第2章　整数の話

2.0　素数の7つの不思議 (朝日新聞 2004/09/14 夕刊より)

話題1 (長い研究の歴史と今も残る難問)

・　Fermat の最終定理 (Fermat 予想)

「$x^n + y^n = z^n$ は $n \geqq 3$ の時，非自明な (どれも 0 ではない) 整数解は存在しない」

の決着=証明に 350 年以上を要した.

・　双子素数予想

「差が 2 である素数の組は無限にある」

は未解決.

・　Goldbach 予想

「2 より大きなすべての偶数は 2 つの素数の和で表わせる」

は未解決.

話題2 (旧石器時代から素数は知られていた？)

コンゴのイシャンゴ遺跡から見つかった骨には 3 列にわたって数字が刻み込まれているが，その 1 列には

11,13,17,19

と素数ばかり並んでいる．また，全部で 16 個の数字のうち 10 個が素数

(2 万年前の遺跡でメソポタミア文明より 1 万年以上前)

話題3 (まだまだ遠い Riemann 予想の解決)

Riemann 予想

「Riemann のゼータ関数

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{k^s} + \cdots$$

のゼロ点は自明なゼロ点 (負の偶数) を除けばすべて $\mathrm{Re}(s) = \frac{1}{2}$ のところにある」の解決はまだまだ時間を要しそう.

話題 4 (自然数の中に素数はどれくらいある？=素数分布)

$\pi(x) = x$ 以下の素数の個数

$\pi(10) = 4 \quad , \quad \pi(100) = 25 \quad , \quad \pi(1000) = 168$

$\pi(10000) = 1229 \quad , \quad \pi(4 \times 10^{22}) = 7.839641598470563038 58 \times 10^{20}$

$\pi(x) \sim \dfrac{x}{\log x} \quad (\lim_{x\to\infty} \dfrac{\pi(x)}{\frac{x}{\log x}} = 1)$

話題 5 (これまでに見つかった最大の素数)

$2^{24036583} - 1$: 723 万 5733 桁の素数

$2^n - 1$ の形の数をメルセンヌ (Mersenne) 数, それが素数である時はメルセンヌ素数

メルセンヌ数は素数かどうか判定しやすい.

一般に大きな数が素数かどうか判定する事より，大きな数の素因数分解はずっと難しい.

話題 6 (10 億桁の素数を見つけると 3 千万円の賞金)

大きな素数は暗号に利用される.

より安全な暗号のためにはより大きな素数の発見が有用.

話題 7 (素数は数学の原子)

素数について調べる事は手触り感覚で味わえるので，プロでなくても可能.

数学のプロにとっても奥が深い．数学のいろんなところに広がりをもつ.

参考書

[1] Neal Koblitz, *A Course in Number Theory and Cryptography (second edition)*,Springer,1994

[2] 笠原 正雄, 境 隆一,「暗号　— ネットワーク社会の安全を守る鍵—」, 共立出版, 2002

[3] 一松 信,「暗号の数理　— 作り方と解読の原理—」, 講談社 BLUE BACKS, 1980

[4] 小川　洋子,「博士の愛した数式」, 新潮社, 2003

以下の章では，[1] の第 1 章にしたがって，話をすすめていく.

2.1 $b-$ 進法

. 10 進法

$(357.062\cdots)_{10} = 3\cdot 10^2 + 5\cdot 10^1 + 7\cdot 10^0 + 0\cdot 10^{-1} + 6\cdot 10^{-2} + 2\cdot 10^{-3} + \cdots$

. $b-$ 進法

$(d_{k-1}d_{k-2}\cdots d_0.d_{-1}d_{-2}\cdots)_b = d_{k-1}\cdot b^{k-1} + d_{k-2}\cdot b^{k-2} + \cdots + d_0\cdot b^0 + d_{-1}\cdot b^{-1} + d_{-2}\cdot b^{-2} + \cdots$

b : base(基数)　　d_i : digit(数字)

2 進法 (binary system)　　bit: binary digit を縮めた言い方　0 or 1

$11 \leqq b \leqq 26$ の時は 0〜25 までの数字に A〜Z を割り当てる．あるいは

$11 \leqq b \leqq 36$ の時は 0〜9 まではそのまま用い，10〜35 の数字に A〜Z を割り当てる．

コンピュータで 16 進法は

0 , 1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , A(10) , B(11) , C(12) , D(13) , E(14) , F(15)

を用いる．

Example II.1.1　(a) $(11001001)_2 = 1\cdot 2^7 + 1\cdot 2^6 + 1\cdot 2^3 + 1 = 128 + 64 + 8 + 1 = 201$

(b) $(\mathrm{BAD})_{26} = 1\cdot 26^2 + 0\cdot 26^1 + 3\cdot 26^0 = 676 + 3 = 679$

$(\mathrm{B.AD})_{26} = 1\cdot 26^0 + 0\cdot 26^{-1} + 3\cdot 26^{-2} = 1 + \frac{3}{676}$

Example II.1.2　160 と 199 を 7 進法で表わし，7 進法で掛け算せよ．

$$\begin{array}{rcl} 7\,)\,160 & \cdots & 6 \\ 7\,)\,22 & \cdots & 1 \\ 7\,)\,3 & \cdots & 3 \\ 0 & & \end{array} \qquad \begin{array}{rcl} 7\,)\,199 & \cdots & 3 \\ 7\,)\,28 & \cdots & 0 \\ 7\,)\,4 & \cdots & 4 \\ 0 & & \end{array} \qquad \begin{array}{r} (316)_7 \\ (403)_7 \\ \hline (1254)_7 \\ (16030)_7 \\ \hline (161554)_7 \end{array}$$

$160 = (316)_7$　　$199 = (403)_7$　　$(316)_7 \times (403)_7 = (161554)_7$

Example II.1.3

$(11001001)_2 \div (100111)_2 = (101)_2 + \dfrac{(110)_2}{(100111)_2}$

$$
\begin{array}{rr}
 & 101 \\
\hline
100111\ ) & 11001001 \\
 & 100111 \\
\hline
 & 101101 \\
 & 100111 \\
\hline
 & 110
\end{array}
$$

Example II.1.4　10^6 を 2 進法，7 進法，26 進法で表わせ．

$10^6 = (11110100001001000000)_2 = (11333311)_7 = (\mathrm{CEXHO})_{26}$

$$
\begin{array}{rrrr}
26\ ) & 1000000 & \cdots & 14(\mathrm{O}) \\
\hline
26\ ) & 38461 & \cdots & 7(\mathrm{H}) \\
\hline
26\ ) & 1479 & \cdots & 23(\mathrm{X}) \\
\hline
26\ ) & 56 & \cdots & 4(\mathrm{E}) \\
\hline
26\ ) & 2 & \cdots & 2(\mathrm{C}) \\
\hline
 & 0 & &
\end{array}
$$

Example II.1.5　$\pi = 3.1415926\cdots$ を 2 進法で小数点以下 15 桁 (7 桁) まで表わせ．また，26 進法で小数点以下 3 桁まで表わせ．

$3 = (11)_2$

$0.1415926\cdots = d_{-1}\cdot 2^{-1} + d_{-2}\cdot 2^{-2} + d_{-3}\cdot 2^{-3} + \cdots$

$\times 2$　　$0.2831852\cdots = d_{-1} + d_{-2}\cdot 2^{-1} + d_{-3}\cdot 2^{-2} + \cdots$　　より　$d_{-1} = 0$

$\times 2$　　$0.5663704\cdots = d_{-2} + d_{-3}\cdot 2^{-1} + d_{-4}\cdot 2^{-2} + \cdots$　　より　$d_{-2} = 0$

$\times 2$　　$1.1327408\cdots = d_{-3} + d_{-4}\cdot 2^{-1} + d_{-5}\cdot 2^{-2} + \cdots$　　より　$d_{-3} = 1$

1 を引いて $\times 2$　　$0.2654816\cdots = d_{-4} + d_{-5}\cdot 2^{-1} + d_{-6}\cdot 2^{-2} + \cdots$　　より　$d_{-4} = 0$

$\times 2$　　$0.5309632\cdots = d_{-5} + d_{-6}\cdot 2^{-1} + d_{-7}\cdot 2^{-2} + \cdots$　　より　$d_{-5} = 0$

$\times 2$　　$1.0619264\cdots = d_{-6} + d_{-7}\cdot 2^{-1} + d_{-8}\cdot 2^{-2} + \cdots$　　より　$d_{-6} = 1$

1 を引いて $\times 2$　　$0.1238528\cdots = d_{-7} + d_{-8}\cdot 2^{-1} + d_{-9}\cdot 2^{-2} + \cdots$　　より　$d_{-7} = 0$

以上より　$\pi = 3.1415926\cdots = (11.0010010\cdots)_2$

$3 = (\mathrm{D})_{26}$

$0.1415926\cdots = d_{-1}\cdot 26^{-1} + d_{-2}\cdot 26^{-2} + d_{-3}\cdot 26^{-3} + \cdots$

$\times 26$　　$3.6814076\cdots = d_{-1} + d_{-2}\cdot 26^{-1} + d_{-3}\cdot 26^{-2} + \cdots$　　より　$d_{-1} = 3 = (\mathrm{D})_{26}$

3 を引いて $\times 26$　　$17.716597\cdots = d_{-2} + d_{-3}\cdot 26^{-1} + \cdots$　　より　$d_{-2} = 17 = (\mathrm{R})_{26}$

17 を引いて$\times 26$　$18.6315227\cdots = d_{-3} + d_{-4}\cdot 26^{-1} + \cdots$　より　$d_{-3} = 18 = (\mathrm{S})_{26}$
以上より　$\pi = 3.1415926\cdots = (\mathrm{D.DRS}\cdots)_{26}$

問題 1-1　$(212)_3 \times (122)_3 = ?$

問題 1-2　$(40122)_7 \div (126)_7 = ?$

問題 1-3　$(101101)_2 \times (11001)_2 = ?$
$(10011001)_2 \div (1011)_2 = ?$

問題 1-4　$(\mathrm{YES})_{26} \times (\mathrm{NO})_{26} = ?$
$(\mathrm{JQVXHJ})_{26} \div (\mathrm{WE})_{26} = ?$

問題 1-5　$e = 2.7182818\cdots$ を 2 進法で小数点以下 15 桁まで表わせ．また，26 進法で小数点以下 3 桁まで表わせ.

