Elliptic Curves

01 October 2020 12:05

| Algorithm Family | Cryptosystems | Security Level (bit) | | | |
|---|---|---|---|---|---|
| | | 80 | 128 | 192 | 256 |
| Integer factorization | RSA | 1024 bit | 3072 bit | 7680 bit | 15360 bit |
| Discrete logarithm | DH, DSA, Elgamal | 1024 bit | 3072 bit | 7680 bit | 15360 bit |
| Elliptic curves | ECDH, ECDSA | 160 bit | 256 bit | 384 bit | 512 bit |
| Symmetric-key | AES, 3DES | 80 bit | 128 bit | 192 bit | 256 bit |

## Elliptic Curves

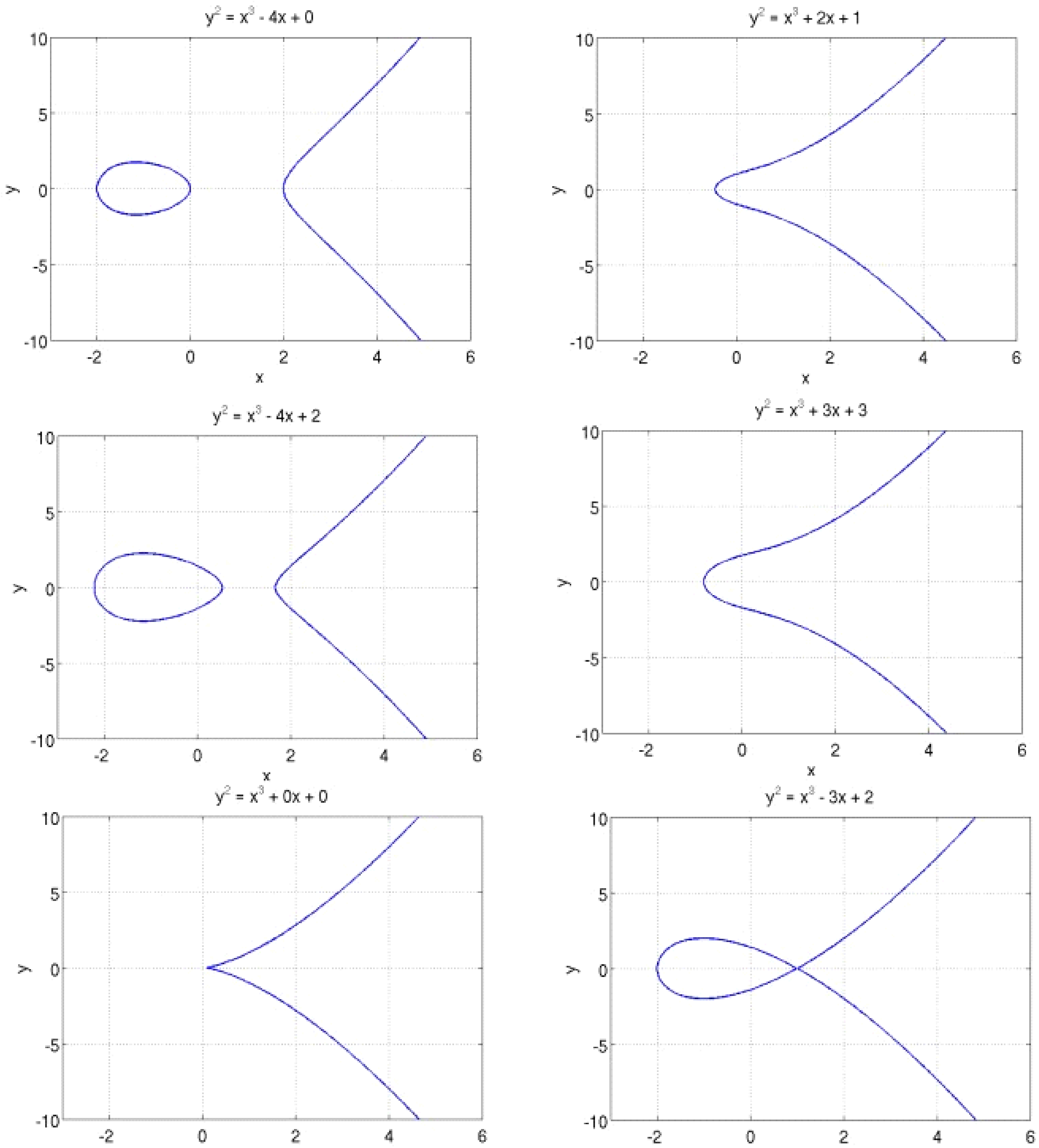
General Eq$^n$: $y^2 + b_1 xy + b_2 y = x^3 + a_1 x^2 + a_2 x + a_3$

