Math 314 - Spring 2024 **Name:** Addison Ralston
Class Notes Homework Due May 14, 2024

Signatures Continued..

DSA (Digital Signature Algorithm)
"Fancy version of El Gamal"
Need medium prime, large prime

- Setup

large prime (p): size 200 digits
Medium prime (q): q needs to divide into (p-1), size 80 digits
Need Primitive root (g) (mod p)
Need $\alpha = g^{p-1/q}$

Alice picks a secret key "a", $2 < a < q$
Compute: $\beta \equiv \alpha^a (\mod p)$
$Alice'spublickey : (\alpha, \beta, p, q)$

Alice wants to send a message $m \mod q$ along with her signature.
Alice picks ephemeral key, e
$r \equiv (\alpha^e (\mod p) \mod q)$
$s \equiv (e^{-1} * (m + a * r) \mod q)$

Signature: (r,s)

- Verification step

Bob computes:

- $u_1 \equiv s^{-1} * m \mod q$
- $u_2 \equiv s^{-1} * r \mod q$

Check if:
$r \equiv \alpha^{u_1} * \beta^{u_2} \mod p \mod q$

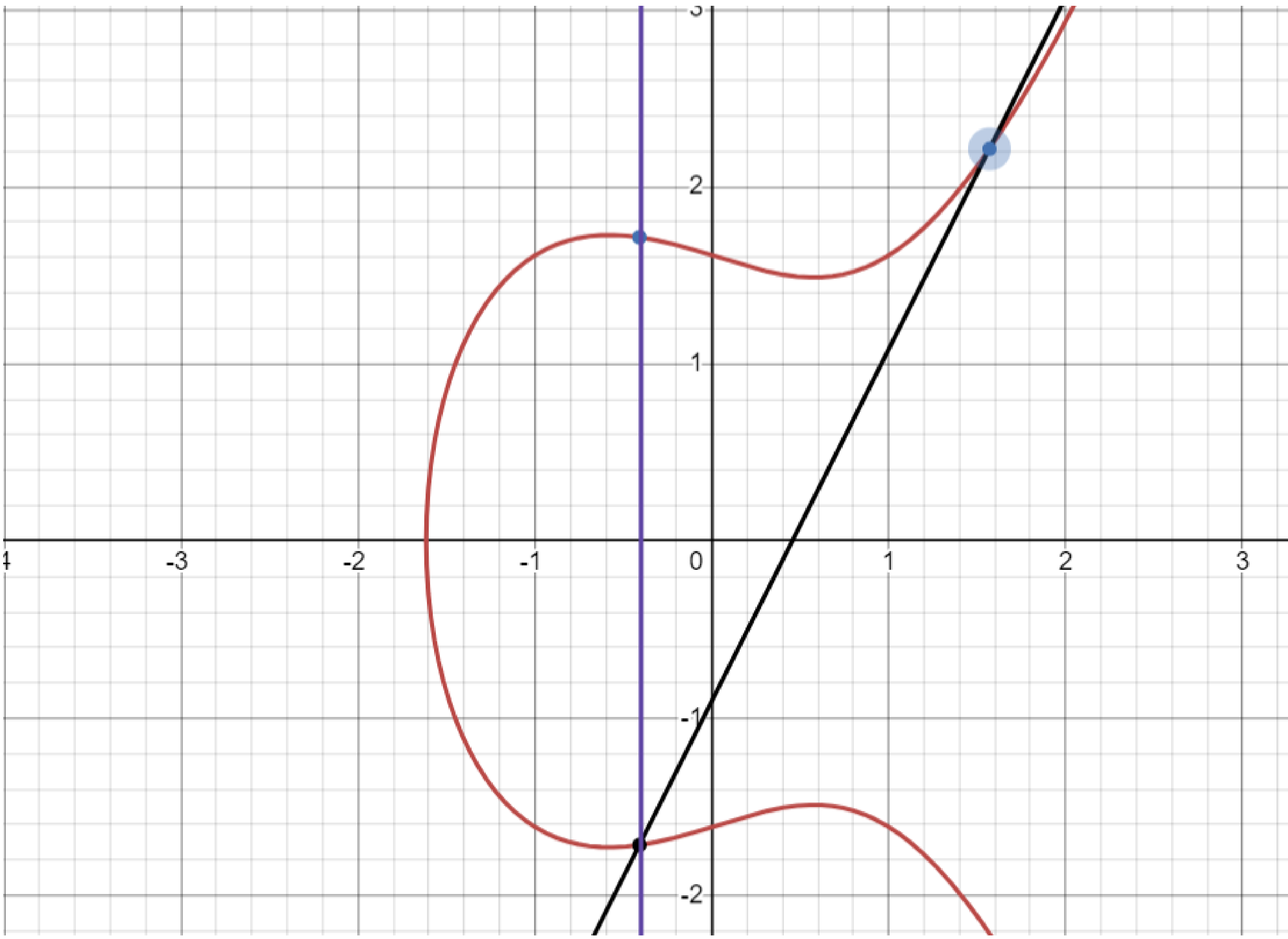
Elliptic Curves

```
An equation of the form:
 y^2 = x^3 + ax + b, "a" and "b" are numbers where 4a^3 + 27b^2 DO NOT equal 0.

 Any computed points (x, y) need to satisfy the equation above.

 Defining "Addition" of points on an elliptic curve.
  - Define: P + Q = R, R = reflection of point across x-axis.
```

Two Important edge cases:
- (1) If P and Q have the same x-coord, R is defined at "infinity" or "cursive O"
  If P is a normal point and O is at infinity, then P + O = P
  O is the identity point.
- (2) If the line is tangent to the point P.



How To Apply elliptic curves to cryptography:
- Use numerical coordinates

If P = (x, y),
then Q = (x2, y2)

To find the coordinates of (x3, y3) of P + Q:
These formulas are needed:
(1) Find the slope:

```
m = (y2 - y1) / (x2 - x1), if P DOES NOT equal Q.
or
m = (3x^2 + a)(2y)^-1, if P = Q ("a" is defined by the equation of the elliptic curve)

(2) Find the points:
x3 = m^2 - x1 - x2
y3 = m(x1 - x3) - y3
```