離散数学及び演習
講義 9　2014. 6.12(木)2限

合同式(続き)
(教科書　pp.131-137, 140-145)

教科書･･･野崎昭弘:離散系の数学、近代科学社

1 次合同方程式

- 係数 $a_1, a_2, \ldots, a_n, b \in \mathbf{Z}$, 変数 $x_1, x_2, \ldots, x_n \in \mathbf{Z}$, 法 $p \in \mathbf{Z}$ についての(n 元)1 次合同方程式 (congruent equation)
  - $a_1x_1+a_2x_2+\ldots+a_nx_n \equiv b \pmod{p}$

定理(1 次合同方程式の解の存在)

- 任意の $a, p \in \mathbf{Z}$ に対して, $x \in \mathbf{Z}$ が存在して, $ax \equiv b \pmod{p}$ であるとき, かつそのときに限り, $\gcd(a, p) \mid b$.
- 任意の $a_1, a_2, \ldots, a_n, p \in \mathbf{Z}$ に対して, $x_1, x_2, \ldots, x_n \in \mathbf{Z}$ が存在して, $a_1x_1+a_2x_2+\ldots+a_nx_n \equiv b \pmod{p}$ であるとき, かつそのときに限り, $\gcd(a_1, a_2, \ldots, a_n, p) \mid b$.

証明

任意の $a, p \in \mathbf{Z}$ に対して, $x \in \mathbf{Z}$ が存在して, $ax \equiv b \pmod{p}$ であるとき, かつそのときに限り, $\gcd(a, p) \mid b$.
- $ax \equiv b \pmod{p}$ iff $y \in \mathbf{Z}$ が存在して $ax-b=y \cdot p$
- 任意の $m, n \in \mathbf{Z}$ に対して, $x, y \in \mathbf{Z}$ が存在して, $mx+ny=k$ iff $\gcd(m, n) \mid k$

任意の $a, p \in \mathbf{Z}$ に対して, $x, y \in \mathbf{Z}$ が存在して, $ax-py=b$
iff $\gcd(a, -p) \mid b$.
iff $\gcd(a, p) \mid b$.
また, $y \in \mathbf{Z}$ が存在して $ax-py=b$ iff $ax \equiv b \pmod{p}$.
ゆえに,
任意の $a, p \in \mathbf{Z}$ に対して, $x, y \in \mathbf{Z}$ が存在して, $ax \equiv b \pmod{p}$
iff $\gcd(a, p) \mid b$.

系(1 次合同方程式の解の存在)

- 任意の $a, p \in \mathbf{Z}$ に対して, $x \in \mathbf{Z}$ が存在して, $ax \equiv 1 \pmod{p}$ であるとき, かつそのときに限り, $\gcd(a, p)=1$.
- 任意の $a \in \mathbf{Z}$, 任意の素数 p に対して, $x \in \mathbf{Z}$ が存在して, $ax \equiv 1 \pmod{p}$ であるとき, かつそのときに限り, $a \not\equiv 0 \pmod{p}$.
  - 合同式に関する整数 a の「逆数 x」の存在条件 … 法と互いに素

- 定理から明らか.
  - 任意の $a, p \in \mathbf{Z}$ に対して, $x \in \mathbf{Z}$ が存在して, $ax \equiv b \pmod{p}$ であるとき, かつそのときに限り, $\gcd(a, p) \mid b$.
- p が素数のとき, $\gcd(a, p)=1$ iff $p \mid a$ でない iff $a \not\equiv 0 \pmod{p}$.

定理(1 次合同方程式の解の全体)

$\gcd(a, p) \mid b$, かつ, 1 次合同方程式 $ax \equiv b \pmod{p}$ の解のひとつ(特殊解)を $x=x_0$ とすると, $x \in \mathbf{Z}$ が解であるとき, かつそのときに限り, $x \equiv x_0 \pmod{p'}$ である. ただし, $p'=p/\gcd(a, p)$.
- 他のすべての解(一般解)は $x \equiv x_0 \pmod{p'}$ と表せる.

- $ax \equiv b \pmod{p}$ の解は p' を法として一意に定まる.
- $\gcd(a, p)=1$ のとき
  - 一般解 $x \equiv x_0 \pmod{p}$

証明

$\gcd(a, p) \mid b$，かつ，$ax \equiv b \pmod{p}$の特殊解を$x = x_0$とすると，
$x \in \mathbf{Z}$ が解であるとき，かつそのときに限り，
$x \equiv x_0 \pmod{p'}$ である．ただし，$p' = p / \gcd(a, p)$．

- 1 次不定方程式 $mx + ny = k$ の特殊解を $x = x_0$，$y = y_0$ とすると，
  $x \in \mathbf{Z}$ が解であるとき，かつそのときに限り，任意の $q \in \mathbf{Z}$ に対して，
  $x = x_0 + (n / d)q$，　$y = y_0 - (m / d)q$．
  ただし，$d = \gcd(m, n)$．

