Sum of Squares!

Number Theory

Annie Xu and Emily Zhu[1]

October 5, 2016

1 Introduction

1.1 Sum of Squares

Theorem 1 (Sum of Two Squares)**.** A positive integer can be represented as a sum of two perfect squares if and only if in its prime factorization, any prime congruent to $3 \pmod 4$ occurs with even exponent.

Example 2. 2, 10, 18, and 20 can be represented as a sum of two perfect squares.
3, 12, 15, and 19 cannot be represented as a sum of two perfect squares.

Theorem 3 (Sum of Three Squares)**.** A positive integer cannot be represented as a sum of three perfect squares if and only if it is in the form $4^m(8k+7)$ for some nonnegative integers m and k.

Example 4. 3, 6, 19, and 32 can be represented as a sum of three perfect squares.
7, 15, 28, and 60 cannot be represented as a sum of three perfect squares.

Theorem 5 (Sum of Four Squares)**.** Any positive integer can be represented as a sum of four perfect squares!

Example 6. Take your favorite positive integer—you can represent it as a sum of four perfect squares. ☺

1.2 Quadratic Residues

Definition 7 (Quadratic Residue)**.** Let a, m be integers with $m > 1$. We say that a is a quadratic residue mod m if there exists an integer x such that $x^2 \equiv a \pmod m$ and it is a quadratic nonresidue otherwise.

Definition 8 (Legendre Symbol)**.** Let a be an integer and p be prime. We define the Legendre Symbol as:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p \end{cases}$$

Proposition 9. Let p be an odd prime and a, b be integers. Then:

1. (Euler's Criterion). $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. If $\gcd(a, p) = 1$, then consider the residue classes $a, 2a, \ldots, \frac{(p-1)}{2}a$. Let v be the number of these residue classes congruent to a number at least $\frac{p}{2}$ and less than p. Then $\left(\frac{a}{p}\right) = (-1)^v$. If a is odd, we also have $v \equiv \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + \cdots + \left\lfloor \frac{((p-1)/2)a}{p} \right\rfloor \pmod 2$.

Example 10.

$$\left(\frac{5}{7}\right) = -1 \qquad \left(\frac{1}{p}\right) = 1 \qquad \left(\frac{14}{7}\right) = 0 \qquad \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = \left(\frac{10}{13}\right) = 1$$

Theorem 11 (Quadratic Reciprocity)**.** Let p, q be odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

[1]Much of the material for this week comes from my professor Péter Maga's Number Theory Notes!

2 Problems

1. Calculate $\left(\frac{10}{17}\right)$, $\left(\frac{8}{11}\right)$, and $\left(\frac{11}{19}\right)$

2. Prove that 1991^{1991} is not the sum of 2 perfect squares.[2]

3. Prove that $x^2 \equiv 0 \pmod 4$ or $x^2 \equiv 1 \pmod 4$ for any integer x.

4. Prove that there are $\frac{p-1}{2}$ quadratic residues mod p among $\{1, 2, \ldots, p-1\}$.

5. Assume that p, q are primes with $p, q \equiv 1 \pmod 4$. Prove that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

6. Assume that p is an odd prime and a, b are quadratic nonresidues mod p. Show that ab is a quadratic residue mod p.

7. A school has installed exactly 2017 lockers, numbered from 1 to 2017, running side by side all the way around its perimeter so that locker #2017 is right next to locker #1. All of the odd numbered ones were left open, and all of the even numbered ones were shut.

   A prankster starts at locker #1, and flips its state from open to shut. He then moves one locker to the left (to #2017), and flips its state from open to shut. He then moves three more lockers to the left (to #2014), and flips its state from shut to open. He then moves five more lockers to the left (to #2009), and flips its state from open to shut. He keeps going until he has flipped a total of 2017 lockers. How many lockers are open after he is finished?[3]

8. Find the sum of the primes less than 50 for which $\left(\frac{2}{p}\right) = 1$. Can you generalize?

9. Prove that if $n = 4^m(8k + 7)$, then it cannot be represented as a sum of three squares.

10. Find the sum of all possible sums $a + b$ where a, b are nonnegative integers such that $4^a + 2^b + 5$ is a perfect square.[4]

3 Challenge: Proving Sum of Two Squares

1. Prove that if two integers m and n can be written as a sum of two squares then their product mn can be written as a sum of two squares.

2. Prove that if a prime $p = 4k + 3$ divides $a^2 + b^2$ (for a, b integers), then p divides a and p divides b.

3. Prove that a prime $p = 4k + 1$ can be written as a sum of two squares. (*Hint: First prove that you can find* $x^2 \equiv -1 \pmod p$.)

4. Put everything together!

5. Done? Prove the proposition/theorem about quadratic residues.

[2]From *Number Theory for Mathematical Contests* by David A. Santos
[3]Putnam Seminar 2016
[4]PUMaC 2012