暗号入門7講の7
「代数曲線と暗号」

松尾和人

2007年7月20日

Diffie-Hellman鍵共有アルゴリズム (1976)

システム設定	p: **素数**, $b \in \mathbb{F}_p^*$ s.t. $\langle b \rangle = \mathbb{F}_p^*$	
	アントニオ	**ババ**
秘密鍵設定	$K_a \in \mathbb{Z}/(p-1)\mathbb{Z}$	$K_b \in \mathbb{Z}/(p-1)\mathbb{Z}$
公開鍵計算	$K_a' = b^{K_a}$	$K_b' = b^{K_b}$
	公開鍵 K_*' **を公開**	
共通鍵計算	$K = {K_b'}^{K_a}$	$K = {K_a'}^{K_b}$
	同一の鍵 K **を共有できた**	

離散対数問題

- $K' \mapsto K$

- Given: p: prime, $b \in \mathbb{F}_p^*$, $a \in \langle b \rangle$
  Find: $x \in [0, \#\langle b \rangle - 1]$ s.t. $a = b^x$
  $\mathrm{Ind}_b a := x$

- **簡単：** $(x, b, p) \mapsto a \equiv b^x \bmod p$

- **困難：** $(a, b, p) \mapsto x$

離散対数問題の難しさ

- **全数探索**
  - $O(p)$
- Square-root **法**
  - $O\left(\sqrt{l}\right)$
  - l **:** $p-1$ **の最大素因子**
- **指数計算法** (Adleman, 1979)
  - $L_x(\alpha,\beta) := \exp\left(\beta(\log x)^{\alpha}(\log\log x)^{1-\alpha}\right)$
  - $O(L_p(1/2, 2+o(1)))$
  - $O(L_p(1/3, 1.903+o(1)))$

指数計算法の実際

Given: $p = 47, a = 40, b = 11$

Find: $\mathrm{Ind}_b a$ i.e. x s.t. $a \equiv b^x \bmod p$

因子基底： $T = \{2, 3, 5, 7, 11, 13\}$

$\#T$ **個の** relation **：**

$$\begin{pmatrix} 11^{42} \\ 11^{3} \\ 11^{29} \\ 11^{11} \\ 11^{31} \\ 11^{1} \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 15 \\ 10 \\ 39 \\ 35 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 3 \times 5 \\ 2 \times 5 \\ 3 \times 13 \\ 5 \times 7 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 11^{\mathrm{Ind}_{11} 2} \\ 11^{\mathrm{Ind}_{11} 3} \times 11^{\mathrm{Ind}_{11} 5} \\ 11^{\mathrm{Ind}_{11} 2} \times 11^{\mathrm{Ind}_{11} 5} \\ 11^{\mathrm{Ind}_{11} 3} \times 11^{\mathrm{Ind}_{11} 13} \\ 11^{\mathrm{Ind}_{11} 5} \times 11^{\mathrm{Ind}_{11} 7} \\ 11^{\mathrm{Ind}_{11} 11} \end{pmatrix} \bmod p$$

$$\begin{pmatrix} 42 \\ 3 \\ 29 \\ 11 \\ 31 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \mathrm{Ind}_{11}2 \\ \mathrm{Ind}_{11}3 \\ \mathrm{Ind}_{11}5 \\ \mathrm{Ind}_{11}7 \\ \mathrm{Ind}_{11}11 \\ \mathrm{Ind}_{11}13 \end{pmatrix} \bmod p-1$$

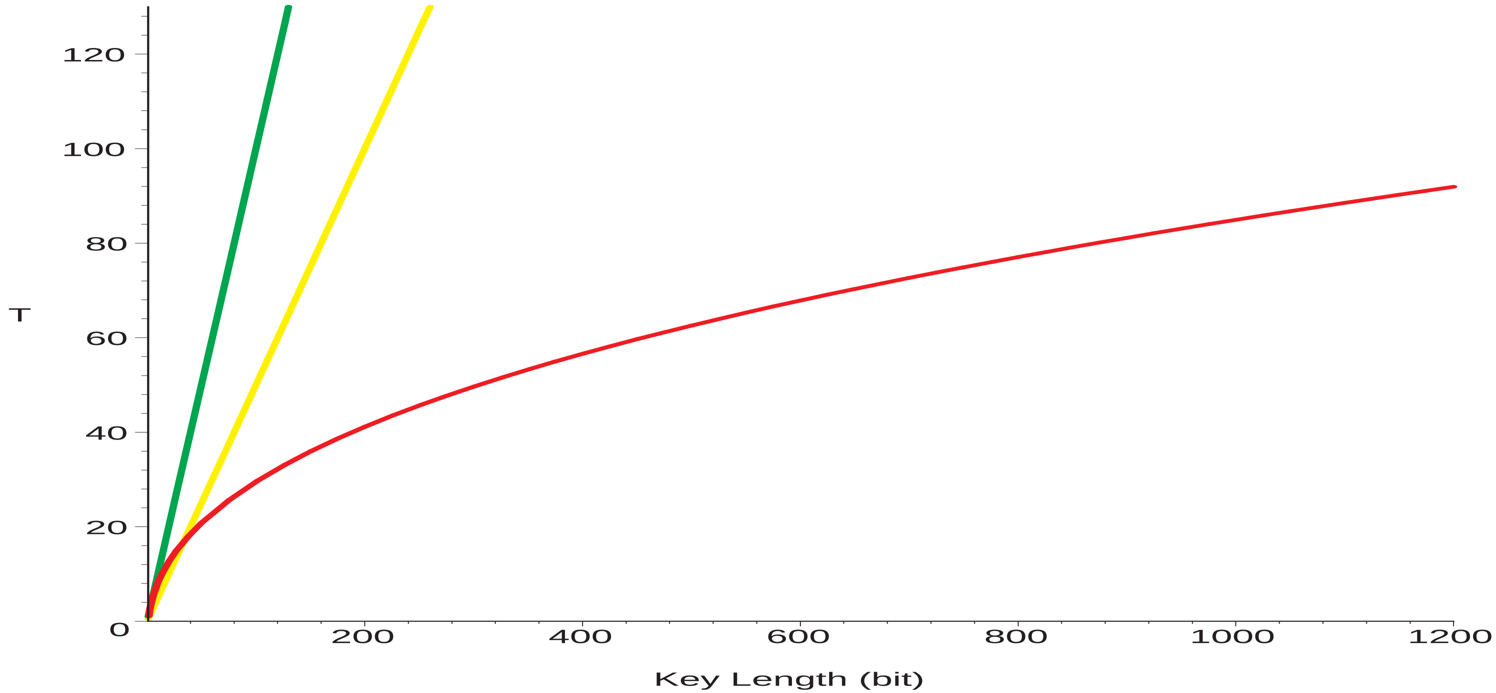
$$\begin{pmatrix} \mathrm{Ind}_{11}2 \\ \mathrm{Ind}_{11}3 \\ \mathrm{Ind}_{11}5 \\ \mathrm{Ind}_{11}7 \\ \mathrm{Ind}_{11}11 \\ \mathrm{Ind}_{11}13 \end{pmatrix} \equiv \begin{pmatrix} 42 \\ 16 \\ 33 \\ 44 \\ 1 \\ 41 \end{pmatrix} \bmod p-1$$

$$\begin{aligned} 40 \times 11^{33} &\equiv 12 \\ &\equiv 2^2 \times 3 \bmod p \end{aligned}$$

$\Rightarrow$

$$
\begin{aligned}
\mathrm{Ind}_{11}40 &\equiv 2\mathrm{Ind}_{11}2 + \mathrm{Ind}_{11}3 - 33 \\
&\equiv 2 \times 42 + 16 - 33 \\
&\equiv 21 \bmod p - 1
\end{aligned}
$$

離散対数問題に必要な計算量



緑：全数探索

黄：Square-root 法

赤：指数計算法的方法

離散対数問題の解読コスト

- 離散対数問題の解読コストはpのサイズに依存
- 2^{80}程度の手間はかけられないと考えられている

$\Rightarrow$ 2^{80}程度の手間が必要なpのサイズは？

- Square-root 法：$\log_2 \mathrm{p} \approx 160$
- 指数計算法　：$\log_2 \mathrm{p} \approx 1024$ (?)

