# Asymmetric Key Cryptography

Elliptic Curve Cryptography (ECC)

***Priyank Kalla***
Professor
Electrical & Computer Engineering

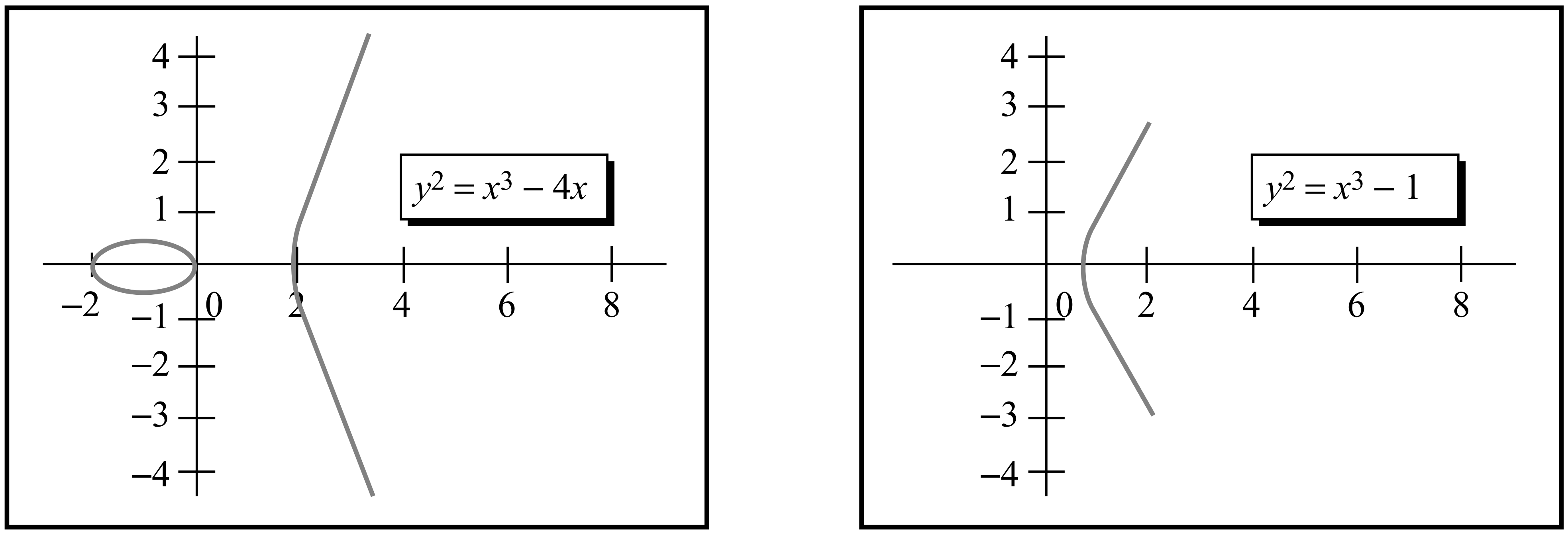
# Background

- In asymmetric key cryptography, we need two algebraic objects:
    - Commutative ring or a field for encryption and decryption: e.g. $\mathbb{Z}_n$ in RSA, $\mathbb{Z}_p$ in El Gamal
    - A group G for key generation: $G = \langle \mathbb{Z}^*_{\phi(n)}, \times \rangle$ in RSA, and $G = \langle \mathbb{Z}^*_p, \times \rangle$ in El Gamal
    - These are multiplicative groups, so multiplication, division, exponentiation and inverses are operations needed for key generation
    - In El Gamal, $\mathbb{Z}^*_p$ has primitive roots $(e_1)$, so $e_1^r, e_1^d \pmod p$ are also elements in $\mathbb{Z}^*_p$, so used in encipherment
- Limitation: key size = at least 1024 bits; now a days, maybe 2048 bits
- Elliptic curve E = degree-3 curve over a field. Under some conditions, points on E form an abelian (commutative) group $G = \langle E, + \rangle$, which is used for both key generation and encipherment
- Elliptic curve ≠ ellipse
- ECC Strength per bit much higher than RSA: 160 bit ECC security ~ 1024 bit RSA security
    - Potential for use in embedded systems, IoT devices, etc.

