9/15/04.

Rational points on rational conic.

Def. rational ~~curve~~ conic

$C: ax^2+bxy+cy^2+dx+ey+f=0$

Def. rational points.

$\mathbb{Q}^2 \subset \mathbb{R}^2$

Def. rational line:

$ax+by+c=0$

Prop 1) intersection of two rationals is rational point

2) 2 rational points → rational line

ex: $\begin{cases} x^2+y^2=1 \\ x=2y \end{cases}$

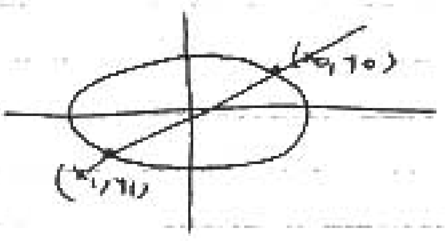
$ax^2+bx+c=0$ $\quad a,b,c\in\mathbb{Q}$.

One root rational $\Rightarrow$ the other is

$-\frac{b}{a}$

$C: \quad ax^2+bxy+cy^2+dx+ey+f=0$

$(x_0,y_0)\in C \quad x_0,y_0\in\mathbb{Q}$.



rational points on C ⟶ rational lines through $(x_0,y_0)$

Ex. $\boxed{C : x^2+y^2=1}$

$(1,0) \in C.$

Solve : $\begin{cases} m(x-1) = y \\ x^2+y^2=1 \end{cases}$

substitute $y = m(x-1)$

$m^2(x-1)^2 + x^2 = 1$

$(m^2+1)x^2 - 2m^2x + (m^2-1) = 0$

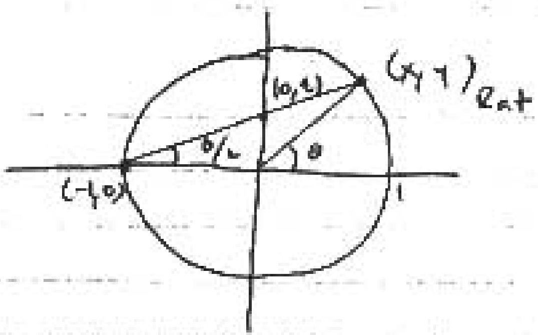
$x = 1$

$\frac{2m^2}{m^2+1}$ = sum of root

$$\boxed{x = \frac{m^2-1}{m^2+1} , y = \frac{2m}{m^2+1}}$$

9/15/04.

$(-1,0)$



$x = \cos\theta$
$y = \sin\theta$

$t = \tan\left(\frac{\theta}{2}\right)$

$$x = \frac{1-t^2}{1+t^2} \quad , \quad y = \frac{2t}{1+t^2}$$

$$X^2+Y^2=Z^2 \qquad \gcd(X,Y,Z)=1$$
$$Z \neq 0.$$

WLOG $x$ odd, $y$ even

Why? $X$ odd $\Rightarrow X^2 \equiv 1 \ (4)$

$$(2n+1)^2 = 4(n^2+n)+1$$

$$X^2+Y^2 \equiv 2 \ (4)$$

Cont.

$$x^2+y^2=1 \qquad x = \frac{X}{Z} \quad y = \frac{Y}{Z}$$

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

$$\frac{X}{Z} = x = \frac{1-\left(\frac{m}{n}\right)^2}{1+\left(\frac{m}{n}\right)^2} = \frac{n^2-m^2}{n^2+m^2}$$

$$\frac{Y}{Z} = y = \frac{2mn}{m^2+n^2}$$

$n^2 - m^2 = \lambda X$

$2mn = \lambda Y$

$m^2 + n^2 = \lambda Z$

Want $\lambda = 1$

$\lambda = 2n^2$

$\lambda = 2m^2$ $\Longrightarrow$ $\lambda | 2$

$\lambda = 1$ or $2$.

Suppose $\lambda = 2$

$X\lambda \equiv 2 \equiv n^2 - m^2$

(mod 4) $(n^2, m^2)$ $(0,0) \longrightarrow 0$

$(1,0) \longrightarrow 1$

$(0,1) \longrightarrow 3$

Cont $(1,1) \longrightarrow 0$

$\lambda = 1$

$X = n^2 - m^2$

$Y = 2mn$

$Z = n^2 + m^2$

$x^2 + y^2 = 3$

$x = \frac{X}{Z} \quad y = \frac{Y}{Z}$

$X^2 + Y^2 = 3Z^2$

$X \equiv \pm 1 \quad Y \equiv \pm 1 \pmod 3$

$X^2 + Y^2 \equiv 2 \mod 3.$

Cont.

$aX^2 + bY^2 \pm cZ^2 \quad (*)$

(Legendre) $aX^2 + bY^2 \equiv cZ^2 \pmod m$