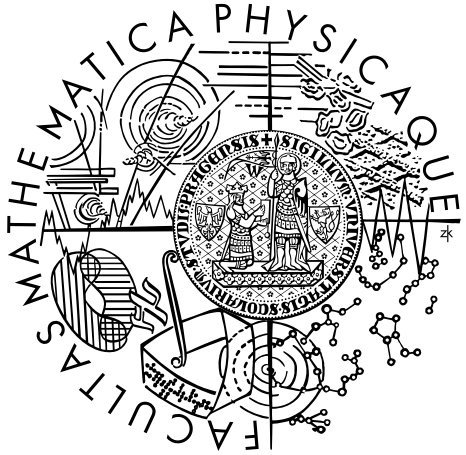
Charles University in Prague
Faculty of Mathematics and Physics

BACHELOR THESIS



Martin Čech

Algebraic proofs of Dirichlet's theorem on arithmetic progressions

Department of Algebra

Supervisor of the bachelor thesis: Mgr. Vítězslav Kala, Ph.D.

Study programme: Mathematics

Study branch: General Mathematics

Prague 2016

This is a second version of the original thesis, where some minor mistakes are corrected.

Title: Algebraic proofs of Dirichlet's theorem on arithmetic progressions

Author: Martin Čech

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: Dirichlet's theorem on arithmetic progressions says that there are infinitely many primes in any arithmetic progression $a_n = kn + \ell$ with coprime k, ℓ. The original proof of this theorem was analytic using a lot of non-elementary methods. The goal of this thesis is to give sufficient and necessary conditions on k and ℓ under which a more elementary algebraic proof of the theorem can exist, and give the proof in these cases.

Keywords: Dirichlet's theorem, algebraic number theory, primes, Chebotarev Density Theorem

I would like to thank my supervisor Mgr. Vítězslav Kala, Ph.D. for his inspiring and useful advice. I am very grateful for his patience and time he dedicated to me during the consultations.

Contents

Introduction

Around 300 BC, Euclid proved that there are infinitely many prime numbers. He gave a very simple and beautiful argument – he supposed there are only finitely many of them, multiplied them all together and added one. This new number had to be divisible by another prime, which was not on the original list.

More than 2000 years later, in 1837 Dirichlet proved that every arithmetic progression of the form $a_n = kn+\ell$ for coprime k, ℓ contains infinitely many prime numbers. His proof was much more complicated and non-elementary, it led for example to the introduction of L-functions and used the power of mathematical analysis.

One may ask – and many people did so – if there is an easier or more elementary way to investigate primes in arithmetic progressions. We will see that in some particular cases, a simplification is really possible. Notice that in all these examples, the arguments are very similar to Euclid's.

Our goal will be to find the conditions on k and ℓ under which the more elementary "Euclidean" proof can exist and prove Dirichlet's Theorem for them. In order to do so, we will need to specify what we actually mean by "Euclidean" proof. There are probably more possibilities, we are going to follow the article by Murty and Thain [1], in which the authors were able to find a definition which can be handled using Galois Theory.

In the last chapter, we will show that the conditions we found are not only sufficient but also necessary. However, as with many other problems within mathematics, showing that an Euclidean proof does not exist is much harder than the proof of Dirichlet's Theorem itself.

We are now going to show two examples of progressions for which there is an elementary way to show that they contain infinitely many prime numbers.

4n+3: Let us suppose that there are only finitely many prime numbers of the form $4n + 3$, denote them $p_1, \ldots, p_m$ and let $P = p_1 \ldots p_m$ be their product. Let us now look at the number $4P - 1$. This is certainly a number of the form $4n + 3$, therefore has to be divisible by such a prime (because by multiplying primes which are $\equiv 1 \pmod 4$, the result will also be $\equiv 1 \pmod 4$), denote it p. But $4P - 1 \equiv -1 \pmod{p_i}$ for each $i = 1, \ldots, m$, therefore p was not on our original list – this is a contradiction.

The next example will be slightly more complicated.

4n+1: Suppose again that there are only finitely many prime numbers of the form $4n + 1$, denote them $p_1, \ldots, p_m$ and their product P. We could try the same method as above – investigate the prime divisors of $4P + 1$, but it doesn't work – the argument fails because a number of the form $4n + 1$ does not need to have any prime divisor of this form, it can have an even number of prime divisors of the form $4n + 3$.

Let us try the number $A = 4P^2 + 1 = (2P)^2 + 1$. We will show that any prime divisor of this number has the desired form. Let p be a prime divisor of A. Then p is not 2 and it is also not equal to any of $p_1, \ldots, p_m$, and we have $A = (2P)^2+1 \equiv 0 \pmod p$, which gives us that -1 is a quadratic residue modulo p. It follows that (for example by quadratic reciprocity, but this can be proved in an elementary way), since p can't be 2, it has to be $\equiv 1$ modulo 4. This again

gives us a contradiction.

There are more cases which can be treated in a more or less similar way. For example in [3] the reader can find elementary proofs of Dirichlet's theorem for all cases when $k = 12$ and in [4] there is a proof for all progressions with $\ell = 1$.

After reading some of the elementary proofs and trying to figure out what they all have in common, one can come up with the conjecture that it is connected with polynomials and prime divisors of their integral values.

There are several ways how to define a Euclidean proof. For example in the case of $4n + 1$, we found a polynomial with the following property – each of its value in the integers (except when $x = 0$) was divisible by a prime of the desired form. Finding such a polynomial would be nice and one feels that it would easily give us Dirichlet's Theorem, but it is probably hard to find or decide whether such a polynomial exists, since we would have to know something about (with perhaps finitely many exceptions) every integral value of the polynomial.

In [1], another condition is used – it is said that there is an Euclidean proof for an arithmetic progression $kn + \ell$ if there exists a polynomial $f \in \mathbb{Z}[x]$ such that, with finitely many exceptions, when a prime number $p|f(n)$ for some $n \in \mathbb{Z}$, then $p \equiv 1, \ell \pmod{k}$. This definition may seem weird at first and it is not even clear that it implies Dirichlet's Theorem for the given arithmetic progression, but we will see that after some experience with the prime divisors of polynomials, this definition arises naturally.

Its main advantage is that it can be handled using Galois Theory, which is already something we can understand. The condition on the prime divisors p of the integral values of the polynomial f to be $\equiv 1, \ell \bmod k$ seems strange, for example because we would like to get rid of the 1, but we will see later that it can't be omitted.

With this definition of Euclidean proof, our main goal will be to prove the next theorem, which characterizes the progressions for which the Euclidean proof of Dirichlet's Theorem exists:

Theorem 1 (Murty)**.** *The Euclidean proof of Dirichlet's Theorem for the arithmetic progression $a_n = nk + \ell$ exists if and only if $l^2 \equiv 1 \pmod{k}$.*

In this thesis, we are going to successively proof the two implications of Theorem 1 and try to answer several additional questions.

In the first chapter, we will review some basics of algebraic number theory and Galois Theory, which we are going to use later. The purpose of this chapter is not to replace a first course in these topics, the objective is rather to gather the notions we are going to use throughout the thesis. Therefore not all the proofs and reasoning are always presented, there are however references to basic course notes and textbooks for a reader not familiar with subjects.

The second chapter already gives the proof of Dirichlet's Theorem for arithmetic progressions satisfying $\ell^2 \equiv 1 \pmod{k}$. At first we proof some properties of the prime divisors of polynomials, then we construct the polynomial needed in the Euclidean proof (Lemma 12 and Theorem 13) and finally show that the existence of this polynomial implies that there are infinitely many primes in the particular arithmetic progression (Theorem 18). We will mainly follow the article of Murty and Thain [1], the proofs are however given with more details. We were also able to fix some minor errors which occurred in the original article.

Some questions arise while proving Dirichlet's Theorem in the algebraic way. One of them is for which numbers k does this method give us the full proof, i.e., for what numbers k is it true that if ℓ is coprime to k, then $\ell^2 \equiv 1 \pmod{k}$. This question is fully answered in Example 20.

The other question is whether the annoying condition in Theorem 18, where we have to assume that at least one prime congruent with ℓ modulo k exists, can be omitted. We will see that in the simplest case when k is a prime, the answer is "yes", but for slightly more complicated cases the argument doesn't work.

We have done some explicit computations of the polynomials in order to find a proof that at least one of the values of the polynomial is congruent to ℓ modulo k, which would guarantee the existence of a prime $\equiv \ell$ modulo k, but it seems that there is no easy way of dealing with the general case.

The last two chapters focus on the other implication that no Euclidean proof exists if the condition $\ell^2 \equiv 1 \pmod{k}$ is not satisfied.

The third chapter gives an outline of a deeper theory, namely the densities of sets of primes, which we are going to need. Same as in the case of the first chapter, this chapter's purpose is only to summarize some statements we are going to use, some simple proofs are however given in order to get used with the slightly more complicated definitions which the reader may not be very familiar with. The main objective of this chapter is to formulate the Chebotarev Density Theorem and its corollary, which we are going to use in the proof of the other implication of Theorem 1.

In the last chapter, we are finally going to prove the harder implication of Murty's Theorem (Theorem 31). This is another example in mathematics where showing that something is impossible to be proven in a particular way is much harder than proof of Dirichlet's theorem itself, because we will have to use the Chebotarev Density Theorem which is its strong generalization into algebraic number fields. In this chapter, we will follow Conrad's paper [5], which is more detailed than the article of Murty and Thain.

1. Preliminaries

In this chapter, we are quickly going to review some basic and important statements from Galois theory and algebraic number theory which will be useful later throughout the thesis. We are not going to proof each of them, however the proofs can be found in most introductory book or course notes on Galois Theory and algebraic number theory, e.g., in J. S. Milne's courses notes on Fields and Galois Theory [8] and Algebraic Number Theory [9].

1.1 Galois Theory

1.1.1 Field extensions, Galois groups and the Galois correspondence

Let K be a field. Then any field L containing K is called a **field extension of** K and this fact will be denoted by L/K.

If we forget in L the multiplication by elements of the larger field and we consider only the multiplication by elements of K, we can think of L as a K-vector space. Therefore we can talk about the **degree of the extension** $[L : K] := \dim_K L$. By an **algebraic number field** we will mean a finite extension of the field of rational numbers, where finite means of finite degree.

If $K \subset L \subset M$ are fields, it isn't hard to see that $[M : K] = [M : L] \cdot [L : K]$. For an element $\alpha \in L$, by $K(\alpha)$ we denote the smallest field extension of K containing α. The **Primitive Element Theorem** states that if L/K is an extension of number fields which has finite degree, L can be obtained from K by adjoining a single element, i.e., there exists some $\alpha \in L$ such that $L = K(\alpha)$. For an arbitrary element $\alpha \in L$ there exists the **minimal polynomial of** α **in** K, which is the monic irreducible polynomial over K which has α as a root. By a minimal polynomial over $\mathbb{Z}$ we will mean the minimal polynomial over $\mathbb{Q}$ multiplied by the LCM of the denominators of its coefficients.

For a field extension L/K, if $f \in K[x]$ is an irreducible polynomial over K, we say that L is the **splitting field of** f if f factors into a product of linear polynomials in L and L is the smallest such field. For every irreducible polynomial f over K, its splitting field does exist.

The **Galois group** $\mathrm{Gal}(L/K)$ is the group of all K-automorphisms of L, i.e., such automorphisms of L which restricted to K are identity. The extension is called **Galois** if $|\mathrm{Gal}(L/K)| = [L : K]$. The extension L/K is Galois if and only if L is a splitting field of some polynomial over K. If L/K is a Galois extension and f is an irreducible polynomial over K which has a root in L, then f factors into a product of linear polynomials in L. If $f \in K[x]$ is an irreducible polynomial and L is the splitting field of f, then a direct computation shows that for every root α of f and $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\alpha)$ is also a root of f. Moreover, the Galois group acts transitively on the roots of f, i.e., for every pair α, β of roots of f there exists a $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) = \beta$.

For a subgroup $H \leq \mathrm{Gal}(L/K)$, the **fix field of** H is defined as the subfield of L on which all automorphisms from H act as identity, i.e.,

$$L^H = \{x \in L : \varphi(x) = x \text{ for all } \varphi \in H\}.$$

We say that the extension L/K is **abelian** if it is Galois and the Galois group $\mathrm{Gal}(L/K)$ is abelian.

The following theorem is called the fundamental theorem of Galois Theory.

Theorem 2. *Let L/K be a Galois extension of finite degree. Then there is a one-to-one correspondence between the intermediate fields $K \subset M \subset L$ and the subgroups H of the Galois group* $\mathrm{Gal}(L/K)$.

The correspondence is given by the map

$$\varphi : \{H : H \leq \mathrm{Gal}(L/K)\} \to \{M : M \text{ is a field and } K \subset M \subset L\}$$
$$H \mapsto L^H.$$

Moreover the following are true about the bijection:

- *the bijection reverses inclusions, i.e., $H \leq G \leq \mathrm{Gal}(L/K)$ if and only if $L^G \subset L^H$.*
- *The extension L^H/K is Galois if and only if H is a normal subgroup of* $\mathrm{Gal}(L/K)$.

If the extension L/K is not Galois, the map from the theorem is injective, but not surjective.

The following corollary will be useful for us:

Corollary 3. *If K, L, M, N are fields such that $K \subset M \subset L$, $K \subset N \subset L$ and L/K is Galois, then $M = N$ if and only if* $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/N)$, *i.e., the automorphisms of L which fix M are exactly those fixing the field N.*

1.1.2 Cyclotomic extensions and polynomials

Throughout the thesis, ζ_k will denote the primitive k-th root of unity in $\mathbb{C}$.

