2005－CSEC－31（12）
2005／12／9

法a^xの剰余環についての考察

五十嵐 育弘　　児玉　英一郎　　高田　豊雄
ikuiga64@msn.com　kodama@iwate_pu.ac.jp　takata@iwate_pu.ac.jp

岩手県立大学大学院　ソフトウエア情報学研究科

a^xを法とする剰余環の位数a^yの元を用いた部分集合には，特殊な加法が定義できるものがあり，また，この剰余環での離散対数は解を求めやすく扱いやすい．この剰余環についての性質について考察する．

Study of Residue Class Ring of Modulo a^x

Ikuhiro Igarashi　Eiichiro Kodama　Toyoo Takata

Iwate Prefectural University

There are some subsets order a^y which can define the additive group in the residue class ring on modulo a^x. In addition, to find solution they are easy to handle the discrete logarithm with this residue class ring. We study characteristics concerning this residue class ring.

１．はじめに

現在の暗号理論の分野では，エルガマル暗号やRSA暗号に代表されるように乗法群の演算を利用したものが主流となっている．本稿では，加法群の演算を利用した暗号のための基礎研究として，法a^xの剰余環（a,xは自然数）の性質について考察する．

２．法a^xの剰余環の位数a^yの元

a,xを2以上の自然数，Zを有理整数環とし，剰余環Z/a^xZを考える．$0<y<x$である任意の自然数yに対して，$0\le k\le a^{y-1}-1$，$1\le m\le a-1$，$(a,m)=1$なる自然数k,mに対して，$(ka+m)a^{x-y}+1$は，乗法群$(Z/a^xZ)^\times$内の位数a^yの元となる．この式で表される位数a^yの元の個数は$(Z/a^xZ)^\times$内に$a^{y-1}\phi(a)$個存在する（ϕはオイラーのϕ関数）．

また，$(ka+m)a^{x-y}-1$は，乗法群$(Z/a^xZ)^\times$内の位数$2a^y$の元となる．この式で表される位数$2a^y$の元の個数は$(Z/a^xZ)^\times$内に$a^{y-1}\phi(a)$個存在する．

［証明］

$a,x\ge 2$，$0<y<x$，$0\le k\le a^{y-1}-1$，$1\le m\le a-1$のとき，法a^xのもとで，$(ka+m)a^{x-y}+1$をa^y乗すると1になることを示す．

$(1+a^{x-y})^{a^y}$を展開し，1以外の項が全てa^xを因子に持っていることを示せば，上記を示したことになる．$1\le r\le a^y$とした時，r番目の項（最初の項を0番目とする）は，${}_{a^y}C_r a^{r(x-y)}$と表される．

${}_{a^y}C_r a^{r(x-y)}={}_{a^y}C_r a^{(r-1+1)(x-y)}={}_{a^y}C_r a^{(r-1)(x-y)+(x-y)}$

$={}_{a^y}C_r a^{(r-1)(x-y)}a^{x-y}$であり，

$a^y|_{a^y}C_r a^{r-1}$ならば$a^y|_{a^y}C_r a^{(r-1)(x-y)}$なので，ある自然数$s$が存在して，

$a^y|_{a^y}C_r a^{r-1}$ならば

${}_{a^y}C_r a^{(r-1)(x-y)} = sa^y a^{x-y} = sa^x$ となる．
以上より，$a^y|_{a^y} C_r a^{r-1}$ ならば
$a^x|_{a^y} C_r a^{r(x-y)}$ となる．したがって，
$a^y|_{a^y} C_r a^{r-1}$ を示せば十分である．
まず，$r = a^y$ の時，$a^y|_{a^y} C_{a^y} a^{(a^y-1)}$ を示す．これは，$y \le a^y - 1$ を示せば十分である．$f(y) = a^y - 1 - y$ とおき，これを y で微分すると，$f'(y) = a^y \log a - 1 > 0$ となり，単調増加である．
次に，$2 \le a, 1 \le y < x$ なので，
$f(y) \ge f(1) = a - 1 - 1 \ge 0$．よって，
$y \le a^y - 1$ が成立する．これより，
$r = a^y$ の時，$a^y|_{a^y} C_{a^y} a^{(a^y-1)}$ が示された．
次に，$1 \le r \le a^y - 1$ の任意の r に対して $a^y|_{a^y} C_r a^{r-1}$ が成立することを示す．
二項係数は必ず整数になるため，
${}_{a^y}C_r = \dfrac{a^y!}{r!(a^y - r)!}$ の分母の $r!$ が a を因子として $r-1$ 個以下しか含まないことを示せば，二項係数 ${}_{a^y}C_r = \dfrac{a^y!}{r!(a^y - r)!}$ の分子の a^y がそのまま残ることになり，$a^y|_{a^y} C_r a^{r-1}$ を示したことになる．
$r!$ の中の 因子 a の個数は $a > r$ の場合 0 であり，$a^y|_{a^y} C_r a^{r-1}$ である．ある自然数 t が存在して，$a^t \le r < a^{t+1}$ とし表せる場合，因子 a の個数 S は，

$$S = \left\lfloor \frac{r-(a-1)}{a} \right\rfloor + \left\lfloor \frac{r-(a^2-1)}{a^2} \right\rfloor + \ldots + \left\lfloor \frac{r-(a^t-1)}{a^t} \right\rfloor$$

