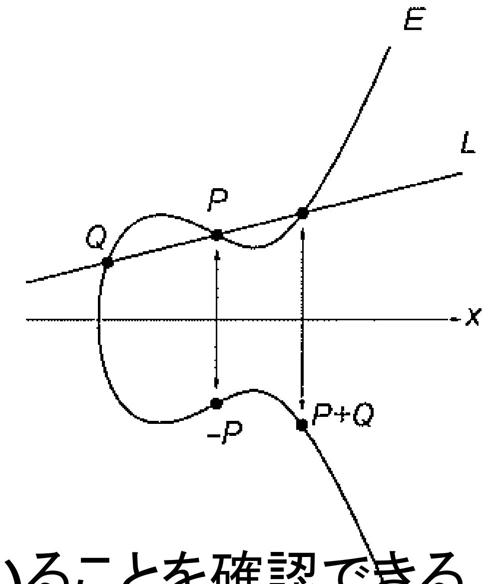
楕円曲線と楕円曲線暗号

楕円曲線とは

- ３次曲線$y^2 = x^3 + ax + b$により定義される曲線E
  - 係数体の標数は５以上、判別式$4a^3 + 27b^2 \neq 0$
  - 無限遠点ＯもＥ上の点と考える
  - 楕円曲線Ｅ上の点について加法を定義することができ、これら点の集合が群になる

E上の点Pと点Qの加算のイメージ（実数体上）
（実際は有限体上で計算する）

1. 点Pと点Qを結ぶ直線Lを求める
2. 直線Lと曲線EのP，Q以外の交点Ｐ‘を求める
3. 点Ｐ‘とx軸に対して対称な点R（E上にある）を点Pと点Qの和とする



零元は無限遠点Oになる。群の公理を満たしていることを確認できる。

群（Group）とは（復習）

- 何らかの集合Gと、Gの要素間に演算○が定義されているとする。以下の条件を満たすとき、集合Gと演算○は群（Group）であるという

1. 【閉性】任意の2元a,b∈Gについて、a○b∈Gである
2. 【結合則】任意の元a,b,c∈Gに対して、a○(b○c)=(a○b)○cが成り立つ
3. 【単位元】任意の元a∈Gに対して、a○e=e○a=aとなる元e（単位元という）が存在する
4. 【逆元】任意の元a∈Gに対して、a○b=b○a=eとなる元b（aの逆元という）が存在する

