmod{k}$[10]. (The proof of the following results for a general subgroup H is given in [RT08]). Since G is finite, the coset representatives[11] of H in G form a finite set S. Observe that $|S| = [G : H] = |G|/|H| = \varphi(k)/2$, so one can write

$$G = \bigsqcup_{s \in S} sH = \bigsqcup_{s \in S} \{s, s\ell\}. \tag{3.1}$$

Note that $|S|$ is well-defined, since the only cases when $\varphi(k)$ is odd happen for $k = 1, 2$, but we are always excluding these cases. Also, we can always suppose that 1 lies in S.

Now define the polynomial

$$h_u(z) := (z - u)(u - z^\ell) \in \mathbb{Z}[z],$$

which depends on some $u \in \mathbb{Z}$. Observe the following lemma.

Lemma 3.2. *The equality $h_u(\zeta)^s = h_u(\zeta^s)$ holds for every $s \in S$.*

Proof. Note that s is coprime to k, so σ_s belongs to $\mathrm{Gal}(K/\mathbb{Q})$. Then,

$$\begin{aligned} h_u(\zeta)^s &= \sigma_s(h_u(\zeta)) = \sigma_s\Big((\zeta - u)(u - \zeta^\ell)\Big) \\ &= (\sigma_s(\zeta) - u)(u - \sigma_s(\zeta^\ell)) = (\zeta^s - u)(u - \zeta^{s\ell}) = h_u(\zeta^s), \end{aligned}$$

where in the third equality we used that σ_s is a field automorphism (hence multiplicative and additive) that fixes the elements in $\mathbb{Q}$. □

[10] The case $\ell \equiv 1 \pmod{k}$ is easier and will be proved in Section 3.1.1.

[11] Since the elements of G are residue classes, the coset representatives of the subgroup H in G are also residue classes.

Set $\eta := h_u(\zeta) = (\zeta - u)(u - \zeta^\ell) \in \mathbb{C}$. The previous result leads to the following result:

Lemma 3.3. *Let $a \in G$. Then $\sigma_a(\eta) = \sigma_s(\eta)$, where s is the coset representative of a.*

Proof. Since a belongs to G, it must happen that $a = s$ or $a = s\ell$ for some coset representative $s \in S$, because of Eq. (3.1). In the first case, there is nothing to prove, so suppose $a = s\ell$. Now,

$$\begin{aligned}\sigma_a(\eta) = \sigma_{s\ell}(\eta) &= \sigma_{s\ell}\Big((\zeta - u)(u - \zeta^\ell)\Big) = (\sigma_{s\ell}(\zeta) - u)(u - \sigma_{s\ell}(\zeta^\ell)) \\ &= (\zeta^{s\ell} - u)(u - \zeta^{s\ell^2}) = (u - \zeta^s)(\zeta^{s\ell} - u) = (\zeta^s - u)(u - \zeta^{s\ell}) = h_u(\zeta^s),\end{aligned}$$

where again we used that $\sigma_{s\ell}$ is a field automorphism in the third equality. In the fifth equality we used that $\zeta^{s\ell^2}$ only depends on the value of $s\ell^2 \bmod k$. Since $\ell^2 \equiv 1 \pmod{k}$, it follows that $\zeta^{s\ell^2} = \zeta^s$. Finally, because of Lemma 3.2,

$$\sigma_a(\eta) = h_u(\zeta^s) = h_u(\zeta)^s = \sigma_s(\eta).$$

□

Observe that ζ (and ζ^s, $s \in S$) are algebraic integers, and h_u has integer coefficients, so $h_u(\zeta^s)$ are also algebraic integers. Consider the monic polynomial

$$f_u(x) := \prod_{s \in S} \Big(x - h_u(\zeta^s)\Big) = \prod_{s \in S} \Big(x - (\zeta^s - u)(u - \zeta^{\ell s})\Big), \tag{3.2}$$

whose coefficients are symmetric polynomials in the algebraic integers $h_u(\zeta^s)$, and so they are algebraic integers themselves. Since $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutes the kth primitive roots of unity ($\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$), $\sigma(h_u(\zeta^s)) = h_u(\sigma(\zeta)^s)$ is another root of f_u, so σ permutes the roots of f_u. Since the coefficients of f_u are symmetric polynomials on $h_u(\zeta^s)$, these coefficients are fixed by every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so $\sigma(f_u) = f_u$. Thus, the coefficients of f_u lie in $\mathbb{Q}$, and they must be integers since the only algebraic integers in $\mathbb{Q}$ are the integers, so f_u belongs to $\mathbb{Z}[x]$. Moreover, this polynomial is irreducible.

Proposition 3.4. *The field $L := \mathbb{Q}(\eta)$ is the fixed field of H, except for finitely many values of u. Excluding these cases, the polynomial f_u is irreducible.*

Proof. Consider the tower of extensions $K/L = \mathbb{Q}(\zeta)^H/\mathbb{Q}$, where we have defined L to be the fixed field of H. If $k = 3, 4, 6$, then η is an integer and the fixed field of H is just $\mathbb{Q}$ since $[K^H : \mathbb{Q}] = \varphi(k)/2 = 1$, due to the Galois correspondence. In these cases, f_u is irreducible since it has degree 1 because $|S| = 1$. Thus, suppose k is such that $\varphi(k) > 2$, that is, $k = 5$ or $k \geqslant 7$. Thanks to the Galois correspondence, we want to see that, except for finitely many values of u, $\sigma(\eta) = \eta$ if and only if σ belongs to H, for every $\sigma \in G$.

The converse implication is simple. Denote by σ_ℓ the only non-trivial automorphism in H. Since the coset representative of ℓ is $s = 1$, it follows from Lemma 3.3 that $\sigma_\ell(\eta) = \sigma_{s=1}(\eta) = \eta$.

We now have to show that the equality $\sigma(\eta) = \eta$ implies that σ belongs to H. We will instead prove the equivalent contrapositive assertion: if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ does not belong to H, then $\sigma(\eta) \neq \eta$. Because of Lemma 3.3, it is enough to check it for the automorphisms

σ_s with $s \neq 1$, which excludes σ_1 and σ_ℓ (the automorphisms in H). From Lemma 3.2, we have

$$\sigma_s(\eta) = \eta^s = h_u(\zeta)^s = h_u(\zeta^s).$$

Thus, we have to prove that $h_u(\zeta^s) \neq \eta$, for every $s \in S^* := S \setminus \{1\}$.

Note that $\eta = h_u(\zeta) = (\zeta - u)(u - \zeta^\ell)$ can be interpreted as a polynomial in u. Now observe that, for every $s \in S^*$, there are only a finite number of values of $u \in \mathbb{Z}$ for which the equality of polynomials in u

$$h_u(\zeta^s) = (\zeta^s - u)(u - \zeta^{\ell s}) = (\zeta - u)(u - \zeta^\ell) = \eta \tag{3.3}$$

holds, so we may exclude these integers and conclude that $\mathbb{Q}(\eta)$ is the fixed field of H. However, one may worry about the fact that

$$\begin{aligned} h_u(\zeta^s) &= \eta, \\ u^2 - (\zeta^s + \zeta^{\ell s})u + \zeta^{s(1+\ell)} &= u^2 - (\zeta + \zeta^\ell)u + \zeta^{1+\ell}, \\ -(\zeta^s + \zeta^{\ell s})u + \zeta^{s(1+\ell)} &= -(\zeta + \zeta^\ell)u + \zeta^{1+\ell} \end{aligned} \tag{3.4}$$

can in principle have infinite solutions for u if $\zeta^s + \zeta^{\ell s} = \zeta + \zeta^\ell$ and $\zeta^{s(1+\ell)} = \zeta^{1+\ell}$. We will show this is never the case. Observe that Eq. (3.4) would have infinitely many solutions for u if and only if $\zeta + \zeta^\ell$ and $\zeta^{1+\ell}$ are fixed by σ_s. In this case, the equality $\zeta^{1+\ell} = \zeta^{s(1+\ell)}$ tells us that $1 + \ell \equiv s(1 + \ell) \pmod{k}$. Rearranging terms, we get $(1 - s)(1 + \ell) \equiv 0 \pmod{k}$. Since $s \not\equiv 1 \pmod{k}$, then $1 - s \not\equiv 0 \pmod{k}$, so $1 - s$ is invertible modulo k. This immediately tells us that $1 + \ell \equiv 0 \pmod{k}$, that is, $\ell \equiv -1 \pmod{k}$. Hence, $\zeta + \zeta^{-1}$ is fixed by σ_s. But $\zeta + \zeta^{-1} = \zeta + \bar{\zeta} = 2\,\mathrm{Re}(\zeta) = 2\cos(2\pi/k)$ generates the totally real subfield of K.

Indeed, observe that complex conjugation $\tau : \zeta \mapsto \bar{\zeta} = \zeta^{-1}$ belongs to G and has order 2, so the fixed field of $\{\mathrm{id}, \tau\}$ is the maximal real subfield of K, which is of degree 2 below K. Also, this field must coincide with the real field $\mathbb{Q}(\zeta + \zeta^{-1}) \subset K$, which is also fixed by $\{\mathrm{id}, \tau\}$ and is of degree 2, since $(x - \zeta)(x - \zeta^{-1}) = x^2 - (\zeta + \zeta^{-1})x + 1$ is the minimal polynomial of ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$. Since this field has degree 2, by the Galois correspondence it must be the fixed field of the group $\{1, -1\} = \{1, \ell\}$, so σ_s belongs to this group. Then, $s = 1$, but this does not happen since we chose the coset s to lie in S^*. Thus, Eq. (3.3) only has a finite number of solutions for u. Excluding these finite values of u, we have that $\sigma_s(\eta) \neq \eta$ for $s \in S^*$, so finally $L = \mathbb{Q}(\eta)$.

To prove the last part of the proposition, take some u such that $L = \mathbb{Q}(\eta)$. We will now show that every $\eta^s = h_u(\zeta^s)$, for $s \in S$, is different. To reach a contradiction, suppose $h_u(\zeta^{s_1}) = h_u(\zeta^{s_2})$ for $s_1 \neq s_2$. We can write $\sigma_{s_1}(h_u(\zeta)) = \sigma_{s_2}(h_u(\zeta))$, because of Lemma 3.2. Thus, in terms of η, we have $\sigma_{s_2}^{-1}\sigma_{s_1}(\eta) = \eta$. Defining $\phi := \sigma_{s_2}^{-1}\sigma_{s_1}$, then ϕ fixes L, so ϕ belongs to $\mathrm{Gal}(K/L) = H$, which implies that $\sigma_{s_1}H = \sigma_{s_2}H$. That is, s_1 and s_2 are in the same coset of H, which is a contradiction. Therefore, η^s for $s \in S$ (which are the roots of f_u) are all distinct. This guarantees that $f_u \in \mathbb{Z}[x]$ is separable.

Now, $L = K^H/\mathbb{Q}$ is a Galois extension from the fact that H is normal on G (see Theorem 2.14), because every subgroup of an abelian group is normal. Thus, every automorphism in $\mathrm{Gal}(L/\mathbb{Q})$ descends from some σ in $\mathrm{Gal}(K/\mathbb{Q})$ due to the Fundamental Theorem of Galois theory. Hence, $\mathrm{Gal}(L/\mathbb{Q})$ also acts transitively on the roots of f_u. Also, L is the splitting field of f_u since its roots are η^s for $s \in S$ and each η^s lies in L. Thus, from Theorem 2.13, we have that f_u is a (monic) irreducible polynomial over $\mathbb{Q}[x]$. $\square$

In the following, we will suppose that $u \in \mathbb{Z}$ is always chosen so that L is the fixed field of H.

Remark 3.5. Some remarks can be made in relation to the tower of extensions $K/L/\mathbb{Q}$. In light of the Galois correspondence, we have that $[L = K^H : \mathbb{Q}] = [G : H] = \varphi(k)/2$, and also $[K : K^H] = |H| = 2$. Similarly, $[K : \mathbb{Q}] = |G| = \varphi(k)$. Also, f_u is the minimal polynomial of η, since it is irreducible, $f_u(\eta) = 0$, and $\deg(f_u) = |S| = \varphi(k)/2$. In short, f_u is a polynomial of degree $\varphi(k)/2$ whose roots generate L and are invariant under the action of the subgroup H. Indeed,

$$\begin{aligned}\sigma_\ell(h_u(\zeta^s)) &= (\zeta^{s\ell} - u)(u - \zeta^{s\ell^2}) = (\zeta^{s\ell} - u)(u - \zeta^s) \\ &= (\zeta^s - u)(u - \zeta^{s\ell}) = h_u(\zeta^s),\end{aligned}$$

since $\ell^2 \equiv 1 \pmod{k}$.

One more remark is needed before moving on to the next theorem. From now on, p will always denote a prime number.

Remark 3.6. For the following results we will need to consider a field $\mathbb{F}$ containing both the finite field $\mathbb{F}_p$ and ζ. For instance, consider $\mathbb{F} = \mathbb{F}_{p^n}$ with a suitable integer $n \geqslant 1$ such that Φ_k has a root ζ. This is possible because $\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}_p}$, where $\overline{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_p$. Obviously, in this context we cannot think of ζ as an element of $\mathbb{C}$, but rather as some root of an irreducible factor of $\overline{\Phi_k} \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$. Alternatively, this field $\mathbb{F}$ can be constructed via $\mathbb{F}_p[x]/(r(x))$ for some factor $r(x)$ of Φ_k that is irreducible over $\mathbb{F}_p$.

The following theorem will play a pivotal role in this thesis.

Theorem 3.7 (Schur). *Every prime divisor of f_u belongs to the residue classes of H (except for finitely many prime divisors).*

Proof. Let T be the set containing every prime that divides k or $\Delta(f_u)$, where $\Delta(f_u)$ is the discriminant of f_u. Note that T is finite, due to the Fundamental Theorem of Arithmetic. Now, take a prime divisor p of f_u such that p does not lie in T.

Since p divides f_u, working in the field $\mathbb{F}$ of Remark 3.6, there exists $a \in \mathbb{Z}$ such that

$$f_u(a) = \prod_{s' \in S} \left(a - h_u(\zeta^{s'})\right) = 0.$$

Since $\mathbb{F}$ is a field, there exists some $s \in S$ such that $a = h_u(\zeta^s)$. We will now prove that the equality $h_u(\zeta^s) = h_u(\zeta^{ps})$ holds in $\mathbb{F}$. Observe that in this field

$$\begin{aligned}h_u(\zeta^s) = a = a^p = h_u(\zeta^s)^p &= (\zeta^s - u)^p(u - \zeta^{\ell s})^p \\ &= (\zeta^{ps} - u^p)(u^p - \zeta^{\ell ps}) = (\zeta^{ps} - u)(u - \zeta^{\ell ps}) = h_u(\zeta^{ps}),\end{aligned} \tag{3.5}$$

where we have used Fermat little theorem in the second equality. The fifth equality, on the other hand, relies on the fact that $\operatorname{char}(\mathbb{F}) = p$ (so that $(c + d)^p = c^p + d^p$ for every $c, d \in \mathbb{F}$) and the following one, on Fermat little theorem. Therefore, equality Eq. (3.5) means that $h_u(\zeta^{ps}) = h_u(\zeta^s)$ is a root of $\overline{f_u} \in \mathbb{F}[x]$.

We will now see that $h_u(\zeta^{ps})$ is also a root of f_u in K. Begin by noting that the value $h_u(\zeta^{ps})$ only depends on the value of $ps \bmod k$ since it only appears as an exponent of

ζ. Since p does not divide k by hypothesis and s is coprime to k, ps is coprime to k (so $ps \bmod k$ is coprime to k) and hence ζ^{ps} is a primitive kth root of unity.

There are now only two options: either $ps \bmod k$ belongs to S or $ps \bmod k$ does not belong to S. In the first case, $h_u(\zeta^{ps})$ is a root of f_u in K, observing expression Eq. (3.2). In the latter case, note that every integer $ps \bmod k$ relatively prime to k not in S satisfies $ps \equiv \ell t \pmod{k}$ for some $t \in S$ (because of Eq. (3.1)). This means that $h_u(\zeta^{ps}) = h_u(\zeta^{\ell t})$. Let us prove that $h_u(\zeta^{\ell t}) = h_u(\zeta^t)$, so $h_u(\zeta^{ps}) = h_u(\zeta^{\ell t}) = h_u(\zeta^t)$ is also a root of f_u in K. Indeed,

$$\begin{aligned} h_u(\zeta^{\ell t}) &= (\zeta^{\ell t} - u)(u - \zeta^{\ell^2 t}) = (\zeta^{\ell^2 t} - u)(u - \zeta^{\ell t}) \\ &= (\zeta^t - u)(u - \zeta^{\ell t}) = h_u(\zeta^t), \end{aligned}$$

where we have used that $\zeta^{\ell^2 t}$ only depends on the value of $\ell^2 t \bmod k$ and the fact that $\ell^2 \equiv 1 \pmod{k}$. Therefore, $h_u(\zeta^{ps}) = h_u(\zeta^t)$ is always a root of f_u in K.

We will now see that $h_u(\zeta^{ps})$ and $h_u(\zeta^s)$ are the same root of f_u in K. If $h_u(\zeta^{ps})$ and $h_u(\zeta^s)$ were two distinct roots of f_u in K, we know because of Eq. (3.5) that they would be the same in $\mathbb{F}$. Therefore, observing the discriminant expression in Eq. (2.4), it follows that $\Delta(f_u \bmod p) = \Delta(f_u) \bmod p = 0$, so p divides $\Delta(f_u)$. This is a contradiction with our choice of p. Thus, $h_u(\zeta^{ps})$ and $h_u(\zeta^s)$ are in fact the same root of f_u in K, so $h_u(\zeta^{ps}) = h_u(\zeta^s)$.