- 将来は？(漸近的計算量)：

  - Square-root 法：$\log_2 \mathrm{p}$の指数関数時間
  - 指数計算法　：$\log_2 \mathrm{p}$の準指数関数時間

何とかならないか？ $\Rightarrow$ 離散対数問題の一般化

有限可換群

- 有限集合で可換な演算が一つ定義され、単位元、逆元有り
  - $+ \Rightarrow \mathbb{F}_p, (\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$
  - $+ \not\Rightarrow (\mathbb{N})$
  - $\times \Rightarrow \mathbb{F}_p \backslash \{0\}, (\mathbb{Q} \backslash \{0\}, \mathbb{R} \backslash \{0\}, \mathbb{C} \backslash \{0\})$
  - $\times \not\Rightarrow (\mathbb{Z})$

- $\mathbb{F}_p^* := \mathbb{F}_p \backslash \{0\}$

- 可換群の演算には$+$を用いる

離散対数問題の一般化

- **離散対数問題**
  - p: **素数**, $b \in \{1, \ldots, p-1\}$, $x \in \{0, \ldots, p-2\}$
  - $a \equiv b^x \bmod p$

$$\Downarrow$$

- **（有限体の乗法群上の）離散対数問題**
  - $b \in \mathbb{F}_p^*$, $x \in \{0, \ldots, \#\mathbb{F}_p^* - 1\}$
  - $a = b^x$

$$\Downarrow$$

- **離散対数問題**
  - G: **有限可換群**, $b \in G$, $x \in \{0, \ldots, \#G - 1\}$
  - $a = [x]b = \underbrace{b + b + \cdots + b}_{x\text{個}}$

楕円・超楕円曲線暗号

- Square-root **法は一般に適用可**: $\sqrt{l}$, l **:** $\#G$ **の最大素因子**

- **有限可換群** G **で指数計算法が適用できないものはあるか？**

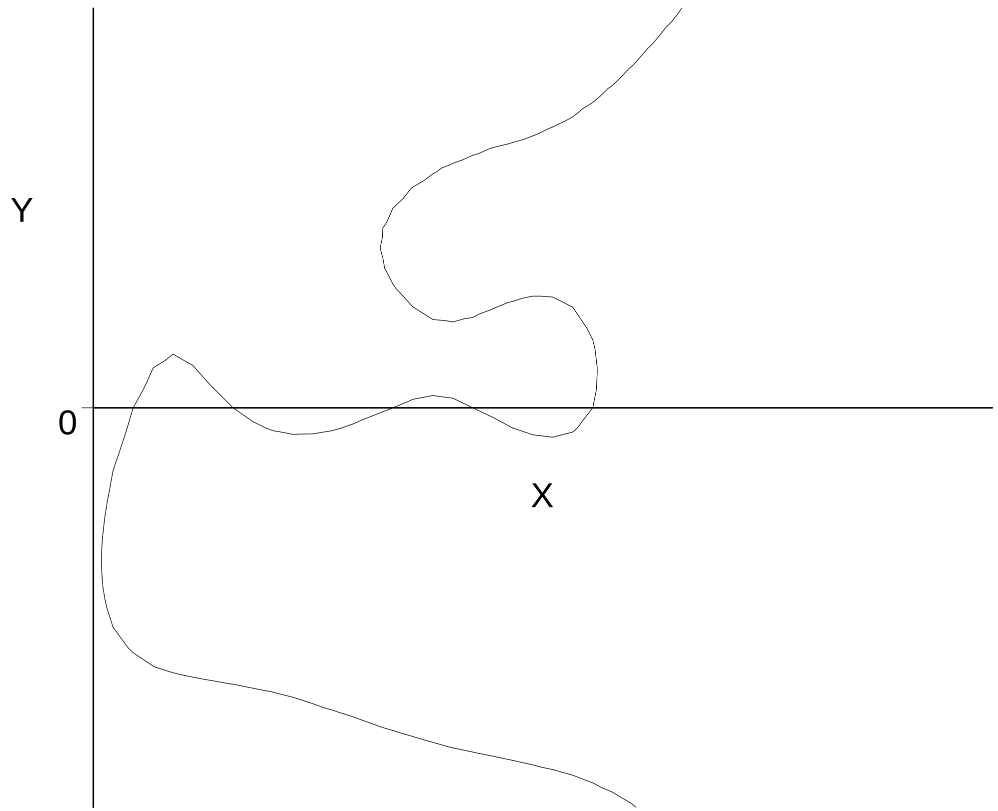
$\Rightarrow$ **代数曲線には可換群の構造を入れられる**

$\Rightarrow$ **楕円・超楕曲線円暗号**
有限体の乗法群上の離散対数問題に基づく暗号アルゴリズムを（有限体上の）楕円曲線、超楕円曲線の群構造を利用して実現したもの

