Representations of Integers as Sums of Squares

Ryan C. Daileda

Trinity University

Number Theory

Introduction

An (integral) *quadratic form* in n variables is a homogeneous polynomial in $X_1, X_2, \ldots, X_n$ of degree 2:

$$Q(X_1, X_2, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j, \;\; a_{ij} \in \mathbb{Z}.$$

One of the central questions in the theory of quadratic forms is that of *representability*: for which $m \in \mathbb{Z}$ does the Diophantine equation $Q(X_1, \ldots, X_n) = m$ admit a solution?

The theory of quadratic forms is rich and deeper than it might first appear.

We will content ourselves with a particular diagonal form, namely $Q(X_1, X_2, \ldots, X_n) = X_1^2 + X_2^2 + \cdots + X_n^2$, and therefore seek to understand the representability of integers as sums of squares.

Representation of Integers as Sums of Two Squares

Let $n \in \mathbb{N}$ and consider the Diophantine equation

$$X^2 + Y^2 = n. \tag{1}$$

Question. For which n does (1) have a solution? That is, which natural numbers can be represented as a sum of two squares?

Our first goal is to give a complete answer to this question.

We begin with a handy observation: if $i = \sqrt{-1}$, then over $\mathbb{C}$ we have the factorization

$$X^2 + Y^2 = (X + iY)(X - iY).$$

Norms of Complex Numbers

We define the *norm* $N : \mathbb{C} \to \mathbb{R}$ by

$$N(a+bi) = (a+bi)(a-bi) = a^2 + b^2.$$

Let $\overline{a+bi} = a - bi$, the *complex conjugate* of $a+bi$. Then

$$N(z) = z\overline{z}$$

for all $z \in \mathbb{C}$.

One can show that $\overline{z+w} = \overline{z} + \overline{w}$ and $\overline{zw} = \overline{z}\overline{w}$ for all $z, w \in \mathbb{C}$.

It follows that

$$N(zw) = (zw)(\overline{zw}) = (z\overline{z})(w\overline{w}) = N(z)N(w).$$

Thus, for any $a, b, c, d \in \mathbb{Z}$ we have

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= N(a+bi)N(c+di) \\ &= N((a+bi)(c+di)) \\ &= N((ac-bd)+(ad+bc)i) \\ &= (ac-bd)^2+(ad+bc)^2.\end{aligned}$$

This proves our first lemma.

Lemma 1

If $m, n \in \mathbb{Z}$ both have the form X^2+Y^2, then so does mn.

Thue's Lemma

We now need a result on the size of solutions to linear congruences modulo p.

Lemma 2 (Thue)

Let p be prime and suppose $p \nmid a$. Then the congruence

$$aX \equiv Y \pmod{p}$$

has a solution x, y with $0 < |x| < \sqrt{p}$ and $0 < |y| < \sqrt{p}$.

Proof. We use the pigeonhole principle. Consider the set

$$S = \{ax - y \,|\, 0 \leq x, y < \sqrt{p}\}.$$

The are $(1+[\sqrt{p}])^2 > (\sqrt{p})^2 = p$ pairs (x, y) defining the elements of S.

It follows that there exist $(x_1, y_1) \neq (x_2, y_2)$ with $x_1, y_1, x_2, y_2 \in [0, \sqrt{p})$ so that

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p} \iff a\underbrace{(x_1 - x_2)}_{x} \equiv \underbrace{y_1 - y_2}_{y} \pmod{p}.$$

If $x = 0$, then $y = y_1 - y_2$ is divisible by p.

But $|y_1 - y_2| < \sqrt{p} < p$, so that $y_1 - y_2 = 0$ as well. This contradicts $(x_1, y_1) \neq (x_2, y_2)$.

We have the same problem if $y = 0$. Thus:

$$0 < |x|, |y| < \sqrt{p},$$

and we are finished.

$\square$

Remark. Because it relies on the pigeonhole principle, the proof we have given is nonconstructive.

Examples.

