ELLIPTIC CURVES OVER $\mathbb{F}_p$

($\mathbb{F}_p$ ← ANY FIELD)

IGNORING CHARACTERISTIC 2, 3 ANY ELLIPTIC CURVE OVER K CAN BE WRITTEN IN THE FORM $y^2 = x^3 - px - q$ WITH $p, q \in K$ AND ($x^3 - px - q$ ← NO DOUBLE ROOTS)

"FORMALLY": A PAIR $(E, \mathcal{O}_E)$ ($\mathcal{O}_E$ ← DISTINGUISHED $\mathbb{F}_p$-RATIONAL POINT WHICH BECOMES id IN GROUP LAW; E ← CURVE OF GENUS 1 / $\mathbb{F}_p$)

FIRST: ISOGENIES

GIVEN 2 ELLIPTIC CURVES E_1 & E_2 DEFINED OVER SAME RING, WE'D LIKE TO BE ABLE TO MAP ONE CURVE TO ANOTHER.

RECALL: FROM KEVIN'S TALKS, MAPS BETWEEN CURVES ARE RATIONAL MAPS

BUT E_1 & E_2 AREN'T JUST CURVES; THEY ALSO HAVE A GROUP STRUCTURE, SO IDEALLY ANY MAP BETWEEN THEM SHOULD PRESERVE THIS INFORMATION.

PROPOSITION (HARTSHORNE 2.6.8) (→ DIVISORS SECTION)

LET X A COMPLETE NONSINGULAR CURVE OVER A FIELD k AND Y ANY CURVE OVER k, AND $f: X \to Y$ A MORPHISM, THEN EITHER:

(i) $f(X) =$ A POINT

(ii) $f(X) = Y$ ------>

Aside: In this situation, $k(X)$ is a finite field extension of $k(Y)$

TLDR: A MAP BETWEEN 2 E.C DOES ONE OF THE FOLLOWING.

(i) MAPS ALL OF E_1 TO $\mathcal{O}_2$

(ii) MAPS E_1 SURJECTIVELY ONTO E_2

SO, WE'LL CALL AN ISOGENY A HOMOMORPHISM $\phi: E_1 \to E_2$ SO THAT $\phi(\mathcal{O}_1) = \mathcal{O}_2$ AND ϕ IS NONZERO/NONTRIVIAL

EXAMPLE.

LET E BE AN ELLIPTIC CURVE DEFINED OVER $\mathbb{F}_p$

THE FROBENIUS ENDOMORPHISM $\varphi_p : E \to E$ IS GIVEN BY $(x,y) \longmapsto (x^p, y^p)$

THEOREM (TATE) LET E_1, E_2 OVER $\mathbb{F}_p$ WITH

$$\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$$

THEN, THERE IS AN ISOGENY FROM E_1 TO E_2 DEFINED OVER $\mathbb{F}_p$.

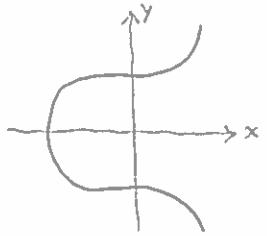
in general, says 2 abelian varieties over $\mathbb{F}_p$ are isogeneous if & only if their Tate modules are isomorphic as Galois reps.

QUESTION. GIVEN AN E.C. $\overset{E}{\vee}$ DEFINED OVER $\mathbb{F}_p$, HOW DO WE KNOW $E(\mathbb{F}_p)$ IS NONEMPTY? (ie. HOW DO WE KNOW E HAS $\mathbb{F}_p$-RATIONAL POINTS?)

Ex. $E: y^2 = x^3 - x + 1$ over $\mathbb{F}_5$ ---------> LOOKING @ $E/\mathbb{F}_p$, WE DON'T GET PRETTY PICTURES, BUT I WANTED TO DRAW ONE ANYWAY

	$Y=0$	
$X=0$	$0=1$	$\times$
$X=1$	$0=1$	$\times$
$X=2$	$0=2$	$\times$
$X=3$	$0=0$	$\checkmark$
$X=4$	$0=1$	$\times$

→ E HAS AN $\mathbb{F}_5$-RATIONAL POINT $(3,0)$



THEOREM (LANG) ANY CUBIC CURVE E DEFINED OVER $\mathbb{F}_q$ (WITH $q = p^n$, $n > 0$) HAS AN $\mathbb{F}_q$-RATIONAL POINT

} EXISTANCE OF $\mathbb{F}_q$-RATIONAL POINT(S)

↳ GENERAL THM IS FOR ABELIAN VARIETIES

IN GENERAL, COUNTING POINTS ON AN E.C / $\mathbb{F}_p$ CAN BE DIFFICULT.

MY NOTES ARE OUT OF ORDER

THM (HASSE-WEIL)

IF C IS A NONSINGULAR IRREDUCIBLE CURVE OF GENUS g DEFINED OVER $\mathbb{F}_p$, THE # OF POINTS ON C WITH COORDS IN $\mathbb{F}_p$ IS

$$p+1-\varepsilon$$

ERROR TERM SATISFIES $|\varepsilon| \leq 2g\sqrt{p}$

THIS IS ALSO CALLED THE RIEMANN HYP FOR CURVES OVER FINITE FIELDS

CLEARLY $\#E(\mathbb{F}_p)$ IS FINITE.. BUT THM ABOVE GIVES US AN IDEA OF HOW BIG IT SHOULD BE

EX HOW MANY POINTS ARE ON A LINE $y = ax+b$ OVER $\mathbb{F}_p$?

TAKING ANY VALUE FOR x, THE VALUE OF y IS DETERMINED.

$\Rightarrow$ p POINTS

BUT WE'D LIKE PROJECTIVE POINTS. SO THROW IN ANOTHER FOR PT @ ∞ (HOMOGENEOUS $Y = aX+b$ is $Y = aX + bZ$

SO EXTRA PT @ $[1,a,0]$)

$\Rightarrow$ A LINE HAS P+1 POINTS

EX. $C: y^2 = f(x)$ $\longrightarrow$ HOW MANY POINTS SHOULD C HAVE / $\mathbb{F}_p$?

NOTE: HALF OF GUYS IN $\mathbb{F}_p$ ARE QUAD. RESIDUES, HALF ARE NONRESIDUES

PLUGGING IN A VALUE FOR x YIELDS..

EITHER... $f(x)=0 \rightsquigarrow$ ONE SOLUTION, $y=0$

OR
- → 50% CHANCE OF 2 SOLUTIONS (QUADRES)
- → 50% CHANCE OF NO SOLUTIONS (NON RES)

} p POSSIBLE VALUES FOR x & POINT AT ∞ AGAIN GIVES $p+1$

$\#C(\mathbb{F}_p) = p+1 + \text{error term}$