1. 沒有給 curve 的 a,b 自己算:把 G,A 代進 y**2 =x**3 +ax +b (mod p) 就可以求得 a,b
2. Check 是否是 singular curve (4*a**3 +27*b**2) %p == 0,發現是
3. 找出 singular point
4. 先把整個 curve 做位移，把 singular point 搬到原點(0,0),讓方程式可以變成 y^2 = x^2*(x-beta) or y^2 = x^3 的形式
5. 知道他是 singular curve 之後還要判斷他是 Node 還是 cusp

   $$y^2 = (x - \alpha)^2 (x - \beta)$$

   發現是 y^2 = x^2*(x-b),所以是 Node

   (x + 25597287335196234621657091569942027389158713451655456247456560619039717972 42) * x^2

   Beta = -25597287335196234621657091569942027389158713451655456247456560619039717972 42
6. Node 可以 mapping 到 multiplicative group

   $$\varphi(P(x, y)) = \frac{y + \sqrt{\alpha - \beta}(x - \alpha)}{y - \sqrt{\alpha - \beta}(x - \alpha)}$$

   $$\varphi(P + Q) = \varphi(P) \times \varphi(Q)$$

   $$\varphi(dP) = \varphi(P)^d$$

   可以發現這個公式 Node 的點的加法會變成實數的乘法,而 A 就是經過加了 d 次的 G 而來,所以 pi(A) = pi(G)^d ,此時 pi(A),pi(G)我們都有了,就可以直接透過計算指數的 func 得到 d
7. 得到 d 之後 B 乘上 d 次,就可以得到 key