数学の研究を始めよう (V)

オイラーをモデルに数論研究
第5章
オイラーの余関数とは何だろう

飯高 茂

平成 30 年 3 月 8 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.

オイラー関数はフェルマの小定理の一般化のためオイラーにより導入された. 記号 $\varphi(a)$ の導入をはじめ本格的研究はガウスが始めた. ガウスは $\varphi(1) = 1$ とする理由を詳しく述べている.

$a > 1$ が素数なら, $1 \leq b < a$ を満たす b は a と互いに素. よって, $\varphi(a) = a - 1$.

この逆が成り立つ.

すなわち, $\varphi(a) = a - 1$ を満たすとき,a と互いに素なので, $1 \leq b < a$ の数 b はすべて a と互いに素なので, a の約数ではない. よって, a は素数.

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

$\langle 1 \rangle$ $a - 1 \geq \varphi(a)$,

$\langle 2 \rangle$ a が素数なら $\varphi(a) = a - 1$. さらに $\varphi(a) = a - 1$ なら a は素数 ,

$\langle 3 \rangle$ a が素数でないなら $a \geq \varphi(a) + \sqrt{a}$,

$\langle 4 \rangle$ a, b が互いに素なら $\varphi(ab) = \varphi(a)\varphi(b)$ (乗法性).

オイラー関数 $\varphi(a)$ は分母が a の既約な真分数の個数のことである. オイラー関数は定義だけなら小学生にもわかるが現代でもその真の性質の解明はあまり進んでいない.

1.1　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
乗法性により $\varphi(p_1^{e_1}) = p_1^{\overline{e_1}}\overline{p_1}, \cdots$ が成り立つので

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

$\varphi(p_1^{e_1}) = p_1^{e_1}(1-\frac{1}{p_1})\cdots$. 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.

1.2 オイラー関数のギャップ値

$N = 14$ や 26 になるオイラー関数の値は存在しない. そこで $N = \varphi(a)$ 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) と表される N はギャップ値である.

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 (Euler cofunction) という.

注意 1 正弦関数 $\sin(x)$ に対して, 余弦関数 $\cos(x)$ があり $\cos(x) = \sin(\frac{\pi}{2} - x)$ が成り立つ. そこで,$co\varphi(a) = a - \varphi(a)$ をオイラー余関数と呼ぶことにした.

こうして名前をつけると「今度はオイラー余関数を研究しよう」と高校生に呼びかけやすくなる.

Wikipedia によると 1879 年に J. J. Sylvester は オイラー余関数 を Euler's totient function または the Euler totient と呼んだ. また cototient of a を $a - \varphi(a)$ で定義した.

さてオイラー余 関数 $\mathrm{co}\varphi(a)$ の性質 ($a > 1$) を列挙してみよう.

⟨1⟩ $co\varphi(a) \geq 1$,

⟨2⟩ $co\varphi(a)$ とは 1 から a までの数 b で a と互いに素でないものの個数である.

⟨3⟩ a が素数なら $co\varphi(a) = 1$. さらに $\mathrm{co}\varphi(a) = 1$ なら a は素数 ,

⟨4⟩ a が素数でないなら co $\varphi(a) \geq \sqrt{a}$.(後で精密化して証明する)

乗法性は成り立たない.

a : 素数なら $\mathrm{co}\varphi(a) = 1$ なので a:非素数に限って次ページの数表に載せた.

ここに $s(a)$ を a の相異なる素因子の個数とする.

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

a	factor	$s(a)$	$\varphi(a)$	$co\varphi(a)$
4	$[2^2]$	1	2	2
9	$[3^2]$	1	6	3
6	$[2,3]$	2	2	4
8	$[2^3]$	1	4	4
25	$[5^2]$	1	20	5
10	$[2,5]$	2	4	6
15	$[3,5]$	2	4	7
49	$[7^2]$	1	42	7
12	$[2^2,3]$	2	2	8
14	$[2,7]$	2	6	8
16	$[2^4]$	1	8	8
21	$[3,7]$	2	6	9
27	$[3^3]$	1	18	9 (10 が無い)
35	$[5,7]$	2	12	11
121	$[11^2]$	1	110	11
18	$[2,3^2]$	2	6	12
20	$[2^2,5]$	2	4	12
22	$[2,11]$	2	10	12
33	$[3,11]$	2	10	13
169	$[13^2]$	1	156	13
26	$[2,13]$	2	12	14
39	$[3,13]$	2	12	15
55	$[5,11]$	2	20	15
24	$[2^3,3]$	2	4	16
28	$[2^2,7]$	2	6	16
32	$[2^5]$	1	16	16
65	$[5,13]$	2	12	17
77	$[7,11]$	2	30	17
289	$[17^2]$	1	272	17
34	$[2,17]$	2	16	18

