6. 整数論

約数と倍数

任意の整数をa とし、任意の正整数をb とするとき、

$$a = bq+r, \quad 0 \leqq r \leqq b-1$$

を満たすq, r が一意的に存在する。このとき、qを**商**、rを**剰余**という。

r = 0 即ち、a = bq のとき、aはbの**倍数**、bはaの**約数**という。

公約数（common devisor）：任意の2つの整数の共通の約数
最大公約数（greatest common devisor）：公約数の中で最大の数

整数a、bの最大公約数を以下で表現

(a, b) または GCD(a, b)

(a, b) = 1の時、aとbは**互いに素**であるという。

公倍数（common multiple）：任意の2つの整数の共通の倍数
最小公倍数（least common multiple）：公倍数の中で最小の数

整数a、bの最小公倍数を以下で表現

LCM(a, b)

約数に関する定理

定理1　任意の整数a(≠0。以降も同じ)に対して、aはaの約数、1はaの約数

定理2　aがb の約数、bがcの約数ならば、aはcの約数

定理3　aがb の約数、bがaの約数ならば、b=±a

証明　b=qa, a=q'b　(q, q' は整数)

a=q'qa

a≠0故、q'q=1, q'=q=±1　　∴　b=±a

補遺　aがb の約数、cがdの約数ならば、acはbdの約数

定理4　aがb とcの公約数ならば、aはb±cの約数

証明　b=qa, c=q'a　(q, q' は整数)

b±c= qa ± q'a = (q ± q')a

q ± q' は整数故、aはb±cの約数

最大公約数に関する定理

定理5　a<b の時、qを整数とすると、(a, b)= (a, b−qa)

証明

d = (a, b), d' = (a, b−qa) とおく
dはqa の約数　　従って、dはqa とbの公約数
∴　定理4より dはb−qaの約数
∴　dはaとb−qaの公約数
d'はaとb−qaの最大公約数故、d≦d'・・・①

逆に、d'はa とb−qaの公約数
d'はqaの約数
∴　d'は(b−qa)+qaの約数　　即ち、d'はbの約数
∴　d'はaとbの公約数
dはaとbの最大公約数故、d'≦d・・・②

式①、②より、d=d'　即ち、(a,b)= (a,b−qa)

例　(6, 15) = (6, 15−2・6) = (6, 3)

ユークリッドの互除法

a と b の最大公約数 (a, b) を求める

$a<b$とすると、$b=q_1a+r_1$とおける

定理5より $(a, b) = (a, b-q_1a) = (a, r_1) = (r_1, a)$ 　　$r_1 < a$

$b=q_1a+r_1$
$a=q_2r_1+r_2$
$r_1=q_3r_2+r_3$
・・・
$r_{n-2}=q_nr_{n-1}+r_n$
$r_{n-1}=q_{n+1}r_n+0$ 　　$b>a>r_1>r_2>\cdots>r_n>0$

$(a, b) = (r_1, a) = (r_2, r_1) = \cdots = (r_n, r_{n-1}) = (0, r_n) = r_n$

例：(85,204)を求める

85=0・204+85
204=2・85+34
85=2・34+17
34=2・17+0

最大公約数は17

例：(3,11)を求める

11=3・3+2
3=1・2+1
2=2・1+0

最大公約数は1

オイラーの関数

素数：1より大きい整数で、1とその整数以外の約数を持たない数
合成数：1とその整数以外にも、約数を持つ正整数
（注）1は素数でも合成数でもない

定理6　合成数は素数の積で表される（**素因数分解**）

定理7　素数の積による合成数の表現方法は1通りである（積の順序は対象外）

オイラーの関数$\varphi(n)$：正整数n に対し、$1 \leqq i \leqq n$ で、$(n, i) = 1$ を満たすi の総数

例：　$n=12$ のとき、$1 \leqq i \leqq 12$ を満たす集合Z_{12}は

$Z_{12}=\{1, 2, 3, \cdots, 12\}$

$(12, i) = 1$ を満たす i の集合$Z_{12}^* = \{1, 5, 7, 11\}$　故、$\varphi(n)=4$

合同式

日	月	火	水	木	金	土
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

日：x mod 7 = 4
月：x mod 7 = 5
火：x mod 7 = 6
水：x mod 7 = 0
木：x mod 7 = 1
金：x mod 7 = 2
土：x mod 7 = 3

2つの整数 a,b が同じ曜日にあれば、7で割った余りが同一ということ
このことを以下のように記述し、「**a は7を法として b に合同である**」という

合同式　$a \equiv b \bmod 7$

反射律　$a \equiv a \bmod n$ 　　　但し、n は自然数
対称律　$a \equiv b \bmod n$ ならば $b \equiv a \bmod n$
推移律　$a \equiv b \bmod n$ かつ $b \equiv c \bmod n$ ならば $a \equiv c \bmod n$

