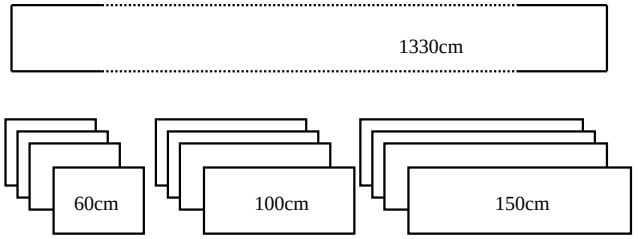
離散数学及び演習
講義 8　2014. 6.12(木)1限

1 次不定方程式
(教科書　pp.117-127)
合同式
(教科書　pp.127-131)

教科書･･･野崎昭弘:離散系の数学、近代科学社

問題

長さ 60cm, 100cm, 150cm の鉄板を使って,
長さ1330cm の溝を覆うためには, どの鉄板を
何枚使えばよいか？



2

問題の定式化

長さ 60cm, 100cm, 150cm の鉄板の枚数をそれぞれ
x, y, z とすると,
$60x+100y+150z=1330$
の非負整数解を求める.

解1　$x=8$, $y=1$, $z=5$
解2　$x=13$, $y=4$, $z=1$
解3　$x=8$, $y=4$, $z=3$
解4　$x=3$, $y=4$, $z=5$
：

3

1 次不定方程式

- 係数 $a_1, a_2, \ldots, a_n, b \in \mathbf{Z}$, 変数 $x_1, x_2, \ldots, x_n \in \mathbf{Z}$ についての(n 元)1 次不定方程式
  (indeterminate equation)
  - $a_1x_1+a_2x_2+\ldots+a_nx_n=b$
  - 1 次不定方程式の解　…　整数解

4

定理(復習)

- 任意の $m, n \in \mathbf{Z}$ に対して, $x, y \in \mathbf{Z}$ が存在して,
  $mx+ny=\gcd(m, n)$.

例:　$\gcd(10, 15)=5=10\cdot(-1)+15\cdot 1$
　　$\gcd(30, 77)=1=30\cdot 18+77\cdot(-7)$

- 任意の $a_1, a_2, \ldots, a_n \in \mathbf{Z}$ に対して,
  $x_1, x_2, \ldots, x_n \in \mathbf{Z}$ が存在して,
  $a_1x_1+a_2x_2+\ldots+a_nx_n=\gcd(a_1, a_2, \ldots, a_n)$.

5

定理(1 次不定方程式の解の存在)

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

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

6

証明

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

- a)「$x, y \in \mathbf{Z}$ が存在して，$mx+ny=k$ ならば，$\gcd(m, n) \mid k$ 」を示す.
- b)「$\gcd(m, n) \mid k$ ならば，$x, y \in \mathbf{Z}$ が存在して，$mx+ny=k$ 」を示す.

---

a)　$x, y \in \mathbf{Z}$ が存在して，$mx+ny=k$ と仮定する.
$\gcd(m, n) \mid m$ かつ $\gcd(m, n) \mid n$ だから，$\gcd(m, n) \mid mx+ny$.
すなわち，$\gcd(m, n) \mid k$.

b)　$\gcd(m, n) \mid k$ と仮定する.
このとき，$q \in \mathbf{Z}$ が存在して，$k=q \cdot \gcd(m, n)$.
一方，定理から，$x', y' \in \mathbf{Z}$ が存在して，$mx'+ny' = \gcd(m, n)$.
ゆえに，$k=q(mx'+ny') = mqx'+nqy'$.
ここで，$x=qx'$, $y=qy'$ とおくと，$x, y \in \mathbf{Z}$ であり，$mx+ny=k$.

系（1 次不定方程式の解の存在）

任意の $m, n \in \mathbf{Z}$ に対して，$\gcd(m, n)=1$ ならば，$x, y \in \mathbf{Z}$ が存在して，$mx+ny=k$.

