Elliptic Curve Cryptography

Elliptic Curves over Real Numbers

- An elliptic curve is defined by an equation in two variables x & y, with coefficients
- For cryptography, the variables and coefficients are restricted to elements in a Finite field.

Consider an elliptic curve

- where x, y, a, b, the variables and coefficients are all real numbers
- In general, the cubic equations for elliptic curves takes the form

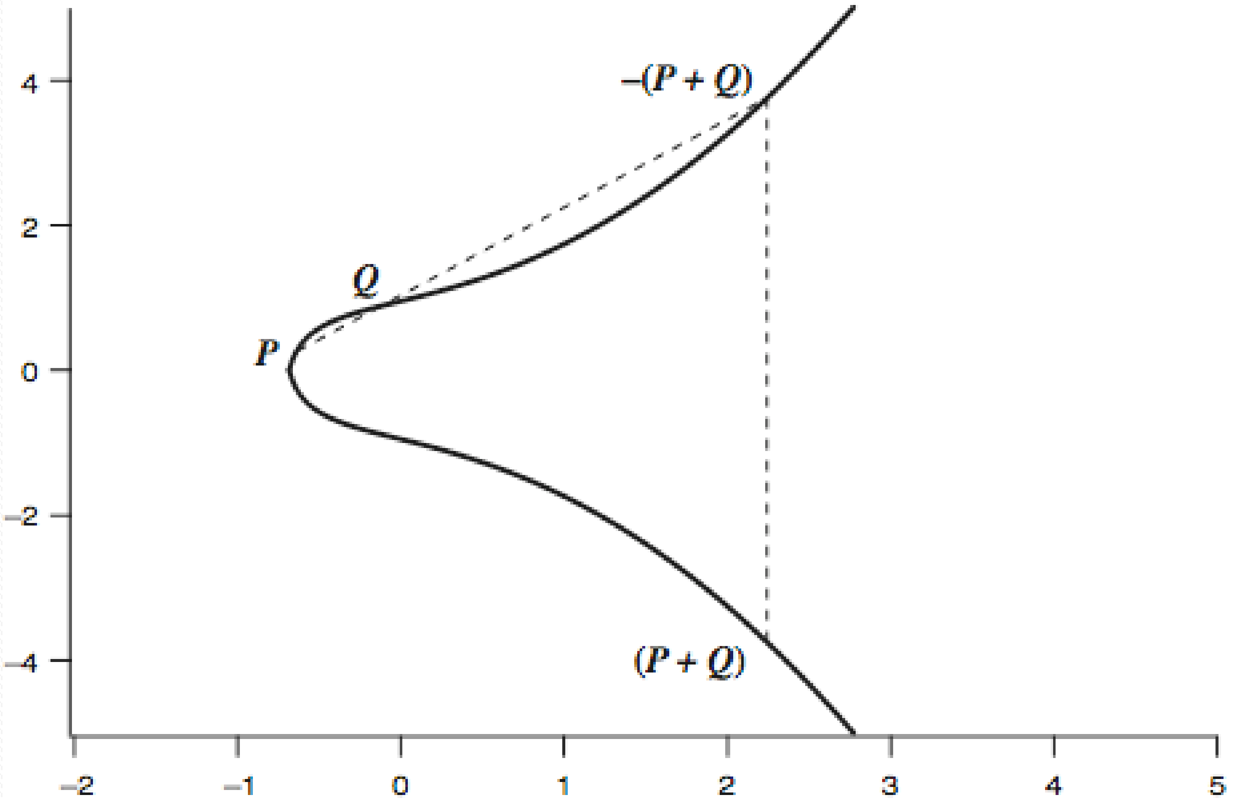
$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

Elliptic Curves over Real Numbers

- Consider a cubic elliptic curve of form
  - $y^2 = x^3 + ax + b$
  - where x, y, a, b are all real numbers
  - also define zero point O or point at infinity
- consider set of points E(a,b) that satisfy the equation $y = \sqrt{(x^3 + ax + b)}$
  - Given a and b, the plot consists of positive and negative values of y for each value of x.
  - Each curve is symmetric about y = 0

Real Elliptic Curve Example

geometrically sum of P+Q is reflection of the intersection R [= - (P+Q)]



(b) $y^2 = x^3 + x + 1$

Elliptic Curve Addition

- Example: Consider an elliptic curve E of form

  E: $y^2 = x^3 - 15x + 18$

  The points P=(7,16) and Q = (1,2) are on the curve E.

