1 Automated proof generator

We have already seen that Euclidean proofs of the infinitude of primes are of particular interest because they mimic the simplicity of Euclid **??**, bypassing the technical difficulties of Dirichlet's argument. This section aims to use the methods developed in **??** to provide a systematic, elemental, and Euclidean proof on the infinitude of primes $\equiv \ell \pmod{k}$ whenever $\ell^2 \equiv 1 \pmod{k}$ (**??** also applies here). One may have observed in the previous section that the Euclidean proofs we developed in **??** and **??** require something more than just basic divisibility properties. In fact, deep number theory results are needed. Now, k and ℓ will be fixed so that the Euclidean essence of the proof will not be "covered" by intricate technicalities, since the existence theorems needed in the previous section will be replaced by simple verifications.

Therefore, the objective of this section is to create an Euclidean, *automated proof generator* of the infinitude of primes $\equiv \ell \pmod{k}$, only using the user-supplied choice of k and ℓ. In particular, given this pair of integers, our code will return a complete proof of the infinitude of primes in the specified arithmetic progression[1], which will slightly vary depending on the supplied values of k and ℓ. As far as the author is aware, this automated approach is a new contribution to the literature concerning not only Euclidean proofs but also general elemental proofs of Dirichlet Theorem. This part of the thesis will shed light on the methods used in previous sections, as well as confirming that the ideas described there work in specific cases.

The final proofs will be presented in an interactive and accessible way, so everyone can get their own Euclidean proof. For this goal, a Git repository with the code and a webpage[2] displaying the final proofs will be created.

We will now present the general method to construct the Euclidean proof. The small cases $k = 1, 2, 3, 4, 6$ are degenerate, and we shall not consider them here. They are discussed in **??** in the Appendix for completeness.

1.1 Building the proof

In order to build the Euclidean proof, it is enough to follow **??**. As we said before, all the technical steps needed to obtain the proof in **??** will be replaced by simple checks. In fact, the only obstacle we will face when trying to build the proof will be justifying that our Euclidean polynomial f_u has all its prime divisors $\equiv 1, \ell \pmod{k}$ (except for finitely many). We will assume this to be true, and prove this property of f_u separately afterwards (following the ideas in **??**).

It will be illustrative to go through a representative example and see how the proof has been built using the results in the previous sections, together with the SageMath functions that effectively implement it (which are hosted in the mentioned Git repository). The boxed paragraphs contain the actual proof generated by our automatic program.

We will start with a case where $\ell \not\equiv 1 \pmod{k}$. Consider the arithmetic progression $\equiv 4 \pmod{15}$ (note that it satisfies Murty's condition[3]). We begin the proof by simply

[1] The code that generates the automatic proofs can be found in **??** in the Appendix. See also this section to understand how Python and LaTeX have been combined to produce these proofs.

[2] Access https://github.com/joarca01/final-math-bsc-thesis to visit the Git repository with the code, and http://167.172.185.115, to access the webpage.

[3] Our webpage can return a list of all the possible values of ℓ that satisfy $\ell^2 \equiv 1 \pmod{k}$, given a

stating what polynomial to consider (this polynomial is obviously the irreducible polynomial f_u in **??**, yet the subscript u is dropped):

> We will prove that the arithmetic progression $\equiv 4 \pmod{15}$ contains infinitely many primes. Equivalently, we will see that there are infinitely many primes of the form $15n+4$, $n \geqslant 0$. For this purpose, consider the polynomial
>
> $$f(x) := x^4 + 883x^3 + 292728x^2 + 43186723x + 2392743361.$$

This polynomial is built using the 15th primitive root of unity $\zeta := e^{2\pi i/15}$ and the coset representatives of $H = \{1, 4\}$ in $G = (\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$, which are $1, 2, 7$ and 11. Also, it suffices to choose $u = 15$ to satisfy **??** and **??** (since u is now fixed, the subscript of f_u is dropped). The SageMath functions that implement these calculations are coprimes, coset_reps, f_polynomial_roots and polynomial. We then write:

