The Final Word

$|N| \leq \sqrt{n}$ and N not a perfect square $\Longrightarrow$ Soln to $x^2 - ny^2 = N$ has $(x,y) = (h_m, k_m)$ some m

Alternate approach to generating new solns from old ones:

$$N = x^2 - ny^2 = (x - \sqrt{n}y)(x + \sqrt{n}y) = \alpha\bar{\alpha} \quad \text{conjugate!}$$

$$1 = x_0^2 - ny_0^2 = (x_0 - \sqrt{n}y_0)(x_0 + \sqrt{n}y_0) = \beta\bar{\beta}$$

Can check $\overline{(\alpha\beta)} = \bar{\alpha}\bar{\beta}$ & write

$$\alpha\beta = (x + \sqrt{n}y)(x_0 + \sqrt{n}y_0) = (xx_0 + nyy_0) + \sqrt{n}(xy_0 + x_0y)$$

then $(\alpha\beta)\overline{(\alpha\beta)} = (\alpha\bar{\alpha})(\beta\bar{\beta}) = N \cdot 1 = N$.

So, e.g., $(\beta^k)\overline{(\beta^k)} = 1$ gives new solns to $x^2 - ny^2 = 1$

Diophantine Eqns

An eqn, like $x^2 - 17y^2 = 3$, where we seek solutions with $x, y \in \mathbb{Z}$, is an example of a Diophantine Eqn.

Often the goal is to describe all solutions.

Ex: $ax + by = c$

(1) Decide if it has a solution. Yes $\Longleftrightarrow (a,b) | c$.

(2) Describe how to generate all solutions.

$$a\overset{\alpha}{\cancel{x_0}}+b\overset{\beta}{\cancel{y_0}}=(a,b) \qquad a\Big(\underbrace{\alpha\tfrac{c}{(a,b)}}_{=x_0}\Big)+b\Big(\underbrace{\beta\tfrac{c}{(a,b)}}_{=y_0}\Big)=c$$

$x_n = x_0 + n\left(\frac{b}{(a,b)}\right)$, $y_n = y_0 + n\left(\frac{a}{(a,b)}\right)$ gives all solutions

---

$ax^2+by=c$ Still need $(a,b)\mid c$.

But also need

$$x_0+n\left(\frac{b}{(a,b)}\right) = x^2 \qquad x^2-x_0 = n\left(\frac{b}{(a,b)}\right)$$

$\cancel{\left(x_0,\frac{b}{(a,b)}\right)=\left(\frac{\alpha c}{(a,b)},\frac{b}{(a,b)}\right)=\left(\frac{\alpha c, b}{(a,b)}\right)}$ $\qquad x^2 \underset{b/(a,b)}{\equiv} x_0.$

Not always true!

x exists $\Longleftrightarrow$ $\cancel{x_0}$ (say $b/(a,b)=p$ prime)

$$x_0^{\frac{p-1}{2}} \underset{p}{\equiv} 1.$$

E.g., $b=4$ $x_0=3$ $a=7$

$21-4k$ $c=1$

$\boxed{7x^2+4y=1 \text{ has no solutions}}$

How about

$$ax^2+by^2=c\ ? \quad \text{Hmm...}$$

Probably the most famous Diophantine eqn is

$$x^2+y^2=z^2.$$

Eqn is homogeneous: (x,y,z) a soln $\Rightarrow$ (cx,cy,cz) sol, all c.

Note: $c\mid x, c\mid y \Rightarrow c^2\mid x^2+y^2=z^2 \Rightarrow c\mid z$

$c\mid x, c\mid z \Rightarrow c^2\mid z^2-x^2=y^2 \Rightarrow c\mid y$

$\Rightarrow$ a common factor of any two is a factor of the third.

Enough to find the solutions with $(x,y)=1$; primitive solns.

First note: z cannot be even:

z even $\Rightarrow$ x,y both even or both odd.

both even $\Rightarrow$ not primitive

both odd $\Rightarrow$ $x^2+y^2 \underset{4}{\equiv} 2$, but $z^2 \underset{4}{\equiv} 0$ $\divideontimes$

$\Rightarrow$ z ~~even~~ odd. $\Rightarrow$ x,y opposite parity, wlog x odd, y even.