- 「任意の $m, n \in \mathbf{Z}$ に対して，$\gcd(m, n) \mid k$ ならば，$x, y \in \mathbf{Z}$ が存在して，$mx+ny=k$」から明らか.

定理（1 次不定方程式の解の全体）

$\gcd(m, n) \mid k$, かつ，1 次不定方程式 $mx+ny=k$ の解のひとつ（特殊解）を x_0, y_0 とすると，
$x, y \in \mathbf{Z}$ が解であるとき，かつそのときに限り，

$$x = x_0 + \frac{n}{d} q$$

$$y = y_0 - \frac{m}{d} q \qquad (q \in \mathbf{Z}).$$

ただし，$d=\gcd(m, n)$.

- 一般解は上記のように表せる.
  - 1 次不定方程式は，解が存在するならば，解は無数に存在する.

証明

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

- a)「$x=x_0+(n/d)q$, $y=y_0-(m/d)q$ ならば，x, y は解である」を示す.
- b)「x, y が解であるならば，$x=x_0+(n/d)q$, $y=y_0-(m/d)q$ 」を示す.

---

a)　$x=x_0+(n/d)q$, $y=y_0-(m/d)q$ とすると，

$$\begin{aligned} mx+ny &= m(x_0+(n/d)q)+n(y_0-(m/d)q) \\ &= mx_0+ny_0 \\ &= k \end{aligned}$$

だから，x, y は解である.

証明

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

- b)「x, yが解であるならば，$x=x_0+(n/d)q$, $y=y_0-(m/d)q$ 」を示す.

---

b)　x, y は解であるとする．このとき，$mx+ny=k$.
x_0, y_0 は特殊解だから，$mx_0+ny_0=k$.
ゆえに，$m(x-x_0)=-n(y-y_0)$.
ところで，d は m, n の最大公約数 だから，$m', n' \in \mathbf{Z}$ が存在して，
$m=m'd$, $n=n'd$ （ただし，$\gcd(m', n')=1$ ）.
ゆえに，$m'd(x-x_0)=-n'd(y-y_0)$ だから，$n' \mid m'(x-x_0)$.
$\gcd(m', n')=1$ だから，$n' \mid x-x_0$.
このとき，$q \in \mathbf{Z}$ が存在して，$x-x_0=q \cdot n'$.
ゆえに，$x=x_0+n' \cdot q = x_0+(n/d)q$.
また，$-n'd(y-y_0)=m'd(x-x_0)=m'dqn'$ だから，$y-y_0=-m'q$.
ゆえに，$y=y_0-(m/d)q$.

1 次不定方程式の解法

- 入力：　$m, n, q \in \mathbf{Z}$　$(m>n)$
- 出力：　$mx+ny = q \cdot \gcd(m, n)$ の整数解 x, y
- 手順：　$mx+ny$

$$\begin{aligned} &= (q_1 n+r_1)x+ny && m=q_1 \cdot n+r_1 \\ &= n(q_1 x+y)+r_1 x && \\ &= nx_1+r_1 x && x_1=q_1 x+y \\ &= (q_2 r_1+r_2)x_1+r_1 x && n=q_2 \cdot r_1+r_2 \\ &= r_1(q_2 x_1+x)+r_2 x_1 && \\ &= r_1 x_2+r_2 x_1 && x_2=q_2 x_1+x \\ &= (q_3 r_2+r_3)x_2+r_2 x_1 && r_1=q_3 \cdot r_2+r_3 \\ &= r_2(q_3 x_2+x_1)+r_3 x_2 && \\ &= r_2 x_3+r_3 x_2 && x_3=q_3 x_2+x_1 \\ &\ \ \vdots && \end{aligned}$$

1 次不定方程式の解法（続き）

- 入力：$m, n, q \in \mathbf{Z}$　$(m>n)$
- 出力：$mx+ny=q\cdot\gcd(m, n)$の整数解 x, y
- 手順：　$mx+ny$

