FERMAT'S LAST THEOREM FOR REGULAR PRIMES AND NON-UNIQUE FACTORIZATION

Fermat's Last Theorem's proof by Andrew Wiles was certainly one of the most exciting mathematical discoveries of the last century, if not of the entire history of mathematics. Despite its simple formulation,"the equation $x^n + y^n = z^n$ has no solutions with x, y and z non-zero integers and $n \geq 3$", it remained an open problem, getting attention of several brilliant mathematicians, for three and half centuries.

A great deal of progress was made during the nineteenth century when Germain, Dirichlet, Legendre, Kummer, Lamé and Cauchy worked actively on the problem.

When working on FLT, Kummer factored the equation $z^p - y^p$ and faced a problem: when dealing with cyclotomic integers, unique factorization, a major tool, fails for all primes bigger than 23! This lead to two important definitions in Number Theory:

- *ideal numbers*: to make up for the lack of unique factorization,
- *the class number*: to measure how badly unique factorization fails.

Kummer then gave a proof of FLT for regular primes, i.e., primes p that do not divide the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$.

The goal of this Bachelor project is to study the proof of Fermat's Last Theorem for n=4 and for regular primes as well as the concepts behind it, such as that of ideal numbers, reformulated by Dedekind as "ideals" and class number.

This project is recommended to students who followed the course on Algebraic Number Theory, although it can certainly be adapted for those who did not.

References

[1] Ribemboim, Paulo. "13 Lectures on Fermat's Last Theorem." *Springer Verlag, Berlin Heidelberg New York, 1986.*

[2] "Introduction to Fermat's Last Theorem". *math.stanford.edu/ lekheng/flt/cox.pdf*