1章

整数 a を10で割ると $a = 10 q_1 + r_0$

$q_1 = 10 q_2 + r_1$

$q_2 = 10 q_3 + r_2$

⋮

$a = 10^n r_n + 10^{n-1} r_{n-1} + \cdots + 10 r_1 + r_0$

k 進法に拡げると $a = r_n k^n + r_{n-1} k^{n-1} + \cdots + r_1 k + r_0$

異なる数でケタが上がるとき ex 1里=36町, 1町=60間, 1間=6尺

$k_1, k_2, k_3 \cdots k_n$ として

$a = q_1 k_1 + r_0$

$q_1 = q_2 k_2 + r_1$

$q_2 = q_3 k_3 + r_2$

⋮

$q_n k_n + r_{n-1}$

$\rightarrow$ $a = q_n k_1 k_2 \cdots k_{n-1} + \cdots + r_1 k_1 + r_0$

$(0 \leqq r_i < k_{i+1})$

2章

$b = qa + r$ $a \rangle b$ $r = 0$ のとき $b = qa$, b は a の倍数 = a は b の約数

$a \rangle b$ もしくは $b \langle a$ と表す

自然数 a の正の約数全体の集合を $D(a)$ で表すと

$D(6) = \{1, 2, 3, 6\}$

$D(17) = \{1, 17\}$

$D(9) = \{1, 3, 9\}$

$D(12) = \{1, 2, 3, 4, 6, 12\}$

$D(100) = \{1, 2, 4, 5, 10, 20, 25, 50, 100\}$

$a \rangle b$ ならば $D(a) \subseteqq D(b)$, 逆に $D(a) \subseteqq D(b)$ ならば $a \rangle b$

証明) $c \in D(a)$ なら $c \rangle a$

$a \rangle b$ だから $c \rangle b$ よって $c \in D(b)$

したがって $D(a) \subseteqq D(b)$

逆に $D(a) \subseteqq D(b)$ なら $a \in D(a)$

よって $a \in D(b)$ したがって $a \rangle b$

公約数は $D(a) \cap D(b)$

3以上の数に対しては $D(a_1) \cap D(a_2) \cap \cdots \cap D(a_n)$

最大公約数は $(8, 12) = 4$ のように $(a_1, a_2, \cdots a_n)$ で表す

$D(8) \cap D(12) = \{1, 2, 4\}$

$D(12) \cap D(18) = \{1, 2, 3, 6\}$ のように

すべての公約数は最大公約数の約数となっている

定理 $a < b$ のとき, q を整数とすると $(a, b) = (a, b - qa)$

証明) $d = (a, b)$, $d' = (a, b - qa)$ ならば $d \rangle a$, $d \rangle b$

よって $d \rangle b - qa$

なので d は a と $b - qa$ の公約数

したがって d は a と $b - qa$ の最大公約数 d' より大きくはない

よって $d \leqq d'$

逆に $d' \rangle a$, $d' \rangle b - qa$

だから $d' \rangle qa$, $d' \rangle (b - qa) + qa = b$

d' は a, b の公約数

よって $d' \leqq d$

$\therefore d = d'$

$(a, b) = (a, b - qa)$

互除法

最大公約数に関する

定理 $(ma, mb) = m(a, b)$

定理 a, b の任意の公約数は a, b の最大公約数 (a, b) の約数

証明) $c \rangle a$, $c \rangle b$ となる c をとり, $a = a'c$, $b = b'c$ と書ける

$(a, b) = (a'c, b'c) = c(a', b')$ $\therefore c \rangle (a, b)$

定理 $D(a) \cap D(b) = D((a, b))$

例 $D(36) \cap D(60)$ を求める場合, まず $(36, 60)$ を求める

36) 60 … 1
36
24) 36 … 1
24
12) 24 … 2
24
0

$(36, 60) = 12$

$D((36, 60)) = D(12)$

$= \{1, 2, 3, 4, 6, 12\}$

例 $D(15) \cap D(25)$, $(15, 25) = 5$

15) 25 … 1
15
10) 15 … 1
10
5) 10 … 2
10

$D(5) = \{1, 5\}$

$D(32) \cap D(54)$ $(32, 54) = 2$

32) 54 … 1
32
22) 32 … 1
22
10) 22 … 2
20
2) 10 … 5

$D(2) = \{1, 2\}$

$D(63) \cap D(91)$ $(63, 91) = 7$

63) 91 … 1
63
28) 63 … 2
56
7) 28 … 4

$D(7) = \{1, 7\}$

定理 $(a, b) = 1$ ならば $(ac, b) = (c, b)$

証明) $(ac, b) = (ac, bc, b) = ((ac, bc), b) = (c(a, b), b)$

$= (c, b)$

$(a, b) = 1$ のとき a と b は互いに素

定理 $(a, b) = 1$ で $a \rangle bc$ のとき $a \rangle c$

証明) $(a, b) = 1$ に c をかけて $(a, b)c = c$

$(ac, bc) = c$

$a \rangle bc$ だから $bc = ad$ と書ける

$(ac, ad) = c$

$a(c, d) = c$

よって $a \rangle c$

定理 $(a, b) = 1$, $a \rangle c$, $b \rangle c$ なら $ab \rangle c$

証明) $b \rangle c$ から $c = bd$ と書ける

$a \rangle c = a \rangle bd$

↑の定理から $a \rangle d$

よって $d = ae$

$c = bd = b(ae) = (ab)e$

$\therefore ab \rangle c$

a の倍数の集合を $M(a)$ で表す

$M(3) = \{3, 6, 9, 12, \cdots\}$　$M(10) = \{10, 20, 30, \cdots\}$

公倍数は $M(a) \cap M(b)$ ，最小公倍数は $[a, b]$ と表す

定理　a, b の任意の公倍数は最小公倍数の倍数である

証明　a) c, b) c となる公倍数 c ，$[a, b]$ で割ると

$$c = q[a,b] + r \quad (0 \leqq r < [a,b])$$

a) $c - q[a,b] = r$, b) $c - q[a,b] = r$

$\therefore$ r は a, b の公倍数

しかも $0 \leqq r < [a,b]$ から $0 < r < [a,b]$ だと

最小公倍数より小さな公倍数が存在し矛盾

よって $r = 0$

すなわち $c = q[a,b]$ ∎

定理　$M(a) \cap M(b) = M([a,b])$

定理　$[ma, mb] = m[a,b]$

定理　$(a, b) = 1$ ならば $[a, b] = ab$

証明　a) $[a,b]$, b) $[a,b]$ から　ab) $[a,b]$

一方 ab は a, b の公倍数だから $[a,b]$) ab

$\therefore$ $[a,b] = ab$ ∎

定理　$[a,b](a,b) = ab$, または $[a,b] = \dfrac{ab}{(a,b)}$

証明　$a = a'(a,b)$, $b = b'(a,b)$ とおく

$$(a,b) = (a'(a,b), b'(a,b)) = (a,b)(a',b')$$

$\therefore$ $(a', b') = 1$

$$\begin{aligned}[a,b] &= [a'(a,b), b'(a,b)] \\ &= (a,b)[a',b'] \\ &= (a,b)a'b' \\ &= (a,b)\frac{a}{(a,b)}\frac{b}{(a,b)} \\ &= \frac{ab}{(a,b)}\end{aligned}$$

∎

例　8 と 12 について

$[8, 12] = 24$,　$(8, 12) = 4$

$24 \times 4 = 96 = 8 \times 12$

$$[8,12] = \frac{8\times 12}{(8,12)} = \frac{96}{4} = 24$$

素数　定理　1でない全ての正整数は素数の積として表せる

証明）数学的帰納法をつかう

これまで成り立つとして $n+1$ を考える

$n+1$ が素数なら この定理は正しい

$n+1$ が素数でないなら 1と $n+1$ 以外の約数をもつ

a）$n+1$ という約数 a を考えると

$n+1=ab$

$a,b<n+1$

$a,b \leqq n$

（したがって a,b はおのおの素数の積なので

$n+1=ab$ も素数の積

または素数なので 帰納法は完了

定理　素数は無限にある

証明）背理法をつかう

素数が有限な数 n 個あるとする，$p_1, p_2 \cdots, p_n$

$N=p_1p_2\cdots p_n+1$

N を素数の積に分けてみる，$N=q_1q_2\cdots q_m$

N は $p_1p_2\cdots p_n$ で割ると余り1．$p_1p_2\cdots p_n$ は素因数とならない

したがって $q_1q_2\cdots q_m$ は $p_1p_2\cdots p_n$ のどれとも異なる素数

最初の仮定だと $p_1p_2\cdots p_n$ は全ての素数なので矛盾

初等整数論の基礎定理

正整数を素数の積として表す仕方は1通りしかない

ただし積の順序のちがいは問題にしない

定理　$b \mid a$ で $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$

$b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s}$ ならば

$\alpha_1 \geqq \beta_1,\ \alpha_2 \geqq \beta_2,\ \cdots,\ \alpha_s \geqq \beta_s$