と表される．

$$S \le \frac{r}{a} + \frac{r}{a^2} + \ldots + \frac{r}{a^t} = \frac{r(a^t-1)}{a^t(a-1)} \le r - 1$$

であるため，$1 \le r \le a^y - 1$ なる任意の r に対して $a^y|_{a^y} C_r a^{r-1}$ が成立する．
よって，法 a^x のもとで $(ka+m)a^{x-y} + 1$ を a^y 乗すると 1 になることが示された．
次に，$1 \le v < a^y$ なる自然数 v に対して $g^v \ne 1 (\mathrm{mod}\, a^x)$ であることを示す．
$1 \le v < a^y$，$g = (ka+m)a^{x-y} + 1$ としたとき，$g^v \equiv 1 (\mathrm{mod}\, a^x)$ なる v が存在すると仮定する．
$g^v - 1$ を二項定理により，a の冪多項式で表現すると，$\sum_{i=1}^{v} {}_vC_i g^i$ と表され，a の次数が最小の項を求めると，$g = (ka+m)a^{x-y} + 1$ であることから ${}_{vi}C_1 (ka+m)a^{x-y}$ となり，$(m,a) = 1$ より，$ka+m$ は因子として a を持つことがないため，次数は高々 $x - y + \lfloor \log_a v \rfloor$ である．これは $1 \le v < a^y$ であることから x より小さいことになる．この a の最小次数を u とし，a^u でこの冪多項式をくくると，$a^u (d_1 a^{f_1} + d_2 a^{f_2} + \ldots + d_U)$ となる．
これが a^x で割れなければならないため，
$d_1 a^{f_1} + d_2 a^{f_2} + \ldots + d_U = \alpha a^{x-u}$
となる必要があるが，左辺は a の因子を持っていないため，これは矛盾である．
よって，$g^v \equiv 1 (\mathrm{mod}\, a^x)$ となるような v は存在しないことになる．
以上より，$(ka+m)a^{x-y} + 1$ は，乗法群 $(Z/a^x Z)^\times$ 内の位数 a^y の元であることが示された．
$(ka+m)a^{x-y} + 1$ で表される元の個数は，言い換えると，$ka+m$ で表される数の個数ということなので，$0 \le k \le a^{y-1} - 1$，$1 \le m \le a-1$，$(m,a) = 1$
より，k のとりうる最大数 a^{y-1} と m のとりうる最大数 $\phi(a)$ との積 $a^{y-1}\phi(a)$ で与えられる．
位数 $2a^y$ の元が $(ka+m)a^{x-y} - 1$ と表される証明は，概略だけ示す．
$(ka+m)a^{x-y} - 1$ を a^y 乗すると，上記の証明から，-1 になり，また，
a^y 乗より小さい冪乗数では -1 にも 1 にもならないことが分かる．-1 を 1 にする最小の冪乗数は 2 であることから，位数

$2a^y$ の元が $(ka+m)a^{x-y}-1$ で表される．

元の個数については，位数 a^y の考察と同様である．

３．位数 a^y の元を用いた加法群の定義

法 a^x のもとでの位数 a^y の加法群 G を以下のように定義する．

$$G \overset{def}{=} \{g^l \bmod a^x \mid g \bmod a^x \in Z/a^xZ,\ g^{a^y} \equiv 1 \bmod a^x, 1 \le l \le a^y\}$$

ここで G に以下の演算を導入する．

$\forall m,n \in G$ に対して，

$$m \circ n \overset{def}{=} m+n-1 \bmod a^x$$

このとき，演算 ∘ は集合 G 上の加法演算となる．零元は１であり，G の任意の元 n の逆元は，a^x-n+2 で与えられる．

４．簡易記法

前述の加法群 G におけるの加法演算について，同じ元を複数回足し合わせるための簡易記法を以下のように定義する．

$$\forall n \in G \text{ に対して } \forall n \in G(n \circ n \overset{def}{=} 2*n)$$

$$\forall n \in G, t < \#G((t*n) \circ n \overset{def}{=} (t+1)*n)$$

ただし，$\#G$ は加法群 G の元の個数．

演算 $*$ は，

$$t*n \overset{def}{=} tn-(t-1) \bmod a^x = t(n-1)+1 \bmod a^x$$

で与えられる．

５．乗算と加算の対応

加法群 G の加法演算は，群の性質を保つために無理に定義したため，加法演算と乗法演算とで不整合が生じている．

$$g^w = (g-1)\sum_{i=0}^{w-1} g^i + 1$$

であるため，加法演算の簡易記法で表現すると，$g^w = g*\sum_{i=0}^{w-1} g^i$ となる．一般的に用いられている加算演算で g^w を表現すると，g 自身を g^{w-1} 回足し合わせたことになるが，ここで定義した加算演算で g^w を表現すると，g 自身を $\sum_{i=0}^{w-1} g^i$ 回足し合わせたことに対応する．

