LECTURE 8: THE PELL EQUATION : CHAPTER 5 OF STILLWELL'S "ELEMENTS OF NUMBER THEORY"

$\boxed{\text{Def}^{\underline{n}}/\ \underline{\text{Pell Eq}^{\underline{n}}}:\ x^2 - ny^2 = 1}$ ← Euler's fault, actually not due to Pell

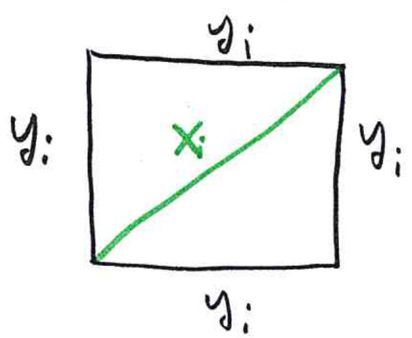
<u>GREEKS</u>: studied $x^2 - 2y^2 = 1$ over $\mathbb{N}$. This gives insight into $\sqrt{2}$. Likewise $x^2 - ny^2 = 1$ gives insight into $\sqrt{n}$. (for $n \neq m^2$). Basically, for nonsquare n there is a nice structure to the sol$^{\underline{n}}$ if we find one then we can construct many. But, $\nexists$ simple way to obtain first $\mathbb{N}$-sol$^{\underline{n}}$... We'll probably skip part of the end of Chapter 5 since the material on the River etc.. is somewhat complicated...

§5.1 SIDE AND DIAGONAL #'s

<u>Claim</u>: large sol$^{\underline{n}}$'s of $x^2 - 2y^2 = 1$ give $x/y \approx \sqrt{2}$.

$$\frac{x_i^2}{y_i^2} = \frac{1 + 2y_i^2}{y_i^2} = 2 + \frac{1}{y_i^2} \longrightarrow 2 \quad \text{as} \quad y_i \longrightarrow \infty$$

Hence $x_i/y_i \longrightarrow \sqrt{2}$ as $y_i \longrightarrow \infty$.



x_i = diagonal # = d_i

y_i = side # = s_i

<u>Sol$^{\underline{n}}$'s known to Greeks</u>:
$d_1 = 3,\ s_1 = 2$
$d_{i+1} = d_i + 2s_i$
$s_{i+1} = d_i + s_i$

<u>some</u> (these solve Pell's Eq$^{\underline{n}}$ 1)

(the odd i) $d_1^2 - 2s_1^2 = 9 - 2(4) \overset{\checkmark}{=} 1$ & $d_{i+1}^2 - 2s_{i+1}^2 = -(d_i^2 - 2s_i^2)$

Continuing,

$$d_{i+1} = d_i + 2s_i \quad \& \quad s_{i+1} = d_i + s_i$$

Consider,

$$\begin{aligned} d_{i+1}^2 - 2s_{i+1}^2 &= (d_i + 2s_i)^2 - 2(d_i + s_i)^2 \\ &= d_i^2 + \cancel{4s_i d_i} + 4s_i^2 - 2(d_i^2 + \cancel{2s_i d_i} + s_i^2) \\ &= -d_i^2 + 2s_i^2 \\ &= -(d_i^2 - 2s_i^2) \end{aligned}$$

But, $d_1^2 - 2s_1^2 = 1 \Rightarrow d_2^2 - 2s_2^2 = -1, \Rightarrow d_3^2 - 2s_3^2 = 1$

etc... for $i = 2j$ have sol$^{\underline{n}}$ of $x^2 - 2y^2 = -1$

whereas for $i = 2j+1$ have sol$^{\underline{n}}$ of $\underbrace{x^2 - 2y^2 = 1}_{\text{Pell Eq}^{\underline{n}}}$.

