HW 5 due before class Tues, May 5
(last day of class).

Cheat sheet for fictional exam
due Wed, May 6.

Final Topic: Pell's Equation.

$$x^2 - dy^2 = 1 \qquad (d \geq 2 \text{ nonsquare}).$$

Better: $|x^2 - dy^2| = 1$.

I will give you an <u>algorithm</u> to find the complete integer solution.

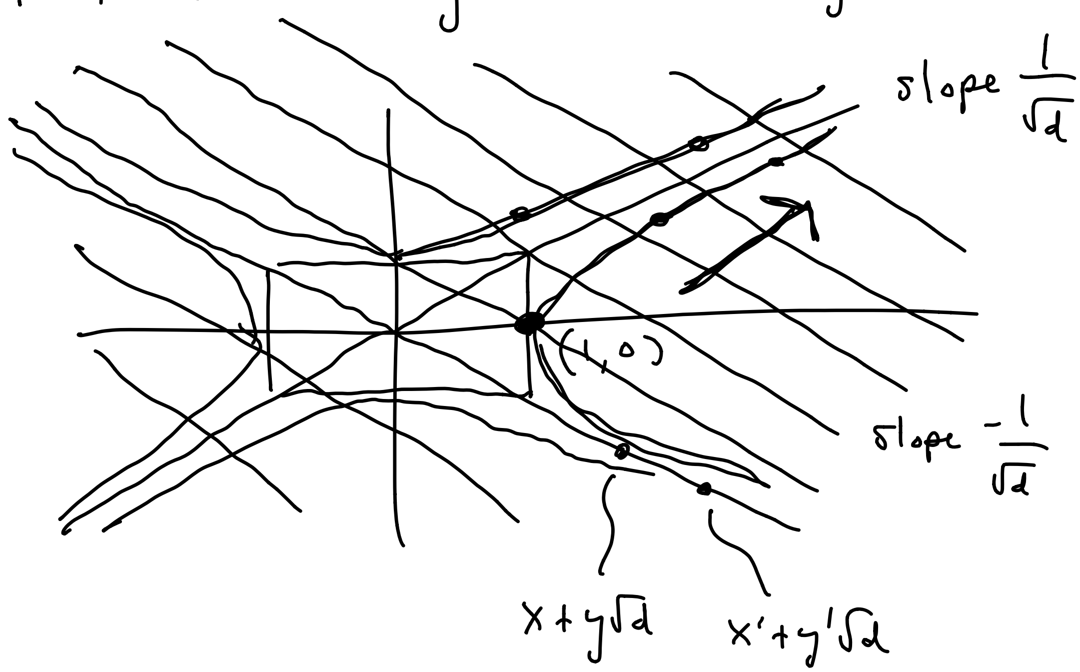
You will practice the algorithm on HW 5.3.

Last Time: Given $d \geq 2$, $\sqrt{d} \notin \mathbb{Q}$.
We proved that $\exists\ x, y \in \mathbb{Z}$ $(y \neq 0)$ such that $x^2 - dy^2 = +1$.

[Lagrange: hard proof, Dirichlet: easier but still hard proof.]

Today: Since $d > 0$, $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{R}$.
Hence elements of $\mathbb{Z}[\sqrt{d}]$ have a natural <u>ordering</u>.

Picture: $x + y\sqrt{d} \longleftrightarrow (x,y) \in \mathbb{R}^2$



$x + y\sqrt{d} = x' + y'\sqrt{d} \iff$ they are on the same line of slope $-1/\sqrt{d}$.

Consider the group of units:

$$U_d = \mathbb{Z}[\sqrt{d}]^\times$$
$$= \{ x + y\sqrt{d} : x, y \in \mathbb{Z},\ |x^2 - dy^2| = 1 \}$$

- This set is ordered
- $x+y\sqrt{d} = x'+y'\sqrt{d}$ & $x,y,x',y' \in \mathbb{Z} \Rightarrow x=x'$ & $y=y'$.
- This set is "discrete"
- From last time $\exists\, u \in \mathcal{U}_d$, $u>1$.
- Hence by well-ordering $\exists$ <u>smallest</u> unit $u>1$.