---

1 次不定方程式 $ax - py = b$ の特殊解は $x = x_0$ となるから，
定理より，x が解であるとき，かつそのときに限り，
任意の $q \in \mathbf{Z}$ に対して，$x = x_0 + (-p / \gcd(a, p))q$．
このとき，$x - x_0 = (-p / \gcd(a, p))q = -q p'$ であり，
$-q \in \mathbf{Z}$ だから，$x \equiv x_0 \pmod{p'}$．

7

1 次合同方程式の解法

例：　$47x \equiv 1 \pmod{7}$

- 解法1：　1 次不定方程式を解く
  - $47x - 7y = 1$ の解を求める

$47x - 7y = -7(-6x - y) + 5x$
$= -7u + 5x$　　$u = -6x - y$
$= 5(-u + x) - 2u$
$= 5v - 2u$　　$v = -u + x$
$= -2(u - 2v) + v$
$= -2w + v$　　$w = u - 2v$

$-2w + v = 1$ だから，$v = 1 + 2w$
$w = 0$ とおくと，$v = 1$．
ゆえに，$u = w + 2v = 2$，　$x = v + u = 3$．　← 特殊解 $x = x_0$
したがって，$x \equiv 3 \pmod{7}$．　← 一般解
$x \equiv x_0 \pmod{p / \gcd(a, p)}$

8

1 次合同方程式の解法（続き）

例：　$47x \equiv 1 \pmod{7}$

- 解法2：　合同式の性質を用いて解く
  - $5x \equiv 1 \pmod{7}$を解く

$47x \equiv 5x \equiv 1 \pmod{7}$ だから，$15x \equiv 3 \pmod{7}$．
$15 \equiv 1 \pmod{7}$ だから，$15x \equiv x \pmod{7}$
ゆえに，$x \equiv 3 \pmod{7}$．

9

問題

（百五減算）お菓子を袋に詰めるとき，
3 個ずつ詰めると 1 個余り，
5 個ずつ詰めると 2 個余り，
7 個ずつ詰めると 3 個余る．
お菓子は全部で何個あるか．

- 「孫子算経」
  （B.C. 3世紀頃，中国）
- 「塵劫記」
  （1627，吉田光由（1598-1673））
  - 和算
  - 命数法
    - 一，十，百，千，万，億，兆，京，垓，秭，穣，溝，澗，正，載，極，恒河沙，阿僧祇，那由他，不可思議，無量大数（10^{68}）

10

問題の定式化

お菓子の個数を x とすると，連立合同方程式

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

の非負整数解を求める．

11

連立合同方程式

係数 $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_m \in \mathbf{Z}$，変数 $x \in \mathbf{Z}$，
法 $p_1, p_2, \ldots, p_m \in \mathbf{Z}$ についての（1 元）連立 1 次
合同方程式（simultaneous congruent equation）

- $$\begin{cases} a_1 x \equiv b_1 \pmod{p_1} \\ a_2 x \equiv b_2 \pmod{p_2} \\ \quad\vdots \\ a_m x \equiv b_m \pmod{p_m} \end{cases}$$

12

定理（連立合同方程式の解の存在）

任意の $a_1, \ldots, a_m, b_1, \ldots, b_m, p_1, \ldots, p_m \in \mathbf{Z}$ に対して，
次の(1)，(2)が成り立つならば，$x \in \mathbf{Z}$ が存在して，

$$\begin{cases} a_1 x \equiv b_1 \pmod{p_1} \\ \quad \vdots \\ a_m x \equiv b_m \pmod{p_m} \end{cases}$$

が成り立つ．

(1)　任意の i $(1 \le i \le m)$ に対して，$\gcd(a_i, p_i) = 1$．

(2)　任意の i, j $(1 \le i \le m,\ 1 \le j \le m,\ i \ne j)$ に対して，
$\gcd(p_i, p_j) = 1$．

- 1次合同方程式の解の存在の十分条件

13

証明

次の(1)，(2)が成り立つならば，$x \in \mathbf{Z}$ が存在して，$a_i x \equiv b_i \pmod{p_i}$ $(1 \le i \le m)$が成り立つ．

(1)　任意の i に対して，$\gcd(a_i, p_i) = 1$．

(2)　任意の i, j $(i \ne j)$ に対して，$\gcd(p_i, p_j) = 1$．

---

(1)から，定理より，
任意の i に対して合同方程式 $a_i x \equiv b_i \pmod{p_i}$ の解が存在する．
そこで，その特殊解を $x = x_{i0}$ とおく．
このとき，その一般解は $x \equiv x_{i0} \pmod{p_i}$ と表せる．
ここで，$M_i = p_1 \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_m$ とおくと，(2)から，$p_i \mid M_i$ でない．
さらに，$M_1, \ldots, M_m$ のすべてに共通の素因数が存在すると仮定すると，
それは $p_1, \ldots, p_m$ のすべてに共通の素因数であり，(2)に矛盾する．
ゆえに，$\gcd(M_1, \ldots, M_m) = 1$．
このとき，1 次不定方程式 $M_1 u_1 + \ldots + M_m u_m = 1$ の解 $u_1, \ldots, u_m$ が存在する．

14

証明（続き）

- $a_i x \equiv b_i \pmod{p_i}$ の特殊解 $x = x_{i0}$，一般解 $x \equiv x_{i0} \pmod{p_i}$
- $M_i = p_1 \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_m$
- $M_1 u_1 + \ldots + M_m u_m = 1$