For $k \in \mathbb{N}$ we define the **k-th cyclotomic polynomial** Φ_k as

$$\Phi_k := \prod_{a \in (\mathbb{Z}/k\mathbb{Z})^\times} (x - \zeta_k^a).$$

This polynomial is monic with integer coefficients and is irreducible over $\mathbb{Q}$.

The following formula is true about cyclotomic polynomials:

$$x^n - 1 = \prod_{(a,n)=1} \Phi_a(x)$$

and after computing $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$ we can see that the absolute term of $\Phi_n(x)$ for $n > 1$ is always 1 (it is clear that the absolute term has to be ± 1 and if there were some $n > 1$ such that $\Phi_n(0) = -1$, we let n to be the smallest such number and then the formula above cannot hold since the absolute term of the right-hand side would be 1).

The extension $\mathbb{Q}(\zeta_k)/\mathbb{Q}$ is called a cyclotomic extension. It is abelian because $\mathbb{Q}(\zeta_k)$ is the splitting field of the k-th cyclotomic polynomial, and

$$\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q}) \simeq (\mathbb{Z}/k\mathbb{Z})^\times$$

where the isomorphism $\varphi : (\mathbb{Z}/k\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ is for example $\varphi(m) = \sigma_m$, where σ_m is the unique element of the Galois group such that $\sigma_m(\zeta_k) = \zeta_k^m$. We are often going to identify these two groups through this isomorphism.

For the same reason, the extension $K(\zeta_k)/K$ is abelian if we start with any algebraic number field K (it is still the splitting field of the k-th cyclotomic polynomial over K) and $\mathrm{Gal}(K(\zeta_k)/K) \leq (\mathbb{Z}/k\mathbb{Z})^\times$.

1.2 Algebraic number theory

We are now going to recall some basics of Algebraic number theory.

1.2.1 Ring of integers

For an algebraic number field K, we denote by $\mathcal{O}_K$ the **ring of integers of K** which is defined as

$$\mathcal{O}_K := \{\alpha \in K : \text{the minimal polynomial of } \alpha \text{ over } \mathbb{Q} \text{ has integer coefficients}\}.$$

It is not obvious that this set is closed under addition and multiplication and therefore forms a ring, two proofs of this can be found for example in [9]. It can also be proved that the ring of integers is always a finitely generated $\mathbb{Z}$-module. It is in fact a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$ so there exist $b_1, \ldots, b_n \in \mathcal{O}_K$ such that $\mathcal{O}_K = b_1\mathbb{Z} + \cdots + b_n\mathbb{Z}$. The set $\{b_1, \ldots, b_n\}$ is called an **integral basis** of $\mathcal{O}_K$.

The reason why we work with this structure is that it satisfies the condition of being a **Dedekind domain**, which means that it has the following properties:

- $\mathcal{O}_K$ is Noetherian
- $\mathcal{O}_K$ is integrally closed (if some $\alpha \in K$ is a root of an irreducible monic polynomial with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$)
- every nonzero prime ideal in $\mathcal{O}_K$ is maximal

Dedekind domains are important because a generalization of the fundamental theorem of arithmetic for ideals holds for them. It states that every ideal can be written uniquely (up to reordering) as a product of prime ideals. If p is a rational prime and K is an algebraic number field, we can factor p uniquely in K as $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_g^{e_g}$ where the $\mathfrak{p}_\mathfrak{i}$ are prime ideals in $\mathcal{O}_K$. In fact, the $\mathfrak{p}_i$ are exactly the prime ideals which contain (p). Moreover, for every prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ there is a unique rational prime p such that $p \in \mathfrak{p}$. If we have such a factorization, then

$$\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}],$$

where f_i is the inertia degree of $\mathfrak{p}_i$ which is to be defined in Definition 7. From this formula, it follows that every rational prime has at most $[K : \mathbb{Q}]$ prime ideal factors in $\mathcal{O}_K$.

We are going not to distinguish between the terms of prime ideals of $\mathcal{O}_K$ and primes in $\mathcal{O}_K$ and we will also call these primes of K. By rational primes, we will mean the ordinary prime numbers in $\mathbb{N}$.

We can extend the notion of divisibility on ideals: for A, B ideals in $\mathcal{O}_K$, we say that **A divides B** and denote it $A|B$ if and only if $B \subset A$. Note that this definition corresponds to the divisibility of rational numbers, where $a|b$ is equivalent to $(b) \subset (a)$.

As in the case of integers, if $a, b \in \mathcal{O}_K$ and $\mathfrak{p}$ is an ideal in K, we write that $a \equiv b \pmod{\mathfrak{p}}$ if $a - b \in \mathfrak{p}$ (equivalently, if $a = b$ in $\mathcal{O}_K/\mathfrak{p}$).

Proposition 4. *Let K be an algebraic number field and $\mathfrak{p}$ a prime in K. Suppose that $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{\mathfrak{p}}$. Then $a \equiv b \pmod{p}$, where p is the rational prime such that $(p) = \mathfrak{p} \cap \mathbb{Z}$.*

Proof. The congruence $a \equiv b \pmod{\mathfrak{p}}$ means by definition that $a - b \in \mathfrak{p}$, but since both a and b are integers, $a - b \in \mathfrak{p} \cap \mathbb{Z}$ so $a \equiv b \pmod{p}$. □

If $\mathfrak{a} \in \mathcal{O}_K$ is an ideal, its **norm** $N(\mathfrak{a})$ is defined to be its index in the ring $\mathcal{O}_K$, i.e., $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$. It is a known fact that $N(\mathfrak{a})$ is always finite (see [2], exercises 4.4.1 – 4.4.5). If $\mathfrak{p}$ is a prime ideal, then it is maximal, so $\mathcal{O}_K/\mathfrak{p}$ is a field. It is an extension of $\mathbb{Z}/p\mathbb{Z}$ for the rational prime p such that $(p) = \mathfrak{p} \cap \mathbb{Z}$, so it is a finite field of characteristic p. In particular, $N(\mathfrak{p})$ is always a prime power.

1.2.2 Factorization of rational primes in $\mathcal{O}_K$

The following theorem shows how to factor a rational prime p in $\mathcal{O}_K$ if we know how does the minimal polynomial of the generator of K factor modulo p (if some technical condition is satisfied):

Theorem 5 (Dedekind)**.** *Let K be an algebraic number field and suppose that p is a rational prime number such that $p \nmid [\mathcal{O}_k : \mathbb{Z}[\vartheta]]$, where $\vartheta \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\vartheta)$. Let f be the minimal polynomial of ϑ over $\mathbb{Z}$, and suppose that*

$$f(x) \equiv f_1(x)^{e_1} \dots f_n(x)^{e_n} \pmod{p},$$

where each $f_i(x)$ is irreducible over $\mathbb{F}_p[x]$. If we denote $\mathfrak{p}_i = (p, f_i(\vartheta))$, then $\mathfrak{p}_i$ are prime ideals and $p\mathcal{O}_k = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n}$, with $N(\mathfrak{p}_i) = p^{\deg f_i}$.

We will not give the proof of this theorem here, it can be found for example in [2] (see Theorem 5.5.1 and Exercise 5.5.2).

We are now going to prove a proposition which will allow us to define the *inertia degree*.

Proposition 6. *Let L/K be an extension of algebraic number fields and $\mathcal{O}_K$, $\mathcal{O}_L$ be their corresponding rings of integers. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$, and let $\mathcal{P}$ be any prime ideal factor of $\mathfrak{p}$ in $\mathcal{O}_L$. Then there is an embedding of $\mathcal{O}_K/\mathfrak{p}$ into $\mathcal{O}_L/\mathcal{P}$.*

Proof. With the notation from the proposition, we have $\mathfrak{p}\mathcal{O}_K \subset \mathfrak{p}\mathcal{O}_L \subset \mathcal{P}$. We will define the embedding as follows: if we choose an arbitrary $a \in \mathcal{O}_K/\mathfrak{p}$, we can represent it as $a'\mathfrak{p} \subset \mathcal{O}_K$ for some $a' \in \mathcal{O}_K$. Then we define the embedding $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathcal{P}$ by taking the coset $a'\mathcal{P} \in \mathcal{O}_L/\mathcal{P}$ and matching a with the corresponding element $a'\mathcal{P} = a'' \in \mathcal{O}_L/\mathcal{P}$.

This map is well-defined, since if $a\mathfrak{p} = b\mathfrak{p}$, then $a - b \in \mathfrak{p} \subset \mathcal{P}$.

In order to show that the map is injective, note that $\mathcal{P} \cap \mathcal{O}_K$ is an ideal in $\mathcal{O}_L$ containing $\mathfrak{p}$ and not containing 1, but since $\mathcal{O}_K$ is a Dedekind domain, $\mathfrak{p}$ is maximal and hence $\mathcal{P} \cap \mathcal{O}_K = \mathfrak{p}$. Therefore if $a \in (\mathcal{O}_K/\mathfrak{p}) \setminus \{0\}$, then $a' \notin \mathfrak{p}$ so $a'' \notin \mathcal{P}$. Hence the kernel of the map is trivial.

By the definition of operations in factor rings, the map is a homomorphism and therefore an embedding. □

Definition 7. *Let L/K be a field extension and $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. Let $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_n^{e_n}$ be the factorization of $\mathfrak{p}$ with distinct prime factors $\mathcal{P}_i$ in $\mathcal{O}_L$. Then we define*

- *The **ramification degree** of $\mathcal{P}_i$ over K as $e_{\mathcal{P}_i|\mathfrak{p}} := e_i$. We say that $\mathfrak{p}$ is **unramified** in L (or in $\mathcal{O}_L$) if $e_i = 1$ for all $i = 1, \ldots, n$. Otherwise, we say that $\mathfrak{p}$ **ramifies** in L (or $\mathcal{O}_L$).*
- *The **inertia degree** of $\mathcal{P}_i$ over K is defined as $f_{\mathcal{P}_i|\mathfrak{p}} := [\mathcal{O}_L/\mathcal{P}_i : \mathcal{O}_K/\mathfrak{p}]$. We say that $\mathfrak{p}$ has a first degree prime ideal factor in L if it has a prime ideal factor of inertia degree 1.*

With the definition of inertia degree, the last conclusion of Dedekind's Theorem that $N(\mathfrak{p}_i) = p^{\deg f_i}$ is equivalent to saying that the inertia degree $f_{\mathfrak{p}_i|p} = \deg f_i$.

The primes which ramify are often exceptions to various theorems. However, in every finite extension there is only a finite number of them and we will see in Section 1.2.4 that we can characterize them.

1.2.3 Polynomials

We are going to work with polynomials modulo a prime number p so we are just going to review some basic facts about polynomials.

For a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, where $a_i \in K$ for a field K, we define the **derivative** of f to be the polynomial $f'(x) := a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$. The derivative is useful if we want to find out whether a polynomial has multiple roots, because if α is a multiple root of f, then $f(\alpha) = f'(\alpha) = 0$. The other implication holds as well – if α is a root of f which is not a double root, then $f'(\alpha) \neq 0$. The proof is only a use of Leibniz formula for multiplication and the fact that α is a simple root of f if and only if $f(x) = (x - \alpha)g(x)$, where $g(\alpha) \neq 0$.

The following facts are true for any $n \in \mathbb{N}$, prime number p and $f \in \mathbb{Z}[x]$:

- If $a \equiv b \pmod{n}$, then $f(a) \equiv f(b) \pmod{n}$.
- $f(n + p) \equiv f(n) + pf'(n) \pmod{p^2}$. This can be proved by a direct computation using the binomial theorem.

1.2.4 Discriminants

The notion of discriminant is rather complicated and is not that important for us, so we will only give the main definitions and properties. For some deeper and more general theory, see ,e.g., the section about discriminants in [9].

Let f be an irreducible polynomial over $\mathbb{Q}$ and let K be its splitting field. If $f = (x - \alpha_1) \ldots (x - \alpha_n)$ is the factorization of f in $K[x]$, we define the

discriminant of f as $\operatorname{disc}(f) := \prod_{i \neq j}(\alpha_i - \alpha_j)$. Note that in the case of a quadratic polynomial $f(x) = ax^2 + bx + c$, $\operatorname{disc}(f)$ is exactly the discriminant we already know.

It follows directly from the definition that the discriminant of f is zero if and only if f has a multiple root. This is also true for polynomials over fields of characteristic p (where the discriminant is defined by the same formula).

The discriminant of a polynomial is a polynomial function of its coefficients. This follows from the formula being symmetric in the roots of the polynomial and the facts, that the coefficients are the elementary symmetric functions of the roots, and that every symmetric function can be expressed as a combination of the elementary ones. Therefore if a polynomial $f \in R[x]$ for an arbitrary ring R, then $\operatorname{disc}(f) \in R$.

In particular, the discriminant of a polynomial with integer coefficients is an integer.

We will now define the discriminant of algebraic number fields.

Let K be an algebraic number field and let $b_1, \ldots, b_n$ be an integral basis of $\mathcal{O}_K$. Then there are exactly n embeddings of K to $\mathbb{C}$, denote them $\sigma_1, \ldots, \sigma_n$. We define the **discriminant of** K as

$$\operatorname{disc}(K/\mathbb{Q}) := \left(\det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \ldots & \sigma_1(b_n) \\ \sigma_2(b_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(b_1) & \ldots & \ldots & \sigma_n(b_n) \end{pmatrix} \right)^2 .$$

The discriminant is always an integer and is independent of the choice of the integral basis.

In the case when $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α, the images of α under the embeddings σ_i are the roots of the minimal polynomial f of α over $\mathbb{Q}$ and we can take the integral basis as $b_1 = 1, b_2 = \alpha, b_3 = \alpha^2, \ldots, b_n = \alpha^{n-1}$. The determinant then becomes the Vandermonde determinant and so the discriminant is exactly the discriminant of the polynomial f.

