Euclidean Proofs of the Infinitude of Primes in Arithmetic Progressions

Leader: Joan Arenillas i Cases.
Writer: Guanzhong Yang.
December 2025

1. READING NOTES

1.1 Fundamental Ideas of Euclidean Proofs

The core idea of Euclid's proof is as follows: assume there are only finitely many primes in a certain arithmetic progression, then construct a number or a polynomial value that leads to a contradiction (i.e., find a prime not in the given list).

Here are some examples:
① For the progression 1(mod 4):
Use the polynomial $f(x) = 4x^2 + 1$. Suppose there are only finitely many primes $p_1, \ldots, p_k \equiv 1(\mathrm{mod}\ 4)$, and consider $N = f(p_1 \ldots p_k) = 4(p_1 \ldots p_k)^2 + 1$. Any prime divisor q of N satisfies $4x^2 \equiv -1(\mathrm{mod}\ q)$, meaning –1 is a quadratic residue modulo q, which implies $q \equiv 1(\mathrm{mod}\ 4)$. However, N is not divisible by any p_i, a contradiction.
② For the progression 3(mod 4):
Use the polynomial $g(x) = 4x - 1$. Suppose there are only finitely many primes $p_1, \ldots, p_k \equiv 3(\mathrm{mod}\ 4)$, and consider $M = g(p_1 \ldots p_k) = 4(p_1 \ldots p_k) - 1$. We have $M \equiv 3(mod\ 4)$, so M must have a prime divisor $q \equiv 3(mod\ 4)$ (because if all prime divisors were congruent to 1(mod 4), then $M \equiv 1(mod\ 4)$). But q is not in the given list, a contradiction.

In the paper, this is achieved by finding a polynomial $f(x) \in Z[x]$ such that all but finitely many prime divisors of $f(x)$ belong to the target progression $l(mod\ k)$.The construction in this paper is generalized to arbitrary k and l satisfying $l^2 \equiv 1(\mathrm{mod}\ k)$ by using cyclotomic fields and Galois theory.

1.2 Concepts of Groups, Fields and Field Extensions

(1) Group:
A set G equipped with a binary operation (e.g., addition or multiplication) that satisfies closure, associativity, the existence of an identity element, and the existence of an inverse element for each element.

Here are some examples:
① The set of integers Z forms a group under addition.
② The set of non-zero real numbers R^* forms a group under multiplication.

(2) Field:
A set F equipped with addition and multiplication that satisfies the properties of a commutative ring, and every non-zero element has a multiplicative inverse.

Here are some examples:
① The field of rational numbers Q.
② Finite fields $F_p = Z/pZ$ (where p is a prime number).

(3) Field Extension:
If K is a field extension of F, then $F \subseteq K$ and K forms a field over F.

Here are some examples:
① C is an extension of R.
② $Q(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in Q\}$ is an extension of Q.

In the paper, field extensions such as the cyclotomic field $Q(\zeta^k)$ (where ζ^k is a primitive k-th root of unity) are key.

1.3 Concepts of Galois Groups

In mathematics, the notation K/F denotes a field extension, where F is the base field and K is the extension field. This means F is a subfield of K (i.e., $F \subseteq K$) and K forms a field over F.

(1) Field Automorphism

A field automorphism of a field *K* is a bijection $\sigma: K \to K$ satisfying:

① preserving addition: $\sigma(a+b) = \sigma(a) + \sigma(b)$

② preserving multiplication: $\sigma(ab) = \sigma(a)\sigma(b)$

③ preserving the multiplicative identity: $\sigma(1) = 1$

Here are examples:

① Complex conjugation on the field of complex numbers C:

$$\sigma(a+bi) = a - bi.$$

② The identity map on the field of rational numbers

$$Q: \sigma(x) = x.$$

(2) $\mathbf{F}$-automorphism

For a field extension K/F, an F-automorphism is an automorphism of K that satisfies $\sigma(a) = a$ for all $a \in F$ (fixing the base field F).

(3) Galois Group

For a field extension K/F, its Galois group is defined as:

$$Gal(K/F) = \{\sigma: K \to K: \sigma \ is \ an \ F-automorphism\}$$

This set forms a group under the composition of mappings.