逆にこのような b は a の約数．

証明）$a=bc$

$c=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_s^{\gamma_s}$ $(\gamma_1 \geqq 0,\ \gamma_2 \geqq 0,\ \cdots\ \gamma_s \geqq 0)$

とする $bc=p_1^{\beta_1+\gamma_1}p_2^{\beta_2+\gamma_2}\cdots p_s^{\beta_s+\gamma_s}$

$\alpha_1=\beta_1+\gamma_1$

$\alpha_2=\beta_2+\gamma_2$

$\vdots$

$\alpha_s=\beta_s+\gamma_s$

これから $\alpha_1 \geqq \beta_1,\ \alpha_2 \geqq \beta_2 \cdots\ \alpha_s \geqq \beta_s$

逆に $c=p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}\cdots p_s^{\alpha_s-\beta_s}$ とすれば $a=bc$

$\therefore\ b \mid a$」

定理　2つの数 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ があり

$(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s} = c$

$[a,b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s} = d$

ここに　$\gamma_1 = \min(\alpha_1, \beta_1)$,　$\gamma_2 = \min[\alpha_2, \beta_2]$, $\gamma_s = \min(\alpha_s, \beta_s)$

$\delta_1 = \max(\alpha_1, \beta_1)$　…　$\delta_s = \max[\alpha_s, \beta_s]$

例　$(180, 600) = 2^2 \cdot 3 \cdot 5 = 60$　← $180 = 2^2 \cdot 3^2 \cdot 5$, $600 = 2^3 \cdot 3 \cdot 5^2$

$[180, 600] = 2^3 \cdot 3^2 \cdot 5^2 = 1800$

$r = \frac{a}{b}$ という正の有理数があるとき

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$

$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$ とすると $r = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \cdot q_1^{-\beta_1} q_2^{-\beta_2} \cdots p_t^{-\beta_t}$

と表せる

また この形に素因数分解でき、この分解は一意的

3章　$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ の約数 m を考えると

$m=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$ $(0\leqq\beta_1\leqq\alpha_1,\ 0\leqq\beta_1\leqq\alpha_2,\ \cdots 0\leqq\beta_k\leqq\alpha_k)$

この形の組の数は $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$ 個ある

定理　$\tau(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$

例　$12=2^2\cdot3$　$\tau(12)=(2+1)(1+1)=6$
1, 2, 3, 4, 6, 12

$100=2^2\cdot5^2$　$\tau(100)=(2+1)(2+1)=9$
1, 2, 4, 5, 10, 20, 25, 50, 100

例　$n\leqq100$, $\tau(n)=6$ を満たす n を求めよ。

n の素因数が1個のとき　$\alpha_1+1=6\to\alpha_1=5$

$2^5=32$, $3^5=243$

したがって $n\leqq100$ にあてはまるのは 2^5 だけ

n の素因数が2個のとき　$\tau(n)=(\alpha_1+1)(\alpha_2+1)=6$

$\alpha_1+1=3$, $\alpha_1=2$

$\alpha_2+1=2$, $\alpha_2=1$

よって $n=p_1^2p_2$

$p_1=2$ のとき　$2^2\cdot3=12$, $2^2\cdot5=20$, $2^2\cdot7=28$
$2^2\cdot11=44$, $2^2\cdot13=52$, $2^2\cdot17=68$
$2^2\cdot19=76$, $2^2\cdot23=92$

$p_1=3$ のとき　$3^2\cdot2=18$, $3^2\cdot5=45$, $3^2\cdot7=63$
$3^2\cdot11=99$

$p_1=5$ のとき　$5^2\cdot2=50$, $5^2\cdot3=75$

$p_1=7$ のとき　$7^2\cdot2=98$

$\tau(n)$ の性質を一般化して

定義　正整数 n に対して定義された関数 $f(n)$ があり
$(m_1,m_2)=1$ のときはつねに $f(m_1m_2)=f(m_1)f(m_2)$
となるとき $f(n)$ は乗法的関数という

例　$f(n)$ が乗法的なら、n の素因数分解 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$
に対して $f(n)=f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_k^{\alpha_k})$ となることを証明せよ

証明)　$p_1^{\alpha_1}$, $p_1^{\alpha_2}$, $\cdots$ $p_k^{\alpha_k}$ は互いに素なので
$(p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_k^{\alpha_k})=1$ であるから

$f(n)=f(p_1^{\alpha_1}(p_2^{\alpha_2}\cdots p_k^{\alpha_k}))$
$=f(p_1^{\alpha_1})f(p_2^{\alpha_2}\cdots p_k^{\alpha_k})$
$\vdots$
$=f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_k^{\alpha_k})$

$\to$ $f(p^\alpha)$ が1つ分かればすべての $f(n)$ の値が定まる

$G(p_1^{\alpha_1})=1+p_1+p_1^2+\cdots+p_1^{\alpha_1}$

初項1, 公比 p_1 の等比数列

両辺に p_1 をかけて

$p_1G(p_1^{\alpha_1})=p_1+p_1^2+\cdots+p_1^{\alpha_1+1}$

元の式から引いて

$G(p_1^{\alpha_1})-p_1G(p_1^{\alpha_1})=(1+p_1+\cdots+p_1^{\alpha_1})-(p_1+p_1^2+\cdots+p_1^{\alpha_1+1})$

$(1-p_1)G(p_1^{\alpha_1})=1-p_1^{\alpha_1+1}$

$G(p_1^{\alpha_1})=\dfrac{p_1^{\alpha_1+1}-1}{p_1-1}$

完全数　$6 = 1+2+3$

$28 = 1+2+4+7+14$

$\underline{G(n) - n = n}$

nの約数の和　$G(n) = 2n$

奇数の完全数は発見されてない

定理　偶数の完全数は $2^{n-1}(2^n-1)$ の形をもつ

ただし 2^n-1 は素数

例　$6 = 2\cdot 3$
$= 2^{(2-1)}\cdot(2^2-1)$

$28 = 2^2\cdot 7$
$= 2^{(3-1)}\cdot(2^3-1)$

$2^{(4-1)}(2^4-1) = 2^3\cdot 15 = 8\cdot 15 = 120$
素数じゃない　完全数じゃない

$496 =$

$2^{(5-1)}\cdot(2^5-1) = 2^4\cdot 31 = 16\cdot 31 = 496$
素数　完全数

31
16
186
31
496

証明)　nを偶数の完全数とすると

$n = 2^k\cdot l$　($k\geq 1$, lは奇数)

$G(n) = G(2^k\cdot l) = G(2^k)\,G(l)$

$G(2^k) = 2^0\cdot 2^1\cdots 2^k$

初項1，公比2

$2G(2^k) = 2^1\cdot 2^2\cdots 2^{k+1}$

$G(2^k) - 2G(2^k)$
$= 2-[2^{k+1}]$

$G(2^k) = \frac{(2^{k+1})-1}{2-1}$

$= \frac{2^{k+1}-1}{2-1}\cdot G(l)$

$= (2^{k+1}-1)G(l)$

完全数の定理より　$G(n) = 2n$ だから

$2n = 2(2^k\cdot l) = 2\cdot 2^k\cdot l$

$(2^{k+1}-1)G(l) = 2\cdot 2^k\cdot l$
$= 2^{k+1}\cdot l$
$= (2^{k+1}-1)l + l$

$\leftrightarrow \quad G(l) = \frac{(2^{k+1}-1)l + l}{2^{k+1}-1}$

$= l + \frac{l}{2^{k+1}-1}$

$G(l)$とlは整数なので $\frac{l}{2^{k+1}-1}$ は整数

したがって $2^{k+1}-1$ はlの約数

$G(l)$は2つの約数lと $\frac{l}{2^{k+1}-1}$ の和の形

したがってlは2つの約数をもつから素数

$\therefore \quad \frac{l}{2^{k+1}-1} = 1$

$\leftrightarrow l = 2^{k+1}-1$

$2^{k+1}-1$が素数であるためには$k+1$が素数で

なければならない、素数でなければ

$k+1 = ab$ ($a>1$, $b>1$)となる

$2^{k+1}-1 = 2^{ab}-1 = (2^a-1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1)$

