

EUCLIDEAN PROOFS OF DIRICHLET'S THEOREM

KEITH CONRAD

*It is rash to assert that a mathematical theorem cannot be proved in a particular way.*¹

Euclid's proof of the infinitude of the primes is a paragon of simplicity: given a finite list of primes, multiply them together and add one. The resulting number, say N , is not divisible by any prime on the list, so any prime factor of N is a new prime.

Some special cases of Dirichlet's theorem admit a simple proof following Euclid's model, such as the case of $1 \bmod 4$ or $5 \bmod 6$. (We mean by 'Dirichlet's theorem' only the assertion that a congruence class contains infinitely many primes, not the stronger assertion about the density of such primes.) One property that these Euclidean proofs of special cases of Dirichlet's theorem have in common is that they use a polynomial, varying from one case to the next, whose integer values have restricted prime factors.

Specifically, a Euclidean proof of Dirichlet's theorem for $a \bmod m$ involves, at the very least, the construction of a nonconstant polynomial $h(T) \in \mathbf{Z}[T]$ for which any prime factor p of any integer $h(n)$ satisfies, with finitely many exceptions, either $p \equiv 1 \bmod m$ or $p \equiv a \bmod m$, and infinitely many primes of the latter type occur.

Here are some cases where Euclidean proofs of Dirichlet's theorem exist.

- $1 \bmod d$: $p \mid \Phi_d(n)$ for some n implies $p \equiv 1 \bmod d$ or $p \mid 2d$. (The notation $\Phi_d(T)$ means the d th cyclotomic polynomial.)
- $3 \bmod 8$: $p \mid n^2 + 2$ for some n implies $p \equiv 1$ or $3 \bmod 8$, or $p = 2$.
- $4 \bmod 5$: $p \mid n^2 - 5$ for some n implies $p \equiv 1$ or $4 \bmod 5$, or $p = 5$.
- $6 \bmod 7$: $p \mid n^3 + n^2 - 2n - 1$ for some n implies $p \equiv 1$ or $6 \bmod 7$, or $p = 7$.
- $-1 \bmod d$: see [3].

Is there a Euclidean proof of Dirichlet's theorem for the congruence class $2 \bmod 5$? What we seek is a polynomial $h(T) \in \mathbf{Z}[T]$ such that all prime factors of all integers $h(n)$ are, with finitely many exceptions, either 1 or $2 \bmod 5$ and infinitely many primes $p \equiv 2 \bmod 5$ arise in this way.

A polynomial $h(T) \in \mathbf{Z}[T]$ will be called a *Euclidean* polynomial for $a \bmod m$, where $(a, m) = 1$, if the prime factors of all $h(n)$, with finitely many exceptions, satisfy either $p \equiv 1 \bmod m$ or $p \equiv a \bmod m$, and infinitely many primes of the latter kind occur. Whatever a 'Euclidean' proof of Dirichlet's theorem for $a \bmod m$ ought to be, at the end of such a proof we should have a Euclidean polynomial for $a \bmod m$.

The following theorems of Schur [8] and Murty [5] show Euclidean polynomials (and thus Euclidean proofs of Dirichlet's theorem) are quite restricted.

Theorem 1 (Schur, 1912). *If $a^2 \equiv 1 \bmod m$, then a Euclidean polynomial for $a \bmod m$ exists.*

Theorem 2 (Murty, 1988). *If there is a Euclidean polynomial for $a \bmod m$, then $a^2 \equiv 1 \bmod m$.*

¹G. H. Hardy, Collected Papers, Vol. I, p. 549

For example, since $2^2 \equiv 4 \not\equiv 1 \pmod{5}$, there is no Euclidean polynomial for $2 \pmod{5}$, so there is no proof of Dirichlet's theorem for $2 \pmod{5}$ that can mimic Euclid's proof of the infinitude of the primes.