　　：

$=(q_k r_{k-1}+r_k)x_{k-1}+r_{k-1}x_{k-2}$　　$r_{k-2}=q_k\cdot r_{k-1}+r_k$

$=r_{k-1}(q_k x_{k-1}+x_{k-2})+r_k x_{k-1}$

$=r_{k-1}x_k+r_k x_{k-2}$　　$x_k=q_k x_{k-1}+x_{k-2}$

$=(q_{k+1}r_k)x_k+r_k x_{k-1}$　　$r_{k-1}=q_{k+1}\cdot r_k+0$

$=r_k(q_{k+1}x_k+x_{k-1})$

$=r_k x_{k+1}$　　$x_{k+1}=q_{k+1}x_k+x_{k-1}$

ゆえに，$r_k x_{k+1}=q\cdot\gcd(m, n)$

Euclid の互除法より，$r_k=\gcd(m, n)$だから，$x_{k+1}=q$.

1 次不定方程式の解法（続き2）

- 入力：$m, n, q \in \mathbf{Z}$　$(m>n)$
- 出力：$mx+ny=q\cdot\gcd(m, n)$の整数解 x, y
- 手順：　$x_{k+1}=q_{k+1}x_k+x_{k-1}=q$
  - 特殊解　$x_k=0$ とおく.

$x_{k-1}=x_{k+1}-q_{k+1}x_k$　　$=q$

$x_{k-2}=x_k-q_k x_{k-1}$　　$=-q_k q$

$x_{k-3}=x_{k-1}-q_{k-1}x_{k-2}$　　$=q-q_{k-1}(-q_k q)$

　　：

$x_1=x_3-q_3 x_2$

$x=x_2-q_2 x_1$

$y=x_1-q_1 x$

1 次不定方程式の解法（続き3）

- 入力：$m, n, q \in \mathbf{Z}$　$(m>n)$
- 出力：$mx+ny=q\cdot\gcd(m, n)$の整数解 x, y
- 手順：　$x_{k+1}=q_{k+1}x_k+x_{k-1}=q$
  - 一般解　$x_k=u$ とおく.　（u … パラメータ）

$x_{k-1}=x_{k+1}-q_{k+1}x_k$　　$=q-q_{k+1}u$

$x_{k-2}=x_k-q_k x_{k-1}$　　$=u-q_k(q-q_{k+1}u)$

$x_{k-3}=x_{k-1}-q_{k-1}x_{k-2}$　　$=\cdots$

　　：

$x_1=x_3-q_3 x_2$

$x=x_2-q_2 x_1$

$y=x_1-q_1 x$

1 次不定方程式の解法（続き4）

例：　$14x-6y=4$ の整数解 x, y

$14x-6y=((-2)\cdot(-6)+2)x+(-6)y$　　$14=(-2)\cdot(-6)+2$

$=(-6)(-2x+y)+2x$

$=-6x_1+2x$　　$x_1=(-2)x+y$

$=((-3)\cdot 2)x_1+2x$　　$-6=(-3)\cdot 2+0$

$=2(-3x_1+x)$　　$x_2=-3x_1+x$

$=2x_2$

ゆえに，$2x_2=4$ だから，$x_2=2$.

- 特殊解　$x_1=0$ とおく.

$x=x_2-(-3)x_1=2$

$y=x_1-(-2)x=4$

- 一般解　$x_1=u$ とおく.

$x=x_2-(-3)x_1=2+3u$

$y=x_1-(-2)x=u+2(2+3u)=4+7u$

1 次不定方程式の解法（続き5）

例：　$14x-6y=4$ の整数解 x, y　　絶対値最小の係数でくくる

$14x-6y$

$=(-6)(-2x+y)+2x$　← -6 でくくる

$=-6x_1+2x$　　$x_1=(-2)x+y$

$=2(-3x_1+x)$　← 2 でくくる

$=2x_2$　　$x_2=-3x_1+x$

ゆえに，$2x_2=4$ だから，$x_2=2$.

