SUM OF TWO SQUARES

JAHNAVI BHASKAR

Abstract. I will investigate which numbers can be written as the sum of two squares and in how many ways, providing enough basic number theory so even the unacquainted reader can follow. Results regarding the sum of four squares problem and Waring's problem are cited with references for further reading.

Contents

1. Introduction

We say that a positive integer n has a *representation as a sum of two squares* if $n = a^2 + b^2$ for some nonnegative $a, b \in \mathbb{Z}$. We deliberately include 0 as a possible value for a or b so that squares themselves will fall into this category, *e.g.*, since $4 = 2^2 + 0^2$. In this paper, we are interested not only in characterizing the numbers that have a representation as the sum of two squares, but also recognizing which numbers have more than one such representation and counting how many representations these numbers have. For instance, notice that $25 = 5^2 + 0^2 = 3^2 + 4^2$.

Naturally, the exploration of this problem inspires curiosity in similar questions, for example: what numbers can be written as the sum of three squares? or four? Is there a number k so that all numbers can be written as the sum of k squares? What if we consider cubes, or fourth powers – is there some k so that all numbers be written as the sum of k cubes? Supposing there is such a k, can we improve it by contenting ourselves with finitely many outliers? A few of these questions are examined at the end of the paper.

Date: August 22, 2008.

2. Preliminaries

We begin with a brief introduction to divisibility and congruence, the fundamentals of number theory. Readers with experience in number theory should feel free to skip to Section 3.

2.1. **Divisibility.**

Theorem 2.1. *(Division Algorithm) For all $a, b \in \mathbb{Z}$, $b \neq 0$, there are unique $q, r \in \mathbb{Z}$, $0 \leq r < |b|$, such that $a = bq + r$.*

See reference [2] for proof.

Definitions 2.2. For $a, b \in \mathbb{Z}$, a is *divisor* of b if there exists an integer x such that

$$ax = b.$$

We say that b is *divisible* by a and refer to b as a *multiple* of a. We write $a \mid b$ (read as "a divides b"), or if a is not a divisor of b, $a \nmid b$.

Example 2.3. The divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$. We indicate this by writing, for instance, $-2 \mid 6$.

Exercise 2.4. Let $a, b, c, s, t \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$.

Definitions 2.5. Notice that for any $a \in \mathbb{Z}$, the following holds:

(1) $1 \mid a$, $-1 \mid a$;
(2) $a \mid a$, $-a \mid a$.

With this in mind, we refer to $-1, 1, a$ and $-a$ as the *trivial* divisors of a. We also call -1 and 1 *units*. Any other divisors of a are called *proper divisors*.

Definitions 2.6. A positive integer a is *prime* if a has no proper divisors. A positive integer a is *composite* if a has proper divisors. If a is a positive integer, then for primes $p_1, \ldots, p_k$ that satisfy $p_1 \cdot p_2 \cdots p_k = a$, the product $p_1 \cdot p_2 \cdots p_k$ is called the *prime factorization* of a.

Theorem 2.7. *(Fundamental Theorem of Arithmetic) The prime factorization of $a \in \mathbb{Z}$, $a > 1$, is unique up to the order of the factors.*

See reference [2] for proof.

Definition 2.8. We call $a, b \in \mathbb{Z}$ *relatively prime* if the only common divisors of a and b are units.

Definition 2.9. Given $a, b \in \mathbb{Z}$, we define the *greatest common divisor* (GCD) of a and b, denoted by $gcd(a, b)$, as some positive integer d such that:

(1) $d \mid a$ and $d \mid b$;
(2) for all e such that $e \mid a$ and $e \mid b$, $e \mid d$.

Remark 2.10. Note that if a, b are relatively prime, $gcd(a, b) = 1$.

Lemma 2.11. *Let $S \subseteq \mathbb{Z}$ be given where S is a subgroup of $\mathbb{Z}$ under addition. Then there exists $d \in \mathbb{Z}$ such that $S = d\mathbb{Z}$, where $d\mathbb{Z} = \{dz : z \in \mathbb{Z}\}$.*

Proof. Since S is a subgroup of $\mathbb{Z}$, we know that given $a, b \in S$, $a + b \in S$. By repeated addition of a to itself, we get that $a\mathbb{Z} \subseteq S$. The proof proceeds in two cases:

(1) $S = \{0\}$.
Then choose $d = 0$, so that $S = 0\mathbb{Z} = \{0\}$.
(2) $S \neq \{0\}$.
Let d be the smallest positive integer in S. We know that $d\mathbb{Z} \subseteq S$. To show that $S \subseteq d\mathbb{Z}$, let $s \in S$. We will show that $d \mid s$, so that $s \in d\mathbb{Z}$. By the Division Algorithm, we know that $s = dq + r$ where $0 \leq r \leq d - 1$. Notice that $d \in S$, so $dq \in S$ and $-s \in S$. Since S is closed under addition, $dq + (-s) = r \in S$. But because $0 \leq r \leq d-1$, $S \subseteq \mathbb{Z}$, and d is the smallest positive integer in S, we know that $r = 0$. Thus $s = dq$ so that $d \mid s$.