Irrational Square Roots

$$\boxed{\text{Th}^{\underline{m}}/ \text{ If } n \neq m^2 \text{ then } \sqrt{n} \text{ is irrational and if } a_1 + b_1\sqrt{n} = a_2 + b_2\sqrt{n} \text{ then } a_1 = a_2 \ \& \ b_1 = b_2}$$

Proof: Suppose that $a_1 + b_1\sqrt{n} = a_2 + b_2\sqrt{n}$ and yet $a_1 \neq a_2$ or $b_1 \neq b_2$. If $b_1 \neq b_2$ then $a_1 - a_2 = (b_2 - b_1)\sqrt{n}$ thus $\sqrt{n} = \frac{a_1 - a_2}{b_2 - b_1} \in \mathbb{Q}$ hence $\rightarrow\leftarrow$ irrationality of $\sqrt{n}$.

Likewise, if $a_1 \neq a_2$ then $a_1 + b_1\sqrt{n} = a_2 + b_2\sqrt{n}$ implies $0 \neq a_1 - a_2 = (b_1 - b_2)\sqrt{n} \Rightarrow (b_1 - b_2) \neq 0$ ~~as $\sqrt{n} \neq 0$~~ hence $\sqrt{n} = \frac{a_1 - a_2}{b_1 - b_2}$ again $\rightarrow\leftarrow$. It follows $a_1 = a_2$, $b_1 = b_2$ //

§5.2 The equation $x^2 - 2y^2 = 1$

Stillwell mentions it's "easy" to find $\mathbb{Q}$-sol$^{\underline{n}}$'s of $x^2 - 2y^2 = 1$. Just take line through $(1,0)$ with slope $t \in \mathbb{Q}$ and find intersections (Diophantus-like-method)

$$y = t(x-1)$$

$$x^2 - 2t^2(x-1)^2 = 1$$

$$x^2 - 2t^2(x^2 - 2x + 1) = 1$$

$$(1-2t^2)x^2 + 4t^2 x - 2t^2 - 1 = 0 \qquad t \in \mathbb{Q} \Rightarrow 1 - 2t^2 \neq 0$$

$$x^2 + \frac{4t^2}{1-2t^2}x - \frac{1+2t^2}{1-2t^2} = 0$$

$$x = \left(\frac{-4t^2}{1-2t^2} \pm \sqrt{\left(\frac{4t^2}{1-2t^2}\right)^2 + \frac{4(1+2t^2)}{1-2t^2}}\right)\frac{1}{2}$$

easy (actually not a joke, this is just algebra.)

$$= \frac{1}{2}\left(\frac{-4t^2}{1-2t^2} \pm \sqrt{\frac{16t^4 + 4(1+2t^2)(1-2t^2)}{(1-2t^2)^2}}\right)$$

$$= \frac{1}{2}\left(\frac{4t^2 \pm \sqrt{\cancel{16t^4} + 4(1 - \cancel{4t^4})}}{2t^2 - 1}\right)$$

$$= \frac{1}{2}\left(\frac{4t^2 \pm 2}{2t^2 - 1}\right)$$

$$= \frac{2t^2 \pm 1}{2t^2 - 1} = \begin{cases} 1 & : \text{for } \pm = - \\ \dfrac{2t^2+1}{2t^2-1} & : \text{for } \pm = + \end{cases}$$

Hence $y = t\left[\frac{2t^2+1}{2t^2-1} - 1\right] = t\left[\frac{2t^2+1-2t^2+1}{2t^2-1}\right] = \frac{2t}{2t^2-1}$

$$\therefore \boxed{(x,y) = \left(\frac{2t^2+1}{2t^2-1}, \frac{2t}{2t^2-1}\right) \text{ for } t \in \mathbb{Z}.}$$

§5.2 continued

I'm currently digressing to look at $\mathbb{Q}$-sol$^{\text{n}}$s of $x^2 - 2y^2 = 1$. I just found

oops. $t \in \mathbb{Q}$.

