

数学の研究を始めよう (10)

オイラー関数の1次関係式

飯高 茂

平成 25 年 10 月 14 日

1 オイラー関数 $\varphi(a)$ は2のべきが得意

$a = 2^e, (e > 0)$ ならば $\varphi(a) = \varphi(2^e) = 2^{e-1}$ なので $2\varphi(a) = a$ を満たす。しかもこの関係を満たす自然数は2のべきしかない。このことは容易にわかる。

類似した結果を約数の和関数 $\sigma(a)$ を用いて考えるとき $a = 2^e, e > 0$ ならば

$$\sigma(a) = \sigma(2^e) = 2^{e+1} - 1 = 2a - 1$$

を得るが、 $\sigma(a) = 2a - 1$ を満たす a は2のべきしかないことは証明されていない。

$\sigma(a) = 2a$ を満たす自然数は完全数と呼ばれるが $\sigma(a) = 2a - 1$ を満たす自然数は概完全数と呼ばれる。これは2のべきしかないと思われが証明は無い。

$\sigma(a)$ で得られた結果を $\varphi(a)$ を用いて定式化し、そこで類似した良い結論を期待するのは甘い研究態度である。しかしとりあえずこの立場でやってみよう。

2 $a - 2\varphi(a)$ の値

$a - 2\varphi(a) = 0$ の場合について a の構造は完全に分かったので、これを平行移動してみよう。すなわち整数 x に対して $a - 2\varphi(a)$ の値が x になる a とその素因数分解を求めてみよう。ただし、 $x \geq -1$ に制限している。実は $x < -1$ の場合、 x は奇数になり、その場合の a はどれも数が少ない。率直に言ってあまり面白くない。このように著者は思うのだが読者は独自の考えをもって研究すればよく、それによってまったく新しい研究ができるかもしれない。

表 1: $a - 2\varphi(a)$ の値

a	素因数分解	$\varphi(a)$	$a - 2\varphi(a)$
3	[3]	2	-1
15	[3,5]	8	-1
255	[3,5,17]	128	-1
2	[2]	1	0
4	[2,2]	2	0
8	[2,2,2]	4	0
16	[2,2,2,2]	8	0
32	[2,2,2,2,2]	16	0
64	[2,2,2,2,2,2]	32	0
128	[2,2,2,2,2,2,2]	64	0
256	[2,2,2,2,2,2,2,2]	128	0
512	[2,2,2,2,2,2,2,2,2]	256	0
6	[2,3]	2	2
10	[2,5]	4	2
14	[2,7]	6	2
22	[2,11]	10	2
26	[2,13]	12	2
34	[2,17]	16	2
38	[2,19]	18	2
46	[2,23]	22	2

表 2: $a - 2\varphi(a)$ の値; 続き

a	素因数分解	$\varphi(a)$	$a - 2\varphi(a)$
195	[3,5,13]	96	3
12	[2,2,3]	4	4
20	[2,2,5]	8	4
28	[2,2,7]	12	4
44	[2,2,11]	20	4
52	[2,2,13]	24	4
68	[2,2,17]	32	4
76	[2,2,19]	36	4
92	[2,2,23]	44	4
165	[3,5,11]	80	5
18	[2,3,3]	6	6
24	[2,2,2,3]	8	8
40	[2,2,2,5]	16	8
56	[2,2,2,7]	24	8
88	[2,2,2,11]	40	8
104	[2,2,2,13]	48	8
136	[2,2,2,17]	64	8
152	[2,2,2,19]	72	8
184	[2,2,2,23]	88	8

パソコン君が作ってくれた表を見つめて与えられた x に対してその解が複数個ある場合に注目しよう. x によっては $a - 2\varphi(a) = x$ の解が無限に出て来ることに注目したい. この表を観察すると興味ある性質がいくつもつけられる. 未知の定理が見えてくるように思われる.

たとえばみると, 油田の鉱区を買ってから採掘を始めるような話である. x 番地の鉱区の権利を得た人は, $x = 0, 2, 4, 8$ などから解 (油) が無限に出て来るから大当たりである.

しかし $x = 6$ なら解は 1 つしかないようだ. 大損の場合であろう.

さて表を観察した結果から見えてきたことを書き出してみた.

- 〈1〉 $x = -1$ のときの表には感動せざるを得ない. 以下ですぐ調べる.
- 〈2〉 $x = 0$ のときは $a = 2^e$. すなわち 2 のべきは無限に多くの解がある.(11 月号で示した)
- 〈3〉 $x = 2, 4, 8$ のときは $a = 2^e p$, (p は奇素数). この場合 無限個の解がある.
- 〈4〉 $x = 6$ のときは $a = 18$ が 唯一の解.

3 $a - 2\varphi(a) = -1$ のとき

このときわずか 3 個の解しか表にでていないが, $255 = 3 \times 5 \times 17$ に注目したい. 3, 5, 17 は, 作図可能な正 p (素数) 多角形 (ガウス) の p なのである.