Here are examples:

① Quadratic extension $Q(\sqrt{2})/Q$:

Identity automorphism: $\sigma_1(a+b\sqrt{2}) = a + b\sqrt{2}$

Conjugation automorphism: $\sigma_2(a+b\sqrt{2}) = a - b\sqrt{2}$

Galois group: $Gal(Q(\sqrt{2})/Q) = \{\sigma_1, \sigma_2\}$

② Cyclotomic extension $Q(\zeta)/Q$, where $\zeta = e^{\frac{2\pi i}{3}}$

Identity automorphism: $\sigma_1(\zeta) = \zeta$

Conjugation automorphism: $\sigma_2(\zeta) = \zeta^2$

Galois group: $Gal(Q(\zeta)/Q) = \{\sigma_1, \sigma_2\}$

1.3 Concepts of Polynomials

(1) Discriminant of a Monic Polynomial

The discriminant of a monic polynomial $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ is given, in terms of its roots $\{r_1, r_2, \cdots, r_d\} \subset C$ (not necessarily distinct), by

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

(2) Prime Divisor of a Monic Polynomial

Let $f(x) \in Z[x]$ be a polynomial. We say that a prime number p is a prime divisor of f if there exists $m \in Z$ such that p divides $f(m)$.

(3) Algebraic Integer

A complex number α is called an algebraic integer if and only if there exists a monic polynomial with integer coefficients $f(x)$ such that $f(\alpha) = 0$.
If α and β are all algebraic integers, then $\alpha + \beta$, $\alpha\beta$, and $g(\alpha)$ where $g(x) \in Z[x]$ are all algebraic integers.

(4) (Primitive) Roots of Unity and Cyclotomic Polynomials

① Roots of Unity:

The roots of the equation $x^n = 1$. A primitive n-th root of unity is a root ζ satisfying $\zeta^n = 1$ but $\zeta^k \neq 1$ for all $0 < k < n$.

② Cyclotomic Polynomial:

The n-th cyclotomic polynomial $\Phi_n(x)$ is the minimal polynomial with integer coefficients whose roots are all primitive n-th roots of unity.

2. FINAL POSTER

Euclidean Proof of the Infinitude of Primes of the form $kn+l$

Abstract

Around 300 BC, Euclid proved that there are infinitely many prime numbers using the so-called “Euclidean method.” He assumed that there are only finitely many primes, then constructed a suitable polynomial $f(x) = x + 1$ by taking the product of these finitely many primes as an independent variable, which led to a contradiction. Today, we will focus on primes of the form $kn + l$ where k and l are fixed positive integers, $l^2 \equiv 1 \ mod \ k$ and $n \in N$, and provide you with a general proof of the infinitude of such primes using the Euclidean method.

Auxiliary Result

Definition 1.1

Let $H = \{1, l \mid l^2 \equiv 1 \ mod \ k\}$ be a subgroup of $G = (Z/kZ)^* = \{a \in Z/kZ \mid gcd(k, a) = 1\}$. By Coset Decomposition Theorem, we can always find the left transversal $S = \{a_i \mid a_i \in G\}$ of H in G, such that $\bigcup_{a_i \in S} a_i H = G$ and $a_i H \cap a_j H = \emptyset$ for $a_i \neq a_j$.

Proof. To prove Coset Decomposition Theorem, we need to show that, for a_i, $a_j \in G$, if $a \in a_i H \cap a_j H$, then $a_i H = a_j H$.
Thus, we assume there exists h_u, $h_v \in H$, $a = a_i h_u = a_j h_v$:

$$a_i = a_j h_v h_u^{-1},$$
$$a_i h = a_j h_v h_u^{-1} h \text{ for any } h \in H,$$
$$a_i H = a_j H \text{ since } h_v h_u^{-1} h \in H.$$

Lemma 2.1

For $H = \{1, l \mid l^2 \equiv 1 \ mod \ k\}$, $G = (Z/kZ)^*$, and left transversal S of H in G, the coefficients of polynomial

$f(x) = \prod_{s \in S} (x - h(\zeta^s))$, where $\zeta = e^{\frac{2\pi i}{k}}$, $h(\zeta^s) = (\zeta^s - k)(k - \zeta^{sl})$, are all integers.

Proof. To obtain the desired conclusion, we need to prove that the coefficients are algebraic integers and that they are rational numbers.

By definition of kth cyclotomic polynomial, ζ is an algebraic integer, and hence so is $h(\zeta^s)$ for $s \in S$. The coefficients of $f(x)$ are elementary symmetric polynomials in the $h(\zeta^s)$, therefore they are algebraic integers as well.