# Elliptic Curve $E_{\mathbb{F}}$

- Let $\mathbb{F}$ be any field. In general: $E_{\mathbb{F}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbb{F}$
- If **for all points** $(x_1, y_1)$, both partial derivatives $dE/dy = 2y_1 + a_1x_1 + a_3$, $dE/dx = 3x_1^2 + 2a_2x_1 + a_4 - a_1y_1$ do not simultaneously vanish: Non-Singular curve, otherwise the curve is Singular.
- We pick non-singular curves for ECC. NIST specifies the curve E: NIST standard
- There is a complicated analytical formula (based on discriminant $\Delta \neq 0$ of E) to select E
- Points on non-singular curves = abelian (commutative) group. Otherwise, on singular curves, commutativity does not hold
- Over $\mathbb{R}$, $E : y^2 = x^3 + ax + b$
  - Non-Singular if $\Delta = 4a^3 + 27b^2 \neq 0$
  - Non-Singular curves have 3 distinct roots (real or complex)

# Examples




a. Three real roots    b. One real and two imaginary roots

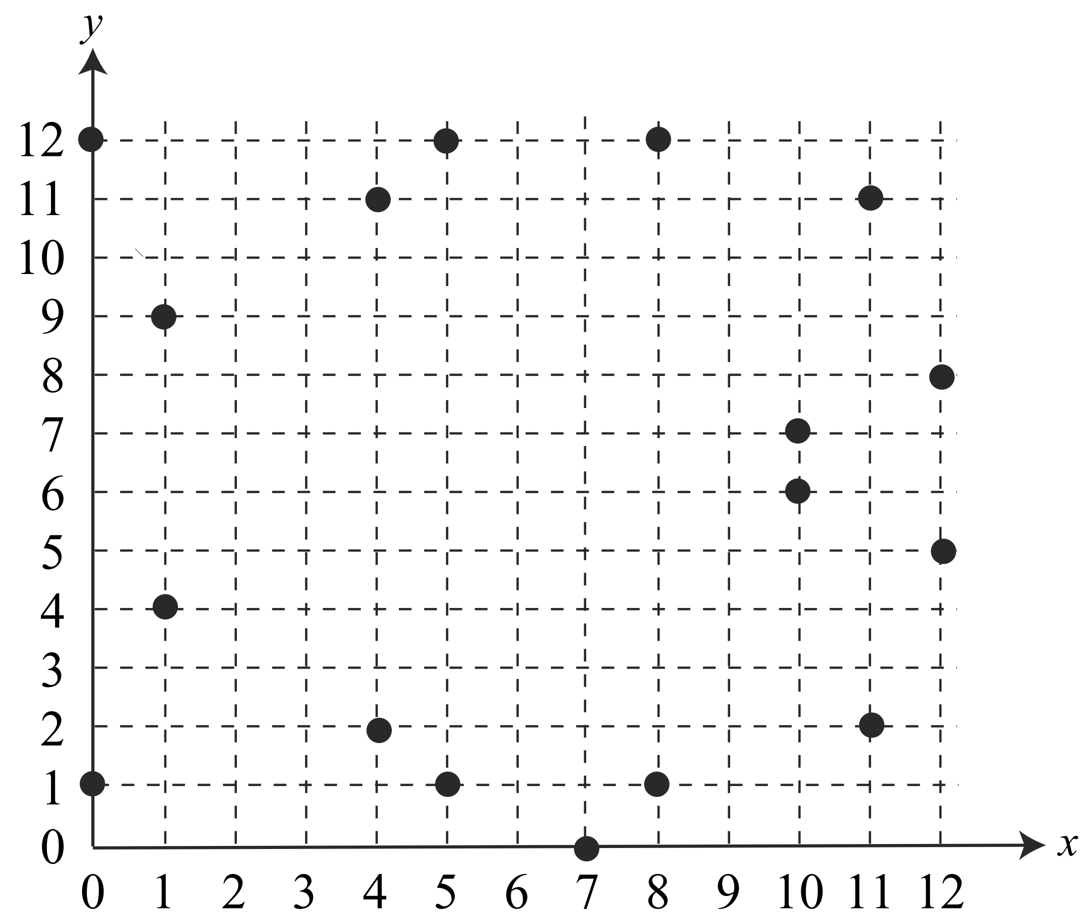
- For Key Generation, we need a group
  - Points on an elliptic curve form a group $G = \langle E, + \rangle$
  - Here $+ =$ point addition over elliptic curve