Since p does not lie in T, it follows that $\gcd(k, p) = 1$, so one can consider the field automorphism $\sigma_p \in \mathrm{Gal}(K/\mathbb{Q})$. Following the spirit of Lemma 3.2, one can easily see that $h_u(\zeta^{ps}) = h_u(\zeta^s)^p$, so $h_u(\zeta^s)^p = h_u(\zeta^{ps}) = h_u(\zeta^s)$ in K. Therefore, $\eta^s = h_u(\zeta^s)$ is fixed by σ_p and so is $\mathbb{Q}(\eta^s)$. Now, $\mathbb{Q}(\eta^s) = L$, because η^s is a conjugate of η (thus, $\mathbb{Q}(\eta^s)/\mathbb{Q}$ is Galois since $L/\mathbb{Q}$ is Galois). Consequently, σ_p also fixes L, and since $L = K^H$ by definition, it must happen that $p \bmod k$ belongs to H, that is, $p \equiv 1, \ell \pmod{k}$. □

The special thing about f_u is that we can "control" its prime divisors: if p is a prime divisor of f_u, then either p divides k, or p divides $\Delta(f_u)$ or $p \equiv 1, \ell \pmod{k}$. Nevertheless, we cannot yet guarantee that f_u is a Euclidean polynomial: it satisfies every condition in Definition 2.6, except that we do not know whether it has infinitely many prime divisors $\equiv \ell \pmod{k}$. This is resolved with the following proposition, which is the converse of the previous theorem.

Proposition 3.8. *Any prime belonging to any residue class of H divides f_u.*

Proof. Let p be a prime belonging to a residue class of H. That means $p \bmod k$ belongs to H. By definition, $\eta = h_u(\zeta)$. Now, since $\gcd(k, p) = 1$ and $1 \in H$ is the coset representative of $p \bmod k$, it holds that

$$\eta^p = \sigma_p(\eta) = \sigma_{s=1}(\eta) = \eta, \tag{3.6}$$

because of Lemma 3.3.

Consider now the equation $x^p - x$ and let us work in the field $\mathbb{F}$ of Remark 3.6. Since $\mathbb{F}$ is a field with $\mathrm{char}(\mathbb{F}) = p$ there are p solutions to this equation, since x lies in $\mathbb{F}$ if and only if $x^p = x$. In fact, there exist exactly p integer solutions to the equation: thanks to Fermat little theorem, $0, \ldots, p-1$ are roots of $x^p - x \bmod p$. Since $\eta^p - \eta = 0$ because of Eq. (3.6), η is also a solution, and it must be an integer, so $\eta = b$ for some integer b. It

is now enough to recall that η is a root of f_u to conclude the proof. Indeed, the equality $0 = f_u(\eta) = f_u(b)$ holds in $\mathbb{F}[x]$. Since $\text{char}(\mathbb{F}) = p$, p divides $f_u(b)$, and so p is a prime divisor of f_u. □

Since there exist infinitely many primes $\equiv \ell \pmod{k}$, f_u has infinitely many prime divisors of this type, and we can finally establish that f_u is a Euclidean polynomial, which will be used in our Euclidean proof.

Remark 3.9. Observe that Theorem 3.7 tells us that, except for finitely many primes, we have $\text{Spl}_1(f_u) \subseteq \{p : p \equiv 1, \ell \pmod{k}\}$. With this last Proposition 3.8 we have that $\{p : p \equiv 1, \ell \pmod{k}\} \subseteq \text{Spl}_1(f_u)$. Thus, $\text{Spl}_1(f_u) = \{p : p \equiv 1, \ell \pmod{k}\}$, except for finitely many primes.

We will also need the following result.

Proposition 3.10 (Schur). *Every prime divisor of Φ_k not dividing k is $\equiv 1 \pmod{k}$.*

Proof. Let T be the set containing every prime that divides k or $\Delta(\Phi_k)$. Recall that the primes that divide $\Delta(\Phi_k)$ also divide k (see Proposition 2.21) so T effectively contains the prime divisors of k. Note that T is finite, due to the Fundamental Theorem of Arithmetic. Now, consider a prime divisor p of Φ_k such that p does not lie in T.

Since p divides Φ_k, working in the field $\mathbb{F}$ of Remark 3.6, there exists $a \in \mathbb{Z}$ such that

$$\Phi_k(a) = \prod_{s' \in S} \left(a - \zeta^{s'}\right) = 0.$$

Since $\mathbb{F}$ is a field, there exists some $s \in S$ such that $a = \zeta^s$. We will now prove that the equality $\zeta^s = \zeta^{ps}$ holds in $\mathbb{F}$. Observe that in this field

$$\zeta^s = a = a^p = \zeta^{ps}, \tag{3.7}$$

where we have used Fermat little theorem in the second equality. Therefore, equality Eq. (3.7) means that $\zeta^{ps} = \zeta^s$ is a root of $\overline{\Phi_k} \in \mathbb{F}[x]$.

We will now show that ζ^{ps} is also a root of Φ_k in K. Begin by noting that the value ζ^{ps} only depends on the value of ps mod k since it only appears as an exponent of ζ. Since p does not divide k by hypothesis and s is coprime to k, ps is coprime to k (so ps mod k is coprime to k), and hence ζ^{ps} is a primitive kth root of unity. Thus, ζ^{ps} is a root of Φ_k in K.

We will now show that ζ^{ps} and ζ^s are the same root of Φ_k in K. If ζ^{ps} and ζ^s were two distinct roots of Φ_k in K, we know because of Eq. (3.7) that they would be the same in $\mathbb{F}$. Therefore, observing expression Eq. (2.4), it follows that $\Delta(\Phi_k \bmod p) = \Delta(\Phi_k) \bmod p = 0$, so p divides $\Delta(\Phi_k)$. This is a contradiction with our choice of p. Thus, ζ^{ps} and ζ^s are in fact the same root of Φ_k in K.

Therefore, the equality

$$\zeta^{ps} = \zeta^s \tag{3.8}$$

holds in K. Writing the above equation in terms of $\theta := \zeta^s$ yields $\theta^p = \theta$, where observe that θ is also a primitive kth root of unity. Now, the right-hand side of the equation above does not depend on p. The left-hand side only depends on the value of $p \bmod k$, since p only appears as an exponent of θ. In conclusion, equality Eq. (3.8) only holds if $p \bmod k = 1$, that is, if $p \equiv 1 \pmod{k}$. □

Remark 3.11. In the same lines of Remark 3.9, Proposition 3.8 tells us that $\{p : p \equiv 1 \pmod{k}\} \subseteq \mathrm{Spl}_1(\Phi_k)$ (observe there was no need to suppose $\ell \not\equiv 1 \pmod{k}$ in the proof of that proposition). This last Proposition 3.10 tells us that, except for finitely many primes, we have $\mathrm{Spl}_1(\Phi_k) \subseteq \{p : p \equiv 1 \pmod{k}\}$. Thus, $\mathrm{Spl}_1(\Phi_k) = \{p : p \equiv 1 \pmod{k}\}$, except for finitely many primes.

Since Proposition 3.4 holds except for a finite number of values of the integer u, we can further suppose u to be a non-zero multiple of k. We then have:

Lemma 3.12. *The equality $f_u(0) = \Phi_k(u)$ holds. Also, every prime divisor of $\Phi_k(u)$ is $\equiv 1 \pmod{k}$.*

Proof. From Eq. (3.2), one has

$$f_u(0) = \prod_{s \in S} (u - \zeta^s)(u - \zeta^{\ell s}) = \prod_{a \in G} (u - \zeta^a), \tag{3.9}$$

where we use Eq. (3.1). Since the kth cyclotomic polynomial is defined by

$$\Phi_k(x) = \prod_{a \in G} (x - \zeta^a),$$

it is clear that $f_u(0) = \Phi_k(u)$. Now, since u is a non-zero multiple of k, and working mod k, we have

$$\Phi_k(u) = \prod_{a \in G} (u - \zeta^a) \equiv (-1)^{\varphi(k)} \prod_{a \in G} \zeta^a = \prod_{a \in G} \zeta^a = 1 \pmod{k}, \tag{3.10}$$

where we used that Euler's function $\varphi(k)$ is always even for $k > 2$. The last equality comes from the fact that the product goes over all kth primitive roots of unity: this excludes -1 and the roots can be grouped in complex-conjugate pairs[12], so every pair equals one: $\zeta^a \overline{\zeta^a} = |\zeta^a|^2 = 1$ for every $a \in G$.

We will finally see that $\Phi_k(u)$ is only divisible by primes $\equiv 1 \pmod{k}$. Let r be a prime divisor of $\Phi_k(u)$. From Proposition 3.10 it follows that $r \equiv 1 \pmod{k}$ or r divides k. However, if r divides k, then $\Phi_k(u) \equiv 1 \pmod{r}$ because of Eq. (3.10). This means that r does not divide $\Phi_k(u)$, a contradiction. Therefore, $\Phi_k(u) = f_u(0)$ is only divisible by primes $\equiv 1 \pmod{k}$. □

The following theorem uses the Euclidean polynomial f_u to deduce there exist infinitely many primes $\equiv \ell \pmod{k}$ in the case $\ell \not\equiv 1 \pmod{k}$.

Theorem 3.13. *There exists an integer $n = n(k, \ell)$ such that if there exists a prime $p \equiv \ell \pmod{k}$ satisfying $p \nmid n$, then there exists a Euclidean proof of the infinitude of primes $\equiv \ell \pmod{k}$.*

Proof. We must first find a special integer b with some special and suitable properties for our Euclidean proof. By hypothesis, pick one prime $p \equiv \ell \pmod{k}$ such that p does not divide $n := \Delta(f_u)$. Now, by Proposition 3.8, we can find some $b \in \mathbb{Z}$ such that p divides

[12]For this to work, one should make sure that the conjugate of ζ^a is not itlself. If that was the case, $\zeta^a \overline{\zeta^a} = \zeta^a \zeta^a = \zeta^{2a} = 1$ means $2a \equiv 0 \pmod{k}$, and since a and k are coprime, $2 \equiv 0 \pmod{k}$, so $k = 1$ or $k = 2$. Since we are excluding these two cases, we can group every kth primitive root of unity with its distinct complex-conjugate pair.

$f_u(b)$. We can be even more precise: b can be chosen so that p^2 does not divide $f_u(b)$. If we suppose otherwise (p^2 divides $f_u(b)$) let us write a Taylor expansion around b:

$$f_u(b+x) = f_u(b) + f_u'(b)x + \frac{f_u''(b)}{2!}x^2 + O(x^3) \in \mathbb{Z}[x]. \tag{3.11}$$

In the case $x = p$, Eq. (3.11) reads

$$f_u(b+p) = f_u(b) + f_u'(b)p + \frac{f_u''(b)}{2!}p^2 + O(p^3).$$

Now, it follows that $f_u(b+p) \equiv f_u(b) + pf_u'(b) \pmod{p^2}$, and since p^2 divides $f_u(b)$, we have $f_u(b+p) \equiv pf_u'(b) \pmod{p^2}$. Since p does not divide $\Delta(f_u)$, f_u has no double roots mod p, and therefore $f_u'(b) \not\equiv 0 \pmod{p}$. This is a direct consequence of Proposition 2.12. In all, we have that $f_u(b) \equiv 0 \pmod{p^2}$ implies $f_u(b+p) \not\equiv 0 \pmod{p^2}$. In any case, either $f_u(b)$ or $f_u(b+p)$ will not be divisible by p^2, but they both are divisible by p.

The above remark enables us to build a Euclidean proof using the Euclidean polynomial f_u. As Euclid himself did in his famous proof of the infinitude of prime numbers (see Theorem 2.2), to prove that there exist infinitely many primes $\equiv \ell \pmod{k}$ we will proceed by contradiction.

Suppose there are finitely many primes $\equiv \ell \pmod{k}$ and denote them by $p_1, p_2, \ldots, p_m$. Since the prime p in the remark above is $\equiv \ell \pmod{k}$, we can write the list as $p, p_2, p_3, \ldots, p_m$ (so $p_1 = p$). Now, let $q_1, q_2, \ldots, q_t$ be the prime divisors of $\Delta(f_u)$ and let $Q := q_1 q_2 \cdots q_t p_2 p_3 \cdots p_m$. Consider the following congruence equation system:

$$\begin{cases} c \equiv b \pmod{p^2} \\ c \equiv 0 \pmod{kQ}, \end{cases}$$

where the integer b is the one guaranteed by the remark above. The Chinese Remainder Theorem guarantees the existence of $c \in \mathbb{Z}$ that is a solution to the above system since p does not divide kQ. It follows that

$$\begin{cases} f_u(c) \equiv f_u(b) \pmod{p^2} \\ f_u(c) \equiv f_u(0) \pmod{kQ}. \end{cases}$$

In particular, observe that the prime p divides $f_u(c)$, but p^2 does not, due to our particular choice of b (recall that we may change b for $b+p$ if necessary).

We will now prove that every prime that divides $f_u(c)$ is $\equiv 1 \pmod{k}$ (except for p). Let r be a prime divisor of $f_u(c)$ different from p. In Theorem 3.7 we have shown that every prime divisor of f_u divides k, divides $\Delta(f_u)$, or is $\equiv 1, \ell \pmod{k}$. To reach a contradiction, suppose $r \not\equiv 1 \pmod{k}$. Thus, $r \equiv \ell \pmod{k}$ or r divides k or $\Delta(f_u)$, so r divides $kq_1q_2\cdots q_t p_2 p_3 \cdots p_m = kQ$. Since $f_u(c) \equiv f_u(0) \pmod{kQ}$ and r is a divisor of kQ, we deduce that $f_u(c) \equiv f_u(0) \pmod{r}$. But r is a divisor of $f_u(c)$, so $f_u(c) \equiv 0 \pmod{r}$. Therefore, $f_u(0) \equiv 0 \pmod{r}$. Thus, it must happen that r is a prime factor of $f_u(0)$, all of which are $\equiv 1 \pmod{k}$, thanks to Lemma 3.12. This forces r to be $\equiv 1 \pmod{k}$, a contradiction. Therefore, $f_u(c)$ is only divisible by primes $\equiv 1 \pmod{k}$ (and by p).

Finally, from the fact that $f_u(c)$ has every prime divisor $\equiv 1 \pmod{k}$ except for p, it follows, mod k, that $f_u(c) = 1 \cdot 1 \cdots 1 \cdot \ell = \ell$ (note that ℓ only appears once because

$p \equiv \ell \pmod{k}$ and the fact that p^2 does not divide $f_u(c)$). However, observe that $f_u(c) \equiv f_u(0) = \Phi_k(u) \equiv 1 \pmod{k}$, due to Lemma 3.12. This is a contradiction since $\ell \not\equiv 1 \pmod{k}$. Therefore, the arithmetic progression $\equiv \ell \pmod{k}$ contains infinitely many primes. □

Observe that we have strongly used the equality $f_u(0) = \Phi_k(u)$. It is therefore important to make the following remark.

Remark 3.14. As we have previously said, the proof of the above theorem is due to Schur, and it is detailed in Murty's article [RT08]. In that article, however, $h_u(z)$ is defined as $h_u(z) := (u - z)(u - z^\ell)$, that is, our definition differs in a sign. Now observe Eq. (3.9). If Murty's definition is followed, then

$$f_u(0) = \prod_{s \in S} (\zeta^s - u)(u - \zeta^{\ell s}) = (-1)^{|S|} \prod_{a \in G} (u - \zeta^a),$$

so $f_u(0) = (-1)^{\varphi(k)/2} \Phi_k(u)$. However, $\varphi(k)/2$ is not necessarily even. In order for the equality $f_u(0) = \Phi_k(u)$ to hold, we changed the sign in $h_u(z)$ with respect to Murty's definition.

One more remark should be made.

Remark 3.15. Observe that to prove the previous theorem we need to suppose the existence of a prime $p \equiv \ell \pmod{k}$ such that p does not divide $\Delta(f_u)$. This hypothesis is indeed necessary. For instance, take $k = 15$, $\ell = 11$, and $u = 15$ (note that $11^2 = 121 \equiv 1 \pmod{15}$). In this case, following Eq. (3.2), $f_{15}(x) = x^4 + 884x^3 + 293206x^2 + 43243679x + 2392743361$, and a quick calculation with SageMath leads to $\Delta(f_{15}) = 5^3 \cdot 11^2 \cdot 19^2 \cdot 41^2 \cdot 1091^2$. In this case, both the primes 11 and 41 are $\equiv 11 \pmod{15}$, but they both divide $\Delta(f_{15})$.

However, in Murty's article he does not require this additional constraint over p. In fact, he states: "Now pick some prime $p \equiv \ell \pmod{k}$ *so that* p does not divide the discriminant of f". The case $k = 15$ and $\ell = 11$ is a counterexample to this statement, so the "so that" in his article should be changed to a "such that". Thus, this extra hypothesis over p is needed for the argument to work[13].

3.1.1 Case $\ell \equiv 1 \pmod{k}$

The particular case when $\ell \equiv 1 \pmod{k}$ can now be easily proved:

Corollary 3.16. *There are infinitely many primes* $\equiv 1 \pmod{k}$.

Proof. Observe that Proposition 3.10 tells us that all prime divisors of Φ_k but finitely many are $\equiv 1 \pmod{k}$. However, in Proposition 2.10 we proved that every non-constant polynomial in $\mathbb{Z}[x]$ has infinitely many prime divisors. Since $\Phi_k \in \mathbb{Z}[x]$ is non-constant, the desired result is finally settled. □

[13] Proving that there exists at least one such prime for every k and ℓ relatively prime is technically demanding. In fact, if there existed an easy proof, Dirichlet Theorem 2.3 would be easy to establish. See Section 6.3 in the Appendix for detail.