□

Theorem 2.12. *Given $a, b \in \mathbb{Z}$, $gcd(a, b)$ exists and satisifes the expression*

$$gcd(a, b) = ax + by$$

for some $x, y \in \mathbb{Z}$.

Proof. Consider $S = \{ax + by : x, y \in \mathbb{Z}\}$. Note that $S \subseteq \mathbb{Z}$, $\{0\} \subseteq S$, and S is closed under subtraction. Therefore we can apply Lemma 2.11 to conclude that there exists a positive integer d such that $S = d\mathbb{Z}$. First, we must show that d is the GCD of a, b:

(1) $d \mid a$ and $d \mid b$
Note that $a \in S$, since $a = a \cdot 1 + b \cdot 0$. So for some $z \in \mathbb{Z}$, $dz = a \implies d \mid a$. For the same reason, $d \mid b$.
(2) for all e such that $e \mid a$ and $e \mid b$, $e \mid d$
We know that $d \in S$, since $S = d\mathbb{Z}$, so $d = ax_0 + by_0$. By Theorem 2.4, since $e \mid a$ and $e \mid b$, $e \mid ax_0 + by_0 \implies e \mid d$.

Since $d \in S$, for some $x, y \in \mathbb{Z}$, $d = ax + by$. □

Theorem 2.13. *If $a, b, c \in \mathbb{Z}$ are given such that $a \mid bc$ and a is relatively prime to b, then $a \mid c$.*

Proof. Since a is relatively prime to b, we have that $gcd(a, b) = 1 = ax + by$ for some $x, y \in \mathbb{Z}$. Now, multiply by c: $c = acx + bcy$. Now, we know $a \mid ac$ and we are given that $a \mid bc$, so by Theorem 2.4, $a \mid acx + bcy$. Thus $a \mid c$. □

2.2. **Congruence.**

Definition 2.14. Let $a, b \in \mathbb{Z}$. We say that a is *congruent* to b modulo m (which we abbreviate as mod m) if

$$m \mid a - b.$$

We write this as $a \equiv b \pmod{m}$.

Remark 2.15. Notice that we can express $m \mid a$ as $a \equiv 0 \pmod{m}$.

Exercise 2.16. For any $a \in \mathbb{Z}$, we have:

(1) $a \equiv a \pmod{m}$;
(2) if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$;
(3) if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

If $a \equiv b \pmod{m}$, then the following hold:

(1) $a + c \equiv b + c \pmod{m}$;
(2) $ac \equiv bc \pmod{m}$.

If additionally $c \equiv d \pmod{m}$, then we have:

(1) $a + c \equiv b + d \pmod{m}$;
(2) $ac \equiv bd \pmod{m}$.

Furthermore, if $ac \equiv bc \pmod{m}$ and c, m are relatively prime, then $a \equiv b \pmod{m}$.

We can now categorize the integers into classes based on their congruence modulo m, for some $m > 1$, by putting integers congruent to each other in the same class. Each integer is assigned one and only one such class, and any pair x, y drawn from the class will satisfy $x \equiv y \pmod{m}$. These classes are called *residue classes modulo* m, denoted by $\bar{a_m}$ where a is an element of that class. A set that contains exactly one element from each residue class may be written as $\mathbb{Z}/m\mathbb{Z}$. For example, when $m = 4$, we may write that $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. For certain operations, namely addition, subtraction, multiplication, and exponentiation, any element of the class is representative of the whole; that is, performing these operations on representatives of two classes gives a residue class result that applies to any element of those two classes. For other operations – greatest common divisor, for instance – this is not the case.

Remark 2.17. Be aware that we will freely interchange between the congruence expression and the algebraic expression of a number. In other words, the statement that n is of the form $4k + 1$ is equivalent to the statement that $n \equiv 1 \pmod{4}$.

