1 The scope of Euclidean proofs

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

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

Remark 1.1. The cases $k = 1, 2$ are highly degenerate, and a Euclidean proof can be easily established (see **??** in the Appendix).

1.1 Schur Theorem

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

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

$$G = \bigsqcup_{s \in S} sH = \bigsqcup_{s \in S} \{s, s\ell\}. \tag{1.1}$$

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

Now define the polynomial

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

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

Lemma 1.2. *The equality $h_u(\zeta)^s = h_u(\zeta^s)$ holds for every $s \in S$.*

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

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

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

[1] The case $\ell \equiv 1 \pmod{k}$ is easier and will be proved in Section 1.1.1.

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

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

Lemma 1.3. *Let $a \in G$. Then $\sigma_a(\eta) = \sigma_s(\eta)$, where s is the coset representative of a.*

Proof. Since a belongs to G, it must happen that $a = s$ or $a = s\ell$ for some coset representative $s \in S$, because of Eq. (1.1). In the first case, there is nothing to prove, so suppose $a = s\ell$. Now,

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

where again we used that $\sigma_{s\ell}$ is a field automorphism in the third equality. In the fifth equality we used that $\zeta^{s\ell^2}$ only depends on the value of $s\ell^2 \bmod k$. Since $\ell^2 \equiv 1 \pmod k$, it follows that $\zeta^{s\ell^2} = \zeta^s$. Finally, because of Lemma 1.2,

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

□

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

$$f_u(x) := \prod_{s\in S} \Big(x - h_u(\zeta^s)\Big) = \prod_{s\in S} \Big(x - (\zeta^s - u)(u - \zeta^{\ell s})\Big), \tag{1.2}$$

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

Proposition 1.4. *The field $L := \mathbb{Q}(\eta)$ is the fixed field of H, except for finitely many values of u. Excluding these cases, the polynomial f_u is irreducible.*

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

The converse implication is simple. Denote by σ_ℓ the only non-trivial automorphism in H. Since the coset representative of ℓ is $s = 1$, it follows from Lemma 1.3 that $\sigma_\ell(\eta) = \sigma_{s=1}(\eta) = \eta$.

We now have to show that the equality $\sigma(\eta) = \eta$ implies that σ belongs to H. We will instead prove the equivalent contrapositive assertion: if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ does not belong to H, then $\sigma(\eta) \neq \eta$. Because of Lemma 1.3, it is enough to check it for the automorphisms

σ_s with $s \neq 1$, which excludes σ_1 and σ_ℓ (the automorphisms in H). From Lemma 1.2, we have

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

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

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

$$h_u(\zeta^s) = (\zeta^s - u)(u - \zeta^{\ell s}) = (\zeta - u)(u - \zeta^\ell) = \eta \tag{1.3}$$

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

$$\begin{aligned} h_u(\zeta^s) &= \eta, \\ u^2 - (\zeta^s + \zeta^{\ell s})u + \zeta^{s(1+\ell)} &= u^2 - (\zeta + \zeta^\ell)u + \zeta^{1+\ell}, \\ -(\zeta^s + \zeta^{\ell s})u + \zeta^{s(1+\ell)} &= -(\zeta + \zeta^\ell)u + \zeta^{1+\ell} \end{aligned} \tag{1.4}$$

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

Indeed, observe that complex conjugation $\tau : \zeta \mapsto \bar{\zeta} = \zeta^{-1}$ belongs to G and has order 2, so the fixed field of $\{\mathrm{id}, \tau\}$ is the maximal real subfield of K, which is of degree 2 below K. Also, this field must coincide with the real field $\mathbb{Q}(\zeta + \zeta^{-1}) \subset K$, which is also fixed by $\{\mathrm{id}, \tau\}$ and is of degree 2, since $(x - \zeta)(x - \zeta^{-1}) = x^2 - (\zeta + \zeta^{-1})x + 1$ is the minimal polynomial of ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$. Since this field has degree 2, by the Galois correspondence it must be the fixed field of the group $\{1, -1\} = \{1, \ell\}$, so σ_s belongs to this group. Then, $s = 1$, but this does not happen since we chose the coset s to lie in S^*. Thus, Eq. (1.3) only has a finite number of solutions for u. Excluding these finite values of u, we have that $\sigma_s(\eta) \neq \eta$ for $s \in S^*$, so finally $L = \mathbb{Q}(\eta)$.