問題 1-6　$\dfrac{c}{d}$ を $b-$ 進法で表わす時，周期 f の純循環小数となるための必要十分条件は $b^f - 1$ が d の倍数になっていることである．このことを示せ.

問題 1-7　(a)　16 進法の数字を 0〜9,10(A),11(B),12(C),13(D),14(E),15(F) で表わすとき，$(131\mathrm{B6C3})_{16} \div (1\mathrm{A2F})_{16} = ?$
(b)　2 進法から 16 進法へ変換する方法を説明せよ．また，16 進法から 2 進法へ変換する方法を説明せよ.

問題 1-8〜問題 1-16　省略

2.2　Divisibility(整除性) と Euclid の互除法

定義　a, b:整数 (integer) とする.

$a|b \overset{\text{def}}{\Longleftrightarrow} \exists d$: 整数　$s.t.$　$b = ad$

このとき,「a は b を割り切る」,「a は b の約数 (diviser) である」,「b は a の倍数 (multiple) である」という.

真の約数 (proper diviser)：自分自身以外の約数

非自明な約数 (non-trivial diviser)：自分自身と 1 以外の約数

素数 (prime number)：1 より大きな整数で，1 と自分自身以外に正の約数をもたないもの

合成数 (composite number)：少なくとも 1 つの非日自明な約数を持つ整数

p を素数とする.

$p^\alpha \| b \overset{\text{def}}{\Longleftrightarrow} p^\alpha | b$　かつ　$p^{\alpha+1} \not| b$

Divisibility の基本的性質

1. $a|b$ かつ $\forall c$: 整数　$\Longrightarrow$　$a|bc$
2. $a|b$ かつ $b|c$　$\Longrightarrow$　$a|c$
3. $a|b$ かつ $a|c$　$\Longrightarrow$　$a|(b \pm c)$

算術の基本定理 (The Fundamental Theorem of Arithmetic)

任意の自然数は (因子の順序を無視すれば) 一通りに素因数分解が出来る．小さい素数の順番に書くのが通常である．(例　$4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$)

Divisibility の基本的性質 (続き)

4. p : 素数　,　$a|bc \Longrightarrow$　$a|b$　または　$p|c$
5. $m|a$　,　$n|a$　かつ　m と n が共通の約数 (公約数) をもたない　$\Longrightarrow$　$mn|a$

自然数 n の約数は何通りあるか？

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$(素因数分解)

とすると，n の任意の約数 d は

$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \quad (0 \leqq \beta_i \leqq \alpha_i)$

の形である．よって，$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ の約数の個数は

$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$

である．(例 $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$ の約数の個数は $(3+1)(1+1)(2+1)(1+1) = 48$ 個)

定義 0 と異なる 2 つの整数 a と b について，a と b の両方を割り切る最大の整数を最大公約数 (greatest common diviser) といい，$g.c.d.(a,b)$ と書く．

$g.c.d.(a,b)$：a と b を割り切り，a と b の任意の公約数によって割り切られる唯一つの正の数

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$

とすると，

$g.c.d.(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$ ここで， $\gamma_i = \min(\alpha_i, \beta_i)$

a と b の両方が割り切る最小整数を最小公倍数 (least common multiple) といい，$l.c.m.(a,b)$ と書く．

$l.c.m.(a,b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_r^{\delta_r}$ ここで， $\delta_i = \max(\alpha_i, \beta_i)$

$l.c.m.(a,b) = \dfrac{|a \cdot b|}{g.c.d.(a,b)} \quad (\max(\alpha,\beta) + \min(\alpha,\beta) = \alpha + \beta)$

例 $4200 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1$, $10780 = 2^2 \cdot 5^1 \cdot 7^2$

$g.c.d.(4200, 10780) = 2^2 \cdot 5^1 \cdot 7^1$

$l.c.m.(4200, 10780) = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^2$

Euclid の互除法 (Euclidean algorithm)

大きな数に対して素因数分解が分からない時でも，2 つの数 a と b の最大公約数 $g.c.d.(a,b)$ を簡単な方法で求める事が出来る．

原理

$a \geqq b$ とする．$a \div b$：商を q，余りを r とする．すなわち，$a = bq + r \quad (0 \leqq r \leqq b-1)$

このとき．$g.c.d.(a,b) = g.c.d.(b,r)$ $\quad (\because\ d : a \text{ と } b \text{ の公約数} \iff d : b \text{ と } r \text{ の公約数})$

algorithm

$a \geqq b$ とする．

(1) $a \div b$：商 q_1，余り $r_1(r_1 > 0)$ $\quad a = bq_1 + r_1$ $\quad g.c.d.(a,b) = g.c.d.(b,r_1)$

(2) $b \div r_1$：商 q_2，余り $r_2(r_2 > 0)$ $\quad b = r_1q_2 + r_2$ $\quad g.c.d.(b,r_1) = g.c.d.(r_1,r_2)$

(3) $r_1 \div r_2$：商 q_3，余り $r_3(r_3 > 0)$ $\quad r_1 = r_2q_3 + r_3$ $\quad g.c.d.(r_1,r_2) = g.c.d.(r_2,r_3)$

(4) $r_2 \div r_3$：商 q_4，余り $r_4(r_4 > 0)$ $\quad r_2 = r_3q_4 + r_4$ $\quad g.c.d.(r_2,r_3) = g.c.d.(r_3,r_4)$

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

(k) $r_{k-2} \div r_{k-1}$：商 q_k，余り $r_k(r_k > 0)$ $\quad r_{k-2} = r_{k-1}q_k + r_k$

$g.c.d.(r_{k-2},r_{k-1}) = g.c.d.(r_{k-1},r_k)$

(k+1) $r_{k-1} \div r_k$：商 q_{k+1}，余り $r_{k+1} = 0$ $\quad r_{k-1} = r_kq_{k+1}$

$d = g.c.d.(a,b) = g.c.d.(r_{k-1},r_k) = r_k$:最大公約数

Example II.2.1 $g.c.d.(1547, 560)$ を見つけよ．

$$1547 = 560 \cdot 2 + 427$$
$$560 = 427 \cdot 1 + 133$$
$$427 = 133 \cdot 3 + 28$$
$$133 = 28 \cdot 4 + 21$$
$$28 = 21 \cdot 1 + 7$$
$$21 = 7 \cdot 3$$
$$g.c.d.(1547, 560) = 7$$

Proposition II.2.1(省略)

Proposition II.2.2 $\quad d = g.c.d.(a,b) \implies \exists u, v : \text{integer} \ \ s.t \ \ d = au + bv$

すなわち，2つの整数 a と b の最大公約数 d は a と b の整数係数の1次結合表わせる．

Outline of proof(以下の方法を **拡張 Euclid の互除法** という) Euclid の互除法の式を逆にたどって,

$d = r_k = r_{k-2} - r_{k-1}q_k$ の式に $r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$ を代入．それに，$r_{k-2}.r_{k-3}, \cdots$ を次々に代入していけば，d は a と b の整数係数の 1 次結合表わせる．

Example II.2.1(続き)

$$\begin{aligned} 7 &= 28 - 21 \cdot 1 = 28 - (133 - 28 \cdot 4) \cdot 1 \\ &= 5 \cdot 28 - 1 \cdot 133 = 5 \cdot (427 - 133 \cdot 3) - 1 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16 \cdot (560 - 427 \cdot 1) \\ &= 21 \cdot 427 - 16 \cdot 560 = 21 \cdot (1547 - 560 \cdot 2) - 16 \cdot 560 \\ &= 21 \cdot 1547 - 58 \cdot 560 \end{aligned}$$

定義 a, b:整数 (integer) とする．

a と b は互いに素 (relatively prime)

$\overset{\text{def}}{\iff} g.c.d.(a, b) = 1$ ($i.e.$ a と b は 1 より大きな公約数を持たない)

定義 (Euler の φ 関数)

n:自然数 (natural number) とする．

$$\varphi(n) \overset{\text{def}}{=} \#\{b \in \boldsymbol{Z} \mid 1 \leqq b \leqq n \text{ かつ } g.c.d.(b, n) = 1\}$$

(# は集合の個数を表わすこと事にする)

$\varphi(n)$ は n 以下の n と互いに素である数の個数である．

例 $\varphi(1) = \#\{1\} = 1$, $\varphi(2) = \#\{1\} = 1$, $\varphi(3) = \#\{1, 2\} = 2$,

$\varphi(4) = \#\{1, 3\} = 2$, $\varphi(5) = \#\{1, 2, 3, 4\} = 4$, $\varphi(6) = \#\{1, 5\} = 2$

p：素数のとき，$\varphi(p) = \#\{1, 2, \cdots, p-1\} = p - 1$

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$$

($\because$ $1 \sim p^\alpha$ のうち，p^α と素でないものは $\{1 \cdot p\ ,\ 2 \cdot p\ ,\ \cdots\ ,\ p^{\alpha-1} \cdot p\}$ の $p^{\alpha-1}$ 個)

問題 2-1 (a) つぎのことを証明せよ．

(i) $p^\alpha \| a$ かつ $p^\beta \| b$ $\implies$ $p^{\alpha+\beta} \| a \cdot b$

(ii)　$p^\alpha \| a$ ，$p^\beta \| b$　かつ　$\alpha < \beta$　$\Longrightarrow$　$p^\alpha \| (a \pm b)$

(b)　次の命題の反例を示せ.「$p^\alpha \| a$　かつ　$p^\alpha \| b$　$\Longrightarrow$　$p^\alpha \| (a+b)$」

問題 2-2　945 の約数は何個あるか？　それらをすべて挙げよ.