Remark 3. In Dickson's book on the history of number theory [2, p. 419], the section *Elementary proofs of the existence of an infinitude of primes in special arithmetic progressions* says E. Lucas in 1878 had found an elementary proof for primes of the form $5n + 2$. His argument [4, p. 309] uses the numbers $a_n = F_{2n}/F_{2n-1}$, where F_m is the m th Fibonacci number. (If $d \mid m$ then $F_d \mid F_m$, so $a_n \in \mathbf{Z}$ for all $n \geq 1$.) The sequence $\{a_n\}$ begins

$$1, 3, 7, 47, 2207, 4870847, 23725150497407, \dots$$

and grows very quickly, *e.g.*, a_{10} has 108 digits. Lucas wrote that $a_n \equiv 2 \pmod{5}$ when $n \geq 3$, which is true, and his proof involved showing each a_n has a prime factor that is $2 \pmod{5}$, which is false: the prime factorization of a_8 is pq where $p \equiv 3 \pmod{5}$ and $q \equiv 4 \pmod{5}$, and the prime factorization of a_9 is pqr where $p \equiv 1 \pmod{5}$, $q \equiv 3 \pmod{4}$, and $r \equiv 4 \pmod{5}$. Lucas clearly didn't know the prime factorization of a_8 or a_9 , and WolframAlpha can't fully factor a_{10} (its known prime factors are $3 \pmod{5}$).

The largest m such that all units modulo m square to 1 (and thus Dirichlet's theorem can be proved by Euclidean methods for all the possibilities modulo m) is $m = 24$. A treatment of Dirichlet's theorem along Euclidean lines for $m = 24$ is given in [1], which was the starting point for Murty's work (see [6]). His paper [5] appeared in a journal that is not widely available and was not reviewed on MathSciNet. An updated account of the work from [5] and [8] is in [7], which is available online (and has a MathSciNet review).

Between Theorems 1 and 2, the second is more unexpected, so we will focus on that. Its proof will require interpreting Euclidean polynomials in the language of algebraic number theory, as well as an application of the Chebotarev density theorem. This last point is quite ironic, since it means the proof that you can't prove special cases of Dirichlet's theorem in a certain way (*à la* Euclid) will use a result that is deeper than Dirichlet's theorem itself.

To transform Euclidean polynomials into something about number fields, note that the divisibility condition $p \mid h(n)$, for some $n \in \mathbf{Z}$, is equivalent to $h \pmod{p}$ having a root in $\mathbf{Z}/p\mathbf{Z}$. For any polynomial $h(T) \in \mathbf{Z}[T]$, set

$$\text{Spl}_1(h) := \{p : p \mid h(n) \text{ for some } n\} = \{p : h \pmod{p} \text{ has a linear factor in } (\mathbf{Z}/p\mathbf{Z})[T]\}.$$

For example, $\text{Spl}_1(T^2 + 1) = \{p \equiv 1 \pmod{4}\} \cup \{2\}$. There is no simple description of $\text{Spl}_1(T^5 - T + 1)$, the set of primes modulo which $T^5 - T + 1$ has a root.

For any number field K , set

$$\text{Spl}_1(K) := \{p : \text{some } \mathfrak{p} \text{ dividing } p \text{ in } K \text{ has } f(\mathfrak{p}|p) = 1\}.$$

For example, $\text{Spl}_1(\mathbf{Q}(i)) = \{p \equiv 1 \pmod{4}\} \cup \{2\}$.

In words, p lies in $\text{Spl}_1(h)$ when h has a root mod p , while p lies in $\text{Spl}_1(K)$ when p has a prime ideal factor in K whose residue field is $\mathbf{Z}/p\mathbf{Z}$.

To prove Theorem 2, we introduce some notation to codify the relation between Euclidean polynomials and Spl_1 sets. Fix a positive integer m . For any nonconstant polynomial $h(T)$ in $\mathbf{Z}[T]$ and any number field K , set

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

and

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

These are subsets of $(\mathbf{Z}/m\mathbf{Z})^\times$. For irreducible h , with θ a root of h , $\text{Spl}_1(h)$ and $\text{Spl}_1(\mathbf{Q}(\theta))$ coincide, with perhaps finitely many exceptions (these exceptions arise if $\mathbf{Z}[\theta]$ is not the ring of integers of $\mathbf{Q}(\theta)$), so $S_1(m, h)$ and $S_1(m, \mathbf{Q}(\theta))$ are equal without exceptions.

In this notation, a Euclidean polynomial for $a \bmod m$ is an $h(T)$ such that $S_1(m, h) = \{1, a \bmod m\}$.

The following theorem is the main technical step in the proof of Theorem 2.

