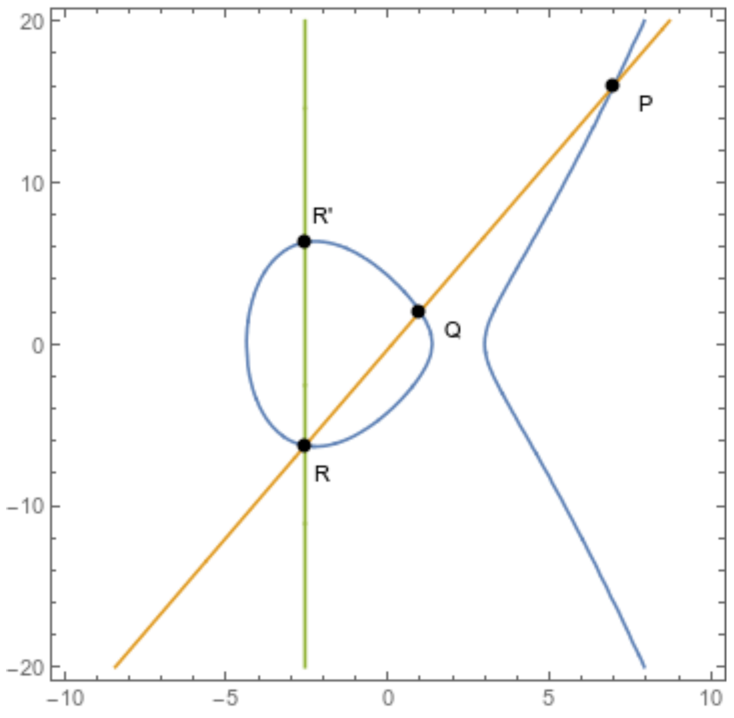
Elliptic Curve Cryptography



$P \oplus Q = R'$

ell curves / $\mathbb{F}_p$

$$y^2 = x^3 + 3x + 8 \quad / \mathbb{F}_{13}$$

$$\Delta = 4a^3 + 27b^2 = 4\cdot 27 + 27\cdot 64 = 1836 \equiv 3 \not\equiv 0 \mod 13$$

$1^2 = 1$	$2^2 = 4$	$3^2 = 9$	$4^2 = 3$	$5^2 = 12$	$6^2 = 10$
$12^2 = 1$	$11^2 = 4$	$10^2 = 9$	$9^2 = 3$	$8^2 = 12$	$7^2 = 10$