Proposition 8. *Let $K = \mathbb{Q}(\alpha)$, where $\alpha \in \mathcal{O}_K$ and let f be the minimal polynomial of α over $\mathbb{Q}$. Then* $\operatorname{disc}(f)$ *divides* $\operatorname{disc}(K/\mathbb{Q})$.

Proof. See the section about discriminants in [9], namely $2.24 - 2.26$ and 2.34. □

We will use the following properties of discriminants and cyclotomic extensions:

- The rational primes that ramify in a field extension K are exactly those dividing the discriminant $\operatorname{disc}(K/\mathbb{Q})$.
- For a cyclotomic extension we have $K = \mathbb{Q}(\zeta_k)$ and $\mathcal{O}_K = \mathbb{Z}[\zeta_k]$, hence $\operatorname{disc}(K/\mathbb{Q}) = \operatorname{disc}(\Phi_k)$. If a prime number p divides $\operatorname{disc}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$, then $p|k$.
- Let $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_k)$ be fields. Then $\operatorname{disc}(K/\mathbb{Q})$ divides $\operatorname{disc}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$.

2. Euclidean proof for progressions with $\ell^2 \equiv 1 \pmod{k}$

2.1 Prime divisors of polynomials

Definition 9. *Let $f \in \mathbb{Z}[x]$ be a polynomial with integer coefficients and p a rational prime number. We say, that p is a prime divisor of f, if there exists some $a \in \mathbb{Z}$ such that $p \mid f(a)$. By $P(f)$ we denote the set of all prime divisors of the polynomial f.*

Note that if f has an integral root, then $P(f)$ contains all rational primes, so it might be natural to suppose that $f(a) \neq 0$ in the definition. We will however mostly work with irreducible polynomials so we do not need to bother with this.

The following theorem is not very surprising. Notice that the proof uses a Euclidean argument.

Theorem 10 (Schur)**.** *If $f \in \mathbb{Z}[x]$ is a non-constant polynomial, then $P(f)$ is infinite.*

Proof. Let $f \in \mathbb{Z}[x]$ be a non-constant polynomial and let $c = f(0)$. If $c = 0$, then $p \mid f(p)$ for any p so we may suppose that $c \neq 0$. Because $f(x) = \pm 1$ has only a finite number of solutions, $P(f)$ is non-empty.

Suppose that $P(f)$ is finite, so that $P(f) = \{p_1, \ldots, p_n\}$ and let $Q = p_1 \cdots p_n$. Then $f(Qcx) = c \cdot g(x)$ for some $g \in \mathbb{Z}[x]$ of the form $g(x) = 1 + a_1 x + \cdots + a_k x^k$ with $Q \mid a_i$ for all $i = 1, \ldots, k$. As above, $P(g)$ is non-empty and for every $p \in P(g)$, p has to be also a prime divisor of f. But for each i, $p_i \notin P(g)$, which gives us a contradiction and $P(f)$ must be infinite. □

If we choose an irreducible monic polynomial $f \in \mathbb{Z}[x]$, then $p \in P(f)$ if and only if f has a root mod p. This is equivalent to f having a linear factor in $\mathbb{F}_p[x]$. If we moreover let ϑ be a root of f, $K = \mathbb{Q}(\vartheta)$ and suppose that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\vartheta]]$, by Dedekind's Theorem the last condition happens if and only if (p) has a prime ideal factor of inertia degree one in $\mathcal{O}_K$.

If $f \in \mathbb{Z}[x]$ is irreducible with leading coefficient $a \neq 1$, then we can work with the polynomial $g(x) = a^{\deg(f)} \cdot f(\frac{x}{a})$. Note that in this case, $P(f)$ and $P(g)$ are equal with finitely many exceptions (namely the primes dividing a). Therefore the argument above works also for polynomials which are not necessarily monic.

The next result is very interesting on its own and it will have an important consequence for us. We will formulate this consequence later as Corollary 16.

Theorem 11 (Nagell)**.** *If $f, g \in \mathbb{Z}[x]$ are non-constant, then $P(f) \cap P(g)$ is infinite.*

Proof. It is easy to see that for polynomials f and g, $P(f) \subset P(fg)$, we may therefore assume that f and g are irreducible (else we can replace them by their irreducible factors).

Let $\alpha \in \mathbb{C}$ be a root of f, $\beta \in \mathbb{C}$ be a root of g and consider the number fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ with their corresponding rings of integers $\mathcal{O}_\alpha$ and $\mathcal{O}_\beta$. By the

remark above, with a finite number of exceptions (for the divisors of $[\mathcal{O}_\alpha : \mathbb{Z}[\alpha]]$) a prime number p lies in $P(f)$ exactly when p has a first degree prime ideal factor in $\mathcal{O}_\alpha$. Consider now $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$ for some $\gamma \in \mathbb{Q}(\alpha, \beta)$, denote its ring of integers by $\mathcal{O}_\gamma$ and let h be the minimal polynomial of γ over $\mathbb{Z}$. By Theorem 10 we know that $P(h)$ is infinite and therefore there are infinitely many prime numbers having a first degree prime ideal factor in $\mathcal{O}_\gamma$.

Pick a $p \in P(h)$ such that $p \nmid \big([\mathcal{O}_\gamma : \mathbb{Z}[\gamma]] \cdot [\mathcal{O}_\alpha : \mathbb{Z}[\alpha]] \cdot [\mathcal{O}_\beta \mathbb{Z}[\beta]] \big)$ and let $\mathfrak{p}$ be its first degree prime ideal factor in $\mathcal{O}_\gamma$. Then $\mathcal{O}_\gamma/\mathfrak{p} \simeq \mathbb{F}_p$. If we look at the factorization of $p\mathcal{O}_\alpha = P_1 \dots P_n$, then $\mathfrak{p}$ is a divisor of some of these factors, WLOG $\mathfrak{p}|P_1$. By Proposition 6, there is an embedding of $\mathcal{O}_\alpha/P_1$ into $\mathcal{O}_\gamma/\mathfrak{p} \simeq \mathbb{F}_p$. But $\mathcal{O}_\alpha/P_1$ is a field of characteristic p, therefore it has to be isomorphic to $\mathbb{F}_p$. Then P_1 is a first degree prime ideal factor of p in $\mathcal{O}_\alpha$ and hence $p \in P(f)$.

For the same reason, $p \in P(g)$ and hence for a finite set E of exceptions, we have $P(h) \setminus E \subset P(f) \cap P(g)$. It follows that $P(f) \cap P(g)$ is infinite. □

2.2 Construction of the polynomial

We will now begin the construction of the polynomial f such that with finitely many exceptions, $p \in P(f)$ implies that $p \equiv 1, \ell \pmod{k}$.

Lets recall that for $k \in \mathbb{N}$, we will denote by ζ_k a primitive k-th root of unity in $\mathbb{C}$ and for $i \in (\mathbb{Z}/k\mathbb{Z})^\times$, σ_i will denote the unique automorphism from $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ such that $\sigma_i(\zeta_k) = \zeta_k^i$.

The next lemma will be crucial for us. It gives the reason why we choose ℓ to satisfy such a weird condition that $\ell^2 \equiv 1 \pmod{k}$ and it gives us a good candidate for the polynomial we are looking for.

Lemma 12. *Let H be a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$ and let $K \subset \mathbb{Q}(\zeta_k)$ be the fix field of H. Then by the Primitive Element Theorem there exists an α such that $K = \mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{Z}[\zeta_k]$, i.e., $\alpha = h(\zeta_k)$ for some polynomial $h \in \mathbb{Z}[x]$. Let $n = [(\mathbb{Z}/k\mathbb{Z})^\times : H]$. Denote by $a_1, \dots, a_n$ the coset representatives of H in $(\mathbb{Z}/k\mathbb{Z})^\times$ and set $\alpha_i = h(\zeta_k^{a_i})$. Now denote*

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i). \tag{2.2.1}$$

Then the following holds:

1. *The numbers α_i are independent of the choice of the coset representatives.*
2. *If $i \neq j$, then $\alpha_i \neq \alpha_j$.*
3. *For $1 \leq i \leq n$ we have $\mathbb{Q}(\alpha_i) = \mathbb{Q}(\alpha)$. Hence, K is the splitting field of f.*
4. *The polynomial f has integer coefficients and is irreducible over $\mathbb{Q}$.*

Proof. **(1) and (2):** It suffices to show that $h(\zeta_k^a) = h(\zeta_k^b) \Leftrightarrow ab^{-1} \in H$. By the main theorem of Galois Theory and the fact that $k \mapsto \sigma_k$ is the isomorphism of $(\mathbb{Z}/k\mathbb{Z})^\times$ onto $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ we get the following chain of equivalences:

- $ab^{-1} \in H \Leftrightarrow$

- $\sigma_{ab^{-1}}$ fixes the field $K = \mathbb{Q}(\alpha) \Leftrightarrow$
- $\sigma_{ab^{-1}}(\alpha) = \alpha \Leftrightarrow$
- $\sigma_a(\alpha) = \sigma_b(\alpha) \Leftrightarrow$
- $\sigma_a(h(\zeta_k)) = \sigma_b(h(\zeta_k)) \Leftrightarrow$
- $h(\zeta_k^a) = h(\zeta_k^b)$.

(3): By Corollary 3 it is enough to prove that the automorphisms of $\mathbb{Q}(\zeta_k)$ which fix $\mathbb{Q}(\alpha_i)$ are exactly the σ_m for $m \in H$. But we have seen that $\alpha_i = h(\zeta_k^{a_i}) = h(\zeta_k^{ma_i}) = \sigma_m(h(\zeta_k^{a_i}))$ if and only if $a_i(ma_i)^{-1} = m^{-1} \in H$ so we are done.
(4): To show that the polynomial f is irreducible, we use the fact that the Galois group acts transitively on the set of roots of f, i.e., for every $i, j \in \{1, \dots, n\}$ there exists some $m \in (\mathbb{Z}/k\mathbb{Z})^\times$ such that $\sigma_m(\alpha_i) = \alpha_j$ – we have seen in the proof of (1) and (2) that if we have arbitrary $i, j \in \{1, \dots, n\}$ set $m = a_i^{-1}a_j$, then $\sigma_m(\alpha_i) = \alpha_j$. If the polynomial f was reducible, say $f = gh$ for some $g, h \in \mathbb{Q}[x]$, the automorphisms σ_j would each have to permute the roots of g and the roots of h among themselves (and since α_i are pairwise different, g and h do not have a common root) so the Galois group would not be transitive.

In order to show that the coefficients of f are integral, we first show that they are rational. For that, it suffices to show that all the $\sigma_j, j \in (\mathbb{Z}/k\mathbb{Z})^\times$, act as identity on them. Since all the coefficients are symmetric functions of α_i, it is enough to show that the automorphisms σ_j are permutations of the set $\{\alpha_i : 1 \leq i \leq n\}$. We have $\sigma_j(\alpha_i) = \sigma_j(h(\zeta_k^{a_i})) = h(\zeta_k^{ja_i})$, and as we have seen above, $\sigma_j(\alpha_m) = h(\zeta_k^{ja_m}) = h(\zeta_k^{ja_n}) = \sigma_j(\alpha_n)$ if and only if $ja_m(ja_n)^{-1} = a_m a_n^{-1} \in H$, which implies $m = n$ (because a_i were chosen to be the coset representatives of H). Therefore every σ_j is injective on the set of alpha's and because this set is finite, each σ_j is a permutation.

By definition of α_i, $\alpha_i \in \mathbb{Z}[\zeta_k] = \mathcal{O}_{\mathbb{Q}(\zeta_k)}$ so α_i are integral over $\mathbb{Q}$. We have that $f_{\alpha,H}$ is irreducible with rational coefficients and has α_i as roots, so it is the minimal polynomial of α_i over $\mathbb{Q}$. But since α_i are integral, their minimal polynomial must have integer coefficients. □

For a subgroup $H \leq (\mathbb{Z}/k\mathbb{Z})^\times$ and α as in Lemma 12, denote by $f_{\alpha,H}$ the polynomial defined by (2.2.1) and $K = \mathbb{Q}(\alpha)$.

Let $D := \operatorname{disc}(f_{\alpha,H})$. Then by Proposition 8, D divides $\operatorname{disc}(K/\mathbb{Q})$ which divides $\operatorname{disc}(\mathbb{Q}(\zeta_k)/\mathbb{Q}) = \operatorname{disc}(\Phi_k)$, because $K \subset \mathbb{Q}(\zeta_k)$ and $\mathbb{Q}(\zeta_k)$ is the splitting field of the k-th cyclotomic polynomial Φ_k. Since the primes dividing $\operatorname{disc}(\Phi_k)$ divide k, we conclude that all the prime divisors of D divide k.

The following theorem shows that the polynomial $f_{\alpha,H}$ is the polynomial we are searching for. It will then be clear why we want $\ell^2 \equiv 1 \pmod{k}$ – because then $\{1, \ell\}$ is a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$.

It also gives us the idea how to show that there is no Euclidean proof if this condition is not satisfied – we will use it in the last chapter, where we show that the residue classes in $P(f)$ modulo k (if we don't count the finitely many exceptions) form a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$.

Theorem 13. *Let k be a positive integer, H a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$ and α a generator of the fixed field of H in $\mathbb{Q}(\zeta_k)$. If $p \in P(f_{\alpha,H})$, then $p \mid k$ or $p \pmod k \in H$.*

Proof. Let n be the index of H in $(\mathbb{Z}/k\mathbb{Z})^\times$ and denote by a_i, $i = 1, \ldots, n$, the coset representatives of H. Let K be the fix field of H in $\mathbb{Q}(\zeta_k)$. Then we have $K = \mathbb{Q}(\alpha)$ for some $h \in \mathbb{Z}[x]$ such that $\alpha = h(\zeta_k)$. Then by Lemma 12 $f_{\alpha,H}(x) = (x - \alpha_1) \ldots (x - \alpha_n)$ and $\mathbb{Q}(\alpha_i) = K$ for all $i = 1, \ldots, n$.

