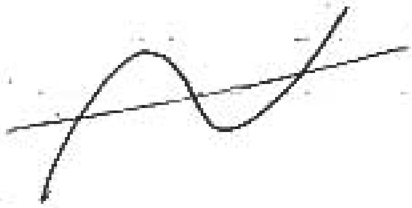
why so many late people today?

9/17/04.

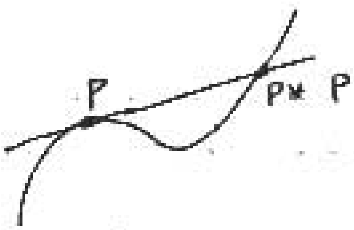
Start 1:06 pm.

$$ax^3 + bx^2y + cxy^2 + dy^2 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

$x^3 + y^3 = 1$ homo $x^3 + y^3 = z^3$



P, Q ~~rational~~ $\in \mathbb{Q} \to P*Q \in \mathbb{Q}$



<u>Mordell's Theorem</u>: If you have a nonsingular rational cubic curve, then there is a <u>finite</u> set of rational points on the curve such that <u>all</u> rational points on the curve can be found using the above method.

*) Two cubic curves generally intersect in 9 places.

1) use the projective plane (i.e. can intersect at ∞)
2) allow multiplicities of intersections

3) Allow complex numbers for coordinates.

ignore this.

Bezout: ~~A~~ Two curves of degree n and m ~~meet~~ intersect at $n \times m$ points. (irreducible).

Thm. Let C, C_1, C_2 be three cubic curves, and C_1 and C_2 intersect in nine points. Then if C goes through 8 of the 9 intersection points, then it also goes through the last one.

(Said: Proof on p. 17.)

Aside No way to know in a finite # of steps if the given rational cubic has a rational point.

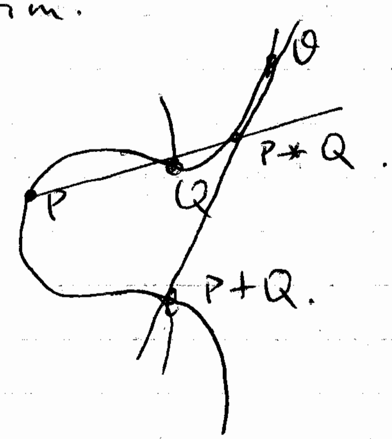
$$aX^2 + bY^2 = cZ^2 \text{ has a solution in } \mathbb{Z} \text{ not } (0,0,0)$$

iff

$$aX^2 + bY^2 \equiv cZ^2 \bmod (m)$$ if this has Solution in $\mathbb{Z}$ relatively prime to m.

$3x^3 + 4y^3 + 5z^3 = 0$ has no integer solutions other than $(0,0,0)$
for all m, $3x^3 + 4y^3 + 5z^3 \equiv 0 \bmod (m)$ has a solution.

Addition



$P+Q = \mathcal{O} * (P * Q)$

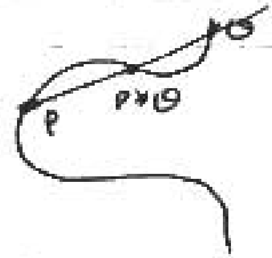
9/17/04.

Recall

Group $(G, +)$

1. identity O, $g \in G$ $g + O = O + g = g$
2. closed $g_1, g_2 \in G$, $g_1 + g_2 \in G$.
3. Every elmt g has an inverse $-g$ s.t. $g + (-g) = O$
4. It must be associative $g_1 + (g_2 + g_3) = (g_1 + g_2) + g_3$

Check: 1. $P + O = P$



2, closure $P, Q \in C$

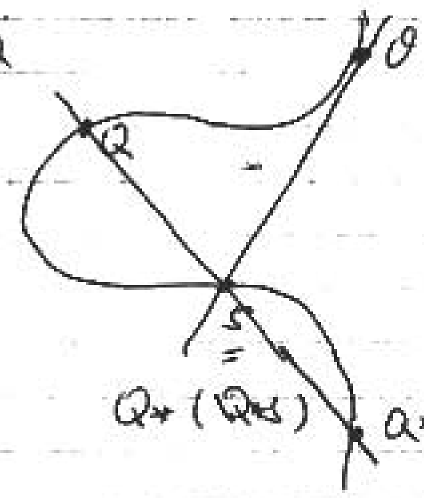
$P * Q \in C$.

$P + Q = O * (P * Q)$

rational

3. inverse Assume non-singular cubic

i.e. given some rational pt. Q we have $-Q$ rational s.t. $Q + (-Q) = O$



Adding

$Q + (Q * S) = O$.

$Q * S = -Q$

Given 3 rational pts P, Q, R
want to show $(P+Q)+R = P+(Q+R)$

See enough to show

$$(P+Q) * R = P * (Q+R)$$

Had drawn complicated diagram

See p. 21 of text

$\mathcal{O}, P, Q, R, P*Q, P+Q, Q*R, Q+R, S$

~~intersection~~

C_1 cubic formed by green lines
C_2 " " orange "

C_1 with zero element $\mathcal{O}$
C' with zero element $\mathcal{O}'$

$$P \longrightarrow P + (\mathcal{O}' + \mathcal{O})$$