表 2: オイラー余関数 ;co$\varphi(a)$ の順, a:非素数 その 2

a	factor	$s(a)$	$\varphi(a)$	$co\varphi(a)$
51	$[3, 17]$	2	16	19
91	$[7, 13]$	2	12	19
361	$[19^2]$	1	342	19
38	$[2, 19]$	2	18	20
45	$[3^2, 5]$	2	12	21
57	$[3, 19]$	2	18	21
85	$[5, 17]$	2	16	21
30	$[2, 3, 5]$	3	4	22
95	$[5, 19]$	2	36	23
119	$[7, 17]$	2	48	23
143	$[11, 13]$	2	60	23
529	$[23^2]$	1	506	23
36	$[2^2, 3^2]$	2	6	24
40	$[2^3, 5]$	2	4	24
44	$[2^2, 11]$	2	10	24
46	$[2, 23]$	2	22	24
69	$[3, 23]$	2	22	25
125	$[5^3]$	1	100	25
133	$[7, 19]$	2	18	25(26 が無い)
63	$[3^2, 7]$	2	6	27
81	$[3^4]$	1	54	27
115	$[5, 23]$	2	44	27
187	$[11, 17]$	2	80	27
52	$[2^2, 13]$	2	12	28
161	$[7, 23]$	2	66	29
209	$[11, 19]$	2	90	29
221	$[13, 17]$	2	48	29
841	$[29^2]$	1	812	29
42	$[2, 3, 7]$	3	6	30
50	$[2, 5^2]$	2	20	30
58	$[2, 29]$	2	28	30

2016 年 6 月に高校生 3 年生だった小室慶太は $\mathrm{co}\varphi(a) \leq 200$ を満たす合成数 a についてその素因数分解をすべて求めた.

その結果,200 以下の余関数のギャップ値は 10,26,34,50,58,86,100,116,130,146,172,186 であることが分かった. これはなかなかの労作である.

[問題]

余関数について次の公式を示せ:

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

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 $\mathrm{co}\varphi(a) > 44$.

[問題]

余関数について次を示せ: 与えられた $N > 1$ に対し $N = \mathrm{co}\varphi(a) > 1$ を満たす a は有限個であることを示せ.

3　オイラー余関数の値が小さい場合

$\mathrm{co}\varphi(a) \leq 12$ の場合の a を調べる.

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.

2)

$s(a) = 1$; すなわち 素数 P によって $a = P^j, j > 1$ とかけるとき $\mathrm{co}\varphi(a) = P^{j-1}$. この場合をはじめに計算しておく.

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

3)

$\mathrm{co}\varphi(a) = 2$ と仮定すると, a に P 以外の素因子 Q があるとき $P, Q, P/Q, PQ$ は a と互いに素でない. よって $\mathrm{co}\varphi(a) \geq 4$. これは矛盾なので, $a = P^j$　と書ける.

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

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, やはり $a = P^j$, と書けるので $\mathrm{co}\varphi(a) = P^{j-1} = 3$ によって $a = 3^2 = 9$.

5)

以後,$s(a) \geq 2$ の場合を考える.

$a = P^j L, (P > \mathrm{Maxp}(L))$ と書ける.

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

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

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

$12 \geq \mathrm{co}\varphi(P^j L)$ のとき ,$P = 3$. したがって,

$a = 3^2 * 2^2 = 36$ 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 $a = PL$. 式が簡単になり $\mathrm{co}\varphi(PL) = L + \overline{P}\rho_0$.

L を素数とすると $a = PL, P > L$ で $\mathrm{co}\varphi(PL) = P + L - 1$.