# Points on Elliptic Curves

- Example: $\mathbb{F}_{13} = \mathbb{Z}_{13} : y^2 = x^3 + x + 1 \pmod{13}$

| | |
|---|---|
| (0, 1) | (0, 12) |
| (1, 4) | (1, 9) |
| (4, 2) | (4, 11) |
| (5, 1) | (5, 12) |
| (7, 0) | (7, 0) |
| (8, 1) | (8, 12) |
| (10, 6) | (10, 7) |
| (11, 2) | (11, 11) |
| (12, 5) | (12, 8) |

Points

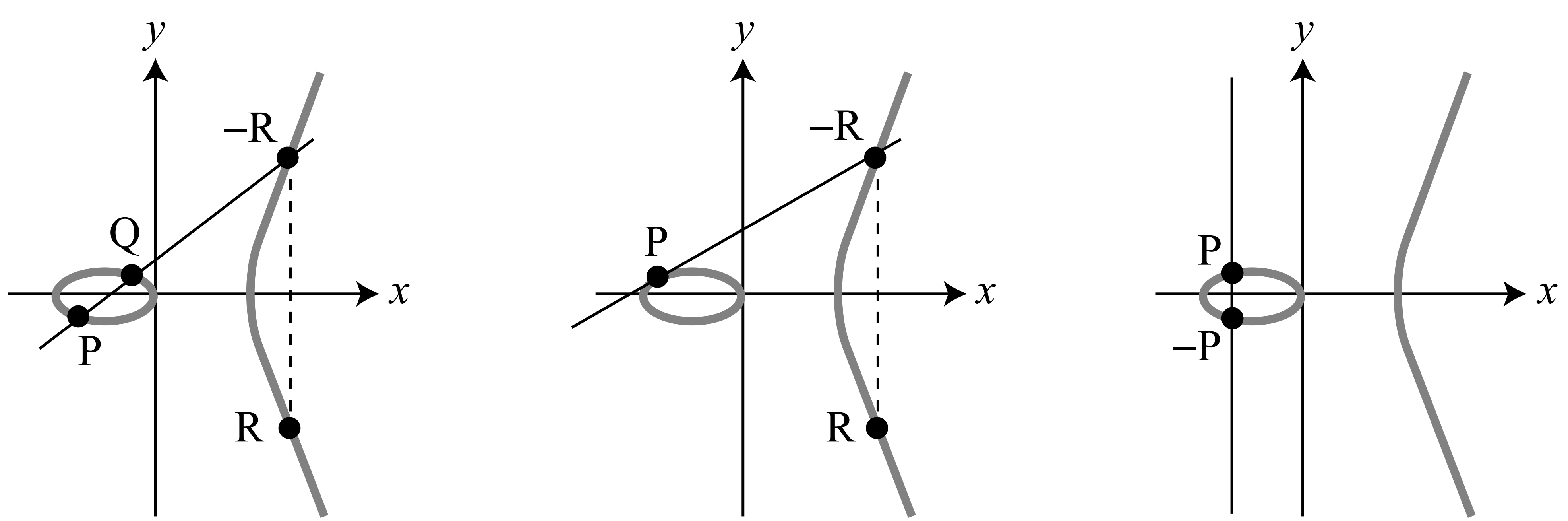


Graph

Given a curve, how to generate points on the curve efficiently? Hard problem, for now just simulate…