$\longrightarrow$ 素数にならない

したがって $k+1 = p$ とならなければならない

$\therefore \quad n = 2^k\cdot l = 2^{p-1}(2^p-1)$

2^p-1 が素数なら $2^{p-1}(2^p-1)$ は偶数の完全数となる

2^p-1 の形の数をメルセンヌ数という

$G(n)-n>n \Leftrightarrow G(n)>2n$ のとき過剰数といい

$G(n)-n<n \Leftrightarrow G(n)<2n$ のとき不足数という

例) 素数の累乗 p^k は不足数となる

$$2\cdot p^k - G(p^k) = 2p^k - \frac{p^{k+1}-1}{p-1}$$

$$= \frac{2(p-1)p^k - p^{k+1}+1}{p-1}$$

$$= \frac{(p-2)p^k+1}{p-1} \quad p\geqq 2 \text{ なので} > 0$$

よって $2p^k > G(p^k)$ ∴ 不足数になる

mの約数の和(m自身を除く)がnに等しく

nの約数の和(n自身を除く)がmに等しいとき

mとnを親和数という $G(m)-m=n$

$G(n)-n=m$

$\leftarrow\!\!\rightarrow G(m)=G(n)=m+n$

220, 284	2620, 2924	6232, 6368	117296, 18416
1184, 1210	5020, 5564	10744, 10856	11144853777712, 11885377937424

100! を素因数分解すると $100! = 2^\alpha 3^\beta 5^\gamma \cdots$

α と γ の小さい方を k とすると

$100! = 2^\alpha 5^\gamma \cdots = 10^k \cdots$

となるから k が求めるもの

$\alpha > \gamma$ は明らかだから $\gamma = \left[\frac{100}{5}\right] + \left[\frac{100}{5^2}\right] = 20+4 = 24$

つまり24個の0が並ぶ

定理 $n!$ の素因数分解における p の指数 α は

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right]$$

定理 n を p 進法で表したとき $n = c_0 + c_1 p + \cdots + c_k p^k$ $(0 \leqq c_k < p)$

とおくと

$$\alpha = \frac{n-(c_0+c_1+\cdots+c_k)}{p-1}$$

$\binom{n}{m} = {}_nC_m = \frac{n!}{m!(n-m)!}$ を素因数に分解する

上の定理より $n!$ は $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right]$

$m!$ は $\left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \cdots + \left[\frac{m}{p^k}\right]$

$(n-m)!$ は $\left[\frac{n-m}{p}\right] + \left[\frac{n-m}{p^2}\right] + \cdots + \left[\frac{n-m}{p^k}\right]$

よって $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots \left[\frac{n}{p^k}\right] - \left[\frac{m}{p}\right] - \left[\frac{m}{p^2}\right] - \cdots - \left[\frac{m}{p^k}\right]$

$$- \left[\frac{n-m}{p}\right] - \left[\frac{n-m}{p^2}\right] - \cdots - \left[\frac{n-m}{p^k}\right]$$

$$= \left(\left[\frac{n}{p}\right] - \left[\frac{m}{p}\right] - \left[\frac{n-m}{p}\right]\right) + \cdots + \left(\left[\frac{n}{p^k}\right] - \left[\frac{m}{p^k}\right] - \left[\frac{n-m}{p^k}\right]\right) \quad \cdots ①$$

ここで一般の項 $\left[\frac{n}{p^k}\right] - \left[\frac{m}{p^k}\right] - \left[\frac{n-m}{p^k}\right]$ とし

$\frac{m}{p^k} = \alpha$, $\frac{n-m}{p^k} = \beta$ とおくと

$\alpha+\beta = \frac{m}{p^k} + \frac{n-m}{p^k} = \frac{n}{p^k}$ から

$[\alpha+\beta] - [\alpha] - [\beta]$

一般に $[\alpha+\beta] \geqq [\alpha]+[\beta] \geqq [\alpha+\beta]-1$ が成り立つから

$1 \geqq [\alpha+\beta]-[\alpha]-[\beta] \geqq 0$

つまり①の各項は0か1、したがって①は $\geqq 0$ となる

$\frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \cdots \frac{n-1}{n}$ を考える，$n=10$ のとき

$\frac{0}{10}, \frac{1}{10}, \frac{2}{10}, \frac{3}{10}, \frac{4}{10}, \frac{5}{10}, \frac{6}{10}, \frac{7}{10}, \frac{8}{10}, \frac{9}{10}$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

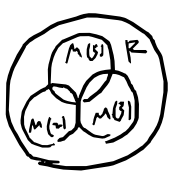
$\frac{0}{1} \quad \frac{1}{5} \quad \frac{2}{5} \quad \frac{1}{2} \quad \frac{3}{5} \quad \frac{1}{5}$

オイラーの関数

$\varphi(n) = \underline{\quad}$ となる

既約の数

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ とすると n と互いに素な集合 $R = \{0, 1, \cdots n-1\}$ の α なかで $p_1, p_2 \cdots p_k$ の倍数になっていないものが $\varphi(n)$ を決める



← 1つの集合から部分集合を除いた残りの集合を求めることをふるいという

集合 A の個数を $|A|$ とすると

$|R| - |M(2)| - |M(3)| - |M(5)|$ を考える

$M(2) \cap M(3)$, $M(2) \cap M(5)$, $M(3) \cap M(5)$ は重複して引かれてる

$M(2) \cap M(3) = M(2 \cdot 3)$

$M(2) \cap M(5) = M(2 \cdot 5)$

$M(3) \cap M(5) = M(3 \cdot 5)$

よって $|M(2) \cap M(3) \cap M(5)| = |M(2 \cdot 3 \cdot 5)|$ も考慮して

$$\begin{aligned}\varphi(60) &= |R| - |M(2)| - |M(3)| - |M(5)| \\ &\quad + |M(2 \cdot 3)| + |M(2 \cdot 5)| + |M(3 \cdot 5)| - |M(2 \cdot 3 \cdot 5)| \\ &= 60 - \frac{60}{2} - \frac{60}{3} - \frac{60}{5} + \frac{60}{2 \cdot 3} + \frac{60}{2 \cdot 5} + \frac{60}{3 \cdot 5} - \frac{60}{2 \cdot 3 \cdot 5} \\ &= 60\left(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2 \cdot 3} + \frac{1}{2 \cdot 5} + \frac{1}{3 \cdot 5} - \frac{1}{2 \cdot 3 \cdot 5}\right) \\ &= 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 16\end{aligned}$$

一般的に特性関数 $\chi(x; A)$ を考える

$x \in A$ のとき $\chi(x; A) = 1$

$x \notin A$ のとき $\chi(x; A) = 0$

$x \in R$, 部分集合 A

定理 $|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_k}|$

$$\begin{aligned}&= |R| - |A_1| - |A_2| \cdots - |A_k| \\ &\quad + |A_1 \cap A_2| + \cdots + |A_{k-1} \cap A_k| \\ &\quad - \cdots \\ &\quad + (-1)^k |A_1 \cap A_2 \cap \cdots \cap A_k|\end{aligned}$$

$R = \{0, 1, 2, \cdots n-1\}$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ とし

R のなかの $p_1, p_2, \cdots p_k$ の倍数の集合を $M(p_1), M(p_2), \cdots M(p_k)$ とすれば

$\varphi(n)$ は R から $M(p_1), M(p_2), \cdots M(p_k)$ を ふるい落とした残りを求めること

つまり $\varphi(n) = |\overline{M(p_1)} \cap \overline{M(p_2)} \cap \cdots \cap \overline{M(p_k)}|$

$$\begin{aligned}&= n - |M(p_1)| - |M(p_2)| - \cdots - |M(p_k)| \\ &\quad + |M(p_1 p_2)| + \cdots + |M(p_{k-1} p_k)| \\ &\quad - \cdots \\ &\quad + (-1)^k |M(p_1 p_2 \cdots p_k)|\end{aligned}$$

ここで $M(p_1)$ は $\{0, p_1, 2p_1, \cdots\}$ の個数だから $\frac{n}{p_1}$

$M(p_1 p_2)$ は $\{0, p_1 p_2, 2p_1 p_2, \cdots\}$ の個数だから $\frac{n}{p_1 p_2}$

したがって

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \cdots - \frac{n}{p_k} + \frac{n}{p_1 p_2} + \cdots + \frac{n}{p_{k-1} p_k} - \cdots + (-1)^k \frac{n}{p_1 p_2 \cdots p_k}$$

$$\begin{aligned}&= n\left(1 - \frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_k} + \frac{1}{p_1 p_2} + \cdots + \frac{1}{p_{k-1} p_k} - \cdots + (-1)^k \frac{1}{p_1 p_2 \cdots p_k}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)\end{aligned}$$

あるいは $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ とすれば

$$\begin{aligned}\varphi(n) &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\ &= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1) \cdots (p_k - 1)\end{aligned}$$