ここで $\mathrm{co}\varphi(PL) \leq 12$ 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)
$j = 1, a = PL, L$: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 $a = 24$, $\mathrm{co}\varphi(a) = 16 > 12$; おきない.
とくに $\mathrm{co}\varphi(a) = 10$ はおきない. すなわち, 10 はオイラー余関数のギャップ値.
$\mathrm{co}\varphi(a) < 12$ 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

$s(a) \geq 2, a = PL$ とする. $\rho_0 = L - \varphi(L)$ とおくと. $\mathrm{co}\varphi(a) = L + \overline{P}\rho_0$
この公式を用いて以下の結果をまとめておく.

$\rho_0 = 1$ 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.
$j \geq 1$ のとき $a = P^j L$ について

$$\mathrm{co}\varphi(P^j L) = P^{j-1}(L + \overline{P}\rho_0) = P^{j-1}L + P^{j-1}\overline{P}\rho_0 = \frac{a}{P} + P^{j-1}\overline{P}\rho_0$$

が成り立つので $\rho_0 \leq 11$ の場合を除くと

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

4.1 オイラー余関数の値から評価

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 $P = 3, j = 4$; $a = 3^4$.

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

3) $j = 1$, $a = PL$.
$\mathrm{co}\varphi(a) = L + \overline{P}\rho_0 = 3^3$ 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
i). $P = 23, L = 5$, ii).$P = 17, L = 11$.

$\rho_0 = 2$ 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 $L = 9, a = 9P$. $\mathrm{co}\varphi(a) = L + \overline{P}\rho_0 = 9 + 3\overline{P} = 27$. $18 = 3\overline{P}$. ゆえに $P = 7.L = 3^2$.
$a = 3^2 * 7$.
$\rho_0 = 4$ のとき $L = 6$ または $L = 8$; 偶数. L は奇数の仮定に反する.
$\rho_0 = 5$ のとき $L = 5^2; a = 25P$. $\mathrm{co}\varphi(a) = L + \overline{P}\rho_0 = 25 + 5\overline{P} \neq 27$.
$\rho_0 = 6$ のとき $L = 10$:偶数. L は奇数の仮定に反する.
$\rho_0 = 7$ のとき $L = 7^2; a = 49P$, $\mathrm{co}\varphi(a) = L + 7\overline{P} > 49$; 矛盾.
$L = 15; a = 15P = 15 * 7 = 105 \cdots > 27$.
$\rho_0 = 8$ 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 $L = 27; a = 27P$, $\mathrm{co}\varphi(a) > 27$.
$L = 21; a = 21P$. $\mathrm{co}\varphi(a) = 21 + 9\overline{P} > 27$; 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, $a = 3^4, 5 * 23, 11 * 17, 7 * 3^2$.

これは高校生:三谷樹さんの結果でもある.

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 P^{j-1} はギャップ値ではない.

2) $P = \mathrm{Maxp}(a)$ とおくと, $a = P^j L(P > Maxp(L))$ 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 $\rho_0 = \mathrm{co}\varphi(L) \geq 2$.

$\mathrm{co}\varphi(a) = L + \overline{P}\rho_0$ になる. $\mathrm{co}\varphi(a) = 2p$ として矛盾を導く.

$\overline{P}$ は偶数なので, L : 偶数. よって,

i). $\rho_0 = 2$ のとき $L = 4; a = 4 + 2P - 2 = 2P + 2 = 2(P + 1) \neq 2p$.

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

$p = 2P + 1; p = 5, 13$ によりそれぞれ, $P = 2, P = 6$; 矛盾.

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

$\rho_0 = 6$ 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 $L = 16, a = 16P$. $\mathrm{co}\varphi(a) = 16 + 8\overline{P} = 8P + 8 \neq 2p$.

$L = 14, a = 14P$. $\mathrm{co}\varphi(a) = 14 + 8\overline{P} = 8P + 6 = 2(4P + 3)$. $4P + 3 \neq 5, 13$.

$L = 12, a = 12P$. $\mathrm{co}\varphi(a) = 12 + 8\overline{P} = 8P + 4 \neq 2p$

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 P, L 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(ゴールドバッハ) 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.

