情報理論 配布資料 #13：最終回

担当：井上 純一 (情報科学研究科棟 8-13)
URL：http://chaosweb.complex.eng.hokudai.ac.jp/~j_inoue/

平成 17 年 7 月 25 日

目 次

演習問題 12 の解答例

標本化定理より, $k = 0, \pm 1, \pm 2, \cdots$ として各標本点 $k/2W$ を 10 ビットのデータに変換する. 標本化間隔は $(k+1)/2W - k/2W = 1/2W$ であるので, $T[s]$ 間の信号では $T/(1/2W) = 2TW$ の標本点が存在する. 従って, 合計では $10 \times 2TW = 20TW$ ビットのデジタル・データが得られることになる.

11 暗号

この講義の最終回では, 現在インターネットのセキュリティ確保に欠かせない技術になっている公開鍵暗号について, その入門的な基礎事項を学ぶことにする.

11.1 ガロア体

集合 F が次の条件 (1)-(3) を満たすとき, F は加法・乗法に関して**体をなす**と言う.

(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.

このとき, 有限個の要素からなる体を**ガロア体**と呼び, 集合 F の要素数 (位数) を p とすれば, 位数 p のガロア体を $GF(p)$ と記すことに約束する.

従って, $F=\{0,1\}$ とし, 2 を法とする加算を加法として採用したものが $GF(2)$ であり, この講義ではもっぱらこの $GF(2)$ を扱ってきたわけである.

11.2 フェルマーの小定理

$GF(p)$ の 0 以外の要素を $Z_p^*=\{1,2,\cdots,p-1\}$ とすると, この Z_p^* の任意の異なる 2 つの要素を b,c とすると, $ba=ca \pmod p$ となる $a\in Z_p^*$ は存在しない.

(証明):

a は Z_p^* の要素であるから, 乗法に関する逆元 a^{-1} が存在することになるが, これを $ba=ca \pmod p$ の両辺にかけると $b=c \pmod p$ となり, b と c が Z_p^* の異なる要素であることに反する. **(証明終わり)**.

従って, Z_p^* の各要素に a をかけたものは全て異なることになり, かつ, Z_p^* はそれらで尽くされる. また, それらの積は等しいので次の関係式が成り立つ.

$$\begin{aligned} 1\cdot 2\cdot 3\cdots(p-1) &= a\cdot(2a)\cdot(3a)\cdots(p-1)a \pmod p \\ &= a^{p-1}\{1\cdot 2\cdot 3\cdots(p-1)\} \pmod p \end{aligned} \tag{448}$$

よって, $a^{p-1}=1 \pmod p$ となる. この結果より, 次の**フェルマーの小定理**が成り立つ.

フェルマーの小定理

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.

これに関して例を見ておこう.

$p=7$ に対して, $a=1,2,\cdots,6,$ として $a^j \pmod 7$ を計算して表にしてみると

a/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

となり, 確かに $a^{7-1}=a^6=1 \pmod 7$ を満たしている. また, この例のように, $j=p-1$ で初めて $a^j=1 \pmod p$ となる場合, $j=0,1,\cdots,p-2$ に対して a^j が Z_p^* を尽くす. このような a を $GF(p)$ の**原始元**と呼び, 上の例では $a=3,5$ が $GF(7)$ の原始元ということになる.

11.3 離散対数問題

今見たように, 素数 p を位数とするガロア体は, その原始元を a として

$$GF(p) = \{0,1,2,\cdots,p-1\}=\{0,1,a,a^2,\cdots,a^{p-2}\} \tag{449}$$

として構成される．つまり，$1 \leq v \leq p-1$ の範囲内にある任意の整数 v に対し，$a^s = v \pmod p$ を満たす s が $0 \leq s \leq p-2$ に一つだけ存在する．このとき

$$s \quad = \quad \log_a v \pmod p \tag{450}$$

を $GF(p)$ 上の a を底とする**離散対数**と呼ぶ．次の例を見てみよう．

j	0	1	2	3	4	5	6
$5^j \pmod 7$	1	5	4	6	2	3	1

この表から，$5 = \log_5 3 \pmod 7$ であることがわかり，5 が $5^j = 3 \pmod 7$ を満たす j，すなわち離散対数ということになる．ところで，この離散対数 $s = \log_5 v$ をプロットしてみると図 33 のようになるが，これ

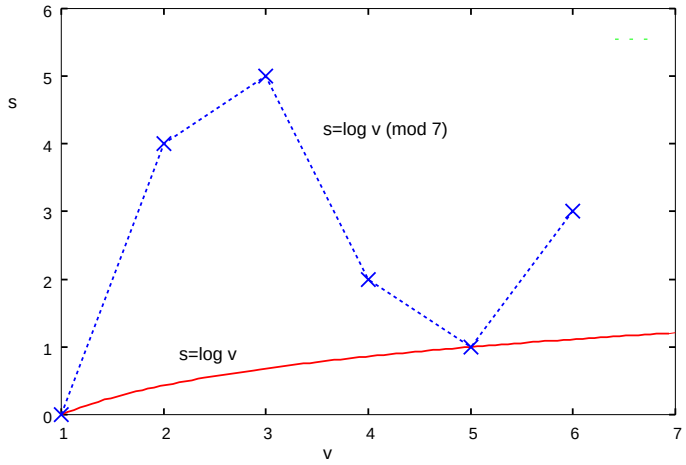

図 33: 離散対数 $s = \log_a v \pmod 7$ と底を $a = 5$ と選んだ場合の対数関数 $s = \log_5 v$．離散対数の挙動は不規則である．

