Last time:

Legendre's Theorem:

$Ax^2 + By^2 + Cz^2 = 0$ has a non-trivial integer solution

iff

A, B, C doesn't all have the same sign

AND $\forall$ odd primes p

- If $p \nmid$, then $-BC \in QR(p)$, etc.

Example:

Show that $15 = a^2 + 7b^2$ has no rational solution.

Solution:

Write $a = x/z$, $b = y/z$, $x, y, z \in \mathbb{Z}$.

Then, we need to show:

$$15z^2 = x^2 + 7b^2 \Rightarrow x^2 + 7b^2 - 15z^2 = 0$$

Note: $1 \cdot (7)(-15)$ is squarefree, so we can use Legendre's

Take $p = 3$, then $p \nmid C$, but $-AB = -7 \notin QR(3)$.

(Since $QR(3) = \{1\}$, but $-7 \equiv 2 \pmod 3$)

$\therefore$ By Legendre's Thm, this has no sol'n's.

Example:

Show that $5 = 12a^2 + 21b^2$ has no rational solution

Solution:

If we did the same things as above:

Let $a = x/z$, $b = y/z$. This gives: $12x^2 + 21y^2 - 5z^2 = 0$

But, $12 \cdot 21 \cdot (-5)$ is not squarefree.

Solution: (cont'd)

Instead, try $a = \frac{1}{6}\cdot\frac{x}{z}$ and $b = \frac{1}{3}\cdot\frac{x}{z}$. This gives:

$$5 = 12\left(\frac{1}{6}\cdot\frac{x}{z}\right)^2 + 21\left(\frac{1}{3}\cdot\frac{y}{z}\right)^2$$

$$\Rightarrow 3x^2 + 7y^2 - 15z^2 = 0$$

And from here, this is just the first example.

Note: Picking the correct rationals is always possible.

Now, let's prove this fact!

Theorem:

$\forall n \in \mathbb{Z}_{>0}$, $n\mathbb{I}_n \tilde{\sim}_{\mathbb{Q}} \mathbb{I}_n$.

Recall:

(1) Euclidean algorithm (for gcds)

(2) Complex numbers can be viewed as matrices:

$$a+bi \longleftrightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Defn

A quaternion is a 4×4 real matrix of the form:

$$A = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$$

The modulus of A is $|A| = \sqrt{a^2+b^2+c^2+d^2}$

(Caution: $|A| \neq \det(A)$. In fact, $\det(A) = |A|^4$)

Denote the set of all quaternions by $\mathbb{H}$

Properties:

- $\mathbb{H}$ is a vector space over $\mathbb{R}$.

Moreover, if $A, B \in \mathbb{H}$, then:

- $AB \in \mathbb{H}$
- $A^\dagger \in \mathbb{H}$. (This plays the role of complex conjugation)
- If $A \neq 0$, then A is invertible and $A^{-1} \in \mathbb{H}$.
- In fact, $AA^\dagger = A^\dagger A = |A|^2 I_4$.
  Hence, $A^{-1} = \frac{1}{|A|^2} A^\dagger$.
- $|AB| = |A| \cdot |B|$.
- $|A| = 0$ iff $A = 0$.

Defn $A \in \mathbb{H}$ is called a Hurwitz quaternion if:

- $A_{ij} \in \mathbb{Z}$ $\forall i,j$ OR
- $A_{ij} \in \mathbb{Z} + \frac{1}{2}$ $\forall i,j$

Denote the set of all Hurwitz quaternions by $\mathbb{A}$.

Additional Properties:

If $A, B \in \mathbb{A}$, then:

- $A + B \in \mathbb{A}$
- $mA \in \mathbb{A}$, $m \in \mathbb{Z}$
- $AB \in \mathbb{A}$.
- $A^\dagger \in \mathbb{A}$
- $A^{-1} \in \mathbb{A}$ iff $|A| = 1$.
- $|A|^2 \in \mathbb{Z}_{\geq 0}$.
- If $X \in \mathbb{H}$, $\exists$ a Hurwitz quaternion $\lfloor X \rceil \in \mathbb{A}$ such that $|X - \lfloor X \rceil| < 1$. ("Rounding")

We will prove that there exists a Hurwitz Quaternion $P \in \mathbb{H}$ s.t. $P^T I_4 P = n I_4$

(and in particular this shows $I_4 \sim_{\mathbb{H}} n I_4$ since all entries in $\mathbb{H}$ are rational)

The thing that makes this work is that we can still do the Euclidean Algorithm in $\mathbb{H}$.

Caution: $\mathbb{H}$ is not commutative.

Lemma: (Euclidean Algorithm for Hurwitz Quaternions)
Let $A_0, A_1 \in \mathbb{H}$ ($A_0 \neq 0$). There exists a Hurwitz Quaternion $G \in \mathbb{H}$ satisfying:

(1) $G^{-1}A_0 \in \mathbb{H}$, $G^{-1}A_1 \in \mathbb{H}$ ($\Leftrightarrow$ G is a left divisor of A_0 and A_1)

(2) $G = A_0 X_0 + A_1 X_1$ for some $X_0, X_1 \in \mathbb{H}$.