小室君はオイラー余関数のギャップ値の研究過程で, $N \geq 7$ ならギャップ値にらないことを示すには偶数 $N + 1$ が 2 つの奇素数の和に書けることを示せばよいことに気付いた. 例を計算すると成立することはおおいにありうると思った.

このようにして小室君は自然に導かれて Goldbach の予想に至ったのであった.

数学好きの少年なら友人たちの会話から耳学問として Goldbach の予想 を知ることもあるだろう. しかし自分で発見すればそれから受ける感激はずっと大きいに違いない.

5.1 Goldbach の予想の近況

耳学問は今は流行らない. そこで net に頼る. wikipedia(英文) にある Goldbach の予想からごく一部を引用する.

1742 年, ドイツの Christian Goldbach はオイラーに手紙を書いて

5 より大きい整数は 2 個の素数の和であらわすことができるようだ, と書いた.

オイラーは返書の中で,「それは確かなようだが証明はできなかった」と述べた.

関連して 7 より大きい奇数は 3 個の奇素数の和で書ける, という予想も述べた. これを,Goldbach の予想の弱い形という.

Goldbach の予想の弱い形は研究がしやすいそうである. 実際, 2013 年にペルーの数学者 Harald Helfgott はこの予想を証明し,2014 にソウル特別市で開かれた ICM(国際数学者会議) で招待講演者に選ばれ証明を公表した.

6 オイラー余関数の平方根評価

オイラー余関数 $\mathrm{co}\varphi(a) = a - \varphi(a)$ を用いると a が素数でないなら $\mathrm{co}\varphi(a) \geq \sqrt{a}$ と書ける.

ここで $\mathrm{Maxp}(a)$ は a の最大素因子を指す記号.

次にこの結果を精密化する.

$s(a) = 1$ のときはすでに扱ったので, $s(a) \geq 2$ とし $P = \mathrm{Maxp}(a)$,$a = P^j L, (P > \mathrm{Maxp}(L))$ とおく.

定理 1 $j \geq 2$ のとき, $a \neq 18$ ならば

$$co\varphi(a) \geq 4\sqrt{a}.$$

ただし $a = 18 = 3^2 \cdot 2$ のときは次の評価になる.

$$co\varphi(a) = 2\sqrt{2}\sqrt{a}.$$

$j = 1$ のとき, $a = PL$, *(P:*素数*, L:*非素数*)* かつ $P > Maxp(L)$ ならば

$$co\varphi(a) \geq 2\sqrt{a}.$$

$a = PL$, *(P, L:*素数*)* ならば

$$co\varphi(a) = P + L - 1 \geq 2\sqrt{PL} - 1 = 2\sqrt{a} - 1.$$

次に証明を行う.
1) $s(a) = 1$ のとき $a = P^j, j > 1$ なら $\mathrm{co}\varphi(a) = P^{j-1} = a^{1-1/j} \geq \sqrt{a}$.

2) $s(a) \geq 2$ のとき $P = \mathrm{Maxp}(a)$ とおくと, $a = P^j L, (P > \mathrm{Maxp}(L))$ と書けて $\mathrm{co}\varphi(a) = P^{j-1}(L + \overline{P}\rho_0)$, ここで $\rho_0 = co\varphi(L)$ とおいた.
$P^{j-1}L = \dfrac{a}{P}$ となるので $\mathrm{co}\varphi(a) = \dfrac{a}{P} + P^{j-1}\overline{P}\rho_0$.

3) $j > 1$ なら相加・相乗平均により

$$\mathrm{co}\varphi(a) = \frac{a}{P} + P^{j-1}\overline{P}\rho_0 \geq 2\sqrt{\overline{P}P^{j-2}\rho_0}\sqrt{a}.$$

$\lambda_0 = \sqrt{(P-1)\rho_0}$ とおけば

$$\mathrm{co}\varphi(a) \geq 2\lambda_0\sqrt{a}.$$

$P \geq 3, \rho_0 \geq 1$ により, $\lambda_0 = \sqrt{(P-1)\rho_0} \geq \sqrt{2}$ なので

$$\mathrm{co}\varphi(a) \geq 2\sqrt{2}\sqrt{a}.$$

実際に $a = 18 = 3^2 \cdot 2$ とおけば $\mathrm{co}\varphi(a) = 12, \sqrt{a} = 3\sqrt{2}$ によって,

$$\mathrm{co}\varphi(a) = 2\sqrt{2a}.$$

これ以外なら $\rho_0 \geq 2$ または $P \geq 5$. したがってこれを唯一の例外として, 次の評価が得られる.