Elliptic curves on real no.

$$y^2 = x^3 + ax + b \quad \text{— (1)}$$

a & b are real constants

(1) is also called Weierstrass equation of characterstic zero



Discriminant of a Polynomial of degree $n$ : Product of squares of difference of polynomial roots.

$$D_n = \prod_{i<j}^{n} (r_i - r_j)^2 \quad , \quad r_i\text{'s are roots of the polynomial.}$$

In case of a polynomial of degree 3

$$D_3 = (r_1-r_2)^2 (r_1-r_3)^2 (r_2-r_3)^2 \quad , \quad r_1, r_2, r_3 \text{ are roots of the poly}$$

If $D_n = 0$ then the poly. $(P_n)$ is called singular and
" $D_n \neq 0$ " " " " " " non-singular

$\Rightarrow$ A polynomial $P$ is non-singular if all of its roots are distinct.

In Cryptography we use ECs whose RHS is a non-singular polynomial

Note: Let $P = x^3 + ax + b$ then

$$D = -16(4a^3 + 27b^2)$$

$\Rightarrow$ $P$ is non-singular if $4a^3 + 27b^2 \neq 0$

* EC are sym. about $x$-axis.

Defining a Group:

Set:

Let $E(a,b)$ denotes the set of all points on the curve $y^2 = x^3 + ax + b$ i.e.

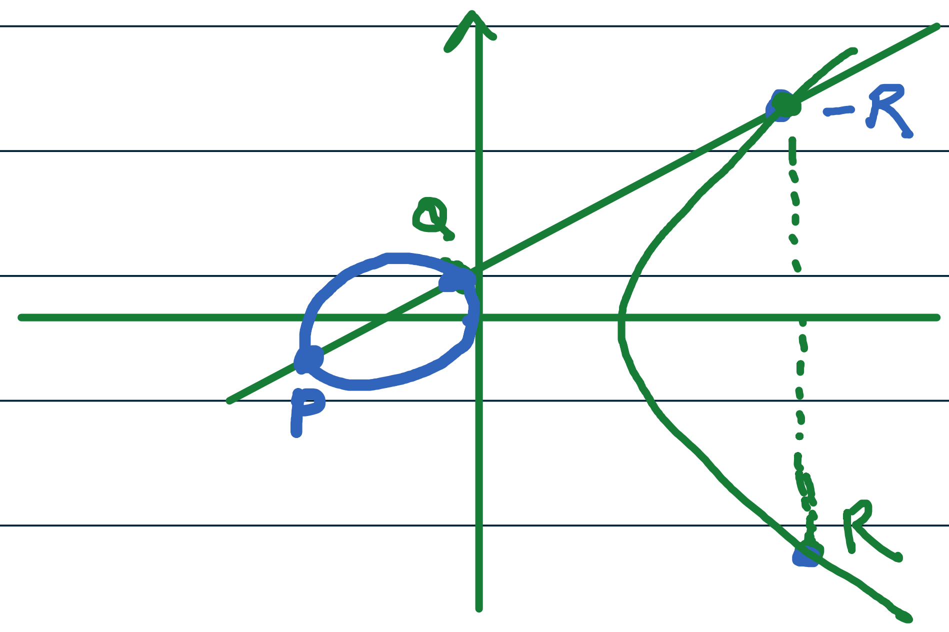
$$E(a,b) = \{ (x,y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = x^3 + ax + b \}$$

