Implementing a Constructive Proof of Fermat's Christmas Theorem in Java

Leopoldo Kraus, Gabriel Scott, Sundarram Singaram

Advisor: Dr. Steven Gubkin, PhD

Cleveland State University

INTRODUCTION

The sum of two squares theorem is an essential proposition in the domain of number theory. Devised on December 25, 1640, by the prominent French mathematician, Pierre de Fermat, this theorem is also known as *Fermat's Christmas Theorem*. This mathematical proposition affirms that if a prime number is equivalent to one modulo four (in other words, has a remainder of one after being divided by four), it can be written as the sum of the squares of two distinct integers. The two key elements that this theorem is composed of are Gaussian integers and the Euclidean Algorithm.

ABSTRACT

In pure mathematics, the study of prime numbers is a fundamental component of number theory. Prime numbers serve important utilizations in the modern world, such as the operation of computer cryptography. The gifted French mathematician, Pierre de Fermat, extensively researched and studied prime numbers, allowing him to formulate the sum of two squares theorem, informally referred to as "Fermat's Christmas Theorem." This theorem argues that if a prime number is equal to one modulo four, it can be written as the sum of two squares. The primary objective of this project is to assess and prove the sum of two squares theorem, using the Euclidean Algorithm along with Java Programming. A Java program is written in order to demonstrate this theorem, by asking a user to enter a prime number, and returning the two integers, whose sum after squaring each integer, is equal to that prime number.

OBJECTIVES

- Understand the principal ideas and mathematical components that constitute the sum of two squares theorem.
- Construct a Java program in order to prove this theorem and demonstrate how it works, with effective examples.
- Explain why this theorem is practical in the mathematical world.

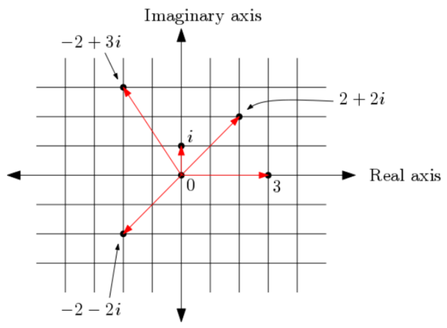

Figure 1: Gaussian integers are the set of imaginary numbers, known as a + bi, where a is called the 'real part' and b is called the 'imaginary part.' The "norm" of a gaussian integer is the square of its length (as a vector): N(a + bi) = a^2 + b^2.

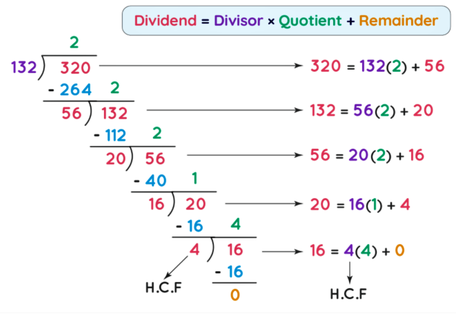

Figure 2: The Euclidean Algorithm is a method used to compute the greatest common divisor (gcd) between two integers. It states that the gcd of two integers is equal to the gcd of the smaller integer of the two and the remainder after dividing the two integers. This process is repeated until a zero remainder is obtained.

Find $\gcd(7+17i, 8-14i)$. First apply the division algorithm:

$$\frac{\alpha}{\beta} = \frac{7+17i}{8-14i} = \frac{(7+17i)(8+14i)}{8^2+14^2} = \frac{-7+9i}{10}$$

Click to add text

so we choose

$$\gamma = -1+i \implies 7+17i = (-1+i)(8-14i)+1-5i$$

Applying again:

$$\frac{8-14i}{1-5i} = \frac{(8-14i)(1+5i)}{26} = 3+i \in \mathbb{Z}[i] \implies \gcd(7+17i, 8-14i) = 1-5i$$

Figure 3: Euclidean Algorithm for Gaussian integers

CODE AND OUTPUT

```
    else if(prime % 4 == 3){
      System.out.println("Sorry " + prime +
                         " cannot be written as the sum" +
                         " of two squares");
    }
    else if(prime % 4 == 1){
      if (sumSquare(prime));
    }
  }
}

 static boolean sumSquare(int n) {
    for (int i = 1; i <= n; i++){
       if( i^((n-1)/2) = -1){
          int s = ( (i^( (n-1)/4) ) % 4);
          findGCD(n, s + sqrt(-1));
          return true;
       }
    }
  return false;
}

 private static int findGCD(int number1, int number2) {
      if(number2 == 0){  //base case
          return number1;
      }
      return findGCD(number2, number1%number2);
   }
}
```

```
Please enter a prime number:
31
Sorry 31 cannot be written as the sum of two squares

Please enter a prime number:
17

1 and 4
1^2 + 4^2 = 17

Please enter a prime number:
53

2 and 7
2^2 + 7^2 = 53

Please enter a prime number:
701

5 and 26
5^2 + 26^2 = 701
```

CONCLUSIONS

A successful Java program demonstrating how the Fermat's Christmas Theorem works, was coded using the Repl.it IDE. The user is first asked to enter a prime number. Next, the program checks whether the inputted prime number is equal to one modulo four. If it's not equal to one modulo four, the program tells the user that the entered prime number cannot be written as the sum of two squares. However, if it is equal to one modulo four, the program recursively performs the Euclidean Algorithm for the two integers that are equal to the prime number after adding the square of each integer.

FUTURE WORK

For future work, research and analysis of some of the other mathematical contributions made by Pierre de Fermat, can be conducted. For instance, Fermat developed a few important concepts in the domain of analytical geometry. His fundamental principle of analytic geometry can be studied.

ACKNOWLEDGEMENTS

- Cleveland State University: Mathematics Department
- Choose Ohio First
- Repl.it IDE
- Dr. Steven Gubkin, PhD
- Pierre de Fermat

REFERENCES

1. Bhaskar, Jahnavi. "Sum of Two Squares." Math.uchicago.edu, https://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Bhaskar.pdf.
2. Richey, Jacob, and Carl de Marcken. "Gaussian Integers - University of Washington." Math.washington.edu, University of Washington, 26 Mar. 2020, https://sites.math.washington.edu/~mathcircle/circle/2019-20/second/2020s_week16_lecture.pdf.