Therefore, a Euclidean proof for the arithmetic progression $\equiv \ell \pmod{k}$ is available if $\ell^2 \equiv 1 \pmod{k}$. In the general case, the proof starts by supposing there are finitely many primes $\equiv \ell \pmod{k}$; it then finds one specific prime $\equiv \ell \pmod{k}$ and finally uses the Euclidean polynomial f_u to reach a contradiction and conclude there are infinitely many primes of this type. In the case $\ell \equiv 1 \pmod{k}$, it is enough to characterise the prime divisors of the Euclidean polynomial Φ_k and observe that this polynomial has infinitely many prime divisors. In both cases, the proofs we developed match our definition of Euclidean proof.

3.2 The converse problem. Murty Theorem

We are now interested in showing that $\ell^2 \equiv 1 \pmod{k}$ is the only case where we can find Euclidean proofs to Dirichlet Theorem in the way defined in Section 2. Thus, let $f \in \mathbb{Z}[x]$ be a monic, irreducible polynomial such that all its prime divisors but finitely many are $\equiv 1, \ell \pmod{k}$, with infinitely many being $\equiv \ell \pmod{k}$. We are then interested in showing that this necessarily implies that $\ell^2 \equiv 1 \pmod{k}$. This was first proved by Ram Murty in 1988.

To prove his theorem, we will use some algebraic number theory and the Chebotarev Denisty Theorem. We shall follow [Con10] to prove Murty's claim in greater detail and clarity than that offered in his article [RT08]. Again, let ζ be a kth primitive root of unity, let K be any number field[14], and recall that in characteristic zero $K(\zeta)/K$ is a Galois extension since $x^k - 1$ is separable over K. Hence, $x^k - 1$ has k different roots in the splitting field over K, which is $K(\zeta)$. Before proceeding to the next theorem, recall the concepts in Section 2.5, Section 2.6 and Section 2.7. Specifically recall that in Section 2.6 we defined the set $S_1(k, K)$ as

$$S_1(k, K) := \{b \bmod k : p \equiv b \pmod{k} \text{ for infinitely many } p \in \mathrm{Spl}_1(K)\}. \tag{3.12}$$

Theorem 3.17 (Conrad). *Let $\psi : \mathrm{Gal}(K(\zeta)/K) \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, where $\psi(\sigma) = \sigma|_{\mathbb{Q}(\zeta)}$ for every $\sigma \in \mathrm{Gal}(K(\zeta)/K)$. Then, $\mathrm{Im}(\psi) = S_1(k, K)$.*

Proof. The initial setup is the number field tower of extensions $K(\zeta)/K/\mathbb{Q}$. We will first justify that the set $S_1(k, K)$ can be more conveniently written as

$$S_1(k, K) = \{q \bmod k : q \in \mathrm{Spl}_1(K), q \text{ unramified in } K(\zeta)\}. \tag{3.13}$$

We will first see that the left side of Eq. (3.13) is contained in the right side. Each congruence class in $S_1(k, K)$ contains infinitely many primes p from $\mathrm{Spl}_1(K)$ by definition, and for each of these primes, there exists some prime ideal $\mathfrak{p}$ dividing $p\mathcal{O}_K$ with $f_{K/\mathbb{Q}}(\mathfrak{p}|p) = 1$. Now, recall Remark 2.19: in any non-trival number field extension over $\mathbb{Q}$ the number of primes that ramify is finite. Thus, each of the classes in $S_1(k, K)$ has a prime representative in $\mathrm{Spl}_1(K)$, q, which is unramified in $K(\zeta)$.

We will now see that the right side of Eq. (3.13) is contained in the left side. Let q belong to $\mathrm{Spl}_1(K)$ with q unramified in $K(\zeta)$. We will prove that q belongs to $S_1(k, K)$ by showing infinitely many primes p lying in $\mathrm{Spl}_1(K)$ that satisfy $p \equiv q \pmod{k}$. By hypothesis, choose $\mathfrak{q}$ dividing $q\mathcal{O}_K$ in K such that $f_{K/\mathbb{Q}}(\mathfrak{q}|q) = 1$.

[14]Here K denotes a general number field, and not specifically $\mathbb{Q}(\zeta)$, as it did in the previous section.

Since q is unramified in $K(\zeta)$, it follows that $\mathfrak{q}$ is also unramified in $K(\zeta)$. Thus, one can define the Frobenius element $\sigma := \mathrm{Frob}_{\mathfrak{q}}$ of $\mathrm{Gal}(K(\zeta)/K)$, which is a unique, well-defined element since $K(\zeta)/K$ is an abelian extension. The defining property of the Frobenius element yields

$$\sigma(\zeta) \equiv \zeta^{\mathrm{N}(\mathfrak{q})} \pmod{\mathfrak{b}}, \tag{3.14}$$

for any prime ideal $\mathfrak{b}$ lying over $\mathfrak{q}$ in $K(\zeta)$. By the canonical isomorphism between $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $(\mathbb{Z}/k\mathbb{Z})^\times$, we identify $\zeta^{\mathrm{N}(\mathfrak{q})}$ with $\mathrm{N}(\mathfrak{q}) \bmod k$. Therefore, since the restriction $\sigma|_{\mathbb{Q}(\zeta)}$ is fully determined by Eq. (3.14) and σ fixes $\mathbb{Q}$, we have

$$\sigma|_{\mathbb{Q}(\zeta)} = \mathrm{N}(\mathfrak{q}) \bmod k = q \bmod k, \tag{3.15}$$

where we use that $\mathrm{N}(\mathfrak{q}) = q^{f_{K/\mathbb{Q}}(\mathfrak{q}|q)}$. Using Chebotarev Density Theorem for the (abelian) cyclotomic extension $K(\zeta)/K$ (Corollary 2.31), there exist infinitely many prime ideals $\mathfrak{p}$ in K satisfying

$$\begin{aligned} &\text{(i)} \ \ \mathfrak{p} \text{ is unramified in } K(\zeta), \\ &\text{(ii)} \ \ \mathrm{Frob}_{\mathfrak{p}} = \sigma, \\ &\text{(iii)} \ \ f_{K/\mathbb{Q}}(\mathfrak{p}|p) = 1, \end{aligned} \tag{3.16}$$

where p arises from $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. In light of Lemma 2.28 and Remark 2.29, the intersection of the set of prime ideals satisfying the third condition and the set of prime ideals satisfying the first two conditions in Eq. (3.16) is indeed infinite: the density of the set of primes $\mathfrak{p}$ with inertia degree 1 is equal to one due to Remark 2.27, and the density of the unramified primes $\mathfrak{p}$ in $K(\zeta)$ with Frobenius element equal to σ is positive due to Corollary 2.31.

We then have that p belongs to $\mathrm{Spl}_1(K)$ by construction. Therefore, since $\mathrm{N}(\mathfrak{p}) = p$ and $\sigma = \mathrm{Frob}_{\mathfrak{p}}$,

$$\sigma|_{\mathbb{Q}(\zeta)} = p \bmod k,$$

which, comparing with Eq. (3.15), yields $p \equiv q \pmod{k}$ for infinitely many primes p of $\mathrm{Spl}_1(K)$. This finally settles Eq. (3.13).

We now turn our attention to the main claim in the theorem. Let $H := \mathrm{Im}(\psi)$[15]. We will start by proving that $S_1(k, K) \subseteq H$. For this goal, pick a congruence class $q \bmod k$ in $S_1(k, K)$ in the notation of Eq. (3.13). We know (see Eq. (3.15)) that $q \bmod k = \sigma|_{\mathbb{Q}(\zeta)}$, because, by hypothesis, there exists some $\mathfrak{q}$ lying over q in K with $f_{K/\mathbb{Q}}(\mathfrak{q}|q) = 1$ and also q is unramified in $K(\zeta)$. This means that $q \bmod k$ belongs to $\mathrm{Im}(\psi)$ and, hence, $S_1(k, K) \subseteq H$.

We will now prove that $H \subseteq S_1(k, K)$. Let $b \bmod k \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, with $\sigma|_{\mathbb{Q}(\zeta)} = b \bmod k$ for some $\sigma \in \mathrm{Gal}(K(\zeta)/K)$. This way, $b \bmod k$ belongs to H. Again, using Chebotarev Density Theorem with this automorphism σ, we have the same three results as in Eq. (3.16). In view of this, pick one prime ideal $\mathfrak{p}$ of K so that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ and p belongs to $\mathrm{Spl}_1(K)$. We have that $\mathrm{N}(\mathfrak{p}) = p$ and $\mathrm{Frob}_{\mathfrak{p}} = \sigma$. Therefore, we may write

$$\sigma|_{\mathbb{Q}(\zeta)} = \mathrm{N}(\mathfrak{p}) \bmod k = p \bmod k.$$

Thus, $p \equiv b \pmod{k}$, and since the number of such primes p is infinite due to Chebotarev Density Theorem, $b \bmod k$ lies in $S_1(k, K)$, using Eq. (3.12). □

[15]The letter H is not chosen randomly, since we will see that $H := \mathrm{Im}(\psi) = S_1(k, K)$ and a Euclidean polynomial f for the arithmetic progression $\equiv \ell \pmod{k}$ satisfies $S_1(k, f) = \{1, \ell\} = H$, following the notation of Section 3.1.

Now, we have that the subset $S_1(k, K)$ is the image of the morphism ψ. Since $\mathrm{Gal}(K(\zeta)/K)$ is a group, one deduces that $S_1(k, K)$ is a subgroup (of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/k\mathbb{Z})^\times$). Murty Theorem now follows easily.

Corollary 3.18 (Murty). *Let $f \in \mathbb{Z}[x]$ be a Euclidean polynomial. Then, $\ell^2 \equiv 1 \pmod{k}$.*

Proof. Suppose $\ell \not\equiv 1 \pmod{k}$, for otherwise the claim of the corollary is obvious. Assume that we have a Euclidean polynomial, f, for the congruence class ℓ mod k with $\gcd(k, \ell) = 1$. In other words, we are supposing that $S_1(k, f) = \{1, \ell\}$, for a monic, irreducible polynomial f, in light of Remark 2.22. Let θ be a root of f. The same remark tells us that we may identify $S_1(k, \mathbb{Q}(\theta))$ with $S_1(k, f)$.

We can now use Theorem 3.17 with $K := \mathbb{Q}(\theta)$. From this result we deduce that $S_1(k, \mathbb{Q}(\theta)) = S_1(k, f) = \{1, \ell\}$ is the image of the morphism ψ. Thus, $H := \{1, \ell\}$ is a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$. In particular, H is a group, so, by Lagrange Theorem, the order of ℓ must divide the order of H, which is 2. Since we are supposing $\ell \not\equiv 1 \pmod{k}$, the order of ℓ must be 2, so $\ell^2 \equiv 1 \pmod{k}$. □

Therefore, the complete theorem stands now in its full form: there exists a Euclidean proof of the infinitude of primes $\equiv \ell \pmod{k}$ if and only if $\ell^2 \equiv 1 \pmod{k}$[16]. While it is true that we managed to find proofs *à la Euclid* in these cases, the path to obtain them is not elemental. For one part, Theorem 3.13 requires a strong hypothesis, since we needed to suppose the existence of one prime $\equiv \ell \pmod{k}$ for every k and ℓ, which is tantamount to Dirichlet Theorem. We also used Dirichlet's result to show that f_u is a Euclidean polynomial. Moreover, we needed Chebotarev Density Theorem, which is, in fact, a deeper result than Dirichlet Theorem itself.

In Section 4 we will see that for *specific* values of k and ℓ we are able to find Euclidean *and* elementary proofs of the infinitude of primes $\equiv \ell \pmod{k}$. Once the arithmetic progression is fixed, the existence theorems and hypothesis we needed in this section will be replaced by simple checks.

3.3 Abundance of Euclidean proofs

Now that we know when Euclidean proofs are possible, it is natural to ask how often the condition $\ell^2 \equiv 1 \pmod{k}$ occurs. In other words, for a fixed k, we ask ourselves how many congruence classes satisfy $\ell^2 \equiv 1 \pmod{k}$ out of the $\varphi(k)$ classes mod k with infinitely many primes. As a first approach, note that, for every k, the congruence class $\ell = k - 1$ contains infinitely many primes, and this can be shown in a Euclidean way since $\ell = k - 1 \equiv -1 \pmod{k}$, so $\ell^2 \equiv (-1)^2 = 1 \pmod{k}$. The same reasoning shows that a Euclidean proof is available for the class $\ell = 1$.

To fully answer our question, recall how the group $G = (\mathbb{Z}/k\mathbb{Z})^\times$ breaks down into cyclic groups (see Lemma 6.1 and Lemma 6.2 in Section 6.1 in the Appendix). In particular,

$$(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}, \quad (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad (\mathbb{Z}/16\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},$$

and every $(\mathbb{Z}/2^r\mathbb{Z})^\times$ with $r \geqslant 3$ will be isomorphic to a product of two cyclic groups.

[16]The condition $\ell^2 \equiv 1 \pmod{k}$ is special because it characterises when $H = \{1, \ell\}$ is a group.

In view of Lemma 6.2 and the Chinese Remainder Theorem, for every k, the group G will be a finite product of some cyclic groups (see Eq. (6.1) and Eq. (6.2) in the Appendix). Therefore, a residue class in G will be a tuple $\bar{x} := (x_1, x_2, \ldots, x_t)$, where t will be determined by the number of odd divisors of k and by the power of 2 that divides k. If we define the natural number $d_o \geqslant 1$ by $d_o := \#\{p \text{ odd prime: } p \text{ divides } k\}$, then the value of $t \geqslant 1$ is given by

$$t = \begin{cases} d_o, & \text{if 4 does not divide } k, \\ d_o + 1, & \text{if } k \equiv 4 \pmod 8, \\ d_o + 2, & \text{if } k \equiv 0 \pmod 8, \end{cases} \tag{3.17}$$

where 2 precisely dividing k adds no extra terms to the tuple $\bar{x}$, $2^2 = 4$ precisely dividing k adds one term to $\bar{x}$, and 2^r precisely dividing k for $r \geqslant 3$ adds two terms to $\bar{x}$.

Recall that we are looking for residue classes of order 2, that is $\bar{x}^2 = (x_1^2, x_2^2, \ldots, x_t^2) = 1$. Thus, every x_i, $1 \leqslant i \leqslant t$, must have order dividing 2 (that is, they must be the trivial element or have order 2).

Let p be an odd prime and let $r \geqslant 1$ be an integer. The question now turns to finding out how many elements of order 2 lie in the group $C_{(p-1)p^{r-1}}$ (the cyclic group of order $(p-1)p^{r-1}$). Observe that the order of $C_{(p-1)p^{r-1}}$ is even, since p is odd. Therefore, since C_n has exactly $\varphi(d)$ elements of order d for any $d \in \mathbb{N}$ dividing $n \geqslant 1$, the cyclic group $C_{(p-1)p^{r-1}}$ has exactly $\varphi(2) = 1$ element of order 2, which must be -1. For the same reason, $C_{2^{r-2}}$ has 1 element of order 2 for every $r \geqslant 3$.

Thus, for $(x_1^2, x_2^2, \ldots, x_t^2) = 1$ to be true, it must happen that $x_i = \pm 1$, so there are two options for every x_i. In conclusion, for a fixed k, the number of residue classes that satisfy $\ell^2 \equiv 1 \pmod k$ is 2^t, with t defined in Eq. (3.17). Therefore, our initial question comes down to the ratio $2^t/\varphi(k)$ for every k.

3.4 An alternative interpretation

Again denote $K := \mathbb{Q}(\zeta)$, where ζ is a kth primitive root of unity. Recall that the set $\mathrm{Spl}_1(L)$ is defined for every number field L as

$$\mathrm{Spl}_1(L) = \{p : \text{some } \mathfrak{p} \text{ lying over } p \text{ in } L \text{ has } f_{L/\mathbb{Q}}(\mathfrak{p}|p) = 1\}.$$

A careful reading of the results in Section 3.1 leads to a characterisation of the set $\mathrm{Spl}_1(L)$ in terms of congruences for every subextension L of K satisfying $[K : L] \leqslant 2$.

By the Fundamental Theorem of Galois Theory, every subfield L of K with $[K : L] \leqslant 2$ must be the fixed field of a subgroup H of $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/k\mathbb{Z})^\times = G$ of index at most 2. The corresponding subset $H \subseteq G$ must be of the form $H = \{1, \ell\}$ for some $\ell \in G$, additionally satisfying $\ell^2 \equiv 1 \pmod k$ for it to be a subgroup of G. Observe that every subgroup of index 2 must be of this form. Observe that in Theorem 3.7 and Proposition 3.8 we have effectively studied the prime divisors of a polynomial generating every subfield L of K with $[K : L] = 2$. In particular, thanks to Remark 3.5, this polynomial is also the minimal polynomial of the algebraic element η which makes $L = \mathbb{Q}(\eta)$. The case $[K : L] = 1$ means that $L = K$, and H is the trivial group. We have also studied the prime divisors of the corresponding generating polynomial in Proposition 3.10, which in this case is the minimal polynomial of ζ.

Furthermore, in the above-cited results we have described the form of these prime divisors in terms of congruences. Let $B \subset A$ be two infinite sets, with $\#(A \setminus B)$ being finite. We shall then write $A \simeq B$. With this notation, and recalling Remark 3.9 and Remark 3.11, we have seen the following:

(a) If $[K : L] = 2$, the subfield $L = K^H = \mathbb{Q}(\eta)$ is generated by the roots of the irreducible polynomial $h := f_u$, which is the minimal polynomial of η. Moreover, the prime divisors of h are

$$\mathrm{Spl}_1(h) \simeq \{p : p \equiv 1, \ell \pmod{k}\}. \tag{3.18}$$

(b) If $L = K$, the field K is generated by the roots of the kth cyclotomic polynomial, $h := \Phi_k$, which is the minimal polynomial of ζ. Moreover, the prime divisors of h are

$$\mathrm{Spl}_1(h) \simeq \{p : p \equiv 1 \pmod{k}\}. \tag{3.19}$$

In order to translate the above reciprocity laws to statements involving the set $\mathrm{Spl}_1(L)$ we need Dedekind Criterion (see Theorem 2.17). Then, p being a prime divisor of h means that $h \bmod p$ has a linear factor $\overline{h_i} \in \mathbb{F}_p[x]$, so $\deg(\overline{h_i}) = f_i = 1$, where f_i is the inertia degree of the prime ideal corresponding to $\overline{h_i}$ lying above p.

