NUMBERS WHICH ARE THE SUM OF TWO SQUARES

RAJIV NELAKANTI

1. Introduction

Euler's paper "On numbers which are the sum of two squares" [E228] pertains to multiplicative properties between two sums of two squares. For readability, we will shorten a number that can be written as a sum of two squares to a SOTS.

2. Background

There are a few lemmas necessary to complete the proofs we will demonstrate here. Since these are covered in papers of partners of the presenter (Archie, Jon), we will solely state them without full proof.

Theorem 2.1. *If p, q are both SOTSs, then pq is a SOTS.*

Euler centers his paper around this first theorem. He then proves several propositions stemming from this theorem.

Lemma 2.2. *Proposition I. If the product pq is a SOTS and p is a prime SOTS, then q is also a SOTS.*

Lemma 2.3. *Proposition II. If the product pq is a SOTS and q is not a SOTS, then there exists some prime factor $r \mid p$ such that r is not a SOTS.*

3. Proposition III

Theorem 3.1. *If $a^2 + b^2$ is a SOTS with $gcd(a, b) = 1$ and has prime divisor p, one can generate a SOTS $c^2 + d^2 \leq \frac{1}{2}p^2$ which is divisible by p.*

Proof. Given $a^2 + b^2$ and p, we can pick integers m, n and $c, d \leq \frac{1}{2}p$ such that $a = mp \pm c$ and $b = np \pm d$ since neither a nor b is divisible by p. Then $a^2 + b^2 = m^2p^2 \pm 2mcp + c^2 + n^2p^2 \pm 2ndp + d^2$. Since p divides this entire expression and p is clearly a divisor of $m^2p^2 \pm 2mcp + n^2p^2 \pm 2ndp$, the remaining portion $c^2 + d^2$ must also be divisible by p. Since $c^2, d^2 \leq (\frac{1}{2}p)^2$, we have that $c^2 + d^2 \leq \frac{1}{2}p^2$. ■

We'll call a SOTS $a^2 + b^2$ satisfying $gcd(a, b) = 1$ a 'relatively prime SOTS' for simplicity's sake.

Corollary 3.2. *Resultingly, if there is no relatively prime SOTS divisible by p less than or equal to $\frac{1}{2}p^2$, then there is no relatively prime SOTS divisible by p at all.*

Euler then provides 3 and 7 as examples of possible such p.

4. Proposition IV

Theorem 4.1. *Any divisor of a relatively prime SOTS $a^2 + b^2$ is also a SOTS.*

Proof. Suppose there exists p dividing $a^2 + b^2$ that is not a SOTS. By Theorem 3.1, we can generate a relatively prime SOTS $c^2 + d^2 = pq \leq \frac{1}{2}p^2$. Since p is not a SOTS, q has a factor r that is also not a SOTS. Since $pq \leq \frac{1}{2}p^2$, $q \leq \frac{1}{2}p$ and $r \leq \frac{1}{2}p$. Then, given $c^2 + d^2$ and r we can generate another SOTS $e^2 + f^2 \leq \frac{1}{2}r^2 \leq \frac{1}{8}p^2$. Since r is not a SOTS, we can continue in this fashion. We keep generating smaller and smaller SOTS that must have a divisor which is not a SOTS, but as Euler puts it:

"Because there is no sum of two squares prime between themselves among the smallest numbers and divisible by a number that is not the sum of two squares, neither among the greatest numbers will there be such sums of two squares which are divisible by numbers that are not themselves sums of two squares." ■

Corollary 4.2. *We have provided a converse statement to Theorem 2.1 provided that the SOTS is relatively prime.*

Corollary 4.3. *We can compose a list of primes L such that any SOTS must either lie in L or must be a product of some elements of L. Euler computes out the first few primes* $L = \{2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, \ldots\}$.

Although Euler notes that this list appears to be of all primes congruent to 1 modulo 4, he is unable flesh out a full proof that every prime $4n + 1$ is a SOTS in this paper.