$j \geq 2$ のとき, $a \neq 18$ ならば

$$\mathrm{co}\varphi(a) \geq 4\sqrt{a}.$$

4) $j = 1$ のとき $a = PL$ になり $\lambda = \sqrt{(1 - 1/P)\rho_0}$ とおくと

$$\mathrm{co}\varphi(a) \geq 2\lambda\sqrt{a},$$

$\rho_0 = 2$ なら $L = 4, a = 4P$. $\mathrm{co}\varphi(a) = 2P + 2, \sqrt{a} = 2\sqrt{P}$ により

$$\mathrm{co}\varphi(a) \geq 4\sqrt{P} = 2\sqrt{a}.$$

$\rho_0 = 3$ なら $L = 9, a = 9P, P \geq 5$. $\mathrm{co}\varphi(a) = 3P + 6, \sqrt{a} = 3\sqrt{P}$ により

$$\mathrm{co}\varphi(a) \geq 2\sqrt{2a}.$$

$\rho_0 \geq 4$ なら $P \geq 3$ として

$$\lambda = \sqrt{(1 - 1/P)\rho_0} \geq \sqrt{(1 - 1/P) \cdot 4} > \sqrt{8/3} = 1.63.$$

よって

$$\mathrm{co}\varphi(a) \geq 3.26\sqrt{a}.$$

$\rho_0 = 1$ なら L : 素数,$a = PL$ になり

$$\mathrm{co}\varphi(a) = P + L - 1 \geq 2\sqrt{PL} - 1 = 2\sqrt{a} - 1.$$

これより良い評価 $\mathrm{co}\varphi(a) = P + L - 1 \geq 2\sqrt{a}$ は双子素数のときなどでは成り立たない.

7 双子素数

2 数 $a, b > 0$ の相加・相乗平均では

$$a + b \geq 2\sqrt{ab}$$

が成り立ち, $a = b$ では等号が成り立つ. 2 素数 $P > L$ では相加・相乗平均式で等号が成り立たないが P, L が近い値なら等号に近づくであろう.

$P, L = P - 2$ がともに素数のとき**双子素数**(twin prime) という.

双子素数は無数にあるという予想がある. 2016 年現在, まだ解けていない. しかし, 事実としてこれは正しいと思われている.

なお $P, L = P - 4$ がともに素数のとき, **いとこ素数**(cousin primes) という.

いとこ素数も無数にありそうだ.

$\mathrm{co}\varphi(a) = P + L - 1 = 2P - 3, \sqrt{a} = \sqrt{P(P-2)}$ なので, 次の数表ができる.

表 3: $P = L + 2$; P, L :ふたご素数の場合

L	P	a	$co\varphi(a)$	$\sqrt{a}$	$co\varphi(a) - 2\sqrt{a} + 1$	$co\varphi(a) - 2\sqrt{a}$
3	5	15	7	3.872983346	0.254033308	−0.745966692
5	7	35	11	5.916079783	0.167840434	−0.832159566
11	13	143	23	11.95826074	0.083478514	−0.916521486
17	19	323	35	17.97220076	0.055598489	−0.944401511
29	31	899	59	29.9833287	0.033342598	−0.966657402
41	43	1763	83	41.98809355	0.023812899	−0.976187101
59	61	3599	119	59.99166609	0.016667824	−0.983332176
71	73	5183	143	71.99305522	0.013889559	−0.986110441
101	103	10403	203	101.9950979	0.009804157	−0.990195843
107	109	11663	215	107.9953703	0.009259458	−0.990740542
137	139	19043	275	137.9963768	0.007246472	−0.992753528
149	151	22499	299	149.9966666	0.006666741	−0.993333259
179	181	32399	359	179.9972222	0.005555598	−0.994444402

