2020

An enticing study of prime numbers of the shape ? = ?^2 + ?^2

Xiaona Zhou
CUNY New York City College of Technology

An enticing study of prime numbers of the shape $p = x^2 + y^2$

Xiaona Zhou
Emerging Scholars Program
Mentor: Professor Satyanand Singh

Abstract

We will study and prove important results on primes of the shape $x^2 + y^2$ using number theoretic techniques. Our analysis involves maps, actions over sets, fixed points and involutions. This presentation is readily accessible to an advanced undergraduate student and lay the groundwork for future studies.

Background

Theorem:
Let $p > 2$ be a prime integer. Then p can be written as $p = a^2 + b^2 \Leftrightarrow p$ is of the form $p = 4k + 1$.

The theorem was posited by Albert Girard in 1625 and again by Fermat in 1640. Euler was the first one to proof this theorem. Many mathematicians have proved this theorem using different methods. This project is taken from a book called "An Open Door to Number Theory.". The whole project consists of 13 exercises, and when we proved all the exercises, we would have proved the theorem. This project is an extension of Zagier's one sentence proof.

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

D. Zagier
Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x, y, z) \mapsto \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{if } x < y - z \\ (2y - x,\ y,\ x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y,\ x - y + z,\ y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \mapsto (x, z, y)$ also has a fixed point. □

Prove the Forward Implication

Theorem 0.1. *Let $p > 2$ be a prime integer. If p can be written as $p = a^2 + b^2$, then p is of form $p = 4k + 1$.*

1 Proof of the forward implication.

Proof. $p > 2$ is a prime integer, which means p is odd. $p = a^2 + b^2$; a^2 and b^2 must be one odd integer and one even integer. Let a^2 be an odd integer. Therefore, a is odd, and $a = 2x + 1$, where $x \in \mathbb{N}$. Let b^2 be an even integer. Therefore, b is even, and $b = 2m$, where $m \in \mathbb{N}$.
$p = a^2 + b^2 = (2x + 1)^2 + (2m)^2 = 4x^2 + 4x + 1 + 4m^2 = 4(x^2 + x + m^2) + 1$
Since $x, m \in \mathbb{N}$, $(x^2 + x + m^2) \in \mathbb{N}$. Therefore, $p = a^2 + b^2 = 4k + 1$, where $k = (x^2 + x + m^2) \in \mathbb{N}$. □

More Proofs

2 Proof that if p is of the form $p = 1+4k$, then the point (1,1,k) is a fixed point for f. Conclude that $p = 4k + 1 \Leftrightarrow$ the function $f : S \to S$ has a fixed point.

define a map $f : \mathbb{N}^3 \to \mathbb{N}^3$ by

$$f(x, y, z) = \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } 2y < x \end{cases} \quad (1)$$

(1). Proof that $p = 4k + 1 \to$ the function $f : S \to S$ has a fixed point.
(2). Proof that $f : S \to S$ has a fixed point $\to p = 4k + 1$

Proof.

Case 1. When $x < y - z$, $f(x, y, z) = (x + 2z, z, y - x - z) = (x, y, z)$. That is

$$\begin{cases} x + 2z = x \\ z = y \\ y - x - z = z \end{cases}$$

solve the system of equations:

$$\begin{cases} x = 0 \\ y = 0 \\ z = 0 \end{cases}$$

Since $x, y, z \in \mathbb{N}$, and $p = x^2 + 4yz$, this is not a solution. Therefore, f does not has a fixed point when $x < y - z$.

Case 2. When $y - z < x < 2y$, $f(x, y, z) = (2y - x, y, x - y + z) = (x, y, z)$. That is

$$\begin{cases} 2y - x = x \\ y = y \\ x - y + z = z \end{cases}$$

solve the system of equations:

$$\begin{cases} x = y \\ \text{z is free} \end{cases}$$

Since $x, y, z \in \mathbb{N}$, and $p = x^2 + 4yz$. $p = x^2 + 4xz = x(x + 4z)$. Therefore,

$$\begin{cases} x = p, x + 4z = 1 \\ x = 1, x + 4z = p, \end{cases}$$

Since $x \neq p$, we further define the solution as

$$\begin{cases} x = 1 \\ y = 1 \\ z = \frac{p-1}{4} \end{cases}$$

That is, $(1, 1, \frac{p-1}{4})$ is a fixed point for f. Therefore, $p = 4k + 1$, where $k \in \mathbb{N}$

Case 3. When $2y < x$, $f(x, y, z) = (x - 2y, x - y + z, y) = (x, y, z)$. That is

$$\begin{cases} x - 2y = x \\ x - y + z = y \\ y = z \end{cases}$$

solve the system of equation:

$$\begin{cases} x = 0 \\ y = 0 \\ z = 0 \end{cases}$$

Since $x, y, z \in \mathbb{N}$, and $p = x^2 + 4yz$, this is not a solution. Therefore, f does not has a fixed point when $x < y - z$.

□

3 We now define $g : \mathbb{N}^3 \to \mathbb{N}^3$ by $g(x, y, z) = (x, z, y)$. Proof that g also maps S to itself, and that it is an involution on S. Conclude that S has a fixed point under g, which must be the form of (a, c, c). Show that this gives the desired solution: $p = a^2 + (2c)^2$. In fact you have shown the stronger statement that a prime p is of the form $p = 4k + 1 \implies p$ can be written uniquely as $p = a^2 + b^2$.

(1). Proof that g also maps S to S.

Proof. Since $g(x, y, z) = (x, z, y)$ and $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$

$$\begin{aligned} g(x, y, z) &= (x, z, y) \\ g(S) &= g(x, y, z) \\ &= x^2 + 4zy \\ &= x^2 + 4yz = p \end{aligned}$$

That is $g(S) = S$. Therefore, g maps S to itself, and it is an involution on S. □

(2). Proof that if S has a fixed point under g, then it must be of the form (a, c, c).

Proof. S has a fixed point under g when $g(x, y, z) = (x, z, y) = (x, y, z)$. Solved the equation, we have

$$\begin{cases} x = x \\ y = z \\ z = y \end{cases}$$

Therefore, a fixed point must be of the form (a, c, c). That is $S_1 = \{(a, c, c) : a^2 + (2c)^2 = p\}$ where $S_1 \in S$.
From Exercise 8, we know that

$$p = 4k + 1 \Leftrightarrow the function f : S \to S has a fixed point.$$

From this exercise we know that when S has a fixed point, $p = a^2 + (2c)^2$. That is the same as $p = a^2 + b^2$, where $b = 2c$. Therefore, we have proved that $p = 4k + 1 \implies p$ can be written uniquely as $p = a^2 + b^2$ □

Selected references

- Campbell, Duff. An Open Door to Number Theory. MAA Press, an Imprint of the American Mathematical Society, 2018.
- "Leonhard Euler." *Wikipedia*, Wikimedia Foundation, 18 Oct. 2019, en.wikipedia.org/wiki/Leonhard_Euler.
- Zagier, Don. *A One-Sentence Proof That Every Prime $p\Equiv 1(\Mod 4)$ Is a Sum of Two Squares Author(s): D. Zagier*. 2011, A One-Sentence Proof That Every Prime $p\equiv 1(\mod 4)$ Is a Sum of Two Squares Author(s): D. Zagier.