φ^k 同値について

梶田光

2025/09/18

1. はじめに

以前, $n \underset{\varphi}{\sim} m \iff \dfrac{\varphi(n)}{n} = \dfrac{\varphi(m)}{m}$ 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, $n \underset{\varphi}{\sim} m \iff \mathrm{rad}(n) = \mathrm{rad}(m)$ がわかった.

ただし, rad は根基を指す; つまり, $\mathrm{rad}(n) = \displaystyle\prod_{p \mid n} p$.

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.

以下は, 整数論でよく使われる記号である.

> **定義 1.1**: 正整数 n と素数 p に対し, $p^e \mid n$ を満たす非負整数 e のうち最大のものを $\nu_p(n)$ と書き, n の p 進付値と呼ぶ.

p を固定すれば, $\nu_p(n)$ は完全加法的関数である; つまり, 任意の (互いに素とは限らない) 正整数 a, b について, $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

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, その証明のために補助関数とその性質を用意する.

3. 重複オイラー関数とその性質

> **定義 3.1**: 正整数 n に対し, 関数 φ' を $\varphi'(n) = n \displaystyle\prod_{p^e \parallel n} \left(1 - \frac{1}{p}\right)^e$ で定義し, 重複オイラー関数と呼ぶ.
>
> そして, $\dfrac{\varphi'(n)}{n} = \dfrac{\varphi'(m)}{m}$ が成り立つことを $n \underset{\varphi'}{\sim} m$ と書く.

なお, 記号 $p^e \parallel n$ は n が p^e をちょうど割り切る, つまり e は $p^e \mid n$ を満たす最大の非負整数であることを表す.

例えば, $n = 2^3 \cdot 5^6 \cdot 11^7$ のとき, $\varphi'(n) = n \cdot \left(1 - \dfrac{1}{2}\right)^3 \cdot \left(1 - \dfrac{1}{5}\right)^6 \cdot \left(1 - \dfrac{1}{11}\right)^7$ となる.

さて, $\varphi'(n) = \displaystyle\prod_{p^e \parallel n} (p-1)^e$ とも書ける

したがって, 任意の正整数 a, b に対して, $\varphi'(ab) = \prod_{p \mid ab} (p-1)^{\nu_p(ab)} = \prod_{p \mid ab} (p-1)^{\nu_p(a)+\nu_p(b)}$ より, $\varphi'(ab) = \varphi'(a)\varphi'(b)$ が成り立つ.
オイラー関数とは異なり, これは a, b が互いに素とは限らなくとも成り立つ.
このことを, φ' は完全乗法的であるという.

命題 3.1: 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,
$A = \prod_{i=1}^{I} \alpha_i$ とおくと, $\prod_{i=1}^{I} \frac{\varphi(\alpha_i)}{\alpha_i} = \frac{\varphi'(A)}{A}$ が成り立つ.

Proof: 任意の無平方数 α について, φ' の定義より $\varphi'(\alpha) = \varphi(\alpha)$ である.
というのも, α の素因数分解の指数は必ず 1 であるからである.
すると証明すべき式は $\prod_{i=1}^{I} \frac{\varphi'(\alpha_i)}{\alpha_i} = \frac{\varphi'(A)}{A}$ となるが, これは重複オイラー関数の完全乗法性から成り立つことがわかる. ■

定義 3.2: $\lambda(n) = \gcd(\varphi'(n), n), \lambda'(n) = \frac{n}{\lambda(n)}$ と定義する.
そして, 非負整数 k について, $\lambda^k(n) = \begin{cases} n & \text{if } k = 0 \\ \lambda(\lambda^{k-1}(n)) & \text{otherwise} \end{cases}$ と定義する.

補題 3.1: $n \underset{\varphi'}{\sim} m$ が成り立つならば, $\lambda'(n) = \lambda'(m)$ かつ $\lambda(n) \underset{\varphi'}{\sim} \lambda(m)$.