$\therefore$ **暗号アルゴリズム自体の研究は（あまり）行なわれない**

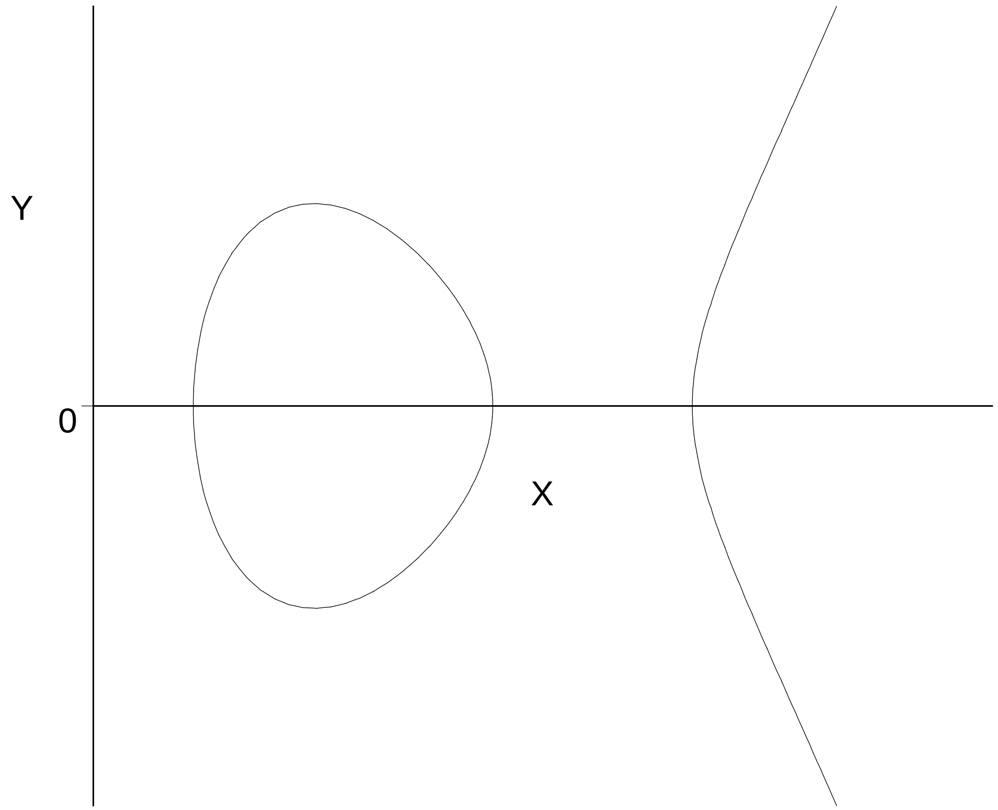
代数曲線の例

$$C : Y^4 + Y - XY^2 - X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X^2 + f_0 = 0,\ f_i \in \mathbb{F}_p$$



楕円曲線

$$E : Y^2 = X^3 + a_4 X + a_6,\ a_i \in \mathbb{F}_p$$



楕円曲線上の群構造

$$E : Y^2 = X^3 + a_4X + a_6,\ a_i \in \mathbb{F}_p$$

$$\downarrow$$

$$E(\mathbb{F}_p) := \{P = (x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + a_4x + a_6\} \cup \{P_\infty\}$$