（注）群の定義では、演算○が具体的にどのような演算であるかは決めていない。これらの性質を満たせば、どのような演算であっても群と呼ぶ

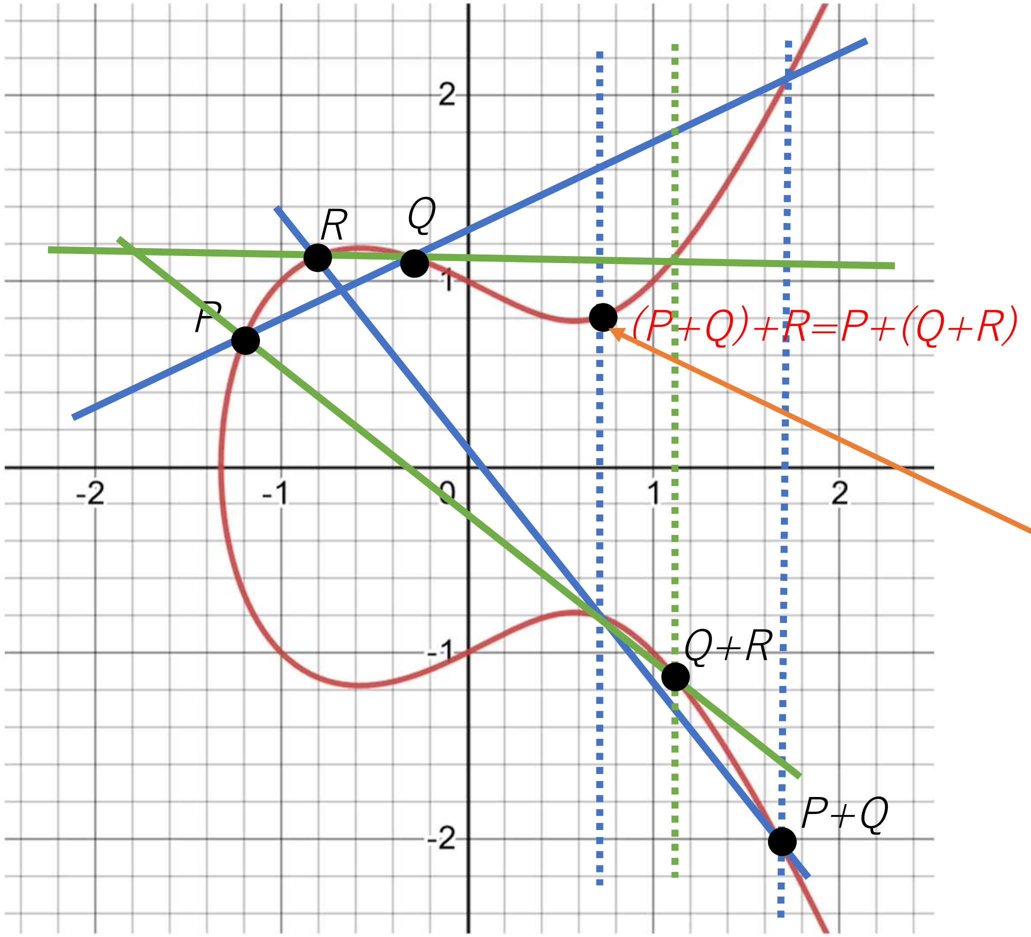
楕円曲線上の点が群をなすことの確認

- 楕円曲線上の点について、先述した加算＋に関して群をなす

1. 点Pと点Qの和P+Qは、定義からE上の点なので閉性を満たす
2. 任意の点P,Q,Rについて、P+(Q+R)=(P+Q)+Rであれば結合則を満たす（これから確認する）