> Suppose there are finitely many primes $\equiv 4 \pmod{15}$ and denote them by $p_1, p_2, \ldots, p_m$. Since $19 \equiv 4 \pmod{15}$, we can write the list as $19, p_2, p_3, \ldots, p_m$ (so $p_1 = 19$). Now, let $Q := 2 \cdot 3 \cdot 5 \cdot 17 \cdot 239 \cdot p_2 p_3 \cdots p_m$. Consider the following congruence equation system:
>
> $$\begin{cases} c \equiv 7 \pmod{19^2} \\ c \equiv 0 \pmod{15Q}. \end{cases}$$
>
> The Chinese Remainder Theorem guarantees the existence of $c \in \mathbb{Z}$ that is a solution to the above system since 19 does not divide $15Q$. It follows that
>
> $$f(c) \equiv f(7) = 2709699364 \equiv 19 \cdot 8 \pmod{19^2},$$
>
> $$f(c) \equiv f(0) = 61 \cdot 39225301 \pmod{15Q}.$$
>
> In particular, observe that the prime $p_1 = 19$ divides $f(c)$, but 19^2 does not.

In order to keep the structure of a Euclidean proof, we first reproduce the contradiction argument of **??**, proving the required properties of f later on in the proof. Observe that we effectively compute the integer b guaranteed by **??** through the function find_b_value. Also, the prime $p \equiv 4 \pmod{15}$ (not dividing $\Delta(f) = 2^6 \cdot 3^8 \cdot 5^6 \cdot 17^2 \cdot 239^2$) which we suppose exists by hypothesis is calculated with find_prime and added as the first term of the list of primes $\equiv 4 \pmod{15}$. Note that we know that such a prime exists due to Dirichlet **??** and the fact that $\Delta(f)$ has finitely many prime divisors. We also look for any other primes $p' < p$ satisfying $p' \equiv 4 \pmod{15}$ with the function prev_primes. If they existed, we would also add them to the list (in the case considered no such primes exist).

Observe how both the existence of the integer b and the prime p needed to be proved or added as a hypothesis in **??**, respectively. However, in this section we do not need these theoretical results. Once k and ℓ are fixed, only a few lines of code are needed to obtain the values of p and b.

Note that the first five terms of Q are the prime divisors of $\Delta(f)$. Note that for this we need the explicit factorization of k and $\Delta(f)$. Also, $f(7) \bmod 19^2$ has been factored this way to clearly show that it is divisible by 19 but not by 19^2. Furthermore, $f(0)$ is explicitly

value of k.

factored into primes, resulting in $f(0) = 61 \cdot 39225301$. All these factorizations use the built-in SageMath method factor, which should in principle work smoothly. However, as k gets bigger, $\Delta(f)$ and $f(0)$ become very large, ultimately making it impossible for SageMath to work out their factorization and, thus, this part of the proof no longer works. This hindrance will be further analysed —and solved— in Section 1.2.

Next, we prove that every prime that divides $f(c)$ is $\equiv 1 \pmod{15}$ (except for $p_1 = 19$). Here we strongly use **??** and the fact that $f(0)$ is only divisible by primes $\equiv 1 \pmod{15}$.

Lemma. *Every prime that divides $f(c)$ is $\equiv 1 \pmod{15}$ (except for $p_1 = 19$).*