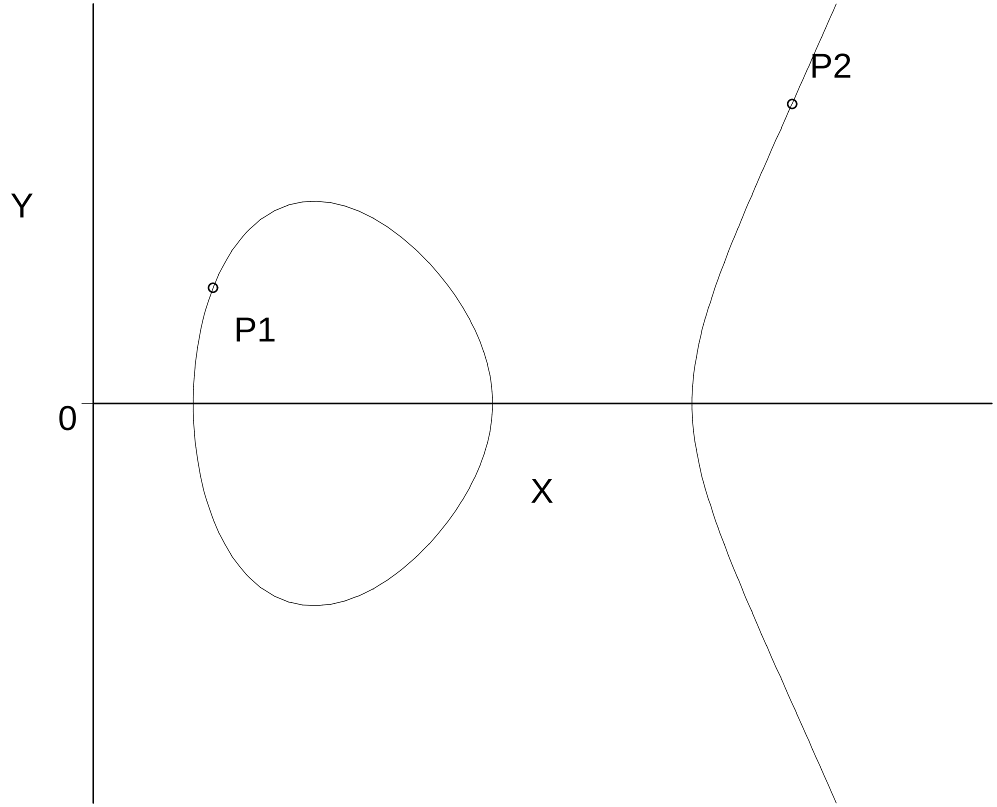
$$\downarrow$$

$E(\mathbb{F}_p)$ **は有限可換群**

$$\#E(\mathbb{F}_p) \approx p$$

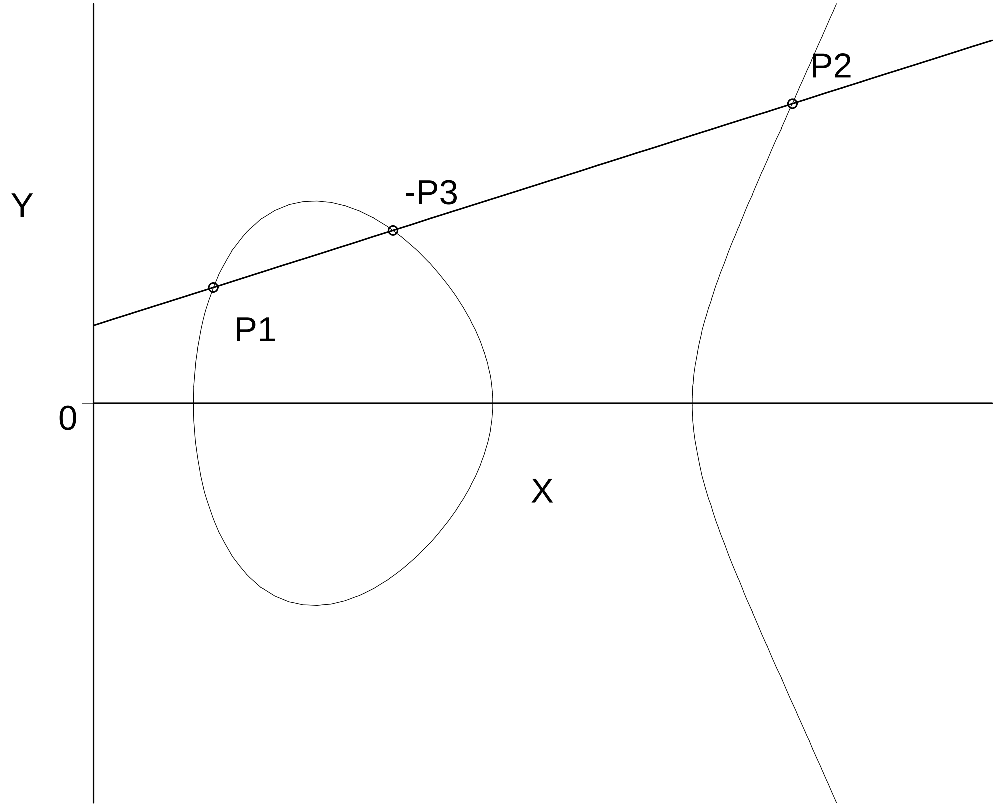
楕円曲線上の加法公式

$$P_3 = P_1 + P_2$$



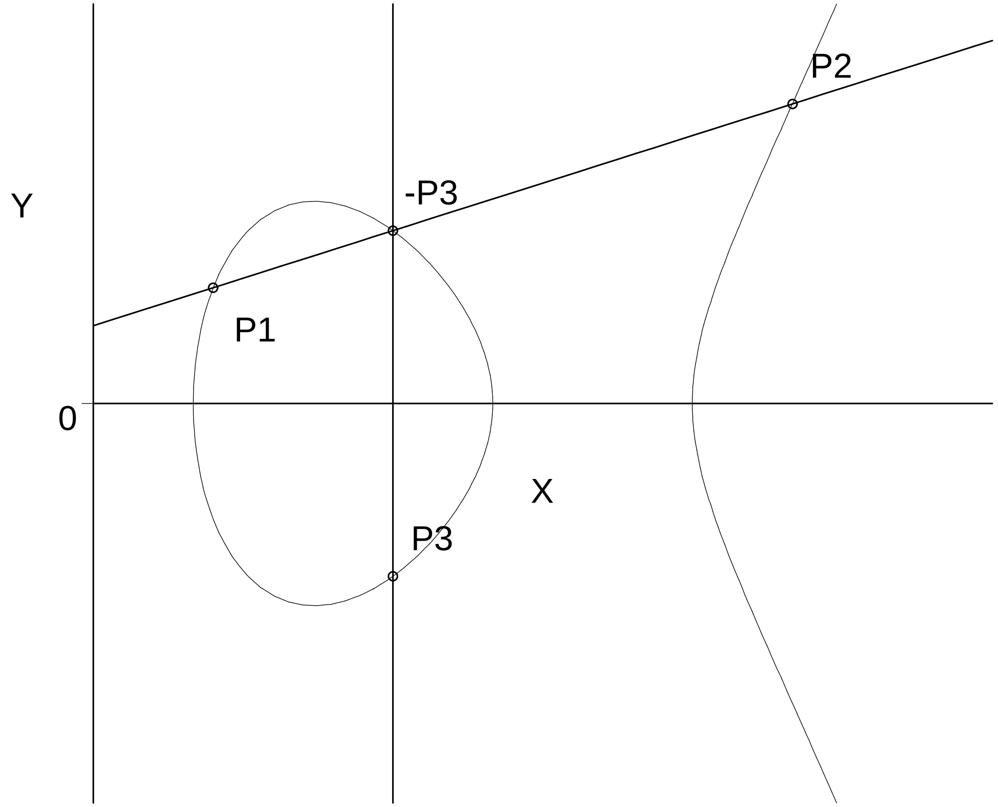
楕円曲線上の加法公式

$$P_3 = P_1 + P_2$$



楕円曲線上の加法公式

$$P_3 = P_1 + P_2$$



楕円曲線上の加法公式

$$E : Y^2 = X^3 + a_4X + a_6$$

$$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2)$$

$$P_3 = (x_3, y_3) = P_1 + P_2$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + a_4}{2x_1} & \text{if } P_1 = P_2 \end{cases}$$

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

逆元計算	乗算
I	3M or 4M

楕円曲線上の加算速度

$\mathbb{F}_p$ 上の演算コスト:

$ab : M = O((\log p)^2)$

$a + b : O(\log p) \ll M$

$a^{-1} : I \approx 20M$

$-a : O(1)$

加算：$I + 3M \approx 23M$

2 倍算：$I + 4M \approx 24M$

解読計算量が同じであるならば、
通常の離散対数問題ベースの暗号のほうが 20 倍以上速いであろう。

逆に、同一の安全性を得るために p のサイズを 1/5 以下にできれば、楕円曲線暗号のほうが速くなりそうだ。

楕円暗号の速度

楕円暗号の安全性

– $\#E(\mathbb{F}_p) = O(p)$

– Square-root **法のみ適用可**
  E **の適切な選択の下**: $O\left(\sqrt{\#E(\mathbb{F}_p)}\right) = O\left(\sqrt{p}\right)$

$\mathbb{F}_p^*$ **に対する指数計算法的方法と** $E(\mathbb{F}_p)$ **に対する** square-root **法の計算量を合わせると：**

$\mathbb{F}_p^*$	$E(\mathbb{F}_p)$	
512	120?	4.3
1024	160?	6.4
2048	220?	9.3

参考：安全な楕円曲線の構成

Algorithm 1 安全な楕円曲線の構成

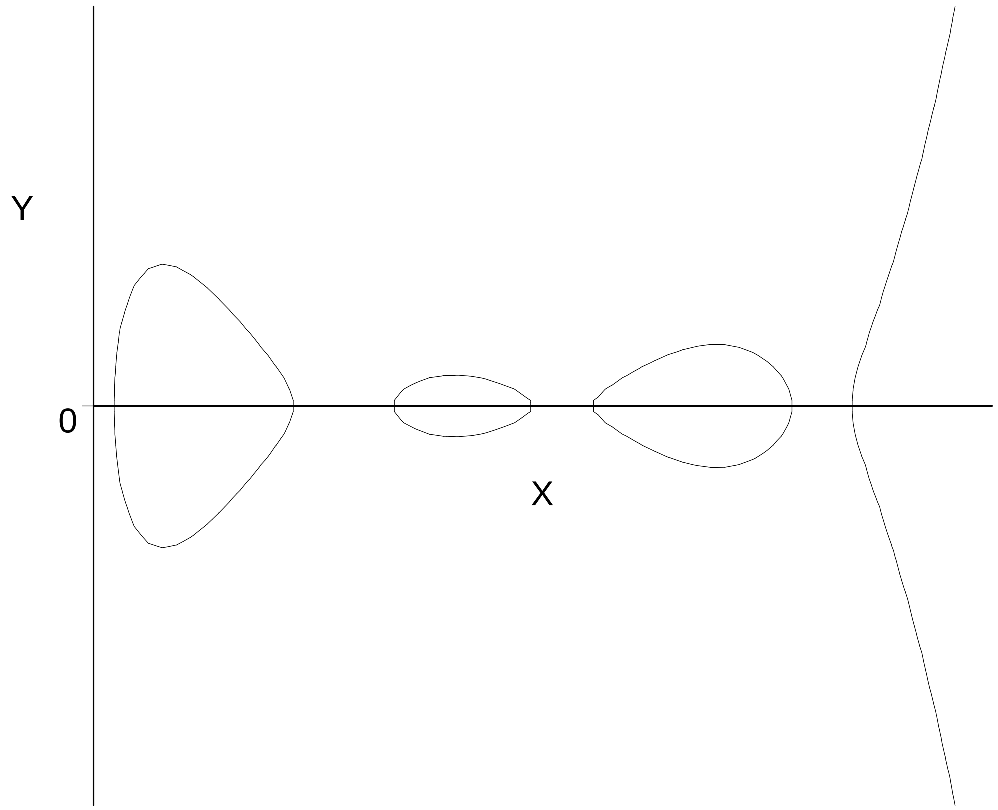
Input: p: 素数

Output: A secure elliptic curve E and $\#E(\mathbb{F}_p)$

```
repeat
    repeat
        Choose an elliptic curve E randmly
        Compute N = #E(F_p) /*ここが楽しい*/
    until N : prime ≠ p
until E satisfies MOV condition
Output E, #E(F_p) and terminate
```

種数 g の超楕円曲線

$$C : Y^2 = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_1X + f_0,\ f_i \in \mathbb{F}_p$$