$p_i \mid M_j$ $(i \ne j)$ だから，

$$M_1 u_1 (x_{i0} - x_{10}) + \ldots + M_{i-1} u_{i-1} (x_{i0} - x_{i-1,\,0}) + M_{i+1} u_{i+1} (x_{i0} - x_{i+1,\,0}) + \ldots + M_m u_m (x_{i0} - x_{m0}) \equiv 0 \pmod{p_i}.$$

ここで，$x_0 = M_1 u_1 x_{10} + \ldots + M_m u_m x_{m0}$ とおくと，

$$(M_1 u_1 + \ldots + M_{i-1} u_{i-1} + M_{i+1} u_{i+1} + \ldots + M_m u_m) x_{i0} \equiv x_0 - M_i u_i x_{i0} \pmod{p_i}.$$

すなわち，$x_0 \equiv (M_1 u_1 + \ldots + M_m u_m) x_{i0} = x_{i0} \pmod{p_i}$．
ゆえに，x_0 は合同方程式 $a_i x \equiv b_i \pmod{p_i}$ の解である．
i は任意だから，x_0 は連立合同方程式の解である．

15

定理（連立合同方程式の解の全体）

次の(1)，(2)が成り立ち，

(1)　任意の i に対して，$\gcd(a_i, p_i) = 1$．

(2)　任意の i, j $(i \ne j)$ に対して，$\gcd(p_i, p_j) = 1$．

かつ，連立 1 次合同方程式

$$\begin{cases} a_1 x \equiv b_1 \pmod{p_1} \\ \quad \vdots \\ a_m x \equiv b_m \pmod{p_m} \end{cases}$$

の解のひとつ（特殊解）を $x = x_0$ とすると，
$x \in \mathbf{Z}$ が解であるとき，かつそのときに限り，$x \equiv x_0 \pmod{M}$．
ただし，$M = p_1 \cdot \ldots \cdot p_m$．

- 一般解は，$x \equiv x_0 \pmod{M}$ と表せる．

16

証明

(1)，(2)が成り立ち，かつ，$a_i x \equiv b_i \pmod{p_i}$ $(1 \le i \le m)$ の特殊解が $x = x_0$ であるとき，$x \in \mathbf{Z}$ が解であるならば，かつそのときに限り，$x \equiv x_0 \pmod{M}$．ただし，$M = p_1 \cdot \ldots \cdot p_m$．

- a)「$x \equiv x_0 \pmod{M}$ ならば，x は解である」を示す．
- b)「x が解であるならば，$x \equiv x_0 \pmod{M}$」を示す．

---

a) $x \equiv x_0 \pmod{M}$ とする．
このとき，$M \mid x - x_0$ だから，$p_i \mid x - x_0$．
また，x_0 は特殊解だから，$a_i x_0 \equiv b_i \pmod{p_i}$．
ゆえに，$p_i \mid a_i x_0 - b_i$．
$a_i x - b_i = (a_i x_0 - b_i) + a_i (x - x_0)$ だから，$p_i \mid a_i x - b_i$．
ゆえに，$a_i x \equiv b_i \pmod{p_i}$ だから，x は解である．

17

証明（続き）

(1)，(2)が成り立つとき，連立 1 次合同方程式 $a_i x \equiv b_i \pmod{p_i}$ $(1 \le i \le m)$ の特殊解が $x = x_0$ ならば，一般解は $x \equiv x_0 \pmod{M}$ と表せる．ただし，$M = p_1 \cdot \ldots \cdot p_m$．

- b)「解 x は $x \equiv x_0 \pmod{M}$ を満たす」を示す．

---

b) 一般解を x とすると，$a_i x \equiv b_i \pmod{p_i}$．
x_0 は特殊解だから，$a_i x_0 \equiv b_i \pmod{p_i}$．
ゆえに，$a_i (x - x_0) \equiv 0 \pmod{p_i}$ だから，$p_i \mid a_i (x - x_0)$．
ところが，$\gcd(a_i, p_i) = 1$ だから，$p_i \mid x - x_0$．
一方，任意の i, j $(i \ne j)$ に対して，$\gcd(p_i, p_j) = 1$ だから，
$p_1 \cdot \ldots \cdot p_m \mid x - x_0$．
すなわち，$M \mid x - x_0$ だから，$x \equiv x_0 \pmod{M}$．

18

中国剰余定理（Chinese Remainder Theorem）

連立 1 次合同方程式

$$\begin{cases} x \equiv b_1 & (\mathrm{mod}\ p_1) \\ \quad\vdots & \\ x \equiv b_m & (\mathrm{mod}\ p_m) \end{cases}$$

に対して，次の(1)，(2)が成り立つ．

(1)任意の i, j ($1 \leq i \leq m$, $1 \leq j \leq m$, $i \neq j$) に対して，
$\gcd(p_i, p_j) = 1$ ならば，解が存在する．

(2)特殊解を $x = x_0$ とすると，$x \in \mathbf{Z}$ が解であるとき，
かつそのときに限り，$x \equiv x_0 \pmod{M}$．ただし，$M = p_1 \cdot \ldots \cdot p_m$．

