# EUCLIDEAN STYLE PROOF OF DIRICHLET'S THEOREM

SREERUPA BHATTACHARJEE, KIN MING TSANG

ABSTRACT. This article deals with the elementary Euclidean proof of the Dirichlet's Theorem regarding infinitude of primes in arithmetic progressions. We start by giving the notion of a Euclidean proof and providing an example of such a proof for the arithmetic progression $\equiv 3 \pmod 4$. We construct a general "Euclidean Polynomial" and show that it always exists for arithmetic progressions satisfying certain properties.

## 1. INTRODUCTION

Euclid is credited with the formulation of the first proof of the infinitude of primes. Euclid's proof assumes that there are finitely many primes, and denotes these primes by $p_1, p_2, \dots p_r$, for some finite $r$. It is trivial to see that the number $Q = \prod_{i=1}^{r} p_i + 1$ is not divisible by any of the primes $p_1, \dots p_r$, and hence it must either be a prime itself or be divisible by some prime not in the list $p_1, p_2 \dots, p_r$. This contradiction forces an infinitude of prime numbers, provided that there is at least one.

Dirichlet's theorem in 1837, which concerns the infinitude of primes in arithmetic progression, can be considered an extension of Euclid's Theorem, and can be stated as follows:

**Theorem 1.1.** ***(Dirichlet**, 1837) For any $l, k$ satisfying the condition $gcd(l, k) = 1$, there are infinitely many primes $p$ such that $p \equiv l \pmod k$. Equivalently, every arithmetic progression of the form $a_n = kn + l$ for coprime $k, l$ contains infinitely many prime numbers.*

Although Dirichlet's original proof uses $L$-functions and analytic methods, for certain arithmetic progressions, Dirichlet's Theorem can be proved with arguments similar to the one used in Euclid's proof. We begin by defining the concept of a "Euclidean proof" :

**Definition 1.2.** Dirichlet's theorem is said to admit a Euclidean Proof for $l \pmod k$, if there exists a non-constant polynomial $f \in \mathbb{Z}[x]$ such that,( with finitely many exceptions), when a prime $p \mid f(n)$ for some $n \in \mathbb{Z}$, then $p \equiv 1 \pmod k$ or $p \equiv l \pmod k$ and infinitely many primes of the latter type occur. We call the polynomial $f$ a Euclidean polynomial for $l \pmod k$.

**Example 1.3.** We assume that there are only finitely many primes of $3 \pmod 4$, say $p_1, \dots, p_k$. Consider the polynomial $f(x) = 4x - 1$. Let $n = p_1 \cdots p_k$. Then $f(n) = 4(p_1 \cdots p_k) - 1$ has prime factors $\equiv 1$ or $3 \pmod 4$ since it is odd. It cannot have all prime factors $\equiv 1 \pmod 4$ otherwise $f(n) \equiv 1 \pmod 4$, which is clearly not the case.

This implies there exists $p \mid f(n)$ and $p \equiv 3 \pmod 4$. Our choice of $n$ ensures that $p \neq p_1, \dots, p_k$. We have found a new prime $p \equiv 3 \pmod 4$ which contradicts to our assumption. This proves an infinitude of primes of $3 \pmod 4$ provided there is at least one.

It is only possible to provide Euclidean proofs to Dirichlet's Theorem for certain restricted classes of arithmetic progressions. The following theorems yield a method to characterize the exhaustive set of arithmetic progressions for which such a proof exists :

**Theorem 1.4.** *(**Schur**, 1912) [6] If $l^2 \equiv 1 \pmod{k}$, for $l$, and $k$ as defined above, then a Euclidean polynomial for $l \pmod{k}$ exists.*

**Theorem 1.5.** *(**Murty**, 1988) [2] If there is a Euclidean polynomial for $l \pmod{k}$, then $l^2 \equiv 1 \pmod{k}$.*

Our aim in this article is to provide a detailed proof of Theorem 1.4 along with certain prerequisite theorems about prime divisors of polynomials, which are required to motivate the construction of a Euclidean polynomial.

## 2. Definitions

We begin by providing certain definitions which are necessary for proving our main result :

**Definition 2.1.** Let $f \in \mathbb{Z}[x]$ be a polynomial. A rational prime $p$ is a prime divisor of $f$ if $p \mid f(n)$ for some $n \in \mathbb{Z}$. We shall denote by $P(f)$ the set of prime divisors of $f$.