<u>Theorem</u>: For all $\alpha \in \mathbb{Z}[\sqrt{d}]$,

$$\begin{matrix} \alpha \in \mathcal{U}_d \\ \alpha > 1 \end{matrix} \iff \alpha = u^k \quad (k \geq 1)$$

In other words, if $u = x_1 + y_1\sqrt{d}$ then $|x^2 - dy^2| = 1$

$$\iff \pm x \pm y\sqrt{d} = (x_1 + y_1\sqrt{d})^k$$

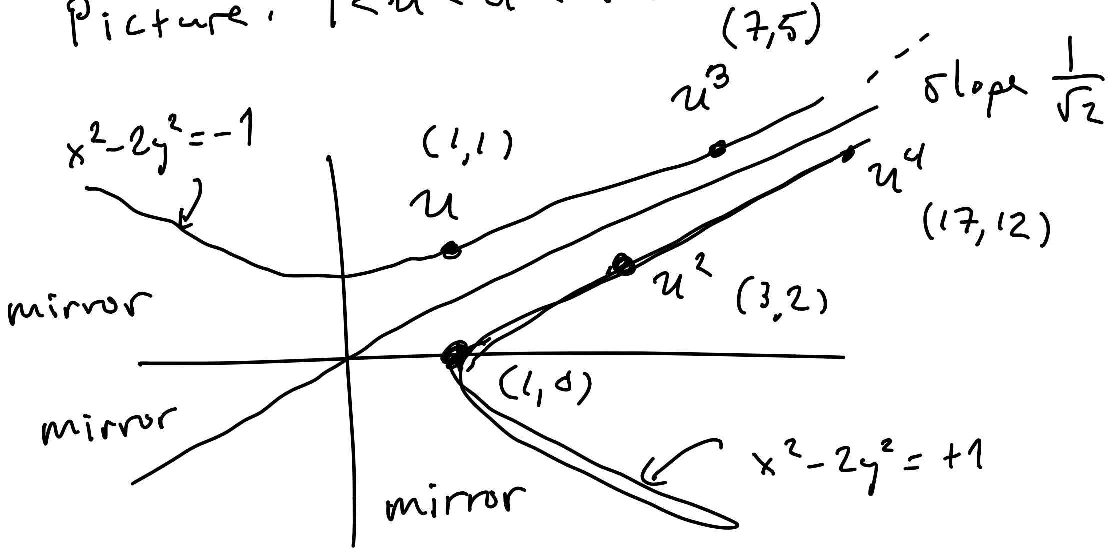
for some $k \geq 0$.

Examples: $d=2$, $u = 1+\sqrt{2}$

$1^2 - 2\cdot 1^2 = -1$ (neg.)

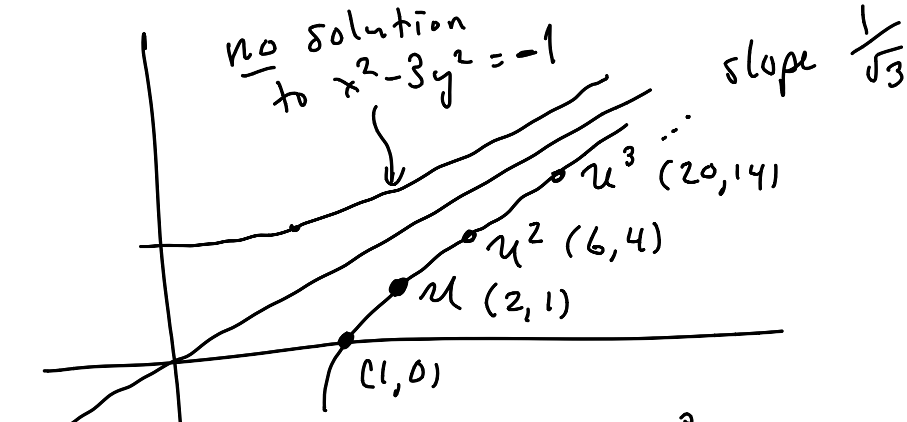
$\downarrow$

Picture: $1 < u < u^2 < u^3 < \cdots$



$d=3$. $\quad u = 2+\sqrt{3}$

$$2^2 - 3\cdot 1^2 = +1 \quad (\text{pos.})$$



$1 < u < u^2 < u^3 < \cdots$

[Remark: $x^2-3y^2=-1 \quad x,y \in \mathbb{Z}$

$\Rightarrow x^2 = -1 \bmod 3$

$x^2 = 2 \bmod 3$ $\lightning$]

Every case looks like one of the two examples above.

Proof: Note $U_d = \{x + y\sqrt{d} : x, y \in \mathbb{Z}, |x^2 - dy^2| = 1\}$ is a "group" under multiplication.

Let $u \in U_d$ be smallest such that $u > 1$. Then for any $\alpha \in U_d$ with $\alpha > 1$ I claim that

$$\alpha = u^k \quad \text{for some } k \geq 1.$$

If not, then we must have

$$1 < u^k < \alpha < u^{k+1} \quad \text{some } k \geq 1$$

Multiply by u^{-k} $(u^{-k} > 0)$ to get

$$1 < \alpha u^{-k} < u.$$

Since $\alpha u^{-k} \in U_d$, this contradicts minimality of u. Q.E.D.

