Sums of Squares

Bianca Homberg and Minna Liu

June 24, 2010

Abstract

For our exploration topic, we researched the sums of squares. Certain properties of numbers that can be written as the sum of two squares or as the sum of three squares have been investigated. We have proved that any number equivalent to

$$2^k \cdot 3 (mod\ 2^{k+2})$$

for all $k \geq 0$ cannot be written as the sum of two squares and that any number equivalent to

$$2^{2k} \cdot 7 (mod\ 2^{2k+3})$$

for all $k \geq 0$ cannot be written as the sum of three squares. We have conjectured that any number not of the form above for sums of three squares can be written as the sum of the respective number of squares. We have also conjectured that all whole numbers can be written as the sum of four squares.

When we say ”sums of squares” we refer to sums of squares of integers. As stated by the trivial inequality, for any $a \in Z, a^2 \geq 0$. Therefore, no negative numbers can be written as the sum of squares since the sum of any number of squares is at least 0.

Sums of Two Squares

Lemma: No number of the form $2^k \cdot 3(mod\ 2^{k+2})$, for all k, can be written as the sum of 2 squares.

Proof: We proceed with proof by induction in 2 parts.

Part 1: Base case ($k = 0$): No sum of two squares is equivalent to $3(mod\ 4) = 3 \cdot 2^0(mod\ 2^{0+2})$. The residues of squares mod 4 are 0 and 1 ($0^2 \equiv 0(mod\ 4), 1^2 \equiv 1(mod\ 4), 2^2 = 4 \equiv 0(mod\ 4), 3^2 = 9 \equiv 1(mod\ 4)$), so the only possibilities for $a^2 + b^2$ (mod 4) are $0+0, 0+1, 1+1$–so a number written as the sum of two squares could be equivalent to 0, 1, or 2 (mod 4), but not 3.

Inductive step: The inductive hypothesis is that no number equal to $3 \cdot 2^{2k}(mod\ 2^{2k+2})$ can be written as the sum of two squares. We need to prove that no number of the form $3 \cdot 2^{2(k+1)}(mod\ 2^{2(k+1)+2})$ can be written as the sum of 2 squares. We assume for the sake of contradiction that there exists some number which can be written as the sum of some two squares, say $n^2 + m^2$ which is equivalent to $3 \cdot 2^{2(k+1)}(mod\ 2^{2(k+1)+2})$.

$$n^2 + m^2 \equiv 3 \cdot 2^{2(k+1)}(mod\ 2^{2(k+1)+2})$$

so

$$n^2 + m^2 \equiv 3 \cdot 4 \cdot 2^{2k}(mod\ 4 \cdot 2^{2k+2})$$

This can be written as $(n^2 + m^2) = 4 \cdot 2^{2k+2} \cdot x + 4 \cdot 3 \cdot 2^{2k}$. Since 4 divides both terms on the right, 4 must also divide the quantity $n^2 + m^2$. As we've seen before, every square is equivalent to 0 or 1 (mod 4). So the only way $n^2 + m^2$ can be divisible by four is if both n^2 and m^2 are divisible by 4. This implies that n and m are each divisible by 2. Let $n = 2n_0$ and $m = 2m_0$.

So then

$$n^2 + m^2 = (2n_0)^2 + (2m_0)^2 \equiv 3 \cdot 4 \cdot 2^{2k}(mod\ 4 \cdot 2^{2k+2})$$

Dividing out by 4,

$$(n_0)^2 + (m_0)^2 \equiv 3 \cdot 2^{2k}(mod\ 2^{2k+2})$$

But this is a contradiction, since the inductive hypothesis states that no number equal to $3 \cdot 2^{2k}(mod\ 2^{2k+2})$ can be written as the sum of two squares.

Part 2: Base case ($k = 0$): No sum of two squares is equivalent to $6(mod\ 8) = 3 \cdot 2^{2(0)+1}(mod\ 2^{2(0)+3})$. The residues of squares mod 8 are 0, 1, and 4, so the only possibilities for $a^2 + b^2$ (mod 8) are $0+0, 0+1, 1+1, 0+4, 1+4$–so a number written as the sum of two squares could be equivalent to 0, 1, 2, 4, or 5 (mod 8), but not 3 or 7 (since both are equivalent to 3 (mod 4)) or 6.