- 特殊解　$x_1=0$ とおく.

$x=x_2-(-3)x_1=2$

$y=x_1-(-2)x=4$

- 一般解　$x_1=u$ とおく.

$x=x_2-(-3)x_1=2+3u$

$y=x_1-(-2)x=u+2(2+3u)=4+7u$

1 次不定方程式の解法（続き6）

例：　$60x+100y+150z=1330$ の整数解 x, y, z

- $6x+10y+15z=133$ の整数解を求める

$6x+10y+15z=6(x+y+2z)+4y+3z$　← 6 でくくる

$=6u+4y+3z$　　$u=x+y+2z$

$=3(2u+y+z)+y$　← 3 でくくる

$=3v+y$　　$v=2u+y+z$

ゆえに，$3v+y=133$ だから，$y=133-3v$.

$z=v-2u-y=v-2u-(133-3v)=-2u+4v-133$

$x=u-y-2z=u-(133-3v)-2(-2u+4v-133)$

$=5u-5v+133$

- $u=19$, $v=44$ のとき，$x=8$, $y=1$, $z=5$
- $u=19$, $v=43$ のとき，$x=13$, $y=4$, $z=1$

整数を法とする合同関係（復習）

- $m, n, p \in \mathbf{Z}$ に対して，
  m と n は p を法（modulo）として合同（congruent）
  $\cdots m \equiv_p n, \quad m \equiv n \pmod{p}$
  - m と n は p で割ったときの剰余が等しい
  - $m - n$ は p の倍数
  - $p \mid m - n$

例：
- $365 \equiv 1 \pmod 7$
  - $365 - 1 = 364 = 52 \cdot 7$
- $-12 \equiv 14 \pmod{13}$
  - $-12 - 14 = -26 = -2 \cdot 13$

19

整数を法とする合同関係（続き）

- $m \equiv n \pmod{p}$
  - $p \mid m - n$
- $m \equiv 0 \pmod{p}$
  - $p \mid m$
- $m \equiv n \pmod{p}$ iff $m \equiv n \pmod{-p}$
  - $p \mid m - n$ iff $-p \mid m - n$

20

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，$m \equiv l \pmod{p}$．

21

定理

任意の $m, n, p \in \mathbf{Z}$ $(p \neq 0)$ に対して，次の(1)～(3)は同値である．

(1) $m \equiv n \pmod{p}$
(2) $k \in \mathbf{Z}$ が存在して，$m = n + k \cdot p$
(3) m を p で割ったときの剰余と
n を p で割ったときの剰余は等しい

22

証明

任意の $m, n, p \in \mathbf{Z}$ $(p \neq 0)$ に対して，次の(1)～(3)は同値である．

(1) $m \equiv n \pmod{p}$
(2) $k \in \mathbf{Z}$ が存在して，$m = n + k \cdot p$
(3) m を p で割ったときの剰余と n を p で割ったときの剰余は等しい
- a)「(1)ならば(2)」を示す．
- b)「(2)ならば(3)」を示す．
- c)「(3)ならば(1)」を示す．

---

a) $m \equiv n \pmod{p}$ と仮定する．
このとき，$p \mid m - n$．
ゆえに，$k \in \mathbf{Z}$ が存在して，$m - n = k \cdot p$．
すなわち，$m = n + k \cdot p$．

23

証明（続き）

任意の $m, n, p \in \mathbf{Z}$ $(p \neq 0)$ に対して，次の(1)～(3)は同値である．

(1) $m \equiv n \pmod{p}$
(2) $k \in \mathbf{Z}$ が存在して，$m = n + k \cdot p$
(3) m を p で割ったときの剰余と n を p で割ったときの剰余は等しい
- b)「(2)ならば(3)」を示す．