- 一般解は $x \equiv x_0 \pmod{M}$ と表せる．

- 定理より明らか（$a_1 = \ldots = a_m = 1$ の場合）．

19

連立合同方程式の解法

例：（百五減算）

$$\begin{cases} x \equiv 1 & (\mathrm{mod}\ 3) \\ x \equiv 2 & (\mathrm{mod}\ 5) \\ x \equiv 3 & (\mathrm{mod}\ 7) \end{cases}$$

- 解法1：　連立 1 次不定方程式を解く
  - $\begin{cases} x - 3u = 1 & \ldots (1) \\ x - 5v = 2 & \ldots (2) \\ x - 7w = 3 & \ldots (3) \end{cases}$
  - (1)，(2)から，$3u - 5v = 1$
    $3u - 5v = 3(u - v) - 2v$
    $= 3s - 2v$　　$s = u - v$
    $= -2(-t + v) + s$
    $= -2t + s$　　$t = -s + v$
    $-2t + s = 1$だから，$s = 1 + 2t$.
    ゆえに，$v = t + s = t + (1 + 2t) = 3t + 1$

20

連立合同方程式の解法（続き）

- 解法1（続き）：　連立 1 次不定方程式を解く
  - $\begin{cases} x - 3u = 1 & \ldots (1) \\ x - 5v = 2 & \ldots (2) \\ x - 7w = 3 & \ldots (3) \end{cases}$
  - (2)，(3)から，$5v - 7w = 1$
    $v = 3t + 1$ だから，$5v - 7w = 5(3t + 1) - 7w = 15t - 7w + 5$
    ゆえに，$15t - 7w = -4$
    $15t - 7w = -7(-2t + w) + t$
    $= -7k + t$　　$k = -2t + w$
    $-7k + t = -4$ だから，$t = 7k - 4$.
    ゆえに，$w = k + 2t = k + 2(7k - 4) = 15k - 8$.
    $x = 3 + 7w = 3 + 7(15k - 8) = 105k - 53 \equiv -53 \equiv 52 \pmod{105}$.

21

連立合同方程式の解法（続き2）

例：（百五減算）

$x \equiv 1 \pmod 3$，　$x \equiv 2 \pmod 5$，　$x \equiv 3 \pmod 7$

- 解法2：　中国剰余定理を用いて解く
  - 法は互いに素だから，中国剰余定理から，解が存在する．

  - 各合同方程式の特殊解　$x_1 = 1$, $x_2 = 2$, $x_3 = 3$
  - $M_1 = p_2 p_3 = 35$,　$M_2 = p_1 p_3 = 21$,　$M_3 = p_1 p_2 = 15$
  - 不定方程式　$35u_1 + 21u_2 + 15u_3 = 1$　の特殊解
    $35u_1 + 21u_2 + 15u_3 = 15(2u_1 + u_2 + u_3) + 5u_1 + 6u_2$
    $= 15s + 5u_1 + 6u_2$　　$s = 2u_1 + u_2 + u_3$
    $= 5(3s + u_1 + u_2) + u_2$
    $= 5t + u_2$　　$t = 3s + u_1 + u_2$
    $5t + u_2 = 1$ だから，$u_2 = 1 - 5t$.
    ゆえに，$u_1 = t - 3s - u_2 = t - 3s - (1 - 5t) = 6t - 3s - 1$.
    $u_3 = s - 2\,u_1 - u_2 = s - 2(6t - 3s - 1) - (1 - 5t) = 7s - 7t + 1$.
    $t = s = 0$ とおくと，特殊解は $u_1 = -1$, $u_2 = 1$, $u_3 = 1$.

22

連立合同方程式の解法（続き3）

例：（百五減算）

$x \equiv 1 \pmod 3$，　$x \equiv 2 \pmod 5$，　$x \equiv 3 \pmod 7$

- 解法2（続き）：　中国剰余定理を用いて解く
  - 各合同方程式の特殊解　$x_1 = 1$, $x_2 = 2$, $x_3 = 3$
  - $M = p_1 p_2 p_3 = 105$
  - $M_1 = p_2 p_3 = 35$,　$M_2 = p_1 p_3 = 21$,　$M_3 = p_1 p_2 = 15$
  - 不定方程式　$35u_1 + 21u_2 + 15u_3 = 1$　の特殊解 $u_1 = -1$, $u_2 = 1$, $u_3 = 1$.

  - 連立合同方程式の特殊解
    $x_0 = M_1 u_1 x_1 + M_2 u_2 x_2 + M_3 u_3 x_3$
    $= 35 \cdot (-1) \cdot 1 + 21 \cdot 1 \cdot 2 + 15 \cdot 1 \cdot 3 = 52$
  - 連立合同方程式の一般解
    $x \equiv 52 \pmod{105}$

23

連立合同方程式の解法（続き4）

例：（百五減算）

$x \equiv 1 \pmod 3$，　$x \equiv 2 \pmod 5$，　$x \equiv 3 \pmod 7$

- 解法3：　合同式の性質を用いて解く
  - $\mathrm{lcm}(3, 5, 7) = 105$
  - $x \equiv 1 \pmod 3$だから，$35x \equiv 35 \pmod{105}$
    - $p \in \mathbf{Z}$ が存在して，$x - 1 = p \cdot 3$ だから，$35x - 35 = p \cdot 3 \cdot 35 = p \cdot 105$
    $x \equiv 2 \pmod 5$だから，$21x \equiv 42 \pmod{105}$
    $x \equiv 3 \pmod 7$だから，$15x \equiv 45 \pmod{105}$
  - $21x + 15x - 35x \equiv 42 + 45 - 35 \pmod{105}$
  - ゆえに，$x \equiv 52 \pmod{105}$

24

定理（復習）

$p \in \mathbf{Z}$ を法とする合同関係は $\mathbf{Z}$ 上の同値関係である.