- Suppose $p = 3$ and $a = 2$. Then $x = -1$ and $y = 1$ satisfy $2x = -2 \equiv 1 = y \pmod 3$, and $0 < |x|, |y| < \sqrt{3}$.
- Suppose $p = 5$ and $a = 2$. Then $x = 1$ and $y = 2$ satisfy $2x \equiv 2 \equiv y \pmod 5$, and $0 < |x|, |y| < \sqrt{5}$.

We need one more (trivial) lemma.

Lemma 3

If n is odd and represented by $X^2 + Y^2$, then $n \equiv 1 \pmod 4$.

Proof. If $x \in \mathbb{Z}$, then $x \equiv 0, 1, 2, 3 \pmod 4$, which implies that $x^2 \equiv 0, 1 \pmod 4$.

It follows that $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$ for all $x, y \in \mathbb{Z}$. The result follows. □

We are now ready for our first main result.

Primes Represented by $X^2 + Y^2$

Theorem 1

Let p be an odd prime. Then p is represented by $X^2 + Y^2$ if and only if $p \equiv 1 \pmod 4$.

Proof. The "only if" statement follows from Lemma 3.

So suppose $p \equiv 1 \pmod 4$.

Then $\left(\frac{-1}{p}\right) = 1$, so there is an integer a satisfying $a^2 \equiv -1 \pmod p$.

By Thue's lemma, there exist integers $0 < |x|, |y| < \sqrt{p}$ so that $ax \equiv y \pmod p$.

We then have

$$-x^2 \equiv a^2x^2 \equiv y^2 \pmod{p} \;\Rightarrow\; p|x^2+y^2.$$

Write $x^2+y^2=kp$. Since $x,y\neq 0$ we must have $k\geq 1$. Moreover

$$kp = x^2+y^2 < p+p = 2p \;\Rightarrow\; k<2.$$

We conclude that $k=1$ and hence $x^2+y^2=p$, as claimed. □

Remark. One can also show that, up to sign changes and the order of the summands, the expression $p=x^2+y^2$ is unique.

Integers Represented by $X^2 + Y^2$

We can now prove the following general result.

Theorem 2

Let $n \in \mathbb{N}$ and write $n = N^2 m$ with m square-free. Then n is represented by $X^2 + Y^2$ if and only if m is not *divisible by any prime of the form $4k + 3$.*

Proof. First suppose that m is not divisible by any prime of the form $4k + 3$.

Then m can only be divisible by 2 or primes of the form $4k + 1$.

Since $2 = 1^2 + 1^2$, Theorem 1 implies that m is the product of primes represented by $X^2 + Y^2$.

Lemma 1 (and a quick induction) then implies that $m = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

Thus

$$n = N^2 m = N^2(x^2 + y^2) = (Nx)^2 + (Ny)^2,$$

as needed.

Now for the converse. Suppose that $n = N^2 m = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

Let $d = (x, y)$ and write $x = rd$, $y = sd$, with $(r, s) = 1$.

Then

$$n = N^2 m = d^2(r^2 + s^2).$$

Because m is square-free, we must have $d | N$.

Thus

$$\left(\frac{N}{d}\right)^2 m = r^2 + s^2.$$

Let p be any prime dividing m. Then $p | r^2 + s^2$.

Since $(r, s) = 1$, WLOG we have $p \nmid r$ (i.e. p can't divide both r and s).

Then $r^{-1} \pmod{p}$ exists and we have

$$s^2 \equiv -r^2 \pmod{p} \;\Rightarrow\; (sr^{-1})^2 \equiv -1 \pmod{p},$$

which means that $p = 2$ or $\left(\frac{-1}{p}\right) = 1$ (which implies $p \equiv 1 \pmod{4}$).

This completes the proof. □

Recall that in the decomposition $n = N^2 m$ with m square-free, the primes dividing m are precisely those that divide n with an odd exponent.

We therefore have the following corollary.

