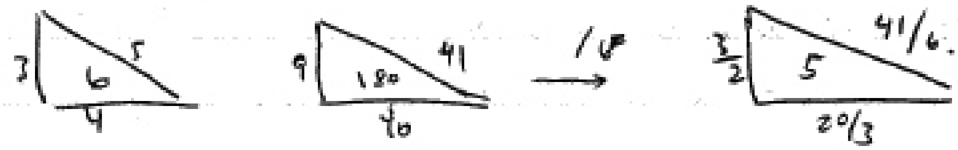
12/8/04

Def. A <u>congruent number</u> is an integer which is the area of a right Δ with rational sides.



Let $E_n(\mathbb{Q})$ be the elliptic curve $y^2 = x^3 - n^2 x$. Then n is congruent $\Longleftrightarrow$ $E_n(\mathbb{Q})$ has nonzero rank. (i.e. ∞-many rational points on E_n).

Thm 1. Let $q = p^f$, $p \nmid 2n$. Suppose $q \equiv 3 \pmod 4$. Then $|E_n(\mathbb{F}_q)| = q+1$.

pf. Four points of order 2: $\infty, (0,0), (\pm n, 0)$.
Find points $(x,y) \in E_n(\mathbb{F}_q)$ with $x \neq 0, \pm n$.
Arrange the $q-3$ x's left in pairs $\pm x$.
$f = x^3 - n^2 x$ Now $f(x) = -f(-x)$ (f is odd)
Since -1 is not a square in $\mathbb{F}_q$, exactly one of $f(x)$, $f(-x)$ is a square. So for each pair $\pm x$ we get 2 points in $E_n(\mathbb{F}_q)$ $(x, \pm\sqrt{f(x)})$ or
$(-x, \pm\sqrt{f(x)})$

So the $q-3$ pairs give $q-3$ points
So $|E_n(\mathbb{F}_q)| = q+1$.

By Mordell's Thm, $E_n(\mathbb{Q})$ is finitely generated.
So $E_n(\mathbb{Q}) \cong E_n(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$ $r = $ rank.

Prop. 2 The ~~# of~~ rational pts of finite order on E_n are ∞, $(0,0)$, $(\pm n, 0)$.

Pf. We will construct a homomorphism from $E_n(\mathbb{Q}) \hookrightarrow E_n(\mathbb{F}_p)$ in the obvious way. Given $[x,y,z] \in \mathbb{P}^2_{\mathbb{Q}}$, choose $[x,y,z]$ to be relatively prime integers; then reduce these mod p to get a point $\bar{p} = [\bar{x}, \bar{y}, \bar{z}] \in \mathbb{P}^2_{\mathbb{F}_p}$.
Let x be a point over $\mathbb{Q}$ on E_n, of finite order >2.
Either x is odd order or else the group of points of order $|4$ has order 8 or 16. So $S = E_n(\mathbb{Q})_{tors}$ ~~So $S = E_n(\mathbb{F}_p)$~~ has a subgroup with $|S| = 8$, or $|S|$ is odd. $|S| = m$.

Now for all p for which E_n "has good reduction" we have $m \mid \# E_n(\mathbb{F}_p)$. Now by Thm 1, for all but finitely many primes $p \equiv 3 \pmod 4$ we have $p \equiv -1 \bmod m$.
If $m = 8$ for all but finitely many primes $p \equiv 3\ (4)$, $p \equiv (7)\ 8$. So there are finitely many primes of the form $8k+3$.
If m odd, $3 \mid m$, then for all but finitely primes $p \equiv 3\ (4)$ $p \equiv (-1 \bmod m) \Rightarrow p \equiv -1 \bmod 3 \Rightarrow p \equiv 11 \bmod (12)$.

So we have finitely many primes of form $12k+7$.

If m odd, $3 \nmid m$, finitely many primes of form $4mk+3$.
Contradicts Dirichlet's Thm. This proves our proposition.

Let $2E_n(\mathbb{Q}) - \{\infty\}$ denote the double of rational points on E_n, minus the point at ∞.

Prop. 3 There is a 1-1 correspondence between right triangles w/ rational sides $X < Y < Z$ and area n, and pairs of points $(x, \pm y) \in 2E_n(\mathbb{Q}) - 0$ by the map

$$(x, \pm y) \longmapsto \left(\sqrt{x+n} - \sqrt{x-n},\ \sqrt{x+n} + \sqrt{x-n},\ 2\sqrt{x}\right)$$

$$\left(\frac{Z^2}{4}, \pm (Y^2 - X^2)Z/8\right) \longleftarrow (X, Y, Z)$$

Prop. 4 Let E be the curve $y^2 = (x-e_1)(x-e_2)(x-e_3)$, $e \in \mathbb{Q}$ and let $P = (x_0, y_0) \in E(\mathbb{Q})$. Then $P \in 2E(\mathbb{Q})$ iff $x_0 - e_i \in \mathbb{Q}^{*2}$, $i = 1, 2, 3$.

Translate x_0 to be 0.

Sketch. Pf. if $Q \in E(\mathbb{Q})$ s.t. $2Q = P$, then there are four points $Q, Q_1, Q_2, Q_3 \in E(\mathbb{Q})$ with $2Q_i = P$. $Q_i = Q + (e_i, 0)$

Choose $Q = (x, y)$ s.t. $2Q = P = (0, y_0)$. We will find conditions for Q to be rational.

Now, $m \in \mathbb{C}$ is the slope of a line from $-P$, tangent to the curve, iff $\exists$ double root of

$$* \quad (mx - y_0)^2 = (x-e_1)(x-e_2)(x-e_3) = x^3 + ax^2 + bx + c$$

$$\Downarrow$$

$x^2 + (a - m^2)x + (b + 2my_0) = 0$ has double root. i.e. $(a - m^2)^2 = 4(b + 2my_0) = 0$.

Will show that $-e_i \in \mathbb{Q}^2$ is equivalent to this.

a, b are symmetric in the e_i, y_0 is not but is symmetric in $\sqrt{e_i} = f_i$.

⋮ part of proof omitted.

<u>Thm 5</u>. n is a congruent # iff $E_n(\mathbb{Q})$ has nonzero rank.

Pf. From Prop. 3, if n is congruent, then $2E_n(\mathbb{Q}) - O \neq \phi$, and conversely.

But ~~iff~~ $2E_n(\mathbb{Q})_{tors} = O$ so $2E_n(\mathbb{Q})_{tors} - O$ is empty.

So to have $2E_n(\mathbb{Q}) - O \neq \phi$, must have a point on curve of order >2, so by prop. 1, of infinite order, so $r \geq 1$.