Proof: $\gcd\left(\lambda'(n), \frac{\varphi'(n)}{\lambda(n)}\right) = \gcd\left(\frac{n}{\lambda(n)}, \frac{\varphi'(n)}{\lambda(n)}\right) = 1.$
したがって, $\frac{\varphi'(n)}{n} = \frac{\frac{\varphi'(n)}{\lambda(n)}}{\frac{n}{\lambda(n)}} = \frac{\frac{\varphi'(n)}{\lambda(n)}}{\lambda'(n)}$ は既約分数形で, これは $\frac{\varphi'(m)}{m}$ に等しい.
よって, 既約分数の一意性から, ある整数 k が存在して $m = k\lambda'(n), \varphi'(m) = k\frac{\varphi'(n)}{\lambda(n)}$ と書ける.
ここで, $\lambda(m) = \gcd(m, \varphi'(m)) = \gcd\left(k\lambda'(n), k\frac{\varphi'(n)}{\lambda(n)}\right) = k\gcd\left(\lambda'(n), \frac{\varphi'(n)}{\lambda(n)}\right) = k.$
$m = k\lambda'(n)$ と $m = \lambda(m)\lambda'(m) = k\lambda'(m)$ を比較すれば, $\lambda'(n) = \lambda'(m)$ を得る.
さて, φ' は完全乗法的関数であるから, $\frac{\varphi'(m)}{m} = \frac{\varphi'(\lambda(m)\lambda'(m))}{\lambda(m)\lambda'(m)} = \frac{\varphi'(\lambda(m))}{\lambda(m)} \cdot \frac{\varphi'(\lambda'(m))}{\lambda'(m)}.$
一方, $\frac{\varphi'(n)}{n} = \frac{\varphi'(\lambda(n)\lambda'(n))}{\lambda(n)\lambda'(n)} = \frac{\varphi'(\lambda(n))}{\lambda(n)} \cdot \frac{\varphi'(\lambda'(n))}{\lambda'(n)}.$
$n \underset{\varphi'}{\sim} m$ と $\lambda'(n) = \lambda'(m)$ を利用すれば, $\frac{\varphi'(\lambda(n))}{\lambda(n)} = \frac{\varphi'(\lambda(m))}{\lambda(m)}$, つまり $\lambda(n) \underset{\varphi'}{\sim} \lambda(m)$ が得られる. ■

命題 3.2: 任意の正整数 n, m に対し, $n \underset{\varphi'}{\sim} m \iff n = m.$

Proof: $\varphi'(n)$ は定義より, $n > 1$ のとき $\varphi'(n) < n$ を満たす.

よって, $n>1$ のとき $\lambda(n)<n$ であるから, $\lambda^i(n)=1$ を満たす正整数 i が存在する.

さて, ここで先の補題が繰り返し適用できることに着目する.

つまり, まず $n \underset{\varphi'}{\sim} m$ を 補題 3.1 に適用すると, $\lambda(n) \underset{\varphi'}{\sim} \lambda(m)$ が得られ, これをさらに 補題 3.1 に適用すると $\lambda^2(n) \underset{\varphi'}{\sim} \lambda^2(m)$ が得られる.

これを繰り返すことで, 任意の非負整数 j について $\lambda^j(n) \underset{\varphi'}{\sim} \lambda^j(m)$ ...(I) が言える.

さて, $\lambda^j(n) \underset{\varphi'}{\sim} \lambda^j(m)$ に 補題 3.1 を適用すれば, 任意の非負整数 j について $\lambda'(\lambda^j(n)) = \lambda'(\lambda^j(m))$ ...(II) が言える.

ここで $j=i$ の場合について考える.

式(I) に $j=i$ を代入して $\lambda^i(n) \underset{\varphi'}{\sim} \lambda^i(m)$ を得るが, $\lambda^i(n)=1$ から $\dfrac{\varphi'(\lambda^i(m))}{\lambda^i(m)} = \dfrac{\varphi'(1)}{1} = 1.$

しかし, $\varphi'(n)$ の定義より一般の n について $n>1$ ならば $\varphi'(n)<n$ であるから, $\lambda^i(m)=1$ が得られる.

よって, $\lambda^i(n)=\lambda^i(m)$.

