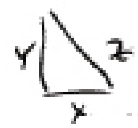
12/6/04

CONGRUENT NUMBER PROBLEM

<u>Def.</u> A positive integer n is called <u>congruent</u> if there exists a right triangle



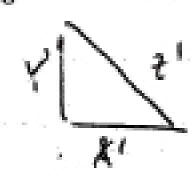
$X, Y, Z \in \mathbb{Q}$ $\frac{1}{2}XY = n$.

Question: Given $n \in \mathbb{Z}_{>0}$ is it congruent?

It is enough to analyze the values $n \in \mathbb{Z}_{>0}$ in squarefree.

$n = m^2 n'$ n' squarefree

$\frac{1}{2}XY = n$



$\frac{1}{2}X'Y' = n'$

$\longleftrightarrow$

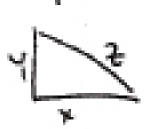
$x = mx'$
$y = my'$

- we shall refer to

$X < Y < Z$ and

<u>Proposition</u> Given $n \in \mathbb{Z}_{>0}$ squarefree, $\exists$ a right triangle $X < Y < Z$ $\frac{1}{2}XY = n$ $X, Y, Z \in \mathbb{Q}$, iff $\exists\, x \in \mathbb{Q}$ s.t. $x, x-n, x+n$ are in $(\mathbb{Q}^*)^2$.

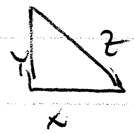
X, Y, Z $\longmapsto$ $x = (Z/2)^2$



$X = \sqrt{x+n} - \sqrt{x-n}$
$Y = \sqrt{x+n} + \sqrt{x-n}$
$Z = 2\sqrt{x}$

$\longleftarrow$ x

Pf.



$\frac{1}{2}XY = n$ $\Rightarrow$ $(X+Y)^2 = Z^2 + 4n$

$X^2+Y^2=Z^2$ $\quad$ $(X-Y)^2 = Z^2 - 4n.$

$$\left(\frac{X\pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n. \qquad x = \left(\frac{Z}{2}\right)^2 \qquad x,\ x+n,\ x-n \text{ all squares.}$$

So map is well-defined.

(Map is surjective)

$x = u^2$ define $X = \sqrt{x+n} - \sqrt{x-n}$, $Y = \sqrt{x+n}+\sqrt{x-n}$ $\quad Z = 2\sqrt{x}$

then show $X^2+Y^2=Z^2$ and $\frac{1}{2}XY = n.$

(map is injective)

if $X_0, Y_0, Z_0 \longrightarrow x$ $\Rightarrow$ $X_0^2+Y_0^2 = Z^2$ $\quad \frac{1}{2}X_0Y_0 = n$

$X_1, Y_1, Z_1 \longrightarrow x$ $\quad X_1^2+Y_1^2 = Z^2$ $\quad \frac{1}{2}X_1Y_1 = n.$

$\Downarrow$

$(X_0+Y_0)^2 = Z^2+4n = (X_1+Y_1)^2$

$X_0+Y_0 = X_1+Y_1$

$X_0Y_0 = X_1Y_1$ $\Rightarrow$ $X_0 = X_1$, $Y_0 = Y_1$ given $X_0 < Y_0$, $X_1 < Y_1$

$$\begin{cases} X, Y, Z \longmapsto x = \left(\frac{Z}{2}\right)^2 \\ X^2+Y^2=Z^2 \\ \frac{1}{2}XY = n \end{cases}$$

$(X\pm Y)^2 = Z^2 \pm 4n$

(multiply 2 relations)

$$\left(\frac{X^2-Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2$$

$\Downarrow$

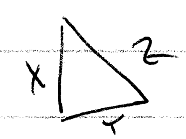
$v = \frac{X^2-Y^2}{4}$ $\quad u = \frac{Z}{2}$

$$u^4 = v^2 + n^2$$

$$u^6 - n^2u^2 = (uv)^2 \qquad \text{Denote} \quad u^2 = x, \; uv = y$$

Then $x^3 - n^2 x = y^2$ (*)

Look for necessary conditions on a solution of (*) s.t. it corresponds to a triple X, Y, Z

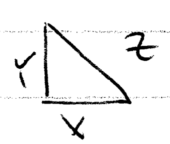


$\frac{1}{2}XY = n$.

① x must be the square of a rational.

② x must have 2 as a factor of its denominator.

X, Y, Z



$\frac{1}{2}XY = n$

$\exists\, a \in \mathbb{Q}$ aX, aY, aZ is a reduced Phythagorean triple

Suppose numerator of Z is even.

$\Downarrow$

aZ is also even or else a is even

③ The numerator of x and n do not have any primes in common.

(p odd) $p \mid$ num of $x \Rightarrow p \mid$ num of $x \pm n \Rightarrow$
$p \mid$ num of $\left(\frac{X \pm Y}{2}\right)^2 \Rightarrow p \mid$ num of $\frac{X \pm Y}{2} \Rightarrow p \mid$ num of X, num of Y,

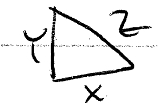
$\Rightarrow p^2 \mid$ num of $\frac{XY}{2} \Rightarrow p^2 \mid n$ (impossible)

$p = 2$ also contradiction.

Proposition. (x,y) is a rational sol. of $y^2 = x^3 - n^2x$ satisfying

(i) $x \in \mathbb{Q}^2$

(ii) the denominator of x is even

(iii) the num. of x and n do not have any common prime factors. Then $\exists$ a triple $\underset{\mathbb{Q}}{X, Y, Z}$  s.t. $\frac{1}{2}XY = n$.

Pf. • $x = (s/t)^2$ $\gcd(s,t) = 1$, $s,t \in \mathbb{Z}$.

• $u = (s/t)$;

• $v = y/u$; $v^2 = \frac{y^2}{u^2} = \frac{y^2}{x} = x^2 - n^2$

So $\boxed{n^2 + v^2 = x^2.}$

$n \in \mathbb{Z} \Rightarrow$ x, v have the same denominator t^2

$x, v, n \Rightarrow$ $t^4x^2 = t^4n^2 + t^4v^2$

t^2x, t^2n, t^2v is a reduced pythagorean triple.

$\Rightarrow \begin{cases} p \mid s^2 \\ p \nmid t. \end{cases} \Rightarrow p^2 \mid t^2x$

$t^2u = 2ab$

$t^2v = a^2 - b^2$

$t^2x = a^2 + b^2$

$X = \frac{2a}{t}$

$Y = \frac{2b}{t}$

$Z = 2a$

$\dashrightarrow$