表 4: $P = L + 4$; P, L :いとこ素数のとき

L	P	a	$co\varphi(a)$	$\sqrt{a}$	$co\varphi(a) - 2\sqrt{a} + 1$	$co\varphi(a) - 2\sqrt{a}$
3	7	21	9	4.582575695	0.83484861	−0.16515139
7	11	77	17	8.774964387	0.450071225	−0.549928775
13	17	221	29	14.86606875	0.267862505	−0.732137495
19	23	437	41	20.90454496	0.190910079	−0.809089921
37	41	1517	77	38.94868419	0.102631623	−0.897368377
43	47	2021	89	44.95553359	0.088932828	−0.911067172
67	71	4757	137	68.9710084	0.057983196	−0.942016804
79	83	6557	161	80.97530488	0.049390245	−0.950609755
97	101	9797	197	98.97979592	0.040408164	−0.959591836
103	107	11021	209	104.9809507	0.038098694	−0.961901306
109	113	12317	221	110.9819805	0.036038961	−0.963961039
163	167	27221	329	164.9878783	0.024243315	−0.975756685
193	197	38021	389	194.9897433	0.02051336	−0.97948664

8　双子素数研究の近況

中国系のアメリカ在住の数学者 Yitang Zhang は ある数 N(だいたい 7 千万) があり, 異なる 2 素数の差が N 以下の素数が無限にあることを示しセンセーションを巻き起こした. 実際この結果は名もない (unknown mathematician) 数学者による歴史的な偉業として朝日新聞や New York Times などで報じられた.

$N=2$ にとることが示されると双子素数が無限にあることが証明できたことになる.

2014 年には James Maynard と Terence Tao は (たぶん独立に) $N=246$ まで下げることに成功した. しかし目標の $N=2$ までの隔たりはきわめて大きい.

$N=4$ のときできればいとこ素数が無限にあることが納得できのだが証明はできるのだろうか.

その昔, 広中平祐先生が特異点解消の定理に成功した後, 東京大学で集中講義をしその後の懇親会で「たとえ D.Mumford が試みて証明できない予想があってもあきらめることはない. 思い切ってやればできるかも知れない」と言って我々若い者を激励した.

9　新しい不変量 copm(a) の値

$s(a)\geq 2$ のとき余関数の値 $\mathrm{co}\varphi(a)$ を下から評価するとき, 平方根を使わないより直接の評価をしてみよう. たとえば, a の最大素因子 $\mathrm{Maxp}(a)$ 用いて下から評価することを試みる.

$P=\mathrm{Maxp}(a)$ とおくとき,$a=P^jL(\ P>\mathrm{Maxp}(L))$ と書く.

$\mathrm{copm}(a)=\mathrm{co}\varphi(a)-\mathrm{Maxp}(a)$(ここから 4 英文字 c,o,p,m を選んだ) によって新しい不変量を導入すると

$$\mathrm{copm}(a)=P^{j-1}(L+\overline{P}\rho_0)-P$$

とりあえず $\mathrm{copm}(a)\leq 35$ の場合をすべて調べてみよう.

1) $j\geq 2$.

下限の評価なので, $j=2$ のときのみ計算する.

$$\mathrm{copm}(a)=P(L+\overline{P}\rho_0-1).$$

a). $\rho_0=1$. すなわち L は素数のとき

$\mathrm{copm}(a)=P(L+\overline{P}\rho_0-1)=P(L+P-2)$.

$P=3$ のときは $L=2$ になり $a=3^2\cdot 2$ のとき $\mathrm{copm}(a)=9$.

$P=5$ のときは $L=3,2$ になる. それに応じて $a=5^2\cdot 3,5^2\cdot 2;\mathrm{copm}(a)=5(L+3)=30,25$.

$P=7$ のときは $L=5,3,2$ になる. それに応じて $a=7^2\cdot 5,7^2\cdot 3,7^2\cdot 2;\mathrm{copm}(a)=7(L+5)=70,56,49$. これは大きすぎ.

b). $\rho_0=2$. すなわち $L=4$. $a=P^2\cdot 2^2(P\geq 3)$.

$\mathrm{copm}(a)=P(2P+1)$. $P=7,5,3$ とすると, それに応じて $\mathrm{copm}(a)=105,55,21$.

$a=2^2\cdot 3^2$ のとき $\mathrm{copm}(a)=21$.

1)*. $j=3,4$.