Proof. Let r be a prime divisor of $f(c)$ different from 19. We will later establish that $r = 2, 3, 5, 17, 239$ or $r \equiv 1, 4 \pmod{15}$. For now, we will assume this is true. To reach a contradiction, suppose $r \not\equiv 1 \pmod{15}$. Thus, $r \equiv 4 \pmod{15}$ or $r = 2, 3, 5, 17, 239$, so r divides $15 \cdot 2 \cdot 3 \cdot 5 \cdot 17 \cdot 239 \cdot p_2 p_3 \cdots p_m = 15Q$. Since $f(c) \equiv 61 \cdot 39225301 \pmod{15Q}$ and r is a divisor of $15Q$, we deduce that $f(c) \equiv 61 \cdot 39225301 \pmod{r}$. But r is a divisor of $f(c)$, so $f(c) \equiv 0 \pmod{r}$. Therefore, $61 \cdot 39225301 \equiv 0 \pmod{r}$. Thus, it must happen that $r = 61, 39225301$, which are $\equiv 1 \pmod{15}$. This forces r to be $\equiv 1 \pmod{15}$, a contradiction. Therefore, $f(c)$ is only divisible by primes $\equiv 1 \pmod{15}$ (and by $p_1 = 19$). □

Note that the primes $r = 2, 3, 5, 17, 239$ are the prime divisors of k and $\Delta(f)$, which are the only possible prime divisors of f not $\equiv 1, 4 \pmod{15}$, as described in **??**. Moreover, the primes $61, 39225301$ are $\equiv 1 \pmod{15}$, which we know will happen in general because in **??** we saw that $f(0) = \Phi_{15}(15) \equiv 1 \pmod{15}$, and we deduced that every prime divisor of $f(0)$ is $\equiv 1 \pmod{15}$. Finally, the contradiction argument is concluded:

Finally, from the fact that $f(c)$ has every prime divisor $\equiv 1 \pmod{15}$ except for $p_1 = 19$ it follows, mod 15, that $f(c) = 1 \cdot 1 \cdots 1 \cdot 4 = 4$ (note that 4 only appears once because $p_1 = 19 \equiv 4 \pmod{15}$ and the fact that 19^2 does not divide $f(c)$). However, observe that $f(c) \equiv f(0) \equiv 1 \pmod{15}$. This is a contradiction. Therefore, the arithmetic progression $\equiv 4 \pmod{15}$ contains infinitely many primes.

We still need to prove the properties that make f suitable for our proof of the infinitude of primes $\equiv 4 \pmod{15}$:

To complete the proof we must justify that every prime divisor p of $f(c)$ either belongs to the finite set

$$T := \{2, 3, 5, 17, 239\} \tag{1.1}$$

or satisfies $p \equiv 1, 4 \pmod{15}$.

To prove the above statement we consider a set S, which is conveniently chosen to be the list of coset representatives of H in G. Since we are interested in calculating the discriminant of f, we write the definition of f in **??**, explicitly showing its roots:

Consider the set $S := \{1, 2, 7, 11\}$ and the values $h(\zeta^s) := (\zeta^s - 15)(15 - \zeta^{4s})$, with $s \in S$ and $\zeta := e^{2\pi i/15}$, a 15th primitive root of unity (thus a root of Φ_{15}). A simple calculation shows that f can be written as

$$f(x) = \prod_{s \in S} (x - h(\zeta^s)) = x^4 + 883x^3 + 292728x^2 + 43186723x + 2392743361. \tag{1.2}$$

After this, we just calculate the discriminant of f with the Sage discriminant method and begin the proof of Eq. (1.1) by supposing that p is a prime divisor of f not dividing $\Delta(f)$ or $k = 15$, that is:

Now, suppose that p is a prime divisor of f such that p does not belong to T.

Next, the argument follows exactly **??**, inserting $\ell = 4$ where necessary:

Next, consider a field $\mathbb{F}$ containing both the finite field $\mathbb{F}_p$ and ζ^a. Since p divides f, working in $\mathbb{F}$, there exists $a \in \mathbb{Z}$ such that

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

Since $\mathbb{F}$ is a field, there exists some $s \in S$ such that $a = h(\zeta^s)$.