To prove the last part of the proposition, take some u such that $L = \mathbb{Q}(\eta)$. We will now show that every $\eta^s = h_u(\zeta^s)$, for $s \in S$, is different. To reach a contradiction, suppose $h_u(\zeta^{s_1}) = h_u(\zeta^{s_2})$ for $s_1 \neq s_2$. We can write $\sigma_{s_1}(h_u(\zeta)) = \sigma_{s_2}(h_u(\zeta))$, because of Lemma 1.2. Thus, in terms of η, we have $\sigma_{s_2}^{-1}\sigma_{s_1}(\eta) = \eta$. Defining $\phi := \sigma_{s_2}^{-1}\sigma_{s_1}$, then ϕ fixes L, so ϕ belongs to $\mathrm{Gal}(K/L) = H$, which implies that $\sigma_{s_1}H = \sigma_{s_2}H$. That is, s_1 and s_2 are in the same coset of H, which is a contradiction. Therefore, η^s for $s \in S$ (which are the roots of f_u) are all distinct. This guarantees that $f_u \in \mathbb{Z}[x]$ is separable.

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

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

Remark 1.5. Some remarks can be made in relation to the tower of extensions $K/L/\mathbb{Q}$. In light of the Galois correspondence, we have that $[L = K^H : \mathbb{Q}] = [G : H] = \varphi(k)/2$, and also $[K : K^H] = |H| = 2$. Similarly, $[K : \mathbb{Q}] = |G| = \varphi(k)$. Also, f_u is the minimal polynomial of η, since it is irreducible, $f_u(\eta) = 0$, and $\deg(f_u) = |S| = \varphi(k)/2$. In short, f_u is a polynomial of degree $\varphi(k)/2$ whose roots generate L and are invariant under the action of the subgroup H. Indeed,

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

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

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

Remark 1.6. For the following results we will need to consider a field $\mathbb{F}$ containing both the finite field $\mathbb{F}_p$ and ζ. For instance, consider $\mathbb{F} = \mathbb{F}_{p^n}$ with a suitable integer $n \geqslant 1$ such that Φ_k has a root ζ. This is possible because $\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}_p}$, where $\overline{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_p$. Obviously, in this context we cannot think of ζ as an element of $\mathbb{C}$, but rather as some root of an irreducible factor of $\overline{\Phi_k} \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$. Alternatively, this field $\mathbb{F}$ can be constructed via $\mathbb{F}_p[x]/(r(x))$ for some factor $r(x)$ of Φ_k which is irreducible over $\mathbb{F}_p$.

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

Theorem 1.7 (Schur). *Every prime divisor of f_u belongs to the residue classes of H (except for finitely many prime divisors).*

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

Since p divides f_u, working in the field $\mathbb{F}$ of Remark 1.6, there exists $a \in \mathbb{Z}$ such that

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

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

$$\begin{aligned}h_u(\zeta^s) = a = a^p = h_u(\zeta^s)^p &= (\zeta^s - u)^p(u - \zeta^{\ell s})^p \\ &= (\zeta^{ps} - u^p)(u^p - \zeta^{\ell ps}) = (\zeta^{ps} - u)(u - \zeta^{\ell ps}) = h_u(\zeta^{ps}),\end{aligned} \tag{1.5}$$

where we have used Fermat little theorem in the second equality. The fifth equality, on the other hand, relies on the fact that $\operatorname{char}(\mathbb{F}) = p$ (so that $(c + d)^p = c^p + d^p$ for every $c, d \in \mathbb{F}$) and the following one, on Fermat little theorem. Therefore, equality Eq. (1.4) means that $h_u(\zeta^{ps}) = h_u(\zeta^s)$ is a root of $\overline{f_u} \in \mathbb{F}[x]$.