これをオイラーの公式という

例 $n = 1, 2, \cdots 30$ に対する $\varphi(n)$ の値

$30 = 2^1 \cdot 3^1 \cdot 5^1$ なので $\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)$

$p_1^1 \quad p_2^1 \quad p_3^1$

$$= 30 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

$$= 30\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 8$$

メビウスの関数 μ $\quad \mu(1) = 1$

$\mu(p_1 p_2 \cdots p_s) = (-1)^s$ ← $p_1 p_2 \cdots p_k$ がみな異なる素数

$\mu(p_1 p_2 \cdots p_s) = 0$ ← $p_1 p_2 \cdots p_k$ の中に等しい素数が存在

これを用いると $\varphi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d} = \sum_{d \mid n} \frac{n}{d} \mu(d)$

n の約数を考える

$\mu(2) = 2 = (-1)^1 = -1$

$\mu(3) = 3 = (-1)^1 = -1$

$\mu(4) = 2 \cdot 2 = 0$

$\mu(5) = 5 = (-1)^1 = -1$

$\mu(6) = 2 \cdot 3 = (-1)^2 = 1$

$\mu(7) = 7 = (-1)^1 = -1$

$\mu(8) = 2 \cdot 2 \cdot 2 = 0$

$\mu(9) = 3 \cdot 3 = 0$

$\mu(10) = 2 \cdot 5 = (-1)^2 = 1$

$\mu(11) = 11 = (-1)^1 = -1$

$\mu(12) = 2 \cdot 2 \cdot 3 = 0$

$\mu(13) = 13 = -1$

$\mu(14) = 2 \cdot 7 = (-1)^2 = 1$

$\mu(15) = 3 \cdot 5 = (-1)^2 = 1$

定理 $\sum_{d \mid n} \mu(d) = \begin{cases} 1 & (n = 1) \\ 0 & (n \neq 1) \end{cases}$

$\sum_{d|n} e(d) = n$ が成り立つとき 逆に未知の $\varphi(n)$ を求めたい

メビウスの反転公式　$\sum_{d|n} f(d) = g(n)$ のとき

$$f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d)$$

が成り立つ

証明)　$\frac{n}{d} = d'$ とすれば

$$g(n) = \sum_{d'd''=n} f(d') \quad \text{と書ける}$$

$\sum_{d'd''=n}$ は $d'd''=n$ を満足するすべての d' について加えよ、という意味

$$\sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d) = \sum_{dd'''=n} g(d)\mu(d''')$$

ここで $g(d) = \sum_{d'd''=d} f(d')$ であるから代えて

$$\sum_{dd'''=n} \left(\sum_{d'd''=d} f(d')\right)\mu(d''') = \sum_{dd'd'''=n} f(d')\mu(d''')$$

$$= \sum_{d'|n} f(d') \sum_{d''d'''=\frac{n}{d'}} \mu(d''')$$

ところで $\sum_{d''d'''=\frac{n}{d'}} \mu(d''')$ は $\frac{n}{d'}=1$ のときだけ 0 で他は 1

よって $= \sum_{d'=n} f(d') = f(n)$

余類

整数 a を m で割った余りが等しい整数全体の集合を $K(a)$ とすると

$K(a) \equiv \mathbb{Z}$　　$\mathbb{Z}$ は整数全体の集合

この $K(a)$ は剰余類という

$K(0), K(1), \cdots K(n-1)$ という n 個の部分集合がつくられ

$\mathbb{Z}$ はこれらに分けられ、しかも共通部分を有しない

すなわち $\mathbb{Z} = K(0) \cup K(1) \cup \cdots \cup K(n-1)$

$K(i) \cap K(k) = \phi$　$(i \neq k)$

$M = \{a, b, c, \cdots\}$ という有限あるいは無限の集合 M に対して

2項関係 R を　aRb と表わし、否定を $a\bar{R}b$ と表す

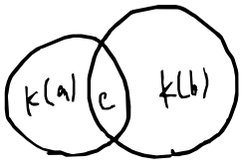
例)

$M = \{a_1, a_2, a_3, a_4, a_5\}$ で表される本の集まり、R は「a は b の上にある」

$a_3 R a_4$,　$a_1 \bar{R} a_5$,　$a_4 \bar{R} a_5$. など

R には 反射律、対称律、推移律が成り立つ。つまり 同値律が成り立つ

$a \sim b\,(R)$



M が要素 a をとり $a \sim x\,(R)$ となる x をとると

この全体を $K(a)$ と表現する　$a \in K(a)$

同じように $K(b)$ をとり　$c \in K(a)$ かつ $c \in K(b)$ なる c をとる

このとき　$a \sim c\,(R)$,　$b \sim c\,(R)$

$\leftrightarrow c \sim b\,(R)$ ← 対称律

$\leftrightarrow a \sim b\,(R)$ ← 推移律

したがって　$b \in K(a)$

$d \in K(b)$ をとると　$b \sim d\,(R)$

$a \sim b\,(R)$,　$b \sim d\,(R)$ なので　$a \sim d\,(R)$

したがって　$d \in K(a)$　だから　$K(a) \supseteq K(b)$

同様にして　$K(b) \supseteq K(a)$

つまり　$K(a) = K(b)$

$K(a)$ と $K(b)$ が共通部分をもつなら同じ集合になる

このような部分集合 $K(a)$, $K(b)$... を類と名づける

例) $1 \leq k < n-1$ のとき $n^k - 1$ は $(n-1)^2$ では整除できない

解) $n^k - 1 = \{(n-1)+1\}^k - 1$

2項定理で展開すると次のようになる

$$n^k - 1 = (n-1)^k + \cdots + \binom{k}{2}(n-1)^2 + k(n-1) + 1 - 1$$
$$= (n-1)^2\{(n-1)^{k-2} + \cdots + \binom{k}{2}\} + k(n-1)$$
$$\equiv k(n-1) \pmod{(n-1)^2}$$

$k < n-1$ だから $\not\equiv 0 \pmod{(n-1)^2}$

mod n による類別は同一組合わせをもつ

$K(a)$ の任意の要素を b, $K(c)$ の任意の要素を d とすれば

$a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$ となるか

$$a + c \equiv b + d \pmod{n}$$
$$a - c \equiv b - d \pmod{n}$$
$$ac \equiv bd \pmod{n}$$

$K(a)$ の要素と $K(c)$ の要素を加・減・乗法すると $K(a+c)$ の類に帰属する

mod 5 を例にとると $K(3) + K(4) = K(2)$ となる

一般に剰余類 $R(n) = \{K(0), K(1), \cdots K(n-1)\}$ に存在と要素間で $+, -, \times$ が定義できて

1. 加法について閉じている
2. 交換法則 $K(a) + K(b) = K(b) + K(a)$
3. 結合法則 $\{K(a) + K(b)\} + K(c) = K(a) + \{K(b) + K(c)\}$
4. 単位元 $K(a) + K(0) = K(a)$
5. 逆元 $K(a) + K(n-a) = K(0)$
6. 乗法に対して閉じている
7. 結合法則 $\{K(a)K(b)\}K(c) = K(a)\{K(b)K(c)\}$
8. 分配法則 $K(a)\{K(b) + K(c)\} = K(a)K(b) + K(a)K(c)$

このような $R(n)$ を剰余環という

完全剰余 $\{0, 1, 2, \cdots n-1\}$ のなかで n と互いに素であるものの個数は $\varphi(n)$, これらの剰余を既約剰余系といい $R'(n)$ で表す

$n = 4$ のとき $\varphi(4) = 2(2-1) = 2$

$R(4) = \{0, 1, 2, 3\}$

$R'(4) = \{1, 3\}$

$n = 12$ のとき $\varphi(12) = 2(2-1)(3-1) = 4$

$R(4) = \{1, 2, \cdots, 12\}$

$R'(4) = \{1, 5, 7, 11\}$

定理 mod n の既約剰余系 $R'(n) = \{a_1, a_2, \cdots a_{\varphi(n)}\}$ の各要素 x にそのうちの1つの要素 a_i を掛けて