Lemma. *The equality $h(\zeta^s) = h(\zeta^{ps})$ holds in $\mathbb{F}$.*

Proof. Observe that the following calculation holds in $\mathbb{F}$:

$$\begin{aligned} h(\zeta^s) = a = a^p = h(\zeta^s)^p &= (\zeta^s - 15)^p (15 - \zeta^{4s})^p \\ &= (\zeta^{ps} - 15^p)(15^p - \zeta^{4ps}) = (\zeta^{ps} - 15)(15 - \zeta^{4ps}) = h(\zeta^{ps}), \end{aligned} \tag{1.3}$$

where we have used Fermat little theorem in the second equality. The fifth equality, on the other hand, relies on the fact that $\mathbb{F}$ has characteristic 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. (1.3) means that $h(\zeta^{ps}) = h(\zeta^s)$ is a root of $\overline{f} \in \mathbb{F}[x]$.

Lemma. *$h(\zeta^{ps})$ is also a root of f in $\mathbb{Q}(\zeta)$ (the smallest subfield of $\mathbb{C}$ containing ζ).*

Proof. Begin by noting that the value $h(\zeta^{ps})$ only depends on the value of ps mod 15 since it only appears as an exponent of ζ. Since p does not divide 15 and s is coprime to 15, ps is coprime to 15 (so ps mod 15 is coprime to 15), and hence ζ^{ps} is a primitive 15th root of unity.

There are now only two options: either ps mod 15 lies in S or ps mod 15 does not lie in S. In the first case, $h(\zeta^{ps})$ is a root of f, observing expression Eq. (1.2). In the latter case, note that every integer ps mod 15 relatively prime to 15 not in S satisfies $ps \equiv 4t \pmod{15}$ for some $t \in S$ (for instance, if ps mod $15 = 13$, pick $t = 7 \in S$ so that $13 \equiv 4 \cdot 7 \pmod{15}$). This means that $h(\zeta^{ps}) = h(\zeta^{4t})$. Let us prove that $h(\zeta^{4t}) = h(\zeta^t)$, so $h(\zeta^{ps}) = h(\zeta^{4t}) = h(\zeta^t)$ is also a root of f. Indeed,

$$\begin{aligned} h(\zeta^{4t}) &= (\zeta^{4t} - 15)(15 - \zeta^{4^2 t}) = (\zeta^{4^2 t} - 15)(15 - \zeta^{4t}) \\ &= (\zeta^t - 15)(15 - \zeta^{4t}) = h(\zeta^t), \end{aligned}$$

where we have used that $\zeta^{4^2 t}$ only depends on the value of $4^2 t \bmod 15$ and the fact that $4^2 \equiv 1 \pmod{15}$. Therefore, $h(\zeta^{ps}) = h(\zeta^t)$ is always a root of f in $\mathbb{Q}(\zeta)$. □

[a]For instance, consider $\mathbb{F} = \mathbb{F}_{p^n}$ with a suitable integer $n \geqslant 1$ such that Φ_{15} has a root ζ.

In the lemma above we choose some element $ps \bmod 15$ to give an example. We precisely pick the second-to-last element of the set formed by the elements of $G = (\mathbb{Z}/15\mathbb{Z})^\times$ not in S, which in this case is 13. Next, to find a suitable $t \in S$ such that $13 \equiv 4t \pmod{15}$ we use the function try_reps_list. We then continue with:

Lemma. *$h(\zeta^{ps})$ and $h(\zeta^s)$ are the same root of f in $\mathbb{Q}(\zeta)$.*

Proof. If $h(\zeta^{ps})$ and $h(\zeta^s)$ were two distinct roots of f in $\mathbb{Q}(\zeta)$, we know because of Eq. (1.3) that they would be the same in $\mathbb{F}$. Therefore, observing expression **??**, it follows that $\Delta(f \bmod p) = \Delta(f) \bmod p = 0$, so p divides $\Delta(f) = 2^6 \cdot 3^8 \cdot 5^6 \cdot 17^2 \cdot 239^2$. This is a contradiction with our choice of p. Thus, $h(\zeta^{ps})$ and $h(\zeta^s)$ are in fact the same root of f in $\mathbb{Q}(\zeta)$. □

Therefore, the equality

$$h(\zeta^{ps}) = (\zeta^{ps} - 15)(15 - \zeta^{4ps}) = (\zeta^s - 15)(15 - \zeta^{4s}) = h(\zeta^s)$$

holds in $\mathbb{Q}(\zeta)$.