3. 任意の点Pに対して、P+O=O+P=Pとなる点Oが単位元（零元）（これから確認する）
4. 任意の点Pに対して、P+Q=Q+P=Oとなる点Qが、Pの逆元である（これから確認する）

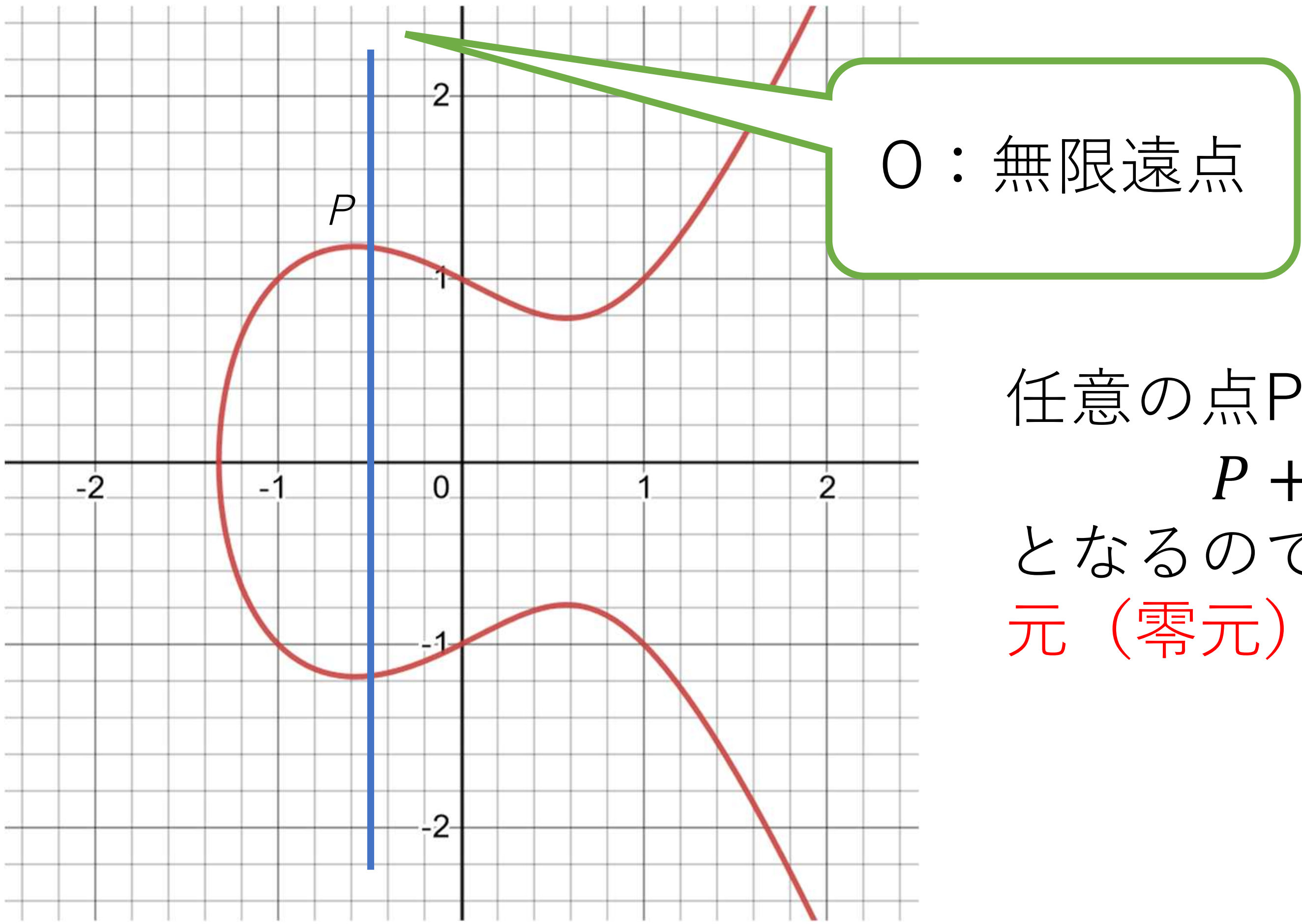
- 任意の点P,Qについて、加法の定義からP+Q=Q+P（交換法則）がいえるので、可換群（アーベル群）である。