Let $\sigma \in Gal(\overline{Q}/Q)$, where $\overline{Q}$ is the algebraic closure of Q, then:
(1) σ permutes the primitive kth roots of unity since $\sigma(\zeta)$ also satisfies $\Phi_k(\sigma(\zeta)) = 0$.
(2) $\sigma(h(\zeta^s)) = h(\sigma(\zeta^s)) = h(\sigma(\zeta)^s)$ since $h(x)$ has rational coefficients.
(3) σ permutes the root set $\{h(\zeta^s) \mid s \in S\}$. This is because, from (2), σ maps a root $h(\zeta^s)$ to $h(\sigma(\zeta)^s)$. Since $\sigma(\zeta) = \zeta^a$ for some $a \in G$, and

$\bigcup_{a_i \in S} a_i H = G$ and $a_i H \cap a_j H = \emptyset$ for $a_i \neq a_j$, there exists some $s' \in S$ such that $\zeta^{as} = \zeta^{s'}$ or $\zeta^{ls'}$. Therefore $\sigma(h(\zeta^s)) = h(\zeta^{s'})$, which is another root.
Since the coefficients of $f(x)$ are just symmetric polynomials in the roots, and permuting the roots does not change its value, by Galois correspondence, the coefficients of $f(x)$ are rational.

Since the coefficients of $f(x)$ are rational and algebraic integers, they are integers.

Lemma 2.2
Pick a prime number p such that p does not divide the discriminant of a monic polynomial $\Delta(f)$. Then there exists an integer $b \in Z$ such that p divides $f(b)$, but p^2 does not divide $f(b)$.

Proof. We shall prove this lemma by contradiction.
Assume for all possible integers $b \in Z$ such that if p divides $f(b)$, p^2 divides $f(b)$ as well.
Then we can rewrite the monic polynomial using Taylor expansion around b:

$$f(b+x) = f(b) + f^{(1)}(b)x + \frac{f^{(2)}(b)}{2!}x^2 + \cdots \in Z[x].$$

In the case $x = p$, we have:

$$f(b+p) = f(b) + f^{(1)}(b)p + \frac{f^{(2)}(b)}{2!}p^2 + \cdots$$

Now, it follows that $f(b+p) \equiv f^{(1)}(b)p \ mod \ p^2$. Since p does not divide $\Delta(f)$, $f(x) \ mod \ p$ does not have double roots, and therefore $f^{(1)}(b) \not\equiv 0 \ mod \ p$, $f(b+p) \not\equiv 0 \ mod \ p^2$, leading to an contradiction.

Lemma 2.3 Chinese Remainder Theory
Let m_1, m_2 be positive integers such that $gcd(m_1, m_2) = 1$, then for any integers a_1, a_2, the system of congruences:

$$x \equiv a_1 \ mod \ m_1,$$
$$x \equiv a_2 \ mod \ m_2,$$

has a unique solution modulo $m_1 m_2$.

Proof. Since $gcd(m_1, m_2) = 1$, then there exist integers u, v such that $um_1 + vm_2 = 1$.
Then $x \equiv a_1 u m_1 + a_2 v m_2 \ mod \ m_1 m_2$.

Lemma 2.4
The following equality of polynomials holds:

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

Lemma 2.5
Given $H = \{1, l \mid l^2 \equiv 1 \ mod \ k\}$, $G = (Z/kZ)^*$, left transversal S of H in G and polynomial

$f(x) = \prod_{s \in S} (x - h(\zeta^s))$, where $\zeta = e^{\frac{2\pi i}{k}}$, $h(\zeta^s) = (\zeta^s - k)(k - \zeta^{sl})$, $k > 2$

then the equality $f(0) = \Phi_k(k)$ holds, and every prime divisor of $\Phi_k(x)$ is $\equiv 1 \bmod k$.

Proof. Notice that

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

Since the kth cyclotomic polynomial is defined by

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

it is clear that $f(0) = \Phi_k(k)$. The equality also works under mod k:

$$f(0) = \prod_{a \in G} (k - \zeta^a) \equiv (-1)^{\varphi(k)} \prod_{a \in G} \zeta^a = \prod_{a \in G} \zeta^a = 1 \ mod \ k,$$

where we used the conclusion that Euler's function $\varphi(k)$ is always even for $k > 2$, and the last equality comes from the fact that the product goes over all kth primitive roots of unity can be grouped in complex-conjugate pairs.

Proof

For the case of $k = 1,2$ or $l = 1$, the proofs are quiet straightforwards. Therefore, we will mainly focus on other cases in the following proof.