A basic technique in solving Diophantine Eqns is to kick the eqn until it reads (product of things) = (product of things), then use what we know about prime factorizations to extract information.

$$\underbrace{x^2+y^2}_{\text{not easy to express as a product!}} = z^2$$

Kick!

$$\underset{(\text{even})}{y^2} = z^2-x^2 = (z-x)(z+x) \Rightarrow \text{one of } (z-x),(z+x) \text{ is even} \Rightarrow \text{both are!}$$

write $z-x = 2a$, $z+x = 2b$, $y=2c$

then $y^2 = z^2-x^2$ becomes $c^2=ab$.

Note: $(a,b)=1$ if $c|a = \frac{z-x}{2}$, $c|b = \frac{z+x}{2}$ then

$c \mid a+b = z$, $c \mid b-a = x$ $\Rightarrow$ $c \mid (x,z)=1$.

Then we use

<u>Lemma</u>: If $(a,b)=1$ and $ab=c^2$ then $a=r^2$, $b=s^2$ for some $r,s\in\mathbb{Z}$.

For p a prime, let $p^\alpha \| \beta$ mean $p^\alpha | \beta$, $p^{\alpha+1} \nmid \beta$.
(α = <u>exact</u> power of p in β)

Suppose $p^\alpha \| a$, then $(a,b)=1 \Rightarrow p \nmid b$ so
$p^\alpha \| ab = c^2 \Rightarrow \alpha$ is even. So every exponent in prime decomp of a is even $\Rightarrow a$ is a perfect square.
b is similar ///

<u>So</u> $\frac{x+z}{2} = a = r^2$, $\frac{z-x}{2} = b = s^2$, some r,s.

Then $x = a-b = r^2-s^2$ (odd, $\Rightarrow r,s$ opposite parity)
$z = a+b = r^2+s^2$
$y^2 = 4ab = 4r^2s^2 = (2rs)^2 \Rightarrow y = 2rs$

<u>Check</u> $(r^2-s^2)^2 + (2rs)^2 = (r^2+s^2)^2$

so these x,y,z <u>are</u> a solution. (r,s opp parity ($r+s$ <u>odd</u>))

<u>So</u>: $x=r^2-s^2$, $y=2rs$, $z=r^2+s^2$ gives <u>all</u> primitive solutions to $x^2+y^2=z^2$ (with x odd, y even) ///

Fri.

If $f(x_1, \dots, x_n) = 0$ has a solution with $x_i \in \mathbb{Z}$ all i,
then it certainly has a soln with $x_i \in \mathbb{R}$ all i.
Also, $f(x_1, \dots, x_n) \underset{m}{\equiv} 0$ has a solution with $x_i \in \mathbb{Z}$
($x_i \in \mathbb{Z}_m$ ...)

A solution to $f(\vec{x}) = 0$ with $\vec{x} \in \mathbb{R}^n$, or
a soln to $f(\vec{x}) \underset{m}{\equiv} 0$ with $\vec{x} \in \mathbb{Z}^n$ is called a <u>local</u> solution to $f(\vec{x}) = 0$.

It is clear that
"global" solution $\Rightarrow$ local soln for all m,
and over $\mathbb{R}$.

Ex:
If $f(\vec{x}) \underset{m}{\equiv} 0$ has no solution for some m, or
$f(\vec{x}) = 0$ has no soln over $\mathbb{R}$, then the
Diophantine eqn $f(\vec{x}) = 0$ has no solution.

Note: The converse is <u>not</u> true: It can be shown that
$x^4 - 17 = 2y^2$ always has a <u>local</u> solution, but has
no <u>global</u> one.

Geometric Approach:

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

Ie. $\alpha^2+\beta^2=1$, $\alpha,\beta\in\mathbb{Q}$.

But since $(0,-1)$ is a solution, then if $(\alpha,\beta)\in\mathbb{Q}^2$ is also a solution, then $\beta+1$, $\alpha-0\in\mathbb{Q}$ so

$\frac{\beta+1}{\alpha}$ = slope of line through $(0,-1)$, (α,β), is $\in\mathbb{Q}$.