Since the extension $L/\mathbb{Q}$ is Galois, every irreducible factor mod p of h has degree 1 (see Proposition 2.16). Dedekind Criterion establishes that the shape of the factorization of p in $\mathcal{O}_L$ mirrors that of $h \bmod p$ into irreducible factors. Thus, p has a prime ideal factor $\mathfrak{p}$ with $f(\mathfrak{p}|p) = 1$ in L exactly when p belongs to $\mathrm{Spl}_1(h)$. This is effectively a description of the set $\mathrm{Spl}_1(L)$ in terms of $\mathrm{Spl}_1(h)$. Observe that Dedekind Criterion works for the primes in Eq. (3.18) and Eq. (3.19), since they do not divide $\Delta(\mathbb{Z}[\eta]) = \Delta(h)$ by construction.

Therefore, one can interpret the results in Section 3.1 as reciprocity laws for L in the following terms:

(a) If $[K : L] = 2$, then

$$\mathrm{Spl}_1(L) \simeq \{p : p \equiv 1, \ell \pmod{k}\}. \tag{3.20}$$

(b) If $L = K$, then

$$\mathrm{Spl}_1(L) \simeq \{p : p \equiv 1 \pmod{k}\}. \tag{3.21}$$

The first result is new to the literature, while the second one was already known. Let g be any polynomial generating the extension $L/\mathbb{Q}$ lying below K. In general, a characterisation of $\mathrm{Spl}_1(g)$ (and of $\mathrm{Spl}_1(L)$) is well-known if g is a quadratic or cyclotomic polynomial (see [Wym72]). In the first case, the explicit rules to describe $\mathrm{Spl}_1(L)$ arise from the Quadratic Reciprocity Law (see Theorem 6.4), while the characterisation of $\mathrm{Spl}_1(L)$ we have obtained for $L = K$ is an example of the second case. However, as far as the author is concerned, an explicit characterisation of $\mathrm{Spl}_1(L)$ for L lying below the kth cyclotomic field with $[K : L] = 2$ had not been explicitly given before.

Remark. While it is true that $\mathrm{Spl}_1(L)$ may contain more primes than those specified in Eq. (3.20) and Eq. (3.21), there can only exist finitely many such primes. Also, the strict equality $\mathrm{Spl}_1(h) = \mathrm{Spl}_1(L)$ is not in general true. Using SageMath one can easily

see that there exists some prime divisor of h not $\equiv 1, \ell \pmod{k}$, for which every prime ideal $\mathfrak{p}$ lying above p has $f_{L/\mathbb{Q}}(\mathfrak{p}|p) \neq 1$. Thus, p belongs to $\mathrm{Spl}_1(h)$ but does not belong to $\mathrm{Spl}_1(L)$.

Take, for example, the case $k = 15$ and $\ell = 11$. The polynomial generating L is $h(x) = x^4 + 884x^3 + 293206x^2 + 43243679x + 2392743361$, with the prime factors of $\Delta(h)$ being $5, 11, 19, 41$ and 1091. A simple calculation reveals that every prime ideal above the prime 19 has inertia degree equal to 2, so 19 does not belong to $\mathrm{Spl}_1(L)$, but it belongs to $\mathrm{Spl}_1(h)$ (since 19 divides $h(4)$).

4 Automated proof generator

This section aims to use the methods developed in Section 3.1 to provide a systematic, elemental, and Euclidean proof on the infinitude of primes $\equiv \ell \pmod{k}$ whenever $\ell^2 \equiv 1 \pmod{k}$ (Remark 2.1 also applies here). One may have observed in the previous section that the Euclidean proofs we developed in Proposition 3.10 and Theorem 3.13 require something more than just basic divisibility properties. In fact, deep number theory results are needed to establish the scope of Euclidean proofs. Now, k and ℓ will be fixed so that the Euclidean essence of the proof will not be covered by intricate technicalities, since the existence theorems needed in the previous section will be replaced by simple verifications. We will evidence that Euclidean proofs of the infinitude of primes are of particular interest because they mimic the simplicity of Euclid Theorem 2.2, bypassing the technical difficulties of Dirichlet's argument. In fact, in this section the term "Euclidean proof" is used to indicate that a certain proof follows the spirit of Euclid's. If one wants to make this concept precise, going back to the technical results of Section 3 is inevitable.

Therefore, the objective of this section is to create a Euclidean, *automated proof generator* of the infinitude of primes $\equiv \ell \pmod{k}$, only using the user-supplied choice of k and ℓ. In particular, given this pair of integers, our code will return a complete proof of the infinitude of primes in the specified arithmetic progression[17], which will slightly vary depending on the supplied values of k and ℓ. As far as the author is aware, this automated approach is a new contribution to the literature concerning not only Euclidean proofs but also general elemental proofs of Dirichlet Theorem. This part of the thesis will shed light on the methods used in previous sections, as well as confirming that the ideas described there work in specific cases.

The final proofs will be presented in an interactive and accessible way, so everyone can get their own Euclidean proof. For this goal, a Git repository with the code and a webpage[18] displaying the final proofs have been created.

We will now present the general method to construct Euclidean proofs. The small cases $k = 1, 2, 3, 4, 6$ are degenerate, and we shall not consider them here. They are discussed in Section 6.4 in the Appendix for completeness.

4.1 Building the proof

In order to build the Euclidean proof, it is enough to follow Theorem 3.13. As we said before, all the technical steps needed to obtain the proof offered in that theorem will be replaced by simple checks. In fact, the only obstacle we will face when trying to build the proof will be justifying that our Euclidean polynomial f_u has all its prime divisors $\equiv 1, \ell \pmod{k}$ (except for finitely many)[19]. We will assume this to be true, and prove this property of f_u separately afterwards (following the ideas in Theorem 3.7).

It will be illustrative to go through a representative example and see how the proof has been built using the results in the previous sections, together with the SageMath functions

[17] The code that generates the automatic proofs can be found in Section 6.5 in the Appendix. See also this section to understand how Python and LaTeX have been combined to produce these proofs.

[18] Access https://github.com/joarca01/final-math-bsc-thesis to visit the Git repository with the code, and http://167.172.185.115, to access the webpage.

[19] We will not need to use the fact that f_u is irreducible and that it has infinitely many prime divisors $\equiv \ell \pmod{k}$.

that effectively implement it (which are hosted in the mentioned Git repository). The boxed paragraphs contain the actual proof generated by our automatic program.

We will start with a case where $\ell \not\equiv 1 \pmod{k}$. Consider the arithmetic progression $\equiv 4 \pmod{15}$ (note that it satisfies Murty's condition[20]). We begin the proof by simply stating what polynomial to consider (this polynomial is obviously the irreducible polynomial f_u in Eq. (3.2), yet the subscript u is dropped):

> We will prove that the arithmetic progression $\equiv 4 \pmod{15}$ contains infinitely many primes. Equivalently, we will see that there are infinitely many primes of the form $15n + 4$, $n \geqslant 0$. For this purpose, consider the polynomial
>
> $$f(x) := x^4 + 883x^3 + 292728x^2 + 43186723x + 2392743361.$$

This polynomial is built using the 15th primitive root of unity $\zeta := e^{2\pi i/15}$ and the coset representatives of $H = \{1, 4\}$ in $G = (\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$, which are $1, 2, 7$ and 11. Also, it suffices to choose $u = 15$ to satisfy Proposition 3.4 and Lemma 3.12 (since u is now fixed, the subscript of f_u is dropped). The SageMath functions that implement these calculations are coprimes, coset_reps, f_polynomial_roots and polynomial. We then write:

> Suppose there are finitely many primes $\equiv 4 \pmod{15}$ and denote them by $p_1, p_2, \ldots, p_m$. Since $19 \equiv 4 \pmod{15}$, we can write the list as $19, p_2, p_3, \ldots, p_m$ (so $p_1 = 19$). Now, let $Q := 2 \cdot 3 \cdot 5 \cdot 17 \cdot 239 \cdot p_2 p_3 \cdots p_m$. Consider the following congruence equation system:
>
> $$\begin{cases} c \equiv 7 \pmod{19^2} \\ c \equiv 0 \pmod{15Q}. \end{cases}$$
>
> The Chinese Remainder Theorem guarantees the existence of $c \in \mathbb{Z}$ that is a solution to the above system since 19 does not divide $15Q$. It follows that
>
> $$f(c) \equiv f(7) = 2709699364 \equiv 19 \cdot 8 \pmod{19^2},$$
>
> $$f(c) \equiv f(0) = 61 \cdot 39225301 \pmod{15Q}.$$
>
> In particular, observe that the prime $p_1 = 19$ divides $f(c)$, but 19^2 does not.

In order to keep the structure of a Euclidean proof, we first reproduce the contradiction argument of Theorem 3.13, proving the required properties of f later on in the proof. Observe that we effectively compute the integer b guaranteed by Proposition 3.8 through the function find_b_value. Also, the prime $p \equiv 4 \pmod{15}$ (not dividing $\Delta(f) = 2^6 \cdot 3^8 \cdot 5^6 \cdot 17^2 \cdot 239^2$) which we suppose exists by hypothesis is calculated with find_prime and added as the first term of the list of primes $\equiv 4 \pmod{15}$. Note that we know that such a prime exists due to Dirichlet Theorem 2.3 and the fact that $\Delta(f)$ has finitely many prime divisors. We also look for any other primes $p' < p$ satisfying $p' \equiv 4 \pmod{15}$ with the function prev_primes. If they existed, we would also add them to the list (in the case considered no such primes exist).

[20]Our webpage can return a list of all the possible values of ℓ that satisfy $\ell^2 \equiv 1 \pmod{k}$, given a value of k, thus showing what progressions can be handled with our code.

Observe how both the existence of the integer b and the prime p needed to be proved or added as a hypothesis in Section 3.1, respectively. However, in this section we do not need these theoretical results. Once k and ℓ are fixed, only a few lines of code are needed to obtain the values of p and b.

Note that the first five terms of Q are the prime divisors of $\Delta(f)$. Note that for this we need the explicit factorization of k and $\Delta(f)$. Also, $f(7) \bmod 19^2$ has been factored this way to clearly show that it is divisible by 19 but not by 19^2. Furthermore, $f(0)$ is explicitly factored into primes, resulting in $f(0) = 61 \cdot 39225301$. All these factorizations use the built-in SageMath method factor, which should in principle work smoothly. However, as k gets bigger, $\Delta(f)$ and $f(0)$ become very large, ultimately making it impossible for SageMath to work out their factorization and, thus, this part of the proof no longer works. This hindrance will be further analysed —and solved— in Section 4.2.

Next, we prove that every prime that divides $f(c)$ is $\equiv 1 \pmod{15}$ (except for $p_1 = 19$). Here we strongly use Theorem 3.7 and the fact that $f(0)$ is only divisible by primes $\equiv 1 \pmod{15}$.

Lemma. *Every prime that divides $f(c)$ is $\equiv 1 \pmod{15}$ (except for $p_1 = 19$).*

Proof. Let r be a prime divisor of $f(c)$ different from 19. We will later establish that $r = 2, 3, 5, 17, 239$ or $r \equiv 1, 4 \pmod{15}$. For now, we will assume this is true. To reach a contradiction, suppose $r \not\equiv 1 \pmod{15}$. Thus, $r \equiv 4 \pmod{15}$ or $r = 2, 3, 5, 17, 239$, so r divides $15 \cdot 2 \cdot 3 \cdot 5 \cdot 17 \cdot 239 \cdot p_2 p_3 \cdots p_m = 15Q$. Since $f(c) \equiv 61 \cdot 39225301 \pmod{15Q}$ and r is a divisor of $15Q$, we deduce that $f(c) \equiv 61 \cdot 39225301 \pmod{r}$. But r is a divisor of $f(c)$, so $f(c) \equiv 0 \pmod{r}$. Therefore, $61 \cdot 39225301 \equiv 0 \pmod{r}$. Thus, it must happen that $r = 61, 39225301$, which are $\equiv 1 \pmod{15}$. This forces r to be $\equiv 1 \pmod{15}$, a contradiction. Therefore, $f(c)$ is only divisible by primes $\equiv 1 \pmod{15}$ (and by $p_1 = 19$). □

Note that the primes $r = 2, 3, 5, 17, 239$ are the prime divisors of k and $\Delta(f)$, which are the only possible prime divisors of f not $\equiv 1, 4 \pmod{15}$, as described in Theorem 3.7. Moreover, the primes $61, 39225301$ are $\equiv 1 \pmod{15}$, which we know will happen in general because in Lemma 3.12 we saw that $f(0) = \Phi_{15}(15) \equiv 1 \pmod{15}$, and we deduced that every prime divisor of $f(0)$ is $\equiv 1 \pmod{15}$. To end, the contradiction argument is concluded:

Finally, from the fact that $f(c)$ has every prime divisor $\equiv 1 \pmod{15}$ except for $p_1 = 19$ it follows, mod 15, that $f(c) = 1 \cdot 1 \cdots 1 \cdot 4 = 4$ (note that 4 only appears once because $p_1 = 19 \equiv 4 \pmod{15}$ and the fact that 19^2 does not divide $f(c)$). However, observe that $f(c) \equiv f(0) \equiv 1 \pmod{15}$. This is a contradiction. Therefore, the arithmetic progression $\equiv 4 \pmod{15}$ contains infinitely many primes.

We still need to prove the properties that make f suitable for our proof of the infinitude of primes $\equiv 4 \pmod{15}$:

To complete the proof we must justify that every prime divisor p of $f(c)$ either belongs to the finite set

$$T := \{2, 3, 5, 17, 239\} \tag{4.1}$$

or satisfies $p \equiv 1, 4 \pmod{15}$.

To prove the above statement we consider a set S, which is conveniently chosen to be the list of coset representatives of H in G. Since we are interested in calculating the discriminant of f, we write the definition of f in Eq. (3.2), explicitly showing its roots:

Consider the set $S := \{1, 2, 7, 11\}$ and the values $h(\zeta^s) := (\zeta^s - 15)(15 - \zeta^{4s})$, with $s \in S$ and $\zeta := e^{2\pi i/15}$, a 15th primitive root of unity (thus a root of Φ_{15}). A simple calculation shows that f can be written as

$$f(x) = \prod_{s \in S} (x - h(\zeta^s)) = x^4 + 883x^3 + 292728x^2 + 43186723x + 2392743361. \tag{4.2}$$

After this, we just calculate the discriminant of f with the Sage discriminant method and begin the proof of Eq. (4.1) by supposing that p is a prime divisor of f not dividing $\Delta(f)$ or $k = 15$, that is:

Now, suppose that p is a prime divisor of f such that p does not belong to T.

Next, the argument follows exactly Theorem 3.7, inserting $\ell = 4$ where necessary:

Next, consider a field $\mathbb{F}$ containing both the finite field $\mathbb{F}_p$ and ζ^a. Since p divides f, working in $\mathbb{F}$, there exists $a \in \mathbb{Z}$ such that

$$f(a) = \prod_{s' \in S} (a - h(\zeta^{s'})) = 0.$$

Since $\mathbb{F}$ is a field, there exists some $s \in S$ such that $a = h(\zeta^s)$.

Lemma. *The equality $h(\zeta^s) = h(\zeta^{ps})$ holds in $\mathbb{F}$.*

Proof. Observe that the following calculation holds in $\mathbb{F}$:

$$\begin{aligned} h(\zeta^s) = a = a^p = h(\zeta^s)^p &= (\zeta^s - 15)^p (15 - \zeta^{4s})^p \\ &= (\zeta^{ps} - 15^p)(15^p - \zeta^{4ps}) = (\zeta^{ps} - 15)(15 - \zeta^{4ps}) = h(\zeta^{ps}), \end{aligned} \tag{4.3}$$

where we have used Fermat little theorem in the second equality. The fifth equality, on the other hand, relies on the fact that $\mathbb{F}$ has characteristic p (so that $(c+d)^p = c^p + d^p$ for every $c, d \in \mathbb{F}$), and the following one, on Fermat little theorem. □

Therefore, equality Eq. (4.3) means that $h(\zeta^{ps}) = h(\zeta^s)$ is a root of $\overline{f} \in \mathbb{F}[x]$.

Lemma. *$h(\zeta^{ps})$ is also a root of f in $\mathbb{Q}(\zeta)$ (the smallest subfield of $\mathbb{C}$ containing ζ).*

Proof. Begin by noting that the value $h(\zeta^{ps})$ only depends on the value of ps mod 15 since it only appears as an exponent of ζ. Since p does not divide 15 and s is coprime to 15, ps

is coprime to 15 (so ps mod 15 is coprime to 15), and hence ζ^{ps} is a primitive 15th root of unity.