Theorem 2.18. *If m, n are relatively prime integers, then m has a multiplicative inverse modulo n.*

Proof. Since m, n are relatively prime, $gcd(m, n) = 1 = am + bn$ by Theorem 2.12. Consider this equation modulo n:

$$1 \equiv am + bn \ (mod\ n)$$
$$1 \equiv am + 0 \equiv am \ (mod\ n).$$

Thus m has a multiplicative inverse modulo n. □

For p prime, $\mathbb{F}_p$=$\mathbb{Z}/p\mathbb{Z}$ is a field, meaning that the nonzero integers modulo p form a multiplicative group $\mathbb{F}_p^*$. The crucial properties of these algebraic structures for the purposes of this paper are the following:

- Since $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$ is a multiplicative group, for each $a \in \mathbb{F}_p^*$ there is exactly one $a^{-1} \in \mathbb{F}_p^*$ so that $a \cdot a^{-1} \equiv 1 \pmod{p}$.
- For $a \in \mathbb{F}_p^*$, $a^2 \equiv 1 \pmod{p}$ if and only if $a \equiv 1 \pmod{p}$ or $a \equiv p - 1 \pmod{p}$. The proof of this fact follows:

  Assume first that $a^2 \equiv 1 \pmod{p}$. Then $p \mid a^2 - 1 = (a + 1)(a - 1)$. Now, since p is prime, $p \mid a + 1$ or $p \mid a - 1$. If $p \mid a + 1$, then since $a \in \mathbb{F}_p^*$, $a \equiv p - 1 \pmod{p}$. If $p \mid a - 1$, then $a \equiv 1 \pmod{p}$.

  Assume now that $a \equiv 1 \pmod{p}$. Then $a^2 \equiv 1 \pmod{p}$. If $a \equiv p - 1 \pmod{p}$, then $a^2 \equiv p^2 - 2p + 1 \equiv 1 \pmod{p}$.

3. Sum of Two Squares Problem

We begin our efforts to characterize which positive integers can be written as the sum of two squares by examining some evidence.

Example 3.1. The following are the possible representations of the first 20 integers:

$1 = 1^2 + 0^2$	11 is not the sum of two squares
$2 = 1^2 + 1^2$	12 is not the sum of two squares
3 is not the sum of two squares	$13 = 3^2 + 2^2$
$4 = 2^2 + 0^2$	14 is not the sum of two squares
$5 = 1^2 + 2^2$	15 is not the sum of two squares
6 is not the sum of two squares	$16 = 4^2 + 0^2$
7 is not the sum of two squares	$17 = 4^2 + 1^2$
$8 = 2^2 + 2^2$	$18 = 3^2 + 3^2$
$9 = 3^2 + 0^2$	19 is not the sum of two squares
$10 = 3^2 + 1^2$	$20 = 2^2 + 4^2$.

The above example illustrates the difficulty of the problem. Can the reader see any pattern above in which numbers can or cannot be represented? To characterize which n can be written as the sum of two squares, we will first tackle the case when n is prime. In the example above, notice that the primes $2, 5, 13$, and 17 can be written as the sum of two squares.

Theorem 3.2. *(Wilson's Theorem) Let p be prime. Then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. As discussed above, since $\mathbb{F}_p^*$ forms a field, each element $a \in \{1, 2, \ldots, p-1\}$ has a unique multiplicative inverse such that $a = a^{-1}$ if and only if $a = 1$ or $a = p-1$. If $p = 2$, then notice that $(p-1)! = 1! = 1 \equiv -1 \pmod{2}$. If $p > 2$, then we can rearrange the product $1 \cdot 2 \cdots (p-1)$ so that each $a \in \{2, 3, \ldots, p-2\}$ is adjacent to its multiplicative inverse. We can then simplify to get $(p-1)! = 1 \cdot 1 \cdot 1 \cdots 1 \cdot (p-1) = p - 1 \equiv -1 \pmod{p}$. □

Definition 3.3. We define the *greatest integer function* to be the function $[-] : \mathbb{R} \to \mathbb{Z}$ such that for $x \in \mathbb{R}$, $[x] = max\{z : z \in \mathbb{Z}, z \leq x\}$.

Example 3.4. For instance, $[3.4] = [\pi] = [3] = 3$. Notice also that $[-3.4] = -4$. We leave it to the reader to show that the greatest integer function satisfies the inequality $[x] \leq x < [x] + 1$.

Remark 3.5. Thue's Theorem below relies on the *pigeonhole principle*, also called the *Dirichlet box principle*, which states that if more than n objects are distributed between n holes, then one of the holes must contain more than one object.