Turn this around! Let L = line through $(0,-1)$ with slope $r\in\mathbb{Q}$, ie. $y=rx-1$, and look at where else this hits $x^2+y^2=1$ $\quad [r=a/b]$

$$1=x^2+(rx-1)^2=x^2+r^2x^2-2rx+1$$

$$x^2+r^2x^2=(1+r^2)x^2=2rx$$

$$x=0 \ \underline{\text{or}} \ x=\frac{2r}{1+r^2}=\frac{2ab}{a^2+b^2}$$

$$y=rx-1=\frac{2r^2}{1+r^2}-1=\frac{r^2-1}{r^2+1}=\frac{a^2-b^2}{a^2+b^2}$$

So any other point $(\alpha,\beta)\in\mathbb{Q}^2$ on $x^2+y^2=1$ is of the form $\left(\frac{2ab}{a^2+b^2},\frac{a^2-b^2}{a^2+b^2}\right)$, ie.,

$$\boxed{x=2ab,\ y=a^2-b^2,\ z=a^2+b^2.}$$

$x^2+y^2=nz^2$ $\qquad$ $\left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2=n$ $\qquad$ DID

$n=5$

$\Longrightarrow \exists\ \alpha,\beta\in\mathbb{Z} \quad \alpha^2+\beta^2=n$

$x^2+y^2=n \quad x,y\in\mathbb{Q} \Rightarrow r=\frac{\beta-y}{\alpha-x}\in\mathbb{Q}.$

$y-\beta=r(x-\alpha) \qquad y=r(x-\alpha)+\beta \qquad r=\frac{a}{b}$

$$n=x^2+(r(x-\alpha)+\beta)^2=x^2+r^2(x-\alpha)^2+2r(x-\alpha)\beta+\beta^2$$

$$=n+(x^2-\alpha^2)+r^2(x-\alpha)^2+2r\beta(x-\alpha)$$

$$0=(x-\alpha)\left((x+\alpha)+r^2(x-\alpha)+2r\beta\right)$$

$\Longrightarrow x=\alpha$ or $\cancel{x+\alpha+r^2+2r\beta=0}$ $\quad x(1+r^2)+\alpha-r^2\alpha+2r\beta=0$

$$x=\frac{r^2\alpha-\alpha-2r\beta}{1+r^2}=\frac{a^2\alpha-b^2\alpha-2ab\beta}{a^2+b^2}$$

$y=r(x-\alpha)+\beta=$

$=$

$$\beta+\frac{a}{b}\left(\frac{a^2\alpha-b^2\alpha-2ab\beta}{a^2+b^2}-\alpha\right)$$

$$=\beta+\frac{a}{b}\left(\frac{-2ab\beta-2b^2\alpha}{a^2+b^2}\right)$$

$$=\frac{a^2\beta+b^2\beta-2a^2\beta-2ab\alpha}{a^2+b^2}=\frac{b^2\beta-a^2\beta-2ab\alpha}{a^2+b^2}$$

$x=(a^2-b^2)\alpha-(2ab)\beta,\quad y=(b^2-a^2)\beta-(2ab)\alpha;\quad z=a^2+b^2$

where $\boxed{\alpha^2+\beta^2=n}$

<u>Check</u>

$$x^2+y^2 = \left((a^2-b^2)\alpha + (2ab)\beta \right)^2 + \left((b^2-a^2)\beta - (2ab)\alpha \right)^2$$

$$= (a^2-b^2)^2\alpha^2 - 2(a^2-b^2)(2ab)\alpha\beta + (2ab)^2\beta^2$$
$$+ (b^2-a^2)^2\beta^2 - 2(b^2-a^2)(2ab)\alpha\beta + (2ab)^2\alpha^2$$

$$= (a^2-b^2)^2(\alpha^2+\beta^2) + (2ab)^2(\alpha^2+\beta^2)$$

$$= n\left((a^4 - 2a^2b^2 + b^4) + 4a^2b^2 \right)$$
$$= n\left((a^2+b^2)^2 \right) = nz^2 \quad \checkmark\checkmark !!$$