さて, $\lambda^{i-1}(n)=\lambda(\lambda^{i-1}(n))\lambda'(\lambda^{i-1}(n))=\lambda^i(n)\lambda'(\lambda^{i-1}(n))$ で, いま式(II) より $\lambda'(\lambda^{i-1}(n)) = \lambda'(\lambda^{i-1}(m))$ も成り立つので, $\lambda^{i-1}(n)=\lambda^{i-1}(m)$.

さらに, $\lambda^{i-2}(n)=\lambda(\lambda^{i-2}(n))\lambda'(\lambda^{i-2}(n))=\lambda^{i-1}(n)\lambda'(\lambda^{i-2}(n))$ で, いま式(II) より $\lambda'(\lambda^{i-2}(n)) = \lambda'(\lambda^{i-2}(m))$ も成り立つので, $\lambda^{i-2}(n)=\lambda^{i-2}(m)$.

これを繰り返すことにより, $n=m$ を得ることができる.

式(I) 式(II)

$$
\begin{array}{ccccc}
n \underset{\varphi'}{\sim} m & \Longrightarrow & \lambda'(n)=\lambda'(m) & \Longrightarrow & n=m \\
\Downarrow & & & & \Uparrow \\
\lambda(n) \underset{\varphi'}{\sim} \lambda(m) & \Longrightarrow & \lambda'(\lambda(n))=\lambda'(\lambda(m)) & \Longrightarrow & \lambda(n)=\lambda(m) \\
\Downarrow & & & & \Uparrow \\
\lambda^2(n) \underset{\varphi'}{\sim} \lambda^2(m) & \Longrightarrow & \lambda'(\lambda^2(n))=\lambda'(\lambda^2(m)) & \Longrightarrow & \lambda^2(n)=\lambda^2(m) \\
\Downarrow & & & & \Uparrow \\
\vdots & & \vdots & & \vdots \\
\Downarrow & & & & \Uparrow \\
\lambda^{i-1}(n) \underset{\varphi'}{\sim} \lambda^{i-1}(m) & \Longrightarrow & \lambda'(\lambda^{i-1}(n))=\lambda'(\lambda^{i-1}(m)) & \Longrightarrow & \lambda^{i-1}(n)=\lambda^{i-1}(m) \\
\Downarrow & & & & \Uparrow \\
\lambda^i(n) \underset{\varphi'}{\sim} \lambda^i(m) & & \Longrightarrow & & \lambda^i(n)=\lambda^i(m)
\end{array}
$$

■

さて, 上のふたつから, 次の補題を導くことができる.

補題 3.2: n, m, k を正整数とする. $\dfrac{\varphi^k(n)}{n} = \dfrac{\varphi^k(m)}{m}$ と
$\mathrm{rad}(n) \cdot \mathrm{rad}(\varphi(n)) \cdot \ldots \cdot \mathrm{rad}\big(\varphi^{k-1}(n)\big) = \mathrm{rad}(m) \cdot \mathrm{rad}(\varphi(m)) \cdot \ldots \cdot \mathrm{rad}\big(\varphi^{k-1}(m)\big)$ 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

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

と同値である.

$N = \mathrm{rad}(n) \cdot \mathrm{rad}(\varphi(n)) \cdot \ldots \cdot \mathrm{rad}\big(\varphi^{k-1}(n)\big), M = \mathrm{rad}(m) \cdot \mathrm{rad}(\varphi(m)) \cdot \ldots \cdot \mathrm{rad}\big(\varphi^{k-1}(m)\big)$ とおくと,
正整数の根基は無平方数であることと 命題 3.1 から 上の式は $\dfrac{\varphi'(N)}{N} = \dfrac{\varphi'(M)}{M}$ に同値で,
これは 命題 3.2 から $N = M$ に同値である. ■

さて, $N = M$ は $n \underset{\varphi^k}{\sim} m$ よりは扱いやすいが, 証明にはまだ補題が必要である.