すなわち，次の(1)～(3)が成り立つ.

(1)　任意の $m \in \mathbf{Z}$ に対して，$m \equiv m \pmod{p}$.

(2)　任意の $m, n \in \mathbf{Z}$ に対して，
$m \equiv n \pmod{p}$ならば，$n \equiv m \pmod{p}$.

(3)　任意の $m, n, l \in \mathbf{Z}$ に対して，
$m \equiv n \pmod{p}$かつ $n \equiv l \pmod{p}$ ならば，
$m \equiv l \pmod{p}$.

25

剰余類（residue class）

- $p \in \mathbf{Z}$ を法とする剰余類
  - $[n]_p = \{ x \in \mathbf{Z} \mid n \equiv x \pmod{p} \}$
  - p を法とする合同関係 $\equiv_p$ ($\subseteq \mathbf{Z}^2$) による n の同値類
  - n …　剰余類 $[n]_p$ の代表元(representative element)

例：　$p=3$

- $[0]_3 = [3]_3 = [6]_3 = \cdots = \{ \ldots, -6, -3, 0, 3, 6, \ldots \}$
  $[1]_3 = [4]_3 = [-2]_3 = \cdots = \{ \ldots, -5, -2, 1, 4, \ldots \}$
  $[2]_3 = [5]_3 = [-1]_3 = \cdots = \{ \ldots, -4, -1, 2, 5, \ldots \}$

26

剰余類系（residue class system）

- $p \in \mathbf{Z}$ を法とする剰余類系 $\mathbf{Z}/\equiv_p$
  - $\mathbf{Z}/\equiv_p = \{ [n]_p \mid n \in \mathbf{Z} \}$
  - p を法とするすべての剰余類からなる集合
  - $\mathbf{Z}$ 上の p を法とする合同関係 $\equiv_p$ による同値分割（商集合）
- $| \mathbf{Z}/\equiv_p | = | p |$

例：　$p=3$

- $\mathbf{Z}/\equiv_3 = \{ [0]_3, [1]_3, [2]_3 \}$
  $= \{ [3]_3, [-2]_3, [2]_3 \} = \cdots$
  $= \{ \{ \ldots, -6, -3, 0, 3, 6, \ldots \},$
  $\{ \ldots, -5, -2, 1, 4, \ldots \},$
  $\{ \ldots, -4, -1, 2, 5, \ldots \} \}$

27

完全剰余系（complete residue system）

- $p \in \mathbf{Z}$ を法とする完全剰余系（完全代表系）$\mathbf{Z}_p$
  - $\mathbf{Z}_p = \{ n_i \mid \mathbf{Z}/\equiv_p = \{ [n_0]_p, \ldots, [n_{p-1}]_p \}, \ 0 \le i \le p-1 \}$
  - p を法とするすべての剰余類の代表元からなる集合
  - $\mathbf{Z}_p = \{ n \mid 0 \le n \le p-1 \}$ とすることが多い.

例：　$p=3$

- $\mathbf{Z}/\equiv_3 = \{ [0]_3, [1]_3, [2]_3 \}$
  - $\mathbf{Z}_3 = \{ 0, 1, 2 \}$
- $\mathbf{Z}/\equiv_3 = \{ [3]_3, [-2]_3, [2]_3 \}$
  - $\mathbf{Z}_3 = \{ 3, -2, 2 \}$

28

既約剰余類（reduced residue class）

- $p \in \mathbf{Z}$ を法とする既約剰余類
  - $[n]_p = \{ x \in \mathbf{Z} \mid n \equiv x \pmod{p}, \ \gcd(n, p) = 1 \}$
  - p と互いに素である n の剰余類

例：　$p=3$

- …, $[-2]_3$, $[-1]_3$, $[1]_3$, $[2]_3$, $[4]_3$, …

29

既約剰余系（reduced residue system）

- $p \in \mathbf{Z}$ を法とする既約剰余系（既約代表系）
  - $X_p = \{ n_i \mid \mathbf{Z}/\equiv_p = \{ [n_0]_p, \ldots, [n_{p-1}]_p \},$
    $\gcd(n_i, p) = 1, \quad 0 \le i \le p-1 \}$
  - p を法とするすべての既約剰余類の代表元からなる集合
  - $X_p = \{ n \mid 1 \le n \le p, \ \gcd(n, p) = 1 \}$ とすることが多い.

