書泉グランデでの講義
高校生も十分わかる新しい数論研究
New Series, 第2期　予稿1
2016 年2月12日

飯高 茂

平成28 年2 月9 日

1　オイラー関数

自然数 $a > 1$ に対して $1 \leq b < a$ を満たし, a と互いに素な自然数 b の個数を $\varphi(a)$ と書き, これを自然数 a の関数とみて**オイラー関数**という. ただし $\varphi(1) = 1$ とする.

オイラー関数 $\varphi(a)$ の性質 ($a > 1$) を列挙してみよう.

1. $a - 1 \geq \varphi(a)$,
2. a が素数なら $\varphi(a) = a - 1$. さらに $\varphi(a) = a - 1$ なら a は素数 ,
3. a が素数でないなら $a \geq \varphi(a) + \sqrt{a}$,
4. a, b が互いに素なら $\varphi(ab) = \varphi(a)\varphi(b)$ (乗法性).

$a = p^2$ のとき $a = \varphi(a) + \sqrt{a}$. 逆も成り立つ.

オイラー関数 $\varphi(a)$ を小学生に説明するなら 分母が a の既約な真分数の個数を $\varphi(a)$ と書くのだ, と言えばよい.

1.1 Gaussの公式

一般に自然数が分母, 分子の真分数 $\frac{b}{a}$ があるとき a, b の最大公約数を d をすれば $a = da', b = db'$ とかけて $\frac{b'}{a'}$ は既約な真分数になる. 分母が a' の既約な真分数の個数は $\varphi(a')$ と書ける. したがって分母が a の真分数の個数は a 個ありこれらは分母が a の約数 a' の既約な真分数の全体として表せるのでこれら a' の $\varphi(a')$ の和が a になる. すなわち

$$a = \sum_{a'|a} \varphi(a') \tag{1}$$

となる. ここに $a'|a$ は a' が a の約数を意味する. これをGaussの公式という.

たとえば $a = 12$ とおくと,$a' = 12, 6, 4, 3, 2, 1$ であり,

$$\varphi(12) = 4, \varphi(6) = 2, \varphi(4) = 2, \varphi(3) = 2, \varphi(2) = 1, \varphi(1) = 1.$$

これらを加えると $4 + 2 + 2 + 2 + 1 + 1 = 12$ となって分母が出て来る.

この公式を使うと, オイラー関数 $\varphi(a)$ の値が楽に計算できる.

a が素数 $p > 1$ なら p の約数は $p, 1$ なので $p = \varphi(p) + \varphi(1) = \varphi(p) + 1$ により $\varphi(p) = p - 1$. (これは当たり前の結果ではあるが)

a が素数の平方 p^2 なら約数は $p^2, p, 1$ なので $p^2 = \varphi(p^2) + \varphi(p) + 1 = \varphi(p^2) + (p - 1) + 1$ により $\varphi(p^2) = p^2 - p = p(p - 1)$.

同様にして $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p - 1)$ が示される.

p, q を相異なる素数とすると pq の約数は $pq, q, p, 1$ なので $pq = \varphi(pq) + \varphi(p) + \varphi(q) + 1 = \varphi(pq) + (p-1) + (q-1) + 1$ により $\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$.

1.2 乗法性

a, b を互いに素な自然数とするとき, $\varphi(ab) = \varphi(a)\varphi(b)$ が成り立つ. これがオイラー関数の乗法性である.

乗法性をGaussの公式を用いて数学的帰納法で証明する.

互いに素な a, b について, a ,b の約数を代表的にそれぞれ d, δ で表す. Gaussの公式により,

$$a = \sum_{d|a} \varphi(d), b = \sum_{\delta|b} \varphi(\delta)$$

これらを掛けると

$$ab = \sum_{d|a, \delta|b} \varphi(d)\varphi(\delta)$$

$(d,\delta) \neq (a,b)$ のとき $d\delta < ab$ なので数学的帰納法の仮定により $\varphi(d)\varphi(\delta) = \varphi(d\delta)$. よって,

$$ab = \sum_{d|a,\delta|b} \varphi(d)\varphi(\delta) = \sum_{(d,\delta)\neq(a,b)} \varphi(d\delta) + \varphi(a)\varphi(b)$$

ab の約数は $d\delta$ と書けるので Gauss の公式によって,

$$ab = \sum \varphi(d\delta) = \sum_{(d,\delta)\neq(a,b)} \varphi(d\delta) + \varphi(ab).$$

よって,

$$\varphi(ab) = \varphi(a)\varphi(b).$$

1.3 オイラーの公式

$a = p_1^{e_1} \cdots p_s^{e_s}$, と素因数分解するとき $\overline{p_1} = p_1 - 1, \cdots \overline{e_1} = e_1 - 1, \cdots$ を用いると

$\varphi(p_1^{e_1}) = p_1^{\overline{e_1}}\overline{p_1}, \cdots$ が成り立つので

$$\varphi(a) = p_1^{\overline{e_1}}\overline{p_1} \cdots p_s^{\overline{e_s}}\overline{p_s}.$$

$\varphi(p_1^{e_1}) = p_1^{e_1}(1 - \dfrac{1}{p_1}), \cdots$. これより

$$\frac{\varphi(a)}{a} = (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_s})$$

をえる. これをオイラーの公式という. 右辺から指数 e_j が消えていることに注意.

