ElGamal Public-key Cryptographic System

Global Public Elements

a prime number q & its primitive root α.

Key generation by Alice

1. Generate a private key X_A, $1 \le X_A \le q-1$.
2. Compute $\underline{Y_A = \alpha^{X_A}} \bmod q$.

   Public key (q, α, Y_A)

Encryption by Bob with Alice's Public key

1. message M : $0 \le M \le q-1$
2. choose a random integer $\overset{X_B}{k}$: $1 \le k \le q-1$.

   Compute a $\boxed{\text{one-time pad}}$ $K = (Y_A)^k \bmod q$
   $= \alpha^{kX_A} \bmod q$.
3. Encrypt M as (C_1, C_2), where $\alpha^{X_B X_A}$.

$$C_1 = \alpha^k \bmod q, \quad C_2 = KM \bmod q$$

Decryption by Alice with her private key

1. Recover $K = C_1^{X_A} \bmod q = \alpha^{kX_A} \bmod q$.
2. Compute $M = (K)^{-1} C_2 \bmod q$.

Ex. $q = 19$. $\alpha = 10$.

Alice $X_A = 5$.

$Y_A = \alpha^{X_A} \bmod q = 10^5 \bmod 19 = 3$.

private key $\{5\}$. public key $\{q, \alpha, Y_A\}$

$= \{19, 10, 3\}$

Bob $M = 17$

chooses $k = 6$.

$K' = Y_A^k \equiv 3^6 \bmod 19 = 7$.

$C_1 = \alpha^k \bmod q = 10^6 \bmod 19 = 11$

$C_2 = K' \cdot M = 7 \times 17 \equiv 5 \bmod 19$.

Alice receives (C_1, C_2).

Calculate $K' = C_1^{X_A} \bmod q = 11^5 \bmod 19 = 7$

$K'^{-1} = 7^{-1} \bmod 19 = 11$

$M = 11 \cdot C_2 \bmod 19 = 17$. #.

A unique k should be used for each block of message

If $C_1^{(1)} = \alpha^k \bmod q$, $C_2^{(1)} = K' M_1 \bmod q$

$C_1^{(2)} = \alpha^k \bmod q$, $C_2^{(2)} = K' M_2 \bmod q$.

$$\Rightarrow \frac{C_2^{(1)}}{C_2^{(2)}} = \frac{M_1}{M_2} \bmod q$$

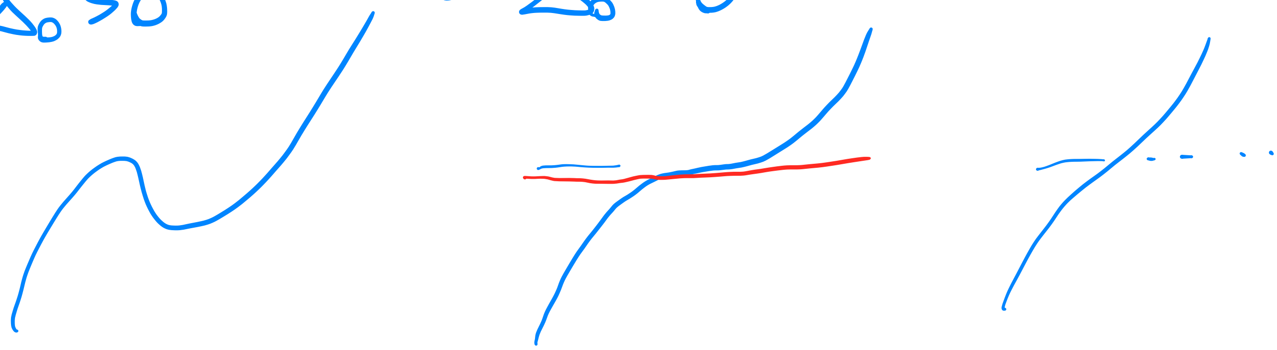
Elliptic Curve

Cubic function $f(x) = ax^3 + bx^2 + cx + d$.

$0 = f'(x) = 3ax^2 + 2bx + c. \Rightarrow x = \dfrac{-b \pm \sqrt{b^2 - 3ac}}{3a}$

$\Delta_0 = b^2 - 3ac$

① $\Delta_0 > 0$ ② $\Delta_0 = 0$ ③ $\Delta_0 < 0$



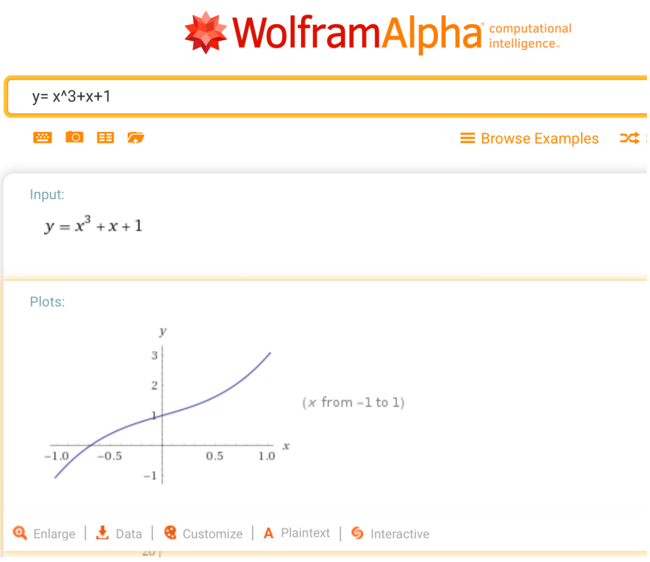
Consider $f(x) = x^3 + px + q$. $p, q \in \mathbb{R}$

