-MONDAY 1/23/2017-

USED:: SILVERMAN'S "THE ARITHMETIC OF ELLIPTIC CURVES"
& NOTES FROM FRANK THORNESS CLASS ON ELLIPTIC CURVES.

LAST TIME WE TALKED ABOUT PROJECTIVE SPACE.

DEFN: WE DEFINE A PROJECTIVE PLANE CURVE AS $V(f) \subseteq \mathbb{P}^2$ WHERE f IS A SINGLE HOMOGENEOUS POLYNOMIAL (AND NONZERO...)

I.E. AN $\mathcal{C}$ IS A CURVE WITH COEFFS IN A FIELD k. FOR EACH EXTENSION K OF k..

$$\mathcal{C}(K) = \{ [x:y:z] \in \mathbb{P}^2(K) \mid f(x,y,z) = 0 \}$$

(BUT! be careful to distinguish things like $V(x+y)$ & $V((x+y)^2)$. These still describe the same subset of $\mathbb{P}^2$..)

WE CALL $\mathcal{C}$ GEOMETRICALLY IRREDUCIBLE IF f DOESN'T FACTOR OVER $\bar{k}$.

THE CURVE $\mathcal{C}$ IS SINGULAR AT A POINT $P = [x_0:y_0:z_0]$ IF:

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0$$

AND $\mathcal{C}$ IS SMOOTH IF THERE ARE NO SINGULAR POINTS IN $\mathcal{C}(\bar{k})$.

ALSO... $\deg(\mathcal{C})$ = ITS COMBINED DEGREE AS A POLYNOMIAL

DEFN. LET k BE ALGEBRAICALLY CLOSED, & SUPPOSE THAT f FACTORS IN $K[x,y,z]$ IS: $f = f_1 \cdots f_n$.
WE CALL THE f_i FOR $1 \le i \le n$ THE IRREDUCIBLE COMPONENTS OF f.

WHICH LEADS US TO..

BEZOUT'S THM: IF $V(f_1)$ AND $V(f_2)$ ARE PROJECTIVE PLANE CURVES, WITH NO COMMON COMPONENTS, THEN THEY INTERSECT AT $(\deg f_1)(\deg f_2)$, COUNTED WITH MULTIPLICITY.

EX. WE ALREADY TALKED ABOUT 2 LINES (DISTINCT) IN $\mathbb{P}^2$ WILL INTERSECT IN EXACTLY ONE PLACE.

$$\left.\begin{aligned} f_1 &= Ax + By + Cz \\ f_2 &= ax + by + cz \end{aligned}\right\} \text{2 DISTINCT LINES}$$

WILL INTERSECT @ EXACTLY ONE POINT.

ALSO, IN FRANK'S NOTES HE MENTIONS THAT $\mathbb{P}^5$ IS THE MODULI SPACE OF CONICS... WHICH I HAD NEVER THOUGHT ABOUT BEFORE... (ASIDE)

↳ 5 POINTS DETERMINE A CONIC.

OK.. NOW WE CAN TALK ABOUT BASIC ELLIPTIC CURVES

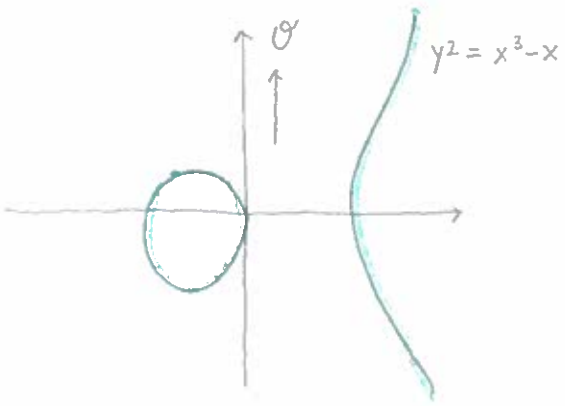
DEFN, A WEIERSTRASS EQN IS:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

OR ITS HOMOGENIZATION:

$$E: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_5Z^3 \ldots$$

AND THE VARIETY $V(E)$, TOGETHER WITH THE POINT $\mathcal{O} = [0:1:0]$ (point at infinity) IS CALLED AN ELLIPTIC CURVE GIVEN THAT V IS SMOOTH.



SOME IMPORTANT INVARIANTS OF ELLIPTIC CURVES..