1.4 オイラー関数のギャップ値

$N = \varphi(a)$ と a で書けない N をオイラー関数のギャップ値という.

素数 p を用いて $N = 2p, (2p+1;$ 非素数) と表せる N はギャップ値である. $N = 14, 26$ などいくらでもある.

1.5 カーマイケルの予想

$N = \varphi(a)$ と書けるとき a と異なる自然数 b があり $N = \varphi(b)$ となる.

この主張をカーマイケルの予想という.

カーマイケルは最初, 証明できたと思い証明を発表したが, 間違いがみつかった. その後, 誰も証明に成功していない. 反例があるなら $n > 10^{400}$ を満たすなどが示されている.

オイラーの逆関数は 1 価にならない, と言い換えてもよいがオイラー関数の問題は一見やさしそうでも証明の困難な問題が多い例としてあげておく. なお, $k > 1$ ならオイラーの逆関数で k 価 になるものが無限に存在する (Ford, 1999).

1.6 Sophie Germain の素数

p : 素数, $2p + 1 = q$: 素数, のとき p を Sophie Germain [1] の素数 という.

p が Sophie Germain の素数のとき $m = 2p$ について, オイラーの逆関数は 2 価 になる.

実際, $\varphi(q) = \varphi(2q) = 2p$. $q, 2q$ 以外 の a で, $\varphi(a) = 2p$ とする.

a : 奇数なら, a の素因子は 1 つになるので $a = P^j$. $\varphi(P^j) = P^{j-1}\overline{P} = 2p$ によって,

$j > 1$ なら $j = 2, P = p, P - 1 = 2$. $a = 6$. しかし $a = 2 * 3, a + 1 = 7$: 素数.

$j = 1$ なら $2p = P - 1$. したがって, $P = 2p + 1$: 素数.

a : 偶数なら, $a = 2P$. になり, $P = p, \overline{P} = 2p$. よって, $2p + 1 = P$:素数.

Sophie Germain の素数は無限に存在すると予想されている. もしこれが正しいなら, オイラーの逆関数で 2 価 になるものが無限に存在する例になるのだが.

[1] フランスの数学者 1776 – 1831,

2　オイラー余関数

$a > 1$ に対して $a - \varphi(a) \geq 1$. かつ $a - \varphi(a) = 1$ なら a : 素数.
そこで $\mathrm{co}\varphi(a) = a - \varphi(a)$ とおき, オイラー余関数という.

表 1: オイラー余関数 ;$\mathrm{co}\varphi(a)$ の順, a:非素数

a	factor	$\varphi(a)$	$a-\varphi(a)$	a	factor	$\varphi(a)$	$a-\varphi(a)$
4	$[2^2]$	2	2	289	$[17^2]$	272	17
9	$[3^2]$	6	3	34	$[2,17]$	16	18
6	$[2,3]$	2	4	51	$[3,17]$	32	19
8	$[2^3]$	4	4	91	$[7,13]$	72	19
25	$[5^2]$	20	5	361	$[19^2]$	342	19
10	$[2,5]$	4	6	38	$[2,19]$	18	20
15	$[3,5]$	8	7	45	$[3^2,5]$	24	21
49	$[7^2]$	42	7	57	$[3,19]$	36	21
12	$[2^2,3]$	4	8	85	$[5,17]$	64	21
14	$[2,7]$	6	8	30	$[2,3,5]$	8	22
16	$[2^4]$	8	8	95	$[5,19]$	72	23
21	$[3,7]$	12	9	119	$[7,17]$	96	23
27	$[3^3]$	18	9	143	$[11,13]$	120	23
35	$[5,7]$	24	11	529	$[23^2]$	506	23
121	$[11^2]$	110	11	36	$[2^2,3^2]$	12	24
18	$[2,3^2]$	6	12	40	$[2^3,5]$	16	24
20	$[2^2,5]$	8	12	44	$[2^2,11]$	20	24
22	$[2,11]$	10	12	46	$[2,23]$	22	24
33	$[3,11]$	20	13	69	$[3,23]$	44	25
169	$[13^2]$	156	13	125	$[5^3]$	100	25
26	$[2,13]$	12	14	133	$[7,19]$	108	25
39	$[3,13]$	24	15	63	$[3^2,7]$	36	27
55	$[5,11]$	40	15	81	$[3^4]$	54	27
24	$[2^3,3]$	8	16	115	$[5,23]$	88	27
28	$[2^2,7]$	12	16	187	$[11,17]$	160	27
32	$[2^5]$	16	16	52	$[2^2,13]$	24	28

余関数について次の公式を示せ:

$$a - \varphi(a) = (p_1{}^{\overline{e_1}} \cdots p_s{}^{\overline{e_s}})(p_1 \cdots p_s - \overline{p_1} \cdots \overline{p_s}).$$

上記の公式によれば, $s(a) \geq 3$ のとき, $a = 2*3*5 = 30, 2*3*7 = 42, 4*3*5 = 60$ のとき $\mathrm{co}\varphi(a) = a - \varphi(a)$ は それぞれ 22,30,44 となりこれらが最小の値と次点, 次次点である.