---

b) ある $k \in \mathbf{Z}$ に対して，$m = n + k \cdot p$ と仮定する．
また，m, n を p で割ったときの剰余をそれぞれ $r, r' \in \mathbf{Z}$ とする．
このとき，$q, q' \in \mathbf{Z}$ に対して，$m = q \cdot p + r$, $n = q' \cdot p + r'$
$(0 \leq r, r' < |p|)$．
ゆえに，$m = (q' \cdot p + r') + k \cdot p = q \cdot p + r$ だから，
$(q - q' - k)p - (r - r') = 0$．
$p \neq 0$ だから，$q - q' = k$, かつ，$r = r'$．
ゆえに，m を p で割ったときの剰余と n を p で割ったときの剰余は等しい．

24

証明（続き2）

任意の $m, n, p \in \mathbf{Z}\ (p \neq 0)$ に対して，次の(1)～(3)は同値である．

(1)　$m \equiv n \pmod{p}$

(2)　$k \in \mathbf{Z}$ が存在して，$m = n + k \cdot p$

(3)　m を p で割ったときの剰余と n を p で割ったときの剰余は等しい

- c)「(3)ならば(1)」を示す．

---

c)　$q, q', r \in \mathbf{Z}$ に対して，

$m = q \cdot p + r,\ n = q' \cdot p + r\ \ (0 \leq r < |p|)$ と仮定する．

このとき，$m - n = (q - q')p$．

$q - q' \in \mathbf{Z}$ だから，$p \mid m - n$．

すなわち，$m \equiv n \pmod{p}$．

定理（合同関係における加減乗算）

任意の $a, b, c, d, p \in \mathbf{Z}$ に対して，

$a \equiv b \pmod{p}$，$c \equiv d \pmod{p}$ ならば，次の(1)～(3)が成り立つ．

(1)　$a + c \equiv b + d \pmod{p}$

(2)　$a - c \equiv b - d \pmod{p}$

(3)　$ac \equiv bd \pmod{p}$

【参考】任意の $a, b, c, d \in \mathbf{Z}$ に対して，
$a = b,\ c = d$ ならば，
次の(1)～(3)が成り立つ．
(1)　$a + c = b + d$
(2)　$a - c = b - d$
(3)　$ac = bd$

例：

- $29 \equiv -1 \pmod{6}$，$13 \equiv 1 \pmod{6}$
  - $29 + 13 \equiv -1 + 1 \pmod{6}$，すなわち，$42 \equiv 0 \pmod{6}$．
  - $29 - 13 \equiv -1 - 1 \pmod{6}$，すなわち，$16 \equiv -2 \pmod{6}$．
- $25 \equiv 14 \pmod{11}$，$79 \equiv 2 \pmod{11}$
  - $25 \cdot 79 \equiv 14 \cdot 2 \pmod{11}$，すなわち，$1975 \equiv 28 \pmod{11}$．

