数論事始め

以下は自らの理解を助けるための記述であるので証明は省略している[1].

1　合成数，素数，約数

n を整数，m を正整数とすると，

$$n = qm + r, \quad 0 \leq r < m, \tag{1}$$

を満たす整数 q, r はただ一組に限って存在する．$r = 0$ のとき，m を n の**約数**という．(1) において $q = 1$ ならば $m = n, r = 0$ で, $q = n$ ならば $m = 1, r = 0$ であるから，n および 1 もともに n の約数であるが，1 と n を除いたものを n の**真の約数**という．$n > 1$ である整数 n が真の約数を有しないとき n を**素数** (prime) といい，有する整数を**合成数** (composite number) という．一般に正整数 n はただ 1 通りの方法で素数の積に分解できる．素数 $p_1, p_2, \ldots$ によって巾の形で

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} \qquad (0 \leq \alpha_j : \ j = 1, \ldots, m) \tag{2}$$

で一意的に与えられる．これを**素因数分解**するという．関数 $T(n)$ を n の約数の個数を表す関数とするとき

$$T(n) = (1 + \alpha_1)(1 + \alpha_2) \ldots (1 + \alpha_m), \tag{3}$$

である．例えば $12 = 2^2 \times 3$ であるから 12 の約数は 2,3,4,6 に 1,12 を加え 6 個，即ち $T(12) = (1 + 2) \times (1 + 1)$ である．

2 つの整数において，共通の約数を**公約数**という．整数 a, b の公約数のうち，最大のものを**最大公約数**といい，(a, b) と表す．1 以外の公約数を持たないとき，これらの数は**互いに素である**という．この場合には $(a, b) = 1$ である．

2　オイラーの関数

自然数 $1, 2, \ldots n$ において n と互いに素なる数の個数を表す関数 $\phi(n)$ を **Euler の関数**という．例えば，5 と互いに素なる 5 以下の数は 1,2,3,4 であるから $\phi(5) = 4$，6 以下の数のうち，互いに素な数は，1,5 であるから $\phi(6) = 2$ である．p が素数のとき，

$$\phi(p) = p - 1 \qquad (p : \text{素数}). \tag{4}$$

素数のべき乗の数 p^α に対しては，1 から p^α の数のうち，p で割り切れる数は $p, 2p, 3p, \ldots p^{\alpha-1}p$ の $p^{\alpha-1}$ 個であるので

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} \qquad (p : \text{素数}). \tag{5}$$

一般に互いに素な整数 a, b に対して次式が成り立つ．

$$\phi(ab) = \phi(a)\phi(b). \tag{6}$$

[1]参考書：「初等整数論講義　高木貞治著」,「整数論　稲葉栄次著（基礎数学講座）」,「数論入門　芹沢正三」

上式を証明抜きで (2) に適応すると

$$\begin{aligned}\phi(n) &= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\dots\phi(p_m^{\alpha_m}) \\ &= (p^{\alpha_1}-p^{\alpha_1-1})(p^{\alpha_2}-p^{\alpha_2-1})\dots(p^{\alpha_m}-p^{\alpha_m-1}) \\ &= p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_m}\right),\end{aligned}$$

従って，次式を得る．

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_m}\right). \tag{7}$$

例えば，$\phi(12) = 12(1-1/2)(1-1/3) = 4$，即ち，1,5,7,11 の 4 個である．

ところで，12 を分数の分母に整数 k $(1 \le k \le 12)$ を分子としてならべると，

$$\frac{1}{12},\ \frac{2}{12},\ \frac{3}{12},\ \frac{4}{12},\ \frac{5}{12},\ \frac{6}{12},\ \frac{7}{12},\ \frac{8}{12},\ \frac{9}{12},\ \frac{10}{12},\ \frac{11}{12},\ \frac{12}{12},$$

既約分数に直すと，それぞれ，

$$\frac{1}{12},\ \frac{1}{6},\ \frac{1}{4},\ \frac{1}{3},\ \frac{5}{12},\ \frac{1}{2},\ \frac{7}{12},\ \frac{2}{3},\ \frac{3}{4},\ \frac{5}{6},\ \frac{11}{12},\ 1,$$