たぶん, $s(a) \geq 3$ のとき, $a > 60$ なら $\mathrm{co}\varphi(a) > 44$.

3　オイラー余関数の値

1)

a が素数なら $\mathrm{co}\varphi(a) = 1$ なので以下 a が非素数の場合について調べる.

$s(a)$ を a の相異なる素因子の個数とする.

2)

$s(a) = 1$; すなわち $a = P^j$ なら $\mathrm{co}\varphi(a) = P^{j-1}$ なのでこの場合をはじめに計算しておく.

$\mathrm{co}\varphi(a) = P^{j-1} \geq 12$ とすると,$P^j = 4, 8, 16, 9, 27, 25, 49, 121$ のときそれぞれ $\mathrm{co}\varphi(a) = 2, 4, 8, 3, 9, 5, 7, 11$.

以後,a は 2 つ以上の異なる素因子を持つ場合のみ考える.

3)

$\mathrm{co}\varphi(a)$ は 1 から a のうち, a と互いに素でないものの個数である.

a が非素数ならその最大素因子を P とすると $a = P\alpha, (P \geq \mathrm{Maxp}(\alpha))$ とかけて P, a はともに a と互いに素でない. よって, $\mathrm{co}\varphi(a) \geq 2$.

$\mathrm{co}\varphi(a) = 2$ と仮定すると, a に P 以外の素因数はないので, $a = P^j$.

しかし $\mathrm{co}\varphi(a) = P^{j-1}$ なので,$2 = P^{j-1}$. ゆえに $j - 1 = 1, P = 2; a = 2^2 = 4$.

以上によって $\mathrm{co}\varphi(a) = 2$ と仮定すると $a = 4$.

4)

$\mathrm{co}\varphi(a) = 3$ と仮定すると, a に P 以外の素因数がなければ, $a = P^j$, $\mathrm{co}\varphi(a) = P^{j-1} = 3$. よって $a = 3^2 = 9$.

a に P 以外の素因数 q があれば $P, q, 2q, a$ が a とそれぞれ互いに素でない. $\mathrm{co}\varphi(a) > 3$ となり矛盾.

$\mathrm{co}\varphi(a) = 3$ と仮定すると $a = 9$.

5)

$j > 1$ とすると $\rho_0 = \mathrm{co}\varphi(L) = L - \varphi(L)$ を用いて

$$\begin{aligned} co\varphi(P^jL) &= P^jL - P^{j-1}\overline{P}\varphi(L) \\ &= P^{j-1}(PL - \overline{P}\varphi(L)) \\ &= P^{j-1}(L + \overline{P}\rho_0). \end{aligned}$$

これより $\mathrm{co}\varphi(P^jL) = P^{j-1}(L + \overline{P}\rho_0) \geq P(L + \overline{P}\rho_0) \geq P(P + L - 1) > P^2$.

$12 \geq \mathrm{co}\varphi(P^jL) > P^2$ のとき ,$P = 3$.

$a = 3^2 * 2^2 = 36$ のとき, $\varphi(36) = 12$. よって, $\mathrm{co}\varphi(36) = 36 - 12 = 24$.

$a = 3^2 * 2 = 18$ のとき, $\varphi(18) = 6$. よって, $\mathrm{co}\varphi(18) = 12$.
6)
$j = 1$ とすると $a = PL$. $\mathrm{co}\varphi(PL) = L + \overline{P}\rho_0$.
L を素数とすると $P > L$ を満たす. $a = PL$ により $\mathrm{co}\varphi(PL) = P + L - 1$.
ここで $\mathrm{co}\varphi(PL) = P + L - 1 \leq 12$ のときは
$PL = 3 * 2 = 6, P + L - 1 = 4$.
$PL = 5 * 2 = 10, P + L - 1 = 6$.
$PL = 7 * 2 = 14, P + L - 1 = 8$.
$PL = 5 * 3 = 15, P + L - 1 = 7$.
$PL = 7 * 3 = 21, P + L - 1 = 9$.
$PL = 7 * 5 = 35, P + L - 1 = 11$.

7)
$j = 1, L$:非素数の場合 $L \geq 4$, $\rho_0 = \mathrm{co}\varphi(L) \geq 2$ なので
$\mathrm{co}\varphi(a) = L + \overline{P}\rho_0 \geq 4 + 2P - 2 = 2P + 2$.
$11 \geq \mathrm{co}\varphi(a)$ のときは $P \leq 3$.
$P = 3$ なら $a = 3 * 2^e$. $\mathrm{co}\varphi(a) = 2^{e+1}$. $e = 2$ なら $a = 12$, $\mathrm{co}\varphi(a) = 8$.
$e = 3$ なら $a = 24$, $\mathrm{co}\varphi(a) = 16$.
さらに $\mathrm{co}\varphi(12) = 8$, $\mathrm{co}\varphi(24) = 16$,
$\mathrm{co}\varphi(a) < 12$ を満たすのは上記で計算された場合のみ.

