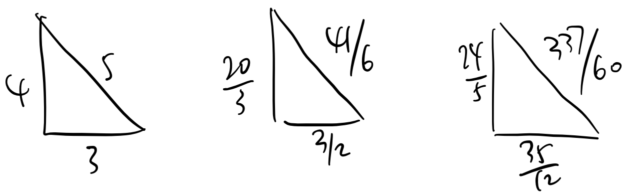
(B) Riemann Surface (Donaldson)

(A) Introduction to Elliptic Curves and Modular Forms

同余数. n. positive integer.

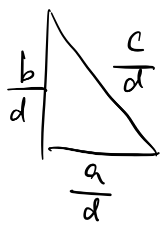
<u>Def.</u> n is a congruent number if it is the area of a rational right triangle



6 5 7

<u>Thm.</u> (Fermat). 1 is not a congruent number

<u>pf.</u> 反证法. If. 1 is $\frac{a}{d}$ $\frac{b}{d}$ $\frac{c}{d}$



a, b, c, d positive integer, $\gcd(a,b,c,d)=1$.

$$\begin{cases} a^2+b^2=c^2 \\ ab=2d^2 \end{cases} \Rightarrow a, b \text{ 互素. (假设有素因子)} \quad (a,b)=1$$

$\Rightarrow$ 一奇一偶 . (如果两奇, $a^2+b^2 \bmod 4$ 余 2 $\neq c^2$)

$$\begin{cases} a. \text{ even} & c \text{ odd} \\ b. \text{ odd} & d. \text{ odd} \end{cases}$$

整体递降成

$$\begin{cases} a'^2+b'^2=c'^2 \\ a'b'=2d'^2 \end{cases}$$

矛盾.

① $ab=2d^2$ 因子要么全给a. 要么全给b

$$\begin{cases} a=2k^2 \\ b=\ell^2 \end{cases} \quad k, \ell \in \mathbb{N}$$

$$4k^4+b^2=c^2$$

$$4k^4=c^2-b^2$$

②

$$k^4=\underbrace{\frac{c+b}{2}\,\frac{c-b}{2}}_{\text{互素}} \Rightarrow \frac{c+b}{2}=r^4,\quad \frac{c-b}{2}=s^4$$

故因子全给个.

$$\Rightarrow b=\frac{c+b}{2}-\frac{c-b}{2}=r^4-s^4$$

$$b=\ell^2$$

$$\boxed{\ell^2=(r^2-s^2)(r^2+s^2)}$$

ℓ odd

r,s 互素

$\Rightarrow (r^2-s^2)$ 与 (r^2+s^2) 互素

同时得到
这个方程无解
$x^n+y^n=z^n$
$n=4$

③

$$\Rightarrow \begin{cases} r^2-s^2=t^2 \\ r^2+s^2=u^2 \end{cases}$$

$$r^2=\frac{t^2+u^2}{2}=\left(\frac{t+u}{2}\right)^2+\left(\frac{t-u}{2}\right)^2$$

$$\frac{t+u}{2}\,\frac{t-u}{2}=\frac{t^2-u^2}{4}=\frac{s^2}{2}$$

$$=2\left(\frac{s}{2}\right)^2$$

$a'=\frac{t+u}{2}$

$b'=\frac{t-u}{2}$

$c'=r$

$d'=\frac{s}{2}$

比较 c': $r=\sqrt[4]{\frac{c+b}{2}}<\sqrt[4]{c}\le c$ 矛盾 无穷递降. □

Conj. $n\equiv 5,6,7\ (8)$. YES!

$n\equiv 1\ 2\ 3\ (8)$ 100%. NO! inf. many YES.

$$\lim_{N\to\infty}\frac{\#\{n\equiv 1,2,3\ (8)\quad n<N,\ n \text{ congruent}\}}{\#\{n\equiv 1,2,3\ (8)\quad n<N\}}=0$$

↓ suppose n. square free

Thm (Tunnell).

n. sq-free positive number.

(A). n is a congruent number

(B). $\#\{(x,y,z)\in\mathbb{Z}^3 \mid 2x^2+y^2+8z^2=n\}$

$=2\#\{(x,y,z)\in\mathbb{Z}^3 \mid 2x^2+y^2+32z^2=n\}$

(A) $\Rightarrow$ (B).

If we assume weak form BSD conj. then (B) $\Rightarrow$ (A)

化归到丢番图方程问题 "不定方程".

some picture

Prop. Fix a sq-free positive integer n some

Then 只需证单射. ?