超楕円曲線上の群構造

$$C : Y^2 = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_1X + f_0,\ f_i \in \mathbb{F}_p$$

$$\downarrow$$

$$C(\mathbb{F}_p) := \{P = (x, y) \in \mathbb{F}_p^2 \mid y^2 = x^{2g+1} + \cdots + f_0\} \cup \{P_\infty\}$$

$$\downarrow$$

$C(\mathbb{F}_p)$ **は群構造を持たない**

超楕円曲線上の群構造

$$C : Y^2 = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_1X + f_0,\ f_i \in \mathbb{F}_p$$

$$\downarrow$$

$$\mathcal{J}_C(\mathbb{F}_p) := \left\{ D = \{P_1, \ldots, P_n \in C(\mathbb{F}_{p^g}) \setminus \{P_\infty\}\} \mid n \leq g, D^p = D \right\}$$

$$C(\mathbb{F}_p) \subseteq \mathcal{J}_C(\mathbb{F}_p)$$

$$\downarrow$$

$\mathcal{J}_C(\mathbb{F}_p)$ は有限可換群

$$\#\mathcal{J}_C(\mathbb{F}_p) \approx p^g$$

Mumford表現

$$C : Y^2 = F(X),\ F \in \mathbb{F}_p[X],\ \deg F = 2g + 1$$

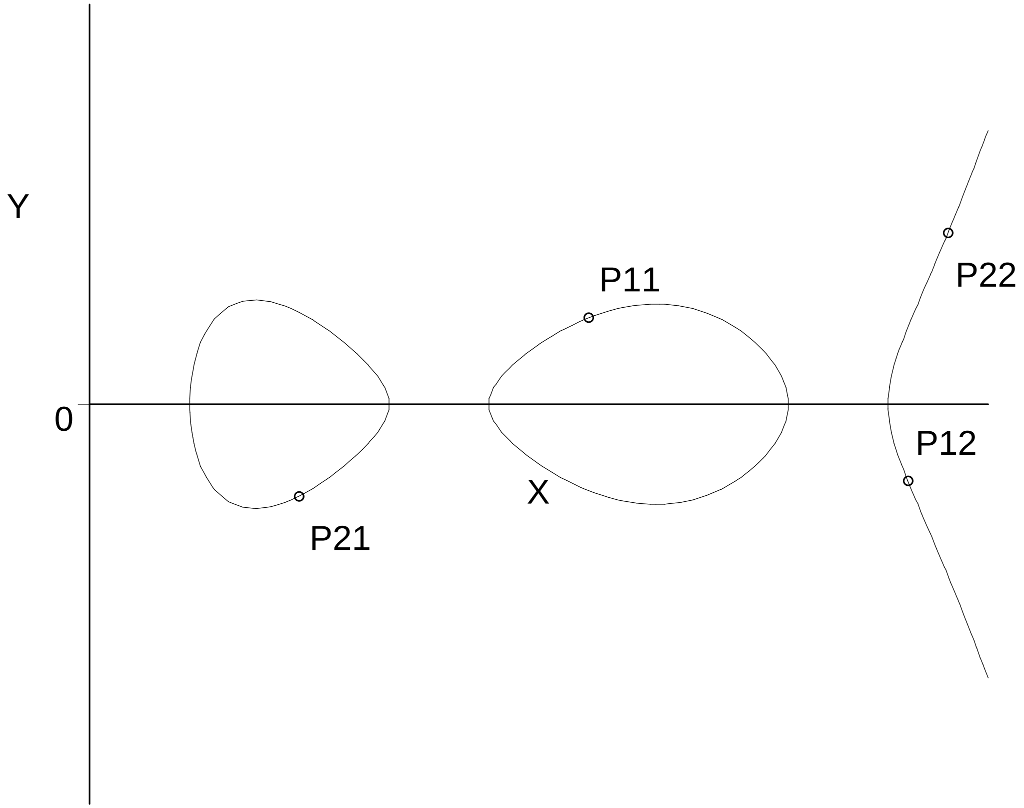
$$D = \{P_1, \ldots, P_n \in C(\mathbb{F}_{p^g}) \setminus \{P_\infty\}\} \mid n \leq g, D^p = D,\ P_i = (x_i, y_i)$$

$$\Downarrow$$

$$^{\exists 1}(U, V) \in (\mathbb{F}_p[X])^2 \text{ s.t. } \begin{aligned} \deg U &> \deg V, \\ U &= \prod_{1 \leq i \leq n} (X - x_i), \\ U &\mid F - V^2, \\ y_i &= V(x_i). \end{aligned}$$

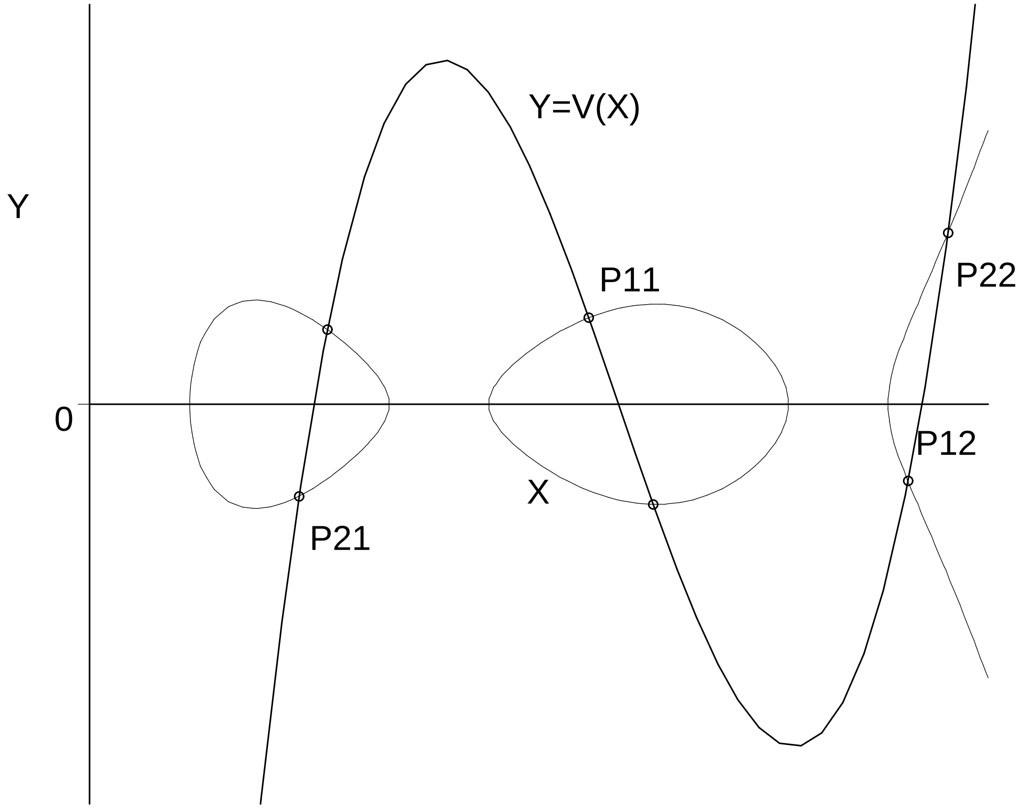
超楕円曲線上の加法公式 ($g = 2$)