There are now only two options: either ps mod 15 lies in S or ps mod 15 does not lie in S. In the first case, $h(\zeta^{ps})$ is a root of f, observing expression Eq. (4.2). In the latter case, note that every integer ps mod 15 relatively prime to 15 not in S satisfies $ps \equiv 4t \pmod{15}$ for some $t \in S$ (for instance, if ps mod $15 = 13$, pick $t = 7 \in S$ so that $13 \equiv 4{\cdot}7 \pmod{15}$). This means that $h(\zeta^{ps}) = h(\zeta^{4t})$. Let us prove that $h(\zeta^{4t}) = h(\zeta^{t})$, so $h(\zeta^{ps}) = h(\zeta^{4t}) = h(\zeta^{t})$ is also a root of f. Indeed,

$$\begin{aligned} h(\zeta^{4t}) &= (\zeta^{4t} - 15)(15 - \zeta^{4^2 t}) = (\zeta^{4^2 t} - 15)(15 - \zeta^{4t}) \\ &= (\zeta^{t} - 15)(15 - \zeta^{4t}) = h(\zeta^{t}), \end{aligned}$$

where we have used that $\zeta^{4^2 t}$ only depends on the value of $4^2 t$ mod 15 and the fact that $4^2 \equiv 1 \pmod{15}$. Therefore, $h(\zeta^{ps}) = h(\zeta^{t})$ is always a root of f in $\mathbb{Q}(\zeta)$. □

[a] For instance, consider $\mathbb{F} = \mathbb{F}_{p^n}$ with a suitable integer $n \geqslant 1$ such that Φ_{15} has a root ζ. In this context, ζ is not the complex root of Φ_{15}, but rather some root of an irreducible factor of $\overline{\Phi_{15}} \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$.

In the lemma above we choose some element ps mod 15 to give an example. We precisely pick the second-to-last element of the set formed by the elements of $G = (\mathbb{Z}/15\mathbb{Z})^{\times}$ not in S, which in this case is 13. Next, to find a suitable $t \in S$ such that $13 \equiv 4t \pmod{15}$ we use the function try_reps_list. We then continue with:

Lemma. *$h(\zeta^{ps})$ and $h(\zeta^{s})$ are the same root of f in $\mathbb{Q}(\zeta)$.*

Proof. If $h(\zeta^{ps})$ and $h(\zeta^{s})$ were two distinct roots of f in $\mathbb{Q}(\zeta)$, we know because of Eq. (4.3) that they would be the same in $\mathbb{F}$. Therefore, observing expression Eq. (2.4), it follows that $\Delta(f \bmod p) = \Delta(f) \bmod p = 0$, so p divides $\Delta(f) = 2^6 \cdot 3^8 \cdot 5^6 \cdot 17^2 \cdot 239^2$. This is a contradiction with our choice of p. Thus, $h(\zeta^{ps})$ and $h(\zeta^{s})$ are in fact the same root of f in $\mathbb{Q}(\zeta)$. □

Therefore, the equality

$$h(\zeta^{ps}) = (\zeta^{ps} - 15)(15 - \zeta^{4ps}) = (\zeta^{s} - 15)(15 - \zeta^{4s}) = h(\zeta^{s})$$

holds in $\mathbb{Q}(\zeta)$.

Up to this point, the proof of Theorem 3.7 has been strictly followed. In order to keep the proof as simple as possible, we avoid using any Galois Theory, so we instead continue the proof as follows:

Next, write the above equation in terms of $\theta := \zeta^{s}$ and multiply both sides by -1. This changes yield

$$\begin{aligned} 225 - 15(\theta^{p} + \theta^{4p}) + \theta^{(1+4)p} &= 225 - 15(\theta + \theta^{4}) + \theta^{1+4}, \\ -15(\theta^{p} + \theta^{4p}) + \theta^{5p} &= -15(\theta + \theta^{4}) + \theta^{5}. \end{aligned} \tag{4.4}$$

The right-hand side of the equation above does not depend on p. The left-hand side only depends on the value of p mod 15, since p only appears as an exponent of θ, since $\theta = \zeta^{s}$ is

a primitive 15th root of unity. The above equality gives information about p, which is what we are interested in.

We will translate the equality in Eq. (4.4) in $\mathbb{Q}(\theta)$ to an equality of polynomials, which can be easily handled. We will see that the fact that Eq. (4.4) holds implies that p mod 15 belongs to $H := \{1, 4\}$.

To prove this, we will check every value of p such that p mod 15 does not belong to H and conclude that Eq. (4.4) is not true in $\mathbb{Q}(\theta)$ in those cases. Therefore, we shall see the following: if p mod 15 belongs to $G \setminus H = \{2, 7, 8, 11, 13, 14\}$, then $-h(\theta^p) \neq -h(\theta)$. This will automatically imply what we want to prove: since Eq. (4.4) holds, p mod 15 lies in H. To see this, rewrite Eq. (4.4) as

$$-15(\theta^p + \theta^{4p}) + \theta^{5p} + 15(\theta + \theta^4) - \theta^5 = 0 \tag{4.5}$$

and trade θ for x, since the condition Eq. (4.5) in $\mathbb{Q}(\theta)$ is equivalent to the condition

$$-15(x^p + x^{4p}) + x^{5p} + 15(x + x^4) - x^5 = 0 \tag{4.6}$$

in $\mathbb{Q}[x]/(\Phi_{15}(x)) \cong \mathbb{Q}(\theta)$ (Φ_{15} is also the minimal polynomial of θ). We will explicitly write the case $p = 2$ mod 15 (the remaining values of p mod 15 in $G \setminus H$ are left as an exercise to the reader). With this value of p, equation Eq. (4.6) becomes

$$\begin{aligned} A(x) &:= -15(x^2 + x^8) + x^{10} + 15(x + x^4) - x^5 \\ &= x^{10} - 15x^8 - x^5 + 15x^4 - 15x^2 + 15x = 0. \end{aligned}$$

In the text above, we took the first element in $G \setminus H$ and built the final polynomial $A(x)$ with dividend_check. We want to see that $A(x) = 0$ is not true, so we will make use of the fact that $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(\Phi_{15})$ to reduce our problem to showing that $A(x)$ is not a multiple of the 15th cyclotomic polynomial, which will mean that Eq. (4.4) is not true:

If we recall that $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(\Phi_{15}(x))$, the above equation is equivalent to $A(x)$ being a multiple of the 15th cyclotomic polynomial, $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$. Therefore, we are interested in showing that the residue $R(x)$ of the division $A(x)/\Phi_{15}(x)$ satisfies $R(x) \neq 0$, from which our result will follow. A simple Euclidean division of polynomials shows that $A(x) = B(x) \cdot \Phi_{15}(x) + (-15x^7 + 13x^5 + 15x^3 - 15x^2 + 14)$, with $B(x)$ a polynomial of degree 2, so $R(x) = -15x^7 + 13x^5 + 15x^3 - 15x^2 + 14 \neq 0$. Therefore, equality Eq. (4.4) implies that p mod 15 belongs to H, that is, $p \equiv 1, 4 \pmod{15}$.

This calculation involves the quo_rem and degree SageMath methods. This concludes the proof of the properties of f and, therefore, of the Euclidean proof that there exist infinitely many primes $\equiv 4 \pmod{15}$.

Remark 4.1. If one reads Murty's article [RT08], they will notice that the proof he gives for the progression $\equiv 4 \pmod{15}$ is very different from the one we just gave, which is nevertheless based on the ideas developed in his article. He instead uses a much simpler argument, taking advantage of the Quadratic Reciprocity Law. In Section 6.6 in the Appendix we explain why his approach for the case $\equiv 4 \pmod{15}$ does not always work for a general progression $\equiv \ell \pmod{k}$ satisfying $\ell^2 \equiv 1 \pmod{k}$.

4.1.1 Case $\ell \equiv 1 \pmod{k}$

In Section 3 we treated the case $\ell \equiv 1 \pmod{k}$ separately. The proof we will give now is an adapted version of Proposition 3.10. No contradiction argument supposing the existence of finitely many primes $\equiv 1 \pmod{k}$ is needed. In fact, it will suffice to characterise the prime divisors of Φ_k, together with an extra property of this polynomial. Following Proposition 3.10, in the case $\ell \equiv 1 \pmod{k}$ we need to consider our Euclidean polynomial to be Φ_k. To fix ideas, take $k = 21$ and $\ell = 1$ and begin by stating:

Consider the polynomial

$$\Phi_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1.$$

We will specifically show that every prime divisor p of Φ_k either belongs to the finite set

$$T := \{3, 7\}$$

or satisfies $p \equiv 1 \pmod{21}$. To see this, consider the set $S := \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ and the values ζ^s, with $s \in S$ and $\zeta := e^{2\pi i/21}$, a 21st primitive root of unity (thus a root of Φ_{21}). A simple calculation shows that Φ_{21} can be written as

$$\Phi_{21}(x) = \prod_{s \in S} (x - \zeta^s) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1.$$

Again, we compute the discriminant of this polynomial and suppose p is a prime divisor of Φ_{21} such that p does not lie in T. This set has been conveniently defined to contain the divisors of k, that are the only possible prime divisors of Φ_{21} which are not $\equiv 1 \pmod{21}$, as shown in Proposition 3.10.

We now follow the proof in that Proposition, adapting it for the case $k = 21$ where necessary. Once the fact that $\zeta^{ps} = \zeta^s$ is settled, it is immediate to establish that every prime divisor of Φ_{21} either belongs to T or satisfies $p \equiv 1 \pmod{21}$.

This, together with the fact that Φ_{21} has infinitely many primes (see Proposition 2.10[21]) already implies that the arithmetic progression $\equiv 1 \pmod{21}$ contains infinitely many primes.

4.2 Program's operational limit

While no theoretical limit exists, there is a practical limit to the utility of the Euclidean proofs we presented in Section 4.1. In particular, the argument we just presented relies on factoring the values of $\Delta(f)$ and $f(0)$ into primes. On one hand, the value of Q at the beginning of the proof is defined in terms of the prime divisors of $\Delta(f)$. Also, we need the explicit factorization of $\Delta(f)$ to build the set T of (possible) prime divisors of f that are not $\equiv 1, \ell \pmod{k}$. On the other hand, we need to show that every prime divisor of $f(0)$ is $\equiv 1 \pmod{k}$ to reach a contradiction and conclude that every prime divisor of $f(c)$ is $\equiv 1 \pmod{k}$, except for p_1. While we know $f(0) \equiv 1 \pmod{k}$ is true because of Lemma 3.12, in order to keep the argument simple we need to explicitly show every factor of $f(0)$.

[21] The proof of this proposition is also included in the webpage for completeness, being adapted for the polynomial Φ_k.

However, it becomes computationally costly to factor $\Delta(f)$ and $f(0)$ as k becomes larger, since these quantities easily become very big. Ultimately, the SageMath built-in function factor fails to factor these quantities[22]. In Table 4.1 we summarise the corresponding number of digits of $\Delta(f)$ and $f(0)$ for different values of k and ℓ (suppose $f = \Phi_k$ for the cases where $\ell = 1$).

Table 4.1: Number of digits of $\Delta(f)$ and $f(0)$ for different values of k and ℓ.

k	ℓ	**Digits of** $\Delta(f)$	**Digits of** $f(0)$
4	3	1	2
15	4	18	10
30	19	21	12
47	46	883	77
51	50	433	55
63	55	610	65
10	1	3	–
47	1	77	–
143	1	236	–

To further analyse the limit of our program[23], we set a threshold of 2 seconds for the factorization of both $\Delta(f)$ and $f(0)$. If any of the two factorizations exceeds this threshold, a Runtime Error will be raised in the code, considering it to have failed for that case[24].

The diagrams in Fig. 6.1 and Fig. 6.2 in Section 6.7 in the Appendix show how many arithmetic progressions can be effectively handled with our code, taking into account the defined threshold. In particular, the images indicate the execution time (in seconds) of the code that yields the Euclidean proof for the congruence class $\equiv \ell \pmod{k}$. The first value of k for which not every possible value of ℓ can be executed with our program under 2 seconds is $k = 47$ and $\ell = 46$. After this value of k, some more cases can still be executed until $k = 51$, where it fails again. From there onwards, the code often fails to factor $\Delta(f)$, $f(0)$, or both.

4.3 Alternative arguments

In order to bypass the setback detailed in the previous section, we have modified the code so that whenever a factorization fails, an alternative argument is shown in the final Euclidean proof. Our goal is to present auxiliary arguments that do not need the factorization of $\Delta(f)$ or $f(0)$, and that will only be used when one (or both) factorization fails. Although elementary, these arguments will be slightly longer and less direct than the ones in Section 4.1.

[22] Other software (such as *Magma*) has also failed to factor big values of $\Delta(f)$ and $f(0)$.

[23] This practical limit only applies to the factorization of $\Delta(\Phi_k)$ in the case $\ell \equiv 1 \pmod{k}$.

[24] We have noticed that the factorization of a number with SageMath is either computed quickly or takes very long, if finishes at all. Therefore, we consider that 2 seconds is a reasonable limit to determine if the factorization will require considerable time, making the program no longer practical. This has been implemented with the function factor_timeout.

Case 1: The factorization of $\Delta(f)$ (or $\Delta(\Phi_k)$) fails.

In this case, the integer Q at the very beginning of the proof needs to be built differently. Take the case $k = 55$ and $\ell = 34$.

> To prove that there exist infinitely many primes $\equiv 34 \pmod{55}$ we can proceed by contradiction. Suppose there are finitely many primes $\equiv 34 \pmod{55}$ and denote them by $p_1, p_2, \ldots, p_m$. Since $89, 199 \equiv 34 \pmod{55}$, we can write the list as $89, 199, p_3, p_4, \ldots, p_m$ (so $p_2 = 199$). Now, let t be the product of every prime divisor of the discriminant of f (denoted by $\Delta(f)$) different from 199. Define $Q := 89 \cdot t \cdot p_3 p_4 \cdots p_m$.

Also, the prime divisors exceptions of Theorem 3.7 are not made explicit, since they involve factoring $\Delta(f)$. Instead, we write:

> Let r be a prime divisor of $f(c)$ different from 199. We will later establish that r is a prime divisor of $\Delta(f)$, of 55, or $r \equiv 1, 34 \pmod{55}$. For now, we will assume this is true.

When the time comes to prove that every prime divisor of f is either $\equiv 1, 34 \pmod{55}$ or divides $\Delta(f)$ or $k = 55$, we do not make the exceptions explicit. We say:

> We must justify that every prime divisor p of $f(c)$ either belongs to the finite set
>
> $$T := \{p : p \text{ is a prime divisor of } \Delta(f) \text{ or a prime divisor of } 55\}$$
>
> or satisfies $p \equiv 1, 34 \pmod{55}$.

If this alternative argument is needed, certainly $\Delta(f)$ is significantly long. Thus, we avoid displaying its actual value.

Case 2: The factorization of $f(0)$ fails.

In this case, we need to prove that every prime divisor of $f(0)$ is $\equiv 1 \pmod{k}$ in an alternative way. For this we use the following lemma, adapted in the final proofs for the specific values of k and ℓ.

Lemma 4.2. *Every prime divisor of* $\Phi_k(u) = f(0)$ *is* $\equiv 1 \pmod{k}$.

Proof. Let q be a prime divisor of $\Phi_k(u)$, so $\Phi_k(u) \equiv 0 \pmod{q}$. Now, $u^k - 1 \equiv 0 \pmod{q}$, since Φ_k divides $x^k - 1$ (observe Eq. (2.3)). Therefore, the order of u as an element of $(\mathbb{Z}/q\mathbb{Z})^\times$ divides k.

If the order of u is a divisor of k different from k, say k', then u is also a root of $\Phi_{k''} \bmod q$ for some divisor k'' of k', and hence of k. Thus, u is a double root of $x^k - 1 \bmod q$, since both Φ_k and $\Phi_{k''}$ divide $x^k - 1$. But then u would also be a root of the derivative of $x^k - 1 \bmod q$, that is, a root of $kx^{k-1} \bmod q$, because of Proposition 2.12. This necessarily means that $k \equiv 0 \pmod{q}$ or $u \equiv 0 \pmod{q}$.

But neither of these is possible. On one hand, the fact that $u^k \equiv 1 \pmod{q}$ means that $u \not\equiv 0 \pmod{q}$. On the other hand, since u is a non-zero multiple of k, if $k \equiv 0 \pmod{q}$, then $u \equiv 0 \pmod{q}$, which we have just seen is not possible.

Therefore, the order of u must be k. Fermat little theorem guarantees that the order of u divides the order of $(\mathbb{Z}/q\mathbb{Z})^\times$, which is $\varphi(q) = q - 1$. Thus, k divides $q - 1$. We then have $q - 1 \equiv 0 \pmod{k}$, so $q \equiv 1 \pmod{k}$. □

This is inserted in the automated proof (adapted when k is a prime, since the argument is then significantly shorter). Observe that in Lemma 3.12 we also proved this fact in general, without factorizing $f(0)$. However, we avoid using that argument in our automated proof because it involves knowing the prime divisors of Φ_k, so the justification would be considerably longer.

These two modifications make our code work for every value of k and ℓ satisfying $\ell^2 \equiv 1 \pmod{k}$, with the only limitation of long execution times for large values of k. This is caused by the large coefficients of the Euclidean polynomial f.

It is then worth noting that some progressions can be tackled via studying progressions with smaller values of k and ℓ. Specifically, let $k = 2m$ (with m an odd integer), and consider ℓ such that $\ell^2 \equiv 1 \pmod{k}$. Note that ℓ must also be odd to satisfy $\gcd(k, \ell) = 1$. By the Chinese Remainder Theorem, we have:

$$(\mathbb{Z}/2m\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times. \tag{4.7}$$

Thus, a prime p will be $\equiv \ell \pmod{2m}$ if and only if $p \equiv \ell \pmod{2}$ and $p \equiv \ell \pmod{m}$. Since ℓ is odd, the first condition is equivalent to $p \equiv 1 \pmod{2}$, which is trivially satisfied by every prime (except for 2). Therefore, proving that there exist infinitely many primes $\equiv \ell \pmod{2m}$ is equivalent to showing there exist infinitely many primes $\equiv \ell' \pmod{m}$, where $\ell' := \ell \bmod m$.

