CIS 3362 11/14/26

Elliptic Curves

general type

$$y^2 = x^3 + c_1x^2 + c_2x + c_3$$

$$\hookrightarrow\ y^2 = x^3 + ax + b$$

essentially rework as cubic in $(x + \frac{c_1}{3})$

Consider

$$\left(x + \frac{c_1}{3}\right)^3 + \left(-\frac{1}{3}c_1 + c_2\right)\left(x + \frac{c_1}{3}\right) + \left[c_3 - \frac{c_1^3}{27} + \frac{c_1^2}{9} - \frac{c_1c_2}{3}\right]$$

$$= x^3 + c_1x^2 + \frac{1}{3}c_1x + \frac{1}{27}c_1^3 + c_3$$

$$-\frac{1}{3}c_1x - \frac{1}{9}c_1^2$$

$$+c_2x + \frac{1}{3}c_1c_2$$

$$-\frac{1}{27}c_1^3$$

$$+\frac{1}{9}c_1^2$$

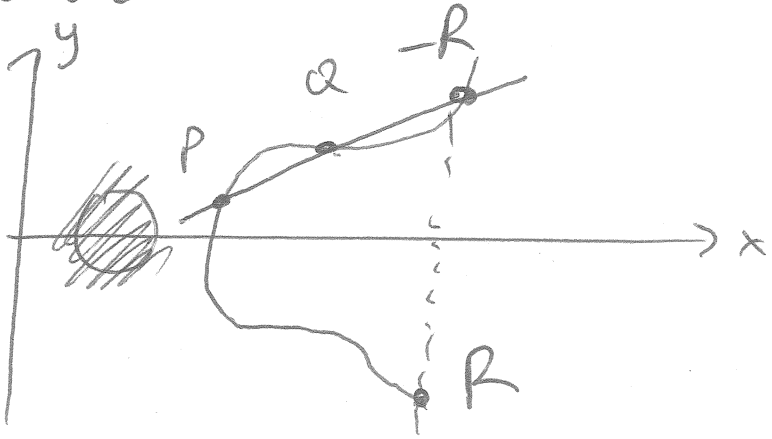
$$-\frac{1}{3}c_1c_2$$

Form we're going to work w/ for crypto

$$y^2 \equiv (x^3 + ax + b) \mod p \quad , p \in \text{Prime}$$

Some ordered pairs (x,y) satisfy this equation, Some do not. Ultimately the equation specifies a set of points.

a real valued curve might look like



$P = (x_P, y_P)$
$Q = (x_Q, y_Q)$

$R = P + Q$

Draw a line through P, Q. Find the 3rd intersection with the curve this point is $-R$

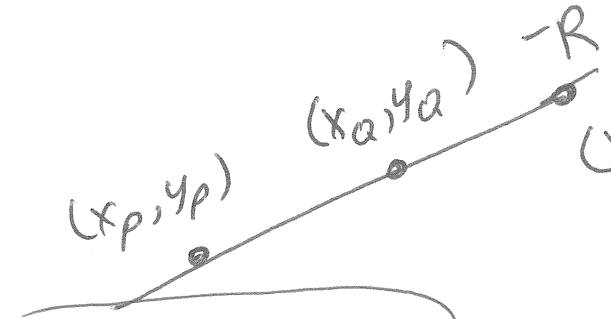
To get R, negate $-R$'s y coordinate

if point P is (x_P, y_P)
then $-P$ is $(x_P, -y_P)$

Note given a prime mod value p

$$-y_P = p - y_P$$

Goal: Given P, Q find x_R, the x coordinate of P+Q.



$$y^2 = x^3 + ax + b$$

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

$$\frac{y - y_P}{x - x_P} = \lambda \rightarrow y - y_P = \lambda(x - x_P)$$

$$y = \lambda(x - x_P) + y_P$$

$$y = \lambda x + (y_P - \lambda x_P)$$

$$(\lambda x + (y_P - \lambda x_P))^2 = x^3 + ax + b$$

$$\lambda^2 x^2 + 2\lambda x(y_P - \lambda x_P) + (y_P - \lambda x_P)^2 = x^3 + ax + b$$