We say that G is a left gcd of A_0, A_1.

Proof:

Construct a sequence $A_0, A_1, A_2, \ldots$ as follows:

For $k = 0, 1, 2, \ldots$ define:

$$A_{k+2} = A_k - A_{k+1}\lfloor A_{k+1}^{-1} A_k \rceil \quad (A)$$
$$= A_{k+1}(A_{k+1}^{-1} A_k - \lfloor A_{k+1}^{-1} A_k \rceil) \quad (B)$$

as long as $A_{k+1} \neq 0$.

Jan 20th

Proof (cont'd)

(A) Shows that $A_k \in \mathbb{A}$

(B) Shows that $|A_{k+1}| < |A_k|$ (since $|A_k^{-1}A_k - \bar{1}A_{k+1}^{-1}A_k| < 1$)

So, this must terminate, i.e. we have $A_{k+1} = 0$ for some k.

Let $G_k = A_k$. and check that we get (1) and (2).

□

Lemma

For every odd prime p, there exists $1 \le m < p$, $m \in \mathbb{Z}$, such that and $x, y \in \mathbb{Z}$ such that $1 + x^2 + y^2 = mp$.

Proof: $p = 2$, Exercise, So, assume p odd.

Consider 2 lists of numbers

(1) $0^2, 1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$ ← All distinct mod p.

(2) $-1-0^2, -1-1^2, -1-2^2, -1-3^2, \ldots, -1-\left(\frac{p-1}{2}\right)^2$ ←

The two lists together have $p+1$ numbers

$\therefore$ $\exists\, x^2$ in first list, $-1-y^2$ in the 2nd list ← Two #'s must be congruent to each other (Pigeonhole)

$x^2 \equiv -1-y^2 \pmod{p}$

$\therefore 1 + x^2 + y^2 = mp$

(Check that $m < p$)

↳ True since the #'s we used weren't big enough

□

Lemma:

For every prime p, there exists a Hurwitz Quaternion G_p s.t. $G_p = \sqrt{p}$.

Proof:

Let $A_0 = \begin{pmatrix} 1 & \dots \\ x & \dots \\ y & \dots \\ 0 & \dots \end{pmatrix} \in \mathbb{A}$ (where x and y are from the previous lemma)

Let $A_1 = p I_4$.

Then, $|A_0| = \sqrt{1+x^2+y^2} = \sqrt{mp}$, $(1 \le m < p)$

$|A_1| = p$

If $p=2$, then $m=1$, so pick $G_p = A_0$.

Otherwise, let G_p be the left gcd of A_0 and A_1.

Since $G_p \in \mathbb{A}$, $G_p^{-1} A_0 \in \mathbb{A}$, $G_p^{-1} A_1 \in \mathbb{A}$

Then:

$$|G_p|^2 |G_p^{-1} \cdot A_0|^2 = |A_0|^2 = mp$$

($|G_p|^2$ must be an integer)

$\therefore |G_p|^2$ divides mp

And, similarly $|G_p|^2 \cdot |G_p^{-1} \cdot A_1|^2 = |A_1|^2 = p^2$, so $|G_p|^2$ divides p^2 and so divides $p = \gcd(p^2, mp)$

Thus, $|G_p| = \sqrt{p}$ or $|G_p| = 1$

To rule out the 2nd case, note that if $|G_p| = 1$, then $G_p^{-1} \in \mathbb{A}$

Write $G_p = A_0 X_0 + A_1 X_1$ $(X_0, X_1 \in \mathbb{A})$

and

$$\begin{aligned} A_0^\dagger &= A_0^\dagger G_p G_p^{-1} = A_0^\dagger (A_0 X_0 + A_1 X_1) G_p^{-1} \\ &= (mp I_4 X_0 + p A_0^\dagger X_1) G_p^{-1} \\ &= p \underbrace{(m I_4 X_0 + A_0^\dagger X_1)}_{\in \mathbb{A}} G_p^{-1} \end{aligned}$$

So, $A_0^\dagger$ is p times a Hurwitz quaternion, but we know what A_0 is! A contradiction.

□.

Jan 24th

Proof (of theorem)

Write $n = p_1 p_2 \cdots p_k$ where $p_1, \ldots, p_k$ primes

Take $P = G_{\mathcal{B}_{p_1}} G_{\mathcal{B}_{p_2}} \cdots G_{\mathcal{B}_{p_k}}$.

Then,

$$|P| = |G_{\mathcal{B}_{p_1}}| |G_{\mathcal{B}_{p_2}}| \cdots |G_{\mathcal{B}_{p_k}}| = \sqrt{n}.$$

So, $P^T I_4 P = P^T P = |P^2| I_4 = n I_4$. □