Up to this point, the proof of **??** has been strictly followed. In order to keep the proof as simple as possible, we avoid using any Galois Theory, so we instead continue the proof as follows:

Next, write the above equation in terms of $\theta := \zeta^s$ and multiply both sides by -1. This changes yield

$$\begin{aligned} 225 - 15(\theta^p + \theta^{4p}) + \theta^{(1+4)p} &= 225 - 15(\theta + \theta^4) + \theta^{1+4}, \\ -15(\theta^p + \theta^{4p}) + \theta^{5p} &= -15(\theta + \theta^4) + \theta^5. \end{aligned} \tag{1.4}$$

The right-hand side of the equation above does not depend on p. The left-hand side only depends on the value of $p \bmod 15$, since p only appears as an exponent of θ. The above equality gives information about p, which is what we are interested in.

We will translate the equality in Eq. (1.4) in $\mathbb{Q}(\theta)$ to an equality of polynomials, which can be easily handled. We will see that the fact that Eq. (1.4) holds implies that $p \bmod 15$ belongs to $H := \{1, 4\}$.

To prove this, we will check every value of p such that $p \bmod 15$ does not belong to H and conclude that Eq. (1.4) is not true in $\mathbb{Q}(\theta)$ in those cases. Therefore, we shall see the following: if $p \bmod 15$ belongs to $G \setminus H = \{2, 7, 8, 11, 13, 14\}$, then $-h(\theta^p) \neq -h(\theta)$. This will automatically imply what we want to prove: since Eq. (1.4) holds, $p \bmod 15$ lies in H. To see this, rewrite Eq. (1.4) as

$$-15(\theta^p + \theta^{4p}) + \theta^{5p} + 15(\theta + \theta^4) - \theta^5 = 0 \tag{1.5}$$

and trade θ for x, since the condition Eq. (1.5) in $\mathbb{Q}(\theta)$ is equivalent to the condition

$$-15(x^p + x^{4p}) + x^{5p} + 15(x + x^4) - x^5 = 0 \tag{1.6}$$

in $\mathbb{Q}[x]/(\Phi_{15}(x)) \cong \mathbb{Q}(\theta)$ (Φ_{15} is also the minimal polynomial of θ, since $\theta = \zeta^s$ is a primitive 15th root of unity). We will explicitly write the case $p = 2 \bmod 15$ (the remaining values of $p \bmod 15$ in $G \setminus H$ are left as an exercise to the reader). With this value of p, equation Eq. (1.6) becomes

$$\begin{aligned} A(x) &:= -15(x^2 + x^8) + x^{10} + 15(x + x^4) - x^5 \\ &= x^{10} - 15x^8 - x^5 + 15x^4 - 15x^2 + 15x = 0. \end{aligned}$$

In the text above, we took the first element in $G \setminus H$ and built the final polynomial $A(x)$ with dividend_check. We want to see that $A(x) = 0$ is not true, so we will make use of the fact that $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(\Phi_{15})$ to reduce our problem to showing that $A(x)$ is not a multiple of the 15th cyclotomic polynomial, which will mean that Eq. (1.4) is not true:

If we recall that $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(\Phi_{15})$, the above equation is equivalent to $A(x)$ being a multiple of the 15th cyclotomic polynomial, $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$. Therefore, we are interested in showing that the residue $R(x)$ of the division $A(x)/\Phi_{15}(x)$ satisfies $R(x) \neq 0$, from which our result will follow. A simple Euclidean division of polynomials shows that $A(x) = B(x) \cdot \Phi_{15}(x) + (-15x^7 + 13x^5 + 15x^3 - 15x^2 + 14)$, with $B(x)$ a polynomial of degree 2, so $R(x) = -15x^7 + 13x^5 + 15x^3 - 15x^2 + 14 \neq 0$. Therefore, equality Eq. (1.4) implies that $p \bmod 15$ belongs to H, that is, $p \equiv 1, 4 \pmod{15}$.

