# オイラー関数とオイラーの定理

負でない整数を自然数と定義する流儀もあるが，以下では正の整数を自然数とする．また，特にことわりの無い限り $p$ や $P$ は素数を表す.

**定義 1**　自然数 $n$ に対して，$n$ 以下の自然数で $n$ との最大公約数が 1 であるものの個数を $\phi(n)$ で表す．$\phi$ は**オイラー関数**と呼ばれる.

$$\phi(1) = 1$$

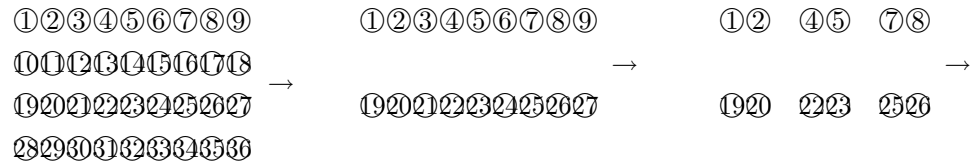
である。

**定理 1**　自然数 $n$ と互いに素の数の個数を，$\phi(n)$ とする．$m, n$ が互いに素のとき

$$\boxed{\phi(mn) = \phi(m)\phi(n)}$$

である.

[**証明**]　この証明はいろいろ考えられるが，視覚的に理解するには，碁石を $mn$ 個長方形に並べる．1 から順に番号をつけるとわかりやすい．つまり，$m$ 行 $n$ 列の長方形に番号付きの碁石を並べる．そのなかから，まず $m$ と互いに素でない 1 以外の碁石を除く．そうすると $m$ の約数が属する行がなくなる．次に と 互いに素でない 1 以外の碁石をとり除く．$n$ の約数（1 以外）が属する列の碁石がなくなる．残った碁石の数が $\phi(mn)$ である．数えるには，上下左右に形をくずさないで縮めると $\phi(m)$ 行 $\phi(n)$ 列の長方形になることがわかる.



[証明おわり]

**定理 2**

$$\boxed{\phi(abc\cdots) = \phi(a)\phi(b)\phi(c)\cdots \quad (\text{ただし，} a, b, c, \cdots \text{は互いに素})}$$

[**証明略**]

**定理 3**　$p^n$ と互いに素でないそれ以下の自然数は $p^{n-1}$ 個ある

[**証明**]　$p^n$ と互いに素でない自然数は $px$ とかける．$x$ は $1 \leq x \leq p^{n-1}$ の全ての自然数の値を取り得，なおかつそのどの $x$ についても $px$ が重複することはない（つまり $p$ の倍数）．よってその個数は $p^{n-1}$ である.

[証明おわり]

**定理 4**

$$\boxed{\phi(p^n) = p^n - p^{n-1}}$$

[**証明略**]　定理 3 より明らか.

**定理 5**　自然数 $n$ が $\prod_{j=1}^{\mathrm{k}} {P_j}^{m_j} (P_i, \cdots, P_k$ は相異なる素数,$m_j \geq 1)$ と素因数分解されたとする．このとき，1 から $n$ までの整数で，$n$ と互いに素なものの個数は

$$\boxed{\phi(n) = n \prod_{j=1}^{\mathrm{k}} \left(1 - \frac{1}{P_j}\right)}$$

である．

[**証明**]

$$\begin{aligned}
\phi\left(\prod_{j=1}^{\mathrm{k}} {P_j}^{m_j}\right) &= \prod_{j=1}^{\mathrm{k}} \phi({P_j}^{m_j}) \\
&= \prod_{j=1}^{\mathrm{k}} ({P_j}^{m_j} - {P_j}^{m_j - 1}) \\
&= \prod_{j=1}^{\mathrm{k}} {P_j}^{m_j} \left(1 - \frac{1}{P_j}\right) \\
&= \prod_{j=1}^{\mathrm{k}} {P_j}^{m_j} \prod_{j=1}^{\mathrm{k}} \left(1 - \frac{1}{P_j}\right) \\
&= n \prod_{j=1}^{\mathrm{k}} \left(1 - \frac{1}{P_j}\right)
\end{aligned}$$

[証明終わり]

この定理は

$$\boxed{\phi\left(\prod_{j=1}^{\mathrm{k}} {P_j}^{m_j}\right) = \prod_{j=1}^{\mathrm{k}} {P_j}^{m_j - 1} (P_j - 1)}$$