補題 3.3: p を素数, n を正整数とする.
$$\nu_p(\varphi(n)) = \max\big(0, \nu_p(n) - 1\big) + \sum_{q > p, q \mid n} \nu_p(q-1).$$

Proof: $\nu_p(\varphi(n)) = \nu_p\left(\prod_{q^e \parallel n} q^{e-1}(q-1)\right)$.

(1) $p \mid n$ の場合

$$\nu_p(\varphi(n)) = \nu_p\left(p^{\nu_p(n)-1}(p-1) \cdot \prod_{q^e \parallel n, q \neq p} q^{e-1}(q-1)\right) = \nu_p(n) - 1 + \nu_p\left(\prod_{q^e \parallel n, q \neq p} q^{e-1}(q-1)\right).$$

$p \mid n$ から $\nu_p(n) \geq 1$ なので, $\nu_p(n) - 1 = \max\big(0, \nu_p(n) - 1\big)$.

したがって $\nu_p\left(\prod_{q^e \parallel n, q \neq p} q^{e-1}(q-1)\right) = \sum_{q > p, q \mid n} \nu_p(q-1)$ が言えれば十分.

(2) $p \nmid n$ の場合

$$\nu_p(\varphi(n)) = \nu_p\left(\prod_{q^e \parallel n} q^{e-1}(q-1)\right) = \nu_p\left(\prod_{q^e \parallel n, q \neq p} q^{e-1}(q-1)\right).$$

$p \nmid n$ から $\nu_p(n) = 0$ なので, $\max\big(0, \nu_p(n) - 1\big) = 0$.

したがってこの場合も $\nu_p\left(\prod_{q^e \parallel n, q \neq p} q^{e-1}(q-1)\right) = \sum_{q > p, q \mid n} \nu_p(q-1)$ が言えれば十分.

よって $\nu_p\left(\prod_{q^e \parallel n, q \neq p} q^{e-1}(q-1)\right) = \sum_{q > p, q \mid n} \nu_p(q-1)$ を示す.

まず, q が p ではない素数なので, q^e は p の倍数にはならない.

したがって, $\nu_p\left(\prod_{q^e \parallel n, q\neq p} q^{e-1}(q-1)\right) = \nu_p\left(\prod_{q^e \parallel n, q\neq p} (q-1)\right)$ で, ν_p の完全加法性からこれは $\sum_{q^e \parallel n, q\neq p} \nu_p(q-1)$ に等しい.

さて, e はもう使わないので条件 $q^e \parallel n$ は $q \mid n$ と書き換えてよく, 上の式は $\sum_{q \mid n, q\neq p} \nu_p(q-1)$ となる.

ここで, $q < p$ であれば, $\nu_p(q-1)$ は 0 であるから, この総和は $q > p$ の場合だけとってもよい.

つまり, これは $\sum_{q \mid n, q>p} \nu_p(q-1)$ に等しい. ■

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 3.4: 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 $0 \leq j < i$ 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 $0 \leq j < i$ 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 $0 \leq j \leq i$ について $\nu_p(\varphi^j(n)) \geq \nu_p(\varphi^j(m))$ 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 $\nu_p(\varphi^j(n)) \geq 1, \nu_p(\varphi^j(m)) = 0$ よりよい.

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

このとき, 補題 3.3 より $\nu_p\big(\varphi^{k+1}(n)\big) = \max\big(0, \nu_p\big(\varphi^k(n)\big) - 1\big) + \sum_{r>p, r \mid \varphi^k(n)} \nu_p(r-1)$.

(ただし r は素数を指す.)

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

1. $\max\big(0, \nu_p\big(\varphi^k(n)\big) - 1\big) \geq \max\big(0, \nu_p\big(\varphi^k(m)\big) - 1\big)$
2. $\sum_{r>p, r \mid \varphi^k(n)} \nu_p(r-1) \geq \sum_{r>p, r \mid \varphi^k(m)} \nu_p(r-1)$

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

1 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 $\max(0, x-1) \geq \max(0, y-1)$ と同じことである.

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

よって $x \geq 1$ かつ $y = 0$, $x \geq 1$ かつ $x \geq y \geq 1$, $x = 0$ 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簡単な計算と考察によって確かめられる.

