Mathematical Enrichment   SAT 28th JAN 2017

Kevin HUTCHINSON: Number Theory

whole numbers, integers : ...−2, −1, 0, 1, 2, 3, 4, 5, ...

properties of integers: prime or composite
factors, divisibility

"Diophantine Equations":   Find (some or all) integer solutions to a given equation.

A very classical example:

Find all integer solutions x, y, z to the equation

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

[The equation has lots of real solutions

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

$\sqrt{2}$ is not an integer

In fact, $\sqrt{2}$ is not even a rational number

is of the form $\frac{m}{n}$ where m, n are integers

$1^2 + 2^2 = (\sqrt{5})^2$ .. and so on

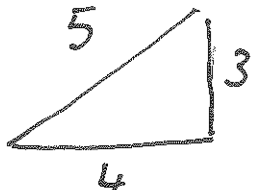
not an integer, not even rational

in general $\underset{\overset{\|}{x}}{a^2} + \underset{\overset{\|}{y}}{b^2} = \underset{\overset{\|}{z}}{\left(\sqrt{a^2+b^2}\right)^2}$]

Want <u>integers</u> x, y, z such that

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

One solution $(x, y, z) = (3, 4, 5)$:



$3^2 + 4^2 = 5^2$

"Pyth<u>agorean</u> tr<u>iple</u>"

["Trivial" solutions : $(0, 0, 0)$

$(\pm m, 0, \pm m)$

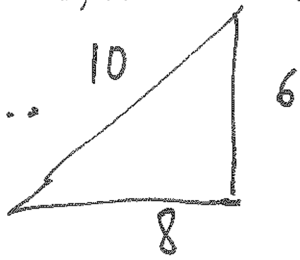
$(0, n, n)$]

$\times 2$

One non-trivial solution:

$(3, 4, 5)$, $(6, 8, 10)$, $(9, 12, 15)$, ... $(3m, 4m, 5m)$....

$(5, 12, 13)$, $(10, 24, 26)$, ...



$$\begin{array}{ccccc} 5^2 & + & 12^2 & = & 13^2 \\ \| & & & & \| \\ 25 & + & 144 & = & 169 \end{array}$$

Suppose (m, n, ℓ) is a solution (Pyth. triple)
$\ell \neq 0$.

So $m^2 + n^2 = \ell^2$

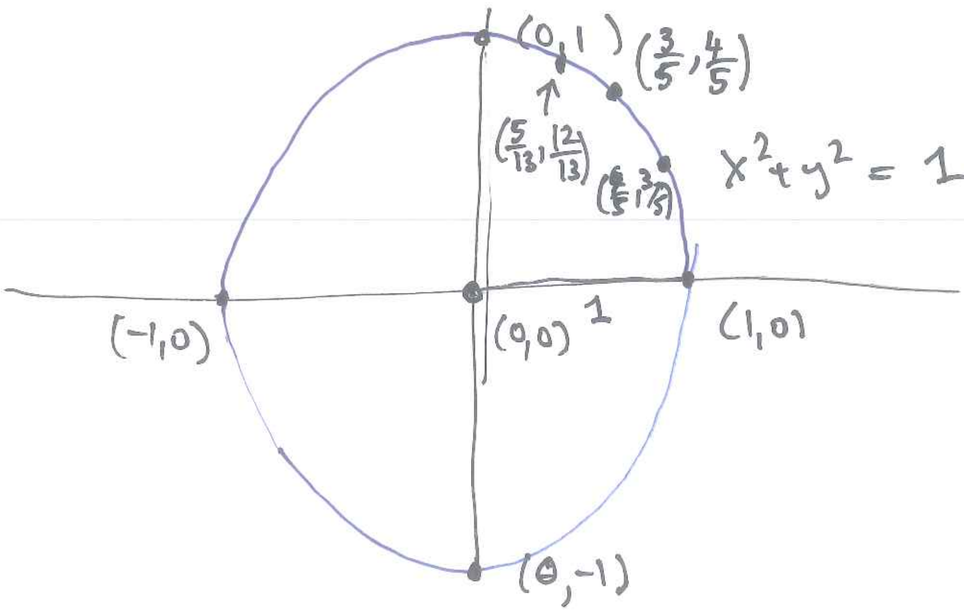
$\Rightarrow \left(\frac{m}{\ell}\right)^2 + \left(\frac{n}{\ell}\right)^2 = 1$