$$D_3 = D_1 + D_2,\ D_i = \{P_{i1}, P_{i2}\}$$



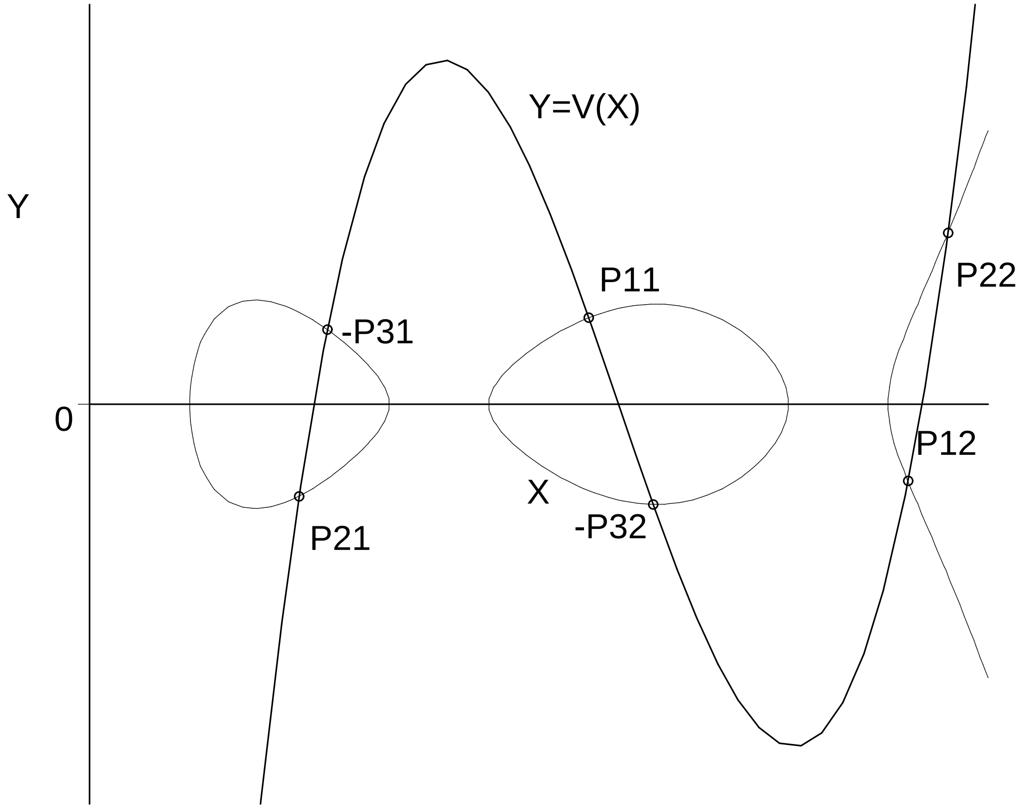
超楕円曲線上の加法公式 ($g = 2$)

$$D_3 = D_1 + D_2,\ D_i = \{P_{i1}, P_{i2}\}$$



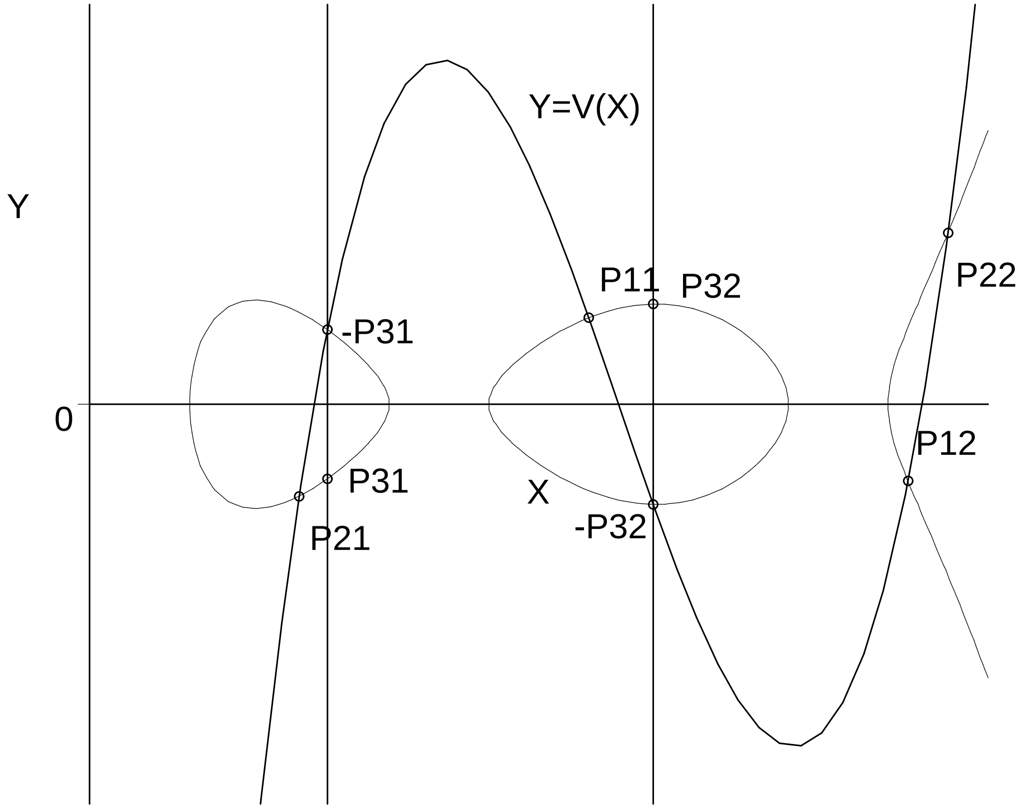
超楕円曲線上の加法公式 ($g = 2$)

$$D_3 = D_1 + D_2,\ D_i = \{P_{i1}, P_{i2}\}$$



超楕円曲線上の加法公式 ($g = 2$)

$$D_3 = D_1 + D_2,\ D_i = \{P_{i1}, P_{i2}\}$$



超楕円曲線上の加法公式 ($g = 2$)

Input	Weight two coprime reduced divisors $D_1 = (U_1, V_1), D_2 = (U_2, V_2)$	
Output	A weight two reduced divisor $D_3 = (U_3, V_3) = D_1 + D_2$	

Step	Procedure	Cost
1	Compute the resultant r of U_1 and U_2. $z_1 \leftarrow u_{21} - u_{11};\ \ z_2 \leftarrow u_{21}z_1;\ \ z_3 \leftarrow z_2 + u_{10} - u_{20};$ $r \leftarrow u_{10}(z_3 - u_{20}) + u_{20}(u_{20} - u_{11}z_1);$	4M
2	If $r = 0$ then call the sub procedure.	—
3	Compute $I_1 \equiv 1/U_1 \bmod U_2$. $w_0 \leftarrow r^{-1};\ \ i_{11} \leftarrow w_1 z_1;\ \ i_{10} \leftarrow w_1 z_3;$	$I + 2M$
4	Compute $S \equiv (V_2 - V_1)I_1 \bmod U_2$. (Karatsuba) $w_1 \leftarrow v_{20} - v_{10};\ \ w_2 \leftarrow v_{21} - v_{11};\ \ w_3 \leftarrow i_{10}w_1;\ \ w_4 \leftarrow i_{11}w_2;$ $s_1 \leftarrow (i_{10} + i_{11})(w_1 + w_2) - w_3 - w_4(1 + u_{21});$ $s_0 \leftarrow w_3 - u_{20}w_4;$	5M
5	If $s_1 = 0$ then call the sub procedure.	—
6	Compute $U_3 = s_1^{-2}((S^2U_1 + 2SV_1)/U_2 - (F - V_1^2)/(U_1U_2))$. $w_1 \leftarrow s_1^{-1};$ $u_{30} \leftarrow w_1(w_1(s_0^2 + u_{11} + u_{21} - f_4) + 2(v_{11} - s_0w_2)) + z_2 + u_{10} - u_{20};$ $u_{31} \leftarrow w_1(2s_0 - w_1) - w_2;$ $u_{32} \leftarrow 1;$	$I + 6M$
7	Compute $V_3 \equiv -(SU_1 + V_1) \bmod U_3$.(Karatsuba) $w_1 \leftarrow u_{30} - u_{10};\ \ w_2 \leftarrow u_{31} - u_{11};$ $w_3 \leftarrow s_1w_2;\ \ w_4 \leftarrow s_0w_1;\ \ w_5 \leftarrow (s_1 + s_0)(w_1 + w_2) - w_3 - w_4$ $v_{30} \leftarrow w_4 - w_3u_{30} - v_{10};$ $v_{31} \leftarrow w_5 - w_3u_{31} - v_{11};$	5M
Total		$2I + 21M$