問題 2-3　n を正の奇数 (positive odd number) とする.

(a)　n の $\sqrt{n}$ より小さい約数と $\sqrt{n}$ より大きい約数には 1 対 1(1 to 1) の対応があることを示せ.(ここでは，n が奇数である必要はない)

(b)　n の $\sqrt{n}$ 以上の約数と n を 2 つの非負整数の平方の差 $s^2 - t^2$ のすべての書き表わし方と 1 対 1(1 to 1) の対応があることを示せ.

(c)　945 を 2 つの非負整数の平方の差に表わす方法をすべて挙げよ.

問題 2-4　(a)　$n!$ を正確に割り切る (exactly divide) 素数 p の巾は

$$[n/p] + [n/p^2] + [n/p^3] + \cdots \quad (\text{有限和})$$

であることを示せ.

(b)　100! は 2 の何乗で割り切れるか？

100! は 3 の何乗で割り切れるか？

100! は 5 の何乗で割り切れるか？

100! は 7 の何乗で割り切れるか？

100! を素因数分解せよ.

(c)　$S_b(n)$：n を $b-$ 進法で表わしたとき，現れる 1 個 1 個の数字の和

とする．$n!$ を正確に割り切る 2 の巾は $n - S_2(n)$ であることを示せ.

さらに，$n!$ を素数 p で正確に割り切る巾についての公式を見つけ，それを証明せよ.

問題 2-5　$d = g.c.d.(360, 294)$ を 2 つの方法で求めよ.

(a)　2 つの数を素因数分解して求める方法

(b)　Euclid の互除法

問題 2-6　つぎの 2 つの数の最大公約数を Euclid の互除法を用いて求め，その最大公約数を 2 つの数の 1 次結合で表わせ.

(a) 26 , 18 (b) 187 , 34 (c) 841 , 160 (d) 2613 , 2171

問題 2-7〜問題 2-11(省略)

問題 2-12 実数係数 (任意の体でも良い) の多項式 (polynomial) について考える.

f, g : 多項式

$f|g \overset{\text{def}}{\iff} \exists h$: 多項式 $s.t.\ g = f \cdot h$ (f は g を割り切る)

$g.c.d.(f, g)$: f と g を割り切る最大次数の多項式

一意的ではないが, 0 でない実数倍の違いだけ.

最高次数の 係数を 1 にする (monic) 多項式とすれば, 一意的

f と g は互いに素 $\overset{\text{def}}{\iff}$ $g.c.d.(f, g) = 1$

Euclid の互除法が整数の場合と同様に可能

(a) $g.c.d.(x^4 + x^2 + 1, x^2 + 1) =?$

(b) $g.c.d.(x^4 - 4x^3 + 6x^2 - 4x + 1, x^3 - x^2 + x - 1) =?$

(a) と (b) の場合に最大公約数を f と g の多項式係数の 1 次結合で表わせ.

($g.c.d. = u(x)f(x) + v(x)g(x)$ となる多項式 $u(x)$ と $v(x)$ を見つけよ)

問題 2-13 $f(x) = 0$ が重根をもつとき,

「α: $f(x) = 0$ の重根 $\implies$ α: $g.c.d.(f(x), f'(x)) = 0$ の根」

であることを示せ. さらに, $x^4 - 2x^3 - x^2 + 2x + 1 = 0$ の重根を求めよ.

問題 2-14(Gaussian integer)

α: Gauss 整数 (Gaussian integer) $\overset{\text{def}}{\iff}$ $\alpha = a + bi$ ($a.b \in \boldsymbol{Z}$)

ここで, $\boldsymbol{Z}$ は整数全体の集合を表わす.

α , β : Gauss 整数であるとき,

$\alpha|\beta \overset{\text{def}}{\iff} \exists\gamma \quad s.t. \quad \beta = \alpha \cdot \gamma$

$g.c.d.(\alpha, \beta) \overset{\text{def}}{=}$ αとβを割り切る絶対値が最大である Gauss 整数

(一意的ではないが, -1 倍, $\pm i$ 倍の違いだけ)

Gauss 整数の場合の Euclid の互除法

$\alpha \div \beta$ ($|\alpha| \geqq |\beta| \neq 0$ とする)

$\frac{\alpha}{\beta}$ に複素数平面上で最も近い Gauss 整数を商 γ とし，余りを $\rho = \alpha - \beta \cdot \gamma$ とする．

(最も近い Gauss 整数が複数個あるときはそのどれでも良い)

このとき，$|\rho| = |(\frac{\alpha}{\beta} - \gamma)| \cdot |\beta| \leqq \frac{1}{\sqrt{2}}|\beta|$

$\alpha = \beta \cdot \gamma + \rho$ $(|\rho| \leqq |\beta|)$ と書け，$g.c.d.(\alpha, \beta) = g.c.d.(\beta, \rho)$

以下，整数の場合の Euclid の互除法と同様にすればよい，

次の最大公約数を求めよ．

(a)　$g.c.d.(5+6i, 3-2i)$　　(b)　$g.c.d.(7-11i, 8-19i)$

問題 2-15　ある種の大きな素数を 2 つの平方の和に表わす方法を与える．

素数 p が b^6+1 の形の数を割り切っているとする．

このとき，$p = c^2 + d^2 = (c+di)(c-di)$ となる c と d を見つけたい．

$$b^6 + 1 = (b^2+1)(b^4-b^2+1)\ , \qquad b^4 - b^2 + 1 = (b^2-1)^2 + b^2$$

p は (b^2+1) か (b^4-b^2+1) のどちらかを割り切っている．

p が $b^2+1 = (b+i)(b-i)$ を割り切っているときは，

$c + di = g.c.d.(p, b+i)$ とすればよい．

p が $b^4 - b^2 + 1 = ((b^2-1)+bi) \cdot ((b^2-1)-bi)$ を割り切っているときは，

$c + di = g.c.d.(p, (b^2-1)+bi)$ とすればよい．

Example　12277 は $20^6+1 = (20^2+1)(20^4-20^2+1)$ を割り切っており，

$20^4 - 20^2 + 1 = 159601$ を割り切っている．

よって，$g.c.d.(1277, (20^2-1)+20i) = g.c.d.(1277, 399+20i)$ を見つけたい．

$$12277 = (399+20i)(31-2i) + (-132+178i)$$

$$399 + 20i = (-132+178i)(-1-i) + (89+66i)$$

$$-132 + 178i = (89+66i)(2i)$$

以上より，$g, c, d, (1277, 399+20i) = 89+66i\ , \qquad 12277 = 89^2 + 66^2$

(a)　$19^6 + 1 = 2 \cdot 13^2 \cdot 181 \cdot 769$ である．素数 769 を Euclid の互除法を用いて，2 つの平方の和で表わせ．

(b)　素数 3877 は 15^6+1 を割り切る．3877 を 2 つの平方の和で表わせ．

(c)　素数 38737 は $2^{36}+1$ を割り切る．38737 を 2 つの平方の和で表わせ．

2.3 Congruences(合同式)

定義

$a \equiv b \mod m \overset{\text{def}}{\iff} m|(a-b)$ $(i.e.\ (a-b)$ が m の倍数$)$

このとき，a は m を法として b と合同である という．

基本的性質

1. (i) $a \equiv a \mod m$

   (ii) $a \equiv b \mod m \iff b \equiv a \mod m$

   (iii) $a \equiv b \mod m$ かつ $b \equiv c \mod m \Longrightarrow a \equiv c \mod m$

   (i)〜(iii) をみたす関係 $\equiv$ を 同値関係 という．

2. 集合に同値関係があるとき，同じ関係をもつものを集めたものを 同値類 という．
   いまの場合，m で割った余りが同じであるものを集めたものであるので，これを
   m を法とする剰余類 といい，$\boldsymbol{Z}/m\boldsymbol{Z}$ で表わす．$\boldsymbol{Z}/m\boldsymbol{Z}$ は

   0 と合同な同値類

   1 と合同な同値類

   2 と合同な同値類

   .....