$x \to a_i x$

という対応を考えると、この対応は1対1である

オイラーの定理 $(a, n) = 1$ ならば $a^{\varphi(n)} \equiv 1 \pmod{n}$ が成り立つ

例) mod 10 に対してオイラーの定理を確かめよ

$R'(10) = \{1, 3, 7, 9\}$

$\varphi(10) = 4$

$1^4 \equiv 1 \pmod{10}$

$3^4 \equiv (3^2)^2 \equiv 9^2 \equiv 81 \equiv 1 \pmod{10}$

$7^4 \equiv (7^2)^2 \equiv (49)^2 \equiv 9^2 \equiv 81 \equiv 1 \pmod{10}$

$9^4 \equiv (9^2)^2 \equiv 81^2 \equiv 1^2 \equiv 1 \pmod{10}$

mod 9 に対して

$R'(9) = \{1, 2, 4, 5, 7, 8\}$

$\varphi(9) = 6$

$1^6 \equiv 1 \pmod{9}$

$2^6 \equiv (2^3)^2 \equiv 8^2 \equiv 64 \equiv 1 \pmod{9}$

$4^6 \equiv (2^6)^2 \equiv 1^2 \equiv 1 \pmod{9}$

$5^6 \equiv 15^3 \equiv (25)^3 \equiv 7^3 \equiv 49 \cdot 7 \equiv 35 \equiv 1 \pmod{9}$

$7^6 \equiv (7^3)^2 \equiv 1^2 \equiv 1 \pmod{9}$

$8^6 \equiv (2^3)^6 \equiv 1^3 \equiv 1 \pmod{9}$

$(a, n) = 1$ のとき　$ax \equiv 1 \pmod{n}$ となる x は

$x = a^{\varphi(n)-1}$ とおくと，オイラーの定理により

$ax \equiv a \cdot a^{\varphi(n)-1} = a^{\varphi(n)} \equiv 1$

だから　$x \equiv a^{\varphi(n)-1} \pmod{n}$

このような x は a の逆元と考えて a^{-1} と表し

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

例）　$7x \equiv 4 \pmod{10}$

$\varphi(10) = 4$ から　$7^{-1} \equiv 7^{4-1} \equiv 7^3 \equiv 49 \cdot 7 \equiv 63 \equiv 3 \pmod{10}$

$7 \cdot 3x \equiv 4 \cdot 3 \pmod{10}$

$\Longleftrightarrow$　$x \equiv 12 \equiv 2 \pmod{10}$

$5x \equiv 9 \pmod{12}$

$\varphi(5) = 4$　　$5^{-1} \equiv 5^{4-1} \equiv 5^3 \equiv 25 \cdot 5 \equiv 5 \pmod{12}$

$5 \cdot 5x \equiv 9 \cdot 5 \pmod{12}$

$x \equiv 45 \equiv 9 \pmod{12}$

問）　$3x \equiv 4 \pmod{8}$

$\varphi(3) = 2$　　$3^{-1} \equiv 3^1 \equiv 3 \pmod{8}$

$3 \cdot 3x \equiv 4 \cdot 3 \pmod{8}$

$x \equiv 4 \pmod{8}$

$11x \equiv 10 \pmod{15}$

$\varphi(11) = 10$　　$11^{-1} \equiv 11^9 \equiv (11^2 \cdot 11)^3 \equiv (1^2 \cdot 11)^3 \equiv 11^3 \equiv 1 \cdot 11$

$\equiv 11$

$11 \cdot 11x \equiv 10 \cdot 11$

$x \equiv 5 \pmod{15}$

$7x \equiv 8 \pmod{16}$

$\varphi(7) = 6$　　$7^{-1} \equiv 7^5 \equiv 49^7 \equiv 1^7 \equiv 1 \pmod{16}$

$x \equiv 8 \pmod{16}$

定理　　$ax + b = c$ が整数解 x, y をもつための必要かつ十分条件は　$(a, b) | c$ である．

例　　4けたの数がある．4の位を1の位と入れ換えた数はその数に $\frac{3}{4}$ を掛けて1を加えた数に等しい

解　　abcd という数で表すと　$bcda = \frac{3}{4}abcd + 1$　となる

$a = x$，$bcd = y$ とすると

$abcd = 1000x + y$

$bcda = 10y + x$

$10y + x = \frac{3}{4}(1000x + y) + 1$

$40y + 4x = 3000x + 3y + 4$

$2996x - 37y = -4$

2996は37で割り切れないので $(2996, 37) = 1$

だから　この方程式は整数解をもつ

$2996x \equiv -4 \pmod{37}$

$2996 \equiv -1 \pmod{37}$ だから

$-x \equiv -4 \pmod{37}$

$x \equiv 4 \pmod{37}$

$0 \leqq x \leqq 9$ だから　$x = 4$

$2996 \times 4 - 37y = -4$

$37y = 4(2996 + 1)$

$= 4 \cdot 2997$

$y = 4 \cdot 81 = 324$

よって $abcd = 4324$

例　　7^{67} を12で割った余り　　　$R = \{1, 5, 7, 11\}$

$(7, 12) = 1$，$\varphi(12) = 4$　オイラーの定理から　$7^4 \equiv 1 \pmod{12}$

$67 = 16 \cdot 4 + 3$ から

$7^{67} = 7^{(16 \cdot 4 + 3)} = (7^4)^{16} \cdot 7^3 \equiv 1^{16} \cdot 7^3 \equiv 7^2 \cdot 7 \equiv 49 \cdot 7$

$\equiv 1 \cdot 7 \equiv 7$

$\pmod{12}$

問　1.　$10^{100} \div 17$ の余り

$(10, 17) = 1$，$\varphi(17) = 16$　　$10^{16} \equiv 1 \pmod{17}$

$10^{(16 \cdot 6) + 4} \equiv 1 \cdot 10^4 \equiv (10^2)^2 \equiv (15)^2 \equiv 4 \pmod{17}$

2.　$(2^{11213} - 1) \div 13$ の余り

$(2, 13) = 1$，$\varphi(13) = 12$　　$2^{12} \equiv 1 \pmod{13}$

$2^{(12 \cdot 934) + 5} \equiv 2^5 \equiv 32 \equiv 6 \pmod{13}$

$\therefore$　$2^{11213} - 1 \equiv 5 \pmod{13}$

九去法　　$10 \equiv 1 \pmod{9}$ の両辺を m 乗すると $10^m \equiv 1 \pmod{9}$

k けたの数 a は　$a = \alpha_k \alpha_{k-1} \cdots \alpha_1$

$= \alpha_k 10^{k-1} + \alpha_{k-1} 10^{k-2} + \cdots + \alpha_2 10 + \alpha_1$

$10^m \equiv 1$ を代入すると

$a \equiv \alpha_k + \alpha_{k-1} + \cdots + \alpha_2 + \alpha_1 \pmod{9}$

この和を $S(a)$ とおくと

$a \equiv S(a) \pmod{9}$

同じような b をとると

$a + b \equiv S(a) + S(b) \pmod{9}$

$a + b \equiv S(a + b) \pmod{9}$

だから　$S(a + b) \equiv S(a) + S(b) \pmod{9}$

同様に　$S(a - b) \equiv S(a) - S(b) \pmod{9}$

$S(ab) \equiv S(a)S(b) \pmod{9}$

例　　$237 \times 386 = 91x82$　の x を求めよ

九去法を使うと　$237 \to 2 + 3 + 7 = 12$

$386 \to 3 + 8 + 6 = 17$

91と82はともに10なので

$12 \times 17 \equiv 20 + x \pmod{9}$

$3 \times 8 \equiv 2 + x \pmod{9}$

$24 \equiv 2 + x \pmod{9}$

$x \equiv 4 \pmod{9}$

$x = 4$

よって　91482

フェルマーの定理　オイラーの定理でとくにnを素数pとすると
$n=p$, $\varphi(p)=p-1$ となる.
$(a,p)=1$ ならば $a^{p-1}\equiv 1 \pmod p$

例　$p=7$ の場合
$k=\{1,2,3,4,5,6\}$
$\varphi(7)=6$

$1^6\equiv 1 \pmod 7$
$2^6\equiv 8^2\equiv 1 \pmod 7$
$3^6\equiv 9^3\equiv 2^3\equiv 1 \pmod 7$
$4^6\equiv 16^3\equiv 9^3\equiv 1 \pmod 7$
$5^6\equiv 25^3\equiv 4^3\equiv 64\equiv 1 \pmod 7$
$6^6\equiv 36^3\equiv 1^3\equiv 1 \pmod 7$

定理　フェルマーの定理から p が素数のとき任意の整数 a に対して
$a^p\equiv a \pmod p$

ウィルソンの定理　p が素数ならば $(p-1)!\equiv -1 \pmod p$

mod 11 で　$10!$ を考えると　$10!=1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10$
$=1\cdot(2\cdot 6)\cdot(3\cdot 4)\cdot(5\cdot 9)\cdot(7\cdot 8)\cdot 10$
$\equiv 10$
$\equiv -1 \pmod{11}$

$ab\equiv 1 \pmod p$ となる b は $b=a^{p-2}$ と選べばよい

ウィルソンの定理の逆も成り立つ.　$n>1$ で $(n-1)!\equiv -1 \pmod n$ ならば
n は素数

中国剰余定理
$m_1, m_2, \cdots m_k$ は2つずつ互いに素なとき
つぎの連立合同式の解は必ず存在し, しかもその解は
$\bmod m_1, m_2, \cdots m_k$ に対して合同