**Operation** We define an operation '+' on $E(a,b)$ as follows

Let $P, Q, R \in E(a,b)$, $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $R = (x_3, y_3)$

$P + Q = R$

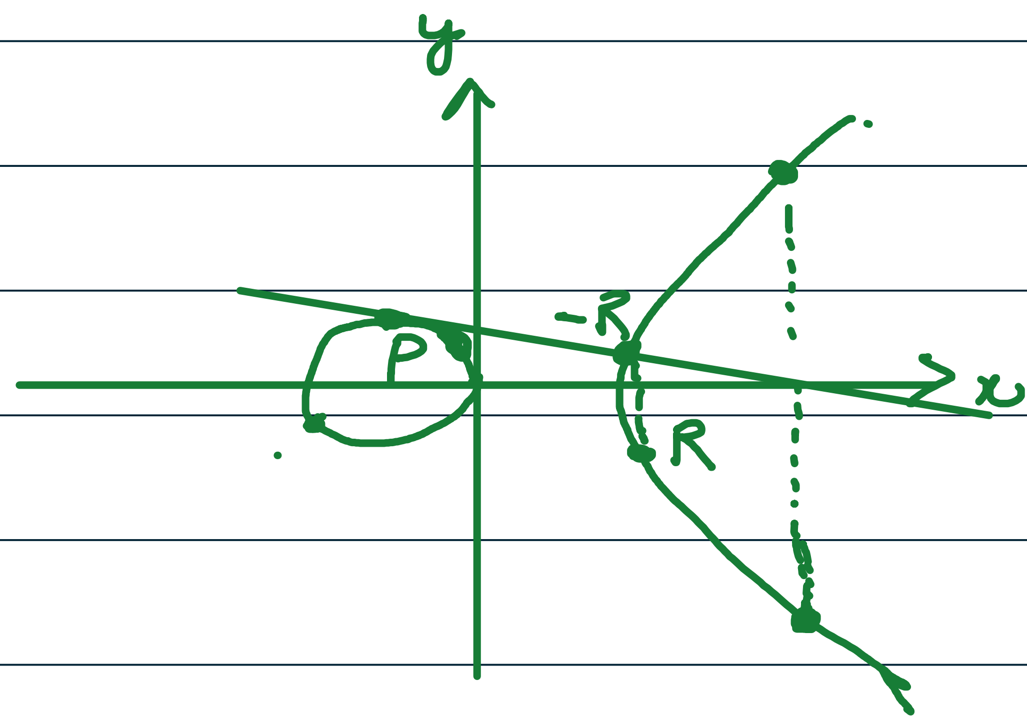
(1) $x_1 \neq y_1$ & $x_2 \neq y_2$




$$R = (\lambda^2 - x_1 - x_2,\ \lambda(x_1 - x_3) - y_1)$$

where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

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



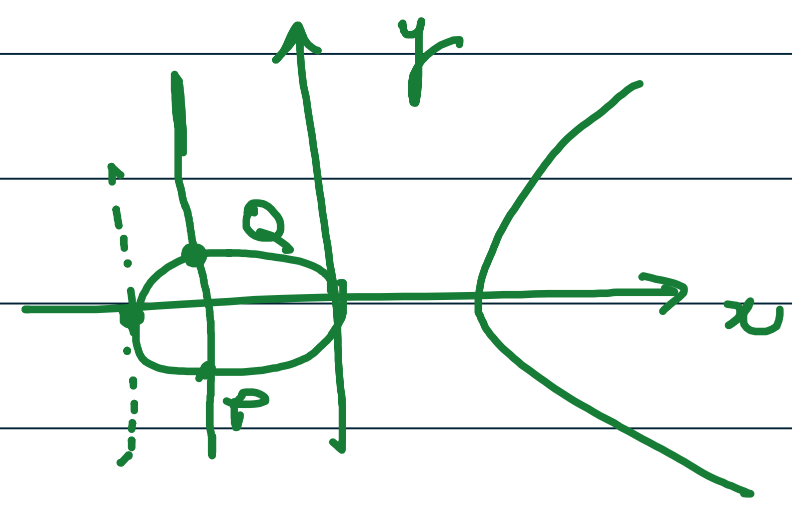

$P + P = R$

$$R = (\lambda^2 - x_1 - x_2,\ \lambda(x_1 - x_3) - y_1) \checkmark$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \checkmark$$

(iii) If $P = (x_1, y_1)$, $Q = (x_1, -y_1)$

Then, we define $R = O$
$\downarrow$
An imaginary point at inf.