This calculation involves the quo_rem and degree SageMath methods. This concludes the proof of the properties of f and, therefore, of the Euclidean proof that there exist infinitely many primes $\equiv 4 \pmod{15}$.

Remark 1.1. If one reads Murty's article [**Murty**], they will notice that the proof he gives for the progression $\equiv 4 \pmod{15}$ is very different from the one we just gave, which is nevertheless based on the ideas developed in his article. He instead uses a much simpler argument, taking advantage of the Quadratic Reciprocity Law. In **??** in the Appendix we explain why his approach for the case $\equiv 4 \pmod{15}$ does not always work for a general progression $\equiv \ell \pmod{k}$ satisfying $\ell^2 \equiv 1 \pmod{k}$.

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

In **??** we treated the case $\ell \equiv 1 \pmod{k}$ separately. The proof we will give now is an adapted version of **??**. No contradiction argument supposing the existence of finitely many primes $\equiv 1 \pmod{k}$ is needed. In fact, it will suffice to give a proof of the type of prime divisors of Φ_k, together with an extra property of this polynomial. Therefore, following **??**, in this case we need to consider our polynomial f to be Φ_k. To fix ideas, take $k = 21$ and $\ell = 1$ and begin by stating:

Consider the polynomial

$$\Phi_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1.$$

We will specifically show that every prime divisor p of Φ_k either belongs to the finite set

$$T := \{3, 7\}$$

or satisfies $p \equiv 1 \pmod{21}$. To see this, consider the set $S := \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ and the values ζ^s, with $s \in S$ and $\zeta := e^{2\pi i/21}$, a 21st primitive root of unity (thus a root of Φ_{21}). A simple calculation shows that Φ_k can be written as

$$\Phi_{21}(x) = \prod_{s \in S} (x - \zeta^s) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1.$$

Again, we compute the discriminant of this polynomial and suppose p is a prime divisor of Φ_{21} such that p does not lie in T. This set has been conveniently defined to contain the divisors of k, that are the only possible prime divisors of Φ_{21} which are not $\equiv 1 \pmod{21}$, as shown in **??**.

We now follow the proof in that Proposition, adapting it for the case $k = 21$ where necessary. Once the fact that $\zeta^{ps} = \zeta^p$ is settled, it is immediate to establish that every prime divisor of Φ_{21} either belongs to T or satisfies $p \equiv 1 \pmod{21}$.

This, together with the fact that Φ_{21} has infinitely many primes (see **??**[4]) already implies that the arithmetic progression $\equiv 1 \pmod{21}$ contains infinitely many primes.

1.2 Program's operational limit

While no theoretical limit exists, there is a practical limit to the utility of the Euclidean proofs we presented in Section 1.1. In particular, the argument relies on factoring the values of $\Delta(f)$ and $f(0)$ into primes. On one hand, the value of Q at the beginning of the proof is defined in terms of the prime divisors of $\Delta(f)$. Also, we need the explicit factorization of $\Delta(f)$ to build the set T of (possible) prime divisors of f that are not $\equiv 1, \ell \pmod{k}$. On the other hand, we need to show that every prime divisor of $f(0)$ is $\equiv 1 \pmod{k}$ to reach a contradiction and conclude that every prime divisor of $f(c)$ is $\equiv 1 \pmod{k}$, except for p_1. While we know this is true because of **??**, in order to keep the argument simple we need to explicitly show every factor of $f(0)$.

However, it becomes computationally costly to factor $\Delta(f)$ and $f(0)$ as k becomes larger, since these quantities easily become very big. Ultimately, the SageMath built-in function factor fails to factor these quantities[5]. In Table 1.1 we summarise the corresponding number of digits of $\Delta(f)$ and $f(0)$ for different values of k and ℓ (suppose $f = \Phi_k$ for the cases where $\ell = 1$).