Let $p \in P(f_{\alpha,H})$ be such that p does not divide $\operatorname{disc}(f_{\alpha,H})$. Then there is some $a \in \mathbb{Z}$ such that $p \mid f_{\alpha,H}(a)$.

Let $\mathfrak{p}$ be any prime ideal in $\mathcal{O}_K$ dividing (p). Then $\mathfrak{p} \mid p \mid f_{\alpha,H}(a) = (a-\alpha_1) \ldots (a-\alpha_n)$ and since $\mathfrak{p}$ is prime and α_i are in $\mathcal{O}_K$, we can find some i such that $\mathfrak{p} \mid (a - \alpha_i)$ so $a \equiv \alpha_i \pmod{\mathfrak{p}}$. Since $a \equiv a^p \pmod p$ we have also $a \equiv a^p \pmod{\mathfrak{p}}$ and similarly $h(x^p) \equiv h(x)^p \pmod{\mathfrak{p}}$. We get the chain of congruences $h(\zeta_k^{a_i}) \equiv \alpha_i \equiv a \equiv a^p \equiv \alpha_i^p \equiv h(\zeta_k^{a_i})^p \equiv h(\zeta_k^{pa_i}) \pmod{\mathfrak{p}}$ so $\mathfrak{p} \mid \big(h(\zeta_k^{a_i}) - h(\zeta_k^{pa_i})\big)$. Since p was chosen not to divide $\operatorname{disc}(f_{\alpha,H})$, it does not divide k. Therefore pa_i is coprime to k so $h(\zeta_k^{pa_i})$ has to be one of the $\alpha_1, \ldots, \alpha_n$. If $h(\zeta_k^{pa_i}) \neq h(\zeta_k^{a_i})$, then there would be some j such that $\mathfrak{p}$ would divide $(\alpha_i - \alpha_j) \mid \operatorname{disc}(f_{\alpha,H})$ and since $\operatorname{disc}(f_{\alpha,H})$ is a rational integer, also p would divide $\operatorname{disc}(f_{\alpha,H})$ which would be a contradiction with our choice of p. Hence $\alpha_i = h(\zeta_k^{a_i}) = h(\zeta_k^{pa_i}) = \sigma_p(h(\zeta_k^{a_i})) = \sigma_p(\alpha_i)$ so σ_p fixes the field $\mathbb{Q}(\alpha_i) = K$. Since K is the fix field of H, $p \pmod k \in H$. □

It is interesting that the converse also holds:

Theorem 14 (Schur)**.** *Let H be a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$ and p a prime number such that $p \pmod k \in H$. If we choose $\alpha \in \mathbb{Z}[\zeta_k]$ such that $K = \mathbb{Q}(\alpha)$ is the fix field of H, then $p \in P(f_{\alpha,H})$.*

Proof. We use the notation from the proof of Theorem 13. If p is a prime such that $p \pmod k \in H$ then σ_p point wise fixes the field K by the definition of K. Therefore we have the congruences $\alpha^p \equiv h(\zeta_k)^p \equiv h(\zeta_k^p) \equiv h(\zeta_k) \equiv \alpha \pmod p$ so for any prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ dividing p we have $\alpha^p \equiv \alpha \pmod{\mathfrak{p}}$. But $\mathcal{O}_K/\mathfrak{p}$ is a field of characteristic p, so there are at most p solutions to the congruence $x^p - x \equiv 0 \pmod{\mathfrak{p}}$ and since all the rational integers satisfy this equation, we have that $\alpha \equiv a \pmod{\mathfrak{p}}$ for some $a \in \mathbb{Z}$. Hence $\mathfrak{p} \mid f_{\alpha,H}(a)$ and since $f_{\alpha,H}(a)$ is a rational integer, it follows that $p \mid f_{\alpha,H}(a)$. □

2.3 Proofs of Dirichlet's Theorem

We are now able to proof Dirichlet's Theorem for the case $\ell = 1$.

Theorem 15. *There exist infinitely many prime numbers $\equiv 1 \pmod k$.*

Proof. If we set $H = \{1\}$ and $\alpha = \zeta_k$, then $f_{\alpha,H} = \Phi_k$. Let S be the set of all prime divisors of k. Since $P(f_{\alpha,H})$ is infinite and S is finite, $P(f_{\alpha,H}) \setminus S$ is infinite. By Theorem 13, the set $P(f_{\alpha,H}) \setminus S$ consists only of primes $\equiv 1 \pmod k$. □

Note that in this case, we did not need to know that there is at least one prime of the desired form, because its existence is implied by the fact that $P(f)$ is infinite.

We can also state an important corollary of Theorems 11 and 13:

Corollary 16. *Let $f \in \mathbb{Z}[x]$ be a non-constant polynomial. For any $k \in \mathbb{N}$, there are infinitely many primes $\equiv 1 \pmod{k}$ which belong to $P(f)$.*

Proof. We use Theorem 11 for the polynomials f and Φ_k. By the proof of Theorem 15, the prime divisors of the polynomial Φ_k are (with finitely many exceptions) $\equiv 1 \pmod{k}$. □

Let us now choose some ℓ, k such that $\ell^2 \equiv 1 \pmod{k}$. Then, by Theorem 13 the polynomial $f_{\alpha,H}$ for $H = \{1, \ell\}$ could provide us a Euclidean proof for the arithmetic sequence $nk + \ell$. The last obstacle, which we are going to deal with in the following lemma, is that we don't know the explicit number α or the polynomial $h(x)$ needed to construct $f_{\alpha,H}$.

Lemma 17. *Let $\ell \in (\mathbb{Z}/k\mathbb{Z})^\times$ be of order 2, $H = \{1, \ell\}$ and set $h(x) = (u - x)(u - x^\ell)$ for some $u \in \mathbb{Z}$. Then there are infinitely many values of $u \in \mathbb{Z}$ such that $\mathbb{Q}(h(\zeta_k))$ is the fix field of H in $\mathbb{Q}(\zeta_k)$.*

In particular, if we let $n = [(\mathbb{Z}/k\mathbb{Z})^\times : H] = \frac{\varphi(k)}{2}$, denote $a_1, \dots, a_n$ the coset representatives of H and choose $u \in \mathbb{Z}$ such that the values $h(\zeta_k^{a_i})$ are pairwise different, then $\mathbb{Q}(h(\zeta_k))$ is the fix field of H in $\mathbb{Q}(\zeta_k)$.

Proof. First note that the values $h(\zeta_k)$ are independent of the choice of coset representatives a_i.

Let us choose $u \in \mathbb{Z}$ as described in the second part of the lemma. We need to prove that then the fix automorphisms of $\mathbb{Q}(h(\zeta_k))$ are exactly σ_1 and σ_ℓ. These automorphisms clearly fix $h(\zeta_k)$, and so they fix $\mathbb{Q}(h(\zeta_k))$.

We need to prove that there are no other such automorphisms, so suppose that σ_j is another $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_k)$ which fixes $h(\zeta_k)$. Then $h(\zeta_k) = \sigma_j(h(\zeta_k)) = (u - \zeta_k^j)(u - \zeta_k^{j\ell}) = h(\zeta_k^j)$, and since we chose u such that the values $h(\zeta_k^{a_i})$ are pairwise different, it follows that $j = 1$ or ℓ.

It remains to prove that there exist infinitely many $u \in \mathbb{Z}$ satisfying the condition. Since $(u - \zeta_k^{a_i})(u - \zeta_k^{a_i\ell}) = h(\zeta_k^{a_i}) = h(\zeta_k^{a_j}) = (u - \zeta_k^{a_j})(u - \zeta_k^{a_j\ell})$ is a quadratic equation in u, it has at most two solutions for every pair $a_i \neq a_j$ so we have excluded only a finite number of solutions. Note that the equation cannot be degenerate because on each side there is a quadratic polynomial in u with different roots. □

We are finally ready to prove the first implication of Theorem 1. The final proof is rather technical though the idea is simple – if there were finitely many primes in the progression $nk+\ell$, we find a value $f(c)$ for some c which is congruent to 1 and ℓ modulo k at the same time, so that $\ell = 1$ and that case we have already solved in Theorem 15.

A little annoying is the fact that we need to suppose the existence of one such prime, which we use also in another way than only to state that the product of all primes which are $\equiv \ell$ modulo k is non-empty. We will make some remarks about this condition later.

Theorem 18. *Let $k, \ell \in \mathbb{N}$ be such that $\ell^2 \equiv 1 \pmod{k}$ and suppose that there exists a prime congruent to ℓ modulo k. Then there are infinitely many such primes.*

Proof. If $\ell = 1$, the theorem follows from Theorem 15. Let's now suppose that $\ell \neq 1$ and $k > 2$. Then $H = \{1, \ell\}$ is a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$ and we can use Theorem 13. Consider the field $\mathbb{Q}(\zeta_k)$ whose Galois group is $(\mathbb{Z}/k\mathbb{Z})^\times$, and let K be the fix field of H. Set $h(x) = (u - x)(u - x^\ell)$ for some $u \in \mathbb{Z}$, which will be chosen later. From Lemma 17 it follows that there are infinitely many values of u such that $K = \mathbb{Q}(h(\zeta_k))$.

By Theorem 13 for $\alpha = h(\zeta_k)$ all the prime divisors of the polynomial $f_{\alpha,H}(x)$ divide k or are congruent to 1 or $\ell \pmod k$. In our case, we can compute the roots of $f_{\alpha,H}$ as $\alpha_i = \sigma_i(\alpha) = (u - \zeta_k^i)(u - \zeta_k^{\ell i})$ so if we let n to be the degree of $f_{\alpha,H}$, we get

$$\begin{aligned} f_{\alpha,H}(x)^2 &= \left(\prod_{i=1}^{n}(x - \alpha_i)\right)^2 = \left(\prod_{i=1}^{n}(x - (u - \zeta_k^{a_i})(u - \zeta_k^{\ell a_i}))\right)^2 \\ &= \prod_{(a,k)=1}(x - (u - \zeta_k^a)(u - \zeta_k^{\ell a})) \end{aligned}$$

where the last equality holds because H has order 2 and for each of its coset, there is only one term on the left-hand side but two equal terms on the right-hand side.

Now note, that

$$f_{\alpha,H}(0) = \prod_{i=1}^{n}[-(u - \zeta_k^a)(u - \zeta_k^{\ell a})] = (-1)^n \prod_{(a,k)=1}(u - \zeta_k^a) = (-1)^n \Phi_k(u)$$

where Φ_k is the k-th cyclotomic polynomial. Since the absolute term of Φ_k is 1, if we choose u to be a non-zero multiple of k, then $f_{\alpha,H}(0) = (-1)^n \Phi_k(u) \equiv (-1)^n \pmod k$ because by Theorem 13 and the proof of Theorem 15, each prime divisor of $f(0) = \Phi_k(u)$ not dividing k is $\equiv 1 \pmod k$. Now we define the polynomial $f := (-1)^n f_{\alpha,H}$, so that at each point, f has the same prime divisors as $f_{\alpha,H}$ and $f(0) \equiv 1 \pmod k$.

By our assumption, there exists a prime number $p \equiv \ell \pmod k$. Then p does not divide $\operatorname{disc}(f)$, because it would also have to divide k. By Theorem 14 $p \in P(f)$ so there exists a rational integer b such that $p \mid f(b)$. We now show that we can choose b such that $p^2 \nmid f(b)$ by replacing b with $b + p$.

If $p^2 | f(b)$, then we have $f(b + p) \equiv f(b) + pf'(b) \equiv pf'(b) \pmod{p^2}$. Since $p \nmid \operatorname{disc}(f)$, we know that f does not have double roots modulo p and because b is a root of f modulo p, $p \nmid f'(b)$. Therefore $f(b) \equiv 0 \pmod{p^2}$ implies that $f(b + p) \not\equiv 0 \pmod p$.

Suppose now that there are only finitely many primes $\equiv l \pmod k$, denote them $p = p_1, \ldots, p_r$. Let $P = p_2 p_3 \ldots p_r$ and find c such that $f(c) > 0$ and

$$\begin{aligned} c &\equiv b \pmod{p^2} \\ c &\equiv 0 \pmod{kP}. \end{aligned}$$

We can find such a c by using the Chinese Remainder Theorem and the fact, that the leading coefficient of f is negative only if f has odd degree, therefore if $f(c) \leq 0$, we can always add or subtract positive multiples of $p^2 kP$ to c to make the value $f(c)$ positive. Then $f(c) \equiv f(b) \pmod{p^2}$ and $f(c) \equiv f(0) \pmod{kP}$. We already know that the prime divisors of f are only the primes which divide k

or are $\equiv 1$ or $\ell \pmod k$. Since $f(0) = (-1)^n \phi_k(u)$ is only divisible by primes $\equiv 1 \pmod k$, kP is coprime with $f(0)$ and $kP \mid f(c) - f(0)$, kP has to be coprime to $f(c)$ and hence $f(c)$ is only divisible by primes $\equiv 1$ and p, which is $\equiv \ell \pmod k$. We know that $p \mid f(c)$, $p^2 \nmid f(c)$ and $f(c) > 0$, therefore we have $f(c) \equiv \ell \pmod k$. But also $f(c) \equiv f(0) \equiv 1 \pmod k$, which gives us a contradiction. Hence there must be infinitely many primes $\equiv \ell \pmod k$. □

What shall we do with the condition of existence of at least one prime $\equiv \ell$ modulo k? It would be enough if we showed that there exists some $a \in \mathbb{Z}$ such that $f_{\alpha,H}(a) \equiv \ell \pmod k$. The next proposition shows that in a particular case, when k is a prime number, the existence of such a is provided.