Inductive step: The inductive hypothesis is that no number equal to $3 \cdot 2^{2k+1}(mod\ 2^{2k+3})$ can be written as the sum of two squares. We need to prove that no number of the form $3 \cdot 2^{2(k+1)+1}(mod\ 2^{2(k+1)+3})$ can be written as the sum of 2 squares. We assume for the sake of contradiction that there exists some number which can be written as the sum of some two squares, say n^2+m^2 which is equivalent to $3\cdot 2^{2(k+1)+1}(mod\ 2^{2(k+1)+3})$.

$$n^2+m^2 \equiv 3\cdot 2^{2(k+1)+1}(mod\ 2^{2(k+1)+3})$$

so

$$n^2+m^2 \equiv 3\cdot 4\cdot 2^{2k+1}(mod\ 4\cdot 2^{2k+3})$$

This can be written as $(n^2+m^2) = 4\cdot 2^{2k+3}\cdot x + 4\cdot 3\cdot 2^{2k+1}$. Since 4 divides both terms on the right, 4 must also divide the quantity n^2+m^2. As we've seen before, every square is equivalent to 0 or 1 (mod 4). So the only way n^2+m^2 can be divisible by four is if both n^2 and m^2 are divisible by 4. This implies that n and m are each divisible by 2. Let $n=2n_0$ and $m=2m_0$.

So then

$$n^2+m^2 = (2n_0)^2+(2m_0)^2 \equiv 3\cdot 4\cdot 2^{2k+1}(mod\ 4\cdot 2^{2k+3})$$

Dividing out by 4,

$$(n_0)^2+(m_0)^2 \equiv 3\cdot 2^{2k+1}(mod\ 2^{2k+3})$$

But this is a contradiction, since the inductive hypothesis states that no number equal to $3\cdot 2^{2k+1}(mod\ 2^{2k+3})$ can be written as the sum of two squares.

Thus we have shown that all numbers equivalent to $3\cdot 2^k(mod\ 2^{k+2})$ cannot be written as the sum of two squares. (By counting 2^{2k} and 2^{2k+1} we have counted all k).

Sums of Three Squares

Lemma: No number equivalent to $2^{2k} \cdot 7 (mod\ 2^{2k+3})$ can be written as the sum of three squares.

Proof: We will proceed with a proof by induction.

Base case: As a base case, no number equivalent to $7 (mod\ 8)$ can be written as the sum of three squares. (Residues of squares mod 8 are 0, 1, and 4).

Inductive step: As the inductive hypothesis, we assume that any number equivalent to $2^{2k} \cdot 7 (mod\ 2^{2k+3})$ cannot be written as the sum of three squares. We would like to prove that any number equivalent to $2^{2(k+1)} (mod\ 2^{2(k+1)+3})$ cannot be written as the sum of three squares. For the sake of contradiction, we assume the opposite.

$$a^2 + b^2 + c^2 \equiv 2^{2(k+1)} \cdot 7 (mod\ 2^{2(k+1)+3})$$

So

$$a^2 + b^2 + c^2 \equiv 4 \cdot 2^{2k} \cdot 7 (mod\ 4 \cdot 2^{2k+3})$$

Since 4 divides both the residue and the modulus, 4 must divide $a^2 + b^2 + c^2$. Since squares are equal to 0 or 1 mod 4, the only possibility is that each square is equivalent to 0 mod 4. So each of a, b, and c must be divisible by 2. Let $a = 2a_0$, $b = 2b_0$, and $c = 2c_0$. So

$$(2a_0)^2 + (2b_0)^2 + (2c_0)^2 \equiv 4 \cdot 2^{2k} \cdot 7 (mod\ 4 \cdot 2^{2k+3})$$

So

$$a_0^2 + b_0^2 + c_0^2 \equiv 2^{2k} \cdot 7 (mod\ 2^{2k+3})$$

But by the inductive hypothesis, we know that no number equivalent to $2^{2k} \cdot 7 (mod\ 2^{2k+3})$ can be written as the sum of three squares. This is a contradiction.

We therefore conclude that for all k, no numbers equivalent to $2^{2k} \cdot 7 (mod\ 2^{2k+3})$ can be written as the sum of three squares.

Conjectures

We have several conjectures based on computation. We tested the first 100,000 numbers and all could be written as the sum of four squares (counting 0 as a square). We also conjecture that every number that is not of the form specified previously can be written as the sum of three squares. (We have another conjecture regarding sums of two squares based on the composition of their primes).

In an attempt to prove the fact for four squares, we tried to reduce the problem by thinking about multiplying two numbers that could be written as the sum of four squares. If it could be shown that their product would necessarily also be able to be written as the sum of four squares, then it would be sufficient to prove that all primes can be written as the sum of four squares to prove that all numbers can be written as the sum of four squares. However, there was not enough time to complete work proving or disproving this conjecture.