repeats b/c $(-a)^2 = a^2$

$x = 0$: $y^2 = 8$ X

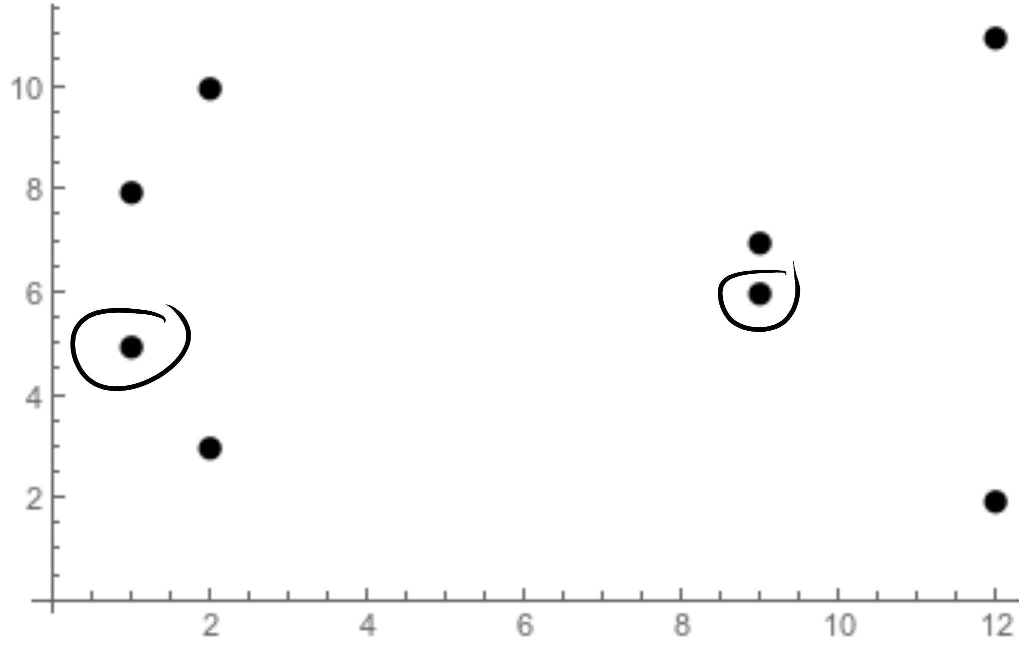
$x = 1$: $y^2 = 12$
$(1,5), (1,8)$

$x = 2$ $y^2 = 9$
$(2,3), (2,10)$

$x = 3$ $y^2 = 5$ X

$\{(1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11), \mathcal{O}\} = E(\mathbb{F}_{13})$