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

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

There are now only two options: either $ps \bmod k$ belongs to S or $ps \bmod k$ does not belong to S. In the first case, $h_u(\zeta^{ps})$ is a root of f_u in K, observing expression Eq. (1.2). In the latter case, note that every integer $ps \bmod k$ relatively prime to k not in S satisfies $ps \equiv \ell t \pmod k$ for some $t \in S$ (because of Eq. (1.1)). This means that $h_u(\zeta^{ps}) = h_u(\zeta^{\ell t})$. Let us prove that $h_u(\zeta^{\ell t}) = h_u(\zeta^t)$, so $h_u(\zeta^{ps}) = h_u(\zeta^{\ell t}) = h_u(\zeta^t)$ is also a root of f_u in K. Indeed,

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

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

We will now see that $h_u(\zeta^{ps})$ and $h_u(\zeta^s)$ are the same root of f_u in K. If $h_u(\zeta^{ps})$ and $h_u(\zeta^s)$ were two distinct roots of f_u in K, we know because of Eq. (1.4) that they would be the same in $\mathbb{F}$. Therefore, observing the discriminant expression in **??**, it follows that $\Delta(f_u \bmod p) = \Delta(f_u) \bmod p = 0$, so p divides $\Delta(f_u)$. This is a contradiction with our choice of p. Thus, $h_u(\zeta^{ps})$ and $h_u(\zeta^s)$ are in fact the same root of f_u in K, so $h_u(\zeta^{ps}) = h_u(\zeta^s)$.

Since p does not lie in T, it follows that $\gcd(k, p) = 1$, so one can consider the field automorphism $\sigma_p \in \mathrm{Gal}(K/\mathbb{Q})$. Following the spirit of Lemma 1.2, one can easily see that $h_u(\zeta^{ps}) = h_u(\zeta^s)^p$, so $h_u(\zeta^s)^p = h_u(\zeta^{ps}) = h_u(\zeta^s)$ in K. Therefore, $\eta^s = h_u(\zeta^s)$ is fixed by σ_p and so is $\mathbb{Q}(\eta^s)$. Now, $\mathbb{Q}(\eta^s) = L$, because η^s is a conjugate of η (thus, $\mathbb{Q}(\eta^s)/\mathbb{Q}$ is Galois since $L/\mathbb{Q}$ is Galois). Consequently, σ_p also fixes L, and since $L = K^H$ by definition, it must happen that $p \bmod k$ belongs to H, that is, $p \equiv 1, \ell \pmod k$. □

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

Proposition 1.8. *Any prime belonging to any residue class of H divides f_u.*

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

$$\eta^p = \sigma_p(\eta) = \sigma_{s=1}(\eta) = \eta, \tag{1.6}$$

because of Lemma 1.3.

Consider now the equation $x^p - x$ and let us work in the field $\mathbb{F}$ of Remark 1.6. Since $\mathbb{F}$ is a field with $\mathrm{char}(\mathbb{F}) = p$ there are p solutions to this equation, since x lies in $\mathbb{F}$ if and only if $x^p = x$. In fact, there exist exactly p integer solutions to the equation: thanks to Fermat little theorem, $0, \ldots, p-1$ are roots of $x^p - x \bmod p$. Since $\eta^p - \eta = 0$ because of Eq. (1.5), η is also a solution, and it must be an integer, so $\eta = b$ for some integer b. It

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

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

Remark 1.9. Observe that Theorem 1.7 tells us that, except for finitely many primes, we have $\text{Spl}_1(f_u) \subseteq \{p : p \equiv 1, \ell \pmod{k}\}$. With this last Proposition 1.8 we have that $\{p : p \equiv 1, \ell \pmod{k}\} \subseteq \text{Spl}_1(f_u)$. Thus, $\text{Spl}_1(f_u) = \{p : p \equiv 1, \ell \pmod{k}\}$, except for finitely many primes.

We will also need the following result.

Proposition 1.10 (Schur). *Every prime divisor of Φ_k not dividing k is $\equiv 1 \pmod{k}$.*

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

Since p divides Φ_k, working in the field $\mathbb{F}$ of Remark 1.6, there exists $a \in \mathbb{Z}$ such that

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

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

$$\zeta^s = a = a^p = \zeta^{ps}, \tag{1.7}$$

where we have used Fermat little theorem in the second equality. Therefore, equality Eq. (1.6) means that $\zeta^{ps} = \zeta^s$ is a root of $\overline{\Phi_k} \in \mathbb{F}[x]$.