[4]The proof of this proposition is also included in the webpage for completeness, being adapted for the case where $f = \Phi_k$.

[5]Other software (such as *Magma*) has also failed to factor big values of $\Delta(f)$ and $f(0)$.

Table 1.1: Number of digits of $\Delta(f)$ and $f(0)$ for different values of k and ℓ.

k	ℓ	**Digits of** $\Delta(f)$	**Digits of** $f(0)$
4	3	1	2
15	4	18	10
30	19	21	12
47	46	883	77
51	50	433	55
63	55	610	65
10	1	3	–
47	1	77	–
143	1	236	–

To further analyse the limit of our program[6], we will set a threshold of 2 seconds for the factorization of both $\Delta(f)$ and $f(0)$. If any of the two factorizations exceeds this threshold, a Runtime Error will be raised in the code, considering it to have failed for that case[7].

The diagrams in **??** and **??** in the Appendix **??** show how many arithmetic progressions can be effectively handled with our code, taking into account the defined threshold. In particular, the images indicate the execution time (in seconds) of the code that yields the Euclidean proof for the congruence class $\equiv \ell \pmod{k}$. The first value of k for which not every possible value of ℓ can be executed with our program under 2 seconds is $k = 47$ and $\ell = 46$. After this value of k, some more cases can still be executed until $k = 51$, where it fails again. From there onwards, the code often fails to factor $\Delta(f)$, $f(0)$ or both.

1.3 Alternative arguments

In order to bypass the setback detailed in Section 1.2, we have modified the code so that whenever a factorization fails, an alternative argument is shown in the final Euclidean proof. Our goal is to present auxiliary arguments that do not need the factorization of $\Delta(f)$ or $f(0)$, and that will only be used when one (or both) factorization fails. Although elementary, these arguments will be slightly longer and less direct than the previous ones.

Case 1: The factorization of $\Delta(f)$ (or $\Delta(\Phi_k)$) fails.

In this case, the integer Q at the very beginning of the proof needs to be built differently. Take the case $k = 55$ and $\ell = 34$.

> To prove that there exist infinitely many primes $\equiv 34 \pmod{55}$ we can proceed by contradiction. Suppose there are finitely many primes $\equiv 34 \pmod{55}$ and denote them by $p_1, p_2, \ldots, p_m$. Since $89,199 \equiv 34 \pmod{55}$, we can write the list as

[6]This practical limit only applies to the factorization of $\Delta(\Phi_k)$ in the case $\ell \equiv 1 \pmod{k}$.

[7]We have noticed that the factorization of a number with SageMath is either done very quickly or takes many seconds, if finishes at all. Therefore, we consider that 2 seconds is a reasonable limit to determine if the factorization will take very long to execute, making the program no longer useful.

$89, 199, p_3, p_4, \ldots, p_m$ (so $p_2 = 199$). Now, let t be the product of every prime divisor of the discriminant of f (denoted by $\Delta(f)$). Define $Q := t \cdot p_3 p_4 \cdots p_m$.

Also, the prime divisors exceptions in **??** are not made explicit, since they involve factoring $\Delta(f)$. Instead, we write:

Let r be a prime divisor of $f(c)$ different from 199. We will later establish that r is a prime divisor of $\Delta(f)$, of 55, or $r \equiv 1, 34 \pmod{55}$. For now, we will assume this is true.

Similarly, when proving that every prime divisor of f is either $\equiv 1, 34 \pmod{55}$ or divides $\Delta(f)$ or k, we do not make the exceptions explicit. We say:

We must justify that every prime divisor p of $f(c)$ either belongs to the finite set

$$T := \{p : p \text{ is a prime divisor of } \Delta(f) \text{ or a prime divisor of } 55\}$$

or satisfies $p \equiv 1, 34 \pmod{55}$.