This is the only case where we can reduce the study of some progression to a simpler one. Observe that a necessary condition to study the progression $\equiv \ell \pmod{k}$ via $\ell' \pmod{k}$ is $\varphi(k) = \varphi(2m) = \varphi(m)$, because of Eq. (4.7). This is the only case such an equality can be established. If we suppose $k := k_1 k_2$ for some integers k_1, k_2, then the equality $\varphi(k_1 k_2) = \varphi(k_2)$ holds if and only if $k_1 = 2$ and k_2 is odd, or $k_1 = 1$ (see Lemma 6.5 in Section 6.1 in the Appendix). This case has been considered in our code. Whenever $k = 2m$ for some odd integer m, the automatic proof conveniently reduces the argument to proving that the arithmetic progression $\equiv \ell' \pmod{m}$ contains infinitely many primes.

5 Conclusions

This thesis admits two possible interpretations. If one is not interested in automated proofs (or even in Euclidean proofs) they could concentrate on reading Section 3.1 and Section 3.4 of this thesis. If such is the interest, one will be happy to learn that we have effectively characterised the set $\mathrm{Spl}_1(L)$ in terms of congruences, where L is a field lying under $\mathbb{Q}(\zeta)$ with $[\mathbb{Q}(\zeta) : L] \leqslant 2$ (ζ is a fixed kth primitive root of unity). This set contains the primes p that have a prime ideal factor in L whose residue field is $\mathbb{Z}/p\mathbb{Z}$. Our characterisation is effectively a reciprocity law, which is nevertheless hidden in Murty and Schur's method to construct Euclidean proofs. As far as the author is concerned, no such characterisation was explicit in the existing literature.

The other possible interpretation of this thesis is to see it as a sort of "instruction manual" to build Euclidean proofs of the infinitude of primes in the arithmetic progression $kn + \ell$ for $n \geqslant 0$. An intrepid reader may want to embark on understanding why these instructions work, so they will again delve into the details explained in Section 3.1 and Section 3.2, ultimately understanding why a Euclidean proof is only possible for progressions satisfying $\ell^2 \equiv 1 \pmod{k}$. The journey towards this result will require going through Schur and Murty's theorems, and making use of advanced results like Chebotarev Density Theorem.

A more practical reader will instead pick an arithmetic progression of their choice and use the webpage to learn in an easier, Euclidean way why it contains infinitely many primes (if that is possible for the chosen progression). The final Euclidean proof is indeed simple, since harder existence theorems are replaced with mere checks once k and ℓ are fixed. Moreover, the definitive proof makes use of polynomials and certain quantities that have been conveniently chosen for the argument to work nicely. If the reader wants to find out how these quantities are built, going back to Section 3 is unavoidable, together with a quick review of Section 4.

Regarding this Section 3, it is important to note that we have clarified some aspects of Murty's article. For example, we have made clear why the integer u in the polynomial h_u needs to be a non-zero multiple of k, which was not previously evident. Moreover, we have also corrected some inaccuracies in that same paper. These include adding a necessary hypothesis to one of its main theorems, as well as defining the polynomial h_u with an opposite sign.

The work we have developed here could be further expanded. For instance, it is natural to ask if there exists a characterisation, in terms of congruences, of $\mathrm{Spl}_1(L)$ in the case $[\mathbb{Q}(\zeta) : L] = n$, for $n \geqslant 3$ (and n dividing $\varphi(k) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$). As of now, no such characterisation is known. With respect to the automated proof generator, it could be investigated whether an alternative, simpler polynomial f could be used to prove the existence of infinitely many primes $\equiv \ell \pmod{k}$. Indeed, the polynomial f we propose contains large coefficients for big values of k, making the final proof somewhat hard to read. Provided a polynomial with smaller coefficients was found, no alternative arguments to bypass the factorization of $f(0)$ or $\Delta(f)$ would be needed.

6 Appendix

6.1 Auxiliary results

In this section, we present additional results that are referenced or utilized throughout the thesis. Due to their supporting nature, these results are included in the Appendix rather than in the main text.

Fix $k > 2$ and recall that G is the multiplicative group of coprime residue classes modulo k. Let $a > 0$ and $r \geqslant 0$ be integers, and let p be a prime. We say that p^r *precisely divides* a if p^r divides a but p^{r+1} does not. We then write $p^r \parallel a$. With this notation, the Chinese Remainder Theorem has the following implication.

Lemma 6.1. *It holds that*

$$G \cong \prod_{p^r \parallel k} (\mathbb{Z}/p^r\mathbb{Z})^\times,$$

where p is a prime and $r \geqslant 0$ is a natural number.

Proof. It is enough to note that every power p^r precisely dividing k will be relatively prime to any other, from which the result follows easily using the Chinese Remainder Theorem. □

Therefore, the group G breaks down as a direct product of abelian finite groups $(\mathbb{Z}/p^r\mathbb{Z})^\times$, of order $\varphi(p^r) = (p-1)p^{r-1}$. This decomposition can be further expressed in terms of cyclic groups (which are unique up to isomorphism). If $p \neq 2$, the group $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is always cyclic. For $p = 2$, the cases $r = 1, 2$ are cyclic, but for $r \geqslant 3$ the group $(\mathbb{Z}/2^r\mathbb{Z})^\times$ breaks down as a direct product of two cyclic groups. Specifically:

Lemma 6.2. *Let C_n denote the cyclic group of order $n \geqslant 1$. If p is an odd prime and $r > 0$ is a natural number, then*

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong C_{(p-1)p^{r-1}}. \tag{6.1}$$

If $p = 2$ and $r \geqslant 3$, then

$$(\mathbb{Z}/2^r\mathbb{Z})^\times \cong C_2 \times C_{2^{r-2}}. \tag{6.2}$$

Moreover, $(\mathbb{Z}/2\mathbb{Z})^\times \cong C_1$ and $(\mathbb{Z}/4\mathbb{Z})^\times \cong C_2$, where we assume that C_1 is the trivial group.

Proof. It is enough to prove that $(\mathbb{Z}/k\mathbb{Z})^\times$ is a cyclic group if $k = 2, 4$ or $k = p^r$, where p is an odd prime and $r \geqslant 1$. This was first proved by Gauss, and a modern version can be found in [Sha93, Pages 61, 62 and 92]. The case $k = 2^r$ for $r \geqslant 3$ can be found in Gauss's original publication [Gau86]. □

We now turn our attention to finding roots of a certain polynomial mod p. This will be relevant due to our Definition 2.6. A useful tool to characterise the set of prime divisors of a polynomial of degree 2 will be the so-called *Quadratic Reciprocity Law* (QRL). Specifically, we are interested in giving conditions on the solutions of the equation $x^2 - a \bmod p$, for some $a \in \mathbb{Z}$.

Let p be a prime not dividing a. We say that a is a *quadratic residue* mod p if there exists a solution to $x^2 \equiv a \pmod{p}$. In other words, a is a quadratic residue mod p if a is a square mod p. Otherwise we say that a is *not a quadratic residue* mod p. With this language we can further define:

Definition 6.3. Given $a \in \mathbb{Z}$ and p an odd prime, the *Legendre symbol* is defined by

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{if } p \text{ divides } a \\ 1, & \text{if } a \text{ is a quadratic residue mod } p \\ -1, & \text{if } a \text{ is not a quadratic residue mod } p. \end{cases}$$

The Legendre symbol has the following properties, which help us determine quadratic residues mod p, and are proved in [Mar87, Chapter 4].

Theorem 6.4 (Gauss Quadratic Reciprocity Law). *Let p and q be two odd primes. Then,*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{if } p \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right), & \text{if } p \text{ and } q \equiv 3 \pmod 4. \end{cases} \tag{6.3}$$

To this, there are two supplemental laws*:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

and

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

To finish this section, we turn our attention to the following property of Euler's phi function:

Lemma 6.5. *Let $m \geqslant 1$ and $n \geqslant 1$ be any integers. Then the equality $\varphi(nm) = \varphi(m)$ holds if and only if $n = 1$ or $n = 2$ and m is odd.*

Proof. We may write

$$m = 2^s \prod_i p_i^{\alpha_i} \prod_j q_j^{\beta_j},$$

for some odd primes p_i, q_j and some integers $s \geqslant 0$ and $\alpha_i, \beta_j \geqslant 1$. Similarly, we write

$$n = 2^t \prod_j q_j^{\gamma_j} \prod_k r_k^{\delta_k}, \tag{6.4}$$

for some odd primes r_k and some integers $t \geqslant 0$ and $\gamma_j, \delta_k \geqslant 1$. Observe that the primes q_j are the common primes in the decomposition of m and n (with possibly different exponents β_j and γ_j). Now, since Euler's function is multiplicative and supposing that m is even ($s \geqslant 1$), we have

$$\varphi(m) = 2^{s-1} \prod_i (p_i - 1) p_i^{\alpha_i - 1} \prod_j (q_j - 1) q_j^{\beta_j - 1}$$

and

$$\begin{aligned} \varphi(nm) &= 2^{t+s-1} \prod_i (p_i - 1) p_i^{\alpha_i - 1} \prod_j (q_j - 1) q_j^{\gamma_j + \beta_j - 1} \prod_k (r_k - 1) r_k^{\delta_k - 1} \\ &= 2^{t+s-1} \prod_i (p_i - 1) p_i^{\alpha_i - 1} \prod_j (q_j - 1) q_j^{\beta_j - 1} \prod_j q_j^{\gamma_j} \prod_k (r_k - 1) r_k^{\delta_k - 1}. \end{aligned}$$

Imposing $\varphi(nm) = \varphi(m)$ and canceling terms we get

$$2^t \prod_j q_j^{\gamma_j} \prod_k (r_k - 1) r_k^{\delta_k - 1} = 1.$$

For the previous equality to hold, the term $\prod_k (r_k - 1) r_k^{\delta_k - 1}$ cannot appear, since r_k are odd primes. Also, $t = 0$ and $\gamma_j = 0$ for every j. Therefore, from Eq. (6.4), we deduce that $n = 1$ if m is even.

However, if m is odd ($s = 0$) we have

$$\varphi(m) = \prod_i (p_i - 1) p_i^{\alpha_i - 1} \prod_j (q_j - 1) q_j^{\beta_j - 1}$$

and

$$\begin{aligned} \varphi(nm) &= 2^{t-1} \prod_i (p_i - 1) p_i^{\alpha_i - 1} \prod_j (q_j - 1) q_j^{\gamma_j + \beta_j - 1} \prod_k (r_k - 1) r_k^{\delta_k - 1} \\ &= 2^{t-1} \prod_i (p_i - 1) p_i^{\alpha_i - 1} \prod_j (q_j - 1) q_j^{\beta_j - 1} \prod_j q_j^{\gamma_j} \prod_k (r_k - 1) r_k^{\delta_k - 1}. \end{aligned}$$

Imposing $\varphi(nm) = \varphi(m)$ we get

$$2^{t-1} \prod_j q_j^{\gamma_j} \prod_k (r_k - 1) r_k^{\delta_k - 1} = 1.$$

For the previous equality to hold, the term $\prod_k (r_k - 1) r_k^{\delta_k - 1}$ cannot appear, since r_k are odd primes. Also, $t = 1$ and $\gamma_j = 0$ for every j. Therefore, from Eq. (6.4), we deduce that $n = 2$ if m is odd. □

We have duplicate labels for some cyclotomic fields: if we let ζ_n denote an nth primitive root of unity, we have $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$ if m is odd. This is the only case two different labels describe the same field in light of Lemma 6.5. Thus, when dealing with the cyclotomic field $\mathbb{Q}(\zeta_n)$, it is common to require n is not twice an odd number, that is, $n \not\equiv 2 \pmod 4$.

6.2 Natural and Dirichlet Density

We have seen in Section 2.7 that, in order to accurately use Chebotarev Density Theorem, one needs to define a measure for sets of primes (or prime ideals). The most natural way to construct a density of a given set of primes is as follows.

Let Π be the set of all prime numbers. Let $S \subseteq \Pi$ be a subset and let p be a prime. For any real number $x \geqslant 1$, we define the *upper natural density* and the *lower natural density* of S in Π as

$$\limsup_{x \to \infty} \frac{\#\{p \in S : p < x\}}{\#\{p \in \Pi : p < x\}}, \quad \liminf_{x \to \infty} \frac{\#\{p \in S : p < x\}}{\#\{p \in \Pi : p < x\}},$$

respectively. If both these densities coincide, we call the common value the *natural density* (or *asymptotic density*) of S in Π, and we write it as

$$\delta(S) := \lim_{x \to \infty} \frac{\#\{p \in S : p < x\}}{\#\{p \in \Pi : p < x\}}.$$

Many properties we would expect are in fact true: if S does have a density, then $0 \leqslant \delta(S) \leqslant 1$, since $\delta(\Pi) = 1$. Also, given that Π is infinite, any finite set of primes will have density equal to 0.

A less restrictive (yet less intuitive) notion of density is obtained via Dirichlet series. Recall that $\sum_{p\in\Pi} p^{-1}$ is divergent, and again let $S \subseteq \Pi$ be a subset. We define the *upper Dirichlet density* and the *lower Dirichlet density* of S in Π as

$$\limsup_{s\to 1^+} \frac{\sum_{p\in S} p^{-s}}{\sum_{p\in\Pi} p^{-s}}, \quad \liminf_{s\to 1^+} \frac{\sum_{p\in S} p^{-s}}{\sum_{p\in\Pi} p^{-s}},$$

respectively. If both these densities coincide, we call the common value the *Dirichlet density* (or *analytic density*) of S in Π, and we write it as

$$d(S) := \lim_{s\to 1^+} \frac{\sum_{p\in S} p^{-s}}{\sum_{p\in\Pi} p^{-s}}. \tag{6.5}$$

The Dirichlet density in Eq. (6.5) can be expressed in a more convenient way. Recall that Euler discovered the following relation between the Riemann zeta function and prime numbers[25]:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\in\Pi} \frac{1}{1-p^{-s}}, \tag{6.6}$$

for any complex number s with $\mathrm{Re}(s) > 1$. Using the formula for the sum of a geometric progression we can further write

$$\zeta(s) = \prod_{p\in\Pi} \sum_{n=0}^{\infty} p^{-ns},$$

since $|p^{-s}| = p^{-\,\mathrm{Re}(s)} < 1$. Now, $\zeta(s)$ has a single pole of order 1 at $s = 1$, so we have that, letting $s \to 1^+$

$$(s-1)\sum_{n=1}^{\infty} \frac{1}{n^s} = (s-1)\zeta(s) = 1 + o(1). \tag{6.7}$$

Taking the logarithm from Eq. (6.7) and using Eq. (6.6) we can write

$$O(1) = \log(s-1) + \log\zeta(s) = \log(s-1) + \sum_{p\in\Pi} \log\left(\frac{1}{1-p^{-s}}\right). \tag{6.8}$$

Now, since $|p^{-s}| < 1$ and $p^{-s} \neq 1$, a Taylor expansion yields

$$\sum_{p\in\Pi} -\log\bigl(1-p^{-s}\bigr) = \sum_{p\in\Pi}\sum_{n=1}^{\infty} \frac{p^{-ns}}{n} \leqslant \sum_{p\in\Pi}\sum_{n=1}^{\infty} p^{-ns}.$$

Since the sum $\sum_{n=1}^{\infty} p^{-ns}$ converges, we can write

$$\sum_{p\in\Pi} -\log\bigl(1-p^{-s}\bigr) = C\sum_{p\in\Pi}\sum_{n=1}^{\infty} p^{-ns}$$

for some constant $C > 0$ and absorb it to write Eq. (6.8) as

$$O(1) = \log(s-1) + \sum_{p\in\Pi}\sum_{n=1}^{\infty} p^{-ns}. \tag{6.9}$$

[25]Here $\zeta(s)$ denotes the Riemann zeta function, not a kth root of unity.

Since the last sum converges absolutely because $\mathrm{Re}(s) > 1$, we can write

$$\sum_{p\in\Pi}\sum_{n=1}^{\infty} p^{-ns} = \sum_{p\in\Pi} p^{-s} + \sum_{p\in\Pi}\sum_{n=2}^{\infty} p^{-ns}. \tag{6.10}$$

We will now see that, in fact,

$$\sum_{p\in\Pi}\sum_{n=2}^{\infty} p^{-ns} = O(1). \tag{6.11}$$

To show this equality, start by noting that

$$\sum_{n=2}^{\infty} p^{-ns} = \frac{p^{-2s}}{1-p^{-s}}.$$

Also, letting $\sigma := \mathrm{Re}(s) > 1$ and observing that $|p^{-s}| = p^{-\sigma} < 1$, we have

$$\left|\frac{p^{-2s}}{1-p^{-s}}\right| \leqslant \frac{p^{-2\sigma}}{1-p^{-\sigma}} \leqslant p^{-2\sigma} C_\sigma,$$

for some constant $C_\sigma > 0$ depending on σ, so the left-hand side of Eq. (6.11) is bounded by

$$\sum_{p\in\Pi}\sum_{n=2}^{\infty} p^{-ns} \leqslant \sum_{p\in\Pi} \frac{p^{-2\sigma}}{1-p^{-\sigma}} \leqslant \sum_{p\in\Pi} \frac{C_\sigma}{p^{2\sigma}}. \tag{6.12}$$

It is now enough to remember that for $\sigma > 1$,

$$\sum_{p\in\Pi} \frac{1}{p^{2\sigma}} < \infty,$$

so, from Eq. (6.12), we finally have

$$\sum_{p\in\Pi}\sum_{n=2}^{\infty} p^{-ns} \leqslant C_\sigma \sum_{p\in\Pi} \frac{1}{p^{2\sigma}} < \infty.$$

Putting Eq. (6.10) and Eq. (6.11) together, we can write Eq. (6.9) as

$$\sum_{p\in\Pi} p^{-s} = -\log(s-1) + O(1),$$

so, observing Eq. (6.5), the Dirichlet density of S is given by

$$\lim_{s\to 1^+} \frac{\sum_{p\in S} p^{-s}}{-\log(s-1)} \tag{6.13}$$

if the limit exists.