4　オイラー余関数の評価式

$s(a) \geq 2, a = P^j * L, j = 1$ とする. すなわち $a = PL$ のとき,$\rho_0 = L - \varphi(L)$ とおく.
$\mathrm{co}\varphi(a) = L + \overline{P}\rho_0$ を用いて以下の計算をする.

$\rho_0 = 1$ のとき L : 素数,$a = PL$. $\mathrm{co}\varphi(a) = P + L - 1$.

$\rho_0 = 2$ のとき $L = 4; a = 4 + 2P - 2 = 2P + 2$.

$\rho_0 = 3$ のとき $L = 9, a = 9P$. $\mathrm{co}\varphi(a) = 9 + 3\overline{P} = 3P + 6$.

$\rho_0 = 4$ のとき $L = 6, a = 6P$. $\mathrm{co}\varphi(a) = 6 + 4\overline{P} = 4P + 2$.
$L = 8, a = 8P$. $\mathrm{co}\varphi(a) = 8 + 4\overline{P} = 4P + 4$.

$\rho_0 = 5$ のとき $L = 5^2; a = 25P$. $\mathrm{co}\varphi(a) = 25 + 5\overline{P} = 5P + 20$.

$\rho_0 = 6$ のとき $L = 10, a = 10P$. $\mathrm{co}\varphi(a) = 10 + 6\overline{P} = 6P + 4$.

$\rho_0 = 7$ のとき $L = 7^2.a = 49P$. $\mathrm{co}\varphi(a) = 49 + 7\overline{P} = 7P + 42$.
$L = 15, a = 15P$. $\mathrm{co}\varphi(a) = 15 + 7\overline{P} = 7P + 8$.

$\rho_0 = 8$ のとき $L = 16, a = 16P$. $\mathrm{co}\varphi(a) = 16 + 8\overline{P} = 8P + 8$.
$L = 14, a = 14P$. $\mathrm{co}\varphi(a) = 14 + 8\overline{P} = 8P + 6$.
$L = 12, a = 12P$. $\mathrm{co}\varphi(a) = 12 + 8\overline{P} = 8P + 4$

$\rho_0 = 9$ のとき $L = 27, a = 27P$. $\mathrm{co}\varphi(a) = 27 + 9\overline{P} = 9P + 18$
$L = 21, a = 21P$. $\mathrm{co}\varphi(a) = 21 + 9\overline{P} = 9P + 12$.

$\rho_0 = 11$ のとき
$L = 35, a = 35P$. $\mathrm{co}\varphi(a) = 35 + 11\overline{P} = 11P + 24$
$L = 121, a = 121P$. $\mathrm{co}\varphi(a) = 121 + 11\overline{P} = 11P + 110$

以上を除外すると $\rho_0 \geq 12$ になるので次の評価式をえる.

$$\mathrm{co}\varphi(a) \geq \frac{a}{P} + 12P^{j-1}\overline{P}.$$

4.1 オイラー余関数の値

例題として $\mathrm{co}\varphi(a) = 27 = 3^3$ となる a を決定してみよう.

1) $s(a) = 1$ のとき $a = P^j$, $\mathrm{co}\varphi(a) = P^{j-1}$ なので $P = 3, j = 4$.

2) $s(a) \geq 2$ のとき $P = \mathrm{Maxp}(a)$ とおくと $a = P^j L$ と書ける $(P > \mathrm{Maxp}(L)$).
$\mathrm{co}\varphi(P^j L) = P^{j-1}(L + \overline{P}\rho_0)$ なので $j > 1$ のとき $P = 3$.
$a = 3^j * 2^e$ とすると, $\mathrm{co}\varphi(P^j L) = 3^{j-1} * 2^{e+1} \neq 27$.

3) $j = 1$, $a = PL$.
$L + \overline{P}\rho_0 = 3^3$ を解く.
$27 = L + \overline{P}\rho_0$ により, L は奇数になる.
$\rho_0 = 1$ のとき L は素数で $P + L - 1 = 27$. よって直ちに $L = 5, P = 23; L = 11, P = 17$.
$\rho_0 = 2$ のとき L は偶数なので L は奇数の仮定に反する.
$\rho_0 = 3$ のとき $L = 9, a = 9P = 45, 63, \cdots$. $\mathrm{co}\varphi(a) = L + \overline{P}\rho_0 = 9 + 3 * \overline{P} = 27$. $18 = 3\overline{P}$. ゆえに $P = 7.L = 3^2$. $a = 3^2 * 7$.

$\rho_0 = 4$ のとき $L = 6$; 偶数. L は奇数の仮定に反する.

$\rho_0 = 5$ のとき $L = 5^2; a = 25P = 25 * 7, 25 * 11, \cdots$. $\mathrm{co}\varphi(a) = L + \overline{P}\rho_0 = 25 + \overline{P}\rho_0 \neq 27$.

$\rho_0 = 6$ のとき $L = 10$:偶数. L は奇数の仮定に反する.