分母が 2,3,4,6,12 のものは，それぞれ，1 個，2 個，2 個，2 個，4 個ある．これらはそれぞれ $\phi(2)$，$\phi(3)$，$\phi(4)$，$\phi(6)$，$\phi(12)$ である．これに $\phi(1) = 1$ を加えると，1〜12 の数が重複なしに 6 種類に分類されたことになり，

$$\phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(12) = 12,$$

である．一般の数 n についても

$$\sum_{d|n}\phi(d) = n, \tag{8}$$

ただし，和は n のすべての約数 d にわたることを意味し，記号 $d|n$ で表している．

3　整数の合同

整数 a, b に対して $a-b$ が m で割り切れるとき「a と b は法 m について合同 (congruent) である」といい，次のように表される．

$$a \equiv b \pmod{m}. \tag{9}$$

整数のすべてを法 m によって m 個に類別することができる．例えば，$m = 7$ のとき，次のように 7 種類の数列に分類できる．

$$\left\{\begin{array}{lccccccccc}
0)\dots & -21 & -14 & -7 & \mathbf{0} & 7 & 14 & 21 & \dots \\
1)\dots & -20 & -13 & -6 & \mathbf{1} & 8 & 15 & 22 & \dots \\
2)\dots & -19 & -12 & -5 & \mathbf{2} & 9 & 16 & 23 & \dots \\
3)\dots & -18 & -11 & -4 & \mathbf{3} & 10 & 17 & 24 & \dots \\
4)\dots & -17 & -10 & -3 & \mathbf{4} & 11 & 18 & 25 & \dots \\
5)\dots & -16 & -9 & -2 & \mathbf{5} & 12 & 19 & 26 & \dots \\
6)\dots & -15 & -8 & -1 & \mathbf{6} & 13 & 20 & 27 & \dots
\end{array}\right.$$

上の数列において j) に属する数 k は $k \equiv j \pmod 7$ である．従って，各数列は数 **j** で代表させることができる．一般に法 m において，このような各数列の組から一つずつ選んだ m 個の数を**剰余系** (system of residues) という．同一の法内において，加法，減法，乗法が成り立つ．即ち

$a \equiv b \pmod m$, $a' \equiv b' \pmod m$ ならば

$$a + a' \equiv b + b' \pmod m, \tag{10}$$

$$a - a' \equiv b - b' \pmod m, \tag{11}$$

$$aa' \equiv bb' \pmod m, \tag{12}$$

$$a^n \equiv b^n \pmod m, \qquad (n : \text{正整数}). \tag{13}$$

例えば，(13) より $123456^6 \pmod{13}$ を求めてみよう．$123456 \equiv 8 \pmod{13}$ であるから

$$123456^6 \equiv 8^6 \equiv 512^2 \equiv 5^2 \equiv 12 \pmod{13}$$

四則計算のうち，割り算は一般に不可能であるが，**一次合同式** $ax \equiv b \pmod m$ は $(a, m) = 1$ のときは，1 つの解を有する．なぜなら，x に m を法としての剰余系 $x_1, x_2, \ldots, x_m$ の値を与えるときに，ax の値 $ax_1, ax_2, \ldots, ax_m$ も m を法とする剰余の一組である．従って b はこの数列の中の 1 つであり得る．

4　フェルマーの定理

12 以下の正整数において 12 と互いに素であるのは $\{1, 5, 7, 11\}$ の $\phi(12) = 4$ 個である．この組の各数に 12 と互いに素な数 5 を乗ずると $\{1 \times 5, 5 \times 5, 5 \times 7, 5 \times 11\} = \{5, 25, 35, 55\} \equiv \{5, 1, 11, 7\} \pmod{12}$. 従って，組 $\{\ldots\}$ の各要素をすべて乗ずると次の等式が得られる．

$$\begin{aligned} 5^4 \times 1 \times 5 \times 7 \times 11 &\equiv 1 \times 5 \times 7 \times 11 \pmod{12} \\ \therefore \quad 5^{\phi(12)} &\equiv 1 \pmod{12} \end{aligned}$$