Since the proof of Theorem 1.4 largely uses Galois Theory and algebraic number theory, the remainder of this section will be majorly concerned with gathering the necessary concepts in those topics that we are going to use throughout the article :

**Definition 2.2.** For a field extension $L/K$, the Galois group $\mathrm{Gal}(L/K)$ is the group of all automorphisms of $L$ which fixes $K$. The field extension is called Galois if $|\mathrm{Gal}(L/K)| = [L : K]$. We say that the extension $L/K$ is abelian if it is Galois and the Galois group $\mathrm{Gal}(L/K)$ is abelian.

The Primitive Element Theorem states that if $L/K$ is an extension of number fields which has finite degree, then there exists $\alpha \in L$ such that $L = K(\alpha)$.

If $f \in K[x]$ is an irreducible polynomial and $L$ is the splitting field of $f$, then for every root $\alpha$ 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 $f$.

**Theorem 2.3** (Fundamental Theorem of Galois Theory)**.** *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*

$$\varphi : \{H : H \subset \mathrm{Gal}(L/K)\} \to \{M : K \subset M \subset L\}$$
$$H \mapsto L^H,$$

*where $L^H = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in H\}$ is fixed field of $H$. Moreover, such bijection is inclusion-reversing.*

**Definition 2.4.** For $k \in \mathbb{N}$, we define the $k$-th cyclotomic polynomial $\Phi_k$ as

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

where $\zeta_k$ is the primitive $k$-th root of unity in $\mathbb{C}$.

The field $K := \mathbb{Q}(\zeta_k)$ is Galois over $\mathbb{Q}$ with Galois group isomorphic to the group of coprime residue classes modulo $k$, which is denoted by $(\mathbb{Z}/k\mathbb{Z})^\times$.

**Definition 2.5.** 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 can be proved that $\mathcal{O}_K$ is indeed a ring.

**Definition 2.6.** For $A, B$ ideals in $\mathcal{O}_K$, we say that $A$ divides $B$ and denote it $A \mid B$ if $B \subset A$.

**Definition 2.7.** Let $f$ be an irreducible polynomial over $\mathbb{Q}$ and let $K$ be its splitting field. If $f = (x - \alpha_1) \cdots (x - \alpha_n)$ is the factorization of $f$ in $K[x]$, we define the discriminant of $f$ as $D(f) = \prod_{i \neq j}(\alpha_i - \alpha_j)$.

The discriminant of a polynomial with integer coefficients is an integer. For a cyclotomic extension $K = Q(\zeta_k)$ and $\mathcal{O}_K = \mathbb{Z}[\zeta_k]$, if a prime number $p$ divides $D(\Phi_k)$, then $p$ divides $k$.

## 3. Euclidean Proof and construction of the Euclidean Polynomial

The first requirement of a Euclidean proof is the existence of a Euclidean polynomial with infinitely many prime divisors. It is not obvious that a polynomial has infinitely many prime divisors and the following theorem provides a proof of this fact:

**Theorem 3.1.** ***(Schur)*** *If $f \in \mathbb{Z}[x]$ is non-constant, then $P(f)$ is infinite.*

*Proof.* Write $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. If $a_0 = 0$, we have $f(p) = a_n p^n + \cdots + a_1 p$ and hence $p \mid f(p)$. Suppose $a_0 \neq 0$. Now, $f(x) = \pm 1$ has only finitely many solutions, so $P(f)$ is non-empty. Suppose $P(f)$ is finite, say $P(f) = \{p_1, p_2, \ldots, p_k\}$ and let $Q = p_1 p_2 \ldots p_k$. Then $f(Qa_0 x) = a_0 g(x)$ for some polynomial $g \in \mathbb{Z}[x]$ of the form $1 + c_1 x + \cdots + c_n x^n$ with $Q \mid c_i$ for each $i$. Note that $p_i \notin P(g)$ for each $i$ from our construction of $g$. Also, $p \mid g$ implies that $p \mid f$, i.e. $P(g) \subset P(f)$. By the exact argument as above, $P(g)$ is non-empty. That means there exists some prime $p \in P(g)$ where $p \neq p_i$ for any $i$ and $p \in P(f)$, which is a contradiction. □

**Theorem 3.2.** ***(Nagell)*** *[5] If $f, g \in \mathbb{Z}[x]$ are non-constant, then $P(f) \cap P(g)$ is infinite.*

Using the properties of prime divisors of polynomials, and basic algebraic number theory, we can now start to construct the notion of a Euclidean Polynomial.