$j=3, P=3, \rho_0=1$. すなわち $a=3^3\cdot 2$. すると, $\mathrm{co}\varphi(a)=3^2\cdot 2^2=36, \mathrm{copm}(a)=33$
$j=4, P=3, \rho_0=1$. すなわち $a=3^4\cdot 2$. すると, $\mathrm{co}\varphi(a)=3^3\cdot 2^2=68, \mathrm{copm}(a)=65$

$j=3, P=5, L=2\rho_0=1$. すなわち $a=5^3\cdot 2$. すると, $\mathrm{co}\varphi(a)=5^2\cdot 6=150, \mathrm{copm}(a)=145$
これらは大きすぎ.

2) $j=1$.
a). $\rho_0=1$. すなわち L は素数 $Q(P>Q)$ のとき,
$a=PQ$, $\mathrm{copm}(a)=P+Q-1-P=Q-1$. これを言い換えれば, 与えられた素数 Q について $\mathrm{copm}(a)=Q-1$ を満たす解は $a=PQ(P>Q)$ でありユークリッドの証明した結果によると 素数 $P(>Q)$ は無限にあるので, この解は無数にある.

b). $\rho_0=2$. このとき $L=4; a=4P$.

$$\mathrm{copm}(a)=2P+2-P=P+2.$$

$P=47,43,41,37,31,23,11,7,5,3$ とすると, それらに応じて
$\mathrm{copm}(a)=49,45,43,39,33,25,13,9,7,5$.
$a=4\cdot 31, 4\cdot 23, 4\cdot 11, 4\cdot 7, 4\cdot 5, 4\cdot 3$ に対応して $\mathrm{copm}(a)=33,25,13,9,7,5$.

c). $\rho_0=3$. このとき $L=9; a=9P$.

$$\mathrm{copm}(a)=3P+6-P=2P+6.$$

$P=23,11,7,5$ とすると, それに応じて $\mathrm{copm}(a)=52,28,20,16$.
$a=9\cdot 7, 9\cdot 5, 9\cdot 3$ に対応して $\mathrm{copm}(a)=9,7,5$.

d). $\rho_0=4$. このとき $L=8,6$.
$L=8, a=8P$

$$\mathrm{copm}(a)=4P+4-P=3P+4.$$

$P=13,11,7,5,3$ とすると, それに応じて $\mathrm{copm}(a)=43,37,25,19,13$.
$a=8\cdot 7, 8\cdot 5, 8\cdot 3$ に対応して $\mathrm{copm}(a)=25,19,13$.
$L=6, a=6P(P\geq 5)$

$$\mathrm{copm}(a)=4P+2-P=3P+2.$$

$P=17,13,11,7,5$ とすると, それに応じて $\mathrm{copm}(a)=53,41,35,23,17$.
$a=6\cdot 5, 6\cdot 3$ に対応して $\mathrm{copm}(a)=23,17$.

e). $\rho_0=5$. このとき $L=25; a=5^2P(P>5)$.

$$\mathrm{copm}(a)=5P+20-P=4P+20.$$

$P=11,7$ とすると, それに応じて $\mathrm{copm}(a)=64,48$. 大きすぎ.

f). $\rho_0=6$. このとき $L=10, a=10P(P>5)$.

$$\mathrm{copm}(a) = 6P + 4 - P = 5P + 4.$$

$P = 11, 7$ とすると, それに応じて $\mathrm{copm}(a) = 59, 39$. 大きすぎ.

g). $\rho_0 = 7$. このとき $L = 49, L = 15$.
$L = 49$ ならば $a = 7^2P, (P > 7)$.

$$\mathrm{copm}(a) = 7P + 8 - P = 6P + 8.$$

$P = 11$ とすると, それに応じて $\mathrm{copm}(a) = 108$. 大きすぎ.
$L = 15$ ならば $a = 15P(P > 5)$. $\rho_0 = 3 + 5 - 1 = 7$.

$$\mathrm{copm}(a) = 7P + 8 - P = 6P + 8.$$

$P = 7, 11$ に応じて $\mathrm{copm}(a) = 6P + 8 = 50, 74..$ 大きすぎ.

h). $\rho_0 = 8$. このとき $L = 12, 14, 16$.

$$\mathrm{copm}(a) = L + 8P - 8 - P = L + 7P - 8.$$

$L = 12$ とすると, $a = 12P(P > 3)$. $\mathrm{copm}(a) = 4 + 7P$.
$P = 5$ とすると,$\mathrm{copm}(a) = 39$. 大きすぎ.
$P = 7$ とすると,$\mathrm{copm}(a) = 63$. 大きすぎ.