So the whole problem is to compute the fundamental solution u.

Warning: It might not be easy.

For example, Bhaskara II (12th centry) showed that $x^2 - 61y^2 = +1$ has smallest nontrivial solution

$$(x,y) = (1766319049, 226153980).$$

How did Bhaskara find this?!

Idea: If $|x^2 - dy^2| = 1$ then

$$\frac{x}{y} \approx \sqrt{d}.$$

Pell's equation is related to problem of finding rational approximations to square roots.

We will use the language of "continued fractions."

Recall the Euclidean Algorithm:

Given $a, b \in \mathbb{Z}$, $b \neq 0$, compute

$$
\begin{aligned}
a &= q_0 b + r_0 & \qquad 0 &\leq r_0 < |b| \\
b &= q_1 r_0 + r_1 & \qquad 0 &\leq r_1 < r_2 \\
r_0 &= q_2 r_1 + r_2 & \qquad 0 &\leq r_2 < r_3 \\
&\vdots & & \\
r_{k-2} &= q_k r_{k-1} + 0 & &
\end{aligned}
$$

Now observe that

$$
\frac{a}{b} = \frac{q_0 b + r_0}{b} = q_0 + \frac{r_0}{b}
$$

$$
= q_0 + \frac{1}{b/r_0} \qquad \text{repeat.}
$$

$$
= q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots \, q_{k-1} + \cfrac{1}{q_k}}}}
$$

the "continued fraction expansion" of $\frac{a}{b}$.

Theorem: For any rational $\alpha \in \mathbb{Q}$, $\exists$ unique $q_0, q_1, \ldots, q_n \in \mathbb{Z}$ such that
- $q_1, q_2, \ldots, q_n > 0$
- $q_n \neq 1$
- $\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_n}}}$

The proof is not difficult. It follows from uniqueness of quotients & remainders.

Notation:

$$\alpha = [q_0; q_1, q_2, \ldots, q_n] \quad \left(\overset{n}{\underset{i=0}{K}} \overset{\text{Gauss}}{\downarrow} q_i \right)$$

Theorem: More generally, for any irrational $\alpha \in \mathbb{R} - \mathbb{Q}$, $\exists$ unique $a_0, a_1, a_2, \ldots \in \mathbb{Z}$, $a_i \geq 1 \ \forall\, i \geq 1$, such that

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}} \quad \text{forever.}$$

Proof sketch:

(1) Algorithm

(2) Convergence.

(1) Define

$\alpha_0 := \alpha$ $\qquad$ $a_0 := \lfloor \alpha_0 \rfloor$

$\alpha_1 := \dfrac{1}{\alpha_0 - a_0}$ $\qquad$ $a_1 := \lfloor \alpha_1 \rfloor$

$\alpha_2 := \dfrac{1}{\alpha_1 - a_1}$ $\qquad$ $a_2 := \lfloor \alpha_2 \rfloor$

$\vdots$

(2) Since α is irrational, the process goes on forever. You can prove some inequalities to show that it converges. ///

Example: $\alpha = \sqrt{2}$

$\alpha_0 = \sqrt{2} = 1.414$ $\qquad$ $a_0 = 1$

$\alpha_1 = \dfrac{1}{\alpha_0 - a_0} = \dfrac{1}{0.414}$

$= 2.414 \ldots$ $\qquad$ $a_1 = 2$

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{0.414}$$

$$= 2.414\cdots \qquad a_2 = 2$$

$$\vdots$$

It looks like this will repeat.

Proof: $\sqrt{2} = 1 + \dfrac{1}{1+\sqrt{2}}$. ((Check!))

It follows that

$$\sqrt{2} = 1 + \cfrac{1}{1+1+\cfrac{1}{1+1+\cfrac{1}{1+\cdots}}} = 1 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cdots}}}$$

///

$$\sqrt{2} = [1; 2, 2, 2, 2, \cdots]$$
$$= [1; \overline{2}]$$

Question: For which irrational numbers is the C.F.E. "periodic"?

Answer: Given $\alpha \in \mathbb{R} - \mathbb{Q}$,

C.F.E. periodic (eventually) $\Longleftrightarrow$ $a\alpha^2 + b\alpha + c = 0$, $a, b, c \in \mathbb{Z}$.

This surprising result tells us that C.F.E. have same relationship to square roots ...

Here is the Big Theorem of Pell Equations. It was known in various forms to Brahmagupta, Bhaskara, Fermat, ... Euler, and was first proved by Lagrange.