一般に，整数 a，正整数 m において，$(a, m) = 1$ であるとき．

$$a^{\phi(m)} \equiv 1 \pmod m. \tag{14}$$

これを **Euler の定理**という．

p が素数で，a が $(a, p) = 1$ である整数であるならば，$\phi(p) = p - 1$ であるから，

$$a^{p-1} \equiv 1 \pmod p. \tag{15}$$

これが **Fermat の定理**である．例えば，$10^6 \equiv 1 \pmod 7$ であるから，999999 は 7 で割り切れる．

5　メビウス関数

正整数 n の関数 $T(n)$ や $\phi(n)$ のように関数値が整数である関数を**整数論的関数**という．いま，任意の整数論的関数を $f(n)$ とする．そして，さらに n の約数 d にについての $f(d)$ をすべての $d|n$ にわたって加えた関数を $F(n)$ と定義する．即ち，

$$F(n) = \sum_{d|n} f(d). \tag{16}$$

例えば，12 の約数は 1,2,3,4,6,12 であるから，

$$F(12) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$$

ところが，$F(1) = f(1)$，$F(2) = f(1) + f(2)$，$F(3) = f(1) + f(3)$，$F(4) = f(1) + f(2) + f(4)$，$F(6) = f(1) + f(2) + f(3) + f(6)$ である．このように，6 個の $F(1)$〜$F(12)$ が 6 個の $f(1)$〜$f(12)$ で表わされるので，次のように，逆に，6 個の $f(1)$〜$f(12)$ が 6 個の $F(1)$ から $F(12)$ で表わされる．

$$\begin{aligned}
f(1) &= F(1), \\
f(2) &= F(2) - F(1), \\
f(3) &= F(3) - F(1), \\
f(4) &= F(4) - F(2), \\
f(6) &= F(6) - F(3) - F(2) + F(1), \\
f(12) &= F(12) - F(6) - F(4) + F(2).
\end{aligned}$$

Möbius 関数 $\mu(n)$ を次のように定義すると一般の場合にも $f(n)$ を $F(n)$ で表わすことができる．

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & n:\ \text{素数の平方で割り切れる} \\ (-1)^r & n:\ \text{相異なる } r \text{ 個の素数の積である} \end{cases} \tag{17}$$

この関数によって，

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right). \tag{18}$$

(8) における関係において，$f(n) = \phi(n)$，$F(n) = n$ であるので，

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}. \tag{19}$$

(2) で表される n から $\phi(n)$ を求めると，Möbius の関数の定義から p_j の 1 乗の項のみ 0 でないから次式が得られる．

$$\phi(n) = n - \frac{n}{p_1} - \ldots - \frac{n}{p_m} + \frac{n}{p_1 p_2} + \ldots + \frac{n}{p_{m-1} p_m} - \ldots + (-1)^m \frac{n}{p_1 p_2 \cdots p_m}. \tag{20}$$

上式は (7) を展開した表現である．

6　素数の個数

一般化した Euler の関数を次のように定義する．即ち，正の実数 x を導入し，x を超えない正の整数のうちで n に素であるものの個数を $\phi(n, x)$ とする．例えば，1 から 12 までの整数のうち 6 に素なものは 1,5,7,11 の 4 個である．即ち，$\phi(6, 12) = 4$ である．(8) に相当するものとして次式が成り立つ．

$$\sum_{d|n} \phi(d, dx) = [nx]. \tag{21}$$

ただし，記号 $[X]$ は X を超えない整数である．上式より (19) と同様な式が得られる．

$$\phi(n, nx) = \sum_{d|n} \mu(d) \left[\frac{nx}{d}\right].$$

さらに，x の代わりに x/n を代入すると

$$\phi(n, x) = \sum_{d|n} \mu(d) \left[\frac{x}{d}\right]. \tag{22}$$

例えば，100 以下の数のうち素数 5 と素数 7 で割り切れないものも個数は $5 \times 7 = 35$ と互いに素であるものの個数であるから，

$$\phi(35, 100) = \mu(1)[100] + \mu(5)\left[\frac{100}{5}\right] + \mu(7)\left[\frac{100}{35}\right] = 100 - 20 - 14 + 2 = 68$$

いま，x を超えないすべての素数を $\pi(x)$ とするとこの関数も整数論的関数である．例えば，15 以下の素数は 2,3,5,7,11,13 の 6 個であるから $\pi(15) = 6$ である．一般に x 以下の素数の個数 $\pi(x)$ は $\sqrt{x}$ 以下の素数 $p_1, p_2, \ldots, p_m$ が求められていれば次式から得ることができる．

$$\pi(x) = \pi(\sqrt{x}) - 1 + \phi(p_1 p_2 \ldots p_m, x),$$

より，

$$\pi(x) = \pi(\sqrt{x}) - 1 + [x] - \left[\frac{x}{p_1}\right] - \ldots - \left[\frac{x}{p_m}\right] + \ldots + (-1)^m \left[\frac{x}{p_1 p_2 \ldots p_m}\right]. \tag{23}$$