超楕円曲線上の加法公式 $(g = 3)$

In.	Genus 3 HEC C : $Y^2 = F(X)$, $F = X^7 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0$; Reduced divisors $D_1 = (U_1, V_1)$ and $D_2 = (U_2, V_2)$, $U_1 = X^3 + u_{12}X^2 + u_{11}X + u_{10}$, $V_1 = v_{12}X^2 + v_{11}X + v_{10}$, $U_2 = X^3 + u_{22}X^2 + u_{21}X + u_{20}$, $V_2 = v_{22}X^2 + v_{21}X + v_{20}$;	
Out.	Reduced divisor $D_3 = (U_3, V_3) = D_1 + D_2$, $U_3 = X^3 + u_{32}X^2 + u_{31}X + u_{30}$, $V_3 = v_{32}X^2 + v_{31}X + v_{30}$;	

Step	Procedure	Cost
1	**Compute the resultant r of U_1 and U_2** $t_1 = u_{11}u_{20} - u_{10}u_{21}$; $t_2 = u_{12}u_{20} - u_{10}u_{22}$; $t_3 = u_{20} - u_{10}$; $t_4 = u_{21} - u_{11}$; $t_5 = u_{22} - u_{12}$; $t_6 = t_4^2$; $t_7 = t_3t_4$; $t_8 = u_{12}u_{21} - u_{11}u_{22} + t_3$; $t_9 = t_3^2 - t_1t_5$; $t_{10} = t_2t_5 - t_7$; $r = t_8t_9 + t_2(t_{10} - t_7) + t_1t_6$;	$14M + 12A$
2	**If $r = 0$ then call the Cantor algorithm**	–
3	**Compute the pseudo-inverse $I = i_2X^2 + i_1X + i_0 \equiv r/U_1 \bmod U_2$** $i_2 = t_5t_8 - t_6$; $i_1 = u_{22}i_2 - t_{10}$; $i_0 = u_{21}i_2 - (u_{22}t_{10} + t_9)$;	$4M + 4A$
4	**Compute $S' = s'_2X^2 + s'_1X + s'_0 = rS \equiv (V_2 - V_1)I \bmod U_2$ (Karatsuba, Toom)** $t_1 = v_{10} - v_{20}$; $t_2 = v_{11} - v_{21}$; $t_3 = v_{12} - v_{22}$; $t_4 = t_2i_1$; $t_5 = t_1i_0$; $t_6 = t_3i_2$; $t_7 = u_{22}t_6$; $t_8 = t_4 + t_6 + t_7 - (t_2 + t_3)(i_1 + i_2)$; $t_9 = u_{20} + u_{22}$; $t_{10} = (t_9 + u_{21})(t_8 - t_6)$; $t_9 = (t_9 - u_{21})(t_8 + t_6)$; $s'_0 = -(u_{20}t_8 + t_5)$; $s'_2 = t_6 - (s'_0 + t_4 + (t_1 + t_3)(i_0 + i_2) + (t_{10} + t_9)/2)$; $s'_1 = t_4 + t_5 + (t_9 - t_{10})/2 - (t_7 + (t_1 + t_2)(i_0 + i_1))$;	$10M + 31A$
5	**If $s'_2 = 0$ then call the Cantor algorithm**	–
6	**Compute S, w and $w_i = 1/w$ s.t. $wS = S'/r$ and S is monic** $t_1 = (rs'_2)^{-1}$; $t_2 = rt_1$; $w = t_1s'^2_2$; $w_i = rt_2$; $s_0 = t_2s'_0$; $s_1 = t_2s'_1$;	$I + 7M$
7	**Compute $Z = X^5 + z_4X^4 + z_3X^3 + z_2X^2 + z_1X + z_0 = SU_1$ (Toom)** $t_6 = s_0 + s_1$; $t_1 = u_{10} + u_{12}$; $t_2 = t_6(t_1 + u_{11})$; $t_3 = (t_1 - u_{11})(s_0 - s_1)$; $t_4 = u_{12}s_1$; $z_0 = u_{10}s_0$; $z_1 = (t_2 - t_3)/2 - t_4$; $z_2 = (t_2 + t_3)/2 - z_0 + u_{10}$; $z_3 = u_{11} + s_0 + t_4$; $z_4 = u_{12} + s_1$;	$4M + 15A$
8	**Compute $U_t = X^4 + u_{t3}X^3 + u_{t2}X^2 + u_{t1}X + u_{t0} =$ $(S(Z + 2w_iV_1) - w_i^2((F - V_1^2)/U_1))/U_2$ (Karatsuba)** $t_1 = s_0z_3$; $t_2 = (u_{22} + u_{21})(u_{t3} + u_{t2})$; $t_3 = u_{21}u_{t2}$; $t_4 = t_1 - t_3$; $u_{t3} = z_4 + s_1 - u_{22}$; $t_5 = s_1z_4 - u_{22}u_{t3}$; $u_{t2} = z_3 + s_0 + t_5 - u_{21}$; $u_{t1} = z_2 + t_6(z_4 + z_3) + w_i(2v_{12} - w_i) - (t_5 + t_2 + t_4 + u_{20})$; $u_{t0} = z_1 + t_4 + s_1z_2 + w_i(2(v_{11} + s_1v_{12}) + w_iu_{12}) - (u_{22}u_{t1} + u_{20}u_{t3})$;	$13M + 26A$
9	**Compute $V_t = v_{t2}X^2 + v_{t1}X + v_{t0} \equiv wZ + V_1 \bmod U_t$** $t_1 = u_{t3} - z_4$; $v_{t0} = w(t_1u_{t0} + z_0) + v_{10}$; $v_{t1} = w(t_1u_{t1} + z_1 - u_{t0}) + v_{11}$; $v_{t2} = w(t_1u_{t2} + z_2 - u_{t1}) + v_{12}$; $v_{t3} = w(t_1u_{t3} + z_3 - u_{t2})$;	$8M + 11A$
10	**Compute $U_3 = X^3 + u_{32}X^2 + u_{31}X + u_{30} = (F - V_t^2)/U_t$** $t_1 = 2v_{t3}$; $u_{32} = -(u_{t3} + v_{t3}^2)$; $u_{31} = f_5 - (u_{t2} + u_{32}u_{t3} + t_1v_{t2})$; $u_{30} = f_4 - (u_{t1} + v_{t2}^2 + u_{32}u_{t2} + u_{31}u_{t3} + t_1v_{t1})$;	$7M + 11A$
11	**Compute $V_3 = v_{32}X^2 + v_{31}X + v_{30} \equiv V_t \bmod U_3$** $v_{32} = v_{t2} - u_{32}v_{t3}$; $v_{31} = v_{t1} - u_{31}v_{t3}$; $v_{30} = v_{t0} - u_{30}v_{t3}$;	$3M + 3A$
Total		$I + 70M + 113A$