Eg. $\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$

$\left(\frac{5}{13}\right)^2 + \left(\frac{12}{13}\right)^2 = 1$

i.e. $\left(\frac{m}{\ell}, \frac{n}{\ell}\right)$ is a point with rational coordinates

on the curve $x^2 + y^2 = 1$



(x,y)-plane

$x^2 + y^2 = 1$. (unit circle)

Conversely, suppose (p, q) is a rational point

on $x^2 + y^2 = 1$: $p = \frac{m}{\ell}$, $q = \frac{n}{\ell}$ (take a common denom ℓ)

$= \frac{tm}{t\ell}$, $q = \frac{tn}{t\ell}$

$\left(\frac{m}{\ell}\right)^2 + \left(\frac{n}{\ell}\right)^2 = 1 \implies m^2 + n^2 = \ell^2$

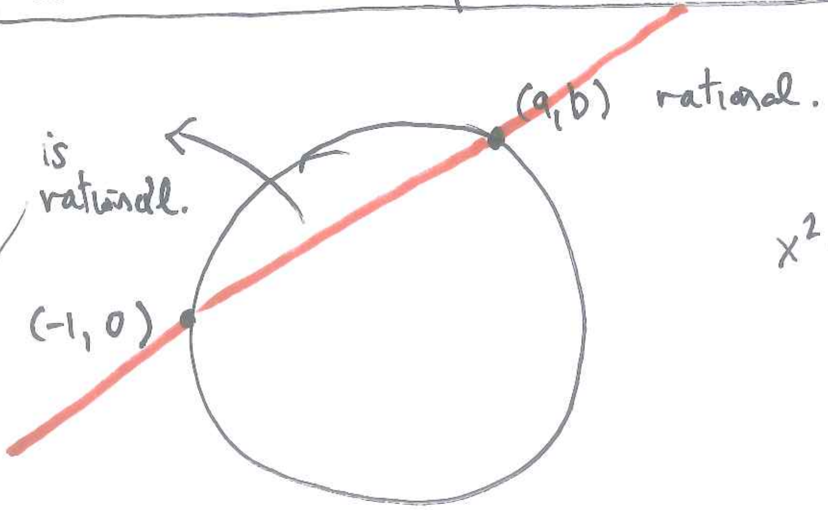
$\Rightarrow (m, n, \ell)$ is a Pyth. triple.

$(tm, tn, t\ell)$

So our problem can be reformulated as an equivalent problem:

<u>Find all rational points on the unit circle.</u>

slope $\frac{b}{a+1}$ is rational.



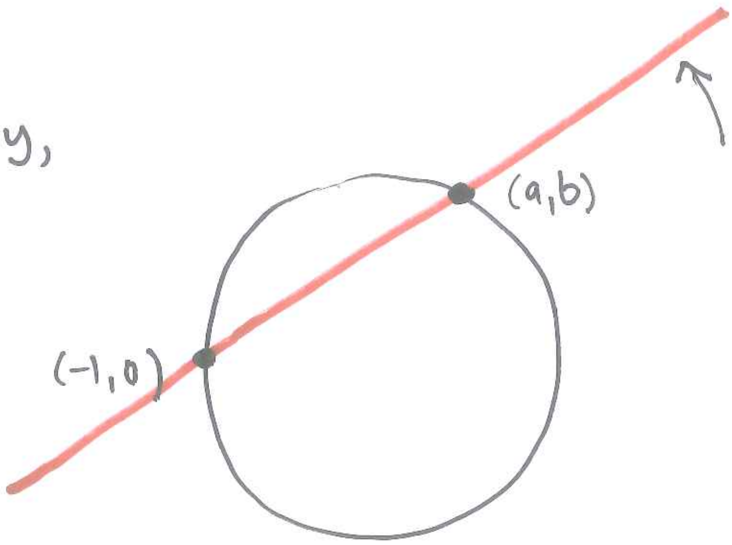
$$x^2+y^2=1.$$

since sums, products quotients of rationals are again rational.