証明

任意の $a, b, c, d, p \in \mathbf{Z}$ に対して，

$a \equiv b \pmod{p}$，$c \equiv d \pmod{p}$ ならば，

(1)　$a + c \equiv b + d \pmod{p}$

$a \equiv b \pmod{p}$，$c \equiv d \pmod{p}$だから，$q, q' \in \mathbf{Z}$ が存在して，

$a - b = q \cdot p,\ \ c - d = q' \cdot p$．

(1)　$(a + c) - (b + d) = (a - b) + (c - d)$

$= q \cdot p + q' \cdot p$

$= (q + q')p$

$q + q' \in \mathbf{Z}$ だから，$a + c \equiv b + d \pmod{p}$．

証明（続き）

任意の $a, b, c, d, p \in \mathbf{Z}$ に対して，

$a \equiv b \pmod{p}$，$c \equiv d \pmod{p}$ ならば，

(3)　$ac \equiv bd \pmod{p}$

$a \equiv b \pmod{p}$，$c \equiv d \pmod{p}$だから，$q, q' \in \mathbf{Z}$ が存在して，

$a - b = q \cdot p,\ \ c - d = q' \cdot p$．

(3)　$ac - bd = (a - b)c + b(c - d)$

$= q \cdot p \cdot c + b \cdot q' \cdot p$

$= (qc + bq')p$

$qc + bq' \in \mathbf{Z}$ だから，$ac \equiv bd \pmod{p}$．

系（合同関係における加減乗算）

任意の $a, b, c, p \in \mathbf{Z}$ に対して，$a \equiv b \pmod{p}$ならば，
次の(1)～(3)が成り立つ．

(1)　$a \pm c \equiv b \pm c \pmod{p}$

(2)　$ac \equiv bc \pmod{p}$

(3)　$a^n \equiv b^n \pmod{p}$　$(n \in \mathbf{N} \cup \{0\})$

【参考】 任意の $a, b, c \in \mathbf{Z}$ に対して，$a = b$ ならば，
次の(1)～(3)が成り立つ．
(1)　$a \pm c = b \pm c$
(2)　$ac = bc$
(3)　$a^n = b^n$　$(n \in \mathbf{N} \cup \{0\})$

証明

任意の $a, b, c, p \in \mathbf{Z}$ に対して，$a \equiv b \pmod{p}$ならば，

(1)　$a \pm c \equiv b \pm c \pmod{p}$

(2)　$ac \equiv bc \pmod{p}$

(3)　$a^n \equiv b^n \pmod{p}$　$(n \in \mathbf{N} \cup \{0\})$

---

(1)，(2)　$c \equiv c \pmod{p}$ だから，定理より明らか．

(3)　n に関する帰納法により示す．

（基底段階）　$n = 0$ のとき．

$a^0 = b^0 = 1,\ 1 \equiv 1 \pmod{p}$ だから，明らか．

（帰納段階）　$a^{n-1} \equiv b^{n-1} \pmod{p}$と仮定する．

$a \equiv b \pmod{p}$だから，定理より，$a^{n-1} \cdot a \equiv b^{n-1} \cdot b \pmod{p}$．

ゆえに，$a^n \equiv b^n \pmod{p}$．

合同関係における乗算（続き）

例：　795^{25} を11で割ったときの剰余

- $795 \equiv 3 \pmod{11}$
- $795^{25} \equiv 3^{25} \pmod{11}$

- $3^2 = 9 \equiv -2 \pmod{11}$
- $3^4 = (3^2)^2 \equiv (-2)^2 = 4 \pmod{11}$
- $3^8 = (3^4)^2 \equiv 4^2 = 16 \equiv 5 \pmod{11}$
- $3^{16} = (3^8)^2 \equiv 5^2 = 25 \equiv 3 \pmod{11}$

- $3^{25} = 3^{16} \cdot 3^8 \cdot 3^1 \equiv 3 \cdot 5 \cdot 3 = 15 \cdot 3 \equiv 4 \cdot 3 \equiv 1 \pmod{11}$
- ゆえに，$795^{25} \equiv 1 \pmod{11}$

31

合同関係の応用

任意の $a, b \in \mathbf{Z}$ に対して，$365a + b \equiv a + b \pmod{7}$

- a 年後（その間に閏日 b 回）の同じ日の曜日

例：　1979年1月1日（月）に対して，2012年1月1日（日）

- $365 \cdot 33 + 8 \equiv 33 + 1 \equiv 5 + 1 \equiv 6 \pmod{7}$
- 7で割ったときの剰余　0→月，1→火，…，6→日

$365 - 1 = 364 = 52 \cdot 7$ だから，$365 \equiv 1 \pmod{7}$

ゆえに，$365a + b \equiv a + b \pmod{7}$

32

合同関係の応用（続き）

- 九去法（casting out nines）（9で割ったときの剰余）

例：　$12{,}345{,}678 \equiv 1 + 2 + \ldots + 7 + 8 = 36 \equiv 0 \pmod{9}$

$n = (a_k a_{k-1} \ldots a_1 a_0)_{10}$

$= a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10^1 + a_0 \quad (a_i \in \mathbf{N}_0,\ 0 \leq a_i < 10)$