結合法則の確認



$(P+Q)+R = P+(Q+R)$
を確認できる。

単位元（零元）の存在

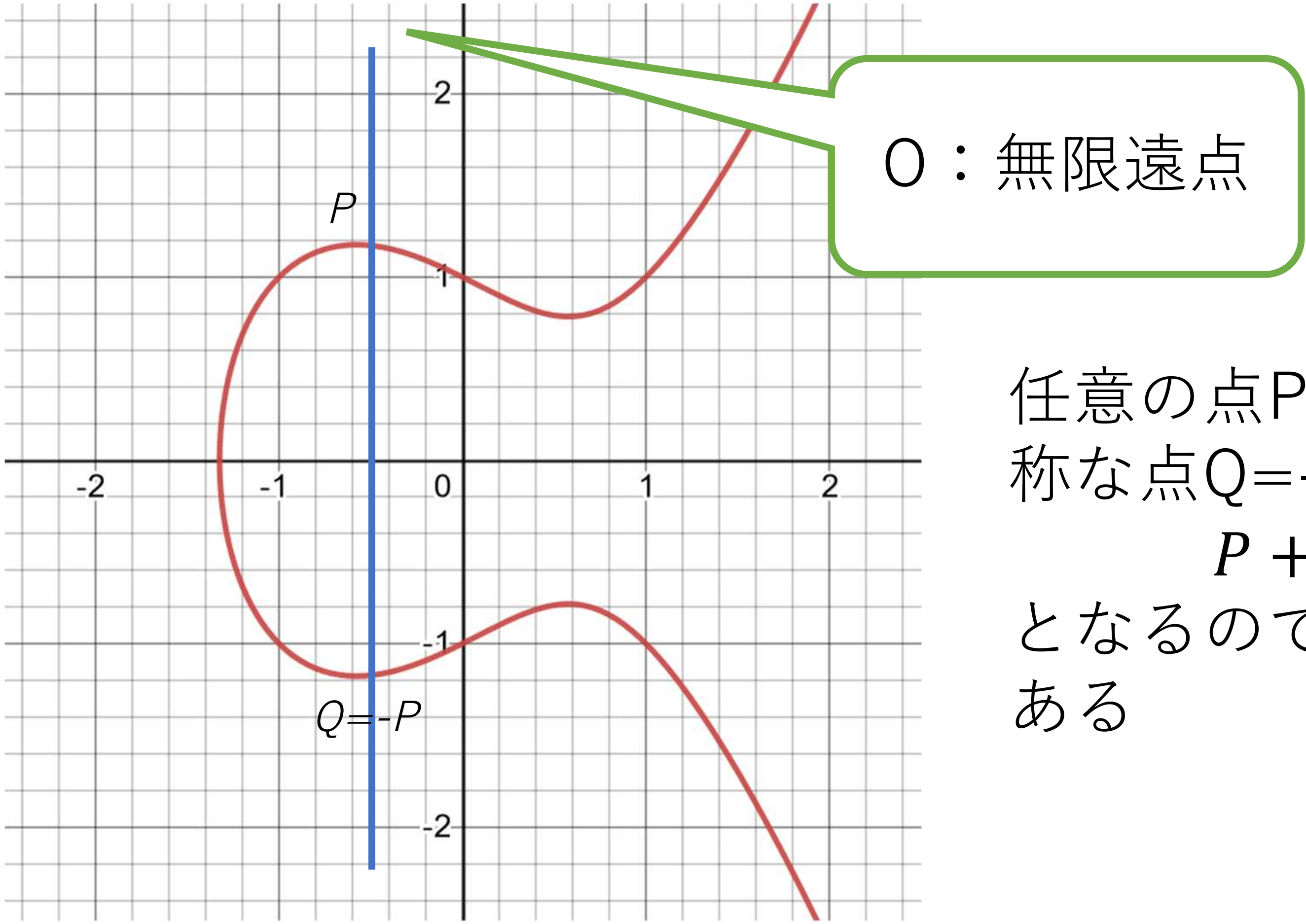


任意の点Pについて、

$$P + O = O + P = P$$

となるので、無限遠点Oは単位元（零元）である

逆元の存在

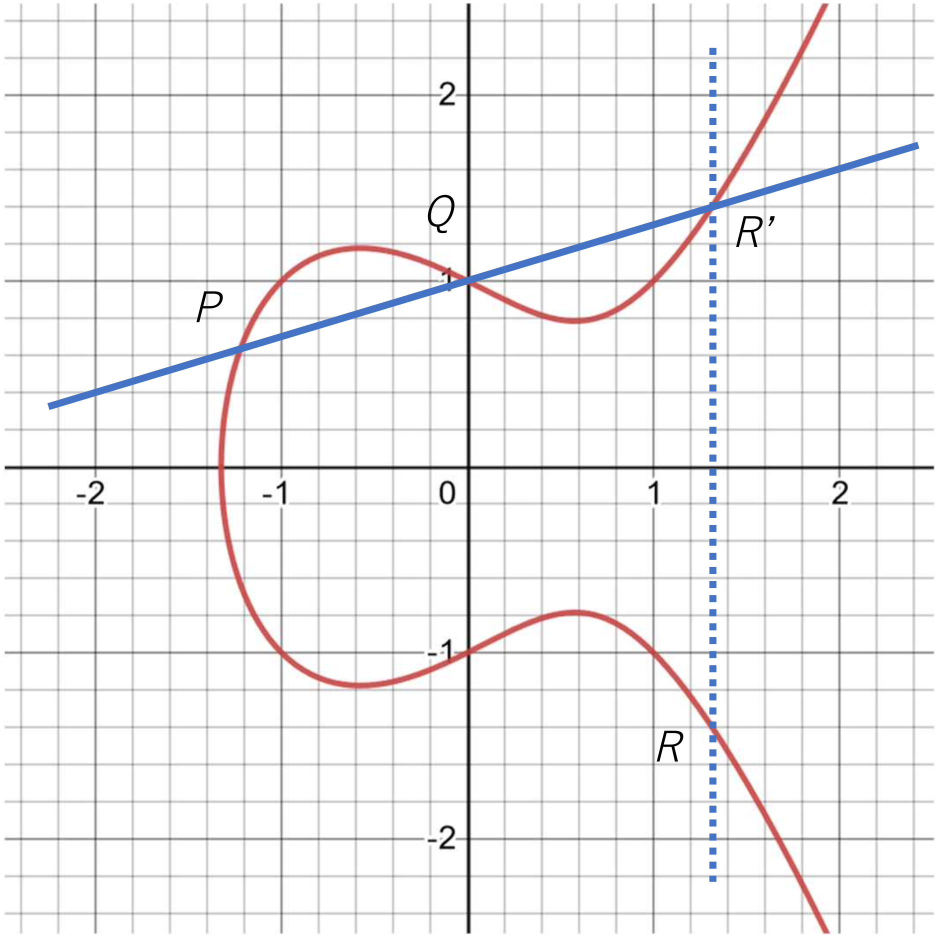


任意の点Pについて、x軸と線対称な点Q=-Pとすると、

$$P + Q = Q + P = O$$

となるので、点Qは点Pの逆元である

加法公式の導出（$P \neq Q(x_1 \neq x_2)$）

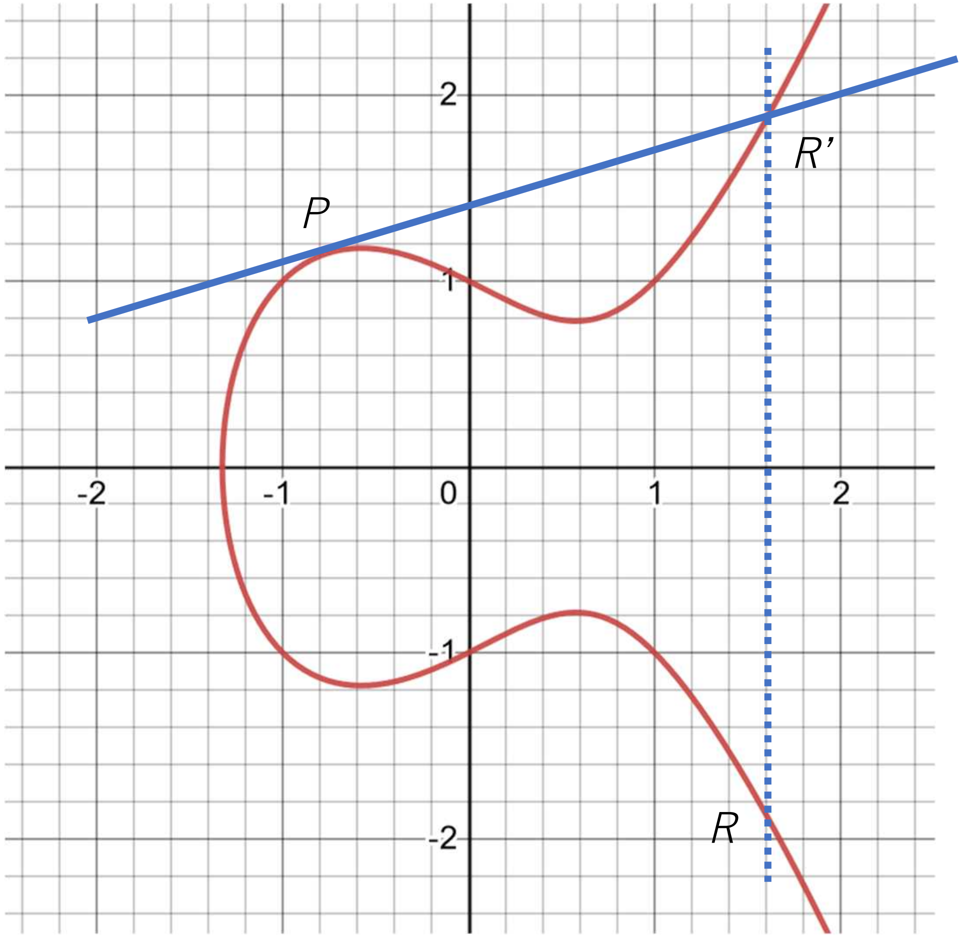


- 点$P(x_1, y_1)$と点$Q(x_2, y_2)$を結ぶ直線をL($y = \alpha x + \beta$)とする。
- このとき、$\alpha = \frac{y_2 - y_1}{x_2 - x_1}, \beta = y_1 - \frac{y_2 - y_1}{x_2 - x_1} \cdot x_1$である。
- 点$R'(x_3, -y_3)$とすると、点P, Q, R'はE上の点であり、$(\alpha x + \beta)^2 = x^3 + ax + b$を満足する。整理すると、$x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + b - \beta^2 = 0$となる。
- 一方、この３次方程式の根は、x_1, x_2, x_3のはずなので左辺は、$(x - x_1)(x - x_2)(x - x_3)$と因数分解できるはず。これを展開して、$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1 x_2 + x_2 x_3 + x_3 x_1)x - x_1 x_2 x_3$と なる。 x^2の 項を係数比較して、