**Theorem 3.3.** *Let $H$ be a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$. Then there is an irreducible polynomial $f$ so that all of the prime divisors of $f$, with a finite number of exceptions, belong to the residue classes of $H$.*

*Proof.* By Primitive Element Theorem, there exists $\eta = h(\zeta_k)$ for some $h \in \mathbb{Z}[x]$ such that $\mathbb{Q}(\eta)$ be the fixed field of $H$. Let $m_1, \ldots, m_s$ be coset representatives of $H$ in $(\mathbb{Z}/k\mathbb{Z})^\times$, where $s = [(\mathbb{Z}/k\mathbb{Z})^\times : H]$. Set $\eta_i = h(\zeta_k^{m_i})$ for $1 \leq i \leq s$. Suppose these are not distinct. Let $\sigma_n \in \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ given by $\sigma_n : \zeta_k \mapsto \zeta_k^n$. Then $\sigma_{m_i}(\eta) = \sigma_{m_j}(\eta)$ for some distinct coset representatives $m_i, m_j$ of $H$. But then $\sigma_{m_i m_j^{-1}}(\eta) = \eta$ so $m_i m_j^{-1}$ fixes $\mathbb{Q}(\eta)$ which implies that $m_i$ and $m_j$ are in the same coset of $H$. A contradiction.

Thus $\eta_i = h(\zeta_k^{m_i})$, $1 \leq i \leq s$, are the distinct conjugates of $\eta$. Note that

$$f(x) = \prod_{i=1}^{s}(x - \eta_i).$$

is the minimal polynomial of $\eta_i$ over $\mathbb{Q}$ with integer coefficients. We will show that $f$ satisfies the conditions in the theorem.

Let $p \in P(f)$ so that $p \nmid k$ and so that $p \nmid D(f)$. Since $p \in P(f)$, there exists $a \in \mathbb{Z}$ such that

$$f(a) = \prod_{i=1}^{s}(a - \eta_i) \equiv 0 \pmod{p}.$$

Let $\mathfrak{p}$ be any prime ideal in $\mathcal{O}_{\mathbb{Q}(\eta)}$ dividing $(p)$. Then $(a-\eta_i) \in \mathfrak{p}$ for some $i$. On the other hand, $a^p \equiv a \pmod{p}$, so $a^p \equiv a \pmod{\mathfrak{p}}$. Similarly, $h(x)^p \equiv h(x^p) \pmod{\mathfrak{p}}$. Thus, we get the following congruence:

$$h(\zeta_k^{m_i}) \equiv \eta_i \equiv a \equiv a^p \equiv \eta_i^p \equiv h(\zeta_k^{m_i})^p \equiv h(\zeta_k^{pm_i}) \pmod{\mathfrak{p}}$$

In particular, we see that $(h(\zeta_k^{m_i}) - h(\zeta_k^{pm_i})) \in \mathfrak{p}$. Now, since $p \nmid k$, we have that $pm_i$ is coprime to $k$, so $h(\zeta_k^{pm_i})$ is one of the $\eta_1, \ldots, \eta_s$. Suppose $h(\zeta_k^{pm_i}) \neq h(\zeta_k^{m_i})$. WLOG, say $h(\zeta_k^{pm_i}) = \eta_j$ with $j \neq i$. Then $h(\zeta_k^{m_i}) - h(\zeta_k^{pm_i}) = \eta_i - \eta_j$ is a factor of $D(f)$. Then $D(f) \in \mathfrak{p}$ and since $D(f)$ is a rational integer, $p \mid D(f)$. This contradicts our choice of $p$. Thus, $h(\zeta_k^{pm_i}) = h(\zeta_k^{m_i})$ and so $\eta_i$ is fixed by the automorphism $\sigma_p$. So $\sigma_p$ fixes $\mathbb{Q}(\eta_i)$. Recall that $\mathbb{Q}(\eta_i)$ is a Galois extension and $\mathbb{Q}(\eta_i) = \mathbb{Q}(\eta)$. Thus $\sigma_p$ fixes $\mathbb{Q}(\eta)$ and so $p$ belongs to a residue class of $H$. □