$$\frac{p}{0\neq q} = \frac{m/n}{a/b} = \frac{mb}{an}$$

$$\frac{m}{n} + \frac{a}{b} \quad \frac{bm}{bn} + \frac{an}{bn} = \frac{bm+an}{bn}$$

Conversely,



line with slope t rational

<u>Claim</u>:

* Then (a,b) is a rational point.

1st: Recall some facts about quadratics

$$\cancel{3}2x^2 - 5x + 3 = 0$$
$$\parallel$$
$$(2x-3)(x-1) = 0$$

roots: $x-1=0$ $\quad \boxed{x=1}$

$2x-3=0$ $\quad \boxed{x=3/2}$

$$ax^2 + bx + c = 0$$

roots $\Big\|$ r_1, r_2.

$$a(x-r_1)(x-r_2) = a(x^2 - (r_1+r_2)x + r_1r_2)$$
$$\parallel$$
$$= ax^2 - a(r_1+r_2)x + ar_1r_2$$

So $\quad b = -a(r_1+r_2)$

$\quad\quad c = ar_1r_2$

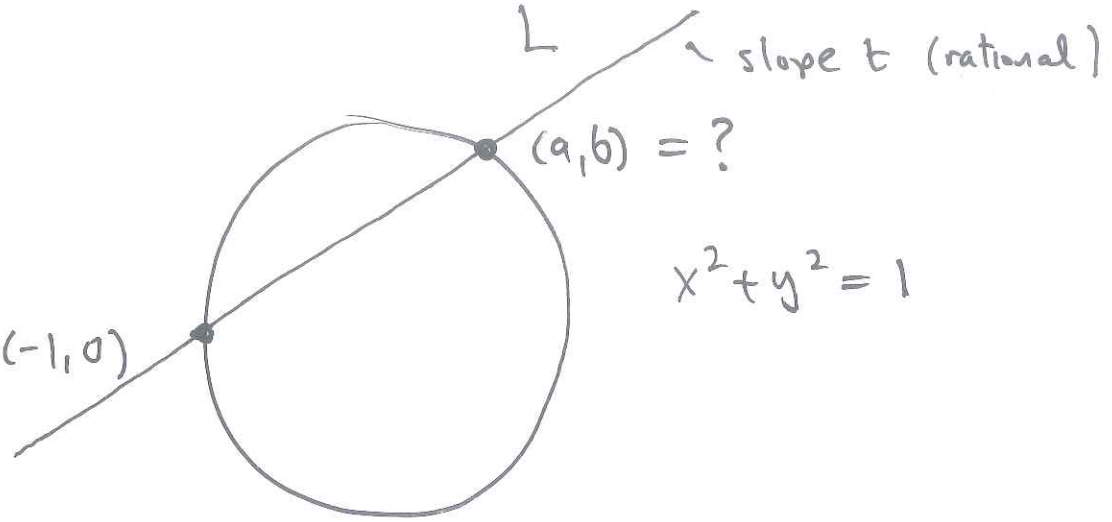
Consequence: Suppose a, b, c are rational and we know $r_1 \neq 0$ is rational.

Then $r_2 = \frac{1}{r_1} \cdot \frac{c}{a}$ is also rational.

Eg. $\quad 2x^2 - 5x + 3 = 0$

Observe $x = 1$ is a root.