Proposition 19. *Let k be a prime number and ℓ an integer such that $\ell^2 \equiv 1 \pmod k$. Then there exists at least one prime number which is $\equiv \ell$ modulo k.*

Proof. When k is a prime, $\mathbb{Z}/k\mathbb{Z}$ is a field. If we let H to be the group $\{1, \ell\}$ and find the polynomial $f_{\alpha,H}$ such that all its prime divisors are $\equiv 1, \ell \pmod k$ or divide k, it can only take values $0, 1, \ell$ modulo k. Since $\mathbb{Z}/k\mathbb{Z}$ is a field, $f_{\alpha,H}$ can attain the same value modulo k only $\deg f_{\alpha,H} = \frac{\varphi(k)}{2} = \frac{k-1}{2}$ times. Therefore the values 0 and 1 together can only be obtained $k-1$ times, so at least one of the k numbers $f_{\alpha,H}(0)$, $f_{\alpha,H}(1)$, …, $f_{\alpha,H}(k-1)$ has to be $\equiv \ell$ modulo k. Since all the prime divisors of $f_{\alpha,H}$ are $\equiv 0, 1, \ell \pmod k$, the value which is $\equiv \ell \pmod k$ has to be divisible by a prime which is also $\equiv \ell \pmod k$ (we should assume here that the value is positive, but we can take $f = (-1)^{k-1} f_{\alpha,H}$ as in the proof of Theorem 18) – therefore at least one such prime exists. □

If k is a prime, the only solutions to $\ell^2 \equiv 1 \pmod k$ are $\ell = \pm 1$. Since the case $\ell = 1$ is already solved, the only new case we get from the last proposition is the case of arithmetic progressions $a_n = kn - 1$ for k prime.

The method from Proposition 19 probably cannot be extended to any other case because polynomials can have more than $\deg f$ roots modulo a composite number and also the polynomial $f_{\alpha,H}$ can attain more "bad" values (we discuss in Section 2.4 which values can it attain for some particular cases of k). There is nevertheless a possibility that if we made a deeper study of the polynomials $f_{\alpha,H}$, some variant could be made to work.

Example 20. What are the numbers k for which does the Theorem 18 give us the proof of Dirichlet's Theorem for all arithmetic progressions $kn + \ell$? We will show that the biggest such number is $k = 24$ and the others are all its divisors. We are searching for a k such that if $(k, \ell) = 1$, then $\ell^2 \equiv 1 \pmod k$. This is equivalent to saying that the group $(\mathbb{Z}/k\mathbb{Z})^\times$ has only elements of order 1 or 2, so it has to be a power of $\mathbb{Z}/2\mathbb{Z}$.

Let $k = p_1^{e_1} \dots p_n^{e_n}$ be the factorization of k. Then (see [7], Sections 2.8 and 2.10)

$$(\mathbb{Z}/k\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_n^{e_n}\mathbb{Z})^\times,$$

for odd primes p we have

$$(\mathbb{Z}/p^e\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)p^{e-1}\mathbb{Z} \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{e-1}\mathbb{Z},$$

and for $e \geq 3$, we have

$$(\mathbb{Z}/2^e\mathbb{Z})^\times \simeq \mathbb{Z}/2^{e-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Therefore the only way how $(\mathbb{Z}/k\mathbb{Z})^\times$ can be a power of $\mathbb{Z}/2\mathbb{Z}$ is that $k \in \{3, 4, 6, 8, 12, 24\}$.

2.4 Numerical examples of the polynomials $f_{\alpha,H}$

In this section we will show some examples of computed polynomials and try to make and prove a few assumptions based on the data we counted. Our goal is to show that there is always a value of $f_{\alpha,H}$ which is $\equiv \ell \pmod{k}$, which would give us the existence of the first prime. In fact, since there are some "bad" primes (namely the primes dividing k), the value does not really need to be $\equiv \ell$ modulo k – it could be $\equiv n\ell$ where n a value modulo k which cannot be obtained only by multiplying the prime divisors of k. For example in Table 2.3, we see that when $k = 24$ and $\ell = 5$, the polynomial takes the value 10 modulo k which also needs to be divisible by a prime which is $\equiv 5$ modulo k.

In this section, the value α will always be $(u - \zeta_k)(u - \zeta_k^\ell)$ and H will be the subgroup $\{1, \ell\}$, we will simply write f instead of $f_{\alpha,H}$.

In the proof of Theorem 18 we used u to be a multiple of k to make sure that $f(0)$ is only divisible by primes which are $\equiv 1 \pmod{k}$. Since our goal here is only to find one prime $\equiv \ell$ modulo k, our only condition on u is that arising from Lemma 17 that the values $\alpha_i = (u-\zeta_k^{a_i})(u-\zeta_k^{\ell a_i})$ are pairwise different for different coset representatives a_i. Then, the polynomial f will be $f(x) = \prod_i (x - \alpha_i)$. Note that if we change u to $u + k$, f modulo k does not change. Since we are mainly interested in the values of f modulo k, we will compute f for $u = 1, \ldots, k$.

The condition that the values α_i are pairwise different is equivalent to f not having a double root. Therefore for an integer u, instead of computing all the α_i we will at first compute f and then find out whether it has a double root by computing $\gcd(f, f')$. We will actually not include this in our tables since it never happened that $\gcd(f, f') \neq 1$ if $u \neq 0$ (and we will not give f when $u = 0$, but when $u = k$ instead).

We will start with the case $k = 24$. Then $(\mathbb{Z}/k\mathbb{Z})^\times = \{1, 5, 7, 11, 13, 17, 19, 23\}$ so f will have degree 4. If $\ell = 5$, the cosets are $\{1, 5\}, \{7, 11\}, \{13, 17\}$ and $\{19, 23\}$ so the cosets representatives can be chosen for example as $1, 7, 13$ and 19. We can now compute the polynomials with different values of u (we used the program Mathematica), the results are shown in Table 2.1.

The first thing we notice is that the polynomials modulo k repeat for different values of u. There are 4 different polynomials modulo k (namely $1+4x+8x^2+20x^3+x^4$, $1+16x+2x^2+8x^3+x^4$, $1+12x+8x^2+12x^3+x^4$ and $1+2x^2+x^4$) and the values of u for which there are the same form the sets $\{1, 5, 7, 11, 13, 17, 19, 23\}$, $\{2, 4, 8, 10, 14, 16, 20, 22\}$, $\{3, 9, 15, 21\}$ and $\{6, 12, 18, 24\}$. The first set is the group $(\mathbb{Z}/k\mathbb{Z})^\times$ and one can notice that all the four sets are closed under multiplication. This property of the sets is independent of ℓ and as Table 2.2 shows, when $\ell = 7$ the polynomials modulo k form the same blocks of numbers. These sets can also be easily described by divisibility – the numbers were divided into blocks of those divisible by 6, 2, 3 and the rest. We will see that for other choices of k, the situation will be more complicated.

One more thing to notice is that the absolute term of the polynomials does not depend on ℓ, but only on k and u. This is easily seen from the formula for

α_i, because if we change ℓ, the product of the α_i will stay the same.

u	f	f modulo 24
1	$1 + 4x + 8x^2 - 4x^3 + x^4$	$1 + 4x + 8x^2 + 20x^3 + x^4$
2	$241 - 224x + 98x^2 - 16x^3 + x^4$	$1 + 16x + 2x^2 + 8x^3 + x^4$
3	$6481 - 2844x + 488x^2 - 36x^3 + x^4$	$1 + 12x + 8x^2 + 12x^3 + x^4$
4	$65281 - 16256x + 1538x^2 - 64x^3 + x^4$	$1 + 16x + 2x^2 + 8x^3 + x^4$
5	$390001 - 62300x + 3752x^2 - 100x^3 + x^4$	$1 + 4x + 8x^2 + 20x^3 + x^4$
6	$1678321 - 186336x + 7778x^2 - 144x^3 + x^4$	$1 + 2x^2 + x^4$
7	$5762401 - 470204x + 14408x^2 - 196x^3 + x^4$	$1 + 4x + 8x^2 + 20x^3 + x^4$
8	$16773121 - 1048064x + 24578x^2 - 256x^3 + x^4$	$1 + 16x + 2x^2 + 8x^3 + x^4$
9	$43040161 - 2125116x + 39368x^2 - 324x^3 + x^4$	$1 + 12x + 8x^2 + 12x^3 + x^4$
10	$99990001 - 3999200x + 60002x^2 - 400x^3 + x^4$	$1 + 16x + 2x^2 + 8x^3 + x^4$
11	$214344241 - 7085276x + 87848x^2 - 484x^3 + x^4$	$1 + 4x + 8x^2 + 20x^3 + x^4$
12	$429960961 - 11942784x + 124418x^2 - 576x^3 + x^4$	$1 + 2x^2 + x^4$
13	$815702161 - 19305884x + 171368x^2 - 676x^3 + x^4$	$1 + 4x + 8x^2 + 20x^3 + x^4$
14	$1475750641 - 30116576x + 230498x^2 - 784x^3 + x^4$	$1 + 16x + 2x^2 + 8x^3 + x^4$
15	$2562840001 - 45560700x + 303752x^2 - 900x^3 + x^4$	$1 + 12x + 8x^2 + 12x^3 + x^4$
16	$4294901761 - 67106816x + 393218x^2 - 1024x^3 + x^4$	$1 + 16x + 2x^2 + 8x^3 + x^4$
17	$6975673921 - 96547964x + 501128x^2 - 1156x^3 + x^4$	$1 + 4x + 8x^2 + 20x^3 + x^4$
18	$11019855601 - 136046304x + 629858x^2 - 1296x^3 + x^4$	$1 + 2x^2 + x^4$
19	$16983432721 - 188180636x + 781928x^2 - 1444x^3 + x^4$	$1 + 4x + 8x^2 + 20x^3 + x^4$
20	$25599840001 - 255996800x + 960002x^2 - 1600x^3 + x^4$	$1 + 16x + 2x^2 + 8x^3 + x^4$
21	$37822664881 - 343060956x + 1166888x^2 - 1764x^3 + x^4$	$1 + 12x + 8x^2 + 12x^3 + x^4$
22	$54875639281 - 453515744x + 1405538x^2 - 1936x^3 + x^4$	$1 + 16x + 2x^2 + 8x^3 + x^4$
23	$78310705441 - 592139324x + 1679048x^2 - 2116x^3 + x^4$	$1 + 4x + 8x^2 + 20x^3 + x^4$
24	$110074982401 - 764407296x + 1990658x^2 - 2304x^3 + x^4$	$1 + 2x^2 + x^4$

Table 2.1: Polynomial f for $k = 24$ and $\ell = 5$ with different values of u

u	f	f modulo 24
1	$1 + 2x + 5x^2 - 2x^3 + x^4$	$1 + 2x + 5x^2 + 22x^3 + x^4$
2	$241 - 214x + 83x^2 - 14x^3 + x^4$	$1 + 2x + 11x^2 + 10x^3 + x^4$
3	$6481 - 2734x + 453x^2 - 34x^3 + x^4$	$1 + 2x + 21x^2 + 14x^3 + x^4$
4	$65281 - 15838x + 1475x^2 - 62x^3 + x^4$	$1 + 2x + 11x^2 + 10x^3 + x^4$
5	$390001 - 61198x + 3653x^2 - 98x^3 + x^4$	$1 + 2x + 5x^2 + 22x^3 + x^4$
6	$1678321 - 183958x + 7635x^2 - 142x^3 + x^4$	$1 + 2x + 3x^2 + 2x^3 + x^4$
7	$5762401 - 465694x + 14213x^2 - 194x^3 + x^4$	$1 + 2x + 5x^2 + 22x^3 + x^4$
8	$16773121 - 1040254x + 24323x^2 - 254x^3 + x^4$	$1 + 2x + 11x^2 + 10x^3 + x^4$
9	$43040161 - 2112478x + 39045x^2 - 322x^3 + x^4$	$1 + 2x + 21x^2 + 14x^3 + x^4$
10	$99990001 - 3979798x + 59603x^2 - 398x^3 + x^4$	$1 + 2x + 11x^2 + 10x^3 + x^4$
11	$214344241 - 7056718x + 87365x^2 - 482x^3 + x^4$	$1 + 2x + 5x^2 + 22x^3 + x^4$
12	$429960961 - 11902174x + 123843x^2 - 574x^3 + x^4$	$1 + 2x + 3x^2 + 2x^3 + x^4$
13	$815702161 - 19249774x + 170693x^2 - 674x^3 + x^4$	$1 + 2x + 5x^2 + 22x^3 + x^4$
14	$1475750641 - 30040918x + 229715x^2 - 782x^3 + x^4$	$1 + 2x + 11x^2 + 10x^3 + x^4$
15	$2562840001 - 45460798x + 302853x^2 - 898x^3 + x^4$	$1 + 2x + 21x^2 + 14x^3 + x^4$
16	$4294901761 - 66977278x + 392195x^2 - 1022x^3 + x^4$	$1 + 2x + 11x^2 + 10x^3 + x^4$
17	$6975673921 - 96382654x + 499973x^2 - 1154x^3 + x^4$	$1 + 2x + 5x^2 + 22x^3 + x^4$
18	$11019855601 - 135838294x + 628563x^2 - 1294x^3 + x^4$	$1 + 2x + 3x^2 + 2x^3 + x^4$
19	$16983432721 - 187922158x + 780485x^2 - 1442x^3 + x^4$	$1 + 2x + 5x^2 + 22x^3 + x^4$
20	$25599840001 - 255679198x + 958403x^2 - 1598x^3 + x^4$	$1 + 2x + 11x^2 + 10x^3 + x^4$
21	$37822664881 - 342674638x + 1165125x^2 - 1762x^3 + x^4$	$1 + 2x + 21x^2 + 14x^3 + x^4$
22	$54875639281 - 453050134x + 1403603x^2 - 1934x^3 + x^4$	$1 + 2x + 11x^2 + 10x^3 + x^4$
23	$78310705441 - 591582814x + 1676933x^2 - 2114x^3 + x^4$	$1 + 2x + 5x^2 + 22x^3 + x^4$
24	$110074982401 - 763747198x + 1988355x^2 - 2302x^3 + x^4$	$1 + 2x + 3x^2 + 2x^3 + x^4$

Table 2.2: Polynomial f for $k = 24$ and $\ell = 7$ with different values of u

Tables 2.3 and 2.4 show the values the polynomials take modulo 24. In these tables, we let f_1, f_2, f_3 and f_4 be the 4 different polynomials modulo k in the order in which they first appear in the corresponding tables (so for $\ell = 5$, we have $f_1 = 1 + 4x + 8x^2 + 20x^3 + x^4$, $f_2 = 1 + 16x + 2x^2 + 8x^3 + x^4$, $f_3 = 1 + 12x + 8x^2 + 12x^3 + x^4$ and $f_4 = 1 + 2x^2 + x^4$).