   $(m-1)$ と合同な同値類

   の m 個の同値類が出来る．

3. $a \equiv b \mod m$ かつ $c \equiv d \mod m$

   $\Longrightarrow$ $(a \pm c) \equiv (b \pm d) \mod m$ かつ $ac \equiv bd \mod m$

   これは，$\boldsymbol{Z}/m\boldsymbol{Z}$ において，足し算・引き算・掛け算が出来る事を示している．
   $\boldsymbol{Z}/m\boldsymbol{Z}$ は次のような性質をみたすと言う意味で 可換環 (commuttive ring) であるという．

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

   (1-2) $(a+b)+c=a+(b+c)$

   (1-3) $\exists 0 \ \ s.t.\ \ a+0=0+a=a$

   (1-4) $\forall a,\ \exists(-a) \ \ s.t.\ \ a+(-a)=(-a)+a=0$

   (2-1) $a \cdot b = b \cdot a$

   (2-2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(2-3)　$(a+b)\cdot c = a\cdot c + b\cdot c$　,　$a\cdot(b+c) = a\cdot b + a\cdot c$

さらに，次の関係もみたすとき，可換体 (commutative field) であるという．

(3-1)　$\exists 1 \;\; s.t. \;\; a\cdot 1 = 1\cdot a = a$

(3-2)　$\forall a \neq 0, \;\; \exists a^{-1} \;\; s.t. \;\; a\cdot a^{-1} = a^{-1}\cdot a = 1$

4. $d|m$ (d が m の約数) であるとき，$a \equiv b \mod m \Longrightarrow a \equiv b \mod d$

5. m と n が互いに素であるとき ($g.c.d.(m,n) = 1$)

$a \equiv b \mod m$, $a \equiv b \mod n \Longrightarrow a \equiv b \mod m\cdot n$

Proposition II.3.1　$\boldsymbol{Z}/m\boldsymbol{Z}$ において，

a が掛け算の逆元 $b = a^{-1}$ ($i.e. \;\; a\cdot b \equiv a\cdot a^{-1} \equiv 1 \mod m$) をもつ

$\Longleftrightarrow \;\; g.c.d.(a,m) = 1$

proof　$\Longrightarrow$ の証明

背理法　$g.c.d.(a,m) = d > 1$ とする．

$ab-1$ は m の倍数 $\Longrightarrow$ $ab-1$ は d の倍数 $\Longrightarrow$ 1 は d の倍数 (矛盾)

$\Longleftarrow$ の証明

$g.c.d.(a,m) = 1$ とすると，$ua + vm = 1$ となる u, v がある ($u, v \in \boldsymbol{Z}$)．

$b = u$ とおくと，$ab - 1 = -vm$ より，$ab \equiv 1 \mod m$ である．

Remark　$g.c.d.(a,m) = 1$, $ab \equiv 1 \mod m$ とするとき，a^{-n} で b^n の剰余類を表わす．

Example II.3.1　841 を法とする 160 の逆元 160^{-1} を見つけよ．

問題 2-6(c) より，

$$841 = 160\cdot 5 + 41$$
$$160 = 41\cdot 3 + 37$$
$$41 = 37\cdot 1 + 4$$
$$37 = 4\cdot 9 + 1$$
$$4 = 1\cdot 4 + 0$$

より，

$$1 = 37 - 4\cdot 9 = 37 - (41 - 37\cdot 1)\cdot 9$$

$$= 37 \cdot 10 - 41 \cdot 9 = (160 - 41 \cdot 3) \cdot 10 - 41 \cdot 9$$
$$= 160 \cdot 10 - 41 \cdot 39 = 160 \cdot 10 - (841 - 160 \cdot 5) \cdot 39$$
$$= 160 \cdot 205 - 841 \cdot 39$$

以上より，$160 \cdot 205 \equiv 1 \mod 841$ すなわち，$160^{-1} \equiv 205 \mod 841$

Corollary 1 of Proposition II.3.1 p を素数とする．$\boldsymbol{Z}/p\boldsymbol{Z}$ の 0 でない剰余類 a は乗法的逆元をもつ．よって，$\boldsymbol{Z}/p\boldsymbol{Z}$ は可換体 (commutative field) になる．これを $\boldsymbol{F}_p$ とあらわし，標数 p の体という．

Corollary 2 of Proposition II.3.1 $0 \leqq a, b < m$ のとき，一次合同方程式

$$ax \equiv b \mod m$$

について考える．

(1) $g.c.d.(a, m) = 1$ のとき，ある解 x_0 が存在し，すべての解 x は $x = x_0 + mn$ の形である．

(2) $g.c.d.(a, m) = d > 1$ のとき，$d|b$ であるときのみ解をもち，

$$a = a'd \ , \ b = b'd \ , \ m = m'd$$

とすると，$g.c.d.(a', m') = 1$ となり，

$$ax \equiv b \mod m \iff a'x \equiv b' \mod m'$$

Corollary 3 of Proposition II.3.1

$a \equiv b \mod m$, $c \equiv d \mod m$, $g.c.d.(c, m) = 1 (\Rightarrow g.c.d.(d, m) = 1)$ とすると，

$$ac^{-1} \equiv bd^{-1} \mod m$$

が成り立つ．

proof

$cd(ac^{-1} - bd^{-1}) \equiv ad - bc \equiv 0 \mod m$ である．$cd(ac^{-1} - bd^{-1})$ が m の倍数となり，$g.c.d.(cd, m) = 1$ より，$(ac^{-1} - bd^{-1})$ が m の倍数で，$ac^{-1} \equiv bd^{-1} \mod m$ が成り立つ．

Proposition II.3.2(Fermat の小定理)　p を素数とし，a を任意の整数とするとき，

$$a^p \equiv a \mod p$$

が成り立つ，さらに，a が p の倍数でなければ，

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

が成り立つ，

proof

$p \not| a$(a が p の倍数でない) とする．

$$0 \cdot a \ , \ 1 \cdot a \ , \ 2 \cdot a \ , \ (p-1) \cdot a$$

はすべて異なる剰余類に属する．[なぜなら，$i \cdot a \equiv j \cdot a \mod p \ \ (0 \leqq i, j \leqq p-1)$ とすると，$(i-j) \cdot a$ は p の倍数となり，a は p と互いに素であることから，$(i-j)$ が p の倍数となり，$0 \leqq i, j \leqq p-1$ より，$i = j$ でなければならない.]

$\{1 \cdot a, \ 2 \cdot a, \ 3 \cdot a, \ (p-1) \cdot a\}$ を並べ替えると，p を法として，$\{1, \ 2, \ 3, \ (p-1)\}$ と等しい．このことから，

$$(1 \cdot a) \cdot (2 \cdot a) \cdot (3 \cdot a) \cdots ((p-1) \cdot a) \equiv (p-1)! \mod p$$

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \mod p$$

$(p-1)!$ は p と互いに素であるので，

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

となる．この両辺に a をかければ，$a^p \equiv a \mod p$ が得られ，これは a が p の倍数のときも成り立つ．

Corollary of Proposition II.3.2　p を素数とし，a を p の倍数でない ($p \not| a$) とする．また，

$$n \equiv m \mod p-1$$

とすると，

$$a^n \equiv a^m \mod p$$

が成り立つ．

proof　$n \equiv m \mod p-1$ であることより，$n = m + c(p-1)$ と書ける．

$$a^n = a^m \cdot (a^{p-1})^c \equiv a^m \mod p \quad (\because a^{p-1} \equiv 1 \mod p)$$

Example II.3.2 $2^{1000000}$ を 7 進法で表示するとき，第 1 位の数字は何か？($2^{1000000}$ を 7 で割った余りを求めよ)

$p = 7$ とすると，$1000000 \div (7-1) = 166666 \cdots 4$ *i.e.* $1000000 = 6 \times 166666 + 4$

$1000000 \equiv 4 \mod (7-1)$ より，$2^{1000000} \equiv 2^4 \equiv 2 \mod 7$

Proposition II.3.3(中国式剰余定理=Chinese Remainder Theorem)

連立合同方程式

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \quad \cdots\cdots \\ x \equiv a_r \mod m_r \end{cases}$$

を考える

$i \neq j$ のとき $g.c.d.(m_i, m_j) = 1$(どの異なる m_i と m_j も互いに素) をみたせば，$M = m_1 m_2 \cdots m_r$ を法として一意的に解は存在する．

proof

M を法として解は一意的であることの証明

x' と x'' を 2 つの解とする．

すべての i について，

$$x = x' - x'' \equiv 0 \mod m_i$$

どの m_i も互いに素であるので，基本的性質 5 より，

$$x = x' - x'' \equiv 0 \mod M = m_1 m_2 \cdots m_r$$

解の存在証明

$M_i = M/m_i$ とおく．$g.c.d.(M_i, m_i) = 1$ より，$\exists N_i \ \ s.t. \ \ N_i M_i \equiv 1 \mod m_i$

$$x = \sum_{j=1}^{r} a_j M_j N_j$$

$i \neq j$ のとき，M_i は m_i の倍数になっており，$M_i N_i \equiv 1 \mod m_i$ より，

$$x \equiv a_i M_i N_i \equiv a_i \mod m_i$$

Corollary of Proposition II.3.3

m と n が互いに素 $(g.c.d.(m,n) = 1) \Longrightarrow \ \varphi(mn) = \varphi(m)\varphi(n)$

proof

0〜$(mn-1)$ に mn と互いに素な数が何個あるか？　$\varphi(mn)$

$0 \leqq \forall j \leqq (mn-1)$　　j_1：j を m で割ったときの余り

j_2：j を n で割ったときの余り

Proposition II.3.3 より，j と (j_1, j_2) は 1 対 1 に対応する．

$(\because \quad \exists 1 j \ \ s.t. \ \ j \equiv j_1 \mod m \quad$ かつ $\quad j \equiv j_2 \mod n)$