$L = 14$ とすると,$\mathrm{copm}(a) = 6 + 7P$.
$P = 11$ とすると,$\mathrm{copm}(a) = 83$

$L = 16$ とすると, $a = 16P$. $\mathrm{copm}(a) = 8 + 7P$.
$P = 3, 5, 7$ とすると, それに応じて $\mathrm{copm}(a) = 29, 43, 57$. 大きすぎ.
i). $\rho_0 = 9$. このとき $L = 21, 27$.
$\mathrm{copm}(a) = 8P - 9 + L$.
$L = 21, a = 21P(P > 7)$ とすると, $\mathrm{copm}(a) = 12 + 8P$. $P = 11$ なら $\mathrm{copm}(a) = 100$. 大きすぎ.
$L = 27; a = 27P(P > 3)$ とすると, $\mathrm{copm}(a) = 18 + 8P$. $P = 5$ なら $\mathrm{copm}(a) = 67$. 大きすぎ.
j). $\rho_0 \geq 12$ のとき copm が最小になるのは, $P = 3, j = 1, L = 2^e, e \geq 5$ になるに違いない. $\mathrm{copm}(a) = 2^{2+1} - 3 \geq 2^6 - 3 = 64 - 3 = 61$. 大きすぎ.
以上の計算をまとめると次の表ができる.

表 5: a:合成数,q:素数; copm(a) の順

a	factor	$s(a)$	$\varphi(a)$	copm(a)
$2q$	$[2, q(q>2)]$	2	$(q-1)$	1
8	$[2^3]$	1	4	2
3q	$[3, q(q>3)]$	2	$2(q-1)$	2
5q	$[5, q(q>5)]$	2	$4(q-1)$	4
12	$[2^2, 3]$	2	4	5
16	$[2^4]$	1	8	6
27	$[3^3]$	1	18	6
7q	$[7, q(q>7)]$	2	$6(q-1)$	6
20	$[2^2, 5]$	2	8	7
18	$[2, 3^2]$	2	6	9
28	$[2^2, 7]$	2	12	9
11q	$[11, q(q>11)]$	2	$10(q-1)$	10
13q	$[13, q(q>13)]$	2	$12(q-1)$	12
24	$[2^3, 3]$	2	8	13
44	$[2^2, 11]$	2	20	13
32	$[2^5]$	1	16	14
52	$[2^2, 13]$	2	24	15
45	$[3^2, 5]$	2	24	16
17q	$[17, q(q>17)]$	2	$16(q-1)$	16
30	$[2, 3, 5]$	3	8	17
19q	$[19, q(q>19)]$	2	$18(q-1)$	18

表 6: a:合成数, q:素数;copm(a) の順

a	factor	$s(a)$	$\varphi(a)$	copm(a)
40	$[2^3, 5]$	2	16	19
68	$[2^2, 17]$	2	32	19
63	$[3^2, 7]$	2	36	20
125	$[5^3]$	1	100	20
36	$[2^2, 3^2]$	2	12	21
76	$[2^2, 19]$	2	36	21
23	$[23, q(q > 23)]$	2	$22(q-1)$	22
42	$[2, 3, 7]$	3	12	23
81	$[3^4]$	1	54	24
50	$[2, 5^2]$	2	20	25
56	$[2^3, 7]$	2	24	25
92	$[2^2, 23]$	2	44	25
99	$[3^2, 11]$	2	60	28
29q	$[29, q(q > 29)]$	2	$28(q-1)$	28
48	$[2^4, 3]$	2	16	29
64	$[2^6]$	1	32	30
75	$[3, 5^2]$	2	40	30
31	$[31, q(q > 31)]$	2	$30(q-1)$	30
116	$[2^2, 29]$	2	56	31
117	$[3^2, 13]$	2	72	32
54	$[2, 3^3]$	2	18	33
124	$[2^2, 31]$	2	60	33
66	$[2, 3, 11]$	3	20	35