Theorem 4. *For any number field K , the subset $S_1(m, K)$ of $(\mathbf{Z}/m\mathbf{Z})^\times$ is a subgroup. In fact, $S_1(m, K)$ is the image of $\text{Gal}(K(\zeta_m)/K) \rightarrow \text{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$.*

Proof. First we classify the congruence classes making up $S_1(m, K)$. We claim

$$(1) \quad S_1(m, K) = \{q \bmod m : q \in \text{Spl}_1(K), q \text{ unramified in } K(\zeta_m)\}.$$

One inclusion is trivial: since each congruence class in $S_1(m, K)$ contains infinitely many primes from $\text{Spl}_1(K)$, certainly each such class is represented by a prime in $\text{Spl}_1(K)$ that doesn't ramify in $K(\zeta_m)$, so the left side of (1) is contained in the right side. For the reverse inclusion, choose q in $\text{Spl}_1(K)$ with q unramified in $K(\zeta_m)$. We will produce infinitely many p in $\text{Spl}_1(K)$ that satisfy $p \equiv q \bmod m$, thus establishing (1).

Pick $\mathfrak{q} \mid q$ in K with $f(\mathfrak{q}|q) = 1$. Since q is unramified in $K(\zeta_m)$, \mathfrak{q} is unramified in $K(\zeta_m)$. Then the Frobenius element $\sigma = \text{Fr}_{\mathfrak{q}}(K(\zeta_m)/K)$ in $\text{Gal}(K(\zeta_m)/K)$ has

$$(2) \quad \sigma|_{\mathbf{Q}(\zeta_m)} = N \mathfrak{q} \bmod m = q \bmod m.$$

By the Chebotarev density theorem for the cyclotomic extension $K(\zeta_m)/K$, there are infinitely many \mathfrak{p} in K such that

- \mathfrak{p} is unramified in $K(\zeta_m)$
- $\text{Fr}_{\mathfrak{p}}(K(\zeta_m)/K) = \sigma$
- $f_{\mathfrak{p}}(K/\mathbf{Q}) = 1$.

The last condition follows from the positive density of \mathfrak{p} with Frobenius element σ and the full density of \mathfrak{p} with absolute degree 1.

Setting $p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z}$, p lies in $\text{Spl}_1(K)$ by construction and

$$(3) \quad \sigma|_{\mathbf{Q}(\zeta_m)} = p \bmod m.$$

Comparing (2) and (3), we have $p \equiv q \bmod m$.

Having proved (1), we now turn to showing $S_1(m, K)$ is the image of $\text{Gal}(K(\zeta_m)/K) \rightarrow \text{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$. Denote this image as H .

Pick a congruence class in $S_1(m, K)$, say $q \bmod m$ in the notation of (1). We have already seen in (2) that $q \bmod m$ is the restriction to $\mathbf{Q}(\zeta_m)$ of the Frobenius element $\text{Fr}_{\mathfrak{q}}(K(\zeta_m)/K)$, where \mathfrak{q} lies over q in K with $f(\mathfrak{q}|q) = 1$. That means $q \bmod m$ lies in H , so $S_1(m, K) \subset H$.

To establish the reverse inclusion, let $b \bmod m \in H$, say $b \bmod m = \sigma|_{\mathbf{Q}(\zeta_m)}$ where $\sigma \in \text{Gal}(K(\zeta_m)/K)$.

By the Chebotarev density theorem for cyclotomic extensions, $\sigma = \text{Fr}_{\mathfrak{p}}(K(\zeta_m)/K)$ for infinitely many \mathfrak{p} in K with $f_{\mathfrak{p}}(K/\mathbf{Q}) = 1$. Let $p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z}$, so p is in $\text{Spl}_1(K)$ and $N \mathfrak{p} = p$. Then

$$\sigma|_{\mathbf{Q}(\zeta_m)} = N \mathfrak{p} \bmod m = p \bmod m,$$

so $p \equiv b \bmod m$. Since the number of such p is infinite, $b \bmod m$ is in $S_1(m, K)$. \square

The fact that the set $S_1(m, K)$ is a group may seem surprising, since we did not directly prove $S_1(m, K)$ is closed under multiplication, or even that it contains the identity. This follows only after Theorem 4 is concluded, though the condition that $1 \bmod m \in S_1(m, K)$

does admit a direct verification, as follows. Infinitely many rational primes p split completely in the field $K(\zeta_m)$, and (with the exception of $p = 2$ if $m = 2$) all such p satisfy $p \equiv 1 \pmod m$ and $p \in \text{Spl}_1(K)$. If the reader is hoping for a direct proof that $S_1(m, K)$ is closed under multiplication, we don't have one to offer. Instead, we will give below a nonabelian generalization of Theorem 4 in which the analogue of $S_1(m, K)$ will usually not be a group.