For any given pairs of (k, l), where $l^2 \equiv 1 \ mod \ k$, $k > 2$, $l \neq 1$, we can find corresponding H and S. Now, consider polynomial

$f(x) = \prod_{s \in S} (x - h(\zeta^s))$, where $\zeta = e^{\frac{2\pi i}{k}}$, $h(\zeta^s) = (\zeta^s - k)(k - \zeta^{sl})$, whose coefficients are integers by Lemma 2.1, and assume that the discriminant of $f(x)$ can be factorised as

$$\Delta(f) = \prod_i q_i^{a_i}, \text{ where } q_i \text{ is a prime.}$$

This polynomial has several beautiful properties that will be essential for our proof, which will be presented later.

Now we start to prove the conclusion using the Euclidean method.
Suppose that there are finitely many primes in the $\text{form of } kn + l$, and denote them by $p_1 < \cdots < p_m$. Now, we define $Q = \prod_i q_i \prod_{j \neq h} p_j$, where p_h is a selected prime that does not divide $\Delta(f)$. We will discuss the choice of p_h further in the Afterword.
Consider the following congruence equation system:

$$c \equiv A \ mod \ p_h^2,$$
$$c \equiv 0 \ mod \ kQ,$$

where p_h divides $f(A)$ but p_h^2 does not divide $f(A)$, and such an A always exists by Lemma 2.2.
By Lemma 2.3, the Chinese Remainder Theorem guarantees the existence of $c \in Z$ that is a solution to the above system since $gcd(p_h^2, kQ) = 1$. It follows that:

$$f(c) \equiv f(A) \ mod \ p_h^2,$$
$$f(c) \equiv f(0) \ mod \ kQ,$$

Next, we want to prove that, if p is a prime divisor of f, then either p belong to T, where

$$T = \{q_1, q_2, \cdots, u_1, u_2, \cdots\}, k = \prod_i u_i^{b_i}, \text{ and } u_i \text{ is a prime,}$$

or $p \equiv 1, \ l \ mod \ k$.

Suppose p is a prime divisor of f such that p does not belong to T, consider a field F containing both the finite field F_p and ζ. Since p divides f, working in F, there exists $a \in Z$ such that $f(a) = \prod_{s \in S} (a - h(\zeta^s)) \equiv 0$ under F.
So in F, for some $s \in S$, $a = h(\zeta^s)$.
Since we want to determine the relationship of $p \ mod \ k$, we need to find an equality involving $h(\zeta^{ps})$ under $Q(\zeta)$.

We first observe that the equality $h(\zeta^s) = h(\zeta^{ps})$ holds in F, because

$$h(\zeta^s) = a = a^p = (h(\zeta^s))^p = (\zeta^s - k)^p (k - \zeta^{sl})^p$$
$$= (\zeta^{ps} - k^p)(k^p - \zeta^{psl}) = (\zeta^{ps} - k)(k - \zeta^{psl}) = h(\zeta^{ps}),$$

where we have used Fermat little theorem and the fact that F has characteristic p(so that $(c + d)^p = c^p + d^p$ for all $c, d \in F$).

We can then show that $h(\zeta^{ps})$ is also a root of $f(x)$ in $Q(\zeta)$.
Notice that the value of $h(\zeta^{ps})$ only depends on the value of $ps \ mod \ k$ as it appears as an exponent of ζ. Since p does not divide k by definition and s is coprime to k, ps and $ps \ mod \ k$ are coprime to k.
There are now only two options: either $ps \bmod k$ belongs to S or $ps \bmod k$ does not belong to S. In the first case, $h(\zeta^{ps})$ is also a root of $f(x)$ in $Q(\zeta)$ by observing the expression of $f(x)$. In the latter case, by definition of left transversal S, there always exist $t \in S$ such that $ps \equiv lt \bmod k$, so $h(\zeta^{ps}) = h(\zeta^{lt}) = h(\zeta^t)$ is also a root of $f(x)$ in $Q(\zeta)$ because:

$$h(\zeta^{ps}) = h(\zeta^{lt}) = (\zeta^{lt} - k)(k - \zeta^{l^2 t}) = (\zeta^{lt} - k)(k - \zeta^t) = h(\zeta^t).$$

Thus, we can conclude that $h(\zeta^s)$ and $h(\zeta^{ps})$ are the same root of $f(x)$ in $Q(\zeta)$. Indeed, if we assume they are two distinct roots of $f(x)$ in $Q(\zeta)$, then $\Delta(f)$ would have to be divisible by p, which is impossible for our choice of p.