$\rho_0 = 7$ のとき $L = 7^2; a = 49P, L = 15; a = 15P$. $a = 49 * 11, \cdots, a = 15P = 15 * 7 = 105 \cdots$. $\mathrm{co}\varphi(a) = L + \overline{P}\rho_0 > 49$:矛盾

$\rho_0 = 8$ のとき $L = 16; a = 16P; L = 12; L = 14$: 偶数. L は奇数の仮定に反する.

$\rho_0 = 9$ のとき $L = 27; a = 27P, L = 21; a = 21P$. $a = 27 * 5, \cdots, a = 3 * 7 * 11, \cdots$, $\mathrm{co}\varphi(a) = 21 + \overline{P} * 9 > 27$: 矛盾

以上を除外すると次の評価式をえる.

$$27 = \mathrm{co}\varphi(a) \geq \frac{a}{P} + 11P^{j-1}\overline{P} > \frac{a}{P} + 11\overline{P}.$$

よって, $P = 3$. $P = 3 * 2^e$ は $\mathrm{co}\varphi(a) = 3^{j-1} * 2^{e+1} \neq 27$.

以上により解は, $a = 3^4, 5 * 23, 11 * 17, 7 * 3^2$.

4.2 オイラー余関数のギャップ値

数表によると, $N = 10, 26, 34, \cdots$ が余関数のギャップ値らしい.

そこで予想:

$N = 2p, p$: 素数, $N + 1$:非素数 なら N は ギャップ値になるか?

これは $s(a) = 2$ なら正しいが, $s(a) = 3$ となる最小値 $a = 2 * 3 * 5 = 30$ のとき $\mathrm{co}\varphi(a) = 30 - 8 = 22 = 2 * 11$, $22 - 1 = 21 = 3 * 7$: 非素数. したがってこれは反例.

10,26 はともにギャップ値であり, 以下で確認する.

$\mathrm{co}\varphi(a) = 2p$, $2p = 10, 26$ として矛盾を導く. 証明は手間がかかる.

1) $a = P^j$ なら $\mathrm{co}\varphi(a) = P^{j-1}$ なのでこの場合は起きない.

2) $P = \mathrm{Maxp}(a)$ とおくと, $a = P^j L$ と書けて

$\mathrm{co}\varphi(a) = P^{j-1}(PL - \overline{P}\varphi(L)) = 2p$.

3) $j > 1$ なら $P = p, j = 2$.

$$PL - \overline{P}\varphi(L) = L + \overline{P}co\varphi(L) = 2.$$

$L \geq 2, \overline{P} \geq 2$ により矛盾.

4) $j = 1$ のとき $a = PL$. L が素数なら $\mathrm{co}\varphi(a) = P + L - 1 = 2p$. $P + L = 2p + 1$ なので $L = 2, P = 2p - 1$.

$p = 5, 13$ のとき $2p - 1$ は素数ではない. 矛盾.
5) L が素数でないなら $\rho_0 = \mathrm{co}\varphi(L) \geq 2$.
$\mathrm{co}\varphi(a) = L + \overline{P}\rho_0$. $\mathrm{co}\varphi(a) = 2p$ として矛盾を導く.
$\overline{P}$ は偶数なので, L :. よって,
$\rho_0 = 2$ のとき $L = 4; a = 4 + 2P - 2 = 2P + 2 = 2(P + 1) \neq 2p$.

$\rho_0 = 4$ のとき $L = 6, a = 6P$. $\mathrm{co}\varphi(a) = 6 + 4\overline{P} = 4P + 2 = 2p$.
$p = 2P + 1$.
$L = 8, a = 8P$. $\mathrm{co}\varphi(a) = 8 + 4\overline{P} = 4P + 4 = \neq 2p$.

$\rho_0 = 6$ のとき $L = 10, a = 10P$. $\mathrm{co}\varphi(a) = 10 + 6\overline{P} = 6P + 4 = 2p$. $p = 3P + 2$.
このとき $p \neq 5, 13$

$\rho_0 = 8$ のとき $L = 16, a = 16P$. $\mathrm{co}\varphi(a) = 16 + 8\overline{P} = 8P + 8$ $new 2p$.
$L = 14, a = 14P$. $\mathrm{co}\varphi(a) = 14 + 8\overline{P} = 8P + 6 = 2(4P + 3)$. $4P + 3 \neq 5, 13$.
$L = 12, a = 12P$. $\mathrm{co}\varphi(a) = 12 + 8\overline{P} = 8P + 4 \neq 2p$

5 Goldbach の予想

P, L がともに奇数なら $P + L = N + 1$ は偶数. N は与えられた余関数の値なので, $N + 1 = P + L$ を満たす異なる奇素数があるためには $N + 1 \geq 8$.

$L = 2$ のとき,$N - 1 = P$. N が偶数で $N - 1$ が素数でない場合, オイラー余関数のギャップ値になることがあるかもしれない.

8 以上の偶数は 2 個の奇素数の和にかけるという命題は Goldbach の予想と呼ばれ, 正しいと思われるが証明ができていない. 未解決の難問として有名である.

6 $a = 2p$ の方程式

$p > 2$ を素数とおき, $a = 2p$ に関してそのオイラー関数を調べる.

$$\varphi(a) = \varphi(2p) = \varphi(p) = p - 1 = a/2 - 1.$$

これより,

$$2\varphi(a) = a - 2$$

をえる. これを $a = 2p$ の方程式という.