But first let's return to Theorem 2 and derive it from Theorem 4. We start with a congruence class $a \pmod m$ where $(a, m) = 1$ and assume this congruence class admits a Euclidean polynomial, say $h(T)$. That is, we assume $S_1(m, h) = \{1, a \pmod m\}$. For each irreducible factor $g(T)$ of $h(T)$, $\text{Spl}_1(g)$ contains infinitely many $p \equiv 1 \pmod m$ since $S_1(m, g) = S_1(m, \mathbf{Q}(\theta))$, where $g(\theta) = 0$. By the pigeonhole principle, at least one such irreducible factor g must have infinitely many $p \equiv a \pmod m$ in $\text{Spl}_1(g)$, so $S_1(m, g) = \{1, a \pmod m\}$. (That is, if $a \pmod m$ admits a Euclidean polynomial, then it admits an irreducible Euclidean polynomial.) Identifying $S_1(m, g)$ with $S_1(m, \mathbf{Q}(\theta))$, where $g(\theta) = 0$, Theorem 4 implies $\{1, a \pmod m\}$ is a group, so $a^2 \equiv 1 \pmod m$. This settles Theorem 2 and explains what makes the condition $a^2 \equiv 1 \pmod m$ distinctive: it characterizes when $\{1, a \pmod m\}$ is a group.

As a generalization of Theorem 4, we replace the cyclotomic extension $\mathbf{Q}(\zeta_m)/\mathbf{Q}$ with an arbitrary finite Galois extension E/F of number fields. Let K/F be an arbitrary finite extension, and set

$$\text{Spl}_1(K/F) := \{\mathfrak{p} \text{ in } F : \text{ some } \mathfrak{P} \text{ dividing } \mathfrak{p} \text{ in } K \text{ has } f(\mathfrak{P}|\mathfrak{p}) = 1\}.$$

(Previously, when the base field was $F = \mathbf{Q}$, we wrote $\text{Spl}_1(K)$ rather than $\text{Spl}_1(K/\mathbf{Q})$.)

In $\text{Gal}(E/F)$, primes in F that are unramified in E have Frobenius conjugacy classes rather than Frobenius elements. With this modification, Theorem 4 generalizes as follows.

Theorem 5. *As C varies over the conjugacy classes of $\text{Gal}(E/F)$, the union of all C such that $C = \text{Fr}_{\mathfrak{p}}(E/F)$ for infinitely many \mathfrak{p} in $\text{Spl}_1(K/F)$ forms the smallest subset of $\text{Gal}(E/F)$ that 1) contains the image of $\text{Gal}(EK/K) \rightarrow \text{Gal}(E/F)$ and 2) is closed under conjugation.*

Proof. Let $S_1(E, K)$ be the union of the conjugacy classes C in $\text{Gal}(E/F)$ such that $C = \text{Fr}_{\mathfrak{p}}(E/F)$ for infinitely many \mathfrak{p} in $\text{Spl}_1(K/F)$. (If $F = \mathbf{Q}$ and $E = F(\zeta_m)$, then $S_1(E, K)$ is the set $S_1(m, K)$ from before.)

To prove the theorem, we show

- $\text{Gal}(E/E \cap K) \subset S_1(E, K)$
- $S_1(E, K)$ is closed under conjugation
- Each conjugacy class in $S_1(E, K)$ contains an element of $\text{Gal}(E/E \cap K)$.

This will show $S_1(E, K)$ is the smallest subset of $\text{Gal}(E/F)$ that contains $\text{Gal}(E/E \cap K)$ and is closed under conjugation.

The second property above is immediate: as a union of conjugacy classes, $S_1(E, K)$ is closed under conjugation.

To prove the first and third properties, we show $S_1(E, K)$ is the union of conjugacy classes $\text{Fr}_{\mathfrak{q}}(E/F)$, where \mathfrak{q} lies in $\text{Spl}_1(K/F)$ and \mathfrak{q} is unramified in EK . Any conjugacy class in $S_1(E, K)$ is, by definition, a Frobenius class for infinitely many primes of $\text{Spl}_1(K/F)$, so we can arrange such a prime to be unramified in EK . For the reverse inclusion, let \mathfrak{q} be a prime $\text{Spl}_1(K/F)$ that is unramified in EK . Choose any \mathfrak{Q} in K lying over \mathfrak{q} with $f(\mathfrak{Q}|\mathfrak{q}) = 1$, so \mathfrak{Q} is unramified in EK and $N\mathfrak{Q} = N\mathfrak{q}$.