  The line L connecting them is L: $y = 7/3\ x - 1/3$

  Solve for x to find the points where E and L intersect

  $(7/3\ x - 1/3)^2 = x^3 - 15x + 18$

  $0 = x^3 - 49/9\ x^2 - 121/9\ x + 161/9$

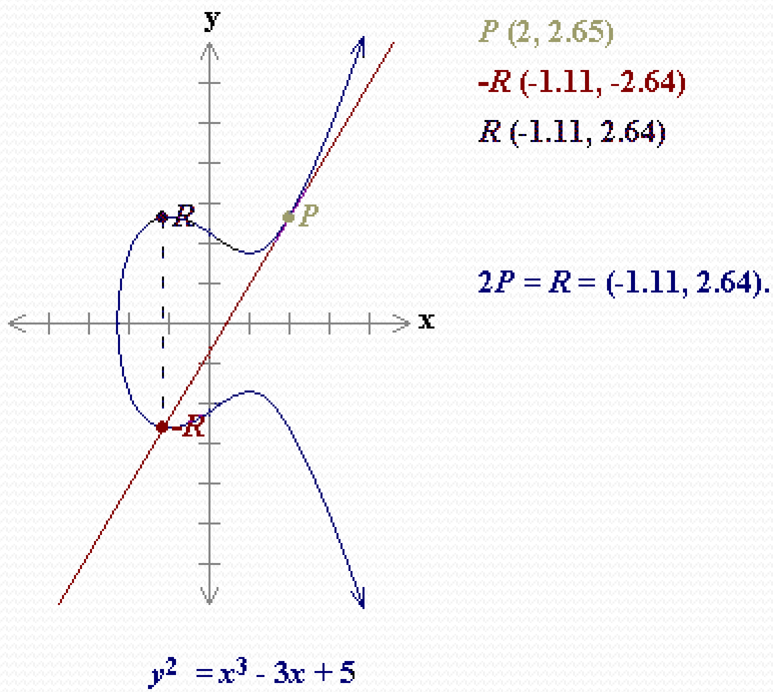
  $x^3 - 49/9\ x^2 - 121/9\ x + 161/9 = (x-7)(x-1)(x+23/9)$

  The 3rd intersection point of E and L is (-23/9, 170/27)

  So, $P + Q = (-23/9, -170/27)$

Elliptic Curve Doubling

P+P = 2P



Elliptic Curves Doubling

- Example: Consider an elliptic curve E of form

  $E: y^2 = x^3 - 15x + 18$

  The point P=(7,16) is on the curve E. $P + P = 2P$

  The line L becomes the tangent line to E at P

  The slope of E at P

  $2y\, dy/dx = 3x^2 - 15$ so, $dy/dx = (3x^2 - 15) / 2y$

  Substituting the co-ordinates of P = (7, 16)

  The slope $\lambda = 33/8$

  So, the tangent line to E at P is

  $L: y = 33/8\, x - 103/8$

Elliptic CurveDoubling

- Example Contd.

Substitute the equation of L into the equ. of E

$(33/8\,x - 103/8\,)^2 = x^3 - 15x + 18$

$x^3 - 1089/64\,x^2 + 2919/32\,x + 9457/64 = 0$

$(x - 7)^2\,(x - 193/64) = 0$

Substituting x = 193/64, we get y = 223/512 and then switch the sign on y

$P + P = 2\,P = (193/64\,,\,223/512)$

Elliptic Curve Addition

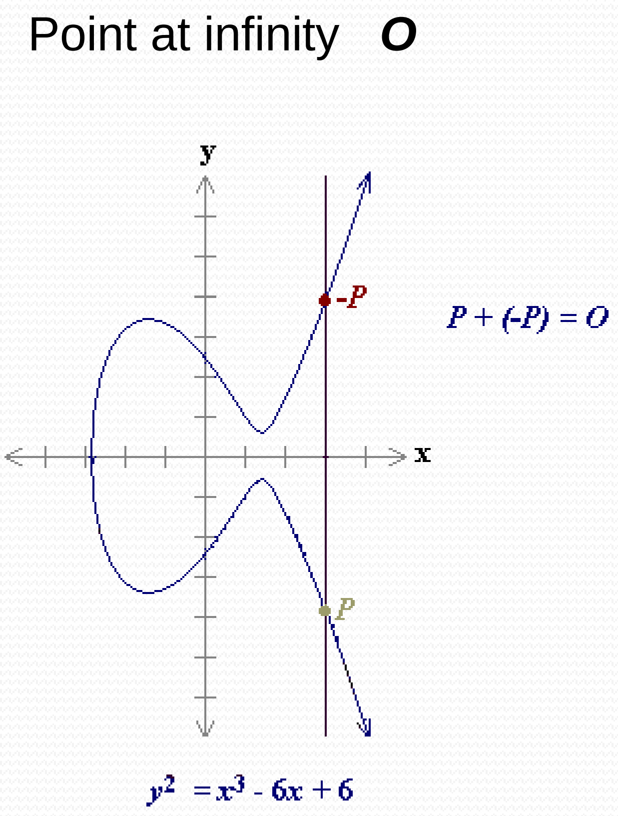
Let P = (a, b) and its reflection P’= (a, -b)