斜边和 Area 固定 ⇒ 三边固定

$$\left\{\begin{array}{l} 0<X<Y<Z\in\mathbb{Q} \\ X^2+Y^2=Z^2 \\ XY=2n \end{array}\right\} \xleftrightarrow{\text{id}} \left\{\begin{array}{l} x\in\mathbb{Q} \\ x,\ x+n,\ x-n \\ \text{are all sq of rationals} \end{array}\right\}$$

$\| $

T_n

$$(X,Y,Z) \longmapsto x=\left(\frac{Z}{2}\right)^2$$

$$\left(\sqrt{x+n}-\sqrt{x-n},\ \sqrt{x+n}+\sqrt{x-n},\ 2\sqrt{x}\right) \longleftarrow x$$

Pf. $\left(\frac{Z}{2}\right)^2\pm n=\frac{Z^2}{4}\pm n=\frac{X^2+Y^2}{4}\pm\frac{XY}{2}=\frac{X^2+Y^2\pm 2XY}{4}=\left(\frac{X\pm Y}{2}\right)^2$

$$\begin{cases} (X+Y)^2 = X^2+Y^2+2XY = Z^2+4n \\ (X-Y)^2 = Z^2-4n \end{cases}$$

$$(X^2-Y^2)^2 = Z^4-16n^2$$

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

$$\left(\left(\frac{X^2-Y^2}{4}\right)\left(\frac{Z}{2}\right)\right)^2 = \left(\frac{Z}{2}\right)^6 - n^2\left(\frac{Z}{2}\right)^2$$

$$\begin{cases} x = \left(\frac{Z}{2}\right)^2 \\ y = \left(\frac{X^2-Y^2}{4}\right)\left(\frac{Z}{2}\right) \end{cases} \qquad \boxed{y^2 = x^3 - n^2x}$$

1. 为什么转化? → 次数已最低

2. 为什么能转化?

(x, y) should satisfy?

① $x \in \mathbb{Q}^2_{>0}$. $X^2+Y^2=Z^2$

② $2 \mid$ denonenter of x $\exists\, s.\ sX, sY, sZ \in \mathbb{Z}_{>0}$

$\mathrm{val}_2(x) < 0$ odd $\gcd(\ldots) = 1$

③ If $p \mid n$, then $\mathrm{val}_p(x) \leq 0$.   若 Z 分子里有 2.

Valuation

p prime. $x = \frac{a}{b} \neq 0$

$p \nmid a$. $\mathrm{val}_p(x) := -d$ s.t. $p^d \parallel b$

$p \mid a$. $\mathrm{val}_p(x) := d$ s.t. $p^d \parallel a$

$\mathrm{val}_3(\frac{1}{3}) = -1$ $\qquad$ $\mathrm{val}_3(\frac{9}{4}) = 2$

$\mathrm{val}_3(\frac{2}{9}) = -2$

<u>claim</u> if $p \mid n$

$\mathrm{val}_p(x) \leq 0$

if $v = \mathrm{val}_p(Z) > 0$.

$\mathrm{val}_p(x) = 2v$

看 $\boxed{y^2 = x^3 - n^2 x}$

$6v > 2v+2$

$\Rightarrow \mathrm{val}_p(y) = v+1$

$\Rightarrow p \parallel \frac{X^2 - Y^2}{2}$ $\qquad$ and we have

$XY = 2n$

$p \mid X$

or $p \mid Y$

$\Downarrow$

$p \mid X.\ p \mid Y \Rightarrow p^2 \mid \frac{X^2 - Y^2}{2}$ $\times$

Prop. Fix a sq-free positive integer n.

If. $(x, y) \in \mathbb{Q}^2_{>0}$ satisfying $y^2 = x^3 - n^2 x$. & ① ② ③

then $x = (\frac{Z}{2})^2$. for some $(X, Y, Z) \in T_n$

Pf. 只需证. $x.\ x+n.\ x-n.$ 为 sq of rationals

$$x(x+n)(x-n) = x^3-n^2x = y^2$$

$y^2 \to$ val_p even for all p.

$\downarrow$

考互素 ✓

$\forall$ odd prime. p. if $p \mid x$, $p \mid x+n$. $\Rightarrow p \mid x-n$. $\triangle$

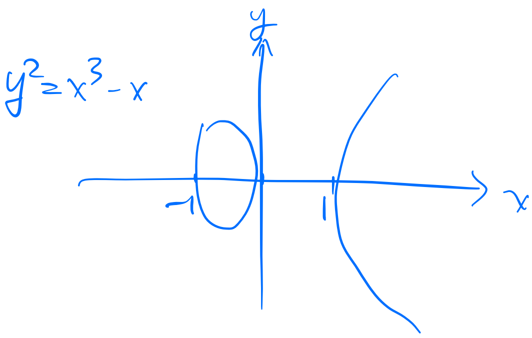
2. x. $\mathrm{val}_2(x) < 0$ $\leftarrow$ because of this.

$$\mathrm{val}_2(x) = \mathrm{val}_2(x+n) = \mathrm{val}_2(x-n)$$

$\nearrow$ $\mathrm{val}_2(x) + \mathrm{val}_2(x+n) + \mathrm{val}_2(x-n) = \mathrm{val}_2(y^2)$ $\to$ even

$\Rightarrow$ $\mathrm{val}_2(x)$, $\mathrm{val}_2(x+n)$, $\mathrm{val}(x-n)$ even. $\square$

elliptic curve



① K field char 0.

$$y^2 = x^3 + ax^2 + bx + c = P(x) \in K[x]$$

satisfying $P(x)$ has no root of multiplicity >1

② All ell curve/R is a geom connected smooth projection curve C over K of genus one, togther with a point O. in $C(K)$.

(C, O).