2 の証明:

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

したがって, $r > p$ を満たす $\varphi^k(n)$ の素因数の集合は $r > p$ を満たす $\varphi^k(m)$ の素因数の集合の superset である.

よって, $\displaystyle\sum_{r>p, r \mid \varphi^k(n)} \nu_p(r-1) \geq \sum_{r>p, r \mid \varphi^k(m)} \nu_p(r-1)$.

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

特に $j = i$ の場合 $\nu_p(\varphi^i(n)) \geq \nu_p(\varphi^i(m))$ 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 $0 \leq j < i$ 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 3.1: 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 3.2 より,

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

から $\mathrm{rad}(n) = \mathrm{rad}(m)$ 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, $\mathrm{rad}(n) \neq \mathrm{rad}(m)$ と補題の式を仮定して, 矛盾を示す.

ここで, 命題「任意の素数 p と $i < k$ を満たす非負整数 i について, $(p \mid \varphi^i(n)) \veebar (p \mid \varphi^i(m))$ ならば, ある p より大きい素数 q と $i' < k$ を満たす非負整数 i' で, $\big(q \mid \varphi^{i'}(n)\big) \veebar \big(q \mid \varphi^{i'}(m)\big)$ を満たすものが存在する」(命題 A と呼ぶことにする)を証明する.

なお, $\veebar$ は排他的論理和を表す; つまり, $p \veebar q \longleftrightarrow (p \wedge \neg q) \vee (\neg p \wedge q)$.

Proof: 排他的論理和は交換するので, 一般性を失わずに $p \mid \varphi^i(n), p \nmid \varphi^i(m)$ を仮定できる.

式 $(*)$ の両辺の ν_p をとると, $\displaystyle\sum_{x=0}^{k-1} \nu_p(\mathrm{rad}(\varphi^x(n))) = \sum_{x=0}^{k-1} \nu_p(\mathrm{rad}(\varphi^x(m)))$ を得る.

しかし, $p \mid \varphi^i(n)$ より $\nu_p(\mathrm{rad}(\varphi^i(n))) = 1$, $p \nmid \varphi^i(m)$ より $\nu_p(\mathrm{rad}(\varphi^i(m))) = 0$.

したがって, $\nu_p(\mathrm{rad}(\varphi^i(n))) > \nu_p(\mathrm{rad}(\varphi^i(m)))$ であるから, $\displaystyle\sum_{0 \leq x < k, x \neq i} \nu_p(\mathrm{rad}(\varphi^x(n))) < \sum_{0 \leq x < k, x \neq i} \nu_p(\mathrm{rad}(\varphi^x(m)))$ が成り立つ.

よって, ある k 未満の i と等しくない非負整数 j で, $\nu_p(\mathrm{rad}(\varphi^j(n))) < \nu_p(\mathrm{rad}(\varphi^j(m)))$ を満たすものが存在する.

しかし, 一般の n について $\mathrm{rad}(n)$ は無平方数であることから, $\nu_p(\mathrm{rad}(n)) = \begin{cases} 0 & \text{if } p \nmid n, \\ 1 & \text{if } p \mid n. \end{cases}$

よって, $p \nmid \varphi^j(n), p \mid \varphi^j(m)$.

ここで $i \neq j$ より $i < j$ もしくは $j < i$ のどちらかが成り立つ.

(1) $i < j$ の場合

$p \nmid \varphi^j(n), p \mid \varphi^j(m)$ を $p \nmid \varphi^{j-i}(\varphi^i(n)), p \mid \varphi^{j-i}(\varphi^i(m))$ と書けば,
補題 3.4 に $n \leftarrow \varphi^i(n), m \leftarrow \varphi^i(m), i \leftarrow j-i$ として代入することで,
ある素数 $q > p$ と $0 \leq i' < j-i$ を満たす整数 i' で, $q \nmid \varphi^{i'}(\varphi^i(n))$ かつ $q \mid \varphi^{i'}(\varphi^i(m))$ を満たすものが存在することがわかる.

i' を $i' + i$ と置き直せば, $i' < j < k$ かつ $q \nmid \varphi^{i'}(n), q \mid \varphi^{i'}(m)$ が成り立つので, $\left(q \mid \varphi^{i'}(n)\right) \veebar \left(q \mid \varphi^{i'}(m)\right)$ が成り立つ例が構成できた.

