MATH 314 - Class Notes

12/6/2016

Scribe: Aman Patel

Summary: Today we went over the Elliptic Curve and its relation to Cryptography

Notes:

- elliptic curves are not ellipses
- An elliptic curve is an equation in the form $y^2 = x^3 + ax + c$ where $4a^3 + 27c^2 \neq 0$
- If you take 2 points on an elliptic curve and draw a line between them, then this line intersects the curve at a third point
- If the coordinates of the first two points are rational, than the points of the third point will be rational as well
- We can use these to write down a way to "add" points and do "arithmetic" on them
- If there are two points P and Q where $P = (X1, Y1), Q = (X2, Y2)$, How do we find P + Q? Since $R = (X3, Y3)$ is on the curve $Y3^2 = X3^3 + AX3 + B$
- Find slope m of the line connecting P,Q. $m = (Y2-Y1)/(X2-X1)$ intercept $C = Y1-MX1$
- R satisfies both $y^2 = x^3 + ax + b$ and $y = mx + c$
- Substitute $(mx + c)^2 = x^3 + ax + b$
- $0 = x^3 - m^2x^2 + x + c$ after foiling
- $= (x - x1)(x - x2)(x - x3)$ where x1, x2, and x3 are all roots
- $m^2 = x1 + x2 + x3$
- $y3 = mx3 + c$
- $P + Q = (X3 - Y3)$ ¡- Rule for points on an elliptic curve
- Ex) E: $y^2 = x^3 + x + 6$
- $P = (2, 4)Q = (3, -6)$
- Check these points are on E:
- $P : 4^2 = 16 = 8 + 2 + 6$
- $Q : (-6)^2 = 36 = 27 + 3 + 6$
- Find P + Q:
- $m = (-6 - 4)/(3 - 2) = -10$

- $c = -6 - (-10)3 = 24$
- $x3 = m^2 - x1 - x2$
- $= (-10)^2 - 2 - 3 = 95$
- $y3 = mx3 + c$
- $(-10)(95) + 24 = -926$
- $P + Q = (95, 926)$
- Note: To add a point to itself we use the tangent line to the curve of the point. Use calculus to find slope
- $m = (3x1 + a)/2y1$
- If we add two points and get a vertical line then the line goes through the "point at infinity"
- Infinity is the identity
- Points on an elliptic curve form a group (Abelian group)

Discrete Log for Elliptic Curve:

1. Idea - If P is a point on an elliptic curve and k is an integer given P, K we can find KP easily (P+P+P+P+P)(K times)
2. Trick - Repeated Squaring. On the other hand given P, KP. It is hard to find K

Important Theorms:

1. Mordell Weil Theorm - If E is any elliptic curve, we can write a finite list of points P1,P2...Pk so that every rational point on the curve can be written as a sum of two points
2. Hasse's Theorm - If E is an elliptic curve (mod p) and n is the number of points on E then: $\mid N - (P + 1) \mid \leq 2\sqrt{p}$