



Title	2005年度 情報理論講義ノート
Author(s)	井上, 純一
Issue Date	2005-11-18T09:19:52Z
Doc URL	http://hdl.handle.net/2115/772
Rights(URL)	http://creativecommons.org/licenses/by-nc-sa/2.1/jp/
Type	learningobject
Note(URL)	http://www005.upp.so-net.ne.jp/j_inoue/index.html ; http://chaosweb.complex.eng.hokudai.ac.jp/~j_inoue/
Additional Information	There are other files related to this item in HUSCAP. Check the above URL.
File Information	InfoTheory05_slide13.pdf (第13回講義スライド)



[Instructions for use](#)



情報理論 #13 (最終回)

第13回講義 7月25日

情報科学研究科 井上純一

http://chaosweb.complex.eng.hokudai.ac.jp/~j_inoue/



ガロア体

集合Fが体をなす条件

- (1) 集合 F 上に加法・乗法が定義されている
- (2) 集合 F に単位元が存在する（加法の単位元を0, 乗法の単位元を1)
- (3) 集合 F の任意の要素 a に対して、 $a + b = 0$ を満たす加法の逆元 $b = -a$, $a \cdot c = 1$ を満たす乗法の逆元 $c = a^{-1}$ が存在する

有限個の要素からなる体 : **ガロア体**

$GF(p)$

集合の要素数 : 位数

例)

$F = \{0, 1\}$ とし、2を法とする加算を加法としたものが $GF(2)$



フェルマーの小定理

$GF(p)$ の 0 以外の要素を $Z_p^* = \{1, 2, \dots, p-1\}$ とする

Z_p^* の異なる要素 b, c に対して

$ba = ca \pmod{p}$ となる $a \in Z_p^*$ は存在しない。

(証明は両辺から a^{-1} をかけて見よ)

$\Rightarrow Z_p^*$ の各要素に a をかけたものは全て異なり、 Z_p^* はこれで尽くされる。

また、次の関係式が成り立つ

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdots (p-1) &= a \cdot (2a) \cdot (3a) \cdots (p-1)a \pmod{p} \\ &= a^{p-1} \{1 \cdot 2 \cdot 3 \cdots (p-1)\} \pmod{p} \end{aligned}$$

任意の素数を p とする。 p の倍数でない任意の整数 a に対して

$$a^{p-1} = 1 \pmod{p}$$

が成り立つ。

フェルマーの小定理 (例)

フェルマーの小定理を $p=7$ の場合に確かめてみる

$a^j \pmod{p}$ を計算する

$a \backslash j$	1	2	3	4	5	6
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