LET $E: y^2 = x^3 + Ax + B$.

DEF^N THE DISCRIMINANT Δ IS GIVEN BY:

$$\Delta := -16(4A^3 + 27B^2)$$

& THE j-INVARIANT IS GIVEN BY: ——→ THERE IS A LOT OF STUFF GOING ON HERE.. WAS ORIGINALLY STUDIED AS A PARAMETERIZATION OF ELL. CURVES OVER $\mathbb{C}$, BUT HAS CONNECTIONS TO MODULAR FORMS (IT IS ONE), CLASS FIELD THEORY, SYMMETRIES OF THE MONSTER GROUP.. "MONSTROUS MOONSHINE" CONJECTURE BY CONWAY & NORTON.

$$j := -1728\,\frac{(4A)^3}{\Delta}$$

(??)

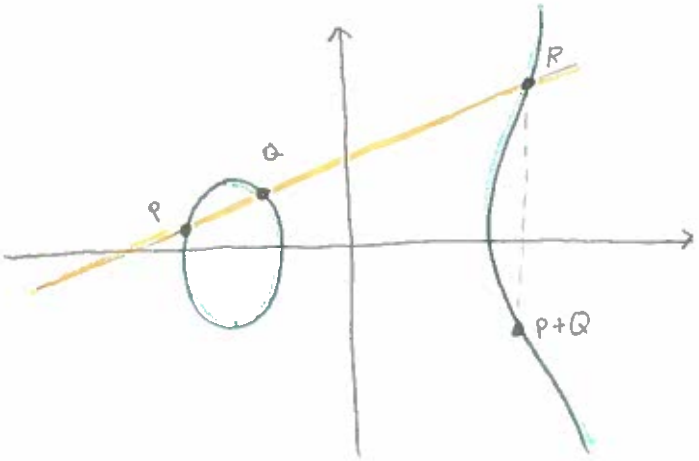
A HANDY PROPOSITION: THE CURVE E IS SINGULAR IF & ONLY IF $\Delta(E) = 0$. IF E IS SINGULAR, WE SAY IT HAS

- A NODE IF $A \neq 0$
- A CUSP IF $A = 0$

NOW... THE GROUP LAW!!

LET P, Q BE 2 POINTS ON E. THEN, DRAW THE LINE GIVEN BY PQ. BEZOUTS THM $\Rightarrow$ THE LINE PQ INTERSECTS E AT A THIRD POINT, SAY R.

THEN, REFLECT R ABOUT THE x AXIS, & CALL THIS POINT $P+Q$.



THEOREM: THIS OPERATION DEFINES AN ABELIAN GROUP LAW ON $E(k)$ FOR ANY FIELD k!!

EX (FROM FRANK'S CLASS NOTES)

LET $E: y^2 = x^3 + 17$.

COMPUTE $(-2,3) + (-1,4)$...

LINE PASSING THROUGH $(-2,3)$ & $(-1,4)$ IS $\boxed{y = x + 5}$

SO...

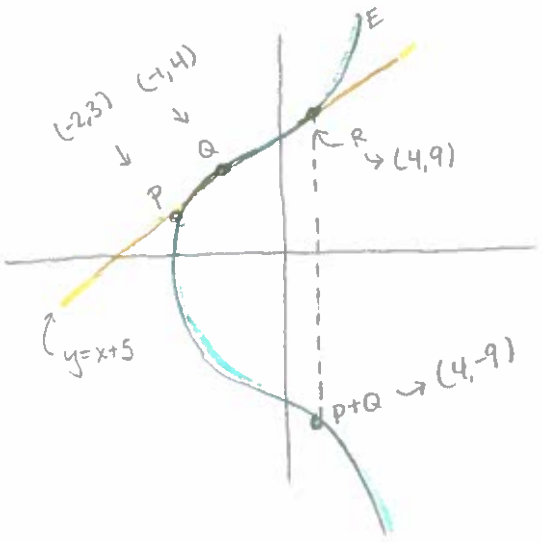
$(x+5)^2 = x^3 + 17$

$\Rightarrow x^3 - x^2 - 10x - 8$

GIVES US $(4,9)$.

FLIPPING ACROSS x-AXIS..

WE GET $(4,-9) = (-2,3) + (-1,4)$



MY PICTURE IS BADLY DRAWN.. BUT YOU SEE WHAT I MEANS