Lecture 22
Four Squares Theorem

Pell-Brahmagupta Equation (continued) - $x^2 - dy^2 = 1, \square \neq d \in \mathbb{N}$, if (x, y) and (z, w) solutions then $x < z \Rightarrow y < w$ if and only if $x + \sqrt{d}y < z + \sqrt{d}w$.

Theorem 78. *If (x_1, y_1) is the least positive solution of $x^2 - dy^2 = 1$ where $\square \neq d \in \mathbb{N}$, then all positive solutions are given by (x_n, y_n) where $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$ for $n = 1, 2, 3 \ldots$*

Proof. First see that (x_n, y_n) is a solution. We know that (x_1, y_1) is a solution $x_1^2 - dy_1^2 = 1$.

$$\begin{aligned}
(x_1 + \sqrt{d}y_1)(x_1 - \sqrt{d}y_1) &= 1 \\
x_n + \sqrt{d}y_n &= (x_1 + \sqrt{d}y_1)^n \\
\text{taking conjugates, } x_n - \sqrt{d}y_n &= (x_1 - \sqrt{d}y_1)^n \\
(x_n + \sqrt{d}y_n)(x_n - \sqrt{d}y_n) &= (x_1 + \sqrt{d}y_1)^n (x_1 - \sqrt{d}y_1)^n \\
x_n^2 - \sqrt{d}y_n &= ((x_1 + \sqrt{d}y_1)(x_1 - \sqrt{d}y_1))^n \\
&= 1^n = 1
\end{aligned}$$

So (x_n, y_n) is indeed a solution. Why are these all the positive solutions? Suppose that (s, t) is a positive solution not of the form (x_n, y_n) for any n. Then $s + t\sqrt{d}$ is a positive (> 1) real number. Not that $\{x_n + \sqrt{d}y_n\}$ is a sequence of positive real numbers which increase to infinity, since

$$x_n + \sqrt{d}y_n = \left(\underbrace{x_1 + \sqrt{d}y_1}_{>1}\right)^n$$

So pick n such that $x_n + y_n\sqrt{d} < s + t\sqrt{d} < x_{n+1} + y_{n+1}\sqrt{d}$. Multiply the sequence of inequalities by $x_n - y_n\sqrt{d}$ (it's a positive real number because it equals $x_n - \sqrt{d}y_n = \frac{1}{x_n + \sqrt{d}y_n}$). We see

$$\begin{aligned}
1 &= (x_n - \sqrt{d}y_n)(x_n + \sqrt{d}y_n) \\
&< \underbrace{(x_n - \sqrt{d}y_n)(s + t\sqrt{d})}_{a + b\sqrt{d},\ a, b \in \mathbb{Z}} \\
&< (x_n - \sqrt{d}y_n)(x_{n+1} + \sqrt{d}y_{n+1}) \\
&= (x_1 - \sqrt{d}y_1)^n (x_1 + \sqrt{d}y_1)^{n+1} \\
&= (x_1 + \sqrt{d}y_1)
\end{aligned}$$

and so

$$1 < a + b\sqrt{d} < x_1 + \sqrt{d}y_1$$

We'll see $a, b \in \mathbb{N}$, then it will contradict minimality of (x_1, y_1)

$$a - b\sqrt{d} = \frac{1}{a + b\sqrt{d}} > 1 \text{ and } a + b\sqrt{d} > 1, \text{ so } 0 < a - b\sqrt{d} < 1$$

Adding $1 + 0 < 2a$ gives $a > \frac{1}{2} > 0$ which means that $a \geq 1$. Also, $b > \frac{a-1}{\sqrt{d}} \geq 0 \Rightarrow (a, b)$ is a positive integer solution. Why is $a + b\sqrt{d}$ a solution?

$$(a + b\sqrt{d})(a - b\sqrt{d}) = (x_n - \sqrt{d}y_n)(s + t\sqrt{d})(x_n + \sqrt{d}y_n)(s - t\sqrt{d})$$
$$a^2 - b^2 d = (x_n^2 - dy_n^2)(s^2 - dt^2) = 1$$

■

P-B equation is quite useful in many diophantine equations.

