Math 312, lecture 22, 20/6/2018

Elliptic curves

Note: This is not examinable

Another source of arithmetic systems ⇒ can be use for crypto
(eg. for DH key exchange)

Let $P(x,y)$ be a cubic polynomial in two variables
(we'll use $P(x,y) = y^2 - (x^3+ax+b)$)

allowed monomials like x^3, y^3, xy, x^2y, but not x^3y^3 or x^3y)

(Example: Fermat cubic $x^3+y^3=1$)

(integer solutions to $X^3+Y^3=Z^3$ ↔ rational solutions to $x^3+y^3=1$
(divide by Z^3)

(we'll work with rational solutions, equivalent to integer solutions of homogeneous eqn: replace

$$y^2 = x^3+ax+b \quad \text{with}$$

$$y^2z = x^3+axz^2+bz^3$$

Let $\in$ be the set of solutions to $P(x,y)=0$

Let L be a line. Then $L \cap \in$ consists of 3 points:

Say $\in$: $y^2 = x^3 + ax + b$

L: $y = Ax + B$

then $(x,y) \in L \cap \in$ if $(Ax+B)^2 = x^3 + ax + b$

this is a cubic equation, has 3 solutions

* counting with mult, always 3 solutions
* but these need not live over "ground field".

Work with circle $x^2+y^2=r$, $r \in \mathbb{Q}$.

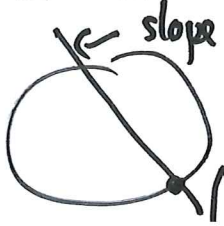
Suppose $(\xi, \eta) \in \mathbb{Q}$ s.t. $\xi^2+\eta^2=r$.

Every other pt is the intersection of a line

$$y = m(x-\xi)+\eta$$ and the circle

Plug this into $x^2+y^2=r$ to find intersection, get eqn for x with coeff depend on r, m, ξ, η, m

this is a quadratic $Ax^2+Bx+C=0$ with $A,B,C \in \mathbb{Q}$ (if m is) has the root ξ



$\Rightarrow$ other root is: $-\frac{B}{A} - \xi$ (roots of quadratic add up to $-\frac{B}{A}$)
$\in \mathbb{Q}$

Back to our elliptic curve $E: y^2 = x^3 + ax + b$: $a, b \in \mathbb{Q}$.

Let $P, Q \in E(\mathbb{Q})$, i.e. P, Q pts in the plane, on the curve, have rational co-ordinates

Let L be the line through P, Q. (if $P = Q$, L is the line tangent to E at P)

the intersection $L \cap E$ determines a cubic poly with rational coeff (say $X^3 + AX^2 + BX + C = 0$) then sum of roots is $-A$

(mult. $(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_r) = X^r - (\alpha_1 + \cdots + \alpha_r)X^{r-1} + \cdots$)

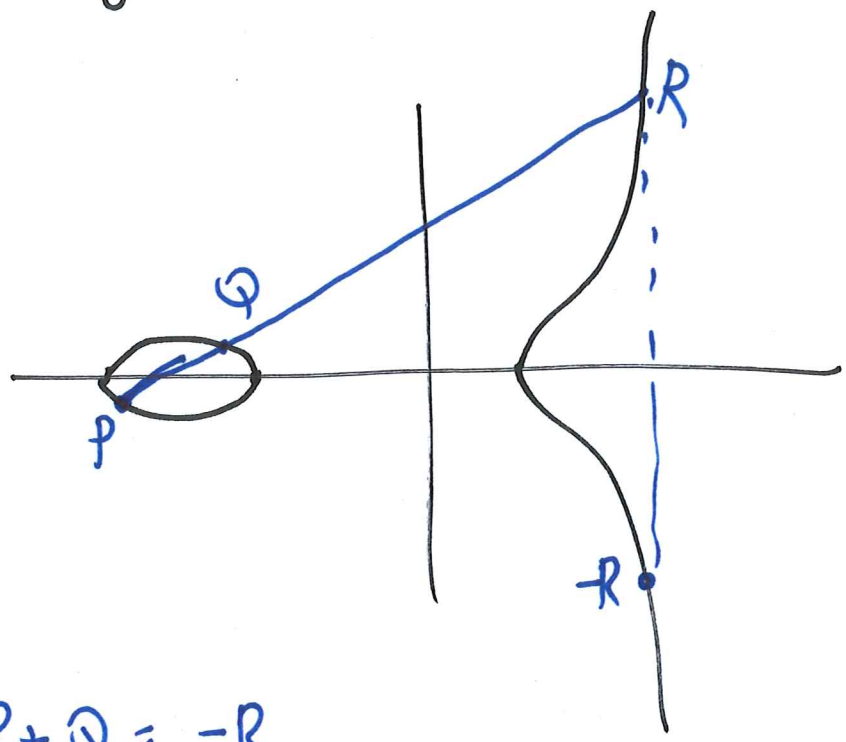
Two roots are rational $\Rightarrow$ third is rational too.

Amazing fact: suppose that $X^3 + ax + b = 0$ has 3 distinct roots

then if $P = (x, y) \in E$ set $-P = (x, -y)$

And if P, Q, R lie on a straight line declare $P + Q + R = 0$

Example: Say x^3+ax+b has 3 real roots



set $P+Q = -R$

Facts: This operation respects laws of $+$:

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

(and, co-ords of $P+Q$ are "easily" computable from those of P, Q)

Line through $R, -R$ meets curve at pt at ∞ (vertical infinity)

For crypto: use Elliptic curve mod p.

Consider eqn $E: y^2 \equiv x^3 + ax + b \pmod{p}$

set of solutions mod p : $E(\mathbb{F}_p)$ & with addition

Can be used for crypto.

Ex: (EC DH): Alice & Bob agree on p, E, pt P.

Alice chooses k, Bob chooses ℓ

Alice sends $kP = \underbrace{P + \cdots + P}_{k \text{ times}}$

Bob sends $\ell P = \underbrace{P + \cdots + P}_{\ell \text{ times}}$

$\Rightarrow$ Alice computes $k\ell P = k \cdot (\ell P)$

Bob computes $k\ell P = \ell \cdot (kP)$

Ideally, $\#E(\mathbb{F}_p) = p$ then every point ($\neq \infty$) has order p

Try to count pts: For every $x \bmod p$, have a pt (x, y)

if $x^3 + ax + b$ is a quadratic residue

$$\text{So } \#E(\mathbb{F}_p) = 1 + \sum_{x \bmod p} \left(1 + \left(\frac{x^3+ax+b}{p}\right)\right) = p + 1 + \sum_{x (p)} \left(\frac{x^3+ax+b}{p}\right)$$

Thm (Hasse): $\#E(\mathbb{F}_p) = 1 + p - a_p$, $|a_p| \leq 2\sqrt{p}$