$$\boxed{(x,y) = \frac{1}{2t^2-1}(2t^2+1,\ 2t) \qquad \cancel{\text{for } t \in \mathbb{Z}}}$$

We can't just clear-out $\frac{1}{2t^2-1}$ since $x^2-2y^2=1$ is not homogeneous. In contrast, we saw in Chapter 1 the Pythag. Eq$^{\text{n}}$ $x^2+y^2=z^2$ allowed easier transition from $\mathbb{Q} \longrightarrow \mathbb{Z}$-sol$^{\text{n}}$s. Here, I have no clue what to do next... so, try some values, see what happens:

$t=1$ $(x,y) = \frac{1}{2-1}(+2+1,\ 2) = (3,2)$

$t=2$ $(x,y) = \frac{1}{3}(9,\ 4)$

ah ha. you all guessed this last class.

$t=3$ $(x,y) = \frac{1}{17}(19,\ 6)$

$\vdots$

$t=6$ $(x,y) = \frac{1}{71}(37,\ 12)$

$t=\frac{3}{4}$ $(x,y) = 8\left(\frac{17}{8},\ 2\left(\frac{3}{4}\right)\right)$

$= (17,\ 3)$

– (this is the next sol$^{\text{n}}$ gen. by group-technique) –

Cheating

$$\frac{2t}{2t^2-1} = 12$$

$$2t = 24t^2 - 12$$

$$24t^2 - 2t - 12 = 0$$

$$12t^2 - t - 6 = 0$$

$$\cancel{(12t \quad)(t \quad) = 0}$$

$$\Longrightarrow t \in \cancel{\tfrac{3}{4}}\ \mathbb{Q}.\ \frac{3}{4},\ \frac{-2}{3}$$

<u>Remark</u>: I have shown how <u>not</u> to do it on pgs. 3-4, now we go on to the nice technique (as shown in Stillwell)

<u>Claim</u>: If (x_i, y_i) solves $x^2 - 2y^2 = 1$ for $i=1,2$ then (x_3, y_3) is also a sol$^{\underline{n}}$ if we set:

$$x_3 = x_1 x_2 + 2y_1 y_2$$
$$y_3 = x_1 y_2 + y_1 x_2$$

<u>Proof</u>: given $\overbrace{x_1^2 - 2y_1^2}^{x_1^2 = 1+2y_1^2} = 1$ <u>and</u> $x_2^2 - 2y_2^2 = 1$ observe for $x_3 = x_1x_2 + 2y_1y_2$ & $y_3 = x_1y_2 + y_1x_2$ we have:

$$\begin{aligned}
x_3^2 - 2y_3^2 &= (x_1x_2 + 2y_1y_2)^2 - 2(x_1y_2 + x_2y_1)^2 \\
&= x_1^2x_2^2 + \cancel{4x_1x_2y_1y_2} + 4y_1^2y_2^2 + \\
&\quad - 2[x_1^2y_2^2 + \cancel{2x_1y_2x_2y_1} + x_2^2y_1^2] \\
&= \underline{x_1}^2x_2^2 - 2x_2^2y_1^2 + 4y_1^2y_2^2 - 2\underline{x_1}^2y_2^2 \\
&= x_2^2(\underline{1+\cancel{2y_1^2}}) - x_2^2(\cancel{2y_1^2}) + \cancel{4y_1^2y_2^2} - 2(\underline{1+2y_1^2})y_2^2 \\
&= x_2^2 - 2y_2^2 \\
&= 1.
\end{aligned}$$

$\therefore$ $\underline{(x_3, y_3) \text{ solves } x^2 - 2y^2 = 1}$.

<u>Remark</u>: I did not use $\mathbb{Z}[\sqrt{2}]$ for the above argument. As you can see, it's ugly.