- $x_3 = \alpha^2 - x_1 - x_2$である。これより、$y_3 = -(\alpha x_3 + \beta)$
- 以上より加法公式

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$$

$P = Q$の場合（２倍算）



- 点$P(x_1, y_1)$における接線をL$(y = \alpha x + \beta)$とすると、$2yy' = 3x^2 + a$より、点Pにおける微係数は$\frac{3x_1^2+a}{2y_1}$
- 従って、$\alpha = \frac{3x_1^2+a}{2y_1}, \beta = y_1 - \frac{3x_1^2+a}{2y_1} \cdot x_1$である。
- 点$R'(x_3, -y_3)$とすると、点P, R'はE上の点であり、$(\alpha x + \beta)^2 = x^3 + ax + b$を満足する。整理すると、$x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + b - \beta^2 = 0$となる。
- 一方、この３次方程式の根は、x_1, x_3のはずなので左辺は、$(x - x_1)^2\ (x - x_3)$と因数分解できるはず。これを展開して、$x^3 - (2x_1 + x_3)x^2 + (x_1^2 + 2x_1x_3)x - x_1^2x_3$となる。$x^2$の項を係数比較して、
- $x_3 = \alpha^2 - 2x_1$である。これより、$y_3 = -(\alpha x_3 + \beta)$
- 以上より加法（２倍算）公式

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)$$

楕円曲線上の離散対数問題(ECDLP)

- 加法公式より、楕円曲線上の点の加算は、数回のF_q上の演算で計算できることがわかる。
- 楕円曲線上の点Ｐが与えられているとき、
$$Q = nP = P + P + \cdots + P$$
（点Pをn回加える）となる点Ｑからｎを求める問題を楕円曲線上の離散対数問題（ＥＣＤＬＰ）という