It can be shown that the Dirichlet density is a generalisation of the natural density: if the natural density exists, then the Dirichlet density also exists, and they both coincide. However, the converse assertion is not always true. There is an example due to Enrico Bombieri (referenced in [Ser73]) that shows this case. If P^1 is the set of prime numbers whose first digit is equal to one, then P^1 does not have a natural density, but its Dirichlet density does exist and equals $d(P^1) = \log_{10} 2 \approx 0.30102999566$.

It is natural to extend Eq. (6.13) to sets of prime *ideals*. Let $\mathfrak{p}$ be some prime ideal lying above p with $\mathrm{N}(\mathfrak{p}) = p^f$ for some inertia degree f. The generalisation is accomplished through the same procedure we have outlined above, instead using the *Dedekind zeta function*.

Let K be a number field and again let $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. The *Dedekind zeta function* $\zeta_K(s)$ is a function in the complex plane given by

$$\zeta_K(s) := \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1 - \mathrm{N}(\mathfrak{p})^{-s}}, \tag{6.14}$$

where $\mathfrak{a}$ ranges over the non-zero ideals of $\mathcal{O}_K$ and $\mathfrak{p}$ ranges over the non-zero prime ideals of $\mathcal{O}_K$. Dedekind zeta function has only one pole, which is simple, at $s = 1$. In the case $K = \mathbb{Q}$, Eq. (6.14) trivially reduces to the Riemann zeta function.

6.3 Schur Theorem hypothesis

Recall that to prove that there are infinitely many primes $\equiv \ell \pmod{k}$ if $\ell^2 \equiv 1 \pmod{k}$ we strongly use the fact that there exists at least one prime $\equiv \ell \pmod{k}$. In particular, the argument in Theorem 3.13 requires the existence of one such prime, and so it is needed in the automated proof if $\ell \not\equiv 1 \pmod{k}$ (see Section 4.1). Affirming that such a prime exists for every k and ℓ relatively prime requires advanced mathematics. In fact, if we assume this claim to be true, Dirichlet Theorem 2.3 follows easily: we would just need the Chinese Remainder Theorem to obtain Dirichlet's well-known result.

Lemma 6.6. *Suppose that k and ℓ are two fixed, non-zero integers satisfying $\gcd(k, \ell) = 1$. Also suppose that for every such k and ℓ there exists a prime p that is $\equiv \ell \pmod{k}$. Then, there are infinitely many primes $\equiv \ell \pmod{k}$.*

Proof. By hypothesis, there exists a prime $p_1 \equiv \ell \pmod{k}$. Now, since

$$\gcd(k, p_1) = \gcd(k, kn_1 + \ell) = \gcd(k, \ell) = 1,$$

for some $n_1 \in \mathbb{Z}$, the Chinese Remainder Theorem guarantees the existence of $\ell_1 \in \mathbb{Z}$, which is a solution to the system

$$\begin{cases} \ell_1 \equiv \ell \pmod{k} \\ \ell_1 \equiv 1 \pmod{p_1}. \end{cases} \tag{6.15}$$

Now observe that $k_1 := kp_1$ and ℓ_1 satisfy the hypothesis of the lemma. Indeed, for some integer m_1 we have:

$$\gcd(k_1, \ell_1) = \gcd(kp_1, \ell_1) = \gcd(k, \ell_1)\gcd(p_1, \ell_1) = \gcd(k, km_1 + \ell) \cdot 1 = 1 \cdot 1 = 1,$$

where we have used well-known properties of the greatest common divisor, the first equality in Eq. (6.15) to write $\ell_1 = km_1 + \ell$, and the second one to deduce that $\gcd(p_1, \ell_1) = 1$. Thus, there exists one prime $p_2 \equiv \ell_1 \pmod{k_1}$. Observe that $p_2 \equiv \ell \pmod{k}$, using the first equation in Eq. (6.15), and $p_2 \equiv 1 \pmod{p_1}$ using the second one (this last condition shows that $p_2 \neq p_1$). We could now start the argument once again. Suppose we have a prime $p_i \equiv \ell \pmod{k}$ for $i \geqslant 2$. Again,

$$\gcd(k, p_i) = \gcd(k, kn_i + \ell) = \gcd(k, \ell) = 1,$$

for some $n_i \in \mathbb{Z}$, so there exists $\ell_i \in \mathbb{Z}$ which is a solution to the system

$$\begin{cases} \ell_i \equiv \ell \pmod{k} \\ \ell_i \equiv 1 \pmod{p_i}, \end{cases} \tag{6.16}$$

and one can find a new prime $\equiv \ell \pmod{k}$ considering $k_i := kp_i$ and ℓ_i for $i \geqslant 2$. We have

$$\gcd(k_i, \ell_i) = \gcd(kp_i, \ell_i) = \gcd(k, \ell_i)\gcd(p_i, \ell_i) = \gcd(k, km_i + \ell) \cdot 1 = 1 \cdot 1 = 1,$$

where we have used again Eq. (6.16). Thus, there exists a prime $p_{i+1} \equiv \ell_i \pmod{k_i}$, and again $p_{i+1} \equiv \ell \pmod{k}$ and $p_{i+1} \equiv 1 \pmod{p_i}$, so p_{i+1} is yet a new prime $\equiv \ell \pmod{k}$ different from p_i. In this way, infinitely many primes $\equiv \ell \pmod{k}$ can be constructed. □

No proof using elementary techniques is known of the fact that there exists one prime $\equiv \ell \pmod{k}$ for every k and ℓ, so this needs to be a hypothesis of Theorem 3.13.

6.4 Small cases

The automated proofs for the cases $k = 1, 2, 3, 4, 6$ are treated separately, since they are degenerate cases and deserve a special (and somewhat easier) treatment.

6.4.1 Case $k = 1, 2$

In these cases, we can only consider $\ell = 1$ and the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ collapses because $\deg(\Phi_k) = 1$, causing $\mathbb{Q}(\zeta) = \mathbb{Q}$. In these cases, a Euclidean proof can be easily established. In fact, the case $k = 1$ follows directly from Euclid Theorem 2.2. The case $k = 2$ and $\ell = 1$ reads as follows:

Lemma 6.7. *There are infinitely many primes* $\equiv 1 \pmod{2}$.

Proof. Suppose there are finitely many primes $\equiv 1 \pmod{2}$, say $p_1, p_2, \ldots, p_m$. Our goal is to show that there exists yet another prime $\equiv 1 \pmod{2}$ not in our list. For this goal, consider $Q := p_1 p_2 \cdots p_m$ and the polynomial $f(x) := 2x - 1$. Now, $f(Q) = 2p_1 p_2 \cdots p_m - 1 = 2Q - 1$. This number has at least one prime divisor, p, since it is greater than one. We then have that p divides $2Q - 1$.

Next, observe that $p \neq p_i$ for every i such that $1 \leqslant i \leqslant m$: if $p = p_i$ for some i, then p would divide $2Q$. Since p also divides $2Q - 1$, we get that p divides 1, so $p = 1$, which is a contradiction (1 is not a prime). Therefore, p is a prime divisor of $2Q - 1$ not in our list. Finally, note that $2Q - 1$ has all its prime divisors $\equiv 1 \pmod{2}$ since it is odd, so p is a new prime $\equiv 1 \pmod{2}$.

This gives us an infinitude of primes $\equiv 1 \pmod{2}$ provided we have one. Since 3 is a prime $\equiv 1 \pmod{2}$, the desired result is finally settled. □

The case $k = 2$ is the only case where the Euclidean polynomial considered for the proof is not monic. However, $f(x) = 2x - 1$ satisfies every other condition in the definition of Euclidean polynomial in Section 2, and it clearly follows the spirit of Euclid Theorem.

6.4.2 Case $k = 3, 4, 6$

In these cases, $\deg(\Phi_k) = \varphi(k) = |G| = 2$, which leads to $G = H$ in the case $\ell \not\equiv 1 \pmod{k}$. We will consider the same polynomial $f_u(x)$ of Proposition 3.4, but it will now be easy to justify the prime divisors of this polynomial[26]. We just have to note that every prime divisor p of f has to be, in particular, a prime, and that rules out many options. For the case $k = 3$, this means that $p \equiv 1, 2 \pmod 3$ (or $p = 3$); for $k = 4$, $p \equiv 1, 3 \pmod 4$ (or $p = 2$); and for $k = 6$, $p \equiv 1, 5 \pmod 6$ (or $p = 2, 3$).

Therefore, the proof for the cases $\equiv 2 \pmod 3$, $\equiv 3 \pmod 4$, and $\equiv 5 \pmod 6$ can be easily handled using only the contradiction argument at the end of Theorem 3.13, as Theorem 3.7 is not necessary to work out the prime divisors of f. To see how the automatic proofs look in these cases, use the webpage link[27].

The cases $\equiv 1 \pmod k$ are trickier, since we have to show that every prime p that divides f satisfies $p \equiv 1 \pmod k$ (except finitely many cases). In fact, every possible value of k (except for $k = 1, 2$) requires the same treatment when dealing with the case $\equiv 1 \pmod k$. This is already fully described in Section 4.1.1.

6.5 Automated proofs' code

The automated proofs are generated with a combination of SageMath and LaTeX. Roughly speaking, the SageMath code[28] generates the necessary calculations for the specific values of k and ℓ, calling various templates to write the necessary quantities in predefined spaces in the final LaTeX file containing the proof.

Specifically, the main function in our code is called ap_euc (which stands for "Arithmetic Progression Euclidean"), and it only takes two arguments, k and ℓ. After some steps, it writes a LaTeX file with the proof for the selected arithmetic progression univocally defined by these two parameters. This is achieved through the following (simplified) steps:

1. First, the supplied values of k and ℓ are checked to ensure they are positive integers, satisfying $\gcd(k, \ell) = 1$, $\ell^2 \equiv 1 \pmod k$, and $k > \ell$. These are, in fact, the same constraints we imposed at the beginning of Section 2. If any of these conditions is not met, the execution stops and an error arises.

2. If $k = 1, 2$ the code points to a file named `proof_1_mod1.tex` or `proof_1_mod2.tex`, where the proofs for the cases $\equiv 1 \pmod 1$ and $\equiv 1 \pmod 2$ are respectively found. No code is used for these two cases, since they are degenerate, and their proof has been written manually, with a very simple Euclidean argument. The function ap_euc returns here in these cases.

3. Next, an empty dictionary is initialized, where every value, polynomial, sentence, or character that will appear in the final proof is stored. A different key is given to each variable. As an example, the values k and ℓ are saved under the keys "k" and "ell"

[26] Since we have already chosen the integer u in f_u to satisfy Lemma 3.12, we shall write f instead of f_u.

[27] Access http://167.172.185.115 to visit the webpage.

[28] The code developed can be entirely found in the Git repository https://github.com/joarca01/final-math-bsc-thesis.

in the dictionary, while the coprime integers to k are calculated with the function coprimes (which is called from the auxiliary file `utils.ipynb`) and assigned to the key "coprimes_list". Every function we call is either defined in this auxiliary file[29] or is a built-in SageMath function. Some variables (like the "factored_k" below) are not included in the dictionary because they are needed for future calculations but are not directly included in the final LaTeX file.

```
d['k'] = k
d['ell'] = l
d['coprimes_list'] = coprimes(k)
factored_k = ZZ(k).factor(proof=False)
primes_div_k_list = prime_divisors(factored_k)
d['sufix_cyclo_alt'] = sufix_cyclo(k) # Contains the string
                                      'st', 'nd' or 'rd'.
d['eulersphi_k'] = euler_phi(k) # Contains Euler totient
                                function value at k.
```

Note that the variables that are lists have their key ending with "_list". This will be necessary for a correct displaying of lists in the final LaTeX document.

4. Then, the file takes two different routes if $\ell \equiv 1 \pmod{k}$ or else. The first case is slightly simpler.

5. The code again splits between the cases $k = 3, 4, 6$ and every other value of k. In this part of the code, the prime divisors of f must be justified. In the cases $k = 3, 4, 6$, this can be easily done with one sentence, which is stored in a LaTeX file, which we call `template3_alt.tex`. This template is then read in the main function and assigned to the dictionary key "prime_divisors_argument_alt" as follows.

```
if k == 3 or k == 4 or k == 6:

template3_alt = Path('template3_alt.tex').read_text()
d['prime_divisors_argument_alt'] = subst_dictionary(
                                   template3_alt,d)
```

The cases $k = 3, 4, 6$ now go directly to the end of the function (corresponding to the last item of this list). In every other possible value of k, the justification of the prime divisors of f is considerably longer. As before, a template stores a sentence stating that the proof of the form of every prime divisor of f will be given later on in the document.

6. The whole code is written so it can overcome a possible stall of the factorization of $\Delta(f)$ or $f(0)$, as described in Section 4.2 and Section 4.3. Whenever a factorization has to be made, it is encapsulated in a "try/except Runtime Error" clause. The

[29] Access the Git Repository to view the exact code of every function we created in the file `utils.ipynb`.

factorization is first tried in the "try". If it fails in the specified time threshold of 2 seconds, the code jumps to the "except RuntimeError" part, where an alternative argument is instead written in the corresponding variables. The function we use to factor any quantity is the following:

```
def factor_timeout(n, timeout = 2):
with stopit.ThreadingTimeout(timeout) as to_ctx_mgr:
ans = fork(lambda n: ZZ(n).factor(), timeout = timeout)(n)
return ans
if to_ctx_mgr.state in [to_ctx_mgr.TIMED_OUT, to_ctx_mgr.
                                    INTERRUPTED]:
print('The factorization takes too long.')
raise RuntimeError
```

7. It is worth showing the code of the subst_dictionary function, which substitutes the values of the dictionary into a given LaTeX document. This function separates the cases where the value of the key is a list or the key ends with "_alt" from every other case. This is done to ensure that the value is correctly displayed in the final document.

```
def subst_dictionary(template, dictionary):
  for ky, val in dictionary.items():
    if type(val) == list: # Remove the square brackets if val is
                                    a Python list.
      template = template.replace(f'{{{ky}}}', str(latex(val))[6:
                                    -7])
    if ky[-3:] == "alt":
      template = template.replace(f'{{{ky}}}', val)
    else:
      template = template.replace(f'{{{ky}}}', latex(val))
  return template
```

8. Finally, the proof is written in the file `template_euc.tex` (or `template_lcong1_euc.tex` in the case $\ell \equiv 1 \pmod{k}$). The function subst_dictionary above writes every dictionary key in its predefined position in the template. Lastly, a file called `proof_euc.tex` (or `proof_lcong1_euc.tex`) is created, which finally contains the proof of the infinitude of primes $\equiv \ell \pmod{k}$.

   This definitive file is saved in the current user path where the function ap_euc has been called. This LaTeX file is then converted to HTML source and inserted in the webpage.

```
template = Path('template_euc.tex').read_text()
output = subst_dictionary(template,d)
```

```
    with open('proof_euc.tex','w') as f:
      f.write(output)

    return
```

6.6 Murty's example

Taking into account all the theorems and ideas we have developed, our version of the Euclidean proof in Section 4.1 seems the most reasonable. However, in Murty's article [RT08], which is the reference we have mostly followed, no example with specific values of k and ℓ is given to the extent that we have. Instead, the author makes use of the Quadratic Reciprocity Law (QRL) to provide a brief proof of the infinitude of primes $\equiv 4 \pmod{15}$. However, not every pair of k and ℓ satisfying $\ell^2 \equiv 1 \pmod{k}$ admits such a proof. It can be checked (see the discussion following Proposition 6.8 below) that a proof using the QRL will only work when $L = \mathbb{Q}(\eta)$ is the compositum of its quadratic subfields[30], which is not always the case (recall Proposition 3.4). While significantly shorter, the proof using the QRL does not cover every possible arithmetic progression satisfying Schur and Murty's condition, so we have chosen not to automatize this approach.

For completeness, we shall reproduce (and improve) Murty's proof for the specific case $k = 15$ and $\ell = 4$ and later explain why his argument is not always possible.

Proposition 6.8. *There exist infinitely many primes* $\equiv 4 \pmod{15}$.

Proof. Consider the polynomial

$$f(x) := \Big(x - (\zeta + \zeta^4)\Big)\Big(x - (\zeta^2 + \zeta^8)\Big)\Big(x - (\zeta^7 + \zeta^{13})\Big)\Big(x - (\zeta^{11} + \zeta^{14})\Big),$$

where $\zeta = e^{2\pi i/15}$ is a 15th primitive root of unity. Simplifying leads to $f(x) = x^4 - x^3 + 2x^2 + x + 1$.

Now, write f as $f(x) = (-x^2 + x/2 - 1/2)^2 + 3(x+1)^2/4$. Suppose p is a prime divisor of f. Thus, for some $n \in \mathbb{Z}$ it is true that

$$\left(-n^2 + \frac{n}{2} - \frac{1}{2}\right)^2 + \frac{3(n+1)^2}{4} \equiv 0 \pmod{p} \Rightarrow -3 \equiv \left(\frac{-n^2 + n/2 - 1/2}{(n+1)/2}\right)^2 \pmod{p},$$

which is of the form $m^2 + 3 = pm'$ for some non-zero integers m and m' (if $p \neq 3$). Therefore, -3 is a quadratic residue for every prime divisor of f unequal to 3, so $\left(\frac{-3}{p}\right) = -1$. By the Legendre symbol's properties, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$, which happens if and only if $p \equiv 1 \pmod{3}$.

If we instead write f as $f(x) = (-x^2 + x/2 - 3/2)^2 - 5(x-1)^2/4$ —and follow the same reasoning as before— we deduce that any prime divisor of f unequal to 5 satisfies $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$, which happens if and only if $p \equiv 1$ or $4 \pmod{5}$.

With these two conditions over p, we deduce that any prime divisor of f is either $\equiv 1$ or $4 \pmod{15}$, except for $p = 2, 3, 5$. (Note that the prime 2 is added since it is never considered in the definition of the Legendre symbol). By Lemma 2.9, the polynomial

[30] A *quadratic extension* of $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{D})$, where $D \in \mathbb{Z}$ is square-free.