Therefore, we derive an equality involving $h(\zeta^{ps})$ under $Q(\zeta)$. The equality

$$h(\zeta^s) = (\zeta^s - k)(k - \zeta^{sl}) = (\zeta^{ps} - k)(k - \zeta^{psl}) = h(\zeta^{ps})$$

holds in $Q(\zeta)$. If we rewrite the above equality in terms of $\theta = \zeta^s$, we yield:

$$\theta^{1+l} - k\theta^l - k\theta = \theta^{p(1+l)} - k\theta^{pl} - k\theta^p,$$
$$\theta^{p(1+l)} - k\theta^{pl} - k\theta^p - \theta^{1+l} + k\theta^l + k\theta = 0.$$

If we replace θ by x, then the equality above in $Q(\theta)$ is equivalent to the condition

$$g(x) = x^{p(1+l)} - kx^{pl} - kx^{p} - x^{1+l} + kx^{l} + kx = 0$$

in $Q[x]/(\Phi_k(x)) \cong Q(\theta)$. Thus, the above equality is equivalent to $g(x)$ being a multiple of the kth cyclotomic polynomial by Lemma 2.4.

Using the idea behind the Euclidean method, we now aim to prove by contradiction that there are infinitely many primes of the form of $kn + l$. To do so, we assume that p is a prime divisor of $f(c)$ and use this assumption to derive a contradiction.

Suppose $p \not\equiv 1 \ mod \ k$ and $p \neq p_h$, then by assumptions, $p|kQ$. Thus, we deduce $f(0) \equiv f(c) \equiv 0 \ mod \ p$, meaning $p \equiv 1 \ mod \ k$ by Lemma 2.5, which is a contradiction. Thus, except for p_h, all the prime divisor divisors p of $f(c)$ satisfy $p \equiv 1 \ mod \ k$.

Simultaneously, since $f(c) \equiv f(A) \ mod \ p_h^2$, and p_h divides $f(A)$ yet p_h^2 does not divide $f(A)$, we could conclude that p_h divides $f(c)$ yet p_h^2 does not divide $f(c)$.

Therefore, if we factorised $f(c)$, $f(c) \equiv 1 \cdot 1 \cdot 1 \cdots l \equiv l \ mod \ k$. However, it is contradict to $p \equiv 1 \ mod \ k$, so other initial assumption, which is there are finite number of primes in the form of $kn + l$, is incorrect.

Afterword

This elegant Euclidean-style proof presented above relies crucially on the existence of a prime p_h satisfying:
(1) $p_h \equiv l \ mod \ k$.
(2) p_h does not divide $\Delta(f)$, where $\Delta(f)$ is the discriminant of the Euclidean polynomial f.
(3) p_h divides $f(A)$ but p_h^2 does not divide $f(A)$.

While in many cases such a prime can be found by inspection, there exist subtle counterexamples where the construction fails if all small primes congruent to $l \ mod \ k$ happen to divide $\Delta(f)$. A notable example occurs for $k = 15$, $l = 11$. In this case, $f(x) = x^4 + 884x^3 + 293206x^2 + 43243679x + 2392743361$, $\Delta(f) = 5^3 \cdot 11^2 \cdot 19^2 \cdot 41^2 \cdot 1091^2$. If both 11 and 41 divide $\Delta(f)$—which indeed happens for the polynomial $f(x)$ constructed—then no candidate p_h satisfying the second condition exists among the first few primes in the progression. This exposes a hidden dependency in the proof: the existence of a "good" primep_h is not guaranteed by elementary means alone; it implicitly assumes a weak form of Dirichlet's theorem.

To resolve this issue rigorously, one must invoke deeper results from analytic or algebraic number theory. For example, we may directly prove the conclusion using Dirichlet's Theorem, which states that there are infinitely many primes $\mathrm{p} \equiv \mathrm{l} \bmod \mathrm{k}$ whenever $\gcd(\mathrm{k}, \mathrm{l}) = 1$.

This observation does not diminish the value of the Euclidean framework but rather highlights its natural limitations. It also suggests interesting further questions: For which pairs (k, l) does $\Delta(f)$ share all small primes of the progression? Can one design an algorithmic criterion to detect such pathological cases? Such inquiries lie at the intersection of computational number theory and the study of polynomial discriminants.

Reference

[1] Joan, A. (2025). Demostracions euclidianes de la infinitud de primers en progressions aritmètiques. July
[2] Dirichlet, P. G. L. (1837). Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.