- ＥＣＤＬＰは一般のＤＬＰと同様困難な問題
1024bitのDLPと160bitのＥＣＤＬＰが同程度の難しさになる
→鍵長が短い公開鍵暗号を構成できる

計算の高速化

- $Q = nP$の計算には、$n-1$回の加算が必要？→否
- 高々$[\log_2 n] - 1$回の２倍算および加算で計算できる。
- （例）$Q = 100P$を求める。100=1100100(2)であるから
- $2P \leftarrow P + P$
- $4P \leftarrow 2P + 2P$
- $8P \leftarrow 4P + 4P$
- $16P \leftarrow 8P + 8P$
- $32P \leftarrow 16P + 16P$
- $64P \leftarrow 32P + 32P$
- $100P \leftarrow 64P + 32P + 4P$
- により、６回の２倍算と２回の加算で計算できる。（普通に計算すると99回の加算）

ECDLPを利用した鍵共有法

（準備）楕円曲線Eと、E上の点G（位数p）を決める

（1）乱数aを決める

（1’）乱数bを決める

（2）$P = aG$
を計算する

（2’）$Q = bG$
を計算する

（3）P を送る

（4）Q を送る

（5）$K = aQ$
を計算する

（5’）$K' = bP$
を計算する

PあるいはQからa, bを求めることはECDLPであり、できない

$$K = aQ = abG = bP = K'$$

$K = K'$であり、同じ鍵の値が共有できた！

ECDLPを利用する公開鍵暗号（楕円エルガマル暗号）

- （準備）
  楕円曲線Eと、E上の点G（位数p）を決める。
  秘密鍵：$s$$(0 < s < p)$、公開鍵：$Y = sG$とする。
- （暗号化）
  平文M（E上の点に写像する）、乱数（暗号化毎に変える）rを生成し、
  暗号文：$(C_1, C_2) = (rG, rY + M)$
- （復号化）

$$C_2 - sC_1 = rsG + M - srG = M$$