# Elliptic Curve Crypto

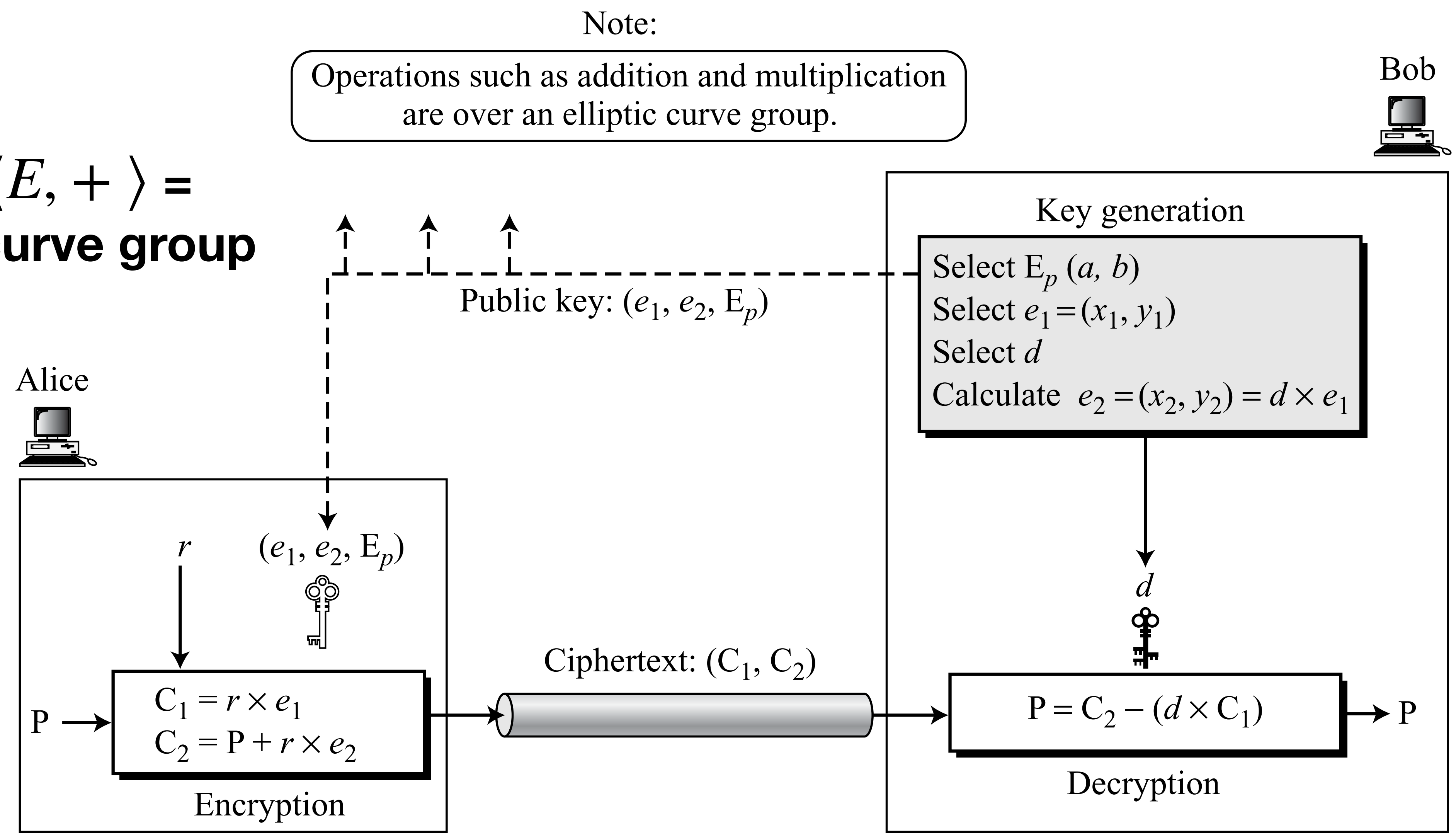
- Encipherment and key generation depends upon (scalar) point multiplications, point additions and point inverses
- Multiplication = repeated addition
- Curves are usually defined over finite fields. Points on curves form a group
- O = P + (-P) = additive identity of the group




a. (R = P + Q) b. (R = P + P) c. ($O$ = P + (– P))