$f(15x+1)$ also has its prime divisors $\equiv 1$ or $4 \pmod{15}$ except for $p = 2, 3, 5$. A Taylor expansion yields:

$$f(1+15x) = f(1) + f'(1)15x + O((15x)^2) = 4 + 6 \cdot 15x + O((15x)^2) = 15xg(x) + 4,$$

for some $g \in \mathbb{Z}[x]$. To reach a contradiction, suppose that there is a finite number of primes $\equiv 4 \pmod{15}$, and let Q be their product. Now, consider $f(1+15Q) = 15Qg(Q) + 4$. We will first show that this number has no prime divisors $\equiv 4 \pmod{15}$. If we suppose otherwise, let q be a prime such that q divides $15Qg(Q)+4$ and $q \equiv 4 \pmod{15}$. Observe that q divides Q by definition, so q also divides $15Qg(Q)$. Then, it follows that q divides 4, so it must happen that $q = 2$, which is a contradiction since then $q \not\equiv 4 \pmod{15}$.

Therefore, $f(1+15Q) = 15Qg(Q) + 4$ has no prime divisors $\equiv 4 \pmod{15}$. Furthermore, $2, 3$ and 5 are also not prime divisors of $f(1+15Q)$. Indeed,

$$f(1+15Q) \equiv f(1) = 4 \pmod{15},$$

so $f(1+15Q)$ is not divisible by 3 or 5. Similarly, observing that Q is odd since it is a product of primes excluding $2 \not\equiv 4 \pmod{15}$,

$$f(1+15Q) \equiv f(1+1) \equiv f(0) = 1 \pmod{2},$$

so $f(1+15Q)$ is not divisible by 2.

Since every prime divisor of f is either $\equiv 1$ or $4 \pmod{15}$ or $2, 3, 5$, it follows that every prime divisor of $f(1+15Q)$ must be $\equiv 1 \pmod{15}$. Therefore, $f(1+15Q) \equiv 1 \pmod{15}$. However, $f(1+15Q) = 15Qg(Q) + 4 \equiv 4 \pmod{15}$. This is a contradiction. Therefore, there exist infinitely many primes $\equiv 4 \pmod{15}$. □

The key to the previous theorem is characterising the prime divisors of f. This is achieved via studying these prime divisors in each of the quadratic subfields of $L = \mathbb{Q}(\eta)$ with $\eta = h_{15}(\zeta) = (\zeta-15)(15-\zeta^4) = -\zeta^5+15\zeta^4+15\zeta-225$, which are $F_1 = \mathbb{Q}(\sqrt{-3})$, $F_2 = \mathbb{Q}(\sqrt{5})$ and $F_3 = \mathbb{Q}(\sqrt{-15})$. This is acceptable since L coincides with the compositum $F_1F_2F_3$. In this case, studying the prime divisors of f in every F_i is equivalent to studying them in L. Since $[F_i : \mathbb{Q}] = 2$ for every i, the QRL effectively gives a characterisation in terms of congruences of these prime divisors (in each quadratic subfield).

Nevertheless, it is not true in general that L is the compositum of its quadratic subfields. Since reciprocity laws of higher order are not in general easy to express via congruences (unless L is a cyclotomic field or quadratic over $\mathbb{Q}$), the argument in Proposition 6.8 does not work for every arithmetic progression satisfying $\ell^2 \equiv 1 \pmod{k}$.

Also, observe that the proof in Proposition 6.8 has both some similarities and some differences with our general Euclidean method. Starting with the similarities, our Euclidean polynomial f^* defined in Section 3 for the progression $\equiv 4 \pmod{15}$ has the same degree and prime divisors as the polynomial f in Proposition 6.8 (despite being significantly different in their coefficients[31]). Indeed, in Murty's proof, we have seen that the prime divisors p of f satisfy $p \equiv 1, 4 \pmod{15}$ or $p = 2, 3, 5$, and the prime divisors of f^*, because of Theorem 3.7, are also those primes $\equiv 1, 4 \pmod{15}$, together with the prime divisors of 15 and $\Delta(f^*) = 900 = 2^2 \cdot 3^2 \cdot 5^2$, which are $2, 3$ and 5. Thus, f also satisfies our definition of Euclidean polynomial.

[31]For the progression $\equiv 4 \pmod{15}$, our general method produces the polynomial $f^*(x) = x^4+883x^3+292728x^2+43186723x+2392743361$.

With respect to the differences, observe that the polynomial f^* is the minimal polynomial of $\eta \in L$. Also, f^* generates the field L, and its special properties (see Lemma 3.12 for example) help us build the Euclidean proof in general. All these constraints on f^* make it a complex polynomial in its coefficients. However, for the specific case proved above, we do not need f to be the minimal polynomial of any element of L. We just want it to generate L and have the right prime divisors. There are multiple polynomials that accomplish this, and Murty has chosen the simplest one in its coefficients, which is the irreducible polynomial $f(x) = x^4 - x^3 + 2x^2 + x + 1$. Nevertheless, this polynomial does not follow directly from the construction Murty gives in his article.

6.7 Program's execution time

Find below the figures that show the performance of our code that yields the proof of the infinitude of primes $\equiv \ell \pmod{k}$, in the cases $k \in [20, 80]$, with ℓ such that $\ell^2 \equiv 1 \pmod{k}$.

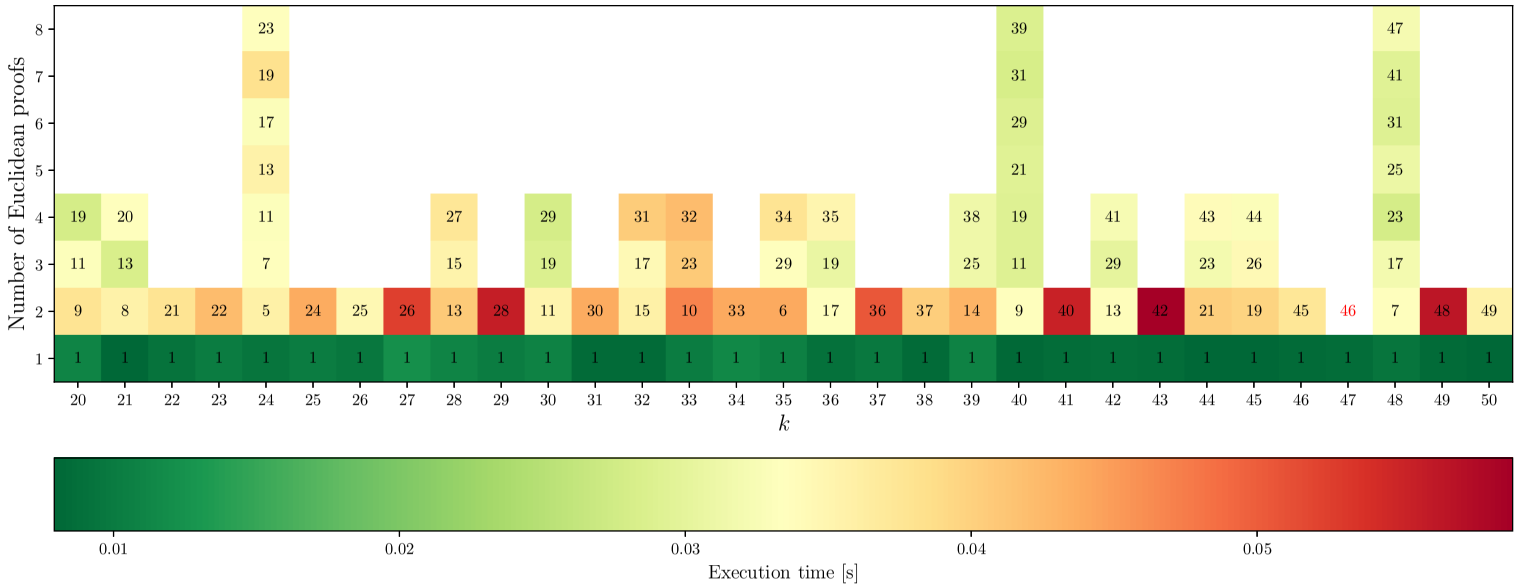

Figure 6.1: Values of k and ℓ that satisfy $\ell^2 \equiv 1 \pmod{k}$, for $k \in [20, 50]$. The horizontal axis indicates the value of k, while the vertical axis accumulates one box for every residue class satisfying $\ell^2 \equiv 1 \pmod{k}$ (the corresponding value of $\ell \bmod k$ is written inside the box). Observe that the number of possible Euclidean proofs (the vertical axis) is always a power of 2, as we deduced in Section 3.3. Each box is coloured in correspondence to the execution time of the code of the arithmetic progression $\equiv \ell \pmod{k}$. If it exceeds the threshold, the corresponding value of ℓ is written in red within a white box.

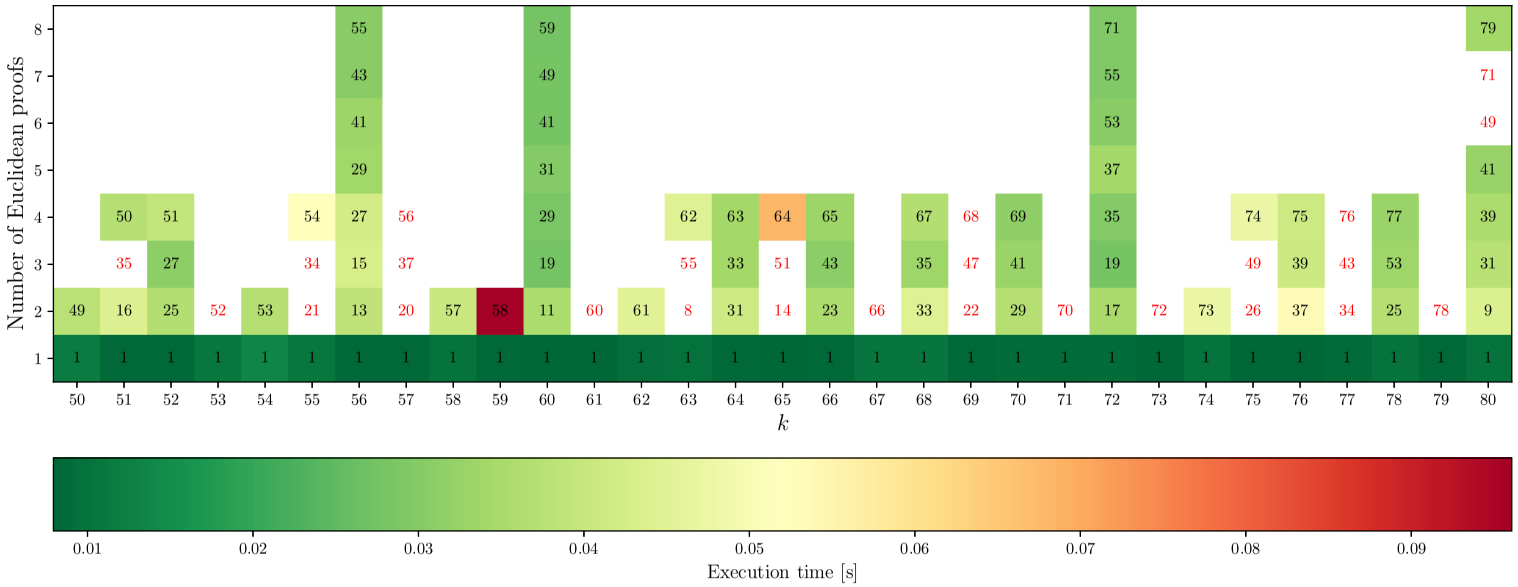

Figure 6.2: Values of k and ℓ that satisfy $\ell^2 \equiv 1 \pmod{k}$, for $k \in [50, 80]$. The horizontal axis indicates the value of k, while the vertical axis accumulates one box for every residue class satisfying $\ell^2 \equiv 1 \pmod{k}$ (the corresponding value of $\ell \bmod k$ is written inside the box). Observe that the number of possible Euclidean proofs (the vertical axis) is always a power of 2, as we deduced in Section 3.3. Each box is coloured in correspondence to the execution time of the code of the arithmetic progression $\equiv \ell \pmod{k}$. If it exceeds the threshold, the corresponding value of ℓ is written in red within a white box.

References

[BL65] Paul T. Bateman and Marc E. Low. "Prime Numbers in Arithmetic Progressions with Difference 24." In: *The American Mathematical Monthly* 72.2 (Feb. 1965), pp. 139–143. ISSN: 00029890, 19300972. DOI: ↗. URL: ↗. Accessed: June 25, 2025.

[Con10] K. Conrad. *Euclidean Proofs of Dirichlet's Theorem*. 2010. URL: ↗. Accessed: June 25, 2025.

[Cox12] D. A. Cox. *Galois Theory*. Eng. 2nd. Newark: John Wiley & Sons, Incorporated., 2012. DOI: ↗.

[Ded78] R. Dedekind. "Ueber den Zusammenhang zwischen der Theorie der ideale und der Theorie der höheren Congruenzen." In: *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen* 23 (1878), pp. 3–38. URL: ↗. Accessed: June 25, 2025.

[EucBC] Euclid. *Elements*. Vol. IX. Clay Mathematics Institute Historical Archive, 300 BC. URL: ↗.

[Gau86] C. F. Gauss. *Disquisitiones Arithmeticae*. Eng. 1st. Springer New York, NY, Apr. 1986. ISBN: 978-0-387-96254-2. DOI: ↗.

[GT02] Shay Gueron and Ran Tessler. "86.18 Infinitely Many Primes in Arithmetic Progressions: The Cyclotomic Polynomial Method." In: *The Mathematical Gazette* 86.505 (Mar. 2002), pp. 110–114. ISSN: 00255572. DOI: ↗. URL: ↗. Accessed: June 25, 2025.

[HW60] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Eng. 4th. Oxford, 1960.

[Leb56] H. L. Lebesgue. "Remarques diverses sur les nombres premiers." In: *Nouvelles annales de mathématiques* 15 (1856), pp. 130–134. URL: ↗. Accessed: June 25, 2025.

[Lin15] Xianzu Lin. "Infinitely Many Primes in the Arithmetic Progression $kn - 1$." In: *The American Mathematical Monthly* 122.1 (Jan. 2015), pp. 48–51. ISSN: 00029890, 19300972. DOI: ↗. URL: ↗. Accessed: June 25, 2025.

[Mar87] Daniel A. Marcus. *Number Fields*. Eng. 2nd print. Universitext. New York Inc.: Springer-Verlag, 1987. ISBN: 0387902791.

[Meš23] Romeo Meštrović. "Euclid's theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.–2022) and another new proof." Version 4. In: (July 2023). DOI: ↗. Accessed: June 25, 2025.

[PS21] P. Pollack and A. Singha Roy. *Steps into Analytic Number Theory: A Problem-Based Introduction*. Eng. 1st. Problem Books in Mathematics. Cham, Switzerland: Springer Cham, 2021. ISBN: 978-3-030-65077-3. DOI: ↗.

[RT08] M. Ram Murty and N. Thain. "Prime Numbers in certain Arithmetic Progressions." In: *Functiones et Approximatio Commentarii Mathematici* XXXV (Jan. 2008), pp. 249–259. URL: ↗. Accessed: June 25, 2025.

[Rom07] S. Roman. *Advanced Linear Algebra*. Eng. 3rd. Graduate Texts in Mathematics. Springer New York, NY, Oct. 2007. ISBN: 978-0-387-72828-5. DOI: ↗.

[Sch12] I. Schur. *Uber die Existenz unendlich vieler Primzahlen in einiger speziellen arithmetischen Progressionen*. De. Vol. 11. S-B Berlin. Math. Ges., 1912, pp. 40–50.

[Sel49] Atle Selberg. "An Elementary Proof of Dirichlet's Theorem About Primes in an Arithmetic Progression." In: *Annals of Mathematics* 50.2 (Apr. 1949), pp. 297–304. ISSN: 0003486X, 19398980. DOI: ↗. Accessed: June 25, 2025.

[Ser73] J-P. Serre. *A Course in Arithmetic*. Eng. 1st. Graduate Texts in Mathematics. Springer-Verlag New York, NY, Nov. 1973. DOI: ↗.

[Sha93] D. Shanks. *Solved and Unsolved Problems in Number Theory*. Eng. 4th. New York: New York: Chelsea Publishing, 1993.

[Sha50a] Harold N. Shapiro. "On Primes in Arithmetic Progressions (I)." In: *Annals of Mathematics* 52.1 (July 1950), pp. 217–230. ISSN: 0003486X, 19398980. DOI: ↗. Accessed: June 25, 2025.

[Sha50b] Harold N. Shapiro. "On Primes in Arithmetic Progressions (II)." In: *Annals of Mathematics* 52.1 (July 1950), pp. 231–243. ISSN: 0003486X, 19398980. DOI: ↗. Accessed: June 25, 2025.

[SL96] P. Stevenhagen and H.W. Lenstra. "Chebotarëv and his density theorem." In: *The Mathematical Intelligencer* 18 (Mar. 1996), pp. 26–37. DOI: ↗. URL: ↗. Accessed: June 25, 2025.

[TH86] E. C. Titchmarsh and D. R. Heat-Brown. *The Theory of the Riemann Zeta-function*. Eng. 2nd. New York: Oxford science publications. Clarendon Press; Oxford University Press, 1986.

[Was96] L. C. Washington. *Introduction to Cyclotomic Fields*. Eng. 2nd. Graduate Texts in Mathematics. Springer New York, NY, Dec. 1996. DOI: ↗.

[Wym72] B. F. Wyman. "What is a Reciprocity Law?" In: *The American Mathematical Monthly* 79.6 (1972), pp. 571–586. DOI: ↗. URL: ↗. Accessed: June 25, 2025.