Sum of Four Squares via Geometry of Numbers

John D Mangual

$$n = a^2 + b^2 + c^2 + d^2$$

Every natural number can be written as the sum of four perfect squares.

Lemma

Let m be an odd number then

$$a^2 + b^2 + 1 = 0 \mod m$$

has a solution in integers $a, b \in \mathbb{Z}$.

Lemma

Let p be an **prime** then

$$a^2 + b^2 + 1 = 0 \mod p$$

has a solution in integers $a, b \in \mathbb{Z}$.

Set $\square = \{x^2 : x \in \mathbb{Z}/p\mathbb{Z}\}$ and $-(\square + 1)$ each have $\frac{p+1}{2}$ elements

So these two sets overlap... this is **Pigeonhole Principle**.

Lemma

Let p be an **prime** then

$$a^2 + b^2 + 1 = 0 \mod p^k$$

has a solution in integers $a, b \in \mathbb{Z}$.

$\square = \{x^2 : x \in \mathbb{Z}/p\mathbb{Z}\}$ and $-(\square+1)$ each have $\frac{p+1}{2} \times p^{k-1}$ elements

So these two sets overlap... this is **Pigeonhole Principle**.

Alternatively. If $a_0^2 + b_0^2 + 1 \equiv 0 \mod p^k$ then:

$$(a_0+p^k a)^2+(b_0+p^k b)^2+1 \equiv (a_0^2+b_0^2+1)+2p^k(a_0 a+b_0 b) \equiv \quad \mod p^{k+1}$$

and we can solve a linear equation in $\mod p$

$$a_0 a + b_0 b \equiv 0 \mod p$$

Lemma

Let $m = pq$ be an **odd number** with p, q **relativly prime** then

$$\begin{aligned} a^2 + b^2 + 1 &= 0 \mod p \\ a^2 + b^2 + 1 &= 0 \mod q \end{aligned}$$

has a solution in integers $a, b \in \mathbb{Z}$.

We can solve these equations individually, but using the **Chinese Remainder Theorem** we can solve these equations at the same time!

This is **Pigeonhole Principle** since we are trying to solve the equation in $(a, b) \in \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ and we need to find a solution that hits both.

Solution Over the Integers

$$\begin{bmatrix} X \\ Y \\ Z \\ W \end{bmatrix} = \left[\begin{array}{cc|cc} m & 0 & a & b \\ 0 & m & b & -a \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix}$$

The solutions $\mod m$ define a lattice inside $\mathbb{Z}^4$. Notice that:

$$X^2 + Y^2 + Z^2 + W^2 \equiv 0 \mod m$$

Solution Over the Integers

$$\begin{bmatrix} X \\ Y \\ Z \\ W \end{bmatrix} = \left[\begin{array}{cc|cc} m & 0 & a & b \\ 0 & m & b & -a \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix}$$

The solutions $\mod m$ define a lattice inside $\mathbb{Z}^4$. We'd like:

$$\begin{aligned} X^2 + Y^2 + Z^2 + W^2 &\equiv 0 \mod m \\ X^2 + Y^2 + Z^2 + W^2 &< 2m \end{aligned}$$

I can't visualize this 4D lattice very well... but we know 4D sphere geometry:

$$\mathrm{Vol}(|x| < 2m) = \frac{1}{2}\pi^2 (2m)^2$$

The unit volume of this lattice is the determinant of the matrix, which we conventiently defined to be m^2.

Solution Over the Integers

$$\begin{bmatrix} X \\ Y \\ Z \\ W \end{bmatrix} = \left[\begin{array}{cc|cr} m & 0 & a & b \\ 0 & m & b & -a \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix}$$

The solutions $\bmod m$ define a lattice inside $\mathbb{Z}^4$. We'd like:

$$X^2 + Y^2 + Z^2 + W^2 < 2m$$

We know 4D sphere geometry and the unit volume of this lattice is the determinant of the matrix m^2

$$\mathrm{Vol}(|x| < 2m) = \frac{1}{2}\pi^2 (2m)^2 < 16 \times m^2$$

By **Minkowski's Theorem** there's a lattice point inside the sphere!

$$X^2 + Y^2 + Z^2 + W^2 = m$$

Because $\boxed{\pi^2 > 8}$ we can ensure ourselves always one solution.

Even Numbers If $m = 2^k\, pq \ldots r$ is even number, we can build more solutions via:

$$(X+Y)^2+(X-Y)^2+(Z+W)^2+(Z-W)^2 = 2\times(X^2+Y^2+Z^2+W^2)$$

and get more powers of 2 if necessary:

$$\left[\begin{array}{c} x+y \\ x-y \\ \hline z+w \\ z-w \end{array}\right] = \left[\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{array}\right] \left[\begin{array}{c} x \\ y \\ \hline z \\ w \end{array}\right]$$

If we multpy by 4 the solution is even more clear since:

$$(2X)^2 + (2Y)^2 + (2Z)^2 + (2W)^2 = 4 \times (X^2 + Y^2 + Z^2 + W^2)$$

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

Solution Strategy Review: Hasse Principle

- solve mod $p > 2$
  - pigeonhole principle (also solve mod p^k)
- combine mod p and mod q into solution mod pq
  - and all odd composite numbers m
  - this is Chinese Remainder Theorem
- use mod p solution to generate solution over $\mathbb{Z}$
  - This uses Minkowski's geometry of numbers

In a way the shape $a^2 + b^2 + 1 = 0$ defines a circle of radius $\sqrt{-1}$

We had to do Pigeonhole Principle (or Minkowski Theorem) on a region define on all moduli p, q, r, ∞ at once. And if we have sufficient **volume** our equation had a solution for all m.

Solution Strategy Review: Geometry of Numbers

For each m, our algorithm solves $X^2 + Y^2 + Z^2 + W^2 = m$

$$\frac{1}{\sqrt{m}}(X, Y, Z, W) \in S^3$$

We don't know much about this vector for any given m. In which direction does it point?