例：　$3 \equiv 10 \bmod 7$ かつ $10 \equiv 17 \bmod 7$ ならば $3 \equiv 17 \bmod 7$

合同式の算法(1)

定理8　$a \equiv b \bmod n$ 、$c \equiv d \bmod n$ のとき、

$a + c \equiv b + d \bmod n$
$a - c \equiv b - d \bmod n$
$ac \equiv bd \bmod n$

証明　$a = pn + r$ 　$b = qn + r$ 　　$c = sn + u$ 　$d = tn + u$

$a+c = (p+s)n + \underline{(r+u)}$ 　　$b+d = (q+t)n + \underline{(r+u)}$
同一なので、nで割った余りも同じ

$a-c = (p-s)n + \underline{(r-u)}$ 　$b-d = (q-t)n + \underline{(r-u)}$
同一なので、nで割った余りも同じ

$ac = (psn + pu + rs)n + \underline{ru}$ 　　$bd = (qtn + qt + rt)n + \underline{ru}$
同一なので、nで割った余りも同じ

合同式の算法(2)

補遺2　$a \equiv b \bmod n$ 、m:整数 のとき、

$a - b \equiv 0 \mod n$ （移項しても成立）
$ma \equiv mb \mod n$ （整数倍しても成立）

証明

$a \equiv b \bmod n$ (1)
$b \equiv b \bmod n$ (2)
$m \equiv m \bmod n$ (3)

(1)−(2): $a - b \equiv 0 \mod n$

(1)×(3): $ma \equiv mb \mod n$

補遺3 abに対する剰余は (aに対する剰余)･b に対する剰余に等しい

証明

ab mod p = (mp+r)b mod p = (mpb+rb) mod p = rb mod p

合同式の算法(3)

定理9　$a \equiv b \bmod n$ ならば $a^k \equiv b^k \bmod n$

証明

$a \equiv b \bmod n$
$a \equiv b \bmod n$
・・・
$a \equiv b \bmod n$
} k個

両辺を掛け合わせると

$a^k \equiv b^k \bmod n$

定理10　$(c, n) = 1$ ならば
$ac \equiv bc \mod n$ の時、$a \equiv b \mod n$

証明

$ac - bc \equiv 0 \bmod n$
$(a-b)c \equiv 0 \bmod n$
$(c, n)=1$故、$a - b \equiv 0 \mod n$
即ち、$a \equiv b \mod n$

剰余類

剰余類R(a):自然数 n と整数 a に対して、n を法としてa と合同な整数の集合
完全剰余系R_n:各剰余類R(i) (i=0,1,…,n-1)それぞれの要素から成る整数集合
既約剰余系R_n* : 完全剰余系R_n の整数のうち、n と互いに素となる($(n, a_i)=1$)
整数a_iの集合

例:　n=10 を法とする剰余類

R(0) = {…, -20, -10, 0, 10, 20, …}
R(1) = {…, -19, -9, 1, 11, 21, …}
・・・
R(9) = {…, -11, -1, 9, 19, 29, …}

完全剰余系 R_{10}= {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}
既約剰余系　R_{10}* = {1, 3, 7, 9}

オイラーの関数(R_n* の要素数) $\varphi(10) = 4$

既約剰余系の乗算

完全剰余系 R_{10}: {0,1,2,3,4,5,6,7,8,9}

乗算結果

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

既約剰余系 R_{10}* : {1,3,7,9}

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

・任意の2つの数の乗算結果は元の既約剰余系の要素
・乗算表の行や列には、すべての要素が繰り返しなしで現れる

乗算の対応は1対1

既約剰余系の乗算対応

定理11　mod n の既約剰余系 $R_n^* = \{a_1, a_2, \cdots, a_{\varphi(n)}\}$ の各要素xに、R_n^* のうちの１つの要素 a_i を掛けて

$$x \rightarrow a_i x$$

という対応を考えると、この対応は１対１である。

証明　$(a_i, n) = 1, (x, n) = 1$ 故、$(a_i x, n) = 1$

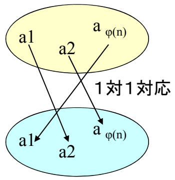
従って、$a_i x$ は既約剰余系 R_n^* に属する

また、$x_1 \rightarrow a_i x_1,\quad x_2 \rightarrow a_i x_2$

で、$a_i x_1 \equiv a_i x_2 \mod n$

ならば、定理8より $a_i(x_1 - x_2) \equiv 0 \mod n$

即ち、nは$a_i(x_1 - x_2)$の約数



ここで、$(a_i, n) = 1$ 故、n は$(x_1 - x_2)$の約数

即ち、$x_1 \equiv x_2 \mod n$

従って、対応は１対１

オイラーの定理

定理12　自然数n、整数aに対し、$(a, n) = 1$ ならば、以下の式が成立

$$a^{\varphi(n)} \equiv 1 \mod n$$

証明　$R_n^* = \{a_1, a_2, \cdots, a_{\varphi(n)}\}$の各要素をx、$R_n^*$のうちの１つの要素$a_i$とした場合

