合同式.

$m \in \mathbb{N}$ とする. $^\forall a, b \in \mathbb{Z}$ に対し.

$a \equiv b \pmod m$

$\overset{\text{def}}{\iff}$ $m \mid a-b$ とする このとき. a と b は m を法として合同 という.

合同が同値関係であることはすでにみた.

<u>定理 6.7</u>. $m \in \mathbb{N}$, $a, b, a', b', c, r \in \mathbb{Z}$,

$a \equiv a' \pmod m$, $b \equiv b' \pmod m$ とするとき.次が成立.

(1) $a+b \equiv a'+b' \pmod m$

(2) $a-b \equiv a'-b' \pmod m$

(3) $ab \equiv a' \cdot b' \pmod m$

(4) $a^r \equiv (a')^r \pmod m$

(5). c と m が互いに素 ($\gcd(c, m) = 1$) ならば.

$ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod m$

☺ 合同であることの必要十分条件は 割ったときのあまりが同じことなので.

(1), (2) は明らか.

(3). $a = km + r$, $a' = k'm + r$

$b = lm + s$, $b' = l'm + s$ として計算すれば

$ab \equiv rs \equiv a'b'$ となる.

(4) (3) を くり返し使えば よい.

(5) (3)の 式を使うと.

$ac \equiv rc$, $bc \equiv sc$ とできるので．

$m \mid rc - sc = c(r-s)$ となるが．

$\gcd(m, c) = 1$ より

$m, c, r-s$ の素因数分解を考えれば． $m \mid r-s$ でないといけない

∴ $a \equiv b$ である．

例 (1) $5x - 4 \equiv 11 \pmod 9$ をとくと．

$$5x \equiv 15 \quad (1)$$

$$x \equiv 3 \quad (5)$$

となる．

(2) $3x - 4 \equiv 4 \pmod 9$ を解くと．

$3x \equiv 8 \pmod 9$ より 解なし となる．

(3) $5x - 4 \equiv 12 \pmod 9$ をとくと．

$5x \equiv 16$

$5x \equiv 25$ より $x \equiv 5$ となる．

(4) (5) は互いに素が必要

$14 \equiv 8 \pmod 6$ であるが．

$7 \equiv 4 \pmod 6$ は間違いである．

(5) $10^{3000} \pmod{11}$ を求めると．

$10^{3000} \equiv (-1)^{3000} \equiv 1$ となる．

(6) $10^{100} \pmod 7$ を求めると． $3^6 \equiv 9^3 \equiv 2^3 \equiv 8 \equiv 1$ より

$10^{100} \equiv 3^{100} \equiv 3^{6 \times 16 + 4} \equiv 3^4 \equiv 81 \equiv 4$ である．

定理6.8　$a, m \in \mathbb{N}$, $b \in \mathbb{Z}$とする.　$a \not\equiv 0 \pmod{m}$とする

(1) 次は同値

(i) $ax \equiv b$,　が解をもつ.

(ii) $ax + my = b$ が整数解をもつ.

(iii) $\gcd(a, m) \mid b$.

(2). aとmが互いに素なら. $ax \equiv b$ $(a \not\equiv 0)$の解はmを法としてただ1つ.

∵ (i)⇒(ii)

xを解とすると.

$m \mid ax - b$ より $ax - b = my$ となる ∴ $ax - my = b$ となり(ii)がいえる

(ii)⇒(i) $ax + my = b$ が整数解をもてば.

$ax - b = -my$ より $ax \equiv b$ となる.

(ii)⇒(iii) $c = \gcd(a, m)$ とすると.

$c \mid ax + my = b$ となる.

(iii)⇒(ii) ユークリッドの互除法を考えると.

$x_0 = \max\{a, m\}$, $x_1 = \min\{a, m\}$, $x_{n-1} = k_n x_n + x_{n+1}$, $\gcd(a, m) = x_\ell$

とできていた. ここで

$x_{n+1} = x_{n-1} - k_n x_n$ と. 前2つの整数倍の和で表されるので.

$c = x_\ell = x_{\ell-2} - k_{\ell-1} x_{\ell-1} = x_{\ell-2} - k_{\ell-1}(x_{\ell-3} - k_{\ell-2} x_{\ell-2}) = \cdots = p \cdot x_0 + q x_1$ とできる

∴ $pa + qm = c$ となる.　ここで $b = r \cdot c$ より.

$rpa + rqm = b$ となり. 解の存在がわかる.

(2). x_1, x_2 を解とすると.

$ax_1 \equiv b \equiv ax_2$ より $x_1 \equiv x_2$ である //.

注 (iii)⇒(ii) の証明は. 整数解の解法も与えている.

しかし. 定理6.5より この計算回数は. ケタ数の 6倍程度で抑えられる.

例 (1) $204x \equiv 34 \pmod{85}$ を考えると.

$204 = 85 \times 2 + 34$.

$85 = 34 \times 2 + 17$

$34 = 17 \times 2$ より $\gcd(204, 85) = 17$, $17 \mid 34$ より解をもつ.

ここで. $17 = 85 - 34 \times 2$

$= 85 - 2 \times (204 - 85 \times 2)$

$= -2 \times 204 + 5 \times 85$ となり

$34 = -4 \times 204 + 10 \times 85$ である.

$\therefore x \equiv -4 \equiv 81$ が解になる.

なお. $x \equiv 1$ も解である.

(2) $10x \equiv 11 \pmod{12}$ は解なしである.