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ x\equiv a_2 \pmod{m_2} \\ \cdots \\ x\equiv a_k \pmod{m_k} \end{cases}$$

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

mod 3 で　$35x_1\equiv 2$
$2x_1\equiv 2$
$x_1\equiv 1$
mod 5 で　$21x_2\equiv 3$
$x_2\equiv 3$
mod 7 で　$15x_3\equiv 2$
$x_3\equiv 2$

$3\cdot 5\cdot 7=105$ であるから
$x=1\cdot 5\cdot 7+3\cdot 3\cdot 7+2\cdot 3\cdot 5=128\equiv 23 \pmod{105}$

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

mod 3　$35x_1\equiv 1$
$2x_1\equiv 1$
$x_1\equiv -1$
mod 5　$21x_2\equiv 2$
$x_2\equiv 2$
mod 7　$15x_3\equiv 3$
$x_3\equiv 3$

$3\cdot 5\cdot 7=105$　　$35(-1)+21\cdot 2+15\cdot 3=52 \pmod{105}$

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

mod 2　$15x_1\equiv 1$
$x_1\equiv 1$
mod 3　$10x_2\equiv 2$
$x_2\equiv 2$
mod 5　$6x_3\equiv 3$
$x_3\equiv 3$

$15\cdot 1+10\cdot 2+6\cdot 3=53\equiv 23 \pmod{30}$

3.　$\begin{cases} x\equiv 6 \pmod 9 \\ x\equiv 10 \pmod 8 \end{cases}$

mod 9　$8x_1\equiv 6$
$-x_1\equiv 6$
$x_1\equiv -6$
mod 8　$9x_2\equiv 10$
$x_2\equiv 10$

$8\cdot(-6)+9\cdot 10=42 \pmod{72}$

4.　$\begin{cases} x\equiv 5 \pmod 7 \\ x\equiv 4 \pmod{11} \\ x\equiv 3 \pmod{13} \end{cases}$

mod 7　$143x_1\equiv 5$
$3x_1\equiv 5$
$3^5\cdot 3x_1\equiv 5\cdot 3^5$
$x_1\equiv 5\cdot 243$
$\equiv 5^2$
$\equiv 4$
mod 11　$91x_2\equiv 4$
$3x_2\equiv 4$
$x_2\equiv 4\cdot 4$
$\equiv 16$
$\equiv 5$
mod 13　$77x_3\equiv 3$
$12x_3\equiv 3$
$x_3\equiv 3$
$\equiv 10$

$143\cdot 4+91\cdot 5+77\cdot 10=1797\equiv 796 \pmod{1001}$

定理　$f(x)\equiv 0 \pmod{p_k^{\alpha_k}}$ の $\bmod p_k^{\alpha_k}$ に対して合同でない解の個数を n_k とすること $(k=1,2,\cdots,k)$, $f(x)\equiv 0 \pmod m$ の $\bmod m$ に対して合同でない解の個数は $n_1 n_2 \cdots n_k$ である.

例1　$x^2-9x-2\equiv 0 \pmod{20}$

$20=2^2\cdot 5=4\cdot 5$ から

$f(x)=x^2-9x-2 \pmod 4$ ---①

$f(x)=x^2-9x-2 \pmod 5$ ---②

①の解 x_1 は　$f(0)=-2\not\equiv 0$

$f(1)=-10\not\equiv 0$

$f(2)=4-18-2=-16\equiv 0 \pmod 4$

$f(3)=9-27-2=-20\equiv 0$

$\therefore x_1=2,3$

②の解 x_2 は　$f(0)=-2\not\equiv 0$

$f(1)=-10\equiv 0 \pmod 5$

$f(2)=-16\not\equiv 0$

$f(3)=-20\equiv 0$

$f(4)=16-36-2=-22\not\equiv 0$

$\therefore x_2=1,3$

組合せてくると

$\begin{cases} x\equiv 2 \pmod 4 \\ x\equiv 1 \pmod 5 \end{cases}$ から $x=6$

$\begin{cases} x\equiv 2 \pmod 4 \\ x\equiv 3 \pmod 5 \end{cases}$ から $x\equiv 18$

$\begin{cases} x\equiv 3 \pmod 4 \\ x\equiv 1 \pmod 5 \end{cases}$ から $x=11$

$\begin{cases} x\equiv 3 \pmod 4 \\ x\equiv 3 \pmod 5 \end{cases}$ から $x=3$

よって $x=3,6,11,18$」

中国剰余定理は mod が互いに素である必要があったが一般化して考えて出た答えに対してもとの合同式は満たすのかを検証する、満たさなければ解なし

例　1.　$\begin{cases} x\equiv 1 \pmod 2 \\ x\equiv 2 \pmod 3 \\ x\equiv 5 \pmod 6 \\ x\equiv 5 \pmod{12} \end{cases}$　$\begin{cases} 6=2\cdot 3 \\ 12=2^2\cdot 3 \end{cases}$ $\begin{cases} x\equiv 1 \pmod 2 \\ x\equiv 2 \pmod 3 \end{cases}$ とすると

$3x_1\equiv 1 \quad 2x_2\equiv 2$

$x_1\equiv 1 \quad x_2\equiv 4$

$x=3\cdot 1+2\cdot 4\equiv 11\equiv 5 \pmod 6$

$x=5$

$5\equiv 1 \pmod 2$

$5\equiv 2 \pmod 3$

$5\equiv 5 \pmod 6$

$5\equiv 5 \pmod{12}$

よって $x=5$」

2.　$\begin{cases} x\equiv 0 \pmod 7 \\ x\equiv 1 \pmod 2 \\ x\equiv 1 \pmod 3 \\ x\equiv 1 \pmod 4 \\ x\equiv 1 \pmod 5 \\ x\equiv 1 \pmod 6 \end{cases}$

$x\equiv 0 \pmod 7$ とおく　$x=7$

$7\equiv 1 \pmod 2$

$7\equiv 1 \pmod 3$

$7\not\equiv 1 \pmod 4$

よって解なし」

3.　$\begin{cases} x\equiv 5 \pmod{12} \\ x\equiv 14 \pmod{15} \\ x\equiv 9 \pmod{20} \end{cases}$

$12=2^2\cdot 3$

$15=3\cdot 5$

$20=2^2\cdot 5$

$\begin{cases} x\equiv 5 \pmod 2 \\ x\equiv 14 \pmod 3 \\ x\equiv 9 \pmod 5 \end{cases}$

$15x_1\equiv 5 \pmod 2$

$x_1=5$

$10x_2\equiv 14 \pmod 3$

$x_2\equiv 14$

$6x_3\equiv 4 \pmod 5$

$x_3\equiv 9$

$15\cdot 5+10\cdot 14+6\cdot 9=269\equiv 29 \pmod{30}$

$29\equiv 5 \pmod{12}$

$29\equiv 14 \pmod{15}$

$29\equiv 9 \pmod{20}$

よって $x=29$」

2.　$x\equiv 0 \pmod 7$ 以外はまとめて

$x\equiv 1 \pmod{(\mathrm{lcm}(2,3,4,5,6))}=1 \pmod{60}$

$1+60k\equiv 0 \pmod 7$

$1+4k\equiv 0 \pmod 7$

$4k\equiv 6 \pmod 7$

$\bmod 7$ で 4 の逆元は 2　($\underbrace{4\cdot 2}_{4^{-1}}\equiv 1 \pmod 7$)

$k\equiv 6\cdot 2=12\equiv 5 \pmod 7$

$x=1+60\cdot 5=301$

最終的な答えは $\mathrm{lcm}(60,7)=420$

$x=301 \pmod{420}$」

5章　2つの要素の組から第3の要素が決まるとき、関数記号を使って
$f(a,b)=c$ と書ける。ある集合Aの上に2変数関数
$f(x,y)$ が定義され、またその値も集合Aに属するとき
$f(x,y)$ を「結合」と呼び、Aを代数的構造と名づける。
ふつう $f(x,y)$ は $x\circ y$ と書く

群Gの定義　1. 結合法則
2. 単位元をもつ
3. 逆元をもつ

例）mod m による整数の剰余類 $R(m)$ は加法に対して
可換の有限群をなす
1. 任意の $x,y,z\in R(m)$ に対して $x+y\in R(m)$
また $(x+y)+z\equiv x+(y+z)$
2. $0\in R(m)$ だから $x+0\equiv x,\ 0+x\equiv x \pmod m$
0は単位元
3. $x\in R(m)$ に対して $-x\in R(m)$ であり
$x+(-x)\equiv 0,\ (-x)+x\equiv 0 \pmod m$