$E(\mathbb{F}_{13})$ has 9 pts



$$y^2 = x^3 + 3x + 8$$

$$(1,5) \oplus (9,6)$$

$$y = \frac{6-5}{9-1}(x-1) + 5$$

$$= \frac{1}{8}(x-1) + 5$$

$$= 5(x-1) + 5$$

$$y = 5x$$

$$25x^2 = x^3 + 3x + 8$$

$$0 = x^3 + x^2 + 3x + 8$$

$$= (x-1)(x-9)(x-x_3)$$

$$= x^3 + (-1-9-x_3)x^2 + (\ )x + (\ )$$

$$\Rightarrow \quad 1 = -1-9-x_3$$

$$x_3 = -1-9-1$$

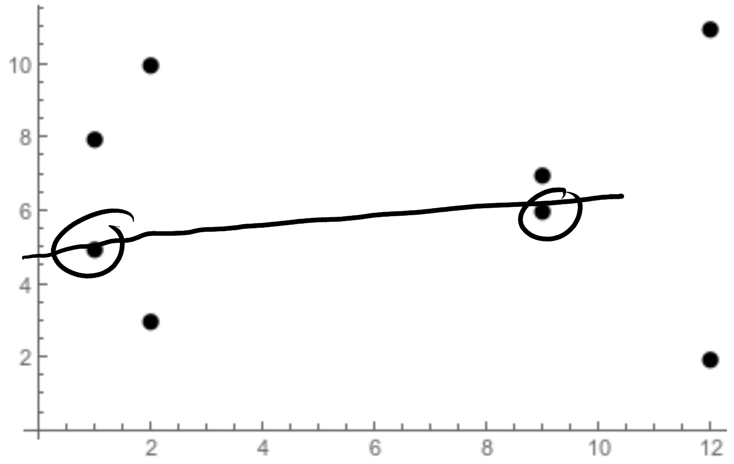
$$= -11 = 2$$

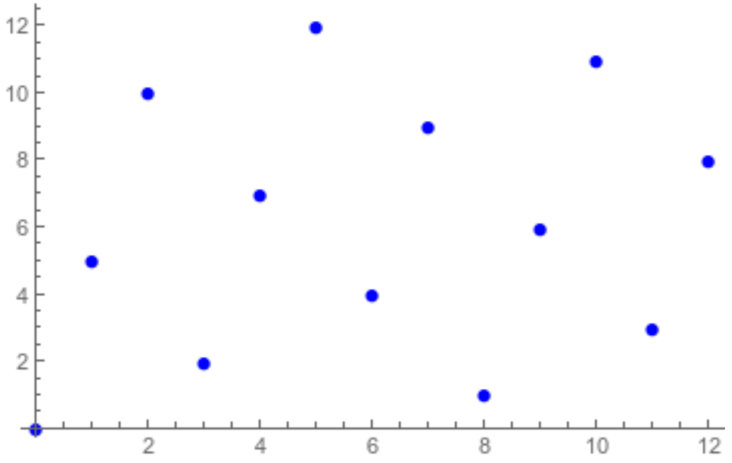
$$x_3 = 2$$

$$y = 5 \cdot 2 = 10$$

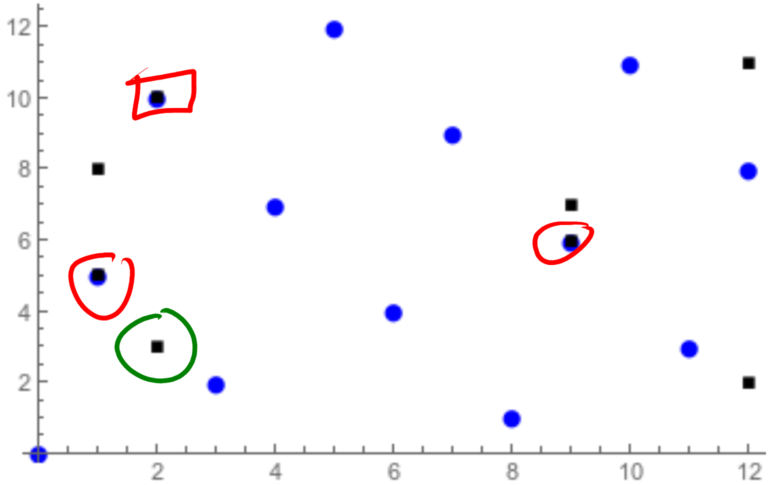
So $(1,5) \oplus (9,6) = (2,-10)$

$$= (2,3).$$





$y = 5x$



$y^2 = x^3 + 3x + 8$

$(12, 2) \oplus (12, 2)$

Tangent line @ $(12, 2)$

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

$4y' = 3 + 3 = 6$

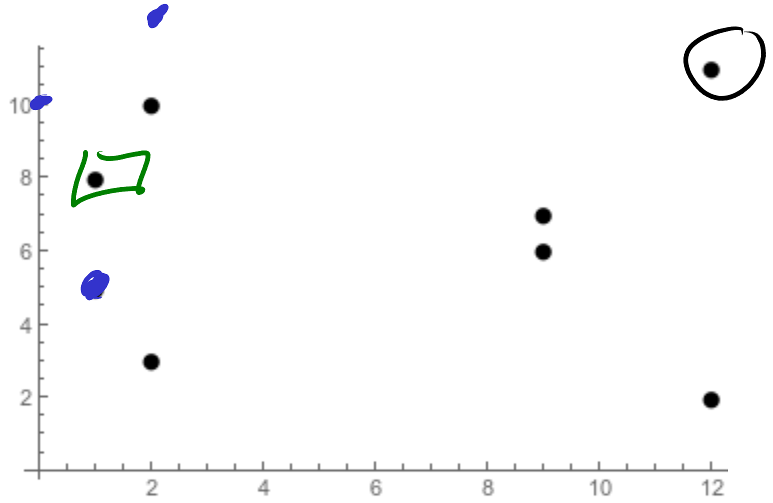
$2y' = 3$

$y' = 3/2 = 3 \cdot 7$

$= 21 = 8$

T line: $y = 8(x-12) + 2$

$y = 8x + 10$



$(8x+10)^2 = x^3 + 3x + 8$

$0 = x^3 + x^2 - x - 1$

$= (x-12)(x-12)(x-x_3)$

$1 = -12 - 12 - x_3$

$25 = -x_3$

$x_3 = 1$

$y = 8 + 10 = 18 = 5$

$(12,2) \oplus (12,2) = (1, -5)$

$= (1, 8)$

$a \equiv b$

$c \equiv d$

then

$a + c \equiv b + d$

$ac \equiv bd$

$-441 = -12 - 12 - x_3$

$x_3 = 441 - 24 = 417$

$y = 21(x-12) + 2$

$= 21x - 250$

$(21x - 250)^2 = x^3 + 3x + 8$

$441x^2 + Ax + B = x^3 + 3x + 8$

$0 = x^3 - 441x^2 +$ ______

Group Law Formula

Prop: $E: y^2 = x^3 + Ax + B \,/K$

$P = (x_1, y_1)$, $Q = (x_2, y_2)$.

then:

1) if $y_1 = -y_2$, then $P \oplus Q = \mathcal{O}$

2) if $P_1 = P_2$, set $\lambda = \dfrac{3x_1^2 + A}{2y_1}$

set $x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

$P \oplus Q = (x_3, y_3)$.

3) if $P_1 \neq P_2$, set $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

$P \oplus Q = (x_3, y_3)$

$E: y^2 = x^3 + 3x + 8$

$(2,3) \oplus (2,3)$

$\lambda = \dfrac{3 \cdot 2^2 + 3}{2 \cdot 3} = \dfrac{2^2+1}{2} = 5/2 = 35 = 9$.