また，

j と mn と互いに素　$\Longleftrightarrow$　j_1 が m と互いに素　かつ　j_2 が n と互いに素

以上より，

$$\begin{aligned}\varphi(mn) &= (mn \text{ と互いに素な } j \text{ の個数}) \\ &= (m \text{ と互いに素な } j_1\text{の個数}) \times (n \text{ と互いに素な } j_2\text{の個数}) \\ &= \varphi(m)\varphi(n)\end{aligned}$$

この Corollary を用いると，素因数分解された $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ とすると，

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \\ &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r}) \\ &= p_1^{\alpha_1}(1 - \frac{1}{p_1}) p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdots p_r^{\alpha_r}(1 - \frac{1}{p_r}) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r})\end{aligned}$$

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r}) = n \times \prod_{\substack{p|n \\ p:\text{素数}}} (1 - \frac{1}{p})$$

<u>例</u>　$\varphi(12) = 12 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 4$　，　$\varphi(100) = 100 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 40$

Proposition II.3.4(省略)

Proposition II.3.5(Euler)　a が m と素 $(g.c.d.(a, m) = 1)$ であるとき，

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

が成り立つ．

proof

(i) $m = p^{\alpha}(p$: 素数) のとき，α に関する帰納法で証明する.

$\alpha = 1$ のとき，$a^{\varphi(m)} = a^{\varphi(p)} = a^{p-1} \equiv 1 \mod p = m$

$\alpha = k$ のとき，成り立つと仮定すると　$a^{\varphi(p^k)} = a^{p^k - p^{k-1}} \equiv 1 \mod p^k$

$\alpha = k+1$ のときは　$a^{\varphi(p^{k+1})} = a^{p^{k+1}-p^k} = a^{p(p^k - p^{k-1})} = \left(a^{p^k - p^{k-1}}\right)^p$

帰納法の仮定より，$a^{p^k - p^{k-1}} = 1 + b \cdot p^k$ と書け,

$a^{\varphi(p^{k+1})} = (1 + b \cdot p^k)^p = {}_pC_0 + {}_pC_1 b \cdot p^k + {}_pC_2 (b \cdot p^k)^2 + \cdots {}_pC_p (b \cdot p^k)^p$

この右辺の第 1 項目を除けばすべての項は p^{k+1} で割り切れるので,

$a^{\varphi(p^{k+1})} \equiv {}_pC_0 = 1 \mod p^{k+1}$

(ii) $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ のとき，任意の i について,

$a^{\varphi(m)} = a^{\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r})} \equiv 1 \mod p_i^{\alpha_i}$　$(\because\ a^{\varphi(p_i^{\alpha_i})} \equiv 1 \mod p_i^{\alpha_i})$

合同式の基本的性質 5 より,

$a^{\varphi(m)} \equiv 1 \mod m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

が成り立つ.

Corollary of Proposition II.3.5

a と m が互いに素 $(g.c.d.(a, m) = 1)$ とし，n を$\varphi(m)$ で割った余りを n' とするとき,

$$a^n \equiv a^{n'} \mod m$$

が成り立つ.

proof　$n = n' + c \cdot \varphi(m)$ と書けるので,

$$a^n = a^{n'} \cdot \left(a^{\varphi(m)}\right)^c \equiv a^{n'} \mod m \quad (\because\ a^{\varphi(m)} \equiv 1 \mod m)$$

Remark

a と m が互いに素であるとき，$a^{\varphi(m)} \equiv 1 \mod m$ であるが，$a^x \equiv 1 \mod m$ となるもっと小さな x を見つけたい.

Proposition II.3.5(Euler) の証明から，$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ のとき，x として,

$\varphi(p_1^{\alpha_1})$, $\varphi(p_2^{\alpha_2})$, $\cdots$, $\varphi(p_r^{\alpha_r})$ の最小公倍数をとれば，$a^x \equiv 1 \mod m$ となる.

例　$m = 105 = 3 \cdot 5 \cdot 7$, a を m と互いに素であるとすれば，$\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(7) = 6$ の最小公倍数 12 をとれば，$a^{12} \equiv 1 \mod 105$　$(\varphi(105) = 2 \cdot 4 \cdot 6 = 48)$

Example II.3.3　$2^{1000000} \equiv ?\mod 77$

解法 1

$77 = 7 \cdot 11$ ， ，$\varphi(7) = 6$, $\varphi(11) = 10$ ， 6 と 10 の最小公倍数は 30

$2^{30} \equiv 1 \mod 77$ ， $1000000 = 30 \cdot 33333 + 10$

$2^{1000000} = (2^{30})^{33333} \cdot 2^{10} \equiv 2^{10} = 1024 = 77 \cdot 13 + 23 \equiv 23 \mod 77$

解法 2

$2^{1000000} \equiv ? \mod 7$

$1000000 = (7-1) \cdot 166666 + 4$ より，$2^{1000000} \equiv 2^4 = 16 \equiv 2 \mod 7$

$2^{1000000} \equiv ? \mod 11$

$1000000 = (11-1) \cdot 100000 + 0$ より，$2^{1000000} \equiv 2^0 \equiv 1 \mod 11$

$x = 2^{1000000} \equiv 2 \mod 7$, $x \equiv 1 \mod 11$, 中国式剰余定理の証明と，

$11^{-1} \equiv 2 \mod 7$ ， $7^{-1} \equiv 8 \mod 11$ より，

$x = 2^{1000000} \equiv 2 \cdot 2 \cdot 11 + 1 \cdot 8 \cdot 7 = 100 \equiv 23 \mod 77$

繰り返し自乗法

m , n が大きいとき，$b^n \equiv ? \mod m$

n を 2 進法で表わす．$n = n_0 + n_1 \cdot 2 + n_2 \cdot 2^2 + n_3 \cdot 2^3 + \cdots + n_{k-1} \cdot 2^{k-1}$

$b_1 \overset{\text{set}}{\equiv} b^2 \mod m$ ， $b_j \overset{\text{set}}{\equiv} (b_{j-1})^2 \mod m \ (j \geqq 2)$

$$\begin{aligned} b^n &= b^{n_0 + n_1 \cdot 2 + n_2 \cdot 2^2 + n_3 \cdot 2^3 + \cdots + n_{k-1} \cdot 2^{k-1}} \\ &\equiv b^{n_0} \cdot (b^2)^{n_1} \cdot ((b^2)^2)^{n_2} \cdots (((b^2)^2)^{\cdots})^{n_{k-1}} \\ &\equiv b^{n_0} \cdot (b_1)^{n_1} \cdot (b_2)^{n_2} \cdots (b_{k-1})^{n_{k-1}} \mod m \end{aligned}$$

(0)　$n_0 = 0$ のとき，$a \overset{\text{set}}{\equiv} 1 \mod m$ ， $n_0 = 1$ のとき，$a \overset{\text{set}}{\equiv} b \mod m$

(1)　$n_1 = 0$ のとき，$a \overset{\text{set}}{\equiv} a \mod m$ ， $n_1 = 1$ のとき，$a \overset{\text{set}}{\equiv} a \cdot b_1 \mod m$

(2)　$n_2 = 0$ のとき，$a \overset{\text{set}}{\equiv} a \mod m$ ， $n_2 = 1$ のとき，$a \overset{\text{set}}{\equiv} a \cdot b_2 \mod m$

. . . . . .

(k-1)　$n_{k-1} = 0$ のとき，$a \overset{\text{set}}{\equiv} a \mod m$ ， $n_{k-1} = 1$ のとき，$a \overset{\text{set}}{\equiv} a \cdot b_{k-1} \mod m$

こうして得られた a について，

$$b^n \equiv a \mod m$$

Proposition II.3.6(省略)

Proposition II.3.7 $\displaystyle\sum_{d|n}\varphi(d)=n$

proof $\displaystyle\sum_{d|n}\varphi(d)=f(n)$ とおく.

m と n が互いに素であるとき，$f(m\cdot n)=f(m)\cdot f(n)$ が成り立つ.

なぜなら，$d|(m\cdot n) \overset{1\text{to}1}{\longleftrightarrow} d_1\cdot d_2=d\ ,\ d_1|m\ ,\ d_2|n$

$$\varphi(d)=\varphi(d_1\cdot d_2)=\varphi(d_1)\cdot\varphi(d_2)$$

$$\begin{aligned}f(m\cdot n)&=\sum_{d|(m\cdot n)}\varphi(d)\\&=\sum_{d_1\cdot d_2|(m\cdot n)}\varphi(d_1)\cdot\varphi(d_2)\\&=\sum_{\substack{d_1|m\\d_2|n}}\varphi(d_1)\cdot\varphi(d_2)\\&=\left(\sum_{d_1|m}\varphi(d_1)\right)\cdot\left(\sum_{d_2|n}\varphi(d_2)\right)\\&=f(m)\cdot f(n)\end{aligned}$$

p が素数のとき，$f(p^\alpha)=p^\alpha$

$$\begin{aligned}\because\quad f(p^\alpha)&=\varphi(1)+\varphi(p)+\varphi(p^2)+\cdots+\varphi(p^\alpha)\\&=1+(p-1)+(p^2-p)+\cdot+(p^\alpha-p^{\alpha-1})\\&=p^\alpha\end{aligned}$$

$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_r^{\alpha_r}$(素因数分解) のとき,

$$f(n)=f(p_1^{\alpha_1})\cdot f(p_2^{\alpha_2})\cdots f(p_r^{\alpha_r})=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_r^{\alpha_r}=n$$

問題 3-1 次の解を求めよ.