Eg. Putnam asked, can we find infinitely many triples of consecutive integers, each of which is a sum of 2 squares?

Yes. Suppose we choose $n-1, n, n+1$ where we set $n = x^2 \Rightarrow n = x^2 + 0^2, n+1 = x^2 + 1^2, x^2 - 1 = n - 1 =$ sum of 2 squares $y^2 + y^2$, so we need to find infinitely many (x, y) such that $x^2 - 2y^2 = 1$. P-B, so ok.

Proposition 79. *Let $N \in \mathbb{Z}, d \in \mathbb{N}, d \neq \square$. If $x^2 - dy^2 = N$ has one solution, it has infinitely many.*

Proof. Let (x_1, y_1) be a solution, so $(x_1 + \sqrt{d}y_1)(x_1 - \sqrt{d}y_1) = N$. Let (s_n, t_n) be infinitely many solutions to $x_2 - dy^2 = 1 \Rightarrow (s_n + \sqrt{d}t_n)(s_n - \sqrt{d}t_n) = 1$. Then if we let $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)(s_n + \sqrt{d}t_n)$ it's easy to see $x_n^2 - dy_n^2 = N$ and that these are all distinct. So we get infinitely many solutions. ■

Eg. Prove that $n^2 + (n+1)^2$ is a perfect square for infinitely many values of n.

Proof.

$$n^2 + n^2 + 2n + 1 = 2n^2 + 2n + 1 = m^2$$
$$4n^2 + 4n + 2 = 2m^2$$
$$(2n+1)^2 + 1 = 2m^2$$

Let l be $2n+1 \Rightarrow$ get a solution of $l^2 + 1 = 2m^2$. Conversely, if $l^2 + 1 = 2m^2$ then l is odd, so $n = \frac{l+1}{2}$ is an integer, and $m^2 = n^2 + (n+1)^2$. (Just want to show that $l^2 - 2m^2 = -1$ has infinitely many solutions. We know it has an obvious solution $(l, m) = (1, 1) \Rightarrow$ it has infinitely many.) ■

Theorem 80 (Four Squares Theorem)**.** *Every non-negative integer is a sum of* 4 *integer squares.*

Proof. Just like how we use complex numbers in the proof of the two squares theorem to establish that $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$, we'll use **quaternions** now

$$Q = \{a + bi + cj + dk : a, b, c, d, \in \mathbb{R}\}$$

i, j, k are "imaginary" where

$$i^2 = j^2 = k^2 = ijk = -1$$

$$\begin{aligned} ij &= k & ji &= -k \\ jk &= i & kj &= -i \\ ki &= j & ik &= -j \end{aligned}$$

Multiplication in Q is non-commutative (but associative - $x_1(x_2x_3) = (x_1x_2)x_3$, etc). Addition is component-wise. If $z = a + bj + cj + dk$, define conjugate $\overline{z} = a - bi - cj - dk$. Norm is $\|z\| = z\overline{z} = a^2 + b^2 + c^2 + d^2$.

Note that $\overline{zw} = \overline{w} \cdot \overline{z}$. It suffices to check things like

$$-k = \overline{k} = \overline{ij} = \overline{j} \cdot \overline{i} = (-j)(-i)$$

so

$$\|zw\| = zw\overline{zw} = zw\overline{w}\overline{z} = z(w\overline{w})\overline{z} = (z\overline{z})(w\overline{w}) = \|z\|\|w\|$$

So $(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2) = (ae-bf-cg-dh)^2 + 3$ other similar terms $\Rightarrow$ product of sum of 4 squares is a sum of 4 squares. So enough to show n is a sum of 4 squares for the case that $n = 0, 1,$ or prime. $0 = 0^2+0^2+0^2+0^2$, $1 = 1^2+0^2+0^2+0^2$, $2 = 1^2+1^2+0^2+0^2$, so enough to show that any odd prime p is a sum of 4 squares.