The converse of Theorem 3.3 can be stated as follows:

**Theorem 3.4.** *If $f$ is as in Theorem 3.3, then any prime belonging to any residue class of $H$ divides $f$.*

*Proof.* Let $p$ be a prime belonging to some residue class of $H$. $\sigma_p$ fixes $\mathbb{Q}(\eta)$, in particular,

$$\eta^p \equiv h(\zeta_k)^p \equiv h(\zeta_k^p) \equiv h(\zeta_k) \equiv \eta \pmod{p}.$$

Hence, for any prime ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{Q}(\eta)}$ dividing $p$, we have $\eta^p \equiv \eta \pmod{\mathfrak{p}}$. Since $\mathcal{O}_{\mathbb{Q}(\eta)}$ is a Dedekind domain, $\mathcal{O}_K/\mathfrak{p}$ is a field and so there are at most $p$ solutions to $x^p - x$ in this field. From this, it follows that $\eta \equiv a \pmod{\mathfrak{p}}$ for some rational integer $a$. Thus, $f(a) \in \mathfrak{p}$ and since $f(a)$ is a rational integer, it follows that $p \mid f(a)$ as desired. □

**Corollary 3.5.** *If $\Phi_k$ is the $k$-th cyclotomic polynomial, then all of the prime divisors of $\Phi_k$ are $\equiv 1 \pmod{k}$ or divide $k$.*

*Proof.* This result follows from setting $H = \{1\}$ in Theorem 3.3 and the fact that the only primes which divide the discriminant of $\Phi_k$ are those primes which divide $k$. Since all the prime divisors of $\Phi_k$, with a finite number of exceptions, belong to the residue classes of $H$, all of the prime divisors of $\Phi_k$ are $\equiv 1 \pmod{k}$ or divide $k$ □

We are now finally able to prove the main result of this article Theorem 1.4, restated as follows:

**Theorem.** *If $l^2 \equiv 1 \pmod{k}$, then there are infinitely many primes $\equiv l \pmod{k}$ provided there is at least one such prime.*

*Proof.* We begin by noting that $k$ has only finitely many prime factors. So all of the prime divisors of $\Phi_k$ with the exception of finitely many are $\equiv 1 \pmod{k}$. Since we know from Theorem 3.1 that $\Phi_k$ has infinitely many prime divisors, we can claim that there exists infinitely many primes $\equiv 1 \pmod{k}$ for any positive integer $k$.

Since we have already proved the infinitude of primes $\equiv 1 \pmod{k}$, we can now assume that $l$ is not congruent to $1 \pmod{k}$. We consider the subgroup $H$ of $(\mathbb{Z}/k\mathbb{Z})^\times$ generated as follows: $H = \{1, l\}$. We assume $L$ to be the fixed field of $H$ and then define $h(x) = (u-x)(u-x^l)$, for some $u \in \mathbb{Z}$, where $u$ will be determined later. Let $m_1, \ldots, m_s$ denote the coset representatives of $H$ in $(\mathbb{Z}/k\mathbb{Z})^\times$, and let $u \in \mathbb{Z}$ be chosen such that $h(\zeta_k^{m_i})$ are distinct for $i = i, \ldots, s$, then $L = \mathbb{Q}(h(\zeta_k))$. To see this, suppose that $\sigma_j \in \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ which fixes $h(\zeta_k)$ and $\sigma_j \neq \sigma_1, \sigma_l$. Then, $h(\zeta_k) = \sigma_j(h(\zeta_k)) = (u-\zeta_k^j)(u-\zeta_k^{jl}) = h(\zeta_k^j)$. Since we choose $u$ such that $h(\zeta_k^{m_i})$ are

distinct, we have $j = 1$ or $l$. Hence, the fix automorphisms of $\mathbb{Q}(h(\zeta_k))$ are exactly $\sigma_1$ and $\sigma_l$. Note that there are also infinitely many $u \in \mathbb{Z}$ satisfying the condition.