逆にこの方程式の解 a を求めよう. $a = 2\varphi(a) + 2$ により a は偶数.
$a = 2^e L, (e > 0, L :$ 奇数) と書けるので

$$2\varphi(a) = 2\varphi(2^e L) = 2\varphi(2^e)\varphi(L) = 2^e\varphi(L), 2\varphi(a) = a - 2 = 2^e L - 2$$

になるので,

$$2^e\varphi(L) = 2^e L - 2.$$

これより,

$$2^{e-1}(L - \varphi(L)) = 1.$$

$e > 1$ なら左辺は偶数. よって, $e = 1, L - \varphi(L) = 1$. $\mathrm{co}\varphi(L) = 1$ により, L は素数 p. したがって $a = 2p$.

$2\varphi(a) = a - 2$ は $a = 2p$ を決定する方程式であり, 美しい結果ということができる.

7 $a = P^{\varepsilon}p$ の方程式

P を素数ととし, その累乗 P^{ε} を考え $a = P^{\varepsilon}p$ に関してそのオイラー関数を調べる.

$a = P^{\varepsilon}p$ のとき

$$P\varphi(a) = \overline{P}P^{\varepsilon}(p - 1) = \overline{P}a - \overline{P}P^{\varepsilon}.$$

よって

$$P\varphi(a) = \overline{P}a - \overline{P}P^{\varepsilon}$$

をえる. これを $a = P^{\varepsilon}p$ の方程式という.

8 計算例

$a = 3^4 p$ の場合, その方程式は

$$3\varphi(a) = 2a - 2 * 3^4$$

コンピュータで確認してみる.

表 2: $a = 3^4 p$ の場合

a	$\varphi(a)$	a 素因数分解
162	54	$[2, 3^4]$
345	176	$[3, 5, 23]$
405	216	$[3^4, 5]$
561	320	$[3, 11, 17]$
567	324	$[3^4, 7]$
891	540	$[3^4, 11]$

8.1 $P = 3, a = 3^4 p$ の場合

$a = 3^4 p$ の場合, その方程式は

$$3\varphi(a) = 2a - 2 * 3^4$$

$m = 3^4$ のとき通常解 $a = 3^4 p$, エイリアン解が $a = 3 * 5 * 23$, $a = 3 * 11 * 17$.

8.2 $P = 3, a = 3^5 p$ の場合

$a = 3^4 p$ の場合, その方程式は $3\varphi(a) = 2a - 2 * 3^5$
$m = 3^5$ のとき通常解 $a = 3^5 p$,
エイリアン解が $a = 1035 = 3^2 * 5 * 23$, $a = 1683 = 3^2 * 11 * 17$
$a = 2343 = 3 * 11 * 71$,$a = 4071 = 3 * 23 * 59$,$a = 4611 = 3 * 29 * 53$.
これらしかないことを証明することは今や容易であろう.
[研究課題] 最大のエイリアン解を評価せよ.
[研究課題] $2 * P^{\varepsilon}$ が最小の解.

表 3: $a = 3^5 p$ の場合

a	$\varphi(a)$	a 素因数分解
486	162	$[2, 3^5]$
1035	528	$[3^2, 5, 23]$
1215	648	$[3^5, 5]$
1683	960	$[3^2, 11, 17]$
1701	972	$[3^5, 7]$
2343	1400	$[3, 11, 71]$
2673	1620	$[3^5, 11]$
3159	1944	$[3^5, 13]$
4071	2552	$[3, 23, 59]$
4131	2592	$[3^5, 17]$
4611	2912	$[3, 29, 53]$
4617	2916	$[3^5, 19]$
5589	3564	$[3^5, 23]$
7047	4536	$[3^5, 29]$
7533	4860	$[3^5, 31]$
8991	5832	$[3^5, 37]$
9963	6480	$[3^5, 41]$
10449	6804	$[3^5, 43]$

8.3 $P = 5, a = 5^3 p$ の場合

$a = 3^4 p$ の場合, その方程式は

$$5\varphi(a) = 4a - 4 * 5^3$$

$m = 5^3$ のとき通常解 $a = 5^3 p$, エイリアン解が
$a = 345 = 3 * 5 * 23$
$a = 375 = 3 * 5^3$
$a = 665 = 5 * 7 * 19$

8.4 $P = 7, a = 7^2 p$ の場合

$a = 7^2 p$ の場合, その方程式は $7\varphi(a) = 6a - 6 * 7^2$.
$m = 7^2$ のとき通常解 $a = 7^2 p$, エイリアン解が $a = 105 = 3 * 5 * 7$
$a = 7 * 5 * 3$ の解なのでおめでたいかも.