(iv) If the tangent a point $P$ has the slope $\pi/2$ and $Q = P$ then

$$P + Q = P + P = 2P = P$$

Let $E(a,b)$ also includes '$O$'.

Then $(E(a,b), +)$ is a group.

(i) closed

(ii) Assoc

(iii) '$O$' is the identity

(iv) Inverse of $P = (x_1, y_1)$ is $-P = (x_1, -y_1)$.

## Elliptic curve over $\mathbb{Z}_p$ $(p>3)$

ECs over $\mathbb{Z}_p$ $(p>3)$ is the set of all points $x, y \in \mathbb{Z}_p$ s.t. $y^2 = (x^3 + ax + b) \bmod p$

together with an imaginary point $O$ at inf where $a, b \in \mathbb{Z}_p$ & $4a^3 + 27b^2 \not\equiv 0 \bmod p$.

$$E_p(a,b) = \{ (x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid y^2 = x^3 + ax + b,\ a,b \in \mathbb{Z}_p \} \cup \{O\}$$

$(E_p(a,b), +)$ is a group where $+$ is define as follows.

$P, Q, R \in E_p(a,b)$ where $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $R = (x_3, y_3)$

Then $P + Q = R = \left( \underbrace{(\lambda^2 - x_1 - x_2) \bmod p}_{x_3},\ \underbrace{\lambda(x_1 - x_3) - y_1) \bmod p}_{y_3} \right)$

where $\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \bmod p, & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} \bmod p, & P = Q \end{cases}$

and if $Q = (x_1, -y_1)$ then

$P + Q = O$

and if the slope of the tangent at $P$ is $\pi/2$ then

$P + P = P$.

**Ex.** $E_{23}(1, 1)$

$4 \times 1^3 + 27 \times 1^2 = 31 \bmod 23 \not\equiv 0$

Let $P = (3, 10)$, $Q = (9, 7)$ then

$P + Q$ ? $\lambda = \dfrac{7-10}{9-3} \bmod 23 = \dfrac{-3}{6} \bmod 23 = \dfrac{-1}{2} \bmod 23$

$= (-1)\ 2^{-1} \bmod 23$

$= 11$

$x_3 = (\lambda^2 - x_1 - x_2) \bmod 23 = (11^2 - 3 - 9) \bmod 23 = 17$

$y_3 = 20$ $R = (17, 20)$

$$y^2 = x^3 + 2x + 2 \mod 17$$

$$P = (5, 1)$$

$$P + P = \underline{(6, 3)}$$

| | |
|---|---|
| $2P = (5,1) + (5,1) = (6,3)$ | $11P = (13,10)$ |
| $3P = 2P + P = (10,6)$ | $12P = (0,11)$ |
| $4P = (3,1)$ | $13P = (16,4)$ |
| $5P = (9,16)$ | $14P = (9,1)$ |
| $6P = (16,13)$ | $15P = (3,16)$ |
| $7P = (0,6)$ | $16P = (10,11)$ |
| $8P = (13,7)$ | $17P = (6,14)$ |
| $9P = (7,6)$ | $18P = (5,16)$ |
| $10P = (7,11)$ | $19P = \mathcal{O}$ |

No. of points $N$ in $E_p(a, b)$ is bounded by

$$p + 1 - 2\sqrt{p} \leq N \leq p + 1 + 2\sqrt{p}$$

Thus, $|E_p(a,b)| \approx |\mathbb{Z}_p|$

Thus, $E_p(a,b)$ has app $p$ elements.