We have highlighted the values which must be divisible by a prime $\equiv \ell$ modulo k. We see that in every table, such a value exists, though it does not need to exist for every polynomial. For example when $\ell = 7$, we see that f_2 only takes value the value 1 modulo 24. This also shows that the proof of Lemma 19 probably cannot be extended for k not prime, since then we are not able to estimate how many times can the polynomial attain the same value.

x	1	2	3	4	5	6	7	8	9	10	11	12
$f_1(x)$	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1
$f_2(x)$	4	1	4	1	4	1	4	1	4	1	4	1
$f_3(x)$	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1
$f_4(x)$	4	1	4	1	4	1	4	1	4	1	4	1
x	13	14	15	16	17	18	19	20	21	22	23	24
$f_1(x)$	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1
$f_2(x)$	4	1	4	1	4	1	4	1	4	1	4	1
$f_3(x)$	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1
$f_4(x)$	4	1	4	1	4	1	4	1	4	1	4	1

Table 2.3: The values of different f modulo 24 for $\ell = 5$

x	1	2	3	4	5	6	7	8	9	10	11	12
$f_1(x)$	**7**	1	**7**	1	**7**	1	**7**	1	**7**	1	**7**	1
$f_2(x)$	1	1	1	1	1	1	1	1	1	1	1	1
$f_3(x)$	**15**	1	**7**	9	**7**	1	**15**	1	**7**	9	**7**	1
$f_4(x)$	9	1	1	9	1	1	9	1	1	9	1	1
x	13	14	15	16	17	18	19	20	21	22	23	24
$f_1(x)$	**7**	1	**7**	1	**7**	1	**7**	1	**7**	1	**7**	1
$f_2(x)$	1	1	1	1	1	1	1	1	1	1	1	1
$f_3(x)$	**15**	1	**7**	9	**7**	1	**15**	1	**7**	9	**7**	1
$f_4(x)$	9	1	1	9	1	1	9	1	1	9	1	1

Table 2.4: The values of different f modulo 24 for $\ell = 7$

It may be surprising that we see the value 15 in Table 2.4, since the values of f when $\ell = 7$ should only be divisible by 2,3 or 7, not by 5. However, we have $15 \equiv 63 = 3 \cdot 3 \cdot 7 \pmod{24}$ which also gives us the reason why this value is highlighted. This situation can happen because when we are solving the equation $9x \equiv 15 \pmod{24}$, we can not multiply both sides by the inverse of 3 modulo 24, we have to divide the modulus as well to obtain $3x \equiv 5 \pmod{8}$. Now we already have $\mathrm{GCD}(8, 3) = 1$ so we get the solution $x \equiv 3 \cdot 5 \equiv 7 \pmod{8}$.

If we do a little bit of computation when $\ell = 7$, we see that the situation is not at all that promising as it may seem. Even though the only prime divisors of the values attained by f are only 2, 3 and the primes which are $\equiv 1, 7$ modulo

24, we can make a table of all the values we can get and choose those which can not be obtained only by multiplying 2 and 3 in order to find out which of them really need to be divisible by a prime that is $\equiv 7$ modulo 24.

We find out that combining the right primes, we can obtain all residues from the set $\{1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 15, 16, 18, 21\}$. From these 14 values, only 4 need to be divisible by a prime which is $\equiv 7$ modulo 24, namely $\{7, 14, 15, 21\}$.

Tables 2.5 – 2.10 show the four different polynomials for all the other choices of ℓ and their values modulo 24. There are again some values which seem to be divisible by a "wrong" prime, but one can easily verify that they can be obtained by combining the right prime divisors.

ℓ	11	13	17
$f_1(x)$	$1 + 4x^2 + x^4$	$1 + 22x + 5x^2 + 20x^3 + x^4$	$1 + 20x + 8x^2 + 20x^3 + x^4$
$f_2(x)$	$1 + 12x + 22x^2 + 12x^3 + x^4$	$1 + 16x + 23x^2 + 8x^3 + x^4$	$1 + 8x + 2x^2 + 8x^3 + x^4$
$f_3(x)$	$1 + 16x + 12x^2 + 16x^3 + x^4$	$1 + 6x + 5x^2 + 12x^3 + x^4$	$1 + 12x + 8x^2 + 12x^3 + x^4$
$f_4(x)$	$1 + 4x + 6x^2 + 4x^3 + x^4$	$1 + 23x^2 + x^4$	$1 + 2x^2 + x^4$
ℓ	19	23	
$f_1(x)$	$1 + 18x + 13x^2 + 18x^3 + x^4$	$1 + 8x + 20x^2 + 16x^3 + x^4$	
$f_2(x)$	$1 + 6x + 19x^2 + 6x^3 + x^4$	$1 + 20x + 14x^2 + 4x^3 + x^4$	
$f_3(x)$	$1 + 10x + 21x^2 + 10x^3 + x^4$	$1 + 8x + 12x^2 + 8x^3 + x^4$	
$f_4(x)$	$1 + 22x + 3x^2 + 22x^3 + x^4$	$1 + 20x + 6x^2 + 20x^3 + x^4$	

Table 2.5: The four different polynomials modulo 24 for other values of ℓ

x	1	2	3	4	5	6	7	8	9	10	11	12
$f_1(x)$	6	9	**22**	9	6	1	6	9	**22**	9	6	1
$f_2(x)$	0	9	16	9	0	1	0	9	16	9	0	1
$f_3(x)$	**22**	9	**22**	1	6	1	**22**	9	**22**	1	6	1
$f_4(x)$	16	9	16	1	0	1	16	9	16	1	0	1
x	13	14	15	16	17	18	19	20	21	22	23	24
$f_1(x)$	6	9	**22**	9	6	1	6	9	**22**	9	6	1
$f_2(x)$	0	9	16	9	0	1	0	9	16	9	0	1
$f_3(x)$	**22**	9	**22**	1	6	1	**22**	9	**22**	1	6	1
$f_4(x)$	16	9	16	1	0	1	16	9	16	1	0	1

Table 2.6: The values of different f modulo 24 for $\ell = 11$

x	1	2	3	4	5	6	7	8	9	10	11	12
$f_1(x)$	1	1	**13**	1	1	1	**13**	1	1	1	**13**	1
$f_2(x)$	1	**13**	1	1	1	**13**	1	1	1	**13**	1	1
$f_3(x)$	1	1	**13**	1	1	1	**13**	1	1	1	**13**	1
$f_4(x)$	1	**13**	1	1	1	**13**	1	1	1	**13**	1	1
x	13	14	15	16	17	18	19	20	21	22	23	24
$f_1(x)$	1	1	**13**	1	1	1	**13**	1	1	1	**13**	1
$f_2(x)$	1	**13**	1	1	1	**13**	1	1	1	**13**	1	1
$f_3(x)$	1	1	**13**	1	1	1	**13**	1	1	1	**13**	1
$f_4(x)$	1	**13**	1	1	1	**13**	1	1	1	**13**	1	1

Table 2.7: The values of different f modulo 24 for $\ell = 13$

x	1	2	3	4	5	6	7	8	9	10	11	12
$f_1(x)$	2	9	**10**	**17**	18	1	2	9	**10**	**17**	18	1
$f_2(x)$	**20**	9	4	**17**	12	1	**20**	9	4	**17**	12	1
$f_3(x)$	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1
$f_4(x)$	4	1	4	1	4	1	4	1	4	1	4	1
x	13	14	15	16	17	18	19	20	21	22	23	24
$f_1(x)$	2	9	**10**	**17**	18	1	2	9	**10**	**17**	18	1
$f_2(x)$	**20**	9	4	**17**	12	1	**20**	9	4	**17**	12	1
$f_3(x)$	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1	**10**	1
$f_4(x)$	4	1	4	1	4	1	4	1	4	1	4	1

Table 2.8: The values of different f modulo 24 for $\ell = 17$

x	1	2	3	4	5	6	7	8	9	10	11	12
$f_1(x)$	3	9	**19**	9	3	1	3	9	**19**	9	3	1
$f_2(x)$	9	9	1	9	9	1	9	9	1	9	9	1
$f_3(x)$	**19**	9	**19**	1	3	1	**19**	9	**19**	1	3	1
$f_4(x)$	1	9	1	1	9	1	1	9	1	1	9	1
x	13	14	15	16	17	18	19	20	21	22	23	24
$f_1(x)$	3	9	**19**	9	3	1	3	9	**19**	9	3	1
$f_2(x)$	9	9	1	9	9	1	9	9	1	9	9	1
$f_3(x)$	**19**	9	**19**	1	3	1	**19**	9	**19**	1	3	1
$f_4(x)$	1	9	1	1	9	1	1	9	1	1	9	1

Table 2.9: The values of different f modulo 24 for $\ell = 19$

x	1	2	3	4	5	6	7	8	9	10	11	12
$f_1(x)$	**22**	1	**22**	1	**22**	1	**22**	1	**22**	1	**22**	1
$f_2(x)$	16	1	16	1	16	1	16	1	16	1	16	1
$f_3(x)$	6	1	**22**	9	**22**	1	6	1	**22**	9	**22**	1
$f_4(x)$	0	1	16	9	16	1	0	1	16	9	16	1
x	13	14	15	16	17	18	19	20	21	22	23	24
$f_1(x)$	**22**	1	**22**	1	**22**	1	**22**	1	**22**	1	**22**	1
$f_2(x)$	16	1	16	1	16	1	16	1	16	1	16	1
$f_3(x)$	6	1	**22**	9	**22**	1	6	1	**22**	9	**22**	1
$f_4(x)$	0	1	16	9	16	1	0	1	16	9	16	1

Table 2.10: The values of different f modulo 24 for $\ell = 23$

Table 2.11 shows the polynomials for $k = 15$ and $\ell = 4$. We see that the sets of u for which the polynomials modulo 15 are the same, are more chaotic. As opposed to $k = 24$, when those groups of u were easily described, here we obtain the sets $\{1, 13\}$, $\{2\}$, $\{3, 6\}$, $\{4, 10\}$, $\{5, 14\}$, $\{7\}$, $\{8, 11\}$, $\{9, 15\}$ and $\{12\}$. We were not able to find any structure which would tell why are the numbers divided as they are. It might seem from all the polynomials we have shown so far that the absolute term always has to be $\equiv 1$ modulo 10, but this rule will be broken in the next case when $k = 21$.

u	f	f modulo 15
1	$1 + x + 2x^2 - x^3 + x^4$	$1 + x + 2x^2 + 14x^3 + x^4$
2	$151 - 138x + 59x^2 - 12x^3 + x^4$	$1 + 12x + 14x^2 + 3x^3 + x^4$
3	$4561 - 2059x + 372x^2 - 31x^3 + x^4$	$1 + 11x + 12x^2 + 14x^3 + x^4$
4	$49981 - 12878x + 1283x^2 - 58x^3 + x^4$	$1 + 7x + 8x^2 + 2x^3 + x^4$
5	$315121 - 52023x + 3278x^2 - 93x^3 + x^4$	$1 + 12x + 8x^2 + 12x^3 + x^4$
6	$1406371 - 160954x + 6987x^2 - 136x^3 + x^4$	$1 + 11x + 12x^2 + 14x^3 + x^4$
7	$4956001 - 415763x + 13184x^2 - 187x^3 + x^4$	$1 + 7x + 14x^2 + 8x^3 + x^4$
8	$14709241 - 942654x + 22787x^2 - 246x^3 + x^4$	$1 + 6x + 2x^2 + 9x^3 + x^4$
9	$38316961 - 1936303x + 36858x^2 - 313x^3 + x^4$	$1 + 2x + 3x^2 + 2x^3 + x^4$
10	$90090991 - 3681098x + 56603x^2 - 388x^3 + x^4$	$1 + 7x + 8x^2 + 2x^3 + x^4$
11	$195019441 - 6575259x + 83372x^2 - 471x^3 + x^4$	$1 + 6x + 2x^2 + 9x^3 + x^4$
12	$394379701 - 11157838x + 118659x^2 - 562x^3 + x^4$	$1 + 2x + 9x^2 + 8x^3 + x^4$
13	$753327121 - 18138599x + 164102x^2 - 661x^3 + x^4$	$1 + x + 2x^2 + 14x^3 + x^4$
14	$1370877691 - 28430778x + 221483x^2 - 768x^3 + x^4$	$1 + 12x + 8x^2 + 12x^3 + x^4$
15	$2392743361 - 43186723x + 292728x^2 - 883x^3 + x^4$	$1 + 2x + 3x^2 + 2x^3 + x^4$

Table 2.11: Polynomial f for $k = 15$ and $\ell = 4$

Table 2.12 shows the computation of f modulo 15 for $\ell = 11$. It seems that the blocks of u for which the polynomials f modulo 15 are equal are again independent of ℓ.

u	f modulo 15
1	$1 + 12x + 4x^2 + 13x^3 + x^4$
2	$1 + 13x + 9x^2 + 2x^3 + x^4$
3	$1 + 7x + 4x^2 + 13x^3 + x^4$
4	$1 + 6x + x^2 + x^3 + x^4$
5	$1 + x + 6x^2 + 11x^3 + x^4$
6	$1 + 7x + 4x^2 + 13x^3 + x^4$
7	$1 + 3x + 4x^2 + 7x^3 + x^4$
8	$1 + 7x + 9x^2 + 8x^3 + x^4$
9	$1 + x + x^2 + x^3 + x^4$
10	$1 + 6x + x^2 + x^3 + x^4$
11	$1 + 7x + 9x^2 + 8x^3 + x^4$
12	$1 + 13x + 4x^2 + 7x^3 + x^4$
13	$1 + 12x + 4x^2 + 13x^3 + x^4$
14	$1 + x + 6x^2 + 11x^3 + x^4$
15	$1 + x + x^2 + x^3 + x^4$

Table 2.12: Polynomial f modulo k for $k = 15$ and $\ell = 11$

Tables 2.13 and 2.14 show the values of f modulo 15 for $\ell = 4$ and $\ell = 11$, where $f_1, \ldots, f_9$ are again the 9 different polynomials f modulo 15 (in the order in

which they appeared in tables 2.11 or 2.12). We can again compute all the values we can obtain modulo 15 by multiplying together 3, 5 and the primes which are $\equiv \ell$ modulo 15. In this case, we can only get the values $\{1, 3, 5, 6, 9, 10, 12, \ell\}$, but the only one which has to be divisible by a prime $\equiv \ell$ is ℓ itself. We have again highlighted those values in the tables.

