Rewriting some notes:

Pell's Equation

- Key tool in proving a^n u Dio is Pell's eq'n
- For fixed $d \in \mathbb{N}$ this u eq'n:

$$x^2 - dy^2 = 1$$

- Can factor LHS of $(x+\sqrt{d}y)(x-\sqrt{d}y)$ ↳ suggests we might consider the integral domain $\mathbb{Z}[\sqrt{d}]$

comm. ring → no zero divisors

$$= \{x+\sqrt{d}y : x, y \in \mathbb{Z}\}$$

- for $\alpha = x + \sqrt{d}y \in \mathbb{Z}[\sqrt{d}]$
  the conjugate of α u $\bar{\alpha} = x - \sqrt{d}y$
  the norm of α u $\|\alpha\| = \alpha \cdot \bar{\alpha}$
  $= x^2 - dy^2$

- Solving Pell's same as finding $\alpha \in \mathbb{Z}[\sqrt{d}]$ s.t. $\|\alpha\| = 1$

Prop'n the set of positive solutions $S = \{\alpha \in \mathbb{Z}[\sqrt{d}] : \alpha > 0, \|\alpha\| = 1\}$ is a group under usual multiplication.

Pf:- Given $\alpha \in S$, since $\overline{\overline{\alpha}} = \alpha$ and $\alpha \cdot \overline{\alpha} = 1$ follows $\|\overline{\alpha}\| = 1$
$\Rightarrow \overline{\alpha} \in S$, also $\overline{\alpha}$ = mult. inverse of $\alpha \Rightarrow S$ closed under inverses

- if $\alpha, \beta \in S$ easy to check $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$
so that $\|\alpha\beta\| = \alpha\beta \cdot \overline{\alpha}\,\overline{\beta} = 1 \cdot 1 = 1$
$\Rightarrow \alpha\beta \in S$ so S closed under products ✓

- We call S "set of positive solutions to Pell's eq'n $x^2 - dy^2 = 1$"
- But really it's the set of $x + \sqrt{d}\,y > 0$ s.t. $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ is a sol'n.

$\mathbb{R}^+ = (0, \infty)$ Here is a general fact about multiplicative subgroups of $(\mathbb{R}^+, \cdot)$

Prop'n Sps $(G, \cdot)$ is a subgroup of $(\mathbb{R}^+, \cdot)$. Then either G is dense in $\mathbb{R}^+$ or discrete (i.e. no limit points)
If G is discrete and γ = least el't of $G > 1$, we have $G = \{\gamma^n : n \in \mathbb{Z}\}$

and not {1} We prove instead.

Additive version: Sps $(G,+)$ is a subgroup of $(\mathbb{R},+)$. Then G is either dense in $\mathbb{R}$ or discrete.

If discrete and g = least el't >0 we have $G = \{n \cdot g : n \in \mathbb{Z}\}$ (and not $\{0\}$)

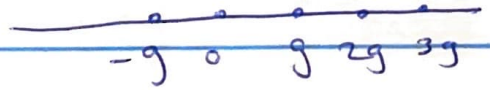
$n \cdot g = g+g+\cdots+g$

Pf: - Sps G is not dense and not $\{0\}$
- then $\exists a, b \in G$ w/ $a<b$ but no elements between.
- Let $g = b-a = b+(-a) \in G$ since a subgroup
- then $g > 0$
- cannot have $0<h<g$ since then would have $a < a+h < b = a+g$
- Similarly cannot have $n \cdot g < h < (n+1)g$ for any $n \in \mathbb{Z}$

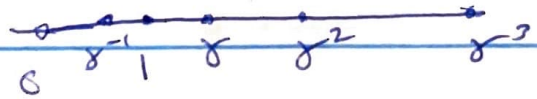
$\Rightarrow G = \{n \cdot g : n \in \mathbb{Z}\}$ as claimed. ✓

To get multiplicative version, note (e.g.) $x \to e^x$ is a group isomorphism of $(\mathbb{R},+)$ with $(\mathbb{R}^+,\cdot)$, and $A \subseteq \mathbb{R}$ is dense iff $e^{[A]} \subseteq \mathbb{R}^+$ is dense. ✓

discrete in $\mathbb{R}$: ex



discrete in $\mathbb{R}^+$



e.g. $\{\frac{1}{2^n} : n \in \mathbb{Z}\}$ is a discrete subgroup of $\mathbb{R}^+$ generated by $\gamma = \frac{1}{2}$

Prop'n says: all non-dense subgroups have such a generator.

Upshot: if S is set of positive sol'ns to Pell's, then if S not dense, then discrete and generated by least sol'n $x + \sqrt{d}y > 1$.

Turns out S is never dense.