Theorem 3.6. *(Thue's Theorem) Let p be prime. For any integer a such that $p \nmid a$, there exist $x, y \in \{1, 2, \ldots, [\sqrt{p}]\}$ such that $ax \equiv y \pmod{p}$ or $ax \equiv -y \pmod{p}$.*

Proof. We define

$$S = \{0, 1, 2, \ldots, [\sqrt{p}]\} \times \{0, 1, 2, \ldots, [\sqrt{p}]\},$$

so that S consists of $([\sqrt{p}]+1)^2$ ordered pairs. Given that $\sqrt{p} < [\sqrt{p}]+1$, by squaring both sides we get $p < ([\sqrt{p}]+1)^2$, so S has more than p elements. Suppose $a \in \mathbb{Z}$ is given so that $p \nmid a$. As (x, y) varies over S, there are more than p expressions of the form $ax - y$. Notice that $ax - y$ is an integer, and every integer is congruent modulo p to exactly one of $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. There are p elements in $\mathbb{F}_p$, and more than p expressions $ax - y$, so by the pigeonhole principle there must be at least two expressions $ax - y$ that are congruent modulo p. Take these pairs $(x_1, y_1) \neq (x_2, y_2)$ such that $ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$. We can simplify to get $a(x_1 - x_2) \equiv y_1 - y_2$

(mod p). Let $x = |x_1 - x_2|, y = |y_1 - y_2|$ so that $(x, y) \in S$. We want to exclude the possibility that $x = 0$ or $y = 0$, so that $x, y \in \{1, 2, \cdots, [\sqrt{p}]\}$.

Suppose first that $x = |x_1 - x_2| = 0$ so that $x_1 = x_2$. Then $a(x_1 - x_2) = 0 \equiv y_1 - y_2 \pmod{p}$. Since $y_1, y_2 \in \{0, 1, \ldots, [\sqrt{p}]\}$, we know that $y_1 < p$ and $y_2 < p$. Then we must have that $y_1 = y_2$, contradicting $(x_1, y_1) \neq (x_2, y_2)$.

Suppose now that $y = |y_1 - y_2| = 0$ so that $y_1 = y_2$. Then $a(x_1 - x_2) \equiv 0 \pmod{p}$. Since $p \nmid a$, by Exercise 2.16, $x_1 - x_2 \equiv 0 \pmod{p}$. Using the same logic as above, we conclude that $x_1 = x_2$, contradicting $(x_1, y_1) \neq (x_2, y_2)$.

Thus we have $ax \equiv \pm y \pmod{p}$, as desired. □

Theorem 3.7. *If the equation $a^2 + 1 \equiv 0 \pmod{p}$ is solvable for some a, then p can be represented as a sum of two squares.*

Proof. Take a as a solution to the equation $a^2 + 1 \equiv 0 \pmod{p}$. Then $p \nmid a$, because if $p \mid a$, then $a^2 \equiv 0 \pmod{p}$, and $a^2 + 1 \equiv 1 \pmod{p}$. Thus we can apply Thue's Theorem: there exist $x, y \in \{1, 2, \ldots, [\sqrt{p}]\}$ such that $ax \equiv \pm y \pmod{p}$. Now, multiplying $a^2 + 1 \equiv 0 \pmod{p}$ by x^2 results in $a^2x^2 + x^2 \equiv y^2 + x^2 \equiv 0 \pmod{p}$, which means that $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}$. Since $x^2 + y^2 \geq 2$, we have $k > 0$. We will show that in fact, $k = 1$. Remember that $x, y \leq [\sqrt{p}]$, so $x^2, y^2 \leq ([\sqrt{p}])^2 < (\sqrt{p})^2 = p$, so $x^2 + y^2 < 2p$. We've shown above that $p \mid x^2 + y^2$. Thus $k = 1$, so that $x^2 + y^2 = p$. □

Theorem 3.8. *A prime number $p > 2$ is a sum of two squares if and only if $p \equiv 1 \pmod{4}$.*

Proof.

- Suppose $p = x^2 + y^2$ for nonnegative integers x, y.
  The result follows from two key properties of the ring $\mathbb{Z}/4\mathbb{Z}$. Notice first that any odd integer is congruent to either 1 (mod 4) or 3 (mod 4). Furthermore, any square is congruent to 0 (mod 4) or 1 (mod 4) for the following reason: as described above, any element of a residue class is representative in that arithmetic performed on that element gives a result for the entire class. Thus, we can consider each element of $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ squared: $0^2 \equiv 0 \pmod{4}$, $1^2 \equiv 1 \pmod{4}$, $2^2 \equiv 0 \pmod{4}$, and $3^2 \equiv 1 \pmod{4}$. So $(\mathbb{Z}/4\mathbb{Z})^2 = \{0, 1\}$. Now, consider $p = x^2 + y^2 \pmod{4}$. Since $x^2, y^2 \in \{0, 1\} \pmod{4}$, we know that $p \equiv x^2 + y^2 \in \{0, 1, 2\} \pmod{4}$. But p is prime greater than 2, so p is odd. Thus $p \equiv 1 \pmod{4}$.