例えば，100 までの素数は 10 以下の素数 2,3,5,7 の $\pi(10) = 4$ 個から得られる．4 個から 2 個を選び積をとると，$C_4^2 = \dfrac{4!}{2!2!} = 6$ 通りの 6,10,14,15,21,35，また，3 個の積では 30,42,70,105 が得られる．4 個の積は 100 を超える．100 をこれらで割り算をし整数部分をとり (23) を書き下すと，

$$\begin{aligned}
\pi(100) \quad = \quad & \pi(10) - 1 + [100] \\
& - \left[\frac{100}{2}\right] - \left[\frac{100}{3}\right] - \left[\frac{100}{5}\right] - \left[\frac{100}{7}\right] \\
& + \left[\frac{100}{6}\right] + \left[\frac{100}{10}\right] + \left[\frac{100}{14}\right] + \left[\frac{100}{15}\right] + \left[\frac{100}{21}\right] + \left[\frac{100}{35}\right] \\
& - \left[\frac{100}{30}\right] - \left[\frac{100}{42}\right] - \left[\frac{100}{70}\right] - \left[\frac{100}{105}\right]
\end{aligned}$$

$\therefore \pi(100) = 4 - 1 + 100 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 - 3 - 2 - 1 = 25$ を得る．10 以上 100 までの残りの素数は 11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97 である．計算は複雑になるが組み合わせのプログラムを組み[2]，コンピュータを使えば $\pi(10000)$ が求めることができる．

7　組み合わせ積の計算方法

m 個の素数 $p_1, p_2, \ldots, p_m$ のあらゆる組み合わせの積 $\Pi_{j=1}^{r} p_{\alpha_j}$ $(r = 1, 2, \ldots, m)$ を求める方法を考えよう．前節において扱った 10 以下の素数の場合には，$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ である．2^4

[2]例えば,「組合せアルゴリズム　仙波一郎著」参照

個の 4 桁の 2 進数の各桁を $b_j(j=1,2,3,4)$ $(b_j=0,1)$ で表し，積 p_jb_k $(j=1,\ldots,4),(k=1,\ldots,4)$ を並べると

$$\begin{bmatrix} 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\ 0 & 0 & 3 & 3 & 0 & 0 & 3 & 3 & 0 & 0 & 3 & 3 & 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 0 & 5 & 5 & 5 & 5 & 0 & 0 & 0 & 0 & 5 & 5 & 5 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \end{bmatrix}$$

上の数表の 0 でないものを縦に乗じると

$$\begin{bmatrix} * & 2 & 3 & 6 & 5 & 10 & 15 & 30 & 7 & 14 & 21 & 42 & 35 & 70 & 105 & 210 \end{bmatrix}$$

100 をこの表の各項で割り整数部分をとると

$$\begin{bmatrix} * & 50 & 33 & 16 & 20 & 10 & 6 & 3 & 14 & 7 & 4 & 2 & 2 & 1 & 0 & 0 \end{bmatrix} \tag{24}$$

縦に 0 でないものの個数は

$$\begin{bmatrix} * & 1 & 1 & 2 & 1 & 2 & 2 & 3 & 1 & 2 & 2 & 3 & 2 & 3 & 3 & 4 \end{bmatrix}$$

上の表より (-1) のべき乗から符号は

$$\begin{bmatrix} * & - & - & + & - & + & + & - & - & + & + & - & + & - & - & + \end{bmatrix} \tag{25}$$

(24) と (25) を各項を乗じて加えると $-50-33+16-20+10+6-3-14+7+4-2+2-1$ で $\pi(100)$ の計算の 2 列目以降と一致する．以上の手続きで $\pi(10000)$ を求める F-BASIC プログラムは以下のごとくである．短時間で $\pi(10000)=1229$ が得られる．

```
'******** Calculation of pi(10000) *****
data 25
data 2,3,5,7,11,13,17,19,23,29,31,37,41
data 43,47,53,59,61,67,71,73,79,83,89,97
deflng A-Z
read N:PI100=N
dim B(N+1),C(N),P(N)
for I=1 to N:read P(I):next
M=0:PI104=PI100-1:B(0)=0:K=0
10 '
if K<N then K=K+1:B(K)=0:goto 10
M=M+1:DE=1
for I=1 to N
 if abs(DE)>10000 then 20
 if B(I)<>0 then DE=-DE*P(I)
 C(I)=B(I)*P(I)
next
NP=fix(10000/DE):PI104=PI104+NP
20 '
if B(K)=1 then K=K-1 :goto 20
B(K)=1
if K=0 then goto 30
goto 10
30 print "*** PI(10000)=";PI104;" ***"
stop
end
```