– (we find better argument soon) –

Application set $(x_1, y_1) = (x_2, y_2) = (3, 2)$ to derive $(x_3, y_3) = (3^2 + 2(2)^2, 3(2) + (3)(2)) = \underline{(17, 12)}$ we can check: $17^2 - 2(12)^2 \neq 1$. We've shown a given sol^{n} $(3,2)$ can be used to generate new sol^{n}s.

§5.3 THE GROUP OF SOLUTIONS (FOR $n=2$)

$$(x + y\sqrt{2})(x - y\sqrt{2}) = x^2 - 2y^2 = 1$$

Essentially (x, y) has inverse $(x, -y)$.

- $\exists$ subgroup of positive # $x + y\sqrt{2}$ s.t. $x^2 - 2y^2 = 1$

Th^{m} (Structure of Positive Sol^{n}s)
The group of positive $x + y\sqrt{2}$ where $(x, y) \in \mathbb{Z}^2$ solves $x^2 - 2y^2 = 1$ is the infinite cyclic group of powers of $3 + 2\sqrt{2}$.

Proof: If $x_i^2 - 2y_i^2 = 1$, $i = 1, 2$ then $x_1 + y_1\sqrt{2}$ & $x_2 + y_2\sqrt{2}$ have $\log(x_1 + y_1\sqrt{2})(x_2 + y_2\sqrt{2}) = \log(x_1 + y_1\sqrt{2}) + \log(x_2 + y_2\sqrt{2})$

$\Rightarrow$ ~~...~~ $\underbrace{\{\log(x + y\sqrt{2}) \mid x^2 - 2y^2 = 1\}}_{G}$ forms group under $+$.

- $\log(3 + 2\sqrt{2})$ is least positive element (of logs!)

Why can't $\log(x + y\sqrt{2})$ with $x, y > 0$ be smaller & positive: Because $x - y\sqrt{2} < 1 \Rightarrow \log(x - y\sqrt{2}) < 0$.

Can build G from successive $+$ of $\log(3 + 2\sqrt{2})$. Finally, Stillwell (pg. 80-81) argues this construction misses nothing

§ 5.4 THE GENERAL PELL EQUATION

<u>Theme</u>: to solve $x^2 - ny^2 = 1$ we study

$$\mathbb{Z}[\sqrt{n}] = \{x + y\sqrt{n} \mid x, y \in \mathbb{Z}\}$$

$$\mathbb{Q}[\sqrt{n}] = \{x + y\sqrt{n} \mid x, y \in \mathbb{Q}\}$$

Def^{n}/ $\text{norm}(x + y\sqrt{n}) = x^2 - ny^2$

think of $x, y \in \mathbb{Q}$ also possible!

$$\overline{x + y\sqrt{n}} = x - y\sqrt{n}$$

<u>Observation</u>: $\text{norm}(z) = z\bar{z}$.

$$\left.\begin{array}{l} z = x + y\sqrt{n} \\ \bar{z} = x - y\sqrt{n} \end{array}\right\} \; z\bar{z} = (x + y\sqrt{n})(x - y\sqrt{n}) = x^2 - ny^2.$$

<u>Proposition</u>
① $\overline{zw} = \bar{z}\,\bar{w}$
② $\text{norm}(zw) = \text{norm}(z)\,\text{norm}(w)$

for $z, w \in \mathbb{Q}[\sqrt{n}]$ (Stillwell focus on $\mathbb{Z}[\sqrt{n}]$ until end, I'm greedier here)

<u>Proof</u>: $z = x + y\sqrt{n}$, $w = a + b\sqrt{n}$ then

① ~~notand~~ $\overline{zw} = \overline{(x + y\sqrt{n})(a + b\sqrt{n})}$

$$= \overline{xa + nby + (ay + bx)\sqrt{n}}$$

$$= xa + nby - (ay + bx)\sqrt{n}$$

$$\bar{z}\,\bar{w} = (x - y\sqrt{n})(a - b\sqrt{n}) = ax + nby - (ay + bx)\sqrt{n}$$

