

Representation of primes as the sums of two squares in the golden section quadratic field*

Michele Elia[†]

Politecnico di Torino

Dipartimento di Elettronica

Corso Duca degli Abruzzi 24

10129 Torino

Italy

Abstract

In the quadratic number field with the golden section unit, any prime p has associated primes that are the sums of two integer squares, if and only if its field norm $N(p)$ is not a rational prime congruent to 11 or 19 modulo 20. A proof of this property is presented, along with a method for computing the two squares with deterministic polynomial complexity, that is, using a number of arithmetical operations proportional to a power of $\log_2 N(p)$ of bounded exponent.

Keywords : Golden section, real quadratic fields, polynomial complexity.

1. Introduction

Fermat stated that every rational prime p congruent to 1 modulo 4 is the sum of two squares of natural numbers. Fermat's theorem has received many proofs [22, p. 66], although early ones did not offer a method of deterministic polynomial complexity for computing the representation $p = s^2 + r^2$, i.e. one using a number of sums and products proportional to some small power of the logarithm of p . However, a reduction algorithm of binary quadratic forms, which can be traced back to Gauss [6], produces

*Presented at XXIVième Journées Arithmétiques, Marseille (FR), July 4-8, 2005.

[†]E-mail: eliamike@tin.it

Journal of Discrete Mathematical Sciences & Cryptography

Vol. 9 (2006), No. 1, pp. 25–37

© Taru Publications