約数の個数

坂本（さかもと） 茂（しげる）

$(1+a_1)(1+a_2)\cdots\cdots(1+a_m)$ の展開を考えると

$$1+\sum_{i=1}^{m}a_i+\sum_{i_1<i_2}a_{i_1}a_{i_2}+\cdots\cdots+\sum_{i_1<i_2<\cdots<i_m}a_{i_1}a_{i_2}\cdots\cdots a_{i_m}$$

となる．ここで Σ の i_j $(j=1,\ 2,\ \cdots\cdots,\ m)$ は $1\leqq i_1<i_2<\cdots\cdots<i_n\leqq m$ となるようなものの総和である．したがって（$a_i=-a_i$ のときの場合も一緒に書くと）

$$\prod_{i=1}^{m}(1\pm a_i)=1+\sum_{k=1}^{m}\left\{(\pm1)^{k+1}\sum_{i_1<i_2<\cdots<i_k}\prod_{j=1}^{k}a_{i_j}\right\}$$

と書ける．たとえば，$1\leqq i_1<i_2<\cdots\cdots<i_k\leqq m$ についての総和 $\Sigma1$ は，m 個から k 個とったものの組合せの数だけ1を加えることであるから，${}_mC_k$ である．よって，$a_i=a$ $(i=1,\ \cdots\cdots,\ m)$ ならば2項定理

$$(1+a)^m=1+\sum_{k=1}^{m}{}_mC_ka^k=\sum_{k=0}^{m}{}_mC_ka^k$$

を得る．

p, q が素数なら p, p^k, pq の約数の個数はそれぞれ1, p^{k-1}, $p+q-1$ である．a の約数に素数が p_1, p_2, $\cdots\cdots$, p_m の m 個あったとする．a 以内の p_i の倍数の集合を S_i とすると，a の約数の個数は $n\left(\bigcup_{i=1}^{m}S_i\right)$ である．これは

$$n\left(\bigcup_{i=1}^{m}S_i\right)=\sum_{i=1}^{m}n(S_i)-\sum_{i_1<i_2}n(S_{i_1}\cap S_{i_2})+\sum_{i_1<i_2<i_3}n(S_{i_1}\cap S_{i_2}\cap S_{i_3})-\cdots\cdots=\sum_{k=1}^{m}\left\{(-1)^{k+1}\sum_{i_1<i_2<\cdots<i_k}n\left(\bigcap_{j=1}^{k}S_{i_j}\right)\right\}$$

となる．ここで

$$n(S_i)=\frac{a}{p_i},\quad n(S_1\cap S_2)=\frac{a}{p_1p_2},$$

$$n\left(\bigcap_{j=1}^{k}S_{i_j}\right)=\frac{a}{p_{i_1}p_{i_2}\cdots\cdots p_{i_k}}$$

であるから，約数の個数は

$$\sum_{k=1}^{m}(-1)^{k+1}\sum_{i_1<i_2<\cdots<i_k}a\prod_{j=1}^{k}\frac{1}{p_{i_j}}$$

と書けるから，次のようになる．

$$n\left(\bigcup_{i=1}^{m}S_i\right)=a\left\{\prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right)-1\right\}$$

ここで a 以内の数で a と互いに素である数の個数を $\varphi(a)$ で表すことにする．たとえば，p, q が素数なら

$$\varphi(p)=p-1,\quad \varphi(p^k)=p^k-p^{k-1},$$
$$\varphi(pq)=pq-p-q+1$$

である．約数でないものの数が $\varphi(a)$ であるから

$$\varphi(a)=a-n\left(\bigcup_{i=1}^{m}S_i\right)=a\prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right)$$

となる．一般に整数は素数 p_i を用いて $a=p_1{}^{a_1}p_2{}^{a_2}\cdots\cdots p_m{}^{a_m}$ と書け，

$$\varphi(a)=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\cdots\left(1-\frac{1}{p_m}\right)$$

である．たとえば

$$\varphi(p)=p\left(1-\frac{1}{p}\right),\quad \varphi(p^k)=p^k\left(1-\frac{1}{p}\right),$$

$$\varphi(pq)=pq\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$$

である．また，式から $\varphi(ab)=\varphi(a)\varphi(b)$ がただちに分かる．

s より小さくて s と互いに素な $\varphi(s)$ 個の数を

$$t_1,\ t_2,\ \cdots\cdots,\ t_{\varphi(s)}$$

とする．これらの1つを a とすると

$$at_1,\ at_2,\ \cdots\cdots,\ at_{\varphi(s)}$$

はどの2つも m を法として合同ではない．もし $xt_i\equiv xt_j \bmod s$ とすると，$a(t_i-t_j)\equiv0$ で $a\not\equiv0$ $\bmod s$ より $t_i\equiv t_j$ となり矛盾である．よって

$$t_1t_2\cdots\cdots t_{\varphi(s)}\equiv t_1t_2\cdots\cdots t_{\varphi(s)}a^{\varphi(s)}$$

である．したがって

$$a^{\varphi(s)}\equiv1 \mod s$$

（a と s は互いに素である）$s=p$ が素数なら $\varphi(s)=p-1$ で

$$a^{p-1}\equiv1 \mod p$$

である（フェルマの定理）．

（東京都立小平高等学校）