4 正 p 多角形の作図問題

オイラー関数の研究からガウスの研究した作図可能な正多角形の角数 p が出てきた。さらにフェルマー数も関わってくる。これにはびっくりせざるをえない。

コンパスと定規だけで作図をすることは、古代ギリシャ人が考えて決めたことである。正三角形や正五角形をコンパスと定規で作図できることは紀元前から彼らによって知られていたが正 17 角形も (コンパスと定規で; 以下このフレーズは略する) 作図出来ることを 18 世紀の末に少年ガウスが示した。これは本質的な点でユークリッドの幾何学を近世数学が乗り越えた事件とされる。しかもその証明は、幾何学的ではなく純数論的なものであった。

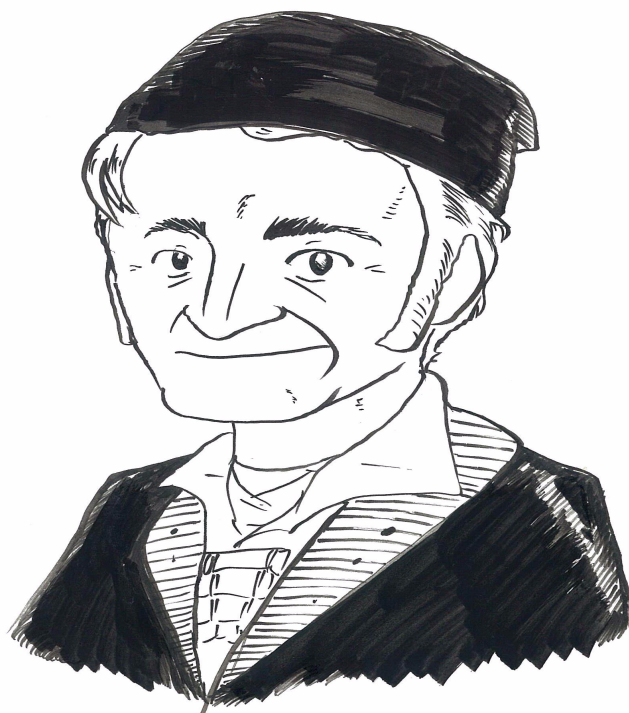


図 1: ガウス (Carolus Fridericus Gauss, 1777 – 1855) イラストは飯高順による

素数 $p > 2$ に対して原点中心の単位円に内接する正 p 多角形を点 $(1,0)$ を始点として考える。ここで平面をガウス平面 (複素平面) と見て点と複素数を同一視する。

$(1,0)$ は複素数 $1 + 0i$ であり、正 p 多角形の点 $(1,0)$ の次の頂点に対応する点を複素数 ζ で示すと正 p 多角形の頂点という条件によって $\zeta^p = 1$ を満たす。

すなわち ζ は $X^p - 1 = 0$ の根である。したがって $\zeta = \cos(2\pi/p) + i \sin(2\pi/p)$ 。

多項式 $X^p - 1$ を有理数係数の多項式の環において既約多項式分解すると

$$X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \cdots + 1)$$

となる。ここで $F(X) = X^{p-1} + X^{p-2} + \cdots + 1$ は有理数係数の多項式として既約であり、その定める有理数体上のガロア群は p 個の元からなる有限体 $\mathbb{F}_p$ の乗法群 $\mathbb{F}_p^*$ であってこれは $p-1$ 個

の元からなる巡回群である。体の理論によると、有理数体 $\mathbb{Q}$ に ζ を付け加えてできた体 $K = \mathbb{Q}(\zeta)$ は $\mathbb{Q}$ 上 $p-1$ 次元のベクトル空間になる。

さて、定規で作図するとき 1 次の関係しか作れない。しかしコンパスを使えば平方根の作図が可能になる。したがって、 ζ の示す点が作図できるためには、 $\mathbb{Q}$ から始めて平方根を作りそれを付け加えることを r 回繰り返すことで K ができないといけな。平方根を付け加える度に体の拡大次数は 2 倍になるので最終的な体 K の $\mathbb{Q}$ に対する拡大次数が 2^r であり、 $p-1=2^r$ となる。

これより $p=2^r+1$ をえるが、 2^r+1 が素数になるためには r を素因数分解するとき奇数の成分があつてはならないので $r=2^n$ と書けなければならない。だから $p=2^{2^n}+1$ となる。

5 フェルマー数

$f_n = 2^{2^n}, F_n = f_n + 1$ において数列 $\{f_n\}$ と $\{F_n\}$ を考える。 F_n をフェルマー数という。ただし $n=0$ から始める。

定義により、

$$f_n^2 = (2^{2^n})^2 = 2^{2^{n+1}} = f_{n+1}.$$

ゆえに

$$f_n^2 = f_{n+1}.$$

表 3: フェルマー素数

n	f_n	F_n
0	2	3
1	4	5
2	16	17
3	256	257
4	65536	65537

$n=0,1,2,3,4$ のときのフェルマー数はみな素数である。そのとき フェルマー素数という。

フェルマーは $n \geq 5$ のときも F_n は素数であると思ったがそれは正しくなかった。

実際 