例：

- $\mathbf{Z}/\equiv_3 = \{ [0]_3, [1]_3, [2]_3 \}$
  - $X_3 = \{ 1, 2 \}$
- $\mathbf{Z}/\equiv_3 = \{ [3]_3, [-2]_3, [2]_3 \}$
  - $X_3 = \{ -2, 2 \}$

30

Euler 関数

- Euler 関数 $\varphi : \mathbf{N} \to \mathbf{N}$
  - $p \in \mathbf{N}$ に対して, $\varphi(p) = |X_p|$
  - $\varphi(p) = |\{n_i \mid \mathbf{Z}/\equiv_p = \{[n_0]_p, \ldots, [n_{p-1}]_p\}, \gcd(n, p) = 1\}|$
    $= |\{[n]_p \in \mathbf{Z}/\equiv_p \mid \gcd(n, p) = 1\}|$
    $= |\{n \mid 1 \le n \le p, \gcd(n, p) = 1\}|$

例:

- $X_1 = \{1\}$, $\varphi(1) = 1$
- $X_2 = \{1\}$, $\varphi(2) = 1$
- $X_3 = \{1, 2\}$, $\varphi(3) = 2$
- $X_4 = \{1, 3\}$, $\varphi(4) = 2$
- $X_5 = \{1, 2, 3, 4\}$, $\varphi(5) = 4$

31

定理

任意の素数 p, 任意の $m, n, e \in \mathbf{N}$ に対して, 次の(1)～(4)が成り立つ.

(1) $\varphi(p) = p - 1$
(2) $\varphi(p^e) = p^e - p^{e-1}$
(3) $\gcd(m, n) = 1$ ならば, $\varphi(mn) = \varphi(m)\varphi(n)$
(4) n の素因数分解が $n = p_1^{e1} \cdot \ldots \cdot p_r^{er}$ であるならば,
$\varphi(n) = n(1 - 1/p_1) \cdot \ldots \cdot (1 - 1/p_r)$

32

証明

任意の素数 p, 任意の $m, n, e \in \mathbf{N}$ に対して,
(1) $\varphi(p) = p - 1$
(2) $\varphi(p^e) = p^e - p^{e-1}$

---

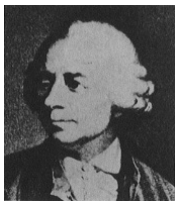
(1) $X_p = \{1, 2, \ldots, p-1\}$ だから, $\varphi(p) = |X_p| = p - 1$.
(2) $\gcd(p, n) \neq 1$ となる $n \in \mathbf{N}$ $(1 \le n \le p^e)$ は p の倍数である.
すなわち, $n \in \{1 \cdot p, 2 \cdot p, \ldots, p^{e-1} \cdot p\}$ だから,
そのような n は p^{e-1} 個ある.
ゆえに, $\varphi(p^e) = p^e - p^{e-1}$.

33

Euler の定理

任意の $n \in \mathbf{N}$ と任意の $a \in \mathbf{Z}$ に対して,
$\gcd(n, a) = 1$ ならば, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

例: $n = 12$, $a = 7$
$\gcd(12, 7) = 1$
$X_{12} = \{1, 5, 7, 11\}$, $\varphi(12) = 4$
$7^{\varphi(12)} = 7^4 = 2{,}401 \equiv 1 \pmod{12}$

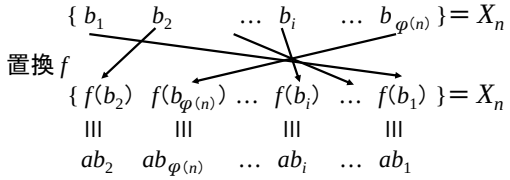


L. Euler
(スイス→露,
1707-1783)

34

補題

$n \in \mathbf{N}$ を法とする既約剰余系 $X_n = \{b_1, \ldots, b_{\varphi(n)}\}$ と
$a \in \mathbf{Z}$ に対して, X_n 上の関係 f を
$(b_i, b_j) \in f$ iff $ab_i \equiv b_j \pmod{n}$
で定めるとき, $\gcd(n, a) = 1$ ならば,
f は X_n 上の全単射, すなわち置換である.



35

Euler の定理の証明

任意の $n \in \mathbf{N}$ と任意の $a \in \mathbf{Z}$ に対して,
$\gcd(n, a) = 1$ ならば, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

補題より, $X_n = \{b_1, \ldots, b_{\varphi(n)}\}$ 上の置換 f が存在して,
$ab_i \equiv f(b_i) \pmod{n}$.
ゆえに, $b_1 \cdot \ldots \cdot b_{\varphi(n)} = f(b_1) \cdot \ldots \cdot f(b_{\varphi(n)})$
$\equiv (ab_1) \cdot \ldots \cdot (ab_{\varphi(n)}) \pmod{n}$
すなわち, $b_1 \cdot \ldots \cdot b_{\varphi(n)} \equiv a^{\varphi(n)} \cdot b_1 \cdot \ldots \cdot b_{\varphi(n)} \pmod{n}$.
任意の i $(1 \le i \le \varphi(n))$ に対して, $\gcd(b_i, n) = 1$ だから,
$1 \equiv a^{\varphi(n)} \pmod{n}$.