② $\text{norm}(zw) = \overline{zw}\, zw$

$$= \bar{z}\,\bar{w}\, z w$$

$$= \bar{z} z\, \bar{w} w = \text{norm}(z)\,\text{norm}(w).$$

We seek to solve $x^2 - ny^2 = 1$ over $\mathbb{Z}^2$. This amounts to seeking $z = x + y\sqrt{n}$ with $\text{norm}(z) = 1$ as

$$x^2 - ny^2 = \underbrace{(x + y\sqrt{n})}_{z}\underbrace{(x - y\sqrt{n})}_{\bar{z}} = 1$$

~~norm(zz̄) = norm~~ $\underline{\text{norm}(z) = 1}$.

<u>Composition Rule (Brahmagupta ~ 600 AD)</u>

$(x_1, y_1), (x_2, y_2)$ solve $x^2 - ny^2 = 1$

$\Rightarrow (x_3, y_3)$ solves $x^2 - ny^2 = 1$ where

$x_3 = x_1 x_2 + n y_1 y_2$ & $y_3 = x_1 y_2 + x_2 y_1$

<u>Proof</u>: $(x_1, y_1), (x_2, y_2)$ solve $x^2 - ny^2 = 1$

$\Rightarrow z_1 = x_1 + y_1\sqrt{n}$ & $z_2 = x_2 + y_2\sqrt{n}$ are of $\text{norm}(z_1) = 1$ and $\text{norm}(z_2) = 1$. But,

$\text{norm}(z_1 z_2) = \text{norm}(z_1)\text{norm}(z_2) = 1 \cdot 1 = 1$.

Hence $z_3 = z_1 z_2$ also corresponds to $z_3 = x_3 + y_3\sqrt{n}$ which gives (x_3, y_3) solving $x^2 - ny^2$. Note,

$$(x_1 + y_1\sqrt{n})(x_2 + y_2\sqrt{n}) = x_1x_2 + y_1y_2(\sqrt{n})^2 + x_1y_2\sqrt{n} + y_1x_2\sqrt{n}$$

$$= \underbrace{x_1x_2 + ny_1y_2}_{x_3} + \underbrace{(x_1y_2 + x_2y_2)}_{y_3}\sqrt{n} \quad //$$

Remark: once again <u>all</u> sol$^{\underline{n}}$'s of $x^2 - ny^2 = 1$ flow from the positive sol$^{\underline{n}}$ $x + y\sqrt{n}$ which is smallest. The sol$^{\underline{n}}$ $(1,0) \longrightarrow 1 + 0\sqrt{n}$ serves as the multiplicative identity.

Example: $x^2 - 3y^2 = 1$

can guess smallest sol$^{\underline{n}}$ is $(2,1)$

$$(2+\sqrt{3})(2+\sqrt{3}) = 4 + 3 + 4\sqrt{3} = 7 + 4\sqrt{3} \rightarrow \underline{(7,4)}.$$

$$(2+\sqrt{3})^3 = (2+\sqrt{3})(7+4\sqrt{3}) = 14 + 12 + 15\sqrt{3} = 26 + 15\sqrt{3} \longrightarrow \underline{(26,15)}.$$

Worlds Collide

ADDITION	MULTIPLICATION
$\log(2+\sqrt{3}) + \log(2-\sqrt{3}) = 0$	$(2+\sqrt{3})(2-\sqrt{3}) = 1$
$\log(x+y\sqrt{3}) + \log(x-y\sqrt{3}) = 0$	$(x+y\sqrt{3})(x-y\sqrt{3}) = 1$

why? prop. of logs.

If $\log(x+y\sqrt{3}) > 0$ then $\log(x-y\sqrt{3}) < 0$

If $\underbrace{(x+y\sqrt{3}) > 1}_{\text{positive log}}$ then $\underbrace{(x-y\sqrt{3}) < 1}_{\text{negative log}}$

$\log = \ln$