$\rightarrow$ other root is $r_2 = \frac{1}{1} \cdot \frac{3}{2} = 3/2$.



Equation of L: $y - 0 = t\cdot(x+1)$

fixed rational number

$y = t(x+1)$.

Let $y = t(x+1)$ in $x^2+y^2=1$:

$x^2 + [t(x+1)]^2 = 1$

(i) This is a quadratic in x

(ii) one root is $x=-1$

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

(iii) The other root is a, which must be rational.

$x^2 + t^2x^2 + 2t^2x + t^2 - 1 = 0$

(iv) $b = t(a+1)$ is also rational.

i.e.

$\otimes$ $(t^2+1)x^2 + 2t^2x + t^2-1 = 0$

$x=-1$ is one root. So the other is

$$a = \frac{1}{-1}\cdot\frac{t^2-1}{t^2+1} = \frac{1-t^2}{1+t^2}$$

$$\therefore\ b = t(a+1) = t\cdot\left(\frac{1-t^2}{1+t^2}+1\right) = t\cdot\frac{2}{1+t^2} = \frac{2t}{1+t^2}$$

Conclusion The rational points on the unit circle are precisely the points

$$a = \frac{1-t^2}{1+t^2}, \quad b = \frac{2t}{1+t^2}, \quad t \text{ any rational number}$$

(and the point $(-1,0)$)

Let $t = \frac{m}{n}$

Then $$a = \frac{1-\frac{m^2}{n^2}}{1+\frac{m^2}{n^2}} = \frac{\frac{n^2-m^2}{n^2}}{\frac{n^2+m^2}{n^2}} = \frac{n^2-m^2}{n^2+m^2}$$

$$b = \frac{2\cdot\left(\frac{m}{n}\right)}{\frac{n^2+m^2}{n^2}} = \frac{\frac{2mn}{n^2}}{\frac{n^2+m^2}{n^2}} = \frac{2mn}{n^2+m^2}$$

So The rational points on the unit circle are

$$a = \frac{n^2-m^2}{n^2+m^2}, \quad b = \frac{2mn}{n^2+m^2} \qquad n, m \text{ integers.}$$

Recipe for

$\Rightarrow$ all Pythagorean triples are ~~obtained~~ of the form

$$(n^2-m^2,\ 2mn,\ n^2+m^2) \qquad n, m \text{ integers.}$$

$$\boxed{\text{i.e.} \quad (n^2-m^2)^2 + (2mn)^2 = (n^2+m^2)^2}$$

eg. $n=2, m=1$: $(3, 4, 5)$

$n=3, m=1$: $(8, 6, 10)$

$n=3, m=2$: $(5, 12, 13)$

$\vdots$

Some exercises.

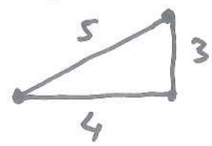
(a) Find all rational points on the ellipse

1 $$2x^2 + 5y^2 = 7$$

(b) Find all triples (a, b, c) of integers satisfying $2a^2 + 5b^2 = 7c^2$

2 Find 4 points in the plane, not all collinear, such that the distance between any pair is a whole number

(Eg. 3 points:



)

. . . 5 points . . . . . .

. . —

. . . 7 points . . . .

Show that for any $N > 2$, there are N points, not all collinear, such that all distances are integers.

Prime factorization

$$12 = 2^2 \cdot 3$$

$$36 = 2^2 \cdot 3^2$$

$$72 = 2^3 \cdot 3^2$$

$$1000 = 10^3 = (2 \cdot 5)^3 = 2^3 \cdot 5^3.$$

$$6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1$$

$$= 2^4 \cdot 3^2 \cdot 5.$$

Exercise (a) Find the prime factorization

of $10! = 1 \times 2 \times \cdots \times 9 \times 10$

of $20! = 1 \times 2 \times \cdots \times 19 \times 20$

(b) Calculate the total number of

divisors / factors of $10!$

of $20!$