36

補題の証明

既約剰余系 $X_n=\{b_1, \ldots, b_{\varphi(n)}\}$ と $a\in\mathbf{Z}$ に対して，
X_n 上の関係 f を $(b_i, b_j)\in f$ iff $ab_i\equiv b_j \pmod n$ で定めるとき，
$\gcd(p, a)=1$ ならば，f は X_p 上の全単射である．

- a)「f は関数である」を示す．
- b)「f は単射である」を示す．
- c)「f は全射である」を示す．
- a)「任意の $b_i\in X_p$ に対して，$b_j\in X_n$ が唯一存在して，$(b_i, b_j)\in f$」を示す．
- a)「任意の $b_i\in X_p$ に対して，$b_j\in X_n$ が唯一存在して，$ab_i\equiv b_j \pmod n$」を示す．
- a-1)「任意の $b_i\in X_n$ に対して，$b_j\in X_n$ が存在して，$ab_i\equiv b_j \pmod n$」を示す．
- a-2)「任意の $b_i\in X_n$ に対して，$b_j\in X_n$ が唯一存在して，$ab_i\equiv b_j \pmod n$」を示す．

37

補題の証明（続き）

既約剰余系 $X_p=\{b_1, \ldots, b_{\varphi(n)}\}$ と $a\in\mathbf{Z}$ に対して，
X_n 上の関係 f を $(b_i, b_j)\in f$ iff $ab_i\equiv b_j \pmod n$ で定めるとき，
$\gcd(n, a)=1$ ならば，f は X_p 上の全単射である．

- a)「f は関数である」を示す．
  - a-1)「任意の $b_i\in X_n$ に対して，$b_j\in X_n$ が存在して，$ab_i\equiv b_j \pmod n$」を示す．
  - a-2)「任意の $b_i\in X_n$ に対して，$b_j\in X_n$ が唯一存在して，$ab_i\equiv b_j \pmod n$」を示す．

---

a-1) 任意の $b_i\in X_n$ に対して，$\gcd(n, a)=1$，$\gcd(n, b_i)=1$ だから，
$\gcd(n, ab_i)\neq 1$．
ゆえに，$ab_i\equiv 0 \pmod n$ だから，$b_j\in X_n$ が存在して，
$ab_i\equiv b_j \pmod n$．

38

補題の証明（続き2）

既約剰余系 $X_p=\{b_1, \ldots, b_{\varphi(n)}\}$ と $a\in\mathbf{Z}$ に対して，
X_p 上の関係 f を $(b_i, b_j)\in f$ iff $ab_i\equiv b_j \pmod n$ で定めるとき，
$\gcd(n, a)=1$ ならば，f は X_n 上の全単射である．

- a)「f は関数である」を示す．
  - a-1)「任意の $b_i\in X_n$ に対して，$b_j\in X_n$ が存在して，$ab_i\equiv b_j \pmod n$」を示す．
  - a-2)「任意の $b_i\in X_n$ に対して，$b_j\in X_n$ が唯一存在して，$ab_i\equiv b_j \pmod n$」を示す．

---

a-2) 任意の $b_i\in X_n$ に対して，
$ab_i\equiv b_j \pmod n$ かつ $ab_i\equiv b_j' \pmod n$ と仮定する．
このとき，$b_j\equiv b_j' \pmod n$．
$b_j, b_j'\in X_n$ だから，$b_j=b_j'$．
ゆえに，任意の $b_i\in X_n$ に対して，$b_j\in X_n$ が唯一存在して，
$ab_i\equiv b_j \pmod n$．

39

補題の証明（続き3）

既約剰余系 $X_p=\{b_1, \ldots, b_{\varphi(n)}\}$ と $a\in\mathbf{Z}$ に対して，
X_n 上の関係 f を $(b_i, b_j)\in f$ iff $ab_i\equiv b_j \pmod n$ で定めるとき，
$\gcd(n, a)=1$ ならば，f は X_n 上の全単射である．

- b)「f は単射である」を示す．
- c)「f は全射である」を示す．

---

b) $b_i, b_i'\in X_n$ に対して，$f(b_i)=f(b_i')$ と仮定する．
このとき，$ab_i\equiv f(b_i)$，$ab_i'\equiv f(b_i') \pmod n$ だから，
$ab_i\equiv ab_i' \pmod n$．
$\gcd(n, a)=1$ だから，$b_i\equiv b_i' \pmod n$．
$b_i, b_i'\in X_n$ だから，$b_j=b_i'$．
ゆえに，f は単射である．
c) X_n は有限集合で，f は X_n 上の単射だから，f は全射である．

40

Fermat の小定理（1640）

任意の素数 p と任意の $a\in\mathbf{Z}$ に対して，
$a\not\equiv 0 \pmod p$ ならば，$a^{p-1}\equiv 1 \pmod p$．

例：$6^{19-1}=6^{18}\equiv 1 \pmod{19}$

- $p=19$（素数），$a=6$
- $\gcd(p, a)=\gcd(19, 6)=1$　（$6\not\equiv 0 \pmod{19}$）

- Euler の定理より明らか．
  - 任意の $p\in\mathbf{N}$ と任意の $a\in\mathbf{Z}$ に対して，
    $\gcd(p, a)=1$ ならば，$a^{\varphi(p)}\not\equiv 1 \pmod p$．
  - p が素数のとき，
    - $\gcd(p, a)=1$　iff　$p\nmid a$ でない．
      iff　$a\not\equiv 0 \pmod p$
    - $\varphi(p)=p-1$．