(a) $3x\equiv 4 \mod 7$
(b) $3x\equiv 4 \mod 12$
(c) $9x\equiv 12 \mod 21$
(d) $27x\equiv 25 \mod 256$
(e) $27x\equiv 72 \mod 900$
(f) $103x\equiv 612 \mod 676$

問題 3-2 完全平方数を 16 進法で表わすとき，第 1 位の数字は何になるか？ 可能な数字をすべてあげよ.

問題 3-3　連続する 2 つの正の奇数の積を 12 進法で表わすとき，第 1 位の数字は何になるか？　可能な数字をすべてあげよ．

問題 3-4　n を 10 進法で表わすとき，次のことを証明せよ．

$$3|n \iff 3|(\text{各桁の数字の和})$$
$$9|n \iff 9|(\text{各桁の数字の和})$$

問題 3-5　$30|(n^5 - n)$ であることを証明せよ．

問題 3-6　8ft×9ft の場所をタイル張りにするのに 72 枚のタイルを買った．価格は\$100 以下であったが忘れてしまった．レシートは \$?0.6? となっているが．?のところはわからない．価格はいくらであったか？

問題 3-7　p を 2 より大きな素数とし，$m = p^\alpha$ あるいは $m = 2 \cdot p^\alpha$ とするとき，次のことを証明せよ．

$$x^2 \equiv 1 \mod m \implies x \equiv 1 \mod m \quad \text{あるいは} \quad x \equiv -1 \mod m$$

問題 3-8　次の Wilson の定理を証明せよ．

$$p \text{が素数} \implies (p-1)! \equiv -1 \mod p$$

また，次のことを証明せよ．

$$n \text{が素数でない} \implies (n-1)! \not\equiv -1 \mod n$$

問題 3-9　次の合同方程式の解で 1000 より小さい非負整数を求めよ．

$$\begin{cases} x \equiv 4 \mod 7 \\ x \equiv 4 \mod 9 \\ x \equiv 4 \mod 11 \end{cases}$$

問題 3-10　次の合同方程式の解で最小の非負整数解を求めよ．

$$\begin{cases} x \equiv 1 \mod 11 \\ x \equiv 2 \mod 12 \\ x \equiv 3 \mod 13 \end{cases}$$

問題 3-11　次の合同方程式の解で最小の非負整数解を求めよ.

(a) $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 4 \mod 11 \\ x \equiv 5 \mod 16 \end{cases}$　(b) $\begin{cases} x \equiv 12 \mod 31 \\ x \equiv 87 \mod 127 \\ x \equiv 91 \mod 255 \end{cases}$　(c) $\begin{cases} 19x \equiv 103 \mod 900 \\ 10x \equiv 511 \mod 841 \end{cases}$

問題 3-12　9 や 10 で割ると 7 余り，11 で割ると 3 あまる 3 桁の数を x とし，9 で割ると 8 余り，10 で割ると 7 余り，11 で割ると 1 余る 6 桁の数を y とするとき，y は x で割り切れる．このときの商を求めよ.

問題 3-13　(省略)

問題 3-14　$38^{75} \equiv ? \mod 103$　(繰り返し自乗法を用いよ)

問題 3-15〜問題 3-16　(省略)

問題 3-17　$\varphi(90)$, $\varphi(91)$, $\varphi(92)$, $\cdots$, $\varphi(100)$ を求めよ.

問題 3-18　$\varphi(n) \leqq 12$ となる n をすべて求めよ.
また，それらがすべてであることを示せ.

問題 3-19　n を完全平方数でないとき，次のことを証明せよ.

$$n-1 > \varphi(n) > n - n^{\frac{2}{3}} \implies n \text{ は 2 つの異なる素数の積である.}$$

問題 3-20　次のことを証明せよ.

$$m \geqq 8 \ , \ m = 2^{\alpha} \ , \ g.c.d.(a,m) = 1 \implies a^{\frac{\varphi(m)}{2}} \equiv 1 \mod m$$

問題 3-21　$m = 7785562197230017200 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 181$ とするとき，次の問に答えよ.

(a)　$x \equiv 6647^{362} \mod m$ を満たす最小の非負整数 x を求めよ.

(b)　a を m より小さい m と互いに素な正の整数とするとき,

$$a^x \equiv a^{-1} \mod m$$

となる 500 より小さな非負整数 x を見つけるアルゴリズムは？

問題 3-22　次のように Proposition II.3.7 の別証明を与えよ．n の各約数 d について，$\boldsymbol{Z}/n\boldsymbol{Z}$ の部分集合 S_d を次のように定める．

$$S_d = \left\{ j \cdot \frac{n}{d} \mid j = 0, 1, \cdots, d-1 \right\}$$

(a)　S_d は $\varphi(d)$ 個の S_d を生成する元 (要素)x を持つことを示せ．ただし，x が S_d を生成するとは，S_d のすべての元が n を法として x の倍数で表わされることをいう．

例　$n = 12$ のとき，$S_1 = \{\underline{0}\}$, $S_2 = \{0, \underline{6}\}$, $S_3 = \{0, \underline{4}, \underline{8}\}$, S_4 $\{0, \underline{3}, 6, \underline{9}\}$

$$S_6 = \{0, \underline{2}, 4, 6, 8, \underline{10}\} \ , \ S_{12} = \{0, \underline{1}, 2, 3, 4, \underline{5}, 6, \underline{7}, 8, 9, 10, \underline{11}\}$$

アンダーラインをつけた元が S_d を生成している元

(b)　$\boldsymbol{Z}/n\boldsymbol{Z}$ の各元 x は丁度 1 つだけの S_d を生成していることを示せ．

(上記の例において，0 は S_1を, 1 は S_{12}を, 2 は S_6を, 3 は S_4を, 4 は S_3を, $\cdots$, 11 は S_{12} を生成している)

(a) と (b) より Proposition II.3.7 が証明できる．

問題 3-23

(a)　算術の基本定理 (素因数分解の定理) を用いて，

$$\prod_{p:\text{素数}} \frac{1}{1 - \frac{1}{p}}$$

が無限大に発散することを示せ．

(b)　(a) を用いて，

$$\sum_{p:\text{素数}} \frac{1}{p}$$

が無限大に発散することを示せ．

(c)　$\lim_{j\to\infty} \dfrac{\varphi(n_j)}{n_j} = 1$ となる数列 $\{n_j\}$ で $n_j \to \infty$ となるものを見つけよ．

また，$\lim_{j\to\infty} \dfrac{\varphi(n_j)}{n_j} = 0$ となる数列 $\{n_j\}$ で $n_j \to \infty$ となるものを見つけよ．

問題 3-24　N は極めて大きな秘密の整数で，これを知っているとミサイル発射装置のカギを解除できる．いま，あなたには一人の指揮官と n 人の中尉がいる．N を知っている指揮官がダメになったとき，中尉たちに N についての部分的情報を与えて，どの 3 人の中尉たちでも賛成すればミサイルを発射できるようにしたい．(ただし，2 人の賛成では

決してミサイル発射をできないとする)
(a) $p_1, p_2, \cdots, p_n$ を異なる素数とし，そのどれも，$\sqrt[3]{N}$ より大きく，$\sqrt{N}$ より小さいとする．$\{p_i\}$ を用いて，中尉たちに与えるべき N についての部分的情報を述べよ．また，それによって，どのようにして N を求めたらよいか？
(b) (a) の場合を拡張して，どの k 人の中尉たちが賛成してもミサイルを発射できるようにするにはどうしたらよいか？ ただし，$k-1$ 人賛成では決してミサイル発射をできないとする．

2.4 因数分解の応用

Proposition II.4.1 任意の整数 b と任意の自然数 n に対して，$b^n - 1$ は $b-1$ で割り切れ，その商は $b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1$ である．

proof 多項式の恒等式として証明すればよい．
第 2 の証明 ($b-$ 進法を用いる証明)
$b^n - 1$ を $b-$ 進法で表わせば n 個の数字 $(b-1)$ が並んで表わされる．他方，$b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1$ は $b-$ 進法では $(111\cdots111)_b$ と書け，これに $(b-1)$ をかければ，$((b-1)(b-1)(b-1)\cdots(b-1)(b-1)(b-1))_b = b^n - 1$ となる．