# El Gamal over ECC

$G = \langle E, + \rangle$ =
**Elliptic curve group**

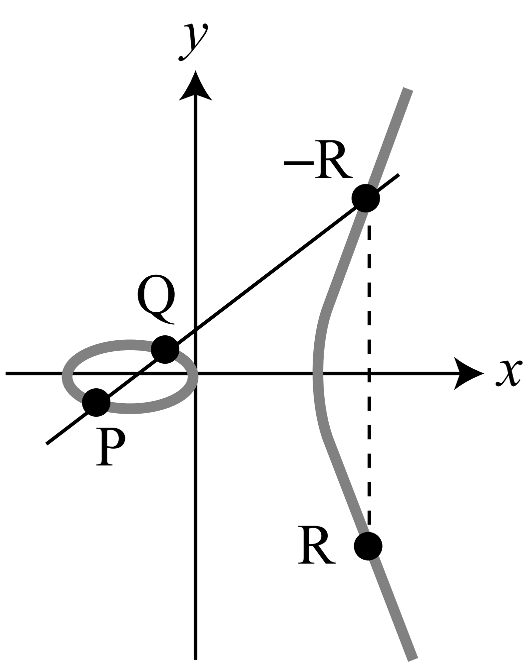



- $e_1$ = point on the curve, $d$ = scalar, $e_2 = d \times e_1$ = point multiplication
- $d \times e_1 = e_1 + e_1 + \ldots + e_1$ ($d$ times) = point multiplication. Example: 3P = 2P + P
- $C_1 = r \times e_1$ = another point on the curve
- P = plaintext = point on E. Create a 1-to-1 map between P and points on E. Tedious.
- C2 = point add, multiply. Decryption: $C_2 - dC_1$ = subtraction = additive inverse. [Group operations!]

# Point Addition over Elliptic Curve = Group Operation

- $G = \langle E, + \rangle$
- Closure: $P, Q \in E, P + Q \in E$
- Associativity: $(P + Q) + R = P + (Q + R)$
- Commutativity: For non-Singular E, $P, Q \in E, P + Q = Q + P$
- Additive Identity: There is a zero-point O, P = P+O = O+P. Also, O is its own inverse: O+O=O.
- Additive inverse: $P = (x_1, y_1), \ -P = (x_1, -y_1), P - P = O$.

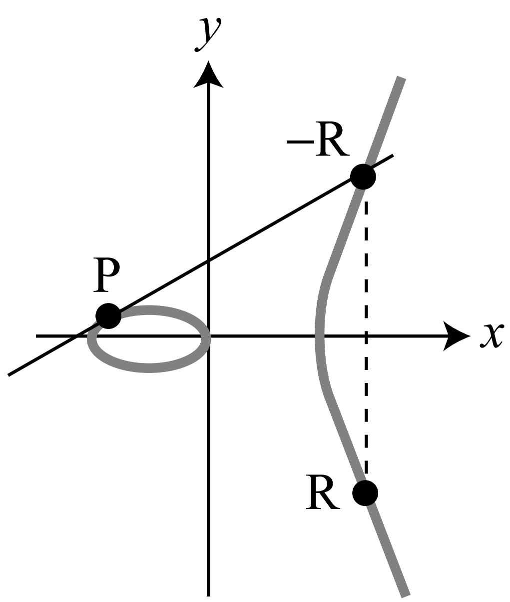
# Point Addition: P+Q=R




a. (R = P + Q)