Theorem: Given $d \geq 2$, $\sqrt{d} \notin \mathbb{Q}$, the C.F.E. of $\sqrt{d}$ has the form

$$\sqrt{d} = [a_0; \underbrace{\overline{a_1, a_2, \dots, a_k, 2a_0}}_{\text{this pattern repeats.}}]$$

Furthermore, if we define

$$\frac{p}{q} = [a_0; a_1, a_2, \dots, a_k]_{\text{STOP}}.$$

with $\gcd(p,q) = 1$,

then:

- $p^2 - dq^2 = (-1)^{k+1}$
- $u = p + q\sqrt{d}$ is the smallest unit $u \in U_d$ such that $u > 1$.

///

Proof: Omitted

Conjecture: It seems that

$$a_1, a_2, \ldots, a_k < 2a_0,$$

so we can stop when we see $2a_0$.

[I don't know if this is known.]

Examples: $\alpha = \sqrt{2}$.

$\alpha_0 = \sqrt{2} = 1.414$ $\qquad$ $a_0 = 1$

$\alpha_1 = \dfrac{1}{0.414} = 2.414$ $\qquad$ $a_2 = 2 = 2a_0$ STOP.

$$\sqrt{2} = [1; \overline{2}]$$

$$\frac{p}{q} = [1; \emptyset] = 1 = \frac{1}{1}$$

Fundamental unit $u = 1 + 1\sqrt{2}$.

$1^2 - 2 \cdot 1^2 = -1$ (neg.)

$\alpha = \sqrt{3}$

$\alpha_0 = \sqrt{3} = 1.732$ $\quad a_0 = 1$

$\alpha_1 = \dfrac{1}{0.732} = 1.366$ $\quad a_1 = 1$

$\alpha_2 = \dfrac{1}{0.366} = 2.733$ $\quad a_2 = 2 = 2a_0$

STOP.

$\sqrt{3} = [1; \overline{1, 2}]$

$\dfrac{p}{q} = [1; 1] = 1 + \dfrac{1}{1} = 2 = \dfrac{2}{1}$.

Fundamental unit $u = 2 + 1\sqrt{3}$.

$2^2 - 3 \cdot 1^2 = +1$ (pos.)

$\alpha = \sqrt{14}$

$\alpha_0 = \sqrt{14} = 3.742$ $\quad a_0 = 3$

$\alpha_1 = \dfrac{1}{0.742} = 1.348$ $\quad a_1 = 1$

$\alpha_2 = \dfrac{1}{0.348} = 2.871$ $\quad a_2 = 2$

$\alpha_3 = \dfrac{1}{0.871} = 1.148 \qquad a_3 = 1$

$\alpha_4 = \dfrac{1}{0.848} = 6.757 \qquad a_4 = 6 = 2a_0$

STOP.

$\sqrt{14} = [3; \overline{1, 2, 1, 6}]$ period length 4

$$\frac{p}{q} = [3; 1, 2, 1]$$

$$= 3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1}}} = \frac{15}{4}$$

Fundamental unit $u = 15 + 4\sqrt{14}$

$15^2 - 14 \cdot 4^2 = (-1)^4 = +1.$

Since u is a "positive Pell" solution, we conclude that the "negative Pell" equation $x^2 - 14y^2 = -1$ has no solution.

There is no known rule for predicting the period length of CFE of $\sqrt{d}$.

Also, no known rule to determine if $x^2 - dy^2 = -1$ has a solution.

One more example : $\alpha = \sqrt{41}$

$\alpha_0 = \sqrt{41} = 6.403$ $\qquad a_0 = 6$

$\alpha_1 = \dfrac{1}{0.403} = 2.481$ $\qquad a_1 = 2$

$\alpha_2 = \dfrac{1}{0.481} = 2.080$ $\qquad a_2 = 2$

$\alpha_3 = \dfrac{1}{0.080} = 12.516$ $\qquad a_3 = 12 = 2a_0$

STOP.

$\sqrt{41} = [6;\overline{2,2,12}]$ period length 3

$$\frac{p}{q} = [6;2,2]$$

$$= 6 + \cfrac{1}{2+\cfrac{1}{2}} = \frac{32}{5}.$$

Fundamental unit $u = 32 + 5\sqrt{41}$.

$$32^2 - 41 \cdot 5^2 = (-1)^{\text{period length}} = -1.$$

Conclusion:

- $x^2 - 41y^2 = -1$ has complete solution

$$\pm x \pm y\sqrt{41} = (32 + 5\sqrt{41})^{\text{odd power}}$$

- $x^2 - 41y^2 = +1$ has complete solution

$$\pm x \pm y\sqrt{41} = (32 + 5\sqrt{41})^{\text{even power}}$$

$$= (2049 + 320\sqrt{41})^{\text{any power}}$$

- $|x^2 - 41y^2| = 1$ has complete solution

$$\pm x \pm y\sqrt{41} = (32 + 5\sqrt{41})^{\text{any power}}$$

///