If we apply Theorem 3.3 to $H$, with $\eta = h(\zeta_k)$, we get a polynomial $f(x)$, all of whose prime divisors (apart from finitely many) are $\equiv 1$ or $l \pmod{k}$. If we write $f$ explicitly, we get

$$f(x)^2 = \prod_{(a,k)=1} (x - (u - \zeta_k^a)(u - \zeta_k^{la})).$$

We note that $f(0) = (-1)^{\varphi(k)}\Phi_k(u)$, where $\varphi$ is the Euler totient function. We now choose $u$ to be a non-zero multiple of $k$, then $f(0) = \Phi_k(u) \equiv (-1)^{\varphi(k)} \pmod{k}$ by Corollary 3.5. We define $g = (-1)^{\varphi(k)} f$, so that at each point, $g$ has the same prime divisors as $f$ and $g(0) \equiv 1 \pmod{k}$.

By assumption, there exists $p \equiv l \pmod{k}$. Then, $p \nmid D(g)$, otherwise it has to divide $k$. By Theorem 3.4, we can find $b \in \mathbb{Z}$ such that $p \mid g(b)$. We are able to choose $b$ such that $p^2 \nmid g(b)$. If $p^2 \mid g(b)$, then $g(b + p) = g(b) + pg'(b) \equiv pg'(b) \pmod{p^2}$. But since $p \nmid D(g)$, we can say that $g$ has no double roots $\pmod{p}$ and therefore $g'(b) \not\equiv 0 \pmod{p}$. So $g(b) \equiv 0 \pmod{p^2}$ implies that $g(b + p) \not\equiv 0 \pmod{p^2}$. Thus, replacing $b$ by $b + p$ if necessary, we can find such $b$.

Now if we suppose there are finitely many primes $\equiv l \pmod{k}$, and denote them by $p_1, p_2, \ldots, p_m$. Also let $q_1, q_2 \ldots, q_t$ be the prime divisors of $D(g)$. We define $Q = p_1 p_2 \ldots p_m q_1 q_2 \ldots q_t$. By the Chinese Remainder Theorem, we can find $c$ so that

$$c \equiv b \pmod{p^2}$$
$$c \equiv 0 \pmod{kQ}$$

Thus $g(c) \equiv g(b) \pmod{p^2}$ and $g(c) \equiv g(0) \pmod{kQ}$. By Theorem 3.2, the only prime divisors of $g$ are those primes which divide $k$, or are $\equiv 1$ or $l \pmod{k}$. Since $g(0)$ is only divisible by those primes $\equiv 1 \pmod{k}$, it follows that $g(c)$ is only divisible by those primes $\equiv 1 \pmod{k}$ and $p \equiv l \pmod{k}$. Since $p^2 \nmid g(c)$, it follows that $g(c) \equiv l \pmod{k}$. But $g(c) = g(0) \equiv 1 \pmod{k}$ which is a contradiction. Thus there must be infinitely many primes $\equiv l \pmod{k}$. □

Theorem 1.5 is the converse of Theorem 1.4 and can be restated as follows :

**Theorem.** *Let $f \in \mathbb{Z}[x]$ . Suppose that with finitely many exceptions, all prime divisors of $f$ are either $\equiv 1$ or $l \pmod{k}$. Then $l^2 \equiv 1 \pmod{k}$.*

The Chebotarev Density Theorem is used to prove the above theorem, however we do not provide the proof in this article.

## REFERENCES


[1] K. Conrad. Euclidean proof of dirichlet's theorem. URL http://www.math.uconn.edu/kconrad/blurbs/dirichleteuclid.pdf.

[2] M. Ram Murty. Primes in certain arithmetic progressions. *J. Madras Univ.*, 51:161–169, 1988.

[3] M. Ram Murty. How I discovered Euclidean proofs. *Nieuw Arch. Wiskd. (5)*, 18(2):101–102, 2017.

[4] M. Ram Murty and Nithum Thain. Prime numbers in certain arithmetic progressions. *Funct. Approx. Comment. Math.*, 35:249–259, 2006.

[5] T. Nagell. Sur les diviseurs premiers des polynômes. *Acta Arith.*, 15:235–244, 1968/69.

[6] I. Schur. *Uber die existenz Unendlich Vieler primzahlen in einigen speziellen arithmetischen Progressionen*. 1912. URL https://books.google.ca/books?id=F3tdnQAACAAJ.