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

We will now show that ζ^{ps} and ζ^s are the same root of Φ_k in K. If ζ^{ps} and ζ^s were two distinct roots of Φ_k in K, we know because of Eq. (1.6) that they would be the same in $\mathbb{F}$. Therefore, observing expression **??**, it follows that $\Delta(\Phi_k \bmod p) = \Delta(\Phi_k) \bmod p = 0$, so p divides $\Delta(\Phi_k)$. This is a contradiction with our choice of p. Thus, ζ^{ps} and ζ^s are in fact the same root of Φ_k in K.

Therefore, the equality

$$\zeta^{ps} = \zeta^s \tag{1.8}$$

holds in K. Writing the above equation in terms of $\theta := \zeta^s$ yields $\theta^p = \theta$, where observe that θ is also a primitive kth root of unity. Now, the right-hand side of the equation above does not depend on p. The left-hand side only depends on the value of $p \bmod k$, since p only appears as an exponent of θ. In conclusion, equality Eq. (1.7) only holds if $p \bmod k = 1$, that is, if $p \equiv 1 \pmod{k}$. □

Remark 1.11. In the same lines of Remark 1.9, Proposition 1.8 tells us that $\{p : p \equiv 1 \pmod{k}\} \subseteq \mathrm{Spl}_1(\Phi_k)$ (observe there was no need to suppose $\ell \not\equiv 1 \pmod{k}$ in the proof of that proposition). This last Proposition 1.10 tells us that, except for finitely many primes, we have $\mathrm{Spl}_1(\Phi_k) \subseteq \{p : p \equiv 1 \pmod{k}\}$. Thus, $\mathrm{Spl}_1(\Phi_k) = \{p : p \equiv 1 \pmod{k}\}$, except for finitely many primes.

Since Proposition 1.4 holds except for a finite number of values of the integer u, we can further suppose u to be a non-zero multiple of k. We then have:

Lemma 1.12. *The equality $f_u(0) = \Phi_k(u)$ holds. Also, every prime divisor of $\Phi_k(u)$ is $\equiv 1 \pmod{k}$.*

Proof. From Eq. (1.2), one has

$$f_u(0) = \prod_{s \in S} (u - \zeta^s)(u - \zeta^{\ell s}) = \prod_{a \in G} (u - \zeta^a), \tag{1.9}$$

where we use Eq. (1.1). Since the kth cyclotomic polynomial is defined by

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

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

$$\Phi_k(u) = \prod_{a \in G} (u - \zeta^a) \equiv (-1)^{\varphi(k)} \prod_{a \in G} \zeta^a = \prod_{a \in G} \zeta^a = 1 \pmod{k}, \tag{1.10}$$

where we used that Euler's function $\varphi(k)$ is always even for $k > 2$. The last equality comes from the fact that the product goes over all kth primitive roots of unity: this excludes -1 and the roots can be grouped in complex-conjugate pairs[3], so every pair equals one: $\zeta^a \overline{\zeta^a} = |\zeta^a|^2 = 1$ for every $a \in G$.

We will finally see that $\Phi_k(u)$ is only divisible by primes $\equiv 1 \pmod{k}$. Let r be a prime divisor of $\Phi_k(u)$. From Proposition 1.10 it follows that $r \equiv 1 \pmod{k}$ or r divides k. However, if r divides k, then $\Phi_k(u) \equiv 1 \pmod{r}$ because of Eq. (1.9). This means that r does not divide $\Phi_k(u)$, a contradiction. Therefore, $\Phi_k(u) = f_u(0)$ is only divisible by primes $\equiv 1 \pmod{k}$. □

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

Theorem 1.13. *There exists an integer $n = n(k, \ell)$ such that if there exists a prime $p \equiv \ell \pmod{k}$ satisfying $p \nmid n$, then there exists a Euclidean proof of the infinitude of primes $\equiv \ell \pmod{k}$.*

Proof. We must first find a special integer b with some special and suitable properties for our Euclidean proof. By hypothesis, pick one prime $p \equiv \ell \pmod{k}$ such that p does not divide $n := \Delta(f_u)$. Now, by Proposition 1.8, we can find some $b \in \mathbb{Z}$ such that p divides

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

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

$$f_u(b+x) = f_u(b) + f_u'(b)x + \frac{f_u''(b)}{2!}x^2 + O(x^3) \in \mathbb{Z}[x]. \tag{1.11}$$