表 4: $a = 5^3 p$ の場合

a	$\varphi(a)$	a 素因数分解
250	100	$[2, 5^3]$
345	176	$[3, 5, 23]$
375	200	$[3, 5^3]$
665	432	$[5, 7, 19]$
875	600	$[5^3, 7]$
1375	1000	$[5^3, 11]$
1625	1200	$[5^3, 13]$

表 5: $a = 7^2 p$ の場合

a	$\varphi(a)$	a 素因数分解
98	42	$[2, 7^2]$
105	48	$[3, 5, 7]$
147	84	$[3, 7^2]$
245	168	$[5, 7^2]$
539	420	$[7^2, 11]$
637	504	$[7^2, 13]$
833	672	$[7^2, 17]$
931	756	$[7^2, 19]$

8.5 $a = P^{\varepsilon} p$ の場合

$a = P^{\varepsilon} p$ のとき

$$P\varphi(a) = \overline{P} P^{\varepsilon}(p-1) = \overline{P} a - \overline{P} P^{\varepsilon}.$$

よって

$$P\varphi(a) = \overline{P} a - \overline{P} P^{\varepsilon}$$

をえる. これを $a = P^{\varepsilon} p$ の方程式という.

逆にこの方程式の解 a を求めよう.

P を法として考えるとすぐわかるように a は P の倍数.

$a = P^e L, (e > 0, L : P$ で割れない,) と書ける.

$P\varphi(a) = \overline{P} P^e \varphi(L)$ により

$$\overline{P}P^e\varphi(L) = \overline{P}P^eL - \overline{P}P^\varepsilon.$$

これより

$$L - \varphi(L) = P^{\varepsilon-e}.$$

$\eta = \varepsilon - e$ とおくとき

$$co\varphi(L) = P^\eta.$$

逆に, オイラーの余関数について $co\varphi(L) = P^\eta$ を満たす $L : P$ と互いに素, があれば, $a = P^eL, \varepsilon = e + \eta$ について, $a = P^\varepsilon p$ を満たす.

$\varepsilon = 1$ のとき, $e > 0$ により $\eta = 1 - e = 0$. $\mathrm{co}\varphi(L) = 1$. L は素数 p になり $a = Pp$.

$P = 2$ のとき, $e > 0$ により $\eta = 1 - e = 0$. $\mathrm{co}\varphi(L) = 1$. L は素数 p になり $a = Pp$. $co\varphi(L) = 2^\eta$ が成立するが, L は奇数なので $co\varphi(L) = L - \varphi(L) = 2^\eta$ より $\eta = 0$. L は素数 p になり $a = 2^ep$.

$a = 2^ep$ と素数 p で書ける条件は $2\varphi(a) = a - 2^\varepsilon$.

$2\varphi(a) = a - 2^\varepsilon$ の解は $2^\varepsilon * p$ なので解は無限にある.

[研究課題]

$2\varphi(a) = a - x$ の解が無限にる場合は $x = 2^\varepsilon$ になるか?

$P = 3, \varepsilon = 2$ のとき, $e = 1, \eta = 2 - e = 1$. $\mathrm{co}\varphi(L) = 3$, $L = 3^2$. しかし L は 3 で割れないので矛盾.

$P = 3, \varepsilon = 3$ のとき, $e = 1, \eta = 3 - e = 2$. $\mathrm{co}\varphi(L) = 9$, $L = 3^3, L = 3 * 7$. しかし L は 3 で割れないので矛盾.

$P = 3, \varepsilon = 4$ のとき, $e = 1, \eta = 4 - e = 3$. $\mathrm{co}\varphi(L) = 27$, $L = 3^4, L = 3^2 * 7, 5 * 23, 11 * 17$. L は 3 で割れないので $L = 5 * 23, 11 * 17$ のみ残る.

$a = 3 * 5 * 23, a = 3 * 11 * 17$ が解になり, これらをエイリアン解という.

$P = 3, \varepsilon = 5$ のとき, $e = 1, \eta = 4 - e = 4$. $\mathrm{co}\varphi(L) = 81$,

$a = 1035 = 3^2 * 5 * 23$, $a = 1683 = 3^2 * 11 * 17$, $a = 2343 = 3 * 11 * 71$,$a = 4071 = 3 * 23 * 59$,$a = 4611 = 3 * 29 * 53$.

これらをエイリアン解という.

$P = 5, \varepsilon = 3$ のとき, $e = 1, \eta = 3 - e = 2$. $\mathrm{co}\varphi(L) = 25$, $L = 5^3, L = 3 * 23$. L は 5 で割れないので $L = 3 * 23$ のみ残る.

$a = 3 * 5 * 23$ が解になり, これをエイリアン解という.

$P = 8, \varepsilon = 2$ のとき, $e = 1, \eta = 2 - e = 1$. $\mathrm{co}\varphi(L) = 7$, $L = 7^2, L = 3 * 5$. L は 7 で割れないので $L = 3 * 5$ のみ残る.

$a = 3 * 5 * 7$ が解になり, これをエイリアン解という.