- Let $E_{\mathbb{R}} : y^2 = x^3 + ax + b$;
- $P = (x_1, y_1) \neq Q = (x_2, y_2), P + Q = R = (x_3, y_3)$. Compute $R(x_3, y_3)$ as follows:
- PQ = line: $y - y_1 = \lambda(x - x_1), \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ = slope
- $y = \lambda(x - x_1) + y_1$: substitute in $E_{\mathbb{R}}$ to get -R
- $\lambda^2(x - x_1)^2 + y_1^2 + 2\lambda y_1(x - x_1) = x^3 + ax + b$
- Cubic equation = 3 roots $(x_1, x_2, x_3)$
- There is a result: “sum of roots = $-$ coefficient of $x^2$ term”, keep terms in $x$ on RHS
- $x_1 + x_2 + x_3 = \lambda^2$ or $\underline{x_3 = \lambda^2 - x_2 - x_1}$
- $-R(x_3, -y_3) : -y_3 = \lambda(x_3 - x_1) + y_1$ . So $\underline{y_3 = \lambda(x_1 - x_3) - y_1}$

# Point Doubling: P+P



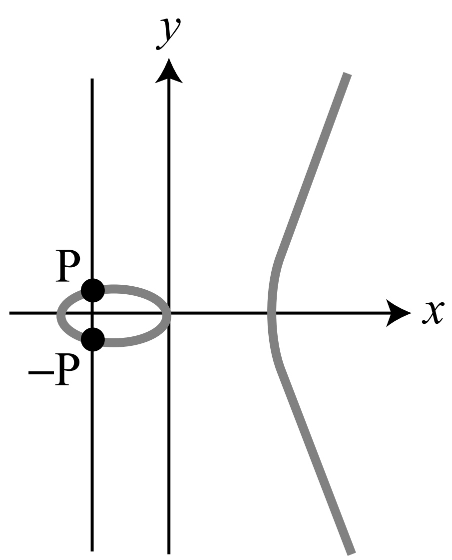
b. (R = P + P)

- $E_{\mathbb{R}} : y^2 = x^3 + ax + b;$
- The two points overlap (P+P = R), $P = (x_1, y_1)$
- Slope of tangent:

$$\lambda = (\frac{dE}{dx}) \div (\frac{dE}{dy}) = \frac{(3x_1^2 + a)}{2y_1}$$

- $\underline{x_3 = \lambda^2 - x_2 - x_1}$, and $\underline{y_3 = \lambda(x_1 - x_3) - y_1}$

# Inverse points



c. $(O = \mathrm{P} + (-\mathrm{P}))$

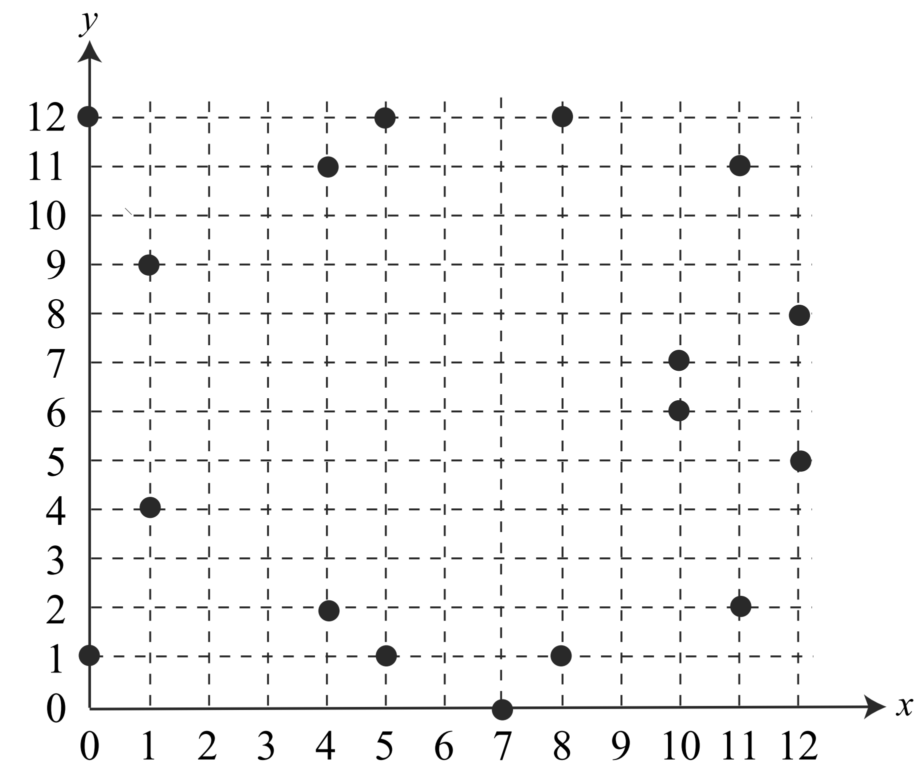
- $P(x_1, y_1), -P = (x_1, -y_1)$
- The line connecting P, -P does not intersect E
- But, we say it “intersects at infinity”
- Point at infinity = zero point = O = additive identity of the group
- P-Q = P + (-Q): get the additive inverse of Q