In the case $x = p$, Eq. (1.10) reads

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

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

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

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

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

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

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

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

We will now prove that every prime that divides $f_u(c)$ is $\equiv 1 \pmod{k}$ (except for p). Let r be a prime divisor of $f_u(c)$ different from p. In Theorem 1.7 we have shown that every prime divisor of f_u divides k, divides $\Delta(f_u)$, or is $\equiv 1, \ell \pmod{k}$. To reach a contradiction, suppose $r \not\equiv 1 \pmod{k}$. Thus, $r \equiv \ell \pmod{k}$ or r divides k or $\Delta(f_u)$, so r divides $kq_1q_2\cdots q_t p_2 p_3 \cdots p_m = kQ$. Since $f_u(c) \equiv f_u(0) \pmod{kQ}$ and r is a divisor of kQ, we deduce that $f_u(c) \equiv f_u(0) \pmod{r}$. But r is a divisor of $f_u(c)$, so $f_u(c) \equiv 0 \pmod{r}$. Therefore, $f_u(0) \equiv 0 \pmod{r}$. Thus, it must happen that r is a prime factor of $f_u(0)$, all of which are $\equiv 1 \pmod{k}$, thanks to Lemma 1.12. This forces r to be $\equiv 1 \pmod{k}$, a contradiction. Therefore, $f_u(c)$ is only divisible by primes $\equiv 1 \pmod{k}$ (and by p).

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

$p \equiv \ell \pmod{k}$ and the fact that p^2 does not divide $f_u(c)$). However, observe that $f_u(c) \equiv f_u(0) = \Phi_k(u) \equiv 1 \pmod{k}$, due to Lemma 1.12. This is a contradiction since $\ell \not\equiv 1 \pmod{k}$. Therefore, the arithmetic progression $\equiv \ell \pmod{k}$ contains infinitely many primes. □

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

Remark 1.14. As we have previously said, the proof of the above theorem is due to Schur, and it is detailed in Murty's article [**Murty**]. In that article, however, $h_u(z)$ is defined as $h_u(z) := (u - z)(u - z^\ell)$, that is, our definition differs in a sign. Now observe Eq. (1.8). If Murty's definition is followed, then

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

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

One more remark should be made.

Remark 1.15. Observe that to prove the previous theorem we need to suppose the existence of a prime $p \equiv \ell \pmod{k}$ such that p does not divide $\Delta(f_u)$. This hypothesis is indeed necessary. For instance, take $k = 15$, $\ell = 11$, and $u = 15$ (note that $11^2 = 121 \equiv 1 \pmod{15}$). In this case, following Eq. (1.2), $f_{15}(x) = x^4 + 884x^3 + 293206x^2 + 43243679x + 2392743361$, and a quick calculation with SageMath leads to $\Delta(f_{15}) = 5^3 \cdot 11^2 \cdot 19^2 \cdot 41^2 \cdot 1091^2$. In this case, both the primes 11 and 41 are $\equiv 11 \pmod{15}$, but they both divide $\Delta(f_{15})$.

However, in Murty's article he does not require this additional constraint over p. In fact, he states: "Now pick some prime $p \equiv \ell \pmod{k}$ *so that* p does not divide the discriminant of f". The case $k = 15$ and $\ell = 11$ is a counterexample to this statement, so the "so that" in his article should be changed to a "such that". Thus, this extra hypothesis over p is needed for the argument to work[4].

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

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

Corollary 1.16. *There are infinitely many primes* $\equiv 1 \pmod{k}$.

Proof. Observe that Proposition 1.10 tells us that all prime divisors of Φ_k but finitely many are $\equiv 1 \pmod{k}$. However, in **??** we proved that every non-constant polynomial in $\mathbb{Z}[x]$ has infinitely many prime divisors. Since $\Phi_k \in \mathbb{Z}[x]$ is non-constant, the desired result is finally settled. □

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

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

1.2 The converse problem. Murty Theorem

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

To prove his theorem, we will use some algebraic number theory and the Chebotarev Denisty Theorem. We shall follow [**Conrad**] to prove Murty's claim in greater detail and clarity than that offered in his article [**Murty**]. Again, let ζ be a kth primitive root of unity, let K be any number field[5], and recall that in characteristic zero $K(\zeta)/K$ is a Galois extension since $x^k - 1$ is separable over K. Hence, $x^k - 1$ has k different roots in the splitting field over K, which is $K(\zeta)$. Before proceeding to the next theorem, recall the concepts in **??**, **??** and **??**. Specifically recall that in **??** we defined the set $S_1(k, K)$ as

$$S_1(k, K) := \{b \bmod k : p \equiv b \pmod{k} \text{ for infinitely many } p \in \mathrm{Spl}_1(K)\}. \tag{1.12}$$