Lemma 81. *There's a positive integer* $m < p$ *such that* mp *is a sum of* 4 *squares.*

Proof. Recall that if p is an odd prime then $x^2 + y^2 + 1 = 0 \mod p$ has a solution (by pigeonhole principle). Let's suppose that we've produced $x, y \mod p$ so $|x|, |y| < \frac{p}{2}$. So

$$x^2 + y^2 + 1 < 2\left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < p^2$$

So $x^2 + y^2 + 1^2 + 0^2 = mp$ for some $0 < m < p$. □

Let m be the smallest positive integer such that mp is a sum of 4 squares. We've showed $m < p$. If $m = 1$ done. So assume $m > 1$ and we'll get a contradiction by producing a smaller value of m. If m is even, $mp = x^2 + y^2 + z^2 + w^2$ is even, so the number of odd elements of $\{x, y, z, w\}$ is even. We can pair these up, say, as $\{x, y\}$ and $\{z, w\}$ such that x and y have same parity and z, w have same parity, so

$$\frac{x+y}{2}, \frac{x-y}{2}, \frac{z+w}{2}, \frac{z-w}{2} \in \mathbb{Z}$$

$$\begin{aligned}\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 &= \frac{x^2+y^2+z^2+w^2}{2} \\ &= \left(\frac{m}{2}\right) p \text{ (decreasing m)}\end{aligned}$$

So suppose l is some prime dividing m, necessarily odd. Write $m = gl$, so $x^2 + y^2 + z^2 + w^2 = glp \equiv 0 \mod l$. Note $l < p$ because $l | m, m < p$. Reduce x, y, z, w to $x', y', z', w' \mod l$ (ie., $x \equiv x' \mod l$, etc.) such that $|x'|, |y'|, |z'|, |w'| < \frac{l}{2}$. If x', y', z', w' are all 0, then x, y, z, w are also $0 \mod l$, and

$$\left(\frac{x}{l}\right)^2 + \left(\frac{y}{l}\right)^2 + \left(\frac{z}{l}\right)^2 + \left(\frac{w}{l}\right)^2 = \frac{glp}{l^2} = \frac{gp}{l}$$

and $\frac{g}{l} < gl = m$ reducing m. So we may assume x', y', z', w' are not all 0.

$$x + yi + zj + wk = x' + y'i + z'j + w'k \mod l$$

Let

$$\begin{aligned}\rho &= x + yi + zj + wk \\ \sigma &= x' + y'i + z'i + w'k\end{aligned}$$

Then

$$\begin{aligned}\|\sigma\| &= \|\overline{\sigma}\| \\ &= \underbrace{x'^2 + y'^2 + z'^2 + w'^2}_{\text{positive}} \\ &\equiv x^2 + y^2 + z^2 + w^2 \mod l \\ &\equiv 0 \mod l\end{aligned}$$

So it's a multiple of l, say hl. Since $|x|, |y|, |z|, |w| < \frac{l}{2}$,

$$x^2 + y^2 + z^2 + w^2 < 4\left(\frac{l}{2}\right)^2 = l^2$$

So $0 < h < l$.

Also $\rho\overline{\sigma} = \rho\overline{\rho} \mod l \equiv x^2 + y^2 + z^2 + w^2 = 0 \mod l$, so the components of quaternion $\rho\overline{\sigma}$ are all divisible by l. Let $\beta = \frac{\rho\overline{\sigma}}{l}$.

$$\begin{aligned}
\|\beta\| &= \left\|\frac{\rho\overline{\sigma}}{l}\right\| \\
&= \left\|\frac{1}{l}\right\| \|\rho\|\|\overline{\sigma}\| \\
&= \frac{1}{l^2}(\underbrace{x^2 + y^2 + z^2 + w^2}_{glp})(\underbrace{x'^2 + y'^2 + z'^2 + w'^2}_{hl}) \\
&= \frac{(glp)(hl)}{l^2} \\
&= (gh)p
\end{aligned}$$

Note that $m = gl$ and $gh < gl$ since $h < l$, so we have a sum of 4 squares which is a smaller multiple of p. ■

18.781 Theory of Numbers
Spring 2012