  N.B. This proof actually shows that if n is any odd integer that can be represented as the sum of two squares, then $n \equiv 1 \pmod{4}$.

- Suppose $p \equiv 1 \pmod{4}$.
  We will show that $a^2 + 1 \equiv 0 \pmod{p}$ is solvable for some a, so that applying Theorem 3.7 above, we get that p is a sum of squares. First, we will examine the factors in $(p-1)!$:

  $$(p-1)! = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \cdots (p-2) \cdot (p-1).$$

  The last $(p-1)/2$ factors in the product can be paired with the negatives of the first $(p-1)/2$ factors in the following way: $(p-1) \equiv -1 \pmod{p}$;

$(p-2) \equiv -2 \pmod{p}$; ...; $\frac{p+1}{2} \equiv -\frac{p-1}{2} \pmod{p}$. The factorial becomes:

$$(p-1)! \equiv 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \cdot - \left(\frac{p-1}{2}\right) \cdots - 2 \cdot -1 \ (mod\ p)$$

$$\equiv (-1)^{(p-1)/2} \left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\right)^2 \ (mod\ p)$$

Wilson's Theorem tells us that $(p-1)! \equiv -1 \pmod{p}$, so we can write:

$$-1 \equiv (-1)^{(p-1)/2} \left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\right)^2 \ (mod\ p)$$

$$\left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\right)^2 \equiv (-1)^{(p+1)/2} \ (mod\ p)$$

Now, we know that $p \equiv 1 \pmod{4}$, so $p = 4k+1$ for some $k \in \mathbb{Z}$. Then $\frac{p+1}{2} = \frac{4k+1+1}{2} = 2k+1$, which is odd. Thus, we have that $(-1)^{(p+1)/2} = (-1)^{2k+1} = -1$ and

$$\left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\right)^2 + 1 \equiv 0 \ (mod\ p).$$

Let $a = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)$, so that we have

$$a^2 + 1 \equiv 0 \ (mod\ p).$$

We can now apply Theorem 3.7 to conclude that p is a sum of squares.

□

Having solved the sum of two squares problem when n is prime, we now consider the case when n is not prime. The following theorems are required to prove the Two Squares Theorem.

Theorem 3.9. *(Fermat's Little Theorem) If p is prime and a is a positive integer such that $p \nmid a$, then $a^{p-1} \equiv 1 \ (mod\ p)$.*

Proof. Consider the $p-1$ integers $a, 2a, \ldots, (p-1)a$. Notice first that none of these integers are divisible by p: if $p \mid ja$ for $1 \leq j \leq p-1$, then because $p \nmid a$, we would have $p \mid j$, which contradicts $1 \leq j \leq p-1$. Notice also that no two of these integers are congruent to each other modulo p: if $ja \equiv ka \pmod{p}$ for $1 \leq j < k \leq p-1$, then because p is prime and $p \nmid a$, $gcd(p, a) = 1$, so we can write $j \equiv k \pmod{p}$. Again, this contradicts that $1 \leq j < k \leq p-1$.

Since these integers $a, 2a, \ldots, (p-1)a$ are a set of $p-1$ pairwise-incongruent integers such that none are congruent to 0 modulo p, we can say the following:

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \ (mod\ p)$$

$$a^{p-1}(p-1)! \equiv (p-1)! \ (mod\ p)$$

Since $(p-1)!$ and p are relatively prime, by Exercise 2.16,

$$a^{p-1} \equiv 1 \ (mod\ p).$$

□

Lemma 3.10. *Let a, b be positive integers such that both a and b can be written as a sum of squares. Then the product ab can be written as a sum of squares in two ways.*

Proof. Let $a = x^2 + y^2$ and $b = z^2 + t^2$ where $x, y, z, t \in \mathbb{Z}$. Then we have the following:

$$\begin{aligned} ab &= (x^2 + y^2)(z^2 + t^2) \\ &= x^2z^2 + x^2t^2 + y^2z^2 + y^2t^2 \\ &= (x^2z^2 + 2xyzt + y^2t^2) + (x^2t^2 - 2xyzt + y^2z^2) \\ ab &= (xz + yt)^2 + (xt - yz)^2 \\ ab &= (xz - yt)^2 + (xt + yz)^2. \end{aligned}$$

□

Remark 3.11. A composite number for which every factor can be written as a sum of squares can also be written as a sum of squares. Now, we know that any number that is composed of prime factors only of the form $4k+1$ can be written as the sum of squares. As we will see in the Two Squares Theorem, a number can be written as the sum of two squares while including prime factors of the form $4k + 3$ as long as those prime factors are raised to an even power.