Theorem 1.17 (Conrad). *Let $\psi : \mathrm{Gal}(K(\zeta)/K) \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, where $\psi(\sigma) = \sigma|_{\mathbb{Q}(\zeta)}$ for every $\sigma \in \mathrm{Gal}(K(\zeta)/K)$. Then, $\mathrm{Im}(\psi) = S_1(k, K)$.*

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

$$S_1(k, K) = \{q \bmod k : q \in \mathrm{Spl}_1(K), q \text{ unramified in } K(\zeta)\}. \tag{1.13}$$

We will first see that the left side of Eq. (1.12) is contained in the right side. Each congruence class in $S_1(k, K)$ contains infinitely many primes p from $\mathrm{Spl}_1(K)$ by definition, and for each of these primes, there exists some prime ideal $\mathfrak{p}$ dividing $p\mathcal{O}_K$ with $f_{K/\mathbb{Q}}(\mathfrak{p}|p) = 1$. Now, recall **??**: in any non-trival number field extension over $\mathbb{Q}$ the number of primes that ramify is finite. Thus, each of the classes in $S_1(k, K)$ has a prime representative in $\mathrm{Spl}_1(K)$, q, which is unramified in $K(\zeta)$.

We will now see that the right side of Eq. (1.12) is contained in the left side. Let q belong to $\mathrm{Spl}_1(K)$ with q unramified in $K(\zeta)$. We will prove that q belongs to $S_1(k, K)$ by showing infinitely many primes p lying in $\mathrm{Spl}_1(K)$ that satisfy $p \equiv q \pmod{k}$. By hypothesis, choose $\mathfrak{q}$ dividing $q\mathcal{O}_K$ in K such that $f_{K/\mathbb{Q}}(\mathfrak{q}|q) = 1$.

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

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

$$\sigma(\zeta) \equiv \zeta^{\mathrm{N}(\mathfrak{q})} \pmod{\mathfrak{b}}, \tag{1.14}$$

for any prime ideal $\mathfrak{b}$ lying over $\mathfrak{q}$ in $K(\zeta)$. By the canonical isomorphism between $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $(\mathbb{Z}/k\mathbb{Z})^\times$, we identify $\zeta^{\mathrm{N}(\mathfrak{q})}$ with $\mathrm{N}(\mathfrak{q}) \bmod k$. Therefore, since the restriction $\sigma|_{\mathbb{Q}(\zeta)}$ is fully determined by Eq. (1.13) and σ fixes $\mathbb{Q}$, we have

$$\sigma|_{\mathbb{Q}(\zeta)} = \mathrm{N}(\mathfrak{q}) \bmod k = q \bmod k, \tag{1.15}$$

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

$$\begin{aligned} &\text{(i)} \ \ \mathfrak{p} \text{ is unramified in } K(\zeta), \\ &\text{(ii)} \ \ \mathrm{Frob}_{\mathfrak{p}} = \sigma, \\ &\text{(iii)} \ \ f_{K/\mathbb{Q}}(\mathfrak{p}|p) = 1, \end{aligned} \tag{1.16}$$

where p arises from $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. In light of **??** and **??**, the intersection of the set of prime ideals satisfying the third condition and the set of prime ideals satisfying the first two conditions in Eq. (1.15) is indeed infinite: the density of the set of primes $\mathfrak{p}$ with inertia degree 1 is equal to one due to **??**, and the density of the unramified primes $\mathfrak{p}$ in $K(\zeta)$ with Frobenius element equal to σ is positive due to **??**.

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

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

which, comparing with Eq. (1.14), yields $p \equiv q \pmod{k}$ for infinitely many primes p of $\mathrm{Spl}_1(K)$. This finally settles Eq. (1.12).