超楕円暗号の速度

- 群演算一回あたりのコスト
  - $g = 1$：$I + 3M = 23M$ if $I = 20M$
  - $g = 2$：$I + 25M = 45M$ if $I = 20M$
  - $g = 3$：$I + 70M = 90M$ if $I = 20M$

- 超楕円暗号の安全性
  - $\#E(\mathbb{F}_p) = O(p) \to \#\mathcal{J}_C(\mathbb{F}_p) = O(p^g)$
  - Square-root 法のみ適用可 (?)
    C の適切な選択の下: $O\left(\sqrt{\#\mathcal{J}_C(\mathbb{F}_p)}\right)$

超楕円暗号の速度

- 解読に2^{80}程度の手間がかかる$p = 2^{160/g}$
  - $g = 1$：$p \approx 2^{160}$
  - $g = 2$：$p \approx 2^{80}$
  - $g = 3$：$p \approx 2^{54}$

- 群演算一回あたりのコスト
  - $g = 1$：$I_{160} + \ 3M_{160} = 23M_{160}$
  - $g = 2$：$I_{80} + 25M_{80} = 45M_{80}$
  - $g = 3$：$I_{54} + 70M_{54} = 90M_{54}$

$\Rightarrow 23M_{160} > 45M_{80} > 90M_{54}$???

超楕円曲線上の離散対数問題に対する指数計算法

- Adleman-DeMarrais-Huang (1991)
  - **因子基底：素数** $< s \to u$ **の既約因子の** $\deg < s$
  - **計算量**: $O(L_{p^{2g+1}}(1/2, c < 2.181))$; $\log p < (2g+1)^{0.98}$, $g \to \infty$
  - **改良の計算量**: $O(L_{p^g}(1/2, *)$; $p^g \to \infty$
    Enge, Gaudry-Enge

  $\Rightarrow$ **種数の大きな曲線は暗号利用不可**

- Gaudry (1997)
  - **因子基底：**u **の既約因子の** $\deg = 1$
  - **計算量**: $O(p^2)$
  - **改良の計算量**: $O(p^{2-2/g})$
    Gaudry-Harley, Thériault, **Nagao**, **Gaudry-Thomé-Thériault-Diem**

Gaudryの指数計算法（簡易版）

$p = 7$

$$
\begin{aligned}
C : Y^2 &= X^{13} + 5X^{12} + 4X^{11} + 6X^9 + 2X^8 + 6X^7 + 5X^4 + 5X^3 \\
&\quad + X^2 + 2X + 6
\end{aligned}
$$

$\#\mathcal{J}_C(\mathbb{F}_p) = 208697$: 18 bit **素数** ($7^6 = 117649$)

$D_a = (X^6 + 2X^5 + 4X^4 + X^3 + 5X^2 + 3, 4X^5 + 5X^3 + 2X^2 + 5X + 4)$
$D_b = (X^5 + 6X^3 + 3X^2 + 1, 3X^4 + X^3 + 4X^2 + X + 3)$

Find $\mathrm{Ind}_{D_b} D_a$ s.t. $D_a = [\mathrm{Ind}_{D_b} D_a] D_b$.

$$C(\mathbb{F}_p) = \{P_\infty, (1,1), (1,6), (2,1), (2,6), (4,1), (4,6)(5,3), (5,4), (6,3), (6,4)\}$$

$$\#C(\mathbb{F}_p) = 11$$

因子基底： $T = \{(1,1), (2,1), (4,1), (5,3), (6,3)\}$

$$[9343]D_b = (X^5 + 6X^4 + 6X^3 + 5X^2 + 6X + 4, X^4 + X^3 + X^2 + 4X + 6)$$

$$X^5 + 6X^4 + 6X^3 + 5X^2 + 6X + 4 = (X-1)^2(X-4)^2(X-5)$$

$$X^4 + X^3 + X^2 + 4X + 6 \mid_{X=1} = 6$$
$$X^4 + X^3 + X^2 + 4X + 6 \mid_{X=4} = 1$$
$$X^4 + X^3 + X^2 + 4X + 6 \mid_{X=5} = 3$$

$\Rightarrow$

$$[9343]D_b = -[2](1,1) + [2](4,1) + (5,3)$$

$$\begin{pmatrix} [9343]D_b \\ [120243]D_b \\ [121571]D_b \\ [120688]D_b \\ [151649]D_b \end{pmatrix} = \begin{pmatrix} -2 & 0 & 2 & 1 & 0 \\ 0 & -2 & 1 & 1 & -2 \\ -1 & 0 & 2 & -1 & -1 \\ 2 & 1 & 0 & 2 & 0 \\ 1 & 0 & 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} (1,1) \\ (2,1) \\ (4,1) \\ (5,3) \\ (6,3) \end{pmatrix}$$

$$\begin{aligned} \begin{pmatrix} \mathrm{Ind}_{D_b}(1,1) \\ \mathrm{Ind}_{D_b}(2,1) \\ \mathrm{Ind}_{D_b}(4,1) \\ \mathrm{Ind}_{D_b}(5,3) \\ \mathrm{Ind}_{D_b}(6,3) \end{pmatrix} &\equiv \begin{pmatrix} 160536 & 88295 & 13378 & 176590 & 189968 \\ 160536 & 192643 & 117727 & 176590 & 85619 \\ 176590 & 128429 & 101673 & 48161 & 149834 \\ 176590 & 128429 & 32107 & 48161 & 80268 \\ 16054 & 40134 & 157860 & 80268 & 29432 \end{pmatrix} \begin{pmatrix} 9343 \\ 120243 \\ 121571 \\ 120688 \\ 151649 \end{pmatrix} \\ &\equiv \begin{pmatrix} 85159 \\ 114347 \\ 182999 \\ 22360 \\ 136908 \end{pmatrix} \bmod \#\mathcal{J}_C(\mathbb{F}_p) \end{aligned}$$

$$D_a + [105454]D_b = (1,1) + [2](2,1) + (4,1) - (6,3)$$

$$\begin{aligned} D_a + [105454]D_b &= (1,1) + [2](2,1) + (4,1) - (6,3) \\ \mathrm{Ind}_{D_b} D_a &\equiv \mathrm{Ind}_{D_b}(1,1) + 2\mathrm{Ind}_{D_b}(2,1) + \mathrm{Ind}_{D_b}(4,1) - \mathrm{Ind}_{D_b}(6,3) \\ &\quad -105454 \\ &\equiv 85159 + 2 \times 114347 + 182999 - 136908 - 105454 \\ &\equiv 45793 \bmod \#\mathcal{J}_C(\mathbb{F}_p) \end{aligned}$$

超楕円暗号の安全性

- 準指数時間計算量ではなく指数時間計算量
- gにより効果が異なる