Definition 3.12. We call a positive integer *a square free* if $n^2 \nmid a$ for any $n > 1, n \in \mathbb{N}$. For instance, $a = 1$ is a square free integer. An arbitrary a is square free when $a = p_1p_2 \cdots p_k$ where $p_1, p_2, \ldots, p_k$ are distinct primes.

Theorem 3.13. *(Two Squares Theorem) A positive integer n is the sum of two squares if and only if each prime factor p of n such that $p \equiv 3$ (mod 4) occurs to an even power in the prime factorization of n.*

Proof. Let $n = s^2m$ for some $s, m \in \mathbb{Z}$, where m is square free.

- Suppose that each prime factor $p \equiv 3 \pmod 4$ occurs to an even power in the prime factorization of n.

  Since for each prime factor p of n such that $p \equiv 3 \pmod 4$, p occurs to an even power, $p \nmid m$. Thus each prime $p_0 > 2$ that divides m satisfies $p_0 \equiv 1 \pmod 4$, so by Theorem 3.8, each $p_0 > 2$ can be written as the sum of two squares. We know that 2 can be written as the sum of two squares: $2 = 1^2 + 1^2$. By Lemma 3.10, the product of integers that can be written as the sum of two squares, m, can also be written as the sum of two squares. Thus $m = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. We can now express as $n = s^2(x^2 + y^2) = (sx)^2 + (sy)^2$, so n is the sum of two squares.
- Suppose that $n = x^2 + y^2$.

  If $m = 1$, then $n = s^2$, so each prime p in the factorization of n such that $p \equiv 3 \pmod 4$ occurs to an even power. Now, assume $m > 1$. We will show that for every odd prime p such that $p \mid m$, $p \equiv 1 \pmod 4$. Observe that x, y can be written as follows: $x = dx_1$ and $y = dx_2$, where x_1, x_2 are relatively prime and $d = gcd(x, y)$. Then we have that:

$$\begin{aligned} n &= d^2(x_1^2 + x_2^2) \\ \frac{n}{d^2} &= x_1^2 + x_2^2 \\ \frac{s^2m}{d^2} &= x_1^2 + x_2^2. \end{aligned}$$

Since m is square free, $d^2 \mid s^2$, with $s^2 = t \cdot d^2$ for some $t \in \mathbb{Z}$, so

$$tm = x_1^2 + x_2^2.$$

Then, we know that $p \mid m$, so $p \mid tm = x_1^2 + x_2^2$. Thus we have the congruence $x_1^2 + x_2^2 \equiv 0 \pmod{p}$, so $x_1^2 \equiv -x_2^2 \pmod{p}$. We will show that $p \equiv 1 \pmod{4}$.

Assume for contradiction that $p = 4k + 3$ for $k \in \mathbb{Z}$. Then notice that $p - 1 = 4k + 2 = 2(2k + 1)$, so we have:

$$x_1^2 \equiv -x_2^2 \ (mod\ p)$$
$$(x_1^2)^{2k+1} \equiv (-1)^{2k+1}(-x_2^2)^{2k+1} \ (mod\ p)$$
$$x_1^{p-1} \equiv -x_2^{p-1} \ (mod\ p).$$

Now, notice first that since x_1, x_2 are relatively prime, p cannot divide both x_1 and x_2. Suppose $p \mid x_1$. Then $p \mid x_1^2$. We know that $p \mid tm$, so $p \mid tm - x_1^2 = x_2^2$ by Theorem 2.4. Since p is prime, $p \mid x_2$, contradicting $gcd(x_1, x_2) = 1$. Thus $p \nmid x_1$ and $p \nmid x_2$. Applying Fermat's Little Theorem, we have $x_1^{p-1} \equiv x_2^{p-1} \equiv 1 \pmod{p}$, so we get that $1 \equiv -1 \pmod{p}$, contradicting $p > 2$. Thus, $p \equiv 1 \pmod{4}$.

□

4. Counting Representations

As we have seen in Section 3, certain numbers can be represented as the sum of two squares, some in more than one way. So far, we have considered only those representations produced by nonnegative integers, and have disregarded the order of the summands in the representation. In this section, for $n = a^2 + b^2$, we will consider the representations $n = (\pm a)^2 + (\pm b)^2 = (\pm b)^2 + (\pm a)^2$ as eight *trivial variations* on a basic representation.