に対して，

$n \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod{9}$

- $9 \mid n$ iff $9 \mid a_k + a_{k-1} + \ldots + a_1 + a_0$

$10 \equiv 1 \pmod{9}$

$10^i \equiv 1^i = 1 \pmod{9}$

$a_i 10^i \equiv a_i \pmod{9}$

ゆえに，

$n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10^1 + a_0 \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod{9}$

33

合同関係の応用（続き2）

- 11で割ったときの剰余

例：　$12{,}345{,}678 \equiv -1 + 2 - 3 + 4 - 5 + 6 - 7 + 8 = 4 \pmod{11}$

$n = (a_k a_{k-1} \ldots a_1 a_0)_{10}$

$= a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10^1 + a_0 \quad (a_i \in \mathbf{N}_0,\ 0 \leq a_i < 10)$

に対して，

$n \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \ldots - a_1 + a_0 \pmod{11}$

- $11 \mid n$ iff $11 \mid (-1)^k a_k + (-1)^{k-1} a_{k-1} + \ldots - a_1 + a_0$

$10 \equiv -1 \pmod{11}$

$10^i \equiv (-1)^i \pmod{11}$

ゆえに，

$n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10^1 + a_0$

$\equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \ldots - a_1 + a_0 \pmod{11}$

$10^{2i} \equiv (-1)^{2i} = 1 \pmod{11}$，$10^{2i+1} \equiv (-1)^{2i+1} = -1 \pmod{11}$

34

合同関係の応用（続き3）

- 7で割ったときの剰余

例：　$12{,}345{,}678 \equiv 12 - 345 + 678 \equiv 5 - 2 + 6 = 9 \equiv 2 \pmod{7}$

$n = u_k 1000^k + u_{k-1} 1000^{k-1} + \ldots + u_1 1000^1 + a_0$

$(u_i \in \mathbf{N}_0,\ 0 \leq u_i < 1000)$

に対して，

$n \equiv (-1)^k u_k + (-1)^{k-1} u_{k-1} + \ldots - u_1 + u_0 \pmod{7}$

- $7 \mid n$ iff $7 \mid (-1)^k u_k + (-1)^{k-1} u_{k-1} + \ldots - u_1 + u_0$

$1001 = 7 \cdot 11 \cdot 13$ だから，$1000 \equiv -1 \pmod{7}$

$1000^i \equiv (-1)^i \pmod{7}$

ゆえに，

$n = u_k 1000^k + u_{k-1} 1000^{k-1} + \ldots + u_1 1000^1 + u_0$

$\equiv (-1)^k u_k + (-1)^{k-1} u_{k-1} + \ldots - u_1 + u_0 \pmod{7}$

$1000^{2i} \equiv (-1)^{2i} = 1 \pmod{7}$，$1000^{2i+1} \equiv (-1)^{2i+1} = -1 \pmod{7}$

35

定理（合同関係における除算）

任意の $a, b, c, p \in \mathbf{Z}$ に対して，

$ac \equiv bc \pmod{p}$ かつ $\gcd(c, p) = d\ (\neq 0)$ ならば，

$a \equiv b \left(\mathrm{mod}\ \frac{p}{d}\right)$．

【参考】 任意の $a, b, c \in \mathbf{Z}$ に対して，
$ac = bc$ かつ $c \neq 0$ ならば，$a = b$.