Gの部分群Hを考える。
$x,y\in G$ のとき $xy^{-1}\in H$ をとり $x\sim y$ という関係と定義すると
反射的、対称的、推移的である
1. $xx^{-1}=1$ または $\in H$ したがって $x\sim x\Leftrightarrow$ 反射的
2. $x\sim y$ ならば $xy^{-1}\in H$、Hは群なので逆元を含む
$yx^{-1}\in H$ したがって $y\sim x\Leftrightarrow$ 対称的
3. $x\sim y,\ y\sim z$ ならば $xy^{-1}\in H,\ yz^{-1}\in H$
Hは群なので積を含む $(xy^{-1})(yz^{-1})\in H$
$xz^{-1}\in H$
だから $x\sim z\Leftrightarrow$ 推移的

1.2.3 を満たすので同値関係であり、Gの類別を引き起こす。

※) 群をなさない集合がある部分集合をとって元の集合を
完全に分割は可能。例えばある学校の生徒を誕生日で
分割するときれいに分割でき余りなし
あるいは数の集合を同じ余りで分類できる
しかしこの場合、どんなルールで分割するのかは外から与えられる
群は剰余類によって、その構造自体から分類が
決定づけられ、自然な性質をもつ
（互いに合同
代表元をずうっと持ち

整数の加法群 $G=\mathbb{Z}$ を考える。
部分群 $H=\mathbb{Z}_3=\{\cdots -3,0,3,\cdots\}$
剰余類は $0+\mathbb{Z}_3=\cdots -3,0,3,\cdots$
$1+\mathbb{Z}_3=\cdots -2,1,4,\cdots$
$2+\mathbb{Z}_3=\cdots -1,2,5,\cdots$
$\mathbb{Z}=(0+\mathbb{Z}_3)\cup(1+\mathbb{Z}_3)\cup(2+\mathbb{Z}_3)$

部分群の元 $a_i\in H=\mathbb{Z}_3$
剰余群の代表元 $b_1=0,\ b_2=1,\ b_3=2$
$x=a_i+b_k$ で表す　$x=11$ の場合
$11\equiv 2 \pmod 3 \rightarrow 11\in 2+\mathbb{Z}_3$
$a_i=9,\ b_k=2$

$x=-4$ の場合 $-4\equiv 2 \pmod 3$
$b_k=2,\quad a_i=-4-2=-6\in\mathbb{Z}_3$

一般に

a_1b_1	a_2b_1	⋯	a_mb_1
a_1b_2	a_2b_2	⋯	a_mb_2
⋯	⋯	⋯	⋯
a_1b_l	a_2b_l	⋯	a_mb_l

群Gの位数nは
$n=ml$

定理 pが素数であるとき、乗法群 $K'(p)$ は巡回群である

補題1 整数係数の多項式 $f(x)=x^m+a_1x^{m-1}+\cdots+a_m$ に対して

$$f(x)\equiv 0 \pmod p$$

となる $K'(p)$ の要素 x は m より多くは存在しない。

証明) $m=1$ の場合 $x+a_1\equiv 0 \pmod p$ から $x=-a_1$ であるから

x は1つしかない

つぎに $m-1$ まで正しいと仮定して m に対して正しいことを証明する

$f(x)\equiv 0 \pmod p$ なるすべての x を $x_1, x_2, \cdots, x_l$ とし、

$$f(x_1)\equiv 0 \pmod p$$

$$f(x)\equiv f(x)-f(x_1)=(x-x_1)g(x)$$

ここで $g(x)$ は $m-1$ 次

$$f(x_2)\equiv (x_2-x_1)g(x_2)\equiv 0 \pmod p$$

$$f(x_3)\equiv (x_3-x_1)g(x_3)\equiv 0 \pmod p$$

$$\vdots$$

$$f(x_l)\equiv (x_l-x_1)g(x_l)\equiv 0 \pmod p$$

$x_i-x_1\not\equiv 0 \pmod p$ で p が素数だから ← 0 でない ナニカ

$$g(x_2)\equiv 0$$

$$g(x_3)\equiv 0$$

$$\vdots$$

$$g(x_l)\equiv 0$$

したがって この個数 $l-1$ は $m-1$ より多くはない

$$l-1\leq m-1 \iff l\leq m$$」

補題2 $K'(p)$ で位数 d $(d\mid p-1)$ の要素の個数は $\varphi(d)$ か 0

証明) 位数 d の要素が1つでも存在したら x_0 とする。

このとき d 個の要素 $1, x_0, x_0^2, \cdots x_0^{d-1}$ は互いに異なる

要素で、しかも $k=0,1,\cdots,d-1$ のとき

$$(x_0^k)^d=x_0^{kd}=(x_0^d)^k\equiv 1^k=1$$

すなわち この d 個の要素はすべて $x^d-1\equiv 0 \pmod p$ を満足する

補題1により $x^d\equiv 1 \pmod p$ となる x は d 個以上はないから

そのような x は $1, x_0, x_0^2, \cdots, x_0^{d-1}$ が全部である

この中で位数 d の要素はいくつあるか

$(k,d)=1$ のとき $(x^k)^r\equiv 1$ ならば $x^{kr}\equiv 1 \pmod p$

これから $kr\equiv 0 \pmod p$

$(k,d)=1$ だから $r\equiv 0 \pmod p$

したがって $0<r<d$ である r については $(x_0^k)^r\equiv 1$ とはならない

つまりその位数は ちょうど d

また $(k,d)>1$ ならば $(k,d)=s>1$ として

$$(x^k)^{\frac{d}{s}}=(x^{\frac{kd}{s}})=(x^d)^{\frac{k}{s}}\equiv 1^{\frac{k}{s}}=1$$

となるから 位数は d より小さい

だから d と互いに素な指数 k をもつ x_0^k $((k,d)=1)$

が位数 d の要素であり、その個数は $\varphi(d)$ である。

x_0 なるものが1つもないとき、もちろん個数は 0」

定理の証明) $K'(p)$ の要素を位数によって分類してみよう

$k(d)$ $(d\mid p-1)$ を位数 d の要素の集合とすると

$k(d)$ の合併集合が $K'(p)$ である。

ところがその個数 $p(d)$ は 0 または $\varphi(d)$ である

したがって $p(d)\leq\varphi(d)$

$p-1$ のすべての約数 d にわたる $p(d)$ の和をつくると もちろん $p-1$

$$\sum_{d\mid p-1}p(d)=p-1$$

一方 $\sum_{d\mid p-1}\varphi(d)=p-1$ であるから $\sum_{d\mid p-1}(\varphi(d)-p(d))=0$

各項は負でないから $\varphi(d)=p(d)$

とくに $p(p-1)=\varphi(p-1)$

つまり位数 $p-1$ の要素は $\varphi(p-1)$ だけ存在する

そのうちの1つを h とすると $1, h, h^2, \cdots, h^{p-2}$ は $K'(p)$ と一致する

つまり $K'(p)$ は h を生成元とする巡回群」

↑

原子根

有限環となる $R(6)$ で乗法を考えると

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$R'(6) = \{1, 5\}$

既約剰余系 ← 逆元をもつ

逆に 0, 2, 3, 4 は逆元をもたず

$\left.\begin{array}{l} 2\cdot 3 \equiv 0 \\ 3\cdot 2 \equiv 0 \\ 4-3 \equiv 0 \end{array}\right\} \bmod 6$

となる、かけて 0 になるときの要素を零因子という

↑ 0 以外で

有限体となる $R(7)$ で乗法を考えると

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

→ 0 以外の要素に 0 が出てこず
零因子がない
→ $R(7)$ は体となる

$R(2)$ で + と × の表をつくると

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

記号論理と密接な関係をもつ

$T(A) = \begin{cases} 1 & (\text{真}) \\ 0 & (\text{偽}) \end{cases}$ $\quad \wedge, \vee, \overline{A}$

$T(A \wedge B) = T(A) \cdot T(B)$

$T(\overline{A}) = 1 - T(A)$

$T(A \vee B) = T(A) + T(B) + T(A \wedge B)$

$x^2 \equiv a \pmod p$ が解をもつかどうかは定理から

$a^{\frac{p-1}{2}} \equiv 1 \pmod p$ が成り立つかで定まる

$x^2 \equiv a \pmod p$ に解があるとき a は p の平方剰余、解がないとき平方非剰余という

ルジャンドルは $\left(\frac{a}{p}\right) = \begin{cases} 1 & (a \text{ が } p \text{ の平方剰余}) \\ -1 & (a \text{ が } p \text{ の平方非剰余}) \end{cases}$ と定義した

