数学の研究を始めよう 2016/nov
オイラーの余関数とは何だろう, 新しい不変数 copm ;
後編

飯高 茂

平成 28 年 8 月 23 日

1　オイラー余関数の平方根評価

a が素数でないなら $a \geq \varphi(a) + \sqrt{a}$. かつ $a = \varphi(a) + \sqrt{a}$ である条件は a が素数の平方, すなわち $a = P^2$.

そこで $\mathrm{co}\varphi(a) = a - \varphi(a)$ とおきこれをオイラー余関数という. これを用いると

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, $a=P^jL, (P>\mathrm{Maxp}(L))$ 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.

2 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.

したがって, 双子素数について, 調べてみよう.

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 1: $P = L + 2$; 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 2: $P = L + 4$; 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

3　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.

$N = 4$ ができればいとこ素数が無限にあることが示されるのだが. 証明はできるものではないだろう.

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」と言ってわれわれ若い者を叱咤激励した.

4　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, 平方根ではなくより直接に評価をしてみよう. 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,$a = P^j L(\ P > \mathrm{Maxp}(L))$ 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 3: 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 4: 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