Prop'n Sps $\alpha = x + \sqrt{d}y$ and $\|\alpha\| = 1$.
If $\alpha \geq 1$ then $x \geq 1$ and $y \geq 0$.
Moreover $S = \{\alpha : \|\alpha\| = 1\}$ is discrete

Pf:- Note $\alpha + \bar{\alpha} = 2x$ and $\alpha - \bar{\alpha} = 2\sqrt{d}y$
- Also $\alpha \geq 1 \Rightarrow \bar{\alpha} \leq 1$ (mult. inverse of α)
- So if $\alpha \geq 1$ then $\alpha + \bar{\alpha} = \alpha + \frac{1}{\alpha}$ which is always ≥ 2 (for $\alpha \geq 0$, check it!)
- Hence $x \geq 1$ as claimed.
- of course $\alpha - \bar{\alpha} = \alpha - \frac{1}{\alpha} \geq 0 \Rightarrow y \geq 0$

For second statement, observe if $S = \{1\}$ (i.e. no sol'ns to $x^2 - dy^2 = 1$

except trivial sol'n $x=1, y=0$) then nothing to show.

- o.w. at least two solutions
- by prev. prop'n must be two sol'ns >1 say $\alpha = x+y\sqrt{d}$, $\alpha' = x'+y'\sqrt{d}$
- follows by above x, x' both >1 and y, y' both >0 and x, x' distinct and y, y' distinct

Important

- Notice $x > x'$ iff $y > y'$ (Why: $x^2 - y^2 d = 1 = x'^2 - y'^2 d$)
- So sps wlog $x > x'$
- Then $\alpha - \alpha' = (x-x') + (y-y')\sqrt{d}$ which is definitely ≥ 1 since $x-x'$ and $y-y'$ both ≥ 1.

Follows S is discrete ✓

Putting prop'ns together: if $x^2 - dy^2 = 1$ has a nontrivial solution then it has a generating sol'n: namely least $\alpha = x+\sqrt{d}y$ sol'n that is >1.

Then $S = \{\alpha^n : n \in \mathbb{Z}\}$ for this α.

Suggests use Pell's to define an exp growing function

- We will consider the specid cases when $d = a^2 - 1$ for some $a \geq 1$

- In this case $(x, y) = (a, 1)$ is a sol'n since $x^2 - dy^2 = a^2 - (a^2-1) \cdot 1 = 1$

e.g. if $a = 2$ $\alpha = 2+\sqrt{3}$

- corresponds to $\alpha = a + \sqrt{a^2-1} \in S$.
- we claim this α generates S
- need to check: $\nexists \alpha' \in S$, $1 < \alpha' < \alpha$
- if there were such $\alpha' = x + \sqrt{a^2-1}\, y$ we knew $\bar{\alpha} = x - \sqrt{a^2-1}\, y$ also a sol'n (and mult. inverse of α')
- since $\alpha' < \alpha$ we have
  $\frac{1}{\alpha'} \alpha > 1$ i.e. $\bar{\alpha'} \cdot \alpha > 1$
  i.e. $(x - \sqrt{a^2-1}\, y)(a + \sqrt{a^2-1}) > 1$
  i.e. $(ax - (a^2-1)y) + (x - ay)\sqrt{a^2-1} > 1$

and thus is also a sol'n

- by prop'n $x - ay \geq 0 \Rightarrow x \geq ay$
- we knew $y \geq 0$ and hence > 0 since not trivid sol'n hence ≥ 1
  $\Rightarrow$ (*) $x \geq a$
- contradiction since thus forces $y \geq 1$ contradicting (*) $\alpha' < \alpha$. ✓

Since $\alpha = a + \sqrt{a^2-1}$ is our generator we have (x, y) solves $x^2 - dy^2 = 1$ iff $x + \sqrt{a^2-1}\, y = (a + \sqrt{a^2-1})^n$ for some $n \in \mathbb{Z}$

- Focus on positive powers
- define: $x(n,a)$, $y(n,a)$ by the eq'n:

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

- We'll show they
  ① satisfies bounds of Lemma from last time
  ② ∪ Diophantine

- Then by the Lemma, we'll be done!

Start w/ ①, ② ∪ harder.

Claim For all $a \geq 1$, $n \geq 0$ we have

$$(2a-1)^n \leq y(n,a) \leq (2a)^n$$

Pf: key point ∪ we can get recurrence relations for x_n's and y_n's separately

Check that: $(a+\sqrt{a^2-1})^{n+2} = 2a(a+\sqrt{a^2-1})^{n+1} - (a+\sqrt{a^2-1})^n$

i.e.

$$x(a,n+2) + y(a,n+2)\sqrt{a^2-1} = 2a\left(x(a,n+1) + y(a,n+1)\sqrt{a^2-1}\right) - \left(x(a,n) + y(a,n)\sqrt{a^2-1}\right)$$

which gives

$$y(a,n+2) = 2a\, y(a,n+1) - y(a,n)$$

(analogously for $x(a,n+2)$)
- From here, easy induction to prove the bounds. ✓

Proving $y(n,a)$ is Dio is harder. Need lots of modular arithmetic lemmas.