P. de Fermat
（仏，1601-1665）

41

位数（order）

- 素数 p を法とする $a\in\mathbf{Z}$（$a\not\equiv 0 \pmod p$）の位数
  - $a^d\equiv 1 \pmod p$ となる最小の $d\in\mathbf{N}$

例：$p=7$，$a=2$

- $2^1\equiv 2 \pmod 7$
- $2^2\equiv 4 \pmod 7$
- $2^3\equiv 1 \pmod 7$　…　位数 $d=3$
- $2^4\equiv 2 \pmod 7$
- $2^5\equiv 4 \pmod 7$
- $2^6\equiv 1 \pmod 7$　…　Fermat の小定理 $p-1=6$

- Fermat の小定理から，$d\leq p-1$．

42

原始根（primitive root）

- 素数 p を法とする原始根
  - 位数 $d=p-1$ となる $a\in\mathbf{Z}$ （$a\not\equiv 0 \pmod p$）

例：$p=7$ のとき，$a=3$
- $3^1\equiv 3 \pmod 7$
- $3^2\equiv 2 \pmod 7$
- $3^3\equiv 6 \pmod 7$
- $3^4\equiv 4 \pmod 7$
- $3^5\equiv 5 \pmod 7$
- $3^6\equiv 1 \pmod 7$ … 位数 $d=6$，Fermat の小定理

例：（教科書p.145　表3.4）
- $p=2$ のとき，原始根 $a=1$　　$1^{2-1}\equiv 1 \pmod 2$
- $p=3$ のとき，原始根 $a=2$　　$2^{3-1}\equiv 1 \pmod 3$
- $p=5$ のとき，原始根 $a=2$　　$2^{5-1}\equiv 1 \pmod 5$

定理

任意の素数 p に対して，p を法とする原始根が存在する．

定理

素数 p を法とする原始根 $a\in\mathbf{Z}$ に対して，
$\{1, a, a^2, \ldots, a^{p-2}\}$
は，p を法とする既約剰余系である．

- 素数 p と任意の $x\in\mathbf{Z}(x\not\equiv 0 \pmod p)$ に対して，
  $i\in\mathbf{N}_0(0\leq i\leq p-2)$が存在して，$x\equiv a^i \pmod p$．

例：
- $p=3, a=2$ … $\{1, 2, 2^1\}=\{1, 2\}=X_2$
- $p=7, a=3$ … $\{1, 3, 3^2, 3^3, 3^4, 3^5\}=X_7$
  - $3^2\equiv 2,\ 3^3\equiv 6,\ 3^4\equiv 4,\ 3^5\equiv 5$
    $\{1, 2, 3, 4, 5, 6\}=X_7$

証明

素数 p を法とする原始根$a\in\mathbf{Z}$に対して，$\{1, a, a^2, \ldots, a^{p-2}\}$は，$p$ を法とする既約剰余系である．
- $|\{1, a, a^2, \ldots, a^{p-2}\}| = p-1 = |X_p|$
- a)「任意の a^i は既約剰余類の代表元である」を示す．
- b)「任意の $a^i, a^j (i\neq j)$に対して，$a^i\not\equiv a^j \pmod p$」を示す．

---

a) $a\not\equiv 0 \pmod p$だから，$p\nmid a$ でない．
ここで，p は素数だから，$\gcd(p, a)=1$．
したがって，$\gcd(p, a^i)=1$．
$a^i\in\mathbf{Z}$ だから，$[a^i]_p\in\mathbf{Z}_p$．
ゆえに，a^i は p を法とする既約剰余類の代表元である．

証明（続き）

素数 p を法とする原始根$a\in\mathbf{Z}$に対して，$\{1, a, a^2, \ldots, a^{p-2}\}$は，$p$ を法とする既約剰余系である．
- $|\{1, a, a^2, \ldots, a^{p-2}\}| = p-1 = |X_p|$
- a)「任意の a^i は既約剰余類の代表元である」を示す．
- b)「任意の $a^i, a^j (i\neq j)$に対して，$a^i\not\equiv a^j \pmod p$」を示す．

---

b) 任意の $a^i, a^j (0\leq i<j<p-1)$に対して，$a^i\equiv a^j \pmod p$ と仮定する．
$\gcd(p, a)=1$ だから，$1\equiv a^{j-i} \pmod p$．
ここで，$0\leq i<j<p-1$ だから，$0<j-i<p-1$．
$p-1$ は a の位数だから，これは矛盾．
ゆえに，$a^i\not\equiv a^j \pmod p$．

まとめ

- 今回の講義
  - 合同式（続き）
- 次回の講義（6／26）
  - 多項式（教科書　pp.151-156）
  - 環（教科書　pp.157-161）
- 次回の演習（6／19）
  - （1限）素数
  - （1限）1次不定方程式
  - （2限）合同式
- 今回の演習
  - なし