Add P and P

P + P’= o

Point at infinity

P + o = P



Elliptic Curves doubling

- Consider a cubic elliptic curve of form
  - $y^2 = x^3 + ax + b$
  - where x, y, a, b are all real numbers
  - also define zero point O or point at infinity
- consider set of points E(a,b) that satisfy

the equation $y = \sqrt{(x^3 + ax + b)}$

- Given a and b, the plot consists of positive and negative values of y for each value of x.
- Each curve is symmetric about y = 0

Geometric Description of Addition

- A group can be defined based on the set E(a,b) provided that $x^3 + ax + b$ *has no repeated factors*

- Equivalent to the condition

  $$4\,a^3 + 27\,b^2 \neq 0$$

- In geometric terms the rules for addition is

  " if three points on an elliptic curve lie on a straight line, their sum is o "

Geometric Description of Addition

- What is this extra condition $4a^3 + 27b^2 \neq 0$?

($4a^3 + 27b^2$) is called the discriminant of E

Discriminant $\neq 0$ is equivalent to the condition that the cubic polynomial have no repeated roots.

$x^3 + ax + b = (x - e1)(x-e2)(x-e3)$ where e1, e2, e3 are allowed to be complex numbers then

$4a^3 + 27b^2 \neq 0$ if and only if ***e1, e2, e3 are distinct***

Curves with discriminant = 0 have singular points. The addition law does not work well on these curves.

So, the requirement $4a^3 + 27b^2 \neq 0$ is included.

Elliptic curve Addition Algorithm

Theorem:

Let *E: $y^2 = x^3 + ax + b$ is an elliptic curve and*

Let P and Q be two points on E

(a) **If** P = 0 then P + Q = Q

(b) Otherwise if Q = 0, then P + Q = P

(c) Otherwise, write $P = (x_1, y_1)$ and $q = (x_2, y_2)$

(d) If $x_1 = x_2$ and $y_1 = -y_2$, then P + Q = 0

(e) P = P, assume $P \neq 0$ and $Q \neq 0$

(f) **Otherwise define** λ

Contd. To next slide

Elliptic curve Addition Algorithm

Contd.

$\Lambda = (y2 - y1) / (x2 - x1)$ if $P \neq Q$

$\Lambda = (3x1^2 + a) / (2\ y1)$ if $P = Q$

$X3 = \lambda^2 - x1 - x2$

$Y3 = (\lambda\ (x1 - x3) - y1)$

Then $P + Q = (x3, y3)$

Elliptic curve Addition Algorithm

Proof:

Parts (a) and (b) are clear.

(d) Is the case that the line through P and Q is vertical, so P + Q = 0.

For (e), if P ≠ Q then *λ is the slope of the line through P and Q and if P = Q then λ is the slope of the tangent line at P .*

In either case, L: y = *λ x + c with c = y1 – λ x1*

Elliptic curve Addition Algorithm

Proof (contd.)

Substituting L on E

$(\lambda x + c)^2 = x^3 + ax + b$

$x^3 - \lambda^2 x^2 + (a - 2 \lambda c) x + (b - c^2) = 0$

We know that this cubic equation has two root x1 and x2. If we cal thethird root as x3, then it factors as

$x^3 - \lambda^2 x^2 + (a - 2 \lambda c) x + (b - c^2) = (x - x1)(x - x2)(x - x3)$

Multiply and look at the coefficient of x^2 on each side.

Elliptic curve Addition Algorithm

Proof (contd.)

The coefficient of x^2 on the right hand side is

$-x1 - x2 - x3$

Which must equal to $-\lambda^2$, the coefficient of x^2 on the left hand side.

This solves $x3 = \lambda^2 - x1 - x2$ and then y-coordinate of third intersection point of L and E

$$Y3 = \lambda\, x3 + c = \lambda\, x3 + c = \lambda\, x3 + y1 - \lambda\, x1$$

$$= -(\lambda\,(x1 - x3) - y1)$$

So the y-coordinate of $(P + Q)$ is $(\lambda\,(x1 - x3) - y1)$

□