Lemma $y(a,n) \equiv n \pmod{a-1}$

Pf: By binom. thm.

$$(a+\sqrt{a^2-1})^n = \sum_{i}^{n} \binom{n}{i} a^{n-i} \left(\sqrt{a^2-1}\right)^i$$

for i even, $\sqrt{a^2-1}^i$ is integer, for odd is $(a^2-1)^{(i-1)/2}\sqrt{a^2-1}$ — hence only odd terms contribute to $y(a,n)$

$$y(a,n) = \sum_{i \le n, \text{odd}} \binom{n}{i} a^{n-i} (a^2-1)^{(i-1)/2}$$

which is $\equiv n a^{n-1} \pmod{a-1}$

but observe

$$n a^{n-1} = n a^{n-2}(a-1) + n a^{n-2}$$

(iterate:) $$= n a^{n-2}(a-1) + n a^{n-3}(a-1) + \cdots + n(a-1) + n$$

$$\equiv n \pmod{a-1}$$ ✓

We need two crucial Lemmas

Crucial Lemma #1: $y(a,k) \equiv y(a,\ell) \pmod{x(a,n)} \Rightarrow k \equiv \pm \ell \pmod{2n}$

To prove CL#1 will need:

Sublemma (I.) if $a \geq 2$ and $1 \leq m \leq n$ then $y(a,m) \leq x(a,n)/2$

will something write x_k, y_k for $x(a,k)$ $y(a,k)$

Pf: $y(a,n)$ is strictly increasing in n (can see in work above, or note explicitly:)

$$x_{k+\ell} + y_{k+\ell}\sqrt{a^2-1} = (x_k + y_k\sqrt{a^2-1})(x_\ell + y_\ell\sqrt{a^2-1})$$

$$= x_k x_\ell + y_k y_\ell (a^2-1) + (x_k y_\ell + x_\ell y_k)\sqrt{a^2-1}$$

which shows

$$x_{k+\ell} = x_k x_\ell + y_k y_\ell (a^2-1)$$

(*) note for future

$$y_{k+\ell} = x_k y_\ell + x_\ell y_k$$

shows increasing nos of y_n in n then are positive integers.

Hence enough to check $y(a,n) \leq \frac{x(a,n)}{2}$

But of course $x_n^2 - (a^2-1)y_n^2 = 1$
$\Rightarrow y_n^2 = x_n^2 - 1/a^2 - 1 < x_n^2/2$ ✓

Will also need following sublemma. Here we consider $x(a,n)$, $y(a,n)$ for possibly negative n (correspond to solns $x<1$)

Sublemma (II): For $M, k \in \mathbb{Z}$

(1) $y(a, 2M+k) \equiv -y(a,k) \mod x(a,M)$
(2) $y(a, 4M+k) \equiv y(a,k) \mod x(a,M)$
(3) $y(a, 2M-k) \equiv y(a,k) \mod x(a,M)$
(4) $y(a, \varepsilon_0 2M + \varepsilon_1 k) \equiv \pm y(a,k) \mod x(a,M)$
for $\varepsilon_0 \in \{-1,0,1\}$, $\varepsilon_1 \in \{-1,1\}$
(i.e. for any such choice of ε_i's LHS $\equiv$ [illegible] y or $-y$)

pf: this is expressing a kind of periodicity of y's [illegible] (in a given M)

Clearly (1) $\Rightarrow$ (2) (take an extra $+2M$ period)
(1) $\Rightarrow$ (3) also:
follows from general observation:
if $x = x(a,1)$ $y = y(a,1)$ are generating sol'n then since

$$x_k + y_k\sqrt{a^2-1} = (x + y\sqrt{a^2-1})^k$$

must have $x_k - y_k\sqrt{a^2-1} = (x + y\sqrt{a^2-1})^{-k}$
since $\cdot$ is mult. inverse

but this gives $-y_k = y_{-k}$
i.e. $-y(a,k) = y(a,-k)$
which gives (3) from (1)

And (1), (2), (3) $\Rightarrow$ (4)

So enough to prove (1).
As above we have

$$y(a,2M+k) = x(a,2M)\,y(a,k) + x(a,k)\,y(a,2M$$

Now consider:

$$x(a,2M) = x(a,M+M)$$
$$\text{(as above)} = x^2(a,M) + (a^2-1)y^2(a,M)$$
$$\equiv (a^2-1)\,y^2(a,M) \mod x(a,M)$$

But this x and y solve Pell's
$x^2 - (a^2-1)y^2 = 1$
$\Rightarrow -(a^2-1)y^2 \equiv 1 \mod x$
$\Rightarrow (a^2-1)y^2 \equiv -1 \mod x$

i.e. (continuing) $x(a,2M) \equiv -1 \mod x(a,M)$

CTOIt:

$$y(a,2M) = x(a,M)\,y(a,M) + x(a,M)\,y(a,M)$$
$$\equiv 0 \mod x(a,M)$$

Combining these two with ✱ gives (1) ✓