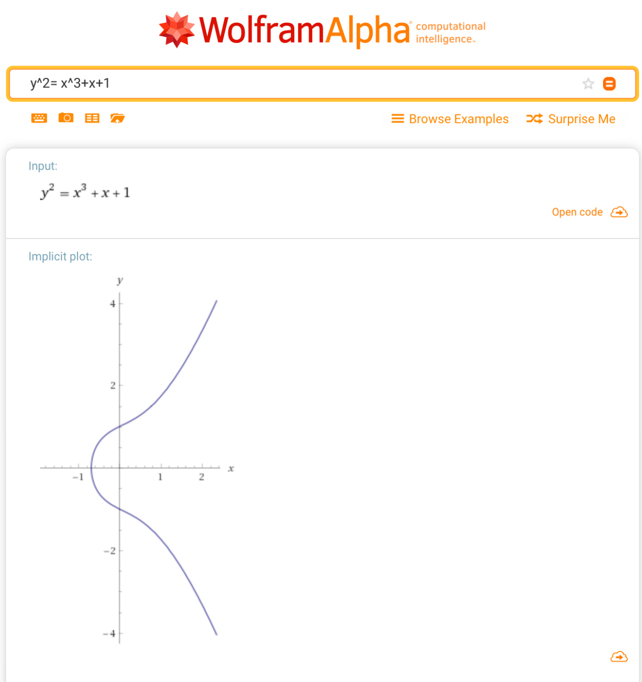
$\Delta = -4p^3 - 27q^2$.

$\Delta_0 = -3p$.

① $\Delta > 0$, $f(x)$ has three distinct roots.

② $\Delta = 0$. $f(x)$ has a multiple root.


WolframAlpha computational intelligence.
y= x^3+x+1
Browse Examples
Input:
$y = x^3 + x + 1$
Plots:
(x from −1 to 1)
Enlarge | Data | Customize | Plaintext | Interactive


WolframAlpha computational intelligence.
y^2= x^3+x+1
Browse Examples
Surprise Me
Input:
$y^2 = x^3 + x + 1$
Open code
Implicit plot:

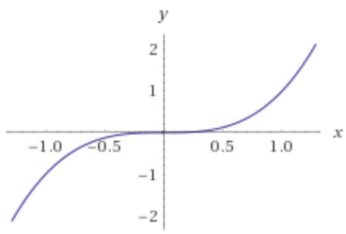
y= x^3

Browse Examples

Input:

$$y = x^3$$

Plot:



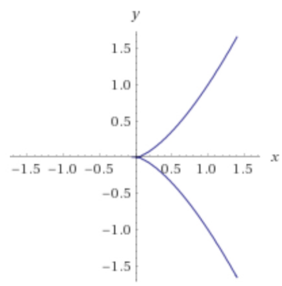
(x from −1.3 to 1.3)

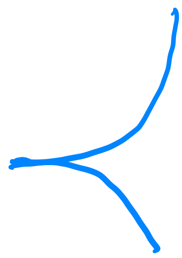
y^2 = x^3

Input:

$$y^2 = x^3$$

Implicit plot:





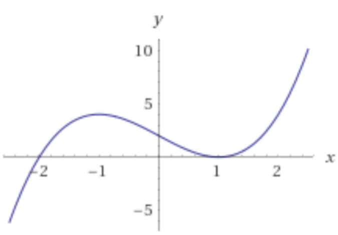
y = x^3-3x+2

Browse Exampl

Input:

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

Plots:



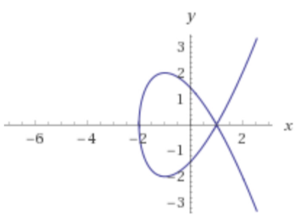
(x from −2.5 to 2.5)

y^2 = x^3-3x+2

Input:

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

Implicit plot:



Elliptic curve arithmetic

$$y^2 = x^3 + px + q, \quad p, q \in \mathbb{R}.$$

the curve is symmetric about $y=0$.

Let O be the point at infinity.

Let $E(p,q) = \{(x,y) \in \mathbb{R}^2 : y^2 = x^3 + px + q\} \cup \{O\}$

Suppose $4p^3 + 27q^2 \neq 0$.

It can be shown that every line intersecting $E(p,q)$ intersects it in exactly three points where a point P is counted twice if the line is tangent to the curve at P and also the point at infinity is also counted (where the line is vertical.)