PRIMES OF THE FORM $x^2 + ny^2$

ELISA LORENZO GARCÍA

Most first courses in Number Theory prove the following statement concerning an odd prime number p:

$$p = x^2 + y^2, \text{ for some } x, y \in \mathbb{Z} \Longleftrightarrow p \equiv 1 \bmod 4.$$

This is only one of the many cases treated in Fermat's works on the more general problem

Question 0.1. *Given a positive integer n, which prime numbers p can be expressed in the form*

$$x^2 + ny^2$$

for some integer numbers x, y?

First, we will study some elemental approaches to the problem following Fermat, Euler, Lagrange, Legendre and Gauss. We will do this via the study of binary quadratic forms and (quadratic, cubic) reciprocity laws. This first approach will solve many cases, but soon, we will realize that, as very frequently happen in Number Theory, a very naive (elementary) statement hides really hard mathematics.

Our second approach will be use Class Field Theory. We will define the Hilbert class field and we will study the orders of the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$. Finally, we will summarize the main theorems of class field theory and Cebotarev Density Theorem.

If time allows us, we will also take a brief look to the connections to this problem and the really nice theory of the Complex Multiplication.

References. David A. Cox, *Primes of the form x^2+ny^2: Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons, Inc. (1989).