とかくこともできる．

**問題 1**　$\phi(2009)$ を求めよ．

[**解**]

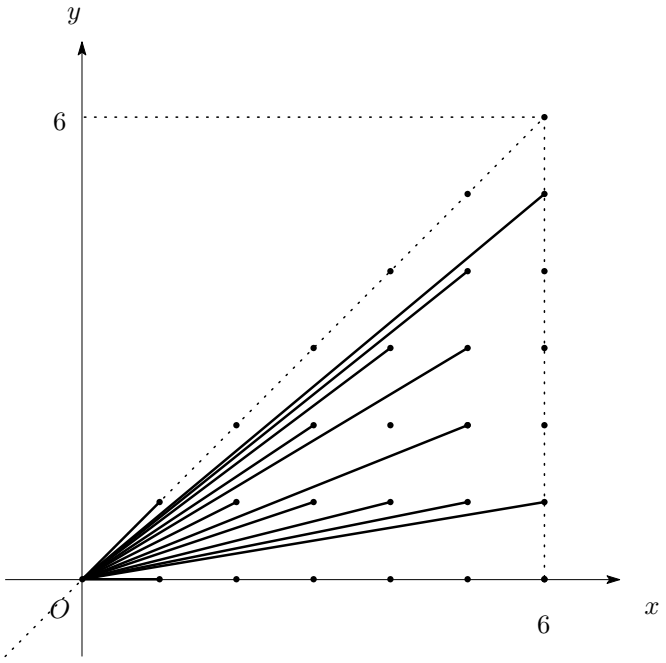
$$\phi(2009) = \phi(7^2 \cdot 41) = 7(7-1)(41-1) = 1680$$

**問題 2**　座標平面上で 3 直線 $y = 0, x = 6, y = x$ に囲まれた直角二等辺三角形の内部と周上の格子点と原点を結ぶ線分で，両端以外に格子点をもたないものの本数を求めよ．

[**解**]　このような線分の原点で無いほうの（右の）端点の座標を (x,y) とすると，$\frac{y}{x}$ は既約分数である．もしそうでなければ途中に格子点をもつ．
$x \geq y > 0$ である既約分数 $\frac{y}{x}$ の個数は $\phi(x)$ に等しい．よって求める線分の本数は

$$\begin{aligned}
&1 + \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(5) + \phi(6) \\
=&1 + 1 + 1 + 2 + 2 + 4 + 2 \\
=&13
\end{aligned}$$

最初の 1 は $\dfrac{0}{1}$ を表し，線分は $(0,0)-(1,0)$ に対応する．$\phi(1)$ は $\dfrac{1}{1}$ を表し，$(0,0)-(1,1)$ に対応する．これらを既約分数と言うには無理があるかもしれない．




**定理 6** 素数は無限にある．

[**証明**]　素数が有限個しかないと仮定する．
最大の素数を $p$ として，

$$q = 1 \times 2 \times 3 \times \cdots \times p + 1$$

という数を考える．

(1) $q$ を素数とすると $\cdots p$ が最大の素数であるということに矛盾する．
(2) $q$ が素数でないとすると $\cdots q$ は $p$ 以下のいずれかの素数で割り切れるはずだが，$q$ の形より，$q$ は 2 から $p$ までのすべての数で割り切れないので矛盾する．

いずれにせよ，矛盾するので素数が有限個であるという仮定が誤りであることがわかる．
よって，素数は無限にある．　[証明おわり]

**問題 3**　次のことを証明せよ．

(1)

$$\lim_{m\to\infty} \phi(m) = \infty$$

(2)

$$a_{\mathrm{m}} = \frac{\phi(m)}{m} \quad (m \geq 1)$$

とおくと，数列 $a_1, a_2, a_3, \cdots$ は極限をもたない．

[**解**]

(1) $m$ より小さい素数の個数を $p(m)$ とすると，

$$\phi(m) \geq p(m)$$

定理 6 より

$$\lim_{m\to\infty} p(m) = \infty$$

よって $\phi(m)$ も $\infty$ に発散する． [証明おわり]

(2) 定理 5 より

$$\frac{\phi(m)}{m} = \prod_{j=1}^{n}\left(1 - \frac{1}{P_j}\right)$$

である．ただし，$p_j$ は $m$ の素因数分解で出てきた $j$ 番目の素数を表す．

このことより素数に限って言えば

$$\frac{\phi(p)}{p} = 1 - \frac{1}{p}$$

なのでこれは 1 に収束する．

偶数に限って言えば $1 - \dfrac{1}{2}$ 以下になるのでこのことだけをとりあげても収束はしない（極限をもたない）． [証明おわり]

**定義 2 （合同式）** 二つの整数 $a, b$ について $a-b$ が自然数 $n$ で割り切れるとき，$n$ を法として**合同**(congruent modulo $n$) であるといい，

$$a \equiv b \quad (\mod n)$$

と表す．

合同式には色々な性質があるが，ここでは一般の等式における除法に相当する性質について証明しておく．

**定理 7** $a$ と $n$ が互いに素で，$b, c$ が整数のとき，自然数 $n$ を法とする合同式において．

$$b \equiv c \Longleftrightarrow ab \equiv ac$$

が成り立つ．

[**証明**] 合同式について何が既知であるかによって証明も色々あるが，$b-c$ が $n$ で割り切れることと，$a(b-c)$ が $n$ で割り切れることとは，$a$ と $n$ が互いに素である場合に限って言えば同値である． [証明おわり]

**定理 8 （オイラーの定理）** 自然数 $n$ と互いに素である自然数 $a$ について，

$$\boxed{a^{\phi(n)} \equiv 1 \quad (\mod n)}$$

が成り立つ．

[**証明**] $n$ 以下の自然数で $n$ と互いに素な数を

$$r_1, r_2, r_3, \cdots, r_{\phi(n)} \tag{1}$$

と表す．これらに，$n$ と互いに素である自然数 $a$ をかけた数，

$$ar_1, ar_2, ar_3, \cdots, ar_{\phi(n)} \tag{2}$$

を考える．これらも全て $n$ と互いに素である．また，

$$i \neq j \Longrightarrow ar_i \not\equiv ar_j$$

である．なぜならば，もし $ar_i \equiv ar_j$ とすると，$a(r_i - r_j) \equiv 0$ つまり $r_i - r_j$ は $n$ で割り切れ，$r_i \equiv r_j$ となってしまい，仮定と矛盾する．つまり (2) の各数は (1) のどれか一つと合同になり，なおかつ重複することはない．したがってこれらをすべてでかけ合わせたものも合同になる．すなわち，

$$a^{\phi(n)} r_1 r_2 r_3 \cdots r_{\phi(n)} \equiv r_1 r_2 r_3 \cdots r_{\phi(n)} \quad (\mod n)$$

よって

$$a^{\phi(n)} \equiv 1$$

[証明おわり]

この定理の特殊な場合が次の定理である．

**定理 9 （フェルマーの小定理）** $p$ の倍数でない自然数 $a$ について，

$$\boxed{a^{p-1} \equiv 1 \quad (\mod p)}$$

が成り立つ．これらの定理は $a$ が正の整数として証明したが，整数全体に拡張してもよい．

**問題 4** $2009^{2009}$ の下 3 桁を求めよ．

[**解**]

$$\begin{aligned}
\phi(1000) &= \phi(2^3 5^3) \\
&= 2^2 5^2 (2-1)(5-1) = 400 \\
2009^{2009} &\equiv 9^{2009} \qquad (\mathrm{mod}\ 1000) \\
&\equiv 9^{400\times 5+9} \\
&\equiv 9^9 \\
&\equiv (81^2)^2 \times 9 \\
&\equiv 561^2 \times 9 \\
&\equiv 721 \times 9 \equiv 489 \cdots (\text{こたえ})
\end{aligned}$$

これらの定理は $n$ を法として 1 を得る最小の冪を与えるものではないことを注意しなければならない．たとえば

$$p = 7, a = 4$$

とすると，フェルマーの小定理は

$$4^6 \equiv 1 \quad (\mathrm{mod}\ 7)$$

となることを主張しているわけだが，

$$4^3 = 64 \equiv 1 \quad (\mathrm{mod}\ 7)$$

なので 6 より小さい冪 3 で既に 1 に合同になっている．この小さい冪はというのは必ず $p-1$ の約数になっている．しかしながら，$p$ の倍数で無いあらゆる整数 $a$ について 1 と合同になる最小の冪は $p-1$ である．これらの証明はここでは記述しない．

また，オイラーの定理の方も，たとえば $n = 21 = 3 \times 7$ のような場合，定理は

$$a^{\phi(21)} = a^{12} \equiv 1 \pmod{21}$$

を主張しているのだが，実際

$$a^{\phi(3)} = a^2 \equiv 1 \pmod{3}$$
$$a^{\phi(7)} = a^6 \equiv 1 \pmod{7}$$

となるので，$(a^2)^3 - 1$ は 3 でも 7 でも割り切れ，

$$a^6 \equiv 1 \pmod{21}$$

が成り立つ．つまり 12 より小さい冪 6 で既に 1 に合同になっている．このとについても証明はここでは行わない．

**定理 10**　自然数 $n$ が $\prod_{j=1}^{\mathrm{k}} {P_j}^{m_j} (P_i, \cdots, P_k$ は相異なる素数,$m_j \geq 1)$ と素因数分解されたとする．このとき，$n$ の約数の個数は

$$\boxed{\prod_{j=1}^{\mathrm{k}} (m_j + 1)}$$

である．

[**証明略**]

**定理 11**　自然数 $n$ が $\prod_{j=1}^{\mathrm{k}} {P_j}^{m_j} (P_i, \cdots, P_k$ は相異なる素数,$m_j \geq 1)$ と素因数分解されたとする．このとき，$n$ の約数の和は

$$\boxed{\prod_{j=1}^{\mathrm{k}} \sum_{i=0}^{m_j} P_j^{m_i} = \prod_{j=1}^{\mathrm{k}} \frac{P_j^{m_j+1} - 1}{P_j - 1}}$$

であり，約数の平均は

$$\boxed{\prod_{j=1}^{\mathrm{k}} \frac{P_j^{m_j+1} - 1}{(P_j - 1)(m_j + 1)}}$$

である．

[**証明略**]

**問題 5** 2009 の約数の和と平均を求めよ．

[**解**]

$$(1 + 7 + 7^2)(1 + 41) = 57 \times 42 = 2394 \cdots (\text{和})$$

$$\frac{2394}{6} = 399 \cdots (\text{平均})$$

**定理 12** 自然数 $n$ と互いに素である $n$ 以下の自然数の和は

$$\boxed{\frac{n\phi(n)}{2}}$$

であり，平均は

$$\boxed{\frac{n}{2}}$$

である．また $n$ と互いに素でない $n$ 以下の自然数の和は

$$\boxed{\frac{n\left\{n-\phi(n)+1\right\}}{2}}$$

であり，平均は

$$\boxed{\frac{n\left\{n-\phi(n)+1\right\}}{2\left\{n-\phi(n)\right\}}}$$

である．

[**証明**]　$n$ と互いに素でない $n$ 以下の自然数に 0 を含めて考えると，次のように重複を含めて全て左右対称に並ぶ．例えば $n=10$ の場合は

$$⓪\,1\,②\,3\,④⑤⑥\,7\,⑧\,9\,⑩$$

である．よってこれらの平均は 0 を含めて考えると

$$\frac{n}{2}$$

である．0 を含めて考えているので個数は

$$n-\phi(n)+1$$

である．合計は

$$\frac{n\left\{n-\phi(n)+1\right\}}{2}$$

0 を含めないで平均を出すと，

$$\frac{n\left\{n-\phi(n)+1\right\}}{2\left\{n-\phi(n)\right\}}$$

また 1 から $n$ の合計

$$\frac{n(n+1)}{2}$$

から引いてやることで，自然数 $n$ と互いに素である $n$ 以下の自然数の和は

$$\frac{n\phi(n)}{2}$$

が求まり，平均は

$$\frac{n}{2}$$

である．　[証明おわり]

やや複雑に見えるが，0 を入れて考えれば，0 から $n$ までの平均も，$n$ と互いに素であるものの平均も，$n$ と互いに素でないものの平均も全て

$$\frac{n}{2}$$

なのである．0 を入れないので微妙に違うだけである．

**問題 6**　2009 以下の自然数で 2009 と互いに素でないものの平均を求めよ．

[**解**]

$$\frac{2009\left\{2009-\phi(2009)+1\right\}}{2\left\{2009-\phi(2009)\right\}}=\frac{2009\left\{2009-1680+1\right\}}{2\left\{2009-1680\right\}}=\frac{47355}{47}$$

**定理 13**　自然数 $n$ 以下の $n$ と互いに素である自然数の総和を $S$ とすると，$n\geq 3$ のとき

$$\boxed{S\equiv 0 \pmod{n}}$$

である．

[**証明**]　定理 12 より

$$S=\frac{n\phi(n)}{2}$$

定理 5 より $n\geq 3$ では $\phi(n)$ は一つ以上の素因数 2 をもつか，あるいは 2 以外の素数 $p$ について素因数 $(p-1)$ をもつ．これらは全て偶数なので $\phi(n)$ は 2 で割り切れる．よって $S$ は必ず $n$ で割り切れる．　[証明おわり]

**定理 14**　自然数 $n$ が 互いに素 である 2 つの自然数 $a,b$ により，$n=ab$ と表されるとき，

$$\boxed{a^{\phi(b)+1}\equiv a \pmod{n}}$$

とくに $b=p$（$p$ は素数）のとき

$$\boxed{a^{p}\equiv a \pmod{n}}$$

[証明]

$$a^{\phi(b)+1}-a\equiv a(a^{\phi(b)}-1) \pmod{n}$$

オイラーの定理より $a^{\phi(b)}-1$ は $b$ で割り切れる．よって

$$a(a^{\phi(b)}-1)\equiv 0 \pmod{n}$$

[証明おわり]

このことは $a^n$ が $n$ について考えると $\phi(b)$ の周期をもっていることを表している．しかしこれが成り立つからといって $a^{\phi(b)}-1\equiv 0 \pmod{n}$ ということではないので注意が必要である．また，$a$ の倍数 $ak$ が b と互いに素であれば，

$$\boxed{(ak)^{\phi(b)+1}\equiv (ak) \pmod{n}}$$

であることも言える．

**問題 7**

$$1^{2009}+2^{2009}+3^{2009}+\cdots+2009^{2009}$$

を 21 で割ると余りはいくつか．

[**解**] 合同式は全て 21 を法とする (mod 21 を省略する).

$$2009 = 7^2 \cdot 41$$

$$21 = 3 \cdot 7$$

21 未満で 21 と互いに素の数は,

$$1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20$$

なので,

$$\phi(21) = 12$$

(定理 5 を用いて $\phi(3 \cdot 7) = (3-1)(7-1) = 12$ としてもよい. )
よって 21 と互いに素である数 $a$ について

$$a^{12} \equiv 1$$

$2009 = 12 \cdot 167 + 5$ であることから, これらの $a$ について

$$a^{2009} \equiv a^5$$

$$a \equiv 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20 \tag{3}$$

に対して,

$$a^5 \equiv 1, 11, 16, 17, 8, 19, 2, 13, 4, 5, 10, 20 \tag{4}$$

実はこれは (3) を並べ変えただけである. またこれら $a^5$ の和は

$$1 + 11 + 16 + 17 + 8 + 19 + 2 + 13 + 4 + 5 + 10 + 20 \equiv 0$$

である. これは定理 13 より当然のことである. ここまでのことを総合すると,

$$2009 = 21 * 95 + 14 \tag{5}$$

であるから 1 から 1995 までの 21 と互いに素である $a$ について $a^{2009}$ の和は 21 を法として 0 である. また 21 の倍数である $a$ について $a^{2009}$ は当然 21 を法として 0 である.
よって問題となるのは 1996 から 2009 までの 21 と互いに素である $a$ について $a^{2009}$ の和と, 3 または 7 の倍数で 21 の倍数でない $a$ について $a^{2009}$ の和を求めればいいのである. まず前者から求めてゆこう.
(4) より 1996 から 2009 までの 21 と互いに素である $a$ について $a^{2009}$ の和は

$$1 + 11 + 16 + 17 + 8 + 19 + 2 + 13 \equiv 87 \equiv 3 \tag{6}$$

次に 3 の倍数の 2009 乗について調べる. 3 の倍数の累乗は定理 14 より,

$$\begin{aligned} &3^{2009} + 6^{2009} + 9^{2009} + 12^{2009} + 15^{2009} + 18^{2009} \\ \equiv &3^5 + 6^5 + 9^5 + 12^5 + 15^5 + 18^5 \\ \equiv &3^5(1^5 + 2^5 + 3^5 + 4^5 + 5^5 + 6^5) \end{aligned}$$

(4) より

$$\begin{aligned}&3^5(1^5+2^5+3^5+4^5+5^5+6^5)\\\equiv&12(1+11+12+16+17+6)\\\equiv&12\times 0\\\equiv&0\end{aligned}$$

(5) より 1 から 1995 までの 3 の倍数の 2009 乗の和は 21 を法として 0 である．よって 1996 から 2009 までの 2009 乗の和を求めると，

$$\begin{aligned}&3^5(1^5+2^5+3^5+4^5)\\\equiv&12(1+11+12+16)\\\equiv&12\times 19\\\equiv&18\end{aligned}\tag{7}$$

7 の倍数の 2009 乗は定理 14 より，

$$\begin{aligned}&7^{2009}+14^{2009}\\\equiv&7+14\\\equiv&\,0\end{aligned}$$

1 から 2009 まで，上記のような 7 の倍数はちょうど偶数個あるので，全て足すと結局 21 を法として 0 となる．よって求める余りは，(6),(7) より，

$$3+18\equiv 0$$

つまり割り切れる．

[**別解**]　21 と互いに素の数の場合，全て 21 を法として

$$a^7\equiv a$$

3 の倍数の場合

$$a^7\equiv a$$

7 の倍数の場合

$$a^3\equiv a$$

21 の倍数の場合

$$a\equiv 0$$

つまり，1,2,6 の最小公倍数 6 で，全ての整数 $a$ について

$$a^7\equiv a$$

がなりたつ，つまり

$$1^{2009}+2^{2009}+3^{2009}+\cdots+2009^{2009}\equiv 1^5+2^5+3^5+\cdots+2009^5$$

5 は素数なのでライプニッツの公式により

$$
\begin{aligned}
\text{与式} &\equiv (1+2+3+\cdots+2009)^5 \\
&= (1005\times 2009)^5 \\
&\equiv (18\times 14)^5 \\
&\equiv 0^5 \\
&= 0
\end{aligned}
$$

**定理 15** $n$ と $a$ が互いに素であるとき，一次合同式

$$ax \equiv b \pmod{n} \tag{8}$$

の解は

$$\boxed{x \equiv a^{\phi(n)-1}b \pmod{n}}$$

である．

**[証明略]**
一次合同式をこのように解くことは少ない．(8) は一次不定方程式

$$ax - ny = b$$

を解くのに等しいので，必ず解ける．実際 $\phi(n)$ を求めることは素因数分解またはそれに匹敵する計算が必要で，さらに $a^{\phi(n)-1}$ を求めるのも $n$ によっては繁雑である．しかしながら，一次方程式を解くように一次合同式を解く事が可能であると実感できる．

**定理 16**　自然数 $n$ について

$$\boxed{\sum_{i=1}^{n}\phi(p^i) = p^n}$$

が成り立つ．

**[証明]**　定理 4 より

$$\text{左辺} = p^n - p^{n-1} + p^{n-1} - p^{n-2} + \cdots + p - 1 + 1 = p^n$$

[証明おわり]

**定理 17**　自然数 $n$ について

$$\boxed{\sum^{d|n}\phi(d) = n}$$

が成り立つ．

**[証明]**　$n = \prod_{j=1}^{\mathrm{k}} {P_j}^{m_j}$ ($P_i, \cdots, P_k$ は相異なる素数,$m_j \geq 1$) と素因数分解されたとする．このとき，

$$
\begin{aligned}
&\sum_{d|n}\phi(d)\\
=&(\phi(P_1^{m_1})+\phi(P_1^{m_1-1})+\cdots+\phi(1))(\phi(P_2^{m_2})+\phi(P_2^{m_2-1})+\cdots+\phi(1))\cdots(\phi(P_k^{m_k})+\cdots+\phi(1))\\
=&P_1^{m_1}P_2^{m_2}\cdots P_k^{m_k}\\
=&n
\end{aligned}
$$

[証明おわり]

**定理 18** $n$ の任意の約数を $d$ とするとき，$n$ 個の数 $1,2,3,\cdots,n$ の中に $(x,d)=d$ である $x$ の個数は

$$\phi\left(\frac{n}{d}\right) \text{ 個}$$

である．

[**証明**]

$$x=dx',n=dn'$$

とおくと，$x$ の個数は $1,2,3,\cdots,n'$ の中で $n'$ と互いに素である数の個数，つまり $(x',n')=1$ である $x'$ の個数に等しい．つまりそれは

$$\phi(n') \text{ 個}$$

である． [証明おわり]