$x_3 = 81 - 2 - 2 = 77 = 12$

$y_3 = 9(2 - 12) - 3$

$= -90 - 3 = -93 = 11$.

$(2,3) \oplus (2,3) = (12, -11)$

$= (12, 2)$.

Hasse: if E is an ell curve $/\mathbb{F}_p$ then

$$\underbrace{\left| \#E(\mathbb{F}_p) - (p+1) \right|}_{t_p} < 2\sqrt{p}$$

trace of Frobenius

Ell curve discrete log:

Dfn: Let $P, Q \in E(\mathbb{F}_p)$

Ell Curve DL: find n s.t.

$$Q = nP$$

Ex: $E: y^2 = x^3 + 3x + 8$

Find $\log_{(2,3)}(1,8)$

$2(2,3) = (12,11)$

$3(2,3) = (12,11) \oplus (2,3) = (9,7)$

$4(2,3) = (9,7) \oplus (2,3) = (1,5)$

$5(2,3) = (1,5) \oplus (2,3) = (1,8)$

$\log_{(2,3)}(1,8) = 5$

Hard!

for known n, finding nP is easy

compute $P, 2P, 4P, 8P, \ldots, 2^K P$

write $n = c_0 \cdot 1 + c_1 2 + c_2 4 + c_3 8 + \cdots + c_K 2^K$

Optimal fast EC multiplication

takes $3K/2 + 1$ operations worst case

where $K = \log_2(n)$

Optimal DL: $\sqrt{p}$ w/ Shanks

Crypto algorithms

Algorithm 3.11 (Elliptic Curve Diffie-Hellman)**.** Alice and Bob wish to exchange a key. They follow the following steps:

1. $\boxed{\text{A public party}}$ chooses a large prime p, and an elliptic curve E over $\mathbb{F}_p$, and a point $P \in E(\mathbb{F}_p)$.
2. Alice chooses a secret integer n_A, and Bob chooses a secret integer n_B. Neither party reveals this integer to anyone.
3. Alice computes $Q_A = n_A P$ and Bob computes $Q_B = n_B P$. They (publicly) exchange these values with each other.
4. Now Alice computes $n_A Q_B$ and Bob computes $n_B Q_A$.
5. $n_A Q_B = n_A n_B P = n_B n_A P = n_B Q_a$, so they now have a shared key.

Algorithm 3.12 (Elliptic Curve ElGamal)**.** First Alice generates a private key and a public key.

1. Choose a large prime number p, an elliptic curve E over $\mathbb{F}_p$, and a point $P \in E(\mathbb{F}_p)$ of large order. This is generally done by a $\boxed{\text{large trusted party.}}$
2. Alice chooses a private key n_A.
3. Alice computes and publishes a public key $Q_A = n_A P \in E(\mathbb{F}_p)$.

Now suppose Bob wishes to send Alice a a message encoded as a point $M \in E(\mathbb{F}_p)$.

1. Bob generates a random ephemeral key k.
2. Bob computes $C_1 = kP \in E(\mathbb{F}_p), C_2 = M + kQ_A \in E(\mathbb{F}_p)$. Bob transmits the pair of points (C_1, C_2) to Alice.

classic	
prime p	$E/\mathbb{F}_p$
generator g	point P
pick exponents	Picking
a, b, k	n_A, n_B, k
g^a	$n_A P$

$$C_2 - n_A C_1 = M + kQ_A - n_A k P$$

$$= M + \cancel{k n_A P - n_A k P} = M.$$

How does it stack up?

a pt contains $\sim \log_2(p)$ bits of info.

but transmitting a pt takes $2 \log_2(p)$ bits

On certain special curves, DL is secretly easy.

Hard to tell if a curve is secure.

NIST

Advantage:

General Number Field Sieve doesn't apply.

$O\left(e^{\sqrt{64/9}\, \log(n)^{1/3} (\log \log n)^{2/3}}\right)$ for RSA, regular DH, regular EG.

$O(\sqrt{p})$ for ECC.

real security	ECC	RSA
80	160	1024
112	224	2048
128	256	3072
256	512	15,360