# Point Addition on Elliptic Curves

- Example: $\mathbb{F}_{13} = \mathbb{Z}_{13} : y^2 = x^3 + x + 1 \pmod{13}$

| | |
|---|---|
| (0, 1) | (0, 12) |
| (1, 4) | (1, 9) |
| (4, 2) | (4, 11) |
| (5, 1) | (5, 12) |
| (7, 0) | (7, 0) |
| (8, 1) | (8, 12) |
| (10, 6) | (10, 7) |
| (11, 2) | (11, 11) |
| (12, 5) | (12, 8) |

Points




Graph

Given a curve, how to generate points on the curve efficiently? Hard problem, for now just simulate…

- P=(4,2), Q = (10,6) R = (11, 2) = point on the curve

a. $\lambda = (6 - 2) \times (10 - 4)^{-1} \bmod 13 = 4 \times 6^{-1} \bmod 13 = 5 \bmod 13.$

b. $x = (5^2 - 4 - 10) \bmod 13 = 11 \bmod 13.$

c. $y = [5\ (4 - 11) - 2] \bmod 13 = 2 \bmod 13.$

# ECC in $\mathbb{F}_{2^k}$

- Over $\mathbb{F}_{2^k} \equiv \mathbb{F}_2[x] \pmod{P(x)}, P(x) =$ primitive polynomial of degree $k$

- Curve equation: $E: \ \ y^2 + xy = x^3 + ax^2 + b, a, b \in \mathbb{F}_{2^k}, b \neq 0$

  - P+Q = R: $$\lambda = (y_2 + y_1) / (x_2 + x_1)$$ $$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \qquad y_3 = \lambda\,(x_1 + x_3) + x_3 + y_1$$

  - P+P = 2P = R: $$\lambda = x_1 + y_1 / x_1$$ $$x_3 = \lambda^2 + \lambda + a \qquad y_3 = x_1^2 + (\lambda + 1)\,x_3$$

# ECC Curve Example

- Let $\mathbb{F}_8 = \mathbb{F}_2[x] \pmod{P(x) = x^3 + x + 1}$
- Let $P(\alpha) = 0 : \alpha^3 + \alpha + 1 = 0$, or $\alpha^3 = \alpha + 1$
- $\mathbb{F}_8 = \{0,1 = \alpha^7, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1\}$
- Let the ECC curve be $E : y^2 + xy = x^3 + \alpha^3 x^2 + 1$
- Find all the valid points on the curve E
    - For all $x \in \mathbb{F}_8$, compute corresponding values of $y$
    - E.g. x=0, $y^2 = 1, y = 1,1$ (two equal roots): two points (0,1),(0,1)
    - $x = \alpha : y^2 + \alpha y = \alpha^3 + \alpha^5 + 1 = \alpha^2 + 1$
    - $x = \alpha : y^2 + \alpha y + \alpha^2 + 1 = 0$. Quadratic equation of the form: $ay^2 + by + c$
    - Find roots: