φ^k 同値について

梶田光

2025/08/05

1. はじめに

以前, $n \underset{\varphi}{\sim} m \Longleftrightarrow \dfrac{\varphi(n)}{n} = \dfrac{\varphi(m)}{m}$ によって定義される φ 同値の条件を解明した.

具体的には, $n \underset{\varphi}{\sim} m \Longleftrightarrow \mathrm{rad}(n) = \mathrm{rad}(m)$ がわかった.

今回はその一般化について考察する.

なお, $\varphi^k(n)$ は φ の k 回合成とし, 特に $\varphi^0(n) = n$ と考える.

2. 弱い条件

結論から述べると, $\dfrac{\varphi^k(n)}{n} = \dfrac{\varphi^k(m)}{m} \Longrightarrow \mathrm{rad}(n) = \mathrm{rad}(m)$ が言える.

さて, その証明のためにいくつか補題と補助関数を用意する.

定義 2.1: 正整数 n に対し, 関数 φ' を $\varphi'(n) = n \displaystyle\prod_{p^e \,\|\, n} \left(1 - \frac{1}{p}\right)^e$ で定義し, 重複オイラー関数と呼ぶ.

$\varphi'(n) = \displaystyle\prod_{p^e \,\|\, n} (p-1)^e$ とも書けることから, φ' は完全乗法的関数である.

つまり, 任意の(互いに素とは限らない)正整数 a, b に対して $\varphi'(ab) = \varphi'(a)\varphi'(b)$ が成り立つ.

命題 2.1: I を正整数とする. 無平方数の正整数からなる数の組 $(\alpha_1, \alpha_2, ..., \alpha_I)$ について,
$A = \displaystyle\prod_{i=1}^{I} \alpha_i$ とおくと, $\displaystyle\prod_{i=1}^{I} \frac{\varphi(\alpha_i)}{\alpha_i} = \frac{\varphi'(A)}{A}$ が成り立つ.

Proof: 式は $\displaystyle\prod_{i=1}^{I} \prod_{p \,|\, \alpha_i} \left(1 - \frac{1}{p}\right) = \prod_{p^e \,\|\, A} \left(1 - \frac{1}{p}\right)^e$ と書き直せる.

さて, いま任意の素数 p を取ったとき, α_i はすべての i について無平方数であるから, $A = \displaystyle\prod_{i=1}^{I} \alpha_i$ より $\nu_p(A)$ は $p \mid \alpha_i$ を満たす i の個数に等しい.

つまり, 任意の p について左辺と右辺には同じ個数の $1 - \dfrac{1}{p}$ が積に含まれているので, 式は成り立つ. ■

命題 2.2: 任意の正整数 n, m に対し, $\dfrac{\varphi'(n)}{n} = \dfrac{\varphi'(m)}{m} \Longleftrightarrow n = m$.

Proof: 右から左は明らかであろう. よって示したいのは $\dfrac{\varphi'(n)}{n} = \dfrac{\varphi'(m)}{m} \Longrightarrow n = m$ である.

(1) $\gcd(\varphi'(n), n) = 1$ の場合

$\dfrac{\varphi'(n)}{n}$ が既約分数なので, ユークリッドの補題からある正整数 k を用いて $m = kn, \varphi'(m) = k\varphi'(n)$ と書ける.

さて, 完全乗法性から $\varphi'(m) = \varphi'(kn) = \varphi'(k)\varphi'(n)$ と書け, したがって $\varphi'(k) = k$.

定義式から, $k > 1$ とすると $\varphi'(k) < k$ となってしまうので, $k = 1$, したがって $n = m$ が言える.

(2) $\gcd(\varphi'(n), n) = n_1 > 1$ の場合

両辺の既約分数形を $\dfrac{x}{y}$ と書けば, $\varphi'(n) = n_1 x, n = n_1 y$ が成り立ち,

さらにある正整数 m_1 で $\varphi'(m) = m_1 x, m = m_1 y$ を満たすものが存在する.

ここでは, $\dfrac{n}{m} = \dfrac{n_1}{m_1}$ が成り立っている.

さて, $\dfrac{\varphi'(n)}{n} = \dfrac{\varphi'(n_1 y)}{n_1 y} = \dfrac{\varphi'(n_1)}{n_1} \cdot \dfrac{\varphi'(y)}{y}$.

同様に, $\dfrac{\varphi'(m)}{m} = \dfrac{\varphi'(m_1)}{m_1} \cdot \dfrac{\varphi'(y)}{y}$ から, $\dfrac{\varphi'(n_1)}{n_1} = \dfrac{\varphi'(m_1)}{m_1}$.

さて, ここで $n_1 = n$ とすると $n \mid \varphi'(n)$ だが, 一般に $n > 1$ なら $\varphi'(n) < n$ より $n = 1$.

これは $n_1 > 1$ に矛盾するので, $n_1 \neq n$, つまり $n_1 < n$ が成り立つことがわかる.

ここから, n_1, m_1 に対して上記の議論をそのまま適用することができる.

つまり, (1) から $n_1 = m_1$ となるか, もしくはある $n_2 < n_1, \dfrac{\varphi'(n_2)}{n_2} = \dfrac{\varphi'(m_2)}{m_2}, \dfrac{n_2}{m_2} = \dfrac{n_1}{m_1}$ を満たす正整数の組 n_2, m_2 が存在する.

さて, ここまでの議論をまとめると以下のようになる.

$$\begin{tikzcd}
\dfrac{\varphi'(n)}{n} = \dfrac{\varphi'(m)}{m} \arrow[r, "\text{otherwise}"'] \arrow[d, "{\gcd(n, \varphi'(n)) = 1}"'] & \dfrac{\varphi'(n_1)}{n_1} = \dfrac{\varphi'(m_1)}{m_1} \arrow[r, "\text{otherwise}"'] \arrow[d, "{\gcd(n_1, \varphi'(n_1)) = 1}"'] & \dfrac{\varphi'(n_2)}{n_2} = \dfrac{\varphi'(m_2)}{m_2} \arrow[r, "\text{otherwise}"'] \arrow[d, "{\gcd(n_2, \varphi'(n_2)) = 1}"'] & \dots \\
n = m & n_1 = m_1 & n_2 = m_2 &
\end{tikzcd}$$

しかし, これは無限に繰り返すことができない; $n > n_1 > n_2 > \dots$ となっているので, 無限降下法の要領で, どこかで脱出する必要がある.

つまり, ある i が存在して, $n_i = m_i$.

ところが, $\dfrac{n}{m} = \dfrac{n_1}{m_1} = \dfrac{n_2}{m_2} = \dots$ となっていたので, これは $n = m$ を導く.

■

さて, 上のふたつから, 次の補題を導くことができる.

補題 2.1: n, m, k を正整数とする. $\dfrac{\varphi^k(n)}{n} = \dfrac{\varphi^k(m)}{m}$ と $\mathrm{rad}(n) \cdot \mathrm{rad}(\varphi(n)) \cdot \dots \cdot \mathrm{rad}\big(\varphi^{k-1}(n)\big) = \mathrm{rad}(m) \cdot \mathrm{rad}(\varphi(m)) \cdot \dots \cdot \mathrm{rad}\big(\varphi^{k-1}(m)\big)$ は同値である.

Proof: $\dfrac{\varphi^k(n)}{n}$ を $\dfrac{\varphi(n)}{n}\cdot\dfrac{\varphi^2(n)}{\varphi(n)}\cdot\dfrac{\varphi^3(n)}{\varphi^2(n)}\cdot\ldots\cdot\dfrac{\varphi^k(n)}{\varphi^{k-1}(n)}$ と変形する.

さらに, 一般に正整数 x について $\dfrac{\varphi(x)}{x}=\dfrac{\varphi(\mathrm{rad}(x))}{\mathrm{rad}(x)}$ より, $\dfrac{\varphi^k(n)}{n}=\dfrac{\varphi^k(m)}{m}$ は

$$\frac{\varphi(\mathrm{rad}(n))}{\mathrm{rad}(n)}\cdot\frac{\varphi(\mathrm{rad}(\varphi(n)))}{\mathrm{rad}(\varphi(n))}\cdot\ldots\cdot\frac{\varphi\left(\mathrm{rad}\left(\varphi^{k-1}(n)\right)\right)}{\mathrm{rad}(\varphi^{k-1}(n))}=\frac{\varphi(\mathrm{rad}(m))}{\mathrm{rad}(m)}\cdot\frac{\varphi(\mathrm{rad}(\varphi(m)))}{\mathrm{rad}(\varphi(m))}\cdot\ldots\cdot\frac{\varphi\left(\mathrm{rad}\left(\varphi^{k-1}(m)\right)\right)}{\mathrm{rad}(\varphi^{k-1}(m))}$$

と同値である.

$N=\mathrm{rad}(n)\cdot\mathrm{rad}(\varphi(n))\cdot\ldots\cdot\mathrm{rad}\left(\varphi^{k-1}(n)\right), M=\mathrm{rad}(m)\cdot\mathrm{rad}(\varphi(m))\cdot\ldots\cdot\mathrm{rad}\left(\varphi^{k-1}(m)\right)$ とおくと,
正整数の根基は無平方数であることと 命題 2.1 から 上の式は $\dfrac{\varphi'(N)}{N}=\dfrac{\varphi'(M)}{M}$ に同値で,
これは 命題 2.2 から $N=M$ に同値である. ■

主定理の証明の前に, もう一つ補題を証明しておく. (この補題の位置づけは, 主定理の証明の流れを見てからのほうがわかりやすいであろう.)

補題 2.2: n,m,i を正整数, p を素数とする.

$p\mid n, p\nmid m, p\nmid\varphi^i(n), p\mid\varphi^i(m)$ が成り立つならば, ある素数 $q>p$ と $0\le j<i$ を満たす整数 j で,
$q\nmid\varphi^j(n)$ かつ $q\mid\varphi^j(m)$ を満たすものが存在する.

$\varphi(n)$ は各 $p^e\parallel n$ について $p^{e-1}(p-1)$ の積である.

つまり, φ を繰り返し適用するにつれて基本的に p の指数は 0 に達するまで 1 ずつ減っていき, それが成り立たないのは $p\mid q-1$ を満たす素数 q が因数のとき.

ここで“供給”される p のべきは q の指数によらない.

いまの設定では, 最初 $p\mid n, p\nmid m$ で m より n のほうが p を多く含んでいたにも関わらず, i 回 φ を適用したらそれが入れ替わった.

ということは, どこかで $\varphi^j(n)$ には含まれない q が $\varphi^j(m)$ に含まれており, その q が p (のべき) を m 側に供給したに違いない, というのが筆者の考えるこの補題の感覚的な説明である.

Proof: 背理法で示す.

つまり, すべての素数 $q>p$ と $0\le j<i$ を満たす j について $q\mid\varphi^j(m)$ ならば $q\mid\varphi^j(n)$ を仮定する.

このとき, すべての $0\le j\le i$ について $\nu_p(\varphi^j(n))\ge\nu_p(\varphi^j(m))$ が成り立ってしまうことを帰納法で示す.

まず, $j=0$ のときは $p\mid n, p\nmid m$ から $\nu_p(\varphi^j(n))\ge 1, \nu_p(\varphi^j(m))=0$ よりよい.

次に, $0\le j=k<i$ のとき $\nu_p\left(\varphi^k(n)\right)\ge\nu_p\left(\varphi^k(m)\right)$ を仮定しよう. (目標は, $\nu_p\left(\varphi^{k+1}(n)\right)\ge\nu_p\left(\varphi^{k+1}(m)\right)$ を示すことである.)

このとき, $$\nu_p\left(\varphi^{k+1}(n)\right)=\nu_p\left(\prod_{r^e\,\parallel\,\varphi^k(n)}r^{e-1}(r-1)\right)=\sum_{r\,\parallel\,\varphi^k(n)}\nu_p(r-1)+\begin{cases}\nu_p(\varphi^k(n))-1 & \text{if } p\mid\varphi^k(n),\\ 0 & \text{otherwise.}\end{cases}$$

(ただし r は素数を指す.)

さて, 同様の変形が $\nu_p\left(\varphi^{k+1}(m)\right)$ についてもできるので,

1. $\displaystyle\sum_{r\,\parallel\,\varphi^k(n)}\nu_p(r-1)\ge\sum_{r\,\parallel\,\varphi^k(m)}\nu_p(r-1)$
2. $\begin{cases}\nu_p(\varphi^k(n))-1 & \text{if } p\mid\varphi^k(n),\\ 0 & \text{otherwise.}\end{cases}\ge\begin{cases}\nu_p(\varphi^k(m))-1 & \text{if } p\mid\varphi^k(m),\\ 0 & \text{otherwise.}\end{cases}$

のふたつを示すことができれば, $\nu_p\left(\varphi^{k+1}(n)\right)\ge\nu_p\left(\varphi^{k+1}(m)\right)$ がそこから導かれる.

1 の証明:

両辺の和の中にある $\nu_p(r-1)$ についてだが, $r \le p$ であれば $\nu_p(r-1)=0$ であるので, $\displaystyle\sum_{r \,\|\, \varphi^k(n), r>p} \nu_p(r-1) \ge \sum_{r \,\|\, \varphi^k(m), r>p} \nu_p(r-1)$ と変形しても同じことである.

背理法の仮定より, すべての素数 $q > p$ と $0 \le j < i$ を満たす j について $q \mid \varphi^j(m) \Longrightarrow q \mid \varphi^j(n)$.

いま $0 \le k < i$ であるから, 右辺の和に入る r は左辺の和にも入る.

よって 1. が言えた.

2 の証明:

簡単のため, $\nu_p\big(\varphi^k(n)\big)=x, \nu_p\big(\varphi^k(m)\big)=y$ とおいてしまおう. (x, y は非負整数.)

すると, 2 は $\begin{cases} x-1 & \text{if } x \ge 1, \\ 0 & \text{otherwise.} \end{cases} \ge \begin{cases} y-1 & \text{if } y \ge 1, \\ 0 & \text{otherwise.} \end{cases}$ と同じことである.

いま帰納法の仮定より $\nu_p\big(\varphi^k(n)\big) \ge \nu_p\big(\varphi^k(m)\big)$ から, $x \ge y$.

よって $x \ge 1$ かつ $y = 0$, $x \ge 1$ かつ $x \ge y \ge 1$, $x = 0$ かつ $y = 0$ の 3 つの場合分けができて,

それぞれについて上の不等式が成り立つことは明らかであろう.

以上より, $\nu_p\big(\varphi^{k+1}(n)\big) \ge \nu_p\big(\varphi^{k+1}(m)\big)$ が示せたので, 帰納法よりすべての $0 \le j \le i$ について $\nu_p\big(\varphi^j(n)\big) \ge \nu_p\big(\varphi^j(m)\big)$.

特に $j = i$ の場合 $\nu_p\big(\varphi^i(n)\big) \ge \nu_p\big(\varphi^i(m)\big)$ だが, これは $p \nmid \varphi^i(n), p \mid \varphi^i(m)$ というもとの設定に矛盾.

したがって背理法より, ある素数 $q > p$ と $0 \le j < i$ を満たす整数 j で, $q \nmid \varphi^j(n)$ かつ $q \mid \varphi^j(m)$ を満たすものが存在する. ■

定理 2.1: n, m, k を正整数とする. $\dfrac{\varphi^k(n)}{n} = \dfrac{\varphi^k(m)}{m} \Longrightarrow \mathrm{rad}(n) = \mathrm{rad}(m)$.

Proof: 補題 2.1 より,

$$\mathrm{rad}(n) \cdot \mathrm{rad}(\varphi(n)) \cdot \ldots \cdot \mathrm{rad}\big(\varphi^{k-1}(n)\big) = \mathrm{rad}(m) \cdot \mathrm{rad}(\varphi(m)) \cdot \ldots \cdot \mathrm{rad}\big(\varphi^{k-1}(m)\big) \quad \ldots(*)$$

が $\mathrm{rad}(n) = \mathrm{rad}(m)$ を導くことができればよい.

いま, $k = 1$ の場合は明らかなので $k > 1$ の場合を考える.

背理法で示す; つまり, $\mathrm{rad}(n) \ne \mathrm{rad}(m)$ と補題の式を仮定して, 矛盾を示す.

一般に任意の素数 p と 正整数 x について $p \mid x \Longleftrightarrow p \mid \mathrm{rad}(x)$ に注意すると, $p \mid n \not\Leftrightarrow p \mid m$.

つまり, 一方の素因子ではなく, もう一方の素因子であるような素数 p_1 が存在する.

今回条件は n と m について対称なので, 適切に入れ替えて $p_1 \mid n$ かつ $p_1 \nmid m$ としよう.

ここで, 式 $(*)$ において, 根基が無平方数であることから, 任意の素数 p について, $0 \le i < k$ の範囲で $p \mid \varphi^i(n)$ を満たす i の個数と, $p \mid \varphi^i(m)$ を満たす i の個数は一致していなければならない.

いま $p_1 \mid n$ かつ $p_1 \nmid m$ より, ある $0 < i_1 < k$ の範囲の i_1 で $p_1 \nmid \varphi^{i_1}(n)$ かつ $p_1 \mid \varphi^{i_1}(m)$ を満たすものが存在する.

補題 2.2 より, ある素数 $p_2 > p_1$ と $0 \le i_2 < i_1$ を満たす整数 i_2 で, $p_2 \nmid \varphi^{i_2}(n)$ かつ $p_2 \mid \varphi^{i_2}(m)$ を満たすものが存在する.

さて, さらに式 $(*)$ において, 両辺に含まれる p_2 の個数を比較することにより, ある $0 \leq i_2' < k, i_2' \neq i_2$ を満たす i_2' で $p_2 \mid \varphi^{i_2'}(n)$ かつ $p_2 \nmid \varphi^{i_2'}(m)$ を満たすものが存在する.

ここで i_2 と i_2', n と m を同時に適切に入れ替えて, $i_2' < i_2, p_2 \mid \varphi^{i_2'}(n), p_2 \nmid \varphi^{i_2'}(m), p_2 \nmid \varphi^{i_2}(n), p_2 \mid \varphi^{i_2}(m)$ が成り立つようにする.

(こうしたことで, 最初の $p_1 \mid n$ などはもう成り立つかわからなくなるが, これから使用するのは n, m に対して対称な式 $(*)$ と上に述べた条件のみであるから問題ない.)

さて, 補題 2.2 の n, m, i, p を $\varphi^{i_2'}(n), \varphi^{i_2'}(m), i_2 - i_2', p_2$ でそれぞれ置き換えて再度適用すると, ある素数 $p_3 > p_2$ と $i_2' \leq i_3 < i_2$ を満たす整数 i_3 で, $p_3 \nmid \varphi^{i_3}(n)$ かつ $p_3 \mid \varphi^{i_3}(m)$ を満たすものが存在することがわかる.

この議論は無限に繰り返すことができ, $\mathrm{rad}(n) \cdot \mathrm{rad}(\varphi(n)) \cdot ... \cdot \mathrm{rad}\left(\varphi^{k-1}(n)\right)$ の任意に大きな素因数を構成できてしまう.

これは矛盾なので, 背理法より, $\mathrm{rad}(n) = \mathrm{rad}(m)$. ■

3. 強い条件

さて, $\dfrac{\varphi^k(n)}{n} = \dfrac{\varphi^k(m)}{m} \Longrightarrow \mathrm{rad}(n) = \mathrm{rad}(m)$ が先の定理の結論であったが, $k > 1$ の場合, 逆は必ずしも成り立たない.

つまり, $\mathrm{rad}(n) = \mathrm{rad}(m)$ は弱い条件である.

より強い条件についても考察することができる:

いま, 正整数 n, i について $\nu_p(n) = i$ を満たす素数 p 全体の集合を $S_i(n)$, $\nu_p(n) \geq i$ を満たす素数 p 全体の集合を $S_{\geq i}(n)$ とおく.

定理 3.1: n, m, k を正整数とする.

すべての $0 \leq i < k$ の範囲の整数 i について $S_i(n) = S_i(m)$ が成り立ち, かつ $S_{\geq k}(n) = S_{\geq k}(m)$ ならば $\dfrac{\varphi^k(n)}{n} = \dfrac{\varphi^k(m)}{m}$.

Proof: 条件 "すべての $0 \leq i < l$ の範囲の整数 i について $S_i(n) = S_i(m)$ が成り立ち, かつ $S_{\geq l}(n) = S_{\geq l}(m)$" を $n \underset{l}{\sim} m$ と書くことにする.

今, $n \underset{l+1}{\sim} m$ は $n \underset{l}{\sim} m$ より強い. $n \underset{l+1}{\sim} m$ を仮定すると, $0 \leq i < l$ の範囲の整数 i について $S_i(n) = S_i(m)$ が直接言えることはもちろん, $S_{\geq l}(n) = S_l(n) \cup S_{\geq l+1}(n) = S_l(m) \cup S_{\geq l+1}(m) = S_{\geq l}(m)$ も言えるからである.

ここから帰納法の要領で, $n \underset{l}{\sim} m$ が成り立つなら $n \underset{l-1}{\sim} m, n \underset{l-2}{\sim} m, ..., n \underset{1}{\sim} m$ も成り立つ.

さて, 定理の証明に戻ると, 補題 2.1 より, $n \underset{k}{\sim} m$ を仮定して

$$\mathrm{rad}(n) \cdot \mathrm{rad}(\varphi(n)) \cdot ... \cdot \mathrm{rad}\left(\varphi^{k-1}(n)\right) = \mathrm{rad}(m) \cdot \mathrm{rad}(\varphi(m)) \cdot ... \cdot \mathrm{rad}\left(\varphi^{k-1}(m)\right) \quad ...(*)$$

を示せばよい.

これは命題 "任意の正整数 n, m, l について $n \underset{l}{\sim} m$ ならば $\mathrm{rad}\left(\varphi^{l-1}(n)\right) = \mathrm{rad}\left(\varphi^{l-1}(n)\right)$" (命題 A と呼ぶことにする) がいえれば十分である.

なぜなら命題 A が成り立てば, $n \underset{k}{\sim} m$ の仮定から $n \underset{k-1}{\sim} m, n \underset{k-2}{\sim} m, ..., n \underset{1}{\sim} m$ と合わせて $\mathrm{rad}(n) = \mathrm{rad}(m), \mathrm{rad}(\varphi(n)) = \mathrm{rad}(\varphi(m)), ..., \mathrm{rad}\big(\varphi^{k-1}(n)\big) = \mathrm{rad}\big(\varphi^{k-1}(m)\big)$ から式 $(*)$ が示せるからである.

よって命題 A を示す.

しかし, 命題 A を示すには命題 "任意の正整数 n, m, l $(l > 1)$ について $n \underset{l}{\sim} m$ ならば $\varphi(n) \underset{l-1}{\sim} \varphi(m)$" (命題 B と呼ぶことにする) がいえれば十分である.

なぜなら命題 B が成り立てば, $n \underset{k}{\sim} m$ の仮定から $\varphi(n) \underset{k-1}{\sim} \varphi(m), \varphi^2(n) \underset{k-2}{\sim} \varphi^2(m), ...$ と順に示していって $\varphi^{k-1}(n) \underset{1}{\sim} \varphi^{k-1}(m)$ が言えるが, 一般に $x \underset{1}{\sim} y$ は $\mathrm{rad}(x) = \mathrm{rad}(y)$ と同値だからである.

よって命題 B を示す.

条件 $n \underset{l}{\sim} m$ や $\varphi(n) \underset{l-1}{\sim} \varphi(m)$ は n, m について対称であるから, すべての $0 \leq i < l-1$ の範囲の整数 i に対して $S_i(\varphi(n)) \subset S_i(\varphi(m))$ かつ $S_{\geq l-1}(\varphi(n)) \subset S_{\geq l-1}(\varphi(m))$ が言えれば十分.

さて, これは任意の素数 p について $\nu_p(\varphi(n)) < l-1$ なら $\nu_p(\varphi(n)) = \nu_p(\varphi(m))$ で, $\nu_p(\varphi(n)) \geq l-1$ なら $\nu_p(\varphi(m)) \geq l-1$ を示せばよい.

$\nu_p(\varphi(n)) < l-1 \Longrightarrow \nu_p(\varphi(n)) = \nu_p(\varphi(m))$ の証明:

さて, $\varphi(n) = \displaystyle\prod_{q^e \,\|\, n} q^{e-1}(q-1)$ より, $\nu_p(\varphi(n)) = \displaystyle\sum_{q \mid n} \nu_p(q-1) + \begin{cases} \nu_p(n) - 1 & \text{if } p \mid n, \\ 0 & \text{otherwise.} \end{cases}$

いま $l > 1$ より $n \underset{1}{\sim} m$ から $S_{\geq 1}(n) = S_{\geq 1}(m)$ から, $q \mid n$ を満たす素数 q の集合と $q \mid m$ を満たす素数 q の集合は等しい, よって $\displaystyle\sum_{q \mid n} \nu_p(q-1) = \sum_{q \mid m} \nu_p(q-1)$.

よって $\begin{cases} \nu_p(n) - 1 & \text{if } p \mid n, \\ 0 & \text{otherwise.} \end{cases} = \begin{cases} \nu_p(m) - 1 & \text{if } p \mid m, \\ 0 & \text{otherwise.} \end{cases}$ がいえれば $\nu_p(\varphi(n)) = \nu_p(\varphi(m))$ がいえる.

ところが $\begin{cases} \nu_p(n) - 1 & \text{if } p \mid n, \\ 0 & \text{otherwise.} \end{cases} \leq \nu_p(\varphi(n)) < l-1$ より $\nu_p(n) < l$.

いま $n \underset{l}{\sim} m$ より, $\nu_p(n) = \nu_p(m)$ から $\nu_p(\varphi(n)) = \nu_p(\varphi(m))$.

$\nu_p(\varphi(n)) \geq l-1 \Longrightarrow \nu_p(\varphi(m)) \geq l-1$ の証明:

先ほどと同様の議論から, $\displaystyle\sum_{q \mid n} \nu_p(q-1) = \sum_{q \mid m} \nu_p(q-1) = Q$ とおくことにする.

すると, $\begin{cases} \nu_p(n) - 1 & \text{if } p \mid n, \\ 0 & \text{otherwise.} \end{cases} \geq l - Q - 1 \Longrightarrow \begin{cases} \nu_p(m) - 1 & \text{if } p \mid m, \\ 0 & \text{otherwise.} \end{cases} \geq l - Q - 1$ を示す問題に帰着される.

だが, いま $n \underset{l}{\sim} m$ より $\nu_p(n) < l \Longrightarrow \nu_p(m) < l$ は保証されているので, 考えるべきは $\nu_p(n) \geq l$ の場合である.

しかしこのとき $\nu_p(m) \geq l$ が $n \underset{l}{\sim} m$ より従うので, $\begin{cases} \nu_p(m) - 1 & \text{if } p \mid m, \\ 0 & \text{otherwise.} \end{cases} = \nu_p(m) - 1 \geq l - 1$.

$Q \geq 0$ より, この式が $l - Q - 1$ 以上であることは明らかであろう.

■