It is interesting that in table 2.14, the only values that appear are 1, 5, 11 and 10 – that is only the values divisible by 5 or a prime $\equiv 11$ modulo 15, none of the values is divisible by 3.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f_1(x)$	**4**	**4**	1	**4**	1	**4**	**4**	1	**4**	1	**4**	**4**	1	**4**	1
$f_2(x)$	1	1	10	1	1	1	1	10	1	1	1	1	10	1	1
$f_3(x)$	9	**4**	1	9	1	**4**	9	1	**4**	6	**4**	**4**	6	**4**	1
$f_4(x)$	**4**	**4**	**4**	1	1	**4**	**4**	**4**	1	1	**4**	**4**	**4**	1	1
$f_5(x)$	**4**	**4**	**4**	1	1	**4**	**4**	**4**	1	1	**4**	**4**	**4**	1	1
$f_6(x)$	1	1	10	1	1	1	1	10	1	1	1	1	10	1	1
$f_7(x)$	**4**	**4**	1	**4**	1	**4**	**4**	1	**4**	1	**4**	**4**	1	**4**	1
$f_8(x)$	9	**4**	**4**	6	1	**4**	9	**4**	1	6	**4**	**4**	9	1	1
$f_9(x)$	6	1	10	6	1	1	6	10	1	6	1	1	0	1	1

Table 2.13: The values of different f modulo 15 for $\ell = 4$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f_1(x)$	1	**11**	10	1	**11**	1	1	5	1	1	**11**	1	10	**11**	1
$f_2(x)$	**11**	5	1	**11**	**11**	1	5	**11**	1	**11**	**11**	10	**11**	**11**	1
$f_3(x)$	**11**	1	10	**11**	1	1	**11**	10	1	**11**	1	1	5	1	1
$f_4(x)$	10	**11**	1	1	**11**	10	1	**11**	1	1	5	1	1	**11**	1
$f_5(x)$	5	**11**	1	**11**	**11**	10	**11**	**11**	1	**11**	5	1	**11**	**11**	1
$f_6(x)$	1	5	1	1	**11**	1	10	**11**	1	1	**11**	10	1	**11**	1
$f_7(x)$	**11**	**11**	10	**11**	**11**	1	**11**	5	1	**11**	**11**	1	5	**11**	1
$f_8(x)$	5	1	1	**11**	1	10	**11**	1	1	**11**	10	1	**11**	1	1
$f_9(x)$	**11**	10	1	**11**	1	1	5	1	1	**11**	1	10	**11**	1	1

Table 2.14: The values of different f modulo 15 for $\ell = 11$

The two following tables show the computations for $k = 21$ and $\ell = 8$. Table 2.15 shows the polynomial f modulo 21 for different values of u. The sets of u for which those polynomials seem again not to admit any simple structure. There are 12 different polynomials and the next table shows their values modulo 21. It is again interesting that none of the values is divisible by 3. Also this is the first case where it happened that $f(0) \equiv \ell \pmod{k}$ instead of 1.

u	f modulo 21
1	$1+19x+4x^2+13x^3+9x^4+17x^5+x^6$
2	$7+7x^2+7x^3+x^6$
3	$1+13x+x^2+13x^3+x^4+13x^5+x^6$
4	$7+7x+7x^2+7x^3+14x^5+x^6$
5	$1+12x+4x^2+13x^3+9x^4+3x^5+x^6$
6	$1+x+x^2+x^3+x^4+x^5+x^6$
7	$1+x+x^2+x^3+15x^4+8x^5+x^6$
8	$1+12x+4x^2+13x^3+9x^4+3x^5+x^6$
9	$7+7x+7x^2+7x^3+7x^4+7x^5+x^6$
10	$1+13x+x^2+13x^3+15x^4+20x^5+x^6$
11	$7+7x^2+7x^3+x^6$
12	$1+19x+4x^2+13x^3+16x^4+10x^5+x^6$
13	$1+x+x^2+x^3+15x^4+8x^5+x^6$
14	$1+15x+x^2+x^3+15x^4+15x^5+x^6$
15	$1+19x+4x^2+13x^3+16x^4+10x^5+x^6$
16	$7+7x+7x^2+7x^3+14x^5+x^6$
17	$1+6x+x^2+13x^3+15x^4+6x^5+x^6$
18	$7+7x+7x^2+7x^3+7x^4+7x^5+x^6$
19	$1+19x+4x^2+13x^3+9x^4+17x^5+x^6$
20	$1+15x+x^2+x^3+15x^4+15x^5+x^6$
21	$1+x+x^2+x^3+x^4+x^5+x^6$

Table 2.15: Polynomial f modulo k for $k=21$ and $\ell=8$

x	1	2	3	4	5	6	7	8	9	10	11
$f_1(x)$	1	**8**	7	1	**8**	1	1	**8**	1	7	**8**
$f_2(x)$	1	**8**	1	1	**8**	1	7	**8**	1	1	**8**
$f_3(x)$	1	1	1	1	1	7	1	1	1	1	1
$f_4(x)$	1	**8**	1	1	**8**	1	7	**8**	1	1	**8**
$f_5(x)$	1	**8**	7	1	**8**	1	1	**8**	1	7	**8**
$f_6(x)$	7	1	1	1	1	1	1	7	1	1	1
$f_7(x)$	7	**8**	1	1	**8**	1	1	**14**	1	1	**8**
$f_8(x)$	1	1	1	1	1	1	7	1	1	1	1
$f_9(x)$	1	**8**	1	1	**8**	7	1	**8**	1	1	**8**
$f_{10}(x)$	1	1	7	1	1	1	1	1	1	7	1
$f_{11}(x)$	7	**8**	1	1	**8**	1	1	**14**	1	1	**8**
$f_{12}(x)$	1	**8**	1	1	**8**	7	1	**8**	1	1	**8**

x	12	13	14	15	16	17	18	19	20	21	
$f_1(x)$	1	1	**8**	1	1	**14**	1	1	**8**	1	
$f_2(x)$	1	1	**14**	1	1	**8**	1	1	**8**	7	
$f_3(x)$	1	7	1	1	1	1	1	1	7	1	
$f_4(x)$	1	1	**14**	1	1	**8**	1	1	**8**	7	
$f_5(x)$	1	1	**8**	1	1	**14**	1	1	**8**	1	
$f_6(x)$	1	1	1	7	1	1	1	1	1	1	
$f_7(x)$	1	1	**8**	7	1	**8**	1	1	**8**	1	
$f_8(x)$	1	1	7	1	1	1	1	1	1	7	
$f_9(x)$	1	7	**8**	1	1	**8**	1	1	**14**	1	
$f_{10}(x)$	1	1	1	1	1	7	1	1	1	1	
$f_{11}(x)$	1	1	**8**	7	1	**8**	1	1	**8**	1	
$f_{12}(x)$	1	7	**8**	1	1	**8**	1	1	**14**	1	

Table 2.16: The values of different f modulo 21 for $\ell=8$

3. Density of prime ideals and the Chebotarev Density Theorem

In order to prove the other implication of Theorem 1, that no Euclidean proof of Dirichlet's Theorem exists if $\ell^2 \not\equiv 1 \pmod{k}$, we will need to use a generalization of Dirichlet's Theorem itself – the Chebotarev Density Theorem. Before we will be ready for the statement, we will need to define the Frobenius element and what we mean by *density* of a set of primes.

3.1 Frobenius element

We will start with a lemma which will allow us to correctly define the *Frobenius element*.

Lemma 21. *Let L/K be a Galois extension and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime which is unramified in L. Then for any prime divisor $\mathcal{P}$ of $\mathfrak{p}$, there exist a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathcal{P}}$ for any $\alpha \in \mathcal{O}_L$.*

Proof. See section C of Chapter 5 in [6]. □

We will call the element σ the **Frobenius element of** $\mathcal{P}$ and denote it as $\mathrm{Fr}_{\mathcal{P}}(L/K)$ (we will write only $\mathrm{Fr}_{\mathcal{P}}$ if there is no ambiguity possible).

For an arbitrary $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\mathcal{P})$ is another prime divisor of $\mathfrak{p}$ and $\mathrm{Fr}_{\sigma(P)} = \sigma \circ \mathrm{Fr}_{\mathcal{P}} \circ \sigma^{-1}$ (this fact follows from the uniqueness and a direct computation, it is a good exercise to get used to the Frobenius elements). Therefore for an abelian extension, $\mathrm{Fr}_{\mathcal{P}}$ only depends on $\mathfrak{p}$ so we can denote it as $\mathrm{Fr}_{\mathfrak{p}}$.

In a non-abelian extension, by $\mathrm{Fr}_{\mathfrak{p}}$ we will mean the whole conjugacy class of $\mathrm{Fr}_{\mathcal{P}}$ in $\mathrm{Gal}(L/K)$.

In order to get familiar with the definition, we are going to prove a simple lemma which will be useful for us later.

Lemma 22. *Let K be an algebraic number field and choose a rational prime p which has a first degree prime ideal factor in K and which is unramified in $K(\zeta_k)$ for some $k \in \mathbb{N}$. Let $\mathfrak{p}$ be a first degree prime ideal factor of p in K and let $\sigma = \mathrm{Fr}_{\mathfrak{p}}(K(\zeta_k)/K)$. Then $\sigma{\restriction_{\mathbb{Q}(\zeta_k)}} = \sigma_q$, where $q = p \bmod k$.*

Proof. Let $\mathcal{P}$ be an arbitrary prime ideal factor of $\mathfrak{p}$ in $K(\zeta_k)$. Then by the definition of the Frobenius Element, $\sigma(\zeta_k) \equiv \zeta_k^{N(\mathfrak{p})} \pmod{\mathcal{P}}$. By the choice of $\mathfrak{p}$, we have $1 = f_{\mathfrak{p}|p} = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$ so $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = p$. Then $\sigma(\zeta_k) \equiv \zeta_k^p = \zeta_k^q \pmod{\mathcal{P}}$. Since $\sigma{\restriction_{\mathbb{Q}(\zeta_k)}} \in \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ and σ_q (which was defined to be the unique element of $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ for which $\sigma_q(\zeta_k) = \zeta_k^q$) has the same property as σ, from uniqueness of the Frobenius element we conclude that $\sigma(\zeta_k) = \zeta_k^q$ holds even without mod $\mathcal{P}$. □

3.2 Density of sets of primes and the Chebotarev Density Theorem

We begin with the definition of density of a set of primes in an algebraic number field.

Definition 23. *Let K be an algebraic number field and M a set of prime ideals of K. Then the Dirichlet density of M is defined as*

$$\delta(M) = \lim_{s \to 1^+} \frac{\sum\limits_{\mathfrak{p} \in M} \frac{1}{N(\mathfrak{p})^s}}{\log \frac{1}{s-1}},$$

if the limit exists.

Dirichlet density has the following properties:

- If $\delta(M)$ exists, then $0 \leq \delta(M) \leq 1$
- If M is the set of all primes in K, then $\delta(M) = 1$.
- For disjoint M, N such that $\delta(M)$ and $\delta(N)$ exist, $\delta(M \cup N) = \delta(M) + \delta(N)$.
- If M is finite, then $\delta(M) = 0$.
- If $\delta(M) > 0$, then M is infinite.

Te first of the listed property is the hardest to prove, one needs to study the ζ-function and its pole in 1 in order to be able to establish it. However, once the first property is proved, the others follow easily.

For us, the most important will be the last property which states that in order to prove that some set of primes is infinite, it suffices to show that it has positive density.

Before stating the Chebotarev Density Theorem, we will be to prove that most of the primes in an algebraic number field K have inertia degree 1 over $\mathbb{Q}$.

Proposition 24. *Let K be an algebraic number field, let P be the set of all primes in K and set*

$$P_1 = \{\mathfrak{p} : \mathfrak{p} \text{ is a prime in } K \text{ of inertia degree } 1 \text{ over } \mathbb{Q}\}.$$

Then $\delta(P_1) = 1$ and $\delta(P \setminus P_1) = 0$.