The motivation for this lies in the geometric underpinning of Theorem 4.4, which gives a formula for the number of representations of any positive integer. The proof of this theorem, which is beyond the scope of this paper, uses the complex numbers, commonly represented as the plane $\mathbb{R}^2$. If we regard $n = a^2 + b^2$ to be the integer solution (a, b) to the equation of the circle $n = x^2 + y^2$ in $\mathbb{R}^2$, a circle of radius $\sqrt{n}$ centered at the origin, then $n = (-a)^2 + b^2$, for instance, is a distinct integer solution to this equation: $(-a, b)$. Thought of in terms of points, (a, b) and $(-a, b)$ obviously differ.

Notation 4.1. Define $r_2(n)$ to be the number of representations of n as a sum of two squares of integers. In standard notation, $r_k(n)$ is the number of representations of n as the sum of k squares.

Example 4.2. Since $1 = 1^2 + 0^2 = (-1)^2 + 0^2 = 0^2 + 1^2 = 0^2 + (-1)^2$, $r_2(1) = 4$. It is left to the reader to show that $r_2(5) = 8$ and $r_2(25) = 12$.

Theorem 4.3. *Let p be prime. Then $r_2(p) \leq 8$.*

Proof. If $p = 2$, then notice that $r_2(2) = 4$. Now assume $p > 2$. Suppose for contradiction that $p = x^2 + y^2 = z^2 + t^2$ for positive integers x, y, z, t, so that $r_2(p) > 8$. We may assume that $x > z > t$.

We may also assume that $gcd(x, y) = gcd(z, t) = 1$, for the following reason: let $d = gcd(x, y)$. Then $p = x^2 + y^2 = (da)^2 + (db)^2 = d^2(a^2 + b^2)$. Then $\frac{p}{d^2} = a^2 + b^2 \in$

$\mathbb{Z}$, so either $d^2 = 1$ or $d^2 = p$. But $d^2 \neq p$, since then $d \mid d^2 = p$, contradicting p prime. Thus $d = 1$. The same argument holds for the pair z, t.

Moreover, we know that each of x, y, z, and t is relatively prime to p, since p is prime. As shown in Lemma 3.10, we can write p^2 as:

$$\begin{aligned} p^2 &= (x^2 + y^2)(z^2 + t^2) \\ &= (xz + yt)^2 + (xt - yz)^2 \\ &= (xz - yt)^2 + (xt + yz)^2. \end{aligned}$$

Furthermore,

$$\begin{aligned} (xz + yt)(xt + yz) &= x^2zt + xyz^2 + xyt^2 + y^2zt \\ &= (x^2 + y^2)zt + xy(z^2 + t^2) \\ &= pzt + pxy \\ &= p(xy + zt), \end{aligned}$$

so that $p \mid (xz + yt)$ or $p \mid (xt + yz)$. Suppose $p \mid (xz + yt)$, so that $xz + yt = kp$ for some $k \in \mathbb{Z}$. Then since $p \mid p$, by Theorem 2.4, $p \mid p^2 - (xz + yt)^2 = (xt - yz)^2$. Since p is prime, $p \mid (xt - yz)$ so $xt - yz = jp$ for some $j \in \mathbb{Z}$. Then, we have

$$p^2 = k^2p^2 + j^2p^2$$

$$1 = k^2 + j^2.$$

Now, we know that $xz + yt > 0$ and $p > 0$, so $k > 0$. Since $j^2 \geq 0$, we must have $k = 1$ and $j = 0$, meaning that $xt - yz = 0$ so that $xt = yz$. We know that x, y are relatively prime, so $x \mid z$, contradicting $x > z$. A similar argument can be made for the case $p \mid (xt + yz)$. Thus $r_2(p) \leq 8$. □

Theorem 4.4. *Let n be a positive integer, written as $n = 2^c n_1 n_3$, where*

$$n_1 = \prod_{p \equiv 1 \pmod 4} p^s = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$$

and

$$n_3 = \prod_{q \equiv 3 \pmod 4} q^t$$

where p and q range over the prime divisors of n, and s, t vary with p, q respectively. If one of the t is odd, then $r_2(n) = 0$. If all t are even, then $r_2(n) = 4(s_1 + 1)(s_2 + 1) \cdots (s_k + 1)$.

We omit the proof of Theorem 4.4, which is highly technical and relies on algebraic facts about $\mathbb{Z}[i]$, the ring of Gaussian integers. The full proof is given in reference [7].

Example 4.5. We know from previous exercises that that $r_2(25) = 12$. We will confirm this using Theorem 4.4: $25 = 2^c n_1 n_3 = 2^0 \cdot (5^2) \cdot 1$, so $r_2(25) = 4(s_1 + 1) = 4(2 + 1) = 12$.

