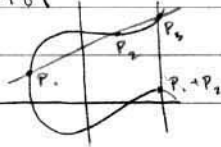


18.781

7 May 2003



$$E: y^2 - x^3 - Ax - B = 0 \quad A, B \in \mathbb{Q}$$

$$E(\mathbb{Q}, +)$$

Notation: If $N > 0$ int, $P \in E(\mathbb{Q})$, then write $N \cdot P = \overbrace{P+P+\dots+P}^{N \text{ times}}$

ex: $x^3 + y^3 = 9$ has infinitely many rational points

$$x_0 = 2 \quad y_0 = 1 \quad z_0 = 1$$

$$x_{n+1} = x_n(x_n^2 + 2y_n^2) \quad y_{n+1} = y_n(2x_n^2 + y_n^2) \quad z_{n+1} = z_n(x_n^3 - y_n^3)$$

In suitable coordinates, this is

$$(-1)^n \cdot 2^n \cdot (2, 1)$$

$$\text{and } -2^n \cdot (2, 1) = P \text{ s.t. } P + 2^n(2, 1) = O.$$

Example of E for which $E(\mathbb{Q})$ is finite.

Thm. The equation $u^4 + v^4 = w^2$ has no integer solutions with $uvw \neq 0$ and $w > 0$.

Proof: "Method of Descent"

suppose (u, v, w) is an integer sol'n with w minimal.

• Assume no prime divides all of u, v, w

If \exists prime p , $p|u, p|v, p|w$.

$$\text{Then } p^4 | L.H.S. \Rightarrow p^4 | R.H.S. \Rightarrow p^2 | w, \text{ so } (u/p, v/p, w/p^2)$$

is a solution.

• $u \neq v$ are not both odd.

$$\text{If } u, v \text{ odd, } u^4 + v^4 \equiv 2 \pmod{4}, \text{ but } w^2 \equiv 0, 1 \pmod{4}.$$

Assume u odd, v even.

$$v^4 = (w - u^2)(w + u^2)$$

$$\text{Claim: } (w - u^2, w + u^2) = 2.$$

since v even, 2 certainly divides $w - u^2, w + u^2$.

$$\text{suppose } p^a | w - u^2, p^b | w + u^2,$$

$$\text{Then } p^a | 2w, p^a | 2u^2 \Rightarrow p|w \text{ and } p|u \Rightarrow p|v,$$

contradiction if $p \neq 2$.

$$\text{case 1: } w - u^2 = 2a^4 \quad a > 0$$

$$w + u^2 = 8b^4 \quad a \text{ odd, } (a, b) = 1$$

$$\text{case 2: } w - u^2 = 8b^4$$

$$w + u^2 = 2a^4 \quad a \text{ odd, } a > 0, (a, b) = 1$$

We know v^4 has a power of 2^n , so we "distribute" this between the two factors s.t. $\gcd = 2$.

$$\text{case 1: } u^2 = -a^4 + 4b^4 \Rightarrow 1 \equiv -1 \pmod{4}. \text{ contradiction.}$$

$$\text{case 2: } w = a^4 + 4b^4 \quad 0 < a < w$$

$$4b^4 - a^4 = -u^2 \Rightarrow 4b^4 = (a^2 - u)(a^2 + u)$$

From the same reasoning as above,

$$(a^2 - v, a^2 + v) = 2$$

so $a^2 - v = 2c^4 \Rightarrow a^2 = c^4 + d^4$ so (c, d, a) is a new sol'n
 $a^2 + v = 2d^4$ with $0 < a < w$. contradiction.

Thrm/Example: The only rational pts. on the curve $E: y^2 = x^5 - 4x$ are
 $(2, 0), (0, 0), (-2, 0), O$

Proof: $P = (x_0, y_0) \in E(\mathbb{Q}), y_0 \neq 0$.

Line through $(0, 0)$ and P :

$$L: y = \frac{y_0}{x_0} x$$

$$\left(\frac{y_0}{x_0} x\right)^2 - x^5 + 4x = 0. \quad (mx)^2 - x^5 + 4x = 0.$$

Notation: $m = y_0/x_0$

$$(x^2 - m^2 x - 4) = 0$$

x_0 is a sol'n and rational $\Rightarrow \sqrt{m^2 + 16}$ is rational.

$$\Rightarrow \left(\frac{m}{2}\right)^2 + 1 = n^2 \text{ for some } n \in \mathbb{Q}.$$

Gives rational sol'n to eqn $u^4 + 1 = v^2$.

$u = \frac{a}{b}, v = \frac{c}{d}$. Multiply by $b^4 d^4$, clearing denominators.

$$(ad)^4 + (bd)^4 = (b^2 dc)^2,$$

which is an int. sol'n to $u^4 + v^4 = w^2$.

can't happen unless $v = 0, \Rightarrow m = 0 \Rightarrow y_0 = 0$.

contradiction.

$A = (2, 0), B = (0, 0), C = (-2, 0)$.

+	O	A	B	C	(Klein 4-grp).
O	O	A	B	C	point: $A+B=C$
A	A	O	C	B	$\Rightarrow P^2 = (-2, 0)$
B	B	C	O	A	Also, $2C=O$, since
C	C	B	A	O	$C=-C$.

O

A

B

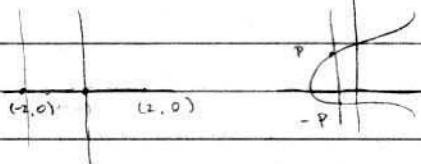
C

point: $A+B=C$

$\Rightarrow P^2 = (-2, 0)$

Also, $2C=O$, since

$C=-C$.



This is $\mathbb{Z}/2 \times \mathbb{Z}/2$

$$(a, b) + (a', b') = (a+a', b+b'), \quad a, a', b, b' \in \mathbb{Z}/2.$$