６．法 a^x の剰余環の性質

法 a^x のもとでの位数 a^y の加法群 G は，

$\forall \alpha,\beta,g \exists h(Ind_g(g^\alpha \circ g^\beta) = Ind_h(h^\alpha \circ h^\beta))$

という性質を持っている．g を加法群 G の任意の元とした場合，位数が a^y であることから，h は $g+la^y$ で与えられる．

例）法 $7^5=16807$　位数 $7^4=2401$

元 $g=(49\times7+1)7+1=2409$

元 $h=g+5\times7^4=14414$

$Ind_{2409}(2409^{744} \circ 2409^{1873}) = 219$

$Ind_{14414}(14414^{744} \circ 14414^{1873}) = 219$

$2409^{744} \circ 2409^{1873} = 2409^{219}$

$8562+6985-1=15546$

$14414^{744} \circ 14414^{1873} = 14414^{219}$

$1359+4584-1=5942$

７．離散対数の求め方

法 a^x のもとでの位数 a^y の乗法群上の離散対数問題は a が小さい数の場合，簡単に解くことができる．このような乗法群の元は $(ka+m)a^{x-y}+1$ であるが，

$$g=(ka+m)a^{x-y}+1, A=a^x$$

$$Y = g^X \pmod A$$

とおき，X を a の冪多項式で表すと，

$$X = m_0 + m_1 a + m_2 a^2 + \ldots = \sum_{i=0}^{y-1} m_i a^i$$

この多項式の係数 m_i を全て決定できれば，Y の離散対数 X を求めることができる．

$$Y^{a^{y-1}} = g^{a^{y-1}X} = g^{m_0 a^{y-1}} \pmod A$$

であるため，m_0 に $0 \le m_0 \le a-1$ の範囲で数を代入し $Y^{a^{y-1}} = g^{m_0 a^{y-1}} \pmod A$ となる m_0 を決定することができる．

$$X_0 = X$$

$$X_{i+1} = X_i - m_i a^i$$

$$Y_i = g^{X_i} \pmod{A}$$

とおくと，

$$Y_i^{a^{y-1}} = g^{a^{y-i-1}X_i} = g^{m_i a^{y-i-1}} \pmod{A}$$

となり，上記m_0の決定方法を帰納的に繰り返すことにより，任意のm_iを決定できる．

例）法6^5位数6^3元1981の剰余環上で1621の離散対数を求める過程を以下に示す．

法　　$6^5 = 7776$

位数　　$6^3 = 216$

元　$1981 = (9\times 6+1)6^{5-3}+1$

$1621 = 1981^X \pmod{7776}$ ・・・(1)

まずXを冪多項式であらわす．

$$X = m_0 + m_1 6 + m_2 6^2$$

位数が6^3であることを利用して，m_0以外の項を消す．

$$6^2 X = m_0 6^2 \pmod{6^3}$$

これを(1)式に利用して，

$$1621^{6^2} = 1981^{m_0 6^2} \pmod{6^3}$$

$$3889 = 1297^{m_0} \pmod{6^3}$$

m_0に$0 \le m_0 \le 5$の範囲で値を代入すると，

$$3889 = 1297^3 \pmod{6^3}$$

$m_0 = 3$が見つかる．次に$X_1 = X - 3$として(1)式のXをX_1でおきかえると，

$$1621\times 1981^{-3} = 7345 = 1981^{X_1} \pmod{6^3}$$

となる．これを(2)式とする．

$$X_1 = m_1 6 + m_2 6^2$$

より，m_1以外の項を上記の要領で消去する．

$$6X_1 = m_1 6^2$$

これを(2)式に利用して，

$$7345^6 = 1981^{m_1 6^2} \pmod{6^3}$$

$$5185 = 1297^{m_1} \pmod{6^3}$$

m_1に$0 \le m_1 \le 5$の範囲で値を代入すると，

$$5185 = 1297^4 \pmod{6^3}$$

$m_1 = 4$が見つかる．次に$X_2 = X_1 - 4\times 6$として(2)式のX_1をX_2でおきかえると，

$$7345\times 1981^{-24} = 6481 = 1981^{X_2} \pmod{6^3}$$

$$6481 = 1981^{m_2 6^2} = 1297^{m_2} \pmod{6^3}$$

m_2に$0 \le m_2 \le 5$の範囲で値を代入すると，

$$6481 = 1297^5 \pmod{6^3}$$

$m_2 = 5$が見つかる．以上で求める離散対数

$$X = 3 + 4\times 6 + 5\times 6^2 = 207$$

が求まる．

8．まとめ

法a^xの剰余環の性質について，位数がa^yの元，加法群，離散対数の視点で考察した．今後は，この剰余環の性質を利用して落とし戸関数の構成を考察をする予定である．

9．参考文献

1) J.A.ブーフマン著，林芳樹訳「暗号理論入門」シュプリンガー・フェアラーク東京

2) ジョセフ．H．シフヴァーマン著　鈴木治郎訳「はじめての数論」ピアソン・エヂュケーション