Corollary 1

Let $n \in \mathbb{N}$. Then n is represented by $X^2 + Y^2$ if and only if its prime factors of the form $4k+3$ occur with an even exponent.

Examples.

- Since $860 = 2^2 \cdot 5 \cdot 43$, and $43 \equiv 3 \pmod 4$, 860 cannot be represented by $X^2 + Y^2$.
- Since $954 = 2 \cdot 3^2 \cdot 53$ and $53 \equiv 1 \pmod 4$, 954 is represented by $X^2 + Y^2$. Indeed, we have $954 = 15^2 + 27^2$.

In the second example, we can find the representation by $X^2 + Y^2$ as follows.

Write $2 = 1^2 + 1^2$ and $53 = 4 + 49 = 2^2 + 7^2$.

Then compute

$$(1+i)(2+7i) = (2-7) + (7+2)i = -5 + 9i$$

and take the norm to obtain

$$2 \cdot 53 = 5^2 + 9^2.$$

Finally multiply by 3^2 to get

$$954 = 2 \cdot 3^2 \cdot 53 = 3^2(5^2 + 9^2) = 15^2 + 27^2.$$

Representation by $X^2 + nY^2$

The question of representation of integers by $X^2 + nY^2$ has been studied extensively.

For example, an odd prime p has the form $X^2 + 27Y^2$ iff $p \equiv 1 \pmod 3$ and 2 is a cubic residue of p.

More generally we have:

Theorem 3

Let $n \in \mathbb{N}$ be squarefree, $n \not\equiv 3 \pmod 4$. There is a monic irreducible polynomial $f_n(X) \in \mathbb{Z}[X]$ such that if an odd prime p divides neither n nor the discriminant of f_n, then $p = x^2 + ny^2$ iff

$$\left(\frac{-n}{p}\right) = 1 \text{ and } f_n(X) \equiv 0 \pmod p \text{ has a solution.}$$

$X^2 + Y^2 + Z^2$

The question of representability of integers as sums of three squares has also been settled.

Theorem 4

A natural number has the form $X^2 + Y^2 + Z^2$ iff it is not *of the form $4^n(8m + 7)$.*

Proof. We will prove that integers of the form $4^n(8m + 7)$ cannot be represented by $X^2 + Y^2 + Z^2$. The converse is too difficult to include here.

We induct on $n \geq 0$. Suppose $n = 0$. For any integer x we have $x^2 \equiv 0, 1, 4 \pmod 8$. Thus

$$x^2 + y^2 + z^2 \equiv 0, 1, 2, 3, 4, 5, 6 \pmod 8.$$

In particular, $x^2 + y^2 + z^2 \not\equiv 7 \pmod 8$, so that we cannot represent $8m + 7 = 4^0(8m + 7)$ as the sum of three squares.

Now let $n \geq 1$ and suppose no integer of the form $4^{n-1}(8m + 7)$ also has the form $X^2 + Y^2 + Z^2$.

Assume $4^n(8m + 7) = x^2 + y^2 + z^2$ for some $x, y, z \in \mathbb{Z}$.

Then $x^2 + y^2 + z^2 \equiv 0 \pmod 4$. Since every square is either 0 or 1 modulo 4, this can only happen if $x \equiv y \equiv z \equiv 0 \pmod 2$.

Write $x = 2a$, $y = 2b$ and $z = 2c$. Then

$$4^n(8m+7) = x^2 + y^2 + z^2 \;\Rightarrow\; 4^{n-1}(8m+7) = a^2 + b^2 + c^2,$$

which contradicts our inductive hypothesis. Hence $4^n(8m+7)$ is not the sum of three squares, which finishes the induction. □

Examples.

- Since $299 \equiv 3 \pmod 8$, Theorem 4 guarantees that 299 is the sum of three squares. Indeed, $299 = 7^2 + 9^2 + 13^2$.

- Since $368 = 16 \cdot 23$ and $23 \equiv 7 \pmod 8$, 368 *cannot* be expressed as the sum of three squares.