Corollary of Proposition II.4.1 任意の整数 b と任意の自然数 m と n に対して，

$$b^{mn} - 1 = (b^m - 1)(b^{m(n-1)} + b^{m(n-2)} + \cdots + b^{2m} + b^m + 1)$$

である．

proof Proposition II.4.1 において，b を b^m に置き換えればよい．

例 $2^{35} - 1$ は $2^5 - 1 = 31$ や $2^7 - 1 = 127$ で割り切れる．

Proposition II.4.2 b を m と素な整数とし，a と c を自然数とする．

$b^a \equiv 1 \mod m$, $b^c \equiv 1 \mod m$, $d = g.c.d(a,c) \implies b^d \equiv 1 \mod m$

proof Euclid の互除法をを用いて，$d = ua + vc$ と表わすことができる．u と v の一方は正の整数であり，他方は 0 か負の整数である．いま，$u > 0$, $v \leqq 0$ として一般性を失わない．$b^a \equiv 1 \mod m$ の両辺を u 乗し，$b^c \equiv 1 \mod m$ の両辺を $(-v)$ 乗して，前者を後者で割れば，$b^d = b^{ua+vc} \equiv 1 \mod m$ が得られる．

Proposition II.4.3 p を $b^n - 1$ を割り切る素数とすれば，次のどちらかが成り立つ．

(i) n のある真の約数 d に対して，$p | b^d - 1$

(ii) $p \equiv 1 \mod n$．もし $p > 2$ で n が奇数であれば，$p \equiv 1 \mod 2n$

proof $b^n \equiv 1 \mod p$であり，Fermat の小定理より $b^{p-1} \equiv 1 \mod p$である．Proposition II.4.2 より，$d = g.c.d.(n, p-1)$ とおけば，$b^d \equiv 1 \mod p$

もし，$d < n$ のとき，n の真の約数 d に対して，$p | b^d - 1$ すなわち (i) が成り立つ．

$d = n$ のときは，d は $p-1$ の約数なので，$d | (p-1)$，$p \equiv 1 \mod d = n$.

さらに，p と n が両方とも奇数のときは，$n | (p-1)$ より，明らかに $2n | (p-1)$ となり，$p \equiv 1 \mod 2n$

この Proposition はあるタイプの大きな整数の因数分解に用いられる．

Example

1. $2^{11} - 1 = 2047$ を因数分解しよう．$p | (2^{11} - 1)$ とすれば，Proposition II.4.3 より，$p \equiv 1 \mod 22$，$p = 23, 67, 89, \cdots$ について割り切れるかテストすればよい (実際，$\sqrt{2047} = 45.\cdots$ より小さい数だけテストすればよい)．

$2047 = 23 \cdot 89$ が得られえる．

また，$2^{13} - 1 = 8191$ が素数であることは同様に簡単にわかる．$2^n - 1$ の形の素数を **Mersenne 素数** という．

2. $3^{12} - 1 = 531440$ を因数分解しよう．Proposition II.4.3 より，より小さな因数 $3^1 - 1, 3^2 - 1, 3^3 - 1, 3^4 - 1, 3^6 - 1 = (3^3 - 1)(3^3 + 1)$ の因数 について，割り切れるか試みよう．そうすると，$2^4 \cdot 5 \cdot 7 \cdot 13$ が得られ，$531440/(2^4 \cdot 5 \cdot 7 \cdot 13) = 73$(素数)

すべての素因数が 3^d-1 (d は 12 の真の約数) の中にあらわれるとは限らない.
すなわち, $73 \equiv 1 \mod 12$ である.

3. $2^{35}-1 = 34359738367$ を因数分解しよう. まず, 2^d-1 ($d=1,5,7$) の因数について考えよう. 素因数 $31, 127$ が得られる. $(2^{35}-1)/(31\cdot 127) = 8727391$.
Proposition II.4.3 より, 残りの素因数は $\equiv 1 \mod 70$ であるので, $71, 211, 281, \cdots$ について, チェックする. $\sqrt{8727391} = 2954.\cdots$ までのすべてについてチェックする必要があると心配されるが, 直ちに $8727391 = 71\cdot 122921$ が得られ,
$\sqrt{122921} = 350.\cdots$ までのすべてについてチェックするだけでよい. 122921 は素数であることがわかり, $2^{35}-1 = 34359738367 = 31\cdot 71\cdot 127\cdot 122921$ と素因数分解される. $(122921 = 70\cdot 1756+1)$

Remark 8 桁電卓を用いて Example 3 を計算する方法
2^{35} を計算するのに, $2^{26} = 67108864$(8 桁) と $2^9 = 512$ を掛け算するには,
$2^{35} = 512\cdot(67108\cdot 1000 + 864) = 34359296\cdot 1000 + 442368 = 34359738368$
次に, $2^{35}-1$ を $31\cdot 127 = 3937$ で割るには, まず, 34359738 を 3937 で割り, その商の整数部分 $\left[\dfrac{34359738}{3937}\right] = 8727$ をとる. 次に, $34359738 = 3937\cdot 8727 + 1539$
その後,

$$\begin{aligned}\frac{34359738367}{3937} &= \frac{(3937\cdot 8727+1539)\cdot 1000+367}{3937}\\ &= 8727000 + \frac{1539367}{3937}\\ &= 8727391\end{aligned}$$

を得る.

問題 4-1 n を奇数とするとき,

$$b^n+1 = (b+1)(b^{n-1}-b^{n-2}+\cdots+b^2-b+1)$$

となることを 2 つの方法で示せ. 1 つは多項式の恒等式を用いる方法. もう一つは $b-$ 進法を用いる方法

問題 4-2 2^n-1 が素数であれば, n も素数であることを示せ.
また, 2^n+1 が素数であれば, n は 2 の巾乗であることを示せ.
2^n-1 のタイプの素数を **Mersenne 素数** といい, 最初のほうは $3, 7, 31, 127, \cdots$

2^n+1 のタイプの素数を **Fermat 素数** といい，最初のほうは $3, 5, 17, 257, \cdots$

問題 4-3　$m>2$ とし，b を m と素な数，a と c を自然数とする．次のことを証明せよ．

$b^a \equiv -1 \mod m$, $b^c \equiv \pm 1 \mod m$, $d = g.c.d(a,c)$

$\Longrightarrow$

$b^d \equiv -1 \mod m$　かつ　a/d は奇数

問題 4-4　次のことを証明せよ．

p を b^n+1 を割り切る素数とすれば，次のどちらかが成り立つ．

(i)　n の n/d が奇数であるようなある真の約数 d に対して，$p|b^d+1$

(ii)　$p \equiv 1 \mod 2n$

問題 4-5　$m = 2^{24}+1 = 16777217$ とするとき，次の問に答えよ．

(a)　m を割り切る Fermat 素数を見つけよ．

(b)　他の素因数は $\equiv 1 \mod 48$ であることを示せ．

(c)　m を素因数分解せよ．

問題 4-6　$3^{15}-1$ と $3^{24}-1$ を素因数分解せよ．

問題 4-7　$5^{12}-1$ を素因数分解せよ．

問題 4-8　10^5-1，10^6-1 と 10^8-1 を素因数分解せよ．

問題 4-9　$2^{33}-1$ と $2^{21}-1$ を素因数分解せよ．

問題 4-10　$2^{15}-1$，$2^{30}-1$ と $2^{60}-1$ を素因数分解せよ．

問題 4-11　(a)　a を 1 より大きな整数とし，$d = g.c.d.(m,n)$ とすれば，

$g.c.d.(a^m-1, a^n-1) = a^d-1$ であることを示せ．

(b)　(省略)

2.5 公開鍵暗号と RSA 暗号

ここで，暗号にしたい元の文を **平文 (plain text)** といい，**暗号化**(**encryption** または **enciphering**) された文を **暗号文 (cipher text)** と呼ぶ．暗号文を元の文に戻すことを復号あるいは **復号化**(**decryption** または **deciphering**) という．平文を何文字かに区切って暗号文に変換する．区切る文字数 k は予め決めておく．その k 個の文字からなる文字列を暗号化されたものは l 個の文字からなる文字列に変換されるとする．

$\mathcal{P}$：k 個の文字からなる文字列の集合

$\mathcal{C}$：l 個の文字からなる文字列の集合

このとき，暗号化 f と復号化 f^{-1} は次のような図式となる．

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

かっての暗号システムは暗号化 f が分かれば，復号化 f^{-1} が用意に分かる暗号であり，そのために f や f^{-1} を秘密にする必要があった．f が分かっても，f^{-1} が分かりにくい暗号である **公開鍵暗号システム (public key cryptosystem)** の考え方が約 30 年前に発見された．

その公開鍵暗号システムに最も古くから用いられ最もポピュラーなものが **RSA 暗号システム (RSA cryptosystem)** である．RSA は 3 人の発見者 Rivest, Shamir, Adleman の頭文字からその名が付いている．

公開鍵暗号システム

公開鍵 (暗号の送り手が知っている．他人に知られても良い)　：f

秘密鍵 (暗号の受け手だけが知っている．他人に知られてはいけない)：f^{-1}

RSA 暗号システム

p と q：極めて大きな 2 つの素数 (十進法で 100 桁ほど，最近はもっと大きなもの)

$n = pq$ ，$\varphi(n) = \varphi(pq) = (p-1)(q-1) = n + 1 - (p+q)$

e：$\varphi(n)$ と互に素な数

$d = e^{-1} \mod \varphi(n)$　(i.e.　$de \equiv 1 \mod \varphi(n)$)

今，$\mathcal{P}$ の元 (暗号文) は n より小さな数に数値化されているとしよう．方法は後で述べることにする．

公開鍵：(n, e)　　$(p.q, \varphi(n), d$ は他の人に知られてはいけない$)$

秘密鍵：(n, d)

