# Lecture 21: Binary Quadratic Forms I: Sums of Two Squares

William Stein

**Math 124** Harvard University **Fall 2001**

Today we study the question of which integers are the sum of two squares.

## 1 Sums of Two Squares

During the next four lectures, we will study binary quadratic forms. A simple example of a binary quadratic form that will occupy us today is

$$x^2 + y^2.$$

A typical question that one asks about a quadratic form is which integers does it represent. "Are there integers $x$ and $y$ so that $x^2+y^2 = 389$? So that $x^2+y^2 = 2001$?"

### 1.1 Which Numbers are the Sum of Two Squares?

The main goal of today's lecture is to prove the following theorem.

**Theorem 1.1.** *A number $n$ is a sum of two squares if and only if all prime factors of $n$ of the form $4m + 3$ have even exponent in the prime factorization of $n$.*

Before tackling a proof, we consider a few examples.

*Example* 1.2.

- $5 = 1^2 + 2^2$.
- 7 is not a sum of two squares.
- 2001 is divisible by 3 because $2 + 1$ is, but not by 9 since $2 + 1$ is not, so 2001 is *not* a sum of two squares.
- $2 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 13$ is a sum of two squares.
- 389 is a sum of two squares, since $389 \equiv 1 \pmod 4$ and 389 is prime.
- $21 = 3 \cdot 7$ is *not* a sum of two squares even though $21 \equiv 1 \pmod 4$.

In preparation for the proof of Theorem 1.1, we recall a result that emerged when we analyzed how partial convergents of a continued fraction converge.

**Lemma 1.3.** *If $x \in \mathbb{R}$ and $n \in \mathbb{N}$, then there is a fraction $\frac{a}{b}$ in lowest terms such that $0 < b \leq n$ and*

$$\left|x - \frac{a}{b}\right| \leq \frac{1}{b(n+1)}.$$

*Proof.* Let $[a_0, a_1, \ldots]$ be the continued fraction expansion of $x$. As we saw in the proof of Theorem 2.3 in Lecture 18, for each $m$

$$\left|x - \frac{p_m}{q_m}\right| < \frac{1}{q_m \cdot q_{m+1}}.$$

Since $q_{m+1}$ is always at least 1 bigger than $q_m$ and $q_0 = 1$, either there exists an $m$ such that $q_m \leq n < q_{m+1}$, or the continued fraction expansion of $x$ is finite and $n$ is larger than the denominator of the rational number $x$. In the first case,

$$\left|x - \frac{p_m}{q_m}\right| < \frac{1}{q_m \cdot q_{m+1}} \leq \frac{1}{q_m \cdot (n+1)},$$

so $\frac{a}{b} = \frac{p_m}{q_m}$ satisfies the conclusion of the lemma. In the second case, just let $\frac{a}{b} = x$. $\square$

**Definition 1.4.** A representation $n = x^2 + y^2$ is *primitive* if $\gcd(x, y) = 1$.

**Lemma 1.5.** *If $n$ is divisible by a prime $p$ of the form $4m+3$, then $n$ has no primitive representations.*

*Proof.* If $n$ has a primitive representation, $n = x^2 + y^2$, then

$$p \mid x^2 + y^2 \quad \text{and} \quad \gcd(x, y) = 1,$$

so $p \nmid x$ and $p \nmid y$. Thus $x^2 + y^2 \equiv 0 \pmod{p}$ so, since $\mathbb{Z}/p\mathbb{Z}$ is a field we can divide by $y^2$ and see that

$$(x/y)^2 \equiv -1 \pmod{p}.$$

Thus the quadratic residue symbol $\left(\frac{-1}{p}\right)$ equals $+1$. However,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4m+3-1}{2}} = (-1)^{2m+1} = -1.$$

$\square$

*Proof of Theorem 1.1.* ($\Longrightarrow$) Suppose that $p$ is of the form $4m+3$, that $p^r \parallel n$ (exactly divides) with $r$ odd, and that $n = x^2 + y^2$. Letting $d = \gcd(x, y)$, we have

$$x = dx', \quad y = dy', \quad n = d^2 n'$$

with $\gcd(x', y') = 1$ and

$$(x')^2 + (y')^2 = n'.$$

Because $r$ is odd, $p \mid n'$, so Lemma 1.5 implies that $\gcd(x', y') > 1$, a contradiction.

($\Longleftarrow$) Write $n = n_1^2 n_2$ where $n_2$ has no prime factors of the form $4m + 3$. It suffices to show that $n_2$ is a sum of two squares. Also note that

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - x_2 y_1)^2,$$

so a product of two numbers that are sums of two squares is also a sum of two squares.[1] Also, the prime 2 is a sum of two squares. It thus suffices to show that if $p$ is a prime of the form $4m + 1$, then $p$ is a sum of two squares.

Since

$$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4m+1-1}{2}} = +1,$$

$-1$ is a square modulo $p$; i.e., there exists $r$ such that $r^2 \equiv -1 \pmod{p}$. Taking $n = \lfloor \sqrt{p} \rfloor$ in Lemma 1.3 we see that there are integers $a, b$ such that $0 < b < \sqrt{p}$ and

$$\left| -\frac{r}{p} - \frac{a}{b} \right| \leq \frac{1}{b(n+1)} < \frac{1}{b\sqrt{p}}.$$

If we write

$$c = rb + pa$$

then

$$|c| < \frac{pb}{b\sqrt{p}} = \frac{p}{\sqrt{p}} = \sqrt{p}$$

and

$$0 < b^2 + c^2 < 2p.$$

But $c \equiv rb \pmod{p}$, so

$$b^2 + c^2 \equiv b^2 + r^2 b^2 \equiv b^2(1 + r^2) \equiv 0 \pmod{p}.$$

Thus $b^2 + c^2 = p$. □

## 1.2 Computing $x$ and $y$

Suppose $p$ is a prime of the form $4m + 1$. There is a construction of Legendre of $x$ and $y$ that is explained on pages 120–121 of Davenport. I'm unconvinced that it is any more efficient than the following naive algorithm: compute $\sqrt{p - x^2}$ for $x = 1, 2, \ldots$ until it's an integer. This takes at most $\sqrt{p}$ steps. Here's a simple PARI program which implements this algorithm.

[1] This algebraic identity is secretely the assertion that the norm map $N : \mathbb{Q}(i)^* \to \mathbb{Q}^*$ sending $x + iy$ to $(x + iy)(x - iy) = x^2 + y^2$ is a homomorphism.

```
{sumoftwosquares(n) =
   local(y);
   for(x=1,floor(sqrt(n)),
      y=sqrt(n-x^2);
      if(y-floor(y)==0, return([x,floor(y)]))
   );
   error(n," is not a sum of two squares.")
}
```

## 2 Sums of More Squares

Every natural number is a sum of **four** squares. See pages 124–126 of Davenport for a proof.

A natural number is a sum of **three** squares if and only if it is not a power of 4 times a number that is congruent to 7 modulo 8. For example, 7 is not a sum of three squares. This is more difficult to prove.