確かに
 $a^{7-1} = a^6 = 1 \pmod{7}$
を満たしている

$j = p - 1 = 7 - 1 = 6$
で初めて $a^j = 1 \pmod{p}$ となっている

a は $GF(p)$ の原始元であるという

離散対数問題と一方向性関数

$$s = \log_a v \pmod{p}$$

をGF(p)上のaを底とする離散対数と呼ぶ

$$a^s = v \pmod{p}$$

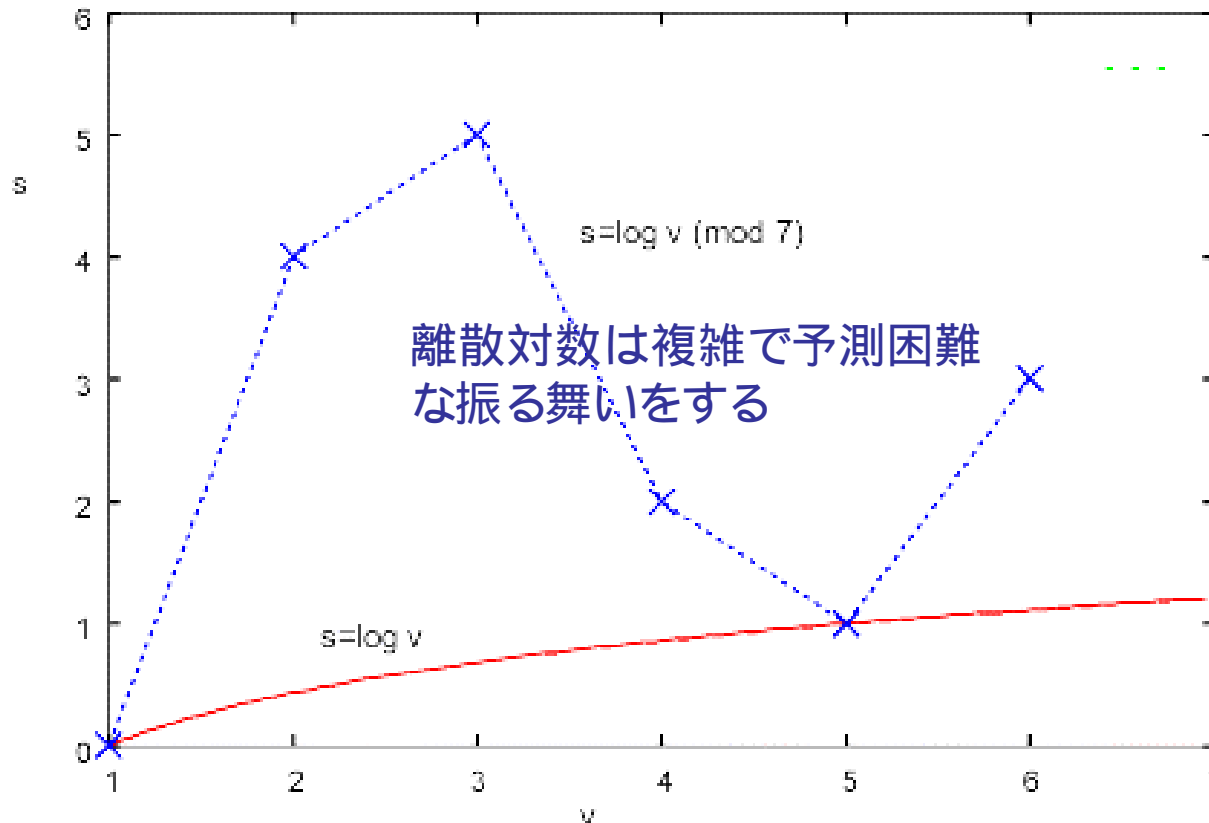
が解sを満たすことを「確認すること」は容易であるが、解sを見つけることは多くの場合にとても難しい

離散対数問題

$$f(x) = a^x \pmod{p} \quad \text{容易}$$

$$f^{-1}(x) = \log_a x \pmod{p} \quad \text{難しい}$$

f(x)は一方向性関数と呼ばれる



公開鍵暗号：エルガマル暗号

古典暗号：秘密鍵を用いて通信内容が他人に漏れないようにする暗号

公開鍵暗号：公開鍵を利用する暗号

離散対数問題の困難性をその安全性の根拠に置く

$$b = a^a \pmod{p}$$

$$b_1 = a_1^{a_1} \pmod{p_1}$$

エルガマル (ElGamal) 暗号系

ユーザ	アリス	ボブ
秘密鍵	a	a_1
公開鍵	p, a, b	p_1, a_1, b_1

を満たすとする

エルガマル暗号の暗号化

エルマガル暗号の暗号手続き

- (1) 適当な乱数で整数を作り、それを k とする
- (2) 送信相手の公開鍵: p, a, b に対し、平文 x を $1 \leq x \leq p-1$ として

$$c_1 = a^k \pmod{p}$$

$$c_2 = x b^k \pmod{p}$$

- (3) 暗号文 $c = (c_1, c_2)$ を送信する

この暗号文からは乱数 k 、平文 x に関して何もわからないことに注意
(外からは既に見えなくなっている)



エルガマル暗号の復号化

エルマガル暗号の復号化手続き

(1) 受信文を $c = (c_1, c_2)$ とする

(2) 秘密鍵 a を用いて

$$(c_1^a)^{-1} \cdot c_2 \pmod{p}$$

を計算すると、平文 x が得られる

(確認)

$$(c_1^a)^{-1} \cdot c_2 = \left((a^k)^a \right)^{-1} \cdot x b^k \pmod{p}$$

$$= (a^{ak})^{-1} \cdot x \cdot a^{ak} \pmod{p}$$

$$= x \pmod{p}$$

秘密鍵 a を知らずに復号することは離散対数問題を解くことに相当し、非常に難しいことになる