9　$a - 2\varphi(a) = x$ の表

表 6: $a - 2\varphi(a)$ その 1

a	factor	$\varphi(a)$	$a - \varphi(a)$	$a - 2\varphi(a)$
29	$[29]$	28	1	-27
81	$[3^4]$	54	27	-27
93	$[3, 31]$	60	33	-27
117	$[3^2, 13]$	72	45	-27
189	$[3^3, 7]$	108	81	-27
357	$[3, 7, 17]$	192	165	-27
405	$[3^4, 5]$	216	189	-27
645	$[3, 5, 43]$	336	309	-27
693	$[3^2, 7, 11]$	360	333	-27
55	$[5, 11]$	40	15	-25
87	$[3, 29]$	56	31	-25
375	$[3, 5^3]$	200	175	-25
615	$[3, 5, 41]$	320	295	-25
23	$[23]$	22	1	-21
99	$[3^2, 11]$	60	39	-21
147	$[3, 7^2]$	84	63	-21
555	$[3, 5, 37]$	288	267	-21
69	$[3, 23]$	44	25	-19
19	$[19]$	18	1	-17

表 7: $a - 2\varphi(a) = x$ その 2

a	factor	$\varphi(a)$	$a - \varphi(a)$	$a - 2\varphi(a)$
17	$[17]$	16	1	-15
25	$[5^2]$	20	5	-15
57	$[3, 19]$	36	21	-15
225	$[3^2, 5^2]$	120	105	-15
273	$[3, 7, 13]$	144	129	-15
465	$[3, 5, 31]$	240	225	-15
35	$[5, 7]$	24	11	-13
51	$[3, 17]$	32	19	-13
435	$[3, 5, 29]$	224	211	-13
13	$[13]$	12	1	-11
11	$[11]$	10	1	-9
27	$[3^3]$	18	9	-9
39	$[3, 13]$	24	15	-9
63	$[3^2, 7]$	36	27	-9
135	$[3^3, 5]$	72	63	-9
231	$[3, 7, 11]$	120	111	-9
855	$[3^2, 5, 19]$	432	423	-9

表 8: $a - 2\varphi(a) = x$ その 3

a	factor	$\varphi(a)$	$a - \varphi(a)$	$a - 2\varphi(a)$
33	$[3, 11]$	20	13	-7
345	$[3, 5, 23]$	176	169	-7
7	$[7]$	6	1	-5
75	$[3, 5^2]$	40	35	-5
5	$[5]$	4	1	-3
9	$[3^2]$	6	3	-3
21	$[3, 7]$	12	9	-3
45	$[3^2, 5]$	24	21	-3
285	$[3, 5, 19]$	144	141	-3
765	$[3^2, 5, 17]$	384	381	-3
3	$[3]$	2	1	-1
15	$[3, 5]$	8	7	-1
255	$[3, 5, 17]$	128	127	-1
2	$[2]$	1	1	0
$-$	$-$	$-$	$-$	0
512	$[2^9]$	256	256	0

この表から $N = a - 2\varphi(a) < 0$ のとき N は奇数に限ることが見て取れる.
案外簡単に証明できた.
N は偶数 $2M$ とおくと a も偶数なので $a = 2^e L, L$: 奇数, と表される.

$$0 > N = 2M = a - 2\varphi(a) = 2^e L - 2^e \varphi(L) = 2^e (L - \varphi(L))$$

によって余関数が負になり矛盾.

表 9: $a-2\varphi(a)=x$ その 4

a	factor	$\varphi(a)$	$a-\varphi(a)$	$a-2\varphi(a)$
6	$[2,3]$	2	4	2
–	–	–	–	2
998	[2,499]	498	500	2
195	$[3,5,13]$	96	99	3
12	$[2^2,3]$	4	8	4
–	–	–	–	4
964	$[2^2,241]$	480	484	4
165	$[3,5,11]$	80	85	5
18	$[2,3^2]$	6	12	6
88	$[2^3,11]$	40	48	8
–	–	–	–	8
904	$[2^3,113]$	448	456	8
105	$[3,5,7]$	48	57	9
585	$[3^2,5,13]$	288	297	9

$a-2\varphi(a)=1$ のとき解はないように思われる. 証明は困難であろう.

$a-2\varphi(a)=6$ のとき解は 1 つだけ. これは容易に証明できる.
a は偶数なので $a=2^eL$ と奇数 L を用いて書ける.
$2^eL-2^e\varphi(a)=6$ により $e=1, L-\varphi(L)=3$.
$co\varphi(L)=3$ のとき $L=3^2$ は容易にわかる. よって $a=18$.

$a - 2\varphi(a) = -27, -9, -3, -1$ の場合の解は個数が多いこと解が類似していることに注意しよう.

10 方程式 $2\varphi(a) - a = 1$ の解

負の場合は気分的に良くないので符号を変えて $2\varphi(a) - a = 1$ の場合を調べる.

表 10: $2\varphi(a) - a = 1$, コンピュータによる全数調査

a	素因数分解
3	3
15	$3 * 5$
255	$3 * 5 * 17$
65535	$3 * 5 * 17 * 257$

方程式 $2\varphi(a) - a = 1$ の解は著しい性格を持っている.
解 a に対して $a < p$ となる素数 p があり ap が次の解になっている.

表 11: $2\varphi(a) - a = 3$, コンピュータによる全数調査

a	素因数分解	*
5	5	new
9	3^2	*
21	$3 * 7$	new
45	$3^2 * 5$	*
285	$3 * 5 * 19$	new
765	$3^2 * 5 * 17$	*
27645	$3 * 5 * 19 * 97$	new
196605	$3^2 * 5 * 17 * 257$	*