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

$$= (x - x_P)(x - x_Q)(x - x_R)$$

$$x_P + x_Q + x_R = -(-\lambda^2)$$

{ Sum of roots equals opposite of 2nd coeff divided by 1st }

$$x_P + x_Q + x_R = \lambda^2$$

$$x_R = \lambda^2 - x_P - x_Q$$

Use point SLOPE form

$$-y_R = \lambda(x_R - x_P) + y_P$$

$$y_R = -\lambda(x_R - x_P) - y_P$$

$$\boxed{y_R = \lambda(x_P - x_R) - y_P}$$

Curve $y^2 \equiv x^3 + ax + b \pmod{p}$

This is referred to as $E_p(a,b)$.

Thus the equation $y^2 \equiv x^3 + x + 1 \pmod{23}$ is described as $E_{23}(1,1)$.

$y^2 \equiv x^3 + 2x + 3 \pmod{29}$ is $E_{29}(2,3)$.

$P(3,10)$ $Q(9,7)$ on $E_{23}(1,1)$.

$$\lambda = \frac{7-10}{9-3} \equiv \frac{-3}{6} \equiv \frac{-1}{2} \pmod{23}$$

$$\equiv (-1)(2^{-1}) \pmod{23}$$

$$\equiv (-1)(12) \equiv -12 \equiv 11 \pmod{23}$$

$$\boxed{\begin{aligned} x_R &= \lambda^2 - x_P - x_Q \\ y_R &= \lambda(x_P - x_R) - y_P \\ \lambda &= \frac{y_Q - y_P}{x_Q - x_P} \end{aligned}}$$

$$x_R = \lambda^2 - x_P - x_Q = 11^2 - 3 - 9 = 121 - 12 = 109 \equiv 17 \pmod{23}$$

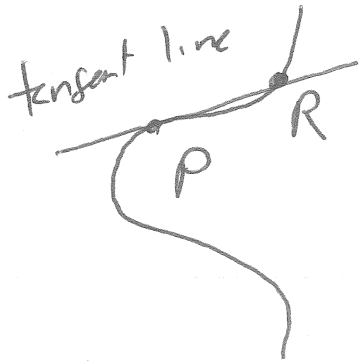
$$y_R = \lambda(x_P - x_R) - y_P = 11(3-17) - 10$$

$$\equiv 11(-14) - 10$$

$$\equiv 11 \times 9 - 10 \equiv 89 \equiv 20 \pmod{23}$$

$$P + Q = (17, 20)$$

What about $P+P$?



Slope of tangent line?

$$y^2 = x^3 + ax + b$$

$$2yy' = 3x^2 + a$$

$$y' = \frac{3x^2+a}{2y}$$

$$\lambda = \frac{3x_P^2 + a}{2y_P}$$

$P(3,10)$ $\quad 2P?$ $\quad E_{23}(1,1)$

$$\lambda = \frac{3(3)^2+1}{2(10)} \equiv \frac{28}{20} \equiv \frac{7}{5} \equiv 7(5^{-1}) \pmod{23}$$
$$\equiv 7\times 14 \equiv 98 \equiv 6 \pmod{23}$$

$23 = 4\times 5 + 3$
$5 = 1\times 3 + 2$
$3 = 1\times 2 + 1$

$3 - 1\times 2 = 1$
$3 - (5-3) = 1$
$2\times 3 - 5 = 1$

$2(23-4\times 5) - 5 = 1$
$2\times 23 - 9\times 5 = 1$

$5^{-1} \equiv -9 \pmod{23}$
$\equiv 14$

$$x_R = (\lambda^2 - x_P - x_Q) \bmod 23$$
$$\equiv (6^2 - 3 - 3) \equiv 30 \equiv 7 \bmod 23$$

$$y_R = \lambda(x_P - x_R) - y_{2P}$$
$$= 6(3-7) - 10 \equiv 6(-4) - 10 \equiv -34 \equiv 12 \bmod 23$$

$P+P = (7,12)$ (ORIGIN)

If you set $x=0 \Rightarrow$ ADDITIVE IDENTITY PT.

Let's investigate what happens when we take a point P on an elliptic curve and compute $P, 2P, 3P, 4P, \ldots$