8 「エラトステネスの篩い」のプログラム

1,2,3,4,5,6,7,8,9,10,11,12,... において 2 は最初の素数である．2 以上の自然数のうちから 2 の倍数 4,6,8,10,12,... を取り除く、次の素数である 3 の倍数 6,9,12,... を取り除く．6,9,12,... のうち 6,12 は 2 の倍数でもある．これを繰り返し残された数がすべて素数である．このようにして素数を得る方法を「エラトステネスの篩い」という．この方法において，残された素数のうち最大のものを p とするとき，p 以上の自然数のうち，$2p, 3p, 4p, \cdots (p-1)p$ はすでに取り除かれているので，$p^2, (p+1)p, \ldots$ を取り除けばよい．この事を考慮した F-BASIC プログラムは右のごとくである．このプログラムを実行すると素数 p に対しては配列 $Q(p)$ の値が 1、素数でない場合には 0 が与えられる．

```
Input “ N= ”;N
dim Q(N)
Q(1)=0:for I=2 to N:Q(I)=1:next
I=1:M=0
10 I=I+1:if N<I*I then 20
If Q(I)=0 then 10
M=M+1:print M,I
I2=I*I
for J=I2 to N step I:Q(J)=0:next
goto 10
20 ’
for J=I to N
  if Q(J)=1 then M=M+1:print M,J
next
end
```

9 素数分布関数

自然数 $2, 3, \ldots, x$ のから 2 の倍数を取り除くと残る数の割合は $\left(1-\frac{1}{2}\right)$，更に 3 の倍数を取り除くとその割合は $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$，5 の倍数を取り除くと $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$，.... p を x 以下で最大の素数とすると，素数密度は

$$\frac{\mathrm{d}\pi(x)}{\mathrm{d}x} = \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\cdots\left(1-\frac{1}{p}\right) = \prod_{p<x}\left(1-\frac{1}{p}\right). \tag{26}$$

然るに，自然数 n は素因数 $p_1, p_2, \ldots, p_m$ によって $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$ と表わされるので

$$\prod_{p<x}\left(1-\frac{1}{p}\right)^{-1} = \prod_{p<x}\left(1+\frac{1}{p}+\frac{1}{p^2}+\ldots\right) = \sum_{(\alpha_1,\alpha_2,\ldots,\alpha_m)} \frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}} = \sum_{n=1}^{x}\frac{1}{n}. \tag{27}$$

上式の和の範囲は $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} < x$ を満たすあらゆる $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ の組み合わせについてなされる．したがって

$$\frac{\mathrm{d}\pi(x)}{\mathrm{d}x} = \left(\sum_{n=1}^{x}\frac{1}{n}\right)^{-1}. \tag{28}$$

さらに

$$\sum_{n=1}^{x}\frac{1}{n} \simeq \int_1^x \frac{1}{x}\mathrm{d}x = \ln x, \quad \therefore \quad \frac{\mathrm{d}\pi(x)}{\mathrm{d}x} \simeq \frac{1}{\ln x}. \tag{29}$$

$x > 2$ であるから

$$\pi(x) \simeq \int_2^x \frac{1}{\ln x}\mathrm{d}x = Li(x). \tag{30}$$

表 1 には $\pi(x)$ と $Li(x)$ の数値計算結果[3]が比較されている．x が大きくなると上式の近似がよいことが分かる．

表 1: $\pi(x)$ と $Li(x)$ の比較

x	$\pi(x)$	$Li(x)$	$\frac{\pi(x)}{Li(x)}$
10	4	5.120	0.78118
100	25	29.081	0.85967
1000	168	176.56	0.95149
10000	1229	1245.09	0.98708
100000	9592	9628.76	0.99618
1000000	78498	78626.5	0.99837
10000000	664579	664917.	0.99949
100000000	5761455	5762210.	0.99987
1000000000	50847534	50849200.	0.99997
10000000000	455052511	455056000.	0.99999

[3]Mathematica の PrimePi および NIntegrate を使用した．