1 Conclusions

This thesis admits two possible interpretations. If one is not interested in automated proofs, or even in Euclidean proofs, they could concentrate in reading **??** of this thesis. If such is the interest, one will be happy to learn that we have effectively characterised the set $\mathrm{Spl}_1(L)$ in terms of congruences, where L is a field lying under $\mathbb{Q}(\zeta)$ with $[\mathbb{Q}(\zeta) : L] \leqslant 2$. This set contains the primes p that have a prime ideal factor in L whose residue field is $\mathbb{Z}/p\mathbb{Z}$. This is effectively a reciprocity law, which is nevertheless hidden in Murty's method to construct Euclidean proofs. As far as the author is concerned, no such characterization was explicit in the existing literature.

The other possible interpretation to this thesis is to see it as a sort of "instruction manual" to build Euclidean proofs of the infinitude of primes in arithmetic pogressions. An intrepid reader may want to embark in understanding why these instructions work, so he will again delve into the details explained in **??**, ultimately understanding why an Euclidean proof is only possible for progressions satisfying $\ell^2 \equiv 1 \pmod{k}$. The journey towards this result will require going through Shur and Murty's theorems, and making use of advanced results like Chebotarev's Density Theorem. A more practical reader will instead pick an arithmetic progression of his choice and use the webpage to learn in an easier, Euclidean way why it contains infinitely many primes (if that is possible for the chosen progression). The final Euclidean proof is indeed easier, since harder existence theorems are replaced with mere checks once k and ℓ are fixed. Moreover, the final proof makes use of polynomials and certain numbers which have been conveniently chosen for the argument to work nicely. If the reader wants to find out how they are built, then going back to **??** is unavoidable.

Regarding this particular section, it is important to note that we have clarified some aspects in Murty's article. For example, we have made clear why the integer u in the polynomial $h_u(z)$ needs to be a non-zero multiple of k, which was not previously evident. We have also shown that Murty's approach to prove there exist infinitely many primes using QRL is not always possible, being in fact only available when L is the compositum of its quadratic subfields. Moreover, we have also corrected some innaccuracies in that same paper. This includes adding a necessary hypothesis to one of the main theorems of the article, as well as defining the polynomial $h_u(z)$ with an opposite sign.

The work we have developed here could be further expanded. For instance, it is natural to ask if there exists a characterisation, in terms of congruences, of $\mathrm{Spl}_1(L)$ in the case $[\mathbb{Q}(\zeta) : L] \leqslant n$, for $n \geqslant 3$ (and n dividing $\varphi(k) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$). As of now, no such characterisation is known. With respect to the automated proof generator, it could be investigated whether an alternative, simpler polynomial $f(x)$ can be used to proof the existence of infinitely many primes. Indeed, the polynomial $f(x)$ we propose contains large coefficients for big values of k, making the final proof somewhat hard to read. Provided a polynomial with smaller coefficients was found, no alternative arguments to bypass the factorization of $f(0)$ or $\Delta(f)$ would need to be used.