We now turn our attention to the main claim in the theorem. Let $H := \mathrm{Im}(\psi)$[6]. We will start by proving that $S_1(k, K) \subseteq H$. For this goal, pick a congruence class $q \bmod k$ in $S_1(k, K)$ in the notation of Eq. (1.12). We know (see Eq. (1.14)) that $q \bmod k = \sigma|_{\mathbb{Q}(\zeta)}$, because, by hypothesis, there exists some $\mathfrak{q}$ lying over q in K with $f_{K/\mathbb{Q}}(\mathfrak{q}|q) = 1$ and also q is unramified in $K(\zeta)$. This means that $q \bmod k$ belongs to $\mathrm{Im}(\psi)$ and, hence, $S_1(k, K) \subseteq H$.

We will now prove that $H \subseteq S_1(k, K)$. Let $b \bmod k \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, with $\sigma|_{\mathbb{Q}(\zeta)} = b \bmod k$ for some $\sigma \in \mathrm{Gal}(K(\zeta)/K)$. This way, $b \bmod k$ belongs to H. Again, using Chebotarev Density Theorem with this automorphism σ, we have the same three results as in Eq. (1.15). In view of this, pick one prime ideal $\mathfrak{p}$ of K so that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ and p belongs to $\mathrm{Spl}_1(K)$. We have that $\mathrm{N}(\mathfrak{p}) = p$ and $\mathrm{Frob}_{\mathfrak{p}} = \sigma$. Therefore, we may write

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

Thus, $p \equiv b \pmod{k}$, and since the number of such primes p is infinite due to Chebotarev Density Theorem, $b \bmod k$ lies in $S_1(k, K)$, using Eq. (1.11). □

[6]The letter H is not chosen randomly, since we will see that $H := \mathrm{Im}(\psi) = S_1(k, K)$ and a Euclidean polynomial f for the arithmetic progression $\equiv \ell \pmod{k}$ satisfies $S_1(k, f) = \{1, \ell\} = H$, following the notation of Section 1.1.

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

Corollary 1.18 (Murty). *Let $f \in \mathbb{Z}[x]$ be a Euclidean polynomial. Then, $\ell^2 \equiv 1 \pmod{k}$.*

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

We can now use Theorem 1.17 with $K := \mathbb{Q}(\theta)$. From this result we deduce that $S_1(k, \mathbb{Q}(\theta)) = S_1(k, f) = \{1, \ell\}$ is the image of the morphism ψ. Thus, $H := \{1, \ell\}$ is a subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$. In particular, H is a group, so, by Lagrange Theorem, the order of ℓ must divide the order of H, which is 2. Since we are supposing $\ell \not\equiv 1 \pmod{k}$, the order of ℓ must be 2, so $\ell^2 \equiv 1 \pmod{k}$. □

Therefore, the complete theorem stands now in its full form: there exists a Euclidean proof of the infinitude of primes $\equiv \ell \pmod{k}$ if and only if $\ell^2 \equiv 1 \pmod{k}$[7]. While it is true that we managed to find proofs *à la Euclid* in these cases, the path to obtain them is not elemental. For one part, Theorem 1.13 requires a strong hypothesis, since we needed to suppose the existence of one prime $\equiv \ell \pmod{k}$ for every k and ℓ, which is tantamount to Dirichlet Theorem. We also used Dirichlet's result to show that f_u is a Euclidean polynomial. Moreover, we needed Chebotarev Density Theorem, which is, in fact, a deeper result than Dirichlet Theorem itself.

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

1.3 Abundance of Euclidean proofs

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

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

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

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

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

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

$$t = \begin{cases} d_o, & \text{if 4 does not divide } k, \\ d_o + 1, & \text{if } k \equiv 4 \pmod 8, \\ d_o + 2, & \text{if } k \equiv 0 \pmod 8, \end{cases} \tag{1.17}$$

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

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

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

Thus, for $(x_1^2, x_2^2, \ldots, x_t^2) = 1$ to be true, it must happen that $x_i = \pm 1$, so there are two options for every x_i. In conclusion, for a fixed k, the number of residue classes that satisfy $\ell^2 \equiv 1 \pmod k$ is 2^t, with t defined in Eq. (1.16). Therefore, our initial question comes down to the ratio $2^t/\varphi(k)$ for every k.

1.4 An alternative interpretation

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

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

A careful reading of the results in Section 1.1 leads to a characterisation of the set $\mathrm{Spl}_1(L)$ in terms of congruences for every subextension L of K satisfying $[K : L] \leqslant 2$.