(2) $j < i$ の場合

この場合も 補題 3.4 に代入する順番を変えるだけで, ほぼ同じ議論である.

$p \mid \varphi^i(n), p \nmid \varphi^i(m)$ を $p \nmid \varphi^{i-j}(\varphi^j(m)), p \mid \varphi^{i-j}(\varphi^i(n))$ と書けば,
補題 3.4 に $n \leftarrow \varphi^j(m), m \leftarrow \varphi^j(n), i \leftarrow i-j$ として代入することで,
ある素数 $q > p$ と $0 \leq i' < i-j$ を満たす整数 i' で, $q \nmid \varphi^{i'}(\varphi^j(m))$ かつ $q \mid \varphi^{i'}(\varphi^j(n))$ を満たすものが存在することがわかる.

i' を $i' + j$ と置き直せば, $i' < i < k$ かつ $q \mid \varphi^{i'}(n), q \nmid \varphi^{i'}(m)$ が成り立つので, この場合も $\left(q \mid \varphi^{i'}(n)\right) \veebar \left(q \mid \varphi^{i'}(m)\right)$ が成り立つ例が構成できた.

■

さて, 命題 A を用いると, 命題「任意の素数 p と $i < k$ を満たす非負整数 i と正整数 X について, $(p \mid \varphi^i(n)) \veebar (p \mid \varphi^i(m))$ ならば, ある X より大きい素数 q と, $i' < k$ を満たす非負整数 i' で, $\left(q \mid \varphi^{i'}(n)\right) \veebar \left(q \mid \varphi^{i'}(m)\right)$ を満たすものが存在する」(命題 B と呼ぶ) を示すことができる.

Proof: X に対する帰納法で示す.

$X = 1$ の場合は, 素数は 1 より大きいので命題 A から直接従う.

X のとき命題 B が成り立つと仮定すると, 帰納法の仮定から X より大きい素数 q_0 と, $i'_0 < k$ を満たす非負整数 i'_0 で, $\left(q_0 \mid \varphi^{i'}(n)\right) \veebar \left(q_0 \mid \varphi^{i'}(m)\right)$ を満たすものが存在する.

命題 A に $p \leftarrow q_0, i \leftarrow i'_0$ を代入すれば, q_0 より大きい素数 q と, $i' < k$ を満たす非負整数 i' で, $\left(q \mid \varphi^{i'}(n)\right) \veebar \left(q \mid \varphi^{i'}(m)\right)$ を満たすものが存在する.

この q は, $X < q_0 < q$ より, $X + 1 < q$ を満たし, したがって $X + 1$ のときも命題 B が成り立つ. ■

さて, この命題 B は適用できてはならない.

もしある素数 p と $i < k$ を満たす非負整数 i について, $(p \mid \varphi^i(n)) \veebar (p \mid \varphi^i(m))$ が成り立つならば, X にはどんな巨大な数も当てはめられるからである.

例えば, $\left(q \mid \varphi^{i'}(n)\right) \veebar \left(q \mid \varphi^{i'}(m)\right)$ は $q \mid \prod_{x=0}^{k-1} \{\varphi^x(n)\varphi^x(m)\}$ を導くので, $X = \prod_{x=0}^{k-1} \{\varphi^x(n)\varphi^x(m)\}$ とすれば q が X より大きいというのは矛盾だからである.

したがって, すべての素数 p と $i < k$ を満たす非負整数 i について, $p \mid \varphi^i(n) \longleftrightarrow p \mid \varphi^i(m)$ が成り立っていなければならない.

特に $i = 0$ とすれば $p \mid n \longleftrightarrow p \mid m$ から, n と m の素因数は等しく, したがって $\mathrm{rad}(n) = \mathrm{rad}(m)$ である.

4. 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.

定義 4.1: n, m, k を正整数とする.