- 整数を法とする合同関係では
  - 「$ac \equiv bc$ かつ $c \not\equiv 0 \pmod{p}$ ならば，$a \equiv b$」は一般に成り立たない．
    例：　$7 \times 2 \equiv 4 \times 2 \pmod{6}$，$2 \not\equiv 0 \pmod{6}$であるが，$7 \not\equiv 4 \pmod{6}$
  - $ac \equiv bc \pmod{p}$かつ $\gcd(c, p) = 1$ ならば，$a \equiv b \pmod{p}$．
    例：　$7 \times 5 \equiv 1 \times 5 \pmod{6}$，$\gcd(5, 6) = 1$ であり，$7 \equiv 1 \pmod{6}$．

36

証明

任意の $a, b, c, p \in \mathbf{Z}$ に対して，
$ac \equiv bc \pmod{p}$ かつ $\gcd(c, p) = d\ (\neq 0)$ ならば，
$a \equiv b \pmod{\frac{p}{d}}$.

---

d は c, p の最大公約数だから，$c', p' \in \mathbf{Z}$ が存在して，
$c = c' \cdot d,\ p = p' \cdot d$.
このとき，$\gcd(c', p') = 1$.
また，$ac \equiv bc \pmod{p}$ だから，$q \in \mathbf{Z}$ が存在して，$ac - bc = q \cdot p$.
ゆえに，$(a-b)c'd = qp'd$ だから，$p' \mid (a-b)c'$.
$\gcd(c', p') = 1$ だから，$p' \mid a-b$.
すなわち，$a \equiv b \pmod{p'}$ だから，$a \equiv b \pmod{\frac{p}{d}}$.

37

合同関係における零因子

- $a \in \mathbf{Z}$ は $p \in \mathbf{Z}$ を法とする合同関係における零因子（zero divisor）である
  - $c \in \mathbf{Z}$ が存在して，$c \not\equiv 0 \pmod{p}$ かつ $ac \equiv ca \equiv 0 \pmod{p}$

例：2 は 6 を法とする合同関係における零因子
- $3 \not\equiv 0 \pmod{6}$ に対して，$2 \cdot 3 = 3 \cdot 2 = 6 \equiv 0 \pmod{6}$

- 通常の等号関係では
  $ac = 0$ ならば $a = 0$ または $c = 0$.
- 整数を法とする合同関係では
  $ac \equiv 0 \pmod{p}$ であっても，
  $a \equiv 0 \pmod{p}$ または $c \equiv 0 \pmod{p}$ とは限らない.

38

系（合同関係における除算）

任意の $a, b, c \in \mathbf{Z}$ と任意の素数 p に対して，
次の(1)，(2)が成り立つ.
(1) $ac \equiv bc \pmod{p}$ かつ $c \not\equiv 0 \pmod{p}$ ならば，
$a \equiv b \pmod{p}$.
(2) $ac \equiv 0 \pmod{p}$ ならば，
$a \equiv 0 \pmod{p}$ または $c \equiv 0 \pmod{p}$.

- 素数を法とする合同関係については，通常の等号関係と同様に除算を行える.

39

証明

任意の $a, b, c \in \mathbf{Z}$ と任意の素数 p に対して，
次の(1)，(2)が成り立つ.
(1) $ac \equiv bc \pmod{p}$ かつ $c \not\equiv 0 \pmod{p}$ ならば，$a \equiv b \pmod{p}$.
(2) $ac \equiv 0 \pmod{p}$ ならば，$a \equiv 0 \pmod{p}$ または $c \equiv 0 \pmod{p}$.

---

(1) $c \not\equiv 0 \pmod{p}$ だから，$p \mid c$ でない.
ゆえに，$\gcd(c, p) = 1$ となり，定理より明らか.
(2) $ac \equiv 0 \pmod{p}$ とする.
ここで，$a \not\equiv 0 \pmod{p}$ かつ $c \not\equiv 0 \pmod{p}$ と仮定する.
(1)において $b = 0$ とおくと，$a \equiv 0 \pmod{p}$.
これは矛盾.
ゆえに，$a \equiv 0 \pmod{p}$ または $c \equiv 0 \pmod{p}$.

40

まとめ

- 今回の講義
  - 1 次不定方程式
  - 合同式
- 次回の講義
  - (2限)合同式(続き)(教科書　pp.131-137, 140-145)
- 今回の演習
  - なし

41