5. Looking Ahead

5.1. **Sum of Multiple Squares.** Having proved that only certain numbers are representable as the sum of two squares, one may wonder whether there is a number n for which all numbers are representable as the sum of n squares. We know that all numbers are not representable as the sum of three squares: 7, for instance, and 47, cannot be represented as such.

All numbers are representable as the sum of four squares. Fermat is thought to be the first to prove this, using his favorite method of *infinite descent*, but he never published it. After significant contributions to the problem by Euler, Lagrange published the solution in 1770. The sum of four squares result relies on an algebraic identity similar to Lemma 3.10, namely that if x and y can be represented as the sum of four squares, then xy can be represented as the sum of four squares. The remaining work is to show that every prime is the sum of four squares. See reference [6] for the proof.

5.2. **Waring's Problem.** Around 1770, Waring considered an interesting generalization of the sum of squares problem: given a positive integer k, can we determine $g(k)$, where $g(k)$ is the least value of s such that every positive integer can be represented as the sum of s k^{th} powers of nonnegative integers? For example, $g(2) = 4$, since Lagrange has shown that every positive integer can be represented as the sum of 4 squares, and no smaller a number than 4 squares can be used to represent every positive integer. For instance, 7 is not representable by 3 squares. What would such a function g look like?

In 1909, Hilbert showed that for every k, $g(k)$ exists. However, his proof did not construct a formula for $g(k)$. A few known results are:

$$g(2) = 4;$$
$$g(3) = 9;$$
$$g(4) \geq 19;$$
$$g(5) = 37;$$

and for $6 \leq k \leq 471600000$,

$$g(k) = \frac{3}{2}^k + 2^k - 2.$$

Consider $k = 3$, for which $g(k) = 9$. Research has shown that it is likely that only two numbers, $23 = 2 \cdot 2^3 + 7 \cdot 1^3$ and $239 = 2 \cdot 4^3 + 4 \cdot 3^3 + 3 \cdot 1^3$, require as many as 9 cubes to express, so that (almost) all numbers can be written as the sum of 8 cubes. In fact, perhaps only 15 numbers, the largest of which is 8042, require a full 8 cubes. All sufficiently large numbers, by which we mean all numbers 8043 onwards, can be expressed in terms of a sum of 7 cubes. It is obvious, then, that 9 is not the crucial number in this problem. Rather, the numbers which need 9 cubes only do so because of insignificant properties of particular numbers – as Hardy says, an "arithmetical fluke." The more challenging problem is determining $G(k)$, the least value of s for which all sufficiently large numbers, that is, all numbers with a finite number of exceptions, can be represented by a sum of s k^{th} powers. Obviously,

$$G(k) \leq g(k)$$

for all $k \in \mathbb{N}$. We will prove that $G(2) = 4$.

Theorem 5.1. *Let $n \in \mathbb{Z}$ such that $n \equiv 7$ (mod 8). Then n cannot be represented by 3 squares.*

Proof. A few simple calculations similar to those in Theorem 3.8 show us that $(\mathbb{Z}/8\mathbb{Z})^2 = \{0, 1, 4\}$. If $x, y, z \in \mathbb{Z}/8\mathbb{Z}$, then $x^2 + y^2 + z^2 = \{0, 1, 2, 3, 4, 5, 6\}$, but no sum of 3 squares yields $n \equiv 7$ (mod 8). □

Theorem 5.2. *(Dirichlet's Theorem) Let h, k be relatively prime integers. Then there are infinitely many primes congruent to h (mod k).*

Since 7 and 8 are relatively prime integers, Dirichlet's Theorem says there are infinitely many primes congruent to 7 (mod 8). By Theorem 5.1, none of these primes can be represented by 3 squares, so $G(2) = 4$.

To read more about Waring's problem, see references [2], [3], and [6].

6. Acknowledgments

I want to thank Mike Shulman and Asaf Hadari for their patience and guidance; Paul Sally for providing me with materials in abundance; and Peter May for his understanding and for organizing the research program.

References

[1] L. Babai. Lectures in Discrete Mathematics. University of Chicago REU Program. 2008.
[2] Erdős, Surányi. Topics in the Theory of Numbers. Springer-Verlag. 2003.
[3] Hardy, Wright. An Introduction to the Theory of Numbers. Oxford. 1954.
[4] Niven, Zuckerman, Montgomery. An Introduction to the Theory of Numbers. John Wiley and Sons. 1960.
[5] O. Ore. Number Theory and Its History. Dover Publications, Inc. 1948.
[6] K. Rosen. Elementary Number Theory and Its Applications. Addison-Wesley Publishing Co. 1993.
[7] Sally, Sally. Roots to Research. American Mathematical Society. 2007.