は通常の対数 $y = \log_a x$ と比べて**複雑で予測困難**な振る舞いを示すことがわかる．

また，$a^s = v \pmod p$ を満たす s を求めるのは極めて困難であることに注意すべきである．例えば，$3^x = 38 \pmod{41}$ を満たす x の値は $x = 35$ であるが，これを「確認する」には，$3 \times 3 = 3^2, 3^2 \times 3^2 \times 3 = 3^5, 3^5 \times 3^5 = 3^{25}, 3^{25} \times 3^5 \times 3^5 = 3^{35}$ のように，4 回の計算で済むのに対し，$3^x = 38 \pmod{41}$ を満たす x を「探す」($x = \log_3 38 \pmod{41}$ を計算することに相当する) には $3^1, 3^2, \cdots 3^{35}$ のように順番に探していくと 35 回目にたどり着く．これは $x = \log_3 38 \pmod{41}$ を計算することに相当するが，この計算は上に述べた離散対数の挙動の予測困難性とあいまって一般的に難しい．このような問題を**離散対数問題**と呼ぶ．

11.4　一方向性関数

$f(x) = a^x \pmod p$ と関数 $f(x)$ を定義すると，その逆写像 $f^{-1}(x)$ も定義できて，$f^{-1}(x) = \log_a x \pmod p$ と書ける．$3^x = 38 \pmod{41}$ を満たす x を見つける例で見たように，$f(x)$ を計算するのは容易だが，$f^{-1}(x)$ を計算するのは難しい．このとき，関数 $f(x)$ は**一方向性関数**と呼ばれる．

11.5　公開鍵暗号

ネットワーク上の特定ユーザに対し, **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を**古典暗号**と呼んでいるが, これに対して, **公開鍵**を利用する**公開鍵暗号**が現在広く用いられており, これは今学んだ離散対数問題の困難性をその安全性の根拠に置いている. そこで, この公開鍵暗号の一つであるエルガマル (ElGamal) 暗号を見ていくことにしょう.

11.6　エルガマル暗号系

ネットワークのユーザ：アリスとボブは次の表に与えられた秘密鍵と公開鍵を有しているものとする.

ユーザ	**アリス**	**ボブ**
秘密鍵	a	a_1
公開鍵	p, α, β	p_1, α_1, β_1

ここで, $\beta = \alpha^a \pmod p, \beta_1 = \alpha_1^{a_1} \pmod{p_1}$ が満たされていることに注意しょう.

このとき, 暗号化は次の手続きに従って行われる.

暗号化

(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, α, β に対し, 平文 (もともとの通信文) x を $1 \leq x \leq p-1$ なる整数として

$$c_1 = \alpha^k \pmod p \tag{451}$$
$$c_2 = x\beta^k \pmod p \tag{452}$$

を計算する.
(3) 暗号文 $c = (c_1, c_2)$ を送信する.

暗号文を受信したアリスは自分のみ知る秘密鍵 a を用いて次の手続きに従って平文を復号化する.

復号化

(1) 受信文を $c = (c_1, c_2)$ とする.
(2) 秘密鍵 a を用いて

$$(c_1^a)^{-1} \cdot c_2 \pmod p \tag{453}$$

を計算すると x が得られる.

(確認)

$$\begin{aligned}(c_1^a)^{-1} \cdot c_2 &= ((\alpha^k)^a)^{-1} \cdot x\beta^k \pmod p \\ &= (\alpha^{ak})^{-1} \cdot x \cdot \alpha^{ak} \pmod p \\ &= x \pmod p \end{aligned} \tag{454}$$

のように確かに平文が復元される. a を知らないとすれば, $(c_1^a)^{-1} \cdot c_2 \pmod{p}$ を計算することは離散対数問題を解くことに相当し, 非常に困難となる.

演習問題 13

1. $GF(5)$ の原始元を求めよ.
2. エルマガル暗号の公開鍵 $p = 17, \alpha = 5$, 秘密鍵 $a = 15$ を持つ受信者のもう一つの公開鍵 β を求めよ. また, 乱数が $k = 6$ であったとし, 平文 $w = 10$ を暗号化した際の $c = (c_1, c_2)$ を求め, これを上で述べた復号化法により平文に復元すれば $w = 10$ が正しく求まることを示せ.

※**注**：今回のレポート締め切りは **8 月 8 日の試験開始前まで**です.