極めて大きな数 n の素因数分解は計算が困難であるので，n と e の情報だけでは，$p, q, \varphi(n), d$ は見つけるのが困難である．秘密鍵 (n, d) が他の人に知れることは無いと考えられる．

暗号化と復号化

P：数値化された平文 $(0 \leqq P \leqq n-1\ )$

C：数値化された暗号文 $(0 \leqq C \leqq n-1\ )$

暗号化

$$C = f(P) \equiv P^e \mod n \quad (0 \leqq f(P) \leqq n-1)$$

復号化

$$f^{-1}(C) \equiv C^d \mod n \quad (0 \leqq f^{-1}(C) \leqq n-1)$$

復号化されていることの証明

$$P^{de} - P = P(P^{de-1} - 1) \equiv 0 \mod p$$

が成り立つ．なぜなら，P が p の倍数のときは明らか．P が p の倍数でないときは，$de-1$ が $p-1$ の倍数なので Fermat の小定理の系 (Corollary of Proposition II.3.2) より $P^{de-1}-1 \equiv 0 \mod p$ となり，成り立つ．

同様に，

$$P^{de} - P = P(P^{de-1} - 1) \equiv 0 \mod q$$

も成り立つので，合同式の基本的性質 5 より，

$$P^{de} - P = P(P^{de-1} - 1) \equiv 0 \mod n = pq$$

すなわち，$f^{-1}(C) \equiv C^d \equiv P^{de} \equiv P \mod n$

となり，復号化される．

注意

$g.c.d.(P, n) = 1$ のときは，$de \equiv 1 \mod \varphi(n)$ と Euler の定理の系 (Corollary of Proposition II.3.5) より，簡単に

$$f^{-1}(C) \equiv P^{de} \equiv P \mod n$$

が証明される．

文字列の数値化と数値の文字列化

・N：使用する文字の種類の数

(アルファベットなら 26，大文字小文字を区別するなら 52,

その他記号なども含めればもっと多くなる)

・N 種類の文字に 0〜$N-1$ の数を割り当てる．

・$N^k \leqq n \leqq N^l$ $(l = k+1$ とすればよい) とする．

・平文を前のほうから k 個ずつ区切り，k 文字からなる各文字列を N 進法表示された k 桁の数値 $(\leqq N^k - 1 \leqq n-1)$ と見る．

・f によって暗号化された数値は n より小さい数となるので，これを l 桁に N 進法し,，これを l 個の文字からなる文字列に変換する．

・復号化のときはこの逆をすればよい．

以下，いくつかの例を挙げるが，計算が複雑にならないように，p, q は大きくない素数を考える．実際の場合にはこれでは他人に解読されてしまう．

Example

1. $p = 2, q = 13$ ， $n = 2 \cdot 13 = 26$ ， $\varphi(2 \cdot 13) = (2-1)(13-1) = 12$

$e = 5$ ， $d = 5^{-1} \equiv 5 \mod 12$

$N = 26$ ， 0(A)〜25(Z) を割り当てる． $k = l = 1$

暗号化 平文=”KOBE” 数値=10,14,1,4

$f(10) = 10^5 \equiv 4, f(14) = 14^5 \equiv 14, f(1) = 1^5 \equiv 1, f(4) = 4^5 \equiv 10 \mod 26$

暗号文=”EOBK”

復号化 暗号文=”EOBK” 数値=4,14,1,10

$f^{-1}(4) = 4^5 \equiv 10, f^{-1}(14) = 14^5 \equiv 14, f^{-1}(1) = 1^5 \equiv 1, f^{-1}(10) = 10^5 \equiv 4 \mod 26$

復号文=”KOBE”

2. $p = 3, q = 11$ ， $n = 3 \cdot 11 = 33$ ， $\varphi(3 \cdot 13) = (3-1)(11-1) = 20$

$e = 7$ ， $d = 7^{-1} \equiv 3 \mod 20$

$N = 30$ ， 0(A)〜25(Z),26(␣),27(,),28(.),29(?) を割り当てる． $k = 1, l = 2$

暗号化　平文=”PRIME NUMBER”　　数値=15,17,8,12,4,26,13,20,12,1,4,17

以下，　mod 33　とする．

$f(15) = 15^7 \equiv 27(\mathrm{A,}), f(17) = 17^7 \equiv 8(\mathrm{AI}), f(8) = 8^7 \equiv 2(\mathrm{AC})$

$f(12) = 12^7 \equiv 12(\mathrm{AM}), f(4) = 4^7 \equiv 16(\mathrm{AQ}), f(26) = 26^7 \equiv 5(\mathrm{AF})$

$f(13) = 13^7 \equiv 7(\mathrm{AH}), f(20) = 20^7 \equiv 26(\mathrm{A}\text{␣}), f(12) \equiv 12(\mathrm{AM}), f(1) \equiv 1(\mathrm{AB})$

$f(4) = 4^7 \equiv 16(\mathrm{AQ}), f(17) \equiv 8(\mathrm{AI})$

暗号文=”A,AIACAMAQAFAHA␣AMABAQAI”

復号化　暗号文=”A,AIACAMAQAFAHA␣AMABAQAI”

数値=27,8,2,12,16,5,7,26,12,1,16,8

$f^{-1}(27) = 27^3 \equiv 15(\mathrm{P}), f^{-1}(8) = 8^3 \equiv 17(\mathrm{R}), f^{-1}(2) = 2^3 \equiv 8(\mathrm{I})$

$f^{-1}(12) = 12^3 \equiv 12(\mathrm{M}), f^{-1}(16) = 16^3 \equiv 4(\mathrm{E}), f^{-1}(5) = 5^3 \equiv 26(\text{␣})$

$f^{-1}(7) = 7^3 \equiv 13(\mathrm{N}), f^{-1}(26) = 26^3 \equiv 20(\mathrm{U}), f^{-1}(12) \equiv 12(\mathrm{M})$

$f^{-1}(1) \equiv 1(\mathrm{B}), f^{-1}(16) \equiv 4(\mathrm{E}), f^{-1}(8) \equiv 17(\mathrm{R})$

復号文=”PRIME␣NUMBER”

3.　$p = 23, q = 89$ ，$n = 23 \cdot 89 = 2047$ ，$\varphi(23 \cdot 89) = (23-1)(89-1) = 1936$

$e = 179$ ，$d = 179^{-1} \equiv 411 \mod 1936$

$N = 40$ ，0(A)〜25(Z),26(␣),27(.),28(?),29($),30(0)〜39(9) を割り当てる．

$k = 2, l = 3$

暗号化　平文=”SEND␣$7500”

数値=$18 \cdot 40 + 4 = 724(\mathrm{SE}), 13 \cdot 40 + 3 = 523(\mathrm{ND}), 26 \cdot 40 + 29 = 1069(\text{␣\$}),$

$37 \cdot 40 + 35 = 1515(75), 30 \cdot 40 + 30 = 1230(00)$

$f(724) = 724^{179} \equiv 1906 = 1 \cdot 40^2 + 7 \cdot 40 + 26(\mathrm{BH}\text{␣})$

$f(523) \equiv 1072 = 0 \cdot 40^2 + 26 \cdot 40 + 32(\mathrm{A}\text{␣}2)$

$f(1069) \equiv 802 = 0 \cdot 40^2 + 20 \cdot 40 + 2(\mathrm{AUC})$

$f(1515) \equiv 364 = 0 \cdot 40^2 + 9 \cdot 40 + 4(\mathrm{AJE})$

$f(1230) \equiv 710 = 0 \cdot 40^2 + 17 \cdot 40 + 30(\mathrm{AR0})$

暗号文=”BH␣A␣2AUCAJEAR0”

Remark

暗号化と復号化における d や e は $\varphi(p\cdot q)=(p-1)(q-1)$ を法として計算しているが, $\varphi(p\cdot q)$ の代わりに $p-1$ と $q-1$ の最小公倍数 $l.c.m.(p-1,q-1)$ を用いてもよい.

例えば, 上記の Example 1 は $\varphi(p\cdot q)=l.c.m.(p-1,q-1)$ である.

Example 2 では 20 の代わりに 10 を法としてもよい. $e=7$, $d=3$ のときは同じである. $e=11$, $d=11$ のときは $e=1$, $d=1$ とするのと同じ (暗号にならない). $e=13$, $d=17$ のときは $e=3$, $d=7$ とするのと同じ, $e=17$, $d=13$ のときは $e=7$, $d=3$ とするのと同じ, $e=19$, $d=19$ のときは $e=9$, $d=9$ とするのと同じである.

Example 3 では $\varphi(23\cdot 89)=1936$ の代わりに $l.c.m.(22,88)=88$ を法としてもよい. そうすると, $e=179$, $d=411$ の代わりに $e=3$, $d=59$ として計算すればよい.

問題 5-1 Example 1 において,

(a) ”HYOGO” を暗号化せよ. (答 ”LUOCO”)

(b) ローマ字表記した自分の名前を暗号化せよ.

(c) 暗号文 ”EANXI” を復号化せよ.

問題 5-2 Example 2 において,

(a) ”KYOTO FU” を暗号化せよ. (答 ”AKASAUANAUAFAOA␣”)

(b) ローマ字表記した自分の名前を暗号化せよ.

(c) 暗号文 ”AKAAAHAIAC” を復号化せよ.

問題 5-3 「十進 BASIC」や「PASCAL」などのプログラミング言語を用いて, Example 1-3 の場合に暗号化や復号化するプログラムを作れ.