$x \rightarrow a_i x$ は１対１対応

即ち、$\{a_1, a_2, \cdots, a_{\varphi(n)}\}$ と$\{a_i a_1, a_i a_2, \cdots, a_i a_{\varphi(n)}\}$は要素の並び順を除いては、同一の集合

従って、その積は同一。即ち、

$$a_1 a_2 \cdots a_{\varphi(n)} \equiv (a_i a_1)(a_i a_2) \cdots (a_i a_{\varphi(n)}) \mod n$$

$$a_1 a_2 \cdots a_{\varphi(n)} \equiv a_i^{\varphi(n)} a_1 a_2 \cdots a_{\varphi(n)} \mod n$$

$$a_1 a_2 \cdots a_{\varphi(n)} (a_i^{\varphi(n)} - 1) \equiv 0 \mod n$$

$a_1 a_2 \cdots a_{\varphi(n)}$は n と互いに素故、

$$a_i^{\varphi(n)} - 1 \equiv 0 \mod n$$

$$a_i^{\varphi(n)} \equiv 1 \mod n$$

付．オイラーの定理の例

定理12　自然数n、整数aに対し、$(a, n) = 1$ ならば、以下の式が成立

$$a^{\varphi(n)} \equiv 1 \mod n$$

例

$n = 12$ のとき、$(a, 12) = 1$ を満たす既約剰余系$R_{12}^* = \{1, 5, 7, 11\}$

オイラーの関数 $\varphi(12) = 4$

$1^4 \equiv 1 \mod 12$
$5^4 = 25^2 \equiv 1 \mod 12$
$7^4 = 49^2 \equiv 1 \mod 12$
$11^4 = 121^2 \equiv 1 \mod 12$

フェルマーの小定理

定理13　整数a に対し、p が素数で、$(a, p) = 1$ ならば、以下の式が成立

$$a^{p-1} \equiv 1 \mod p$$

∵　pが素数故、オイラー関数$\varphi(p) = p - 1$

例　$p = 5$ のとき

$a = 1, 2, 3, 4$
$p - 1 = 4$

$1^4 \equiv 1 \mod 5$
$2^4 = 16 \equiv 1 \mod 5$
$3^4 = 81 \equiv 1 \mod 5$
$4^4 = 256 \equiv 1 \mod 5$

逆数

素数pの既約剰余系 $R_p^* = \{1, 2, \cdots, p-1\}$ の任意の要素 a に対して

$ab \equiv 1 \mod p$

となるb が存在する。

$b = a^{p-2}$ を選べばよい

フェルマーの小定理

pが素数で、$(a, p) = 1$ ならば、以下の式が成立

$a^{p-1} \equiv 1 \mod p$

b をa の**逆数(逆元)**といい、a^{-1}で表す。

a の逆数は唯一に定まる。

証明

$ab \equiv 1 \mod p$
$ab' \equiv 1 \mod p$

とすると、$a(b-b') \equiv 0 \mod p$

$(a, p) = 1$ 故、$b-b' \equiv 0 \mod p$

即ち、$b \equiv b' \mod p$

ある数の逆数の逆数はその数自身 $(a^{-1})^{-1} = a$

17

逆数の計算(1)

例　mod 11での既約剰余系の逆数

$b = a^{p-2}$ を計算

$1^{-1} \equiv 1^{11-2} = 1^9 \equiv 1$
$2^{-1} \equiv 2^{11-2} = 2^9 = 512 \equiv 6$
$3^{-1} \equiv 3^{11-2} = 3^9 = (3^3)^3 = 27^3 \equiv 5^3 = 125 \equiv 4$
$4^{-1} \equiv 3$
$5^{-1} \equiv 5^{11-2} = 5^9 = (5^3)^3 = 125^3 \equiv 4^3 = 64 \equiv 9$
$6^{-1} \equiv 2$
$7^{-1} \equiv 7^{11-2} = 7^9 = (7^3)^3 = 343^3 \equiv 2^3 = 8$
$8^{-1} \equiv 7$
$9^{-1} \equiv 5$
$10^{-1} \equiv 10^{11-2} = 10^9 = (10^3)^3 = 1000^3 \equiv 10^3 = 1000 \equiv 10$

18

逆数の計算(2)

例　$3b \equiv 1 \mod 11$におけるb(3の逆数)の計算

ユークリッドの互除法の利用

$3b \equiv 1 \mod 11$　(1)

恒等的に成り立つ式　$11b \equiv 0 \mod 11$　(2)

11と3にユークリッドの互除法を適用

$11=3 \cdot 3+2$　(3)
$3=1 \cdot 2+1$　(4)
$2=2 \cdot 1$

(3)より、×3 が必要

(1) × 3　$9b \equiv 3 \mod 11$　(5)

(2) – (5)　$2b \equiv -3 \mod 11$　(6)

(4)より、(1) – (6)　$b \equiv 4 \mod 11$

19