ルジャンドルの記号

定理 $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ となる

例 $\left(\frac{2}{5}\right) \equiv 2^{\frac{5-1}{2}} \equiv 2^2 \equiv 4 \equiv -1 \pmod 5$

$\left(\frac{3}{7}\right) \equiv 3^{\frac{7-1}{2}} \equiv 3^3 \equiv 27 \equiv -1 \pmod 7$

$\left(\frac{2}{7}\right) \equiv 2^{\frac{7-1}{2}} \equiv 2^3 \equiv 8 \equiv -1 \pmod 7$

$\left(\frac{6}{11}\right) \equiv 6^{\frac{11-1}{2}} \equiv 6^5 \equiv (6^2)^2 \cdot 6 \equiv 36^2 \cdot 6 \equiv 3^2 \cdot 6 \equiv 54 \equiv -1 \pmod{11}$

定理 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

証明 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod p$

p の平方剰余と非剰余を見分けるには、p の原子根 h にたして
h の偶数乗が平方剰余で、奇数乗が非剰余である。

$\sqrt{2}$ を連分数で表す

$a_0 = [\sqrt{2}] = [1.41\cdots] = 1$

$a_1 = \left[\frac{1}{\sqrt{2}-1}\right] = \left[\frac{\sqrt{2}+1}{2-1}\right] = [\sqrt{2}+1] = 2$

$a_2 = \left[\frac{1}{\sqrt{2}+1-a_1}\right] = \left[\frac{1}{\sqrt{2}+1-2}\right] = \left[\frac{1}{\sqrt{2}-1}\right] = 2$

以下は同じく $a_3 = a_4 = \cdots = 2$

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2+\cdots}}$$

$\sqrt{3}$ を連分数で表す

$a_0 = [\sqrt{3}] = 1$

$a_1 = \left[\frac{1}{\sqrt{3}-1}\right] = \left[\frac{\sqrt{3}+1}{3-1}\right] = \left[\frac{\sqrt{3}+1}{2}\right] = 1$

$a_2 = \left[\frac{1}{\frac{\sqrt{3}+1}{2}-1}\right] = \left[\frac{1}{\frac{\sqrt{3}-1}{2}}\right] = \left[\frac{2}{\sqrt{3}-1}\right] = \left[\frac{2(\sqrt{3}+1)}{3-1}\right] = [\sqrt{3}+1] = 2$

$a_3 = \left[\frac{1}{\sqrt{3}+1-2}\right] = \left[\frac{1}{\sqrt{3}-1}\right]$, a_1 と同じ

したがって $a_4 = 2$, $a_5 = 1$

$a_6 = 2$, $a_7 = 1$

$\vdots$

$a_0, a_1, a_2, a_3 \cdots$ は $1, 1, 2, 1, 2, 1, 2 \cdots$ となる

広義の1次関数 $y = \frac{\alpha x + \beta}{\gamma x + \delta}$ $(\alpha\delta - \beta\gamma \neq 0)$

$\begin{cases} y_1 = \alpha x_1 + \beta x_2 \\ y_2 = \gamma x_1 + \delta x_2 \end{cases}$ において $\frac{y_1}{y_2} = y$, $\frac{x_1}{x_2} = x$ とおいた

ときの x の y への変換ともいえる

行列で書くと $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ において $\begin{matrix} x_1 \\ x_2 \end{matrix} \to \begin{matrix} y_1 \\ y_2 \end{matrix}$ の変換

したがって $y = \frac{\alpha x + \beta}{\gamma x + \delta} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}(x)$ と書くことにする

このとき2つの関数の合成は

$$z = \frac{\alpha' y + \beta'}{\gamma' y + \delta'} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}(y)$$

$$= \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}\left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}(x)\right)$$

$$= \left(\begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}(x)\right)$$

行列の乗法になる

この記法を用いると

$$w_n = a_n + \frac{1}{w_{n+1}} = \frac{a_n w_{n+1} + 1}{w_{n+1}} = \frac{a_n w_{n+1} + 1}{1 \cdot w_{n+1} + 0} = \begin{bmatrix} a_n & 1 \\ 1 & 0 \end{bmatrix}(w_{n+1})$$

$\begin{bmatrix} a_n & 1 \\ 1 & 0 \end{bmatrix}$ を $H(a_n)$ とすると $w_n = H(a_n)(w_{n+1})$

$$w = H(a_0)(w_1) = H(a_0)H(a_1)(w_2)$$

$$= \cdots$$

$$= H(a_0)H(a_1)\cdots H(a_n)(w_{n+1})$$

ここで $H(a_0)H(a_1)\cdots H(a_n) = \begin{bmatrix} h_{11}^{(n)} & h_{12}^{(n)} \\ h_{21}^{(n)} & h_{22}^{(n)} \end{bmatrix}$ とおく

$$\begin{bmatrix} h_{11}^{(n+1)} & h_{12}^{(n+1)} \\ h_{21}^{(n+1)} & h_{22}^{(n+1)} \end{bmatrix} = H(a_0)H(a_1)\cdots H(a_n)H(a_{n+1})$$

$$= \begin{bmatrix} h_{11}^{(n)} & h_{12}^{(n)} \\ h_{21}^{(n)} & h_{22}^{(n)} \end{bmatrix}\begin{bmatrix} a_{n+1} & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} h_{11}^{(n)} a_{n+1} + h_{12}^{(n)} & h_{11}^{(n)} \\ h_{21}^{(n)} a_{n+1} + h_{22}^{(n)} & h_{21}^{(n)} \end{bmatrix}$$

この式から $h_{12}^{(n+1)} = h_{11}^{(n)}$

$h_{22}^{(n+1)} = h_{21}^{(n)}$

ここで $h_{11}^{(n)} = q_n$, $h_{21}^{(n)} = p_n$ とおくと

$h_{12}^{(n)} = h_{11}^{(n-1)} = q_{n-1}$, $h_{22}^{(n)} = h_{21}^{(n-1)} = p_{n-1}$ から

$$H(a_0)H(a_1)\cdots H(a_n) = \begin{bmatrix} q_n & q_{n-1} \\ p_n & p_{n-1} \end{bmatrix}$$

$n=0$ のときは $H(a_0) = \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix}$

一方行列式 $|H(a_n)|$ は $|H(a_n)| = a_n \cdot 0 - 1 \cdot 1 = -1$

したがって $|H(a_0)H(a_1)\cdots H(a_n)| = |H(a_0)|\cdot|H(a_1)|\cdots|H(a_n)|$

$= (-1)^{n+1}$

定理 $\begin{vmatrix} q_n & q_{n-1} \\ p_n & p_{n-1} \end{vmatrix} = q_n p_{n-1} - q_{n-1} p_n = (-1)^{n+1}$

$$w = H(a_0)H(a_1)\cdots H(a_n)(w_{n+1})$$

$$= \begin{bmatrix} q_n & q_{n-1} \\ p_n & p_{n-1} \end{bmatrix}(w_{n+1})$$

$$= \frac{q_n w_{n+1} + q_{n-1}}{p_n w_{n+1} + p_{n-1}}$$

ここで $w - \frac{q_n}{p_n} = \frac{q_n w_{n+1} + q_{n-1}}{p_n w_{n+1} + p_{n-1}} - \frac{q_n}{p_n}$

$$= \frac{p_n(q_n w_{n+1} + q_{n-1}) - q_n(p_n w_{n+1} + p_{n-1})}{p_n(p_n w_{n+1} + p_{n-1})}$$

$$= \frac{q_{n-1} p_n - q_n p_{n-1}}{p_n(p_n w_{n+1} + p_{n-1})}$$

$$= \frac{-(q_n p_{n-1} - q_{n-1} p_n)}{p_n(p_n w_{n+1} + p_{n-1})}$$

$$= \frac{-(-1)^{n+1}}{p_n(p_n w_{n+1} + p_{n-1})} = \frac{(-1)^{n+2}}{p_n(p_n w_{n+1} + p_{n-1})}$$

$$= \frac{(-1)^n}{p_n(p_n w_{n+1} + p_{n-1})}$$

定理 $w - \frac{q_n}{p_n} = \frac{(-1)^n}{p_n(p_n w_{n+1} + p_{n-1})}$

このとき $w_{n+1} > 1$ であるから右辺の分母は p_n^2 より大きい

$$\left|w - \frac{q_n}{p_n}\right| < \frac{1}{p_n^2}$$

つまり $\frac{q_n}{p_n}$ は w に近似する分数であり,

しかも w との差は $\frac{1}{p_n^2}$ より小さくなるから, それなりに良い近似である

また分子の $(-1)^n$ は n が偶数のとき正で $w > \frac{q_n}{p_n}$

奇数のとき負で $w < \frac{q_n}{p_n}$