すべての $1 \leq i < k$ の範囲の整数 i について $S_i(n) = S_i(m)$ が成り立ち, かつ $S_{\geq k}(n) = S_{\geq k}(m)$ であることを $n \underset{k}{\sim} m$ と書き, n と m は k 同値であるという.

補題 4.1: $n \underset{k}{\sim} m$ ならば, すべての $1 \leq k' < k$ の範囲の整数 k' について $n \underset{k'}{\sim} m$.

Proof: 任意の 1 より大きい整数 k について $n \underset{k}{\sim} m \longrightarrow n \underset{k-1}{\sim} m$ が言えれば十分なので, 以下これを示す.

$n \underset{k}{\sim} m$ を仮定すれば, $n \underset{k-1}{\sim} m$ の定義の前の部分「すべての $1 \leq i < k-1$ の範囲の整数 i について $S_i(n) = S_i(m)$」は明らかであろう.

一方, $S_{\geq k-1}(n) = S_{k-1}(n) \cup S_{\geq k}(n)$ より, $n \underset{k}{\sim} m$ を仮定すれば $S_{\geq k-1}(n) = S_{\geq k-1}(m)$ も成り立つ. ■

定理 4.1: n, m, k を正整数とする. $n \underset{k}{\sim} m$ ならば $n \underset{\varphi^k}{\sim} m$.

Proof: 補題 3.2 より, $n \underset{k}{\sim} m \longrightarrow \mathrm{rad}(n) \cdot \mathrm{rad}(\varphi(n)) \cdot \ldots \cdot \mathrm{rad}\big(\varphi^{k-1}(n)\big) = \mathrm{rad}(m) \cdot \mathrm{rad}(\varphi(m)) \cdot \ldots \cdot \mathrm{rad}\big(\varphi^{k-1}(m)\big)$ を示せばよい.

これは命題「任意の正整数 n, m, k について $n \underset{k}{\sim} m$ ならば $\mathrm{rad}\big(\varphi^{k-1}(n)\big) = \mathrm{rad}\big(\varphi^{k-1}(m)\big)$」(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, 補題 4.1 より, $n \underset{k-1}{\sim} m, n \underset{k-2}{\sim} m, \ldots, n \underset{1}{\sim} m$ と合わせて $\mathrm{rad}(n) = \mathrm{rad}(m), \mathrm{rad}(\varphi(n)) = \mathrm{rad}(\varphi(m)), \ldots, \mathrm{rad}\big(\varphi^{k-1}(n)\big) = \mathrm{rad}\big(\varphi^{k-1}(m)\big)$ が成り立つからである.

そして, 命題 A を示すには, 命題「任意の正整数 n, m, k $(k > 1)$ について $n \underset{k}{\sim} m$ ならば $\varphi(n) \underset{k-1}{\sim} \varphi(m)$」(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 $\varphi(n) \underset{k-1}{\sim} \varphi(m), \varphi^2(n) \underset{k-2}{\sim} \varphi^2(m), \ldots$ と順に示していって $\varphi^{k-1}(n) \underset{1}{\sim} \varphi^{k-1}(m)$ までが言えるが, 一般に $x \geq 1$ について 補題 4.1 より $\underset{x}{\sim}$ は $\underset{1}{\sim}$ を含み, また $n \underset{1}{\sim} m$ は $\mathrm{rad}(n) = \mathrm{rad}(m)$ と同じ意味だからである.

よって命題 B を示す.

つまり, $n, m, k > 1$ を正整数, $n \underset{k}{\sim} m$ を仮定したときに, $\varphi(n) \underset{k-1}{\sim} \varphi(m)$ をいう.

さて, $\varphi(n) \underset{k-1}{\sim} \varphi(m)$ とはすべての $1 \leq i < k-1$ の範囲の整数 i について $S_i(\varphi(n)) = S_i(\varphi(m))$ かつ $S_{\geq k-1}(\varphi(n)) = S_{\geq k-1}(\varphi(m))$ ということであるが, いま条件は n, m に対して対称であるから, すべての

$1 \leq i < k-1$ の範囲の整数 i について $S_i(\varphi(n)) \subset S_i(\varphi(m))$ ...(1) かつ $S_{\geq k-1}(\varphi(n)) \subset S_{\geq k-1}(\varphi(m))$ ...(2) を示せば十分である.