Choose any σ in the conjugacy class $\text{Fr}_\Omega(EK/K)$, and write $\sigma = (\tilde{\Omega}, EK/K)$ for $\tilde{\Omega}$ lying over Ω in EK . Set $\tilde{q} = \tilde{\Omega} \cap E$. From the definitions of Frobenius elements, $\sigma|_E = (\tilde{q}, E/F) \in \text{Gal}(E/F)$, so $\sigma|_E$ lies in the conjugacy class $\text{Fr}_q(E/F)$.

By the Chebotarev density theorem for $\text{Gal}(EK/K)$, there are infinitely many \mathfrak{P} in K that are unramified in EK and satisfy $\text{Fr}_\mathfrak{P}(EK/K) = \text{Fr}_\Omega(EK/K)$ and $f_\mathfrak{P}(K/F) = 1$.

Let $\mathfrak{p} = \mathfrak{P} \cap F$, so \mathfrak{p} lies in $\text{Spl}_1(K/F)$ and $N\mathfrak{P} = N\mathfrak{p}$. Discarding finitely many \mathfrak{P} , we may assume \mathfrak{p} is unramified in EK .

Choose $\tilde{\mathfrak{P}}$ lying over \mathfrak{P} in EK such that $\sigma = (\tilde{\mathfrak{P}}, EK/K)$. Note $\sigma|_E = (\tilde{\mathfrak{p}}, E/F)$, where $\tilde{\mathfrak{p}} = \tilde{\mathfrak{P}} \cap E$, so the conjugacy classes $\text{Fr}_\mathfrak{p}(E/F)$ and $\text{Fr}_q(E/F)$ both contain $\sigma|_E$ and thus coincide. This proves the conjugacy classes making up $S_1(E, K)$ are the Frobenius conjugacy classes for primes in $\text{Spl}_1(K/F)$ that are unramified in EK .

In the course of the above argument, we showed $\text{Fr}_q(E/F)$ contains $\sigma|_E$ for some (explicit) σ in $\text{Gal}(EK/K)$, and therefore each conjugacy class in $S_1(E, K)$ contains an element of $\text{Gal}(E/E \cap K)$. This settles the third item above.

As for the first item, that $\text{Gal}(E/E \cap K) \subset S_1(E, K)$, pick any element of $\text{Gal}(E/E \cap K)$, say $\sigma|_E$ where $\sigma \in \text{Gal}(EK/K)$. The method of the proof so far shows $\sigma|_E = (\tilde{\mathfrak{p}}, E/F)$ for a prime $\tilde{\mathfrak{p}}$ in K where $\mathfrak{p} = \tilde{\mathfrak{p}} \cap F$ lies in $\text{Spl}_1(K/F)$ and \mathfrak{p} is unramified in EK . Therefore $\sigma|_E$ is in $S_1(E, K)$. \square

Since $S_1(E, K)$ is the smallest union of conjugacy classes containing a certain group, it has no right to be a group automatically unless $\text{Gal}(E/F)$ is abelian, in which case $S_1(E, K) = \text{Gal}(E/E \cap K)$.

REFERENCES

- [1] P. T. Bateman and M. E. Low, *Prime numbers in arithmetic progressions with difference 24*, Amer. Math. Monthly **72** (1965), 139–143.
- [2] L. E. Dickson, “History of the Theory of Numbers, Vol I: Divisibility and Primality,” Chelsea, NY, 1971.
- [3] X. Lin, *Infinitely many primes in the arithmetic progression $kn - 1$* , Amer. Math. Monthly **122** (2015), 48–51.
- [4] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques*, Amer. J. Math. **1** (1878), 184–196, 197–240, 289–321.
- [5] M. R. Murty, *Primes in certain arithmetic progressions*, J. Madras Univ. (1988), 161–169.
- [6] M. R. Murty, *How I discovered Euclidean proofs*, Nieuw Archief voor Wiskunde **5/18** (2017), 101–102. Online at <http://www.nieuwarchief.nl/serie5/pdf/naw5-2017-18-2-101.pdf>.
- [7] M. R. Murty and N. Thain, *Primes in certain arithmetic progressions*, Funct. Approx. Comment. Math. **35** (2006), 249–259. Online at <https://projecteuclid.org/euclid.facm/1229442627>
- [8] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, Sitzungber. Berliner Math. Ges. **11** (1912), 40–50.