By the Fundamental Theorem of Galois Theory, every subfield L of K with $[K : L] \leqslant 2$ must be the fixed field of a subgroup H of $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/k\mathbb{Z})^\times = G$ of index at most 2. The corresponding subset $H \subseteq G$ must be of the form $H = \{1, \ell\}$ for some $\ell \in G$, additionally satisfying $\ell^2 \equiv 1 \pmod k$ for it to be a subgroup of G. Observe that every subgroup of index 2 must be of this form. Observe that in Theorem 1.7 and Proposition 1.8 we have effectively studied the prime divisors of a polynomial generating every subfield L of K with $[K : L] = 2$. In particular, thanks to Remark 1.5, this polynomial is also the minimal polynomial of the algebraic element η which makes $L = \mathbb{Q}(\eta)$. The case $[K : L] = 1$ means that $L = K$, and H is the trivial group. We have also studied the prime divisors of the corresponding generating polynomial in Proposition 1.10, which in this case is the minimal polynomial of ζ.

Furthermore, in the above-cited results we have described the form of these prime divisors in terms of congruences. Let $B \subset A$ be two infinite sets, with $\#(A \setminus B)$ being

finite. We shall then write $A \simeq B$. With this notation, and recalling Remark 1.9 and Remark 1.11, we have seen the following:

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

$$\mathrm{Spl}_1(h) \simeq \{p : p \equiv 1, \ell \pmod{k}\}. \tag{1.18}$$

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

$$\mathrm{Spl}_1(h) \simeq \{p : p \equiv 1 \pmod{k}\}. \tag{1.19}$$

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

Since the extension $L/\mathbb{Q}$ is Galois, every irreducible factor mod p of h has degree 1 (see **??**). Dedekind Criterion establishes that the shape of the factorization of p in $\mathcal{O}_L$ mirrors that of $h \bmod p$ into irreducible factors. Thus, p has a prime ideal factor $\mathfrak{p}$ with $f(\mathfrak{p}|p) = 1$ in L exactly when p belongs to $\mathrm{Spl}_1(h)$. This is effectively a description of the set $\mathrm{Spl}_1(L)$ in terms of $\mathrm{Spl}_1(h)$. Observe that Dedekind Criterion works for the primes in Eq. (1.17) and Eq. (1.18), since they do not divide $\Delta(\mathbb{Z}[\eta]) = \Delta(h)$ by construction.

Therefore, one can interpret the results in Section 1.1 as reciprocity laws for L in the following terms:

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

$$\mathrm{Spl}_1(L) \simeq \{p : p \equiv 1, \ell \pmod{k}\}. \tag{1.20}$$

(b) If $L = K$, then

$$\mathrm{Spl}_1(L) \simeq \{p : p \equiv 1 \pmod{k}\}. \tag{1.21}$$

The first result is new to the literature, while the second one was already known. Let g be any polynomial generating the extension $L/\mathbb{Q}$ lying below K. In general, a characterisation of $\mathrm{Spl}_1(g)$ (and of $\mathrm{Spl}_1(L)$) is well-known if g is a quadratic or cyclotomic polynomial (see [**Chebotarev2**]). In the first case, the explicit rules to describe $\mathrm{Spl}_1(L)$ arise from the Quadratic Reciprocity Law (see **??**), while the characterisation of $\mathrm{Spl}_1(L)$ we have obtained for $L = K$ is an example of the second case. However, as far as the author is concerned, an explicit characterisation of $\mathrm{Spl}_1(L)$ for L lying below the kth cyclotomic field with $[K : L] = 2$ had not been explicitly given before.

Remark. While it is true that $\mathrm{Spl}_1(L)$ may contain more primes than those specified in Eq. (1.19) and Eq. (1.20), there can only exist finitely many such primes. Also, the strict equality $\mathrm{Spl}_1(h) = \mathrm{Spl}_1(L)$ is not in general true. Using SageMath one can easily see that there exists some prime divisor of h not $\equiv 1, \ell \pmod{k}$, for which every prime ideal $\mathfrak{p}$ lying above p has $f_{L/\mathbb{Q}}(\mathfrak{p}|p) \neq 1$. Thus, p belongs to $\mathrm{Spl}_1(h)$ but does not belong to $\mathrm{Spl}_1(L)$.

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