(1) の証明:

$S_i(\varphi(n)) \subset S_i(\varphi(m))$ とは, 任意の素数 p について $p \in S_i(\varphi(n)) \longrightarrow p \in S_i(\varphi(m))$ ということで, つまり $\nu_p(\varphi(n)) = i \longrightarrow \nu_p(\varphi(m)) = i$ ということである.

これが任意の $1 \leq i < k-1$ の範囲の整数 i について成り立っていることを示したい.

そのためには, $\nu_p(\varphi(n)) < k-1 \longrightarrow \nu_p(\varphi(n)) = \nu_p(\varphi(m))$ が言えればよい.

補題 3.3 の結果を再掲すると, $\nu_p(\varphi(n)) = \max\bigl(0, \nu_p(n)-1\bigr) + \displaystyle\sum_{q>p, q \mid n} \nu_p(q-1)$.

いま, $n \underset{k}{\sim} m$ より $n \underset{1}{\sim} m$, つまり $\mathrm{rad}(n) = \mathrm{rad}(m)$ が成り立っているので, n の素因数全体の集合と m の素因数全体の集合は等しい.

したがって, $\displaystyle\sum_{q>p, q \mid n} \nu_p(q-1) = \sum_{q>p, q \mid m} \nu_p(q-1)$ が成り立つので, $\max\bigl(0, \nu_p(n)-1\bigr) = \max\bigl(0, \nu_p(m)-1\bigr)$ が言えればよい.

ところが, $\max\bigl(0, \nu_p(n)-1\bigr) \leq \nu_p(\varphi(n)) < k-1$ より $\nu_p(n) < k$.

$\nu_p(n) = 0$ のときは, $\mathrm{rad}(n) = \mathrm{rad}(m)$ より $p \nmid m$, したがって $\nu_p(m) = 0$ なので $\nu_p(n) = \nu_p(m)$.

それ以外のときも, $n \underset{k}{\sim} m$ より, $p \in S_{\nu_p(n)}(n) = S_{\nu_p(n)}(m)$ から, $\nu_p(n) = \nu_p(m)$ が成り立ち, よって式 (1) は証明された.

(2) の証明:

$S_{\geq k-1}(\varphi(n)) \subset S_{\geq k-1}(\varphi(m))$ とは, 任意の素数 p について $p \in S_{\geq k-1}(\varphi(n)) \longrightarrow p \in S_{\geq k-1}(\varphi(m))$ ということで, つまり $\nu_p(\varphi(n)) \geq k-1 \longrightarrow \nu_p(\varphi(m)) \geq k-1$ ということである.

先ほどの議論から, $\displaystyle\sum_{q>p, q \mid n} \nu_p(q-1) = \sum_{q>p, q \mid m} \nu_p(q-1)$ で, これを X とおこう.

すると, $\max\bigl(0, \nu_p(n)-1\bigr) \geq k-X-1 \longrightarrow \max\bigl(0, \nu_p(m)-1\bigr) \geq k-X-1$ が示したい問題になる.

もし $\nu_p(n) < k$ であれば, $n \underset{k}{\sim} m$ より $\nu_p(n) = \nu_p(m)$ が先の議論から成り立つので, 上式はただちに成り立つ.

よって, $\nu_p(n) \geq k$ の場合を考える.

このとき, $n \underset{k}{\sim} m$ より, $p \in S_{\geq k}(n) = S_{\geq k}(m)$ から, $\nu_p(m) \geq k$ が成り立つ.

$k > 1$ より, $\max\bigl(0, \nu_p(m)-1\bigr) = \nu_p(m)-1$ で, これが $k-1$ 以上, よって $X \geq 0$ から $k-X-1$ 以上であることがわかる.

■

リンク

GitHub にアップロードされた本論文のリンク: https://github.com/hikaru-kajita/mathematics/blob/main/multiphi-equivalence/multiphi-equivalence.pdf