If this alternative argument is needed, certainly $\Delta(f)$ is significantly long. Thus, we avoid displaying its actual value.

Case 2: The factorization of $f(0)$ fails.

In this case, we need to prove that every prime divisor of $f(0)$ is $\equiv 1 \pmod{k}$ in an alternative way. For this we use the following lemma.

Lemma 1.2. *Every prime divisor of* $\Phi_k(u) = f(0)$ *is* $\equiv 1 \pmod{k}$.

Proof. Let q be a prime divisor of $\Phi_k(u)$, so $\Phi_k(u) \equiv 0 \pmod{q}$. Now, $u^k - 1 \equiv 0 \pmod{q}$, since Φ_k divides $x^k - 1$ (observe **??**). Therefore, the order of u as an element of $(\mathbb{Z}/q\mathbb{Z})^\times$ divides k.

If the order of u is a divisor of k different from k, say k', then u is also a root of $\Phi_{k''} \bmod q$ for some divisor k'' of k', and hence of k. Thus, u is a multiple root of $x^k - 1 \bmod q$, since both Φ_k and $\Phi_{k''}$ divide $x^k - 1$. But then u would also be a root of the derivative of $x^k - 1 \bmod q$, that is, a root of $kx^{k-1} \bmod q$, because of **??**. This necessarily means that $k \equiv 0 \pmod{q}$ or $u \equiv 0 \pmod{q}$. But neither of these is possible. On one hand, the fact that $u^k \equiv 1 \pmod{q}$ means that $u \not\equiv 0 \pmod{q}$. On the other hand, since u is a non-zero multiple of k, if $k \equiv 0 \pmod{q}$, then $u \equiv 0 \pmod{q}$, which we have just seen is not possible.

Therefore, the order of u must be k. Fermat little theorem guarantees that the order of u divides the order of $(\mathbb{Z}/q\mathbb{Z})^\times$, which is $\varphi(q) = q - 1$. Thus, k divides $q - 1$. We then have $q - 1 \equiv 0 \pmod{k}$, so $q \equiv 1 \pmod{k}$. □

This is inserted in the automated proof (adapted when k is a prime, since the argument is then significantly shorter). Observe that in **??** we also proved this fact in general, without factorizing $f(0)$. However, we avoid using that argument in our automated proof because it involves knowing the prime divisors of Φ_k, so the justification would be considerably longer.

These two modifications make our code work for every value of k and ℓ satisfying $\ell^2 \equiv 1 \pmod{k}$, with the only limitation that the code may take very long to execute for large values of k.

Since our proofs involve polynomials with large coefficients, it is worth noting that some progressions can be tackled via studying progressions with smaller values of k and ℓ. Specifically, let $k = 2m$ (with m an odd integer) and ℓ identify an arithmetic progression. Note that ℓ must also be odd to satisfy $\gcd(k, \ell) = 1$. By the Chinese Remainder Theorem, a prime p will be $\equiv \ell \pmod{2m}$ if and only if $p \equiv \ell \pmod{2}$ and $p \equiv \ell \pmod{m}$. Since ℓ is odd, the first condition is equivalent to $p \equiv 1 \pmod{2}$, which is trivially satisfied by every prime (except for 2). Therefore, proving that there exist infinitely many primes $\equiv \ell \pmod{2m}$ is equivalent to showing there exist infinitely many primes $\equiv \ell' \pmod{m}$, where $\ell' := \ell \bmod m$.

This is the only case where we can reduce the study of some progression to a simpler one. Observe that a necessary condition for the above argument to work is $\varphi(k) = \varphi(2m) = \varphi(m)$, which only happens for $k = 2m$, with m odd (see **??** in **??** in the Appendix).

This case has been considered in our code. Whenever $k = 2m$ for some odd integer m, the automatic proof conveniently reduces the argument to proving that the arithmetic progression $\equiv \ell' \pmod{m}$ contains infinitely many primes.