Proof. For a prime ideal $\mathfrak{p}$ in K, $N(\mathfrak{p}) = p^f$, where $(p) = \mathfrak{p} \cap \mathbb{Z}$ and $f = f_{\mathfrak{p}|p}$.

By the properties of Dirichlet density listed above, it suffices to show that the set $S = P \setminus P_1$ has Dirichlet density equal to 0. In order to do so, it suffices to show that the sum in the numerator from the definition of $\delta(S)$ with $s = 1$ converges. Let $n = [K : \mathbb{Q}]$ and let's count (for a prime p, by $f_{\mathfrak{p}}$ we mean the lowest inertia degree of a prime in S dividing p, in particular f_p is always greater or equal to 2):

$$\sum_{\mathfrak{p} \in S} \frac{1}{N(\mathfrak{p})} = \sum_{\mathfrak{p} \in S} \frac{1}{p^{f_{\mathfrak{p}|p}}} \leq n \sum_{p \text{ prime}} \frac{1}{p^{f_p}} \leq n \sum_{p \text{ prime}} \frac{1}{p^2} < \infty.$$

In the first inequality, we used the fact that the number of prime ideals dividing a fixed rational prime p is at most n. □

Note that the last proposition can be easily generalized to the case of an arbitrary extension L/K with the same proof using the fact that the inertia degree of a prime in L over K is at most the inertia degree of the prime over $\mathbb{Q}$.

Lemma 25. *Let K be an algebraic number field and denote by $P_1(K)$ the set of primes in K of inertia degree 1 over $\mathbb{Q}$. If M is an arbitrary set of primes in K whose Dirichlet density exists, then $\delta(M) = \delta(M \cap P_1(K))$.*

Proof. Let P be the set of all primes in K. From the properties of Dirichlet density, we have

$$\begin{aligned}\delta(M) &= \delta(M \cap P_1(K)) + \delta(M \setminus P_1(K)) \leq \delta(M \cap P_1(K)) + \delta(P \setminus P_1(K)) \\ &= \delta(M \cap P_1(K)),\end{aligned}$$

where the last equality holds because the set of primes of inertia degree greater than 1 has Dirichlet density 0. Because $M \subset M \cap P_1(K)$, the other inequality is trivial and we are done. □

If we know that the set of primes with certain property has a positive density, this lemma tells us that there are infinitely many of these primes with inertia degree one – the primes of inertia degree 1 over $\mathbb{Q}$ are those we are especially interested in.

We will now state the Chebotarev Density Theorem.

Theorem 26 (Chebotarev Density Theorem)**.** *Let L/K be a Galois extension and let $\sigma \in \mathrm{Gal}(L/K)$. Denote by $\langle\sigma\rangle$ the conjugacy class of σ. Then the set*

$$S = \{\mathfrak{p} : \mathfrak{p} \text{ is a prime of } K \text{ unramified in } L \text{ and } \mathrm{Fr}_\mathfrak{p} = \langle\sigma\rangle\}$$

has density

$$\delta(S) = \frac{|\langle\sigma\rangle|}{[L:K]} = \frac{|\langle\sigma\rangle|}{|\mathrm{Gal(L/K)}|}.$$

In particular, S is infinite for every choice of σ.

For a proof of this theorem, see for example [10] (see Chapter VIII, §4).

Note that if we set $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_k)$, we get Dirichlet's Theorem (Since then the extension is abelian so the primes belonging to a particular conjugacy class $\langle\ell\rangle$ are exactly those which are $\equiv \ell \pmod{k}$).

The following corollary will be important for us:

Corollary 27. *Let K be an algebraic number field and $k \in \mathbb{N}$. Then for any $\sigma \in \mathrm{Gal}(K(\zeta_k)/K)$ there are infinitely many primes $\mathfrak{p}$ in K which are unramified in $K(\zeta_k)$, have inertia degree 1 over $\mathbb{Q}$ and satisfy $\mathrm{Fr}_\mathfrak{p} = \sigma$.*

Proof. Choose an arbitrary $\sigma \in \mathrm{Gal}(K(\zeta_k)/K)$. The extension $K(\zeta_k)/K$ is abelian, therefore by the Chebotarev Density Theorem, the set of primes $\mathfrak{p}$ in K which are unramified in $K(\zeta_k)$ and such that $\mathrm{Fr}_\mathfrak{p} = \sigma$ has positive density. By Lemma 25 and the remark after this Lemma, we can add the condition on the inertia degree over $\mathbb{Q}$. □

4. Necessity of the condition $\ell^2 \equiv 1 \pmod{k}$

The fact that there is no Euclidean proof of Dirichlet Theorem in the case when $\ell^2 \neq 1 \pmod{k}$ was first proved by Murty in 1988. In our proof, we are going to follow Conrad's paper [5].

As we have already noted in the second chapter, our goal will be to show that the classes modulo k in $P(f)$ form a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$. Strictly speaking, this is of course not true, because there are still finitely many exceptions. Therefore we will work with the sets defined below.

Definition 28. *Let K be an algebraic number field and h a polynomial with integer coefficients. By $P(K)$ we denote the set of rational primes which have a first degree prime ideal factor in K. If $k \in \mathbb{N}$, let*

$$P(k,h) := \{a \bmod k : p \equiv a \bmod k \text{ for infinitely many } p \in P(h)\},$$

$$P(k,K) := \{a \bmod k : p \equiv a \bmod k \text{ for infinitely many } p \in P(K)\}.$$

With this notation we have already seen that if $h \in \mathbb{Z}[x]$ is irreducible with a root α, then $P(\mathbb{Q}(\alpha))$ differs from $P(h)$ with at most finitely many exceptions so $P(k,h) = P(k,\mathbb{Q}(\alpha))$ without exceptions.

We would now like to prove that $P(k,f)$ is a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$. By the remark above we can translate this into the language of number fields and prove that it holds for $P(k,\mathbb{Q}(\alpha))$, where α is a root of f. We will begin with a lemma which characterizes the residue classes in $P(k,K)$.

Lemma 29. *Let K be an algebraic number field and $k \in \mathbb{N}$. Then*

$$P(k,K) = \{q \bmod k : q \in P(K),\ q \text{ unramified in } K(\zeta_k)\}.$$

Proof. We are going to prove two inclusions.

$\subseteq$: Let us choose an arbitrary $q \in P(k,K)$. Then q has infinitely many representatives in $P(K)$, therefore (because there are only finitely many ramified primes) it has infinitely many unramified representatives. Therefore the left hand side is contained in the right side.

$\supseteq$: Now choose arbitrary $q \in P(K)$ which is unramified in $K(\zeta_k)$. We need to find infinitely many primes $p \equiv q \pmod{k}$ which lie in $P(K)$. Because $q \in P(K)$, there is a prime ideal $\mathfrak{q} \mid q$ in K which has inertia degree one over $\mathbb{Q}$. Since q is unramified in $K(\zeta_k)$, so is $\mathfrak{q}$. Let σ be the Frobenius element of $\mathfrak{q}$ in $\mathrm{Gal}(K(\zeta_k)/K)$. Then by Lemma 22, $\sigma\restriction_{\mathbb{Q}(\zeta_k)} = q \bmod k$ (after the identification of $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ with $(\mathbb{Z}/k\mathbb{Z})^\times$). By Corollary 27, there are infinitely many prime ideals $\mathfrak{p}$ in K unramified over $K(\zeta_k)$ of inertia degree 1 over $\mathbb{Q}$ whose Frobenius element is σ. For such $\mathfrak{p}$, find the prime number p such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$, then $p \in P(K)$ (because we chose only primes of inertia degree 1) and Lemma 22 again implies that $\sigma(\zeta_k) = \zeta_k^{p \bmod k}$. Combining this equality with the definition of σ, we get that $p \equiv q \pmod{k}$. Since there are infinitely many $\mathfrak{p}$, each of them gives us a rational prime p we are looking for and a particular p can be received from at most $[K:\mathbb{Q}]$ different prime ideals $\mathfrak{p}$, there are infinitely many prime numbers p having the required properties. □

The second inclusion from this lemma is basically what we needed to proof in Theorem 18, except that now we used the Chebotarev Density Theorem which gave us what we needed. Note that the equality of the sets tells us something interesting about the prime divisors of a polynomial f – it tells us that if we find a prime divisor in $P(f)$ which is congruent to some a modulo k such that $(a,k)=1$, then there are infinitely many prime divisors of f which are $\equiv a \pmod{k}$.

This theorem can therefore be thought of as a generalization of Dirichlet's Theorem to prime divisors of polynomials. It is important that we speak about the prime *divisors* and not prime values, since the problem whether a polynomial of degree greater than 1 attains infinitely many prime values is very hard and still open.

We are now ready to prove the key theorem.

Theorem 30. *Let K be an algebraic number field and $k \in \mathbb{N}$. Then $P(k,K)$ is a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$. It is the image of the homomorphism*

$$\begin{aligned} \mathrm{Gal}(K(\zeta_k)/K) &\to \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q}) \\ \sigma &\mapsto \sigma\restriction_{\mathbb{Q}(\zeta_k)} . \end{aligned}$$

Proof. Let H be the image from the statement of the theorem. We want to prove that $H = P(k,K)$, we will do this by showing the two inclusions.

$P(k,K) \subseteq H$: Pick an arbitrary congruence class $a \in P(k,K)$. Then by Lemma 29, there is some $q \in P(K)$ which is unramified over $K(\zeta_k)$ and satisfies $q \equiv a \pmod{k}$. Denote by $\mathfrak{q}$ a first degree prime ideal factor of q in K. Then $\mathfrak{q}$ is also unramified over $K(\zeta_k)$ so we can let $\sigma := \mathrm{Fr}_{\mathfrak{q}}(K(\zeta_k)/K)$. Then by Lemma 22, $\sigma\restriction_{\mathbb{Q}(\zeta_k)} = q \bmod k = a$ (again after the identification of $(\mathbb{Z}/k\mathbb{Z})^\times$ with $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$). Therefore $a \in H$, so $P(k,K) \subset H$.

$H \subseteq P(k,K)$: For the other inclusion, let $b \in H$. Then there exists some $\sigma \in \mathrm{Gal}(K(\zeta_k)/K)$ such that $\sigma\restriction_{\mathbb{Q}(\zeta_k)} = b$. By the Chebotarev Density Theorem, there are infinitely many prime ideals $\mathfrak{p}$ in K which have inertia degree over $\mathbb{Q}$ equal to one. For such $\mathfrak{p}$, let p be the prime number such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Then $p \in P(K)$ and $b = \sigma\restriction_{\mathbb{Q}(\zeta_k)} = N(\mathfrak{p}) \bmod k = p \bmod k$, where the last equality holds because $f_{\mathfrak{p}|p} = 1$. Since there are infinitely many such prime ideals $\mathfrak{p}$, each of them gives us a rational prime p and a particular p can be obtained from at most $[K:\mathbb{Q}]$ different prime ideals $\mathfrak{p}$, there are infinitely many rational primes $p \in P(K)$ which are $\equiv b$ modulo k. Hence $b \in P(k,K)$ and since $b \in H$ was arbitrary, $H \subset P(k,K)$. □

It is now easy to show that Euclidean proof of Dirichlet's Theorem for the progression $a_n = kn + \ell$ exists if and only if $\ell^2 \equiv 1 \pmod{k}$. The precise statement of the second implication is as follows:

Theorem 31. *Let f be a polynomial with integer coefficients for which there exists some integers k, ℓ such that with finitely many exceptions, all prime divisors of f are $\equiv 1$ or ℓ mod k and infinitely many of these prime divisors are $\equiv \ell \pmod{k}$. Then $\ell^2 \equiv 1 \pmod{k}$.*

Proof. If f is irreducible, let α be a root of f. We can now apply Theorem 30 for $K = \mathbb{Q}(\alpha)$. Because we know that $P(k,K) = P(k,f) = \{1, \ell\}$ is a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$, the only option is that $\ell^2 \equiv 1 \pmod{k}$.

If f is not irreducible, write $f = f_1 \cdots f_n$ as a factor of irreducible polynomials. Because f has infinitely many prime divisors congruent to ℓ modulo k and $P(f) = P(f_1) \cup \cdots \cup P(f_n)$, one of the f_i must also have infinitely many prime divisors which are $\equiv \ell$ modulo k, WLOG assume for f_1. Then it suffices to use the first part of the proof for the polynomial f_1. $\square$

Bibliography

[1] M. Ram Murty, N. Thain *Prime Numbers in Certain Arithmetic Progressions*, Functiones et Approximatio XXXV (2006), 249 – 259

[2] J. Esmonde, M. Ram Murty, *Problems in Algebraic Number Theory*, Springer-Verlag, 1999, ISBN 0-387-98617-0

[3] J. O. Turner, *An Exposition of Dirichlet's Theorem*, 2013, https://etd.ohiolink.edu/rws_etd/document/get/osu1366202528/inline

[4] J. Jönsonn, *On Special Cases of Dirichlet's Theorem on Arithmetic Progressions*, 2015, http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=5042097&fileOId=5042100

[5] K. Conrad, *expository paper on Euclidean proofs of Dirichlet's theorem*, http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/dirichleteuclid.pdf

[6] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*, John Wiley & Sons, Inc., 1989, ISBN 0-471-50654-0

[7] A. Drápal, *course notes from Number Theory and RSA* (czech), http://www.karlin.mff.cuni.cz/~drapal/teorie_cisel.pdf

[8] J.S. Milne, *course notes on Fields and Galois Theory*, http://www.jmilne.org/math/CourseNotes/ft.html

[9] J.S. Milne, *course notes on Algebraic Number Theory*, http://www.jmilne.org/math/CourseNotes/ant.html

[10] S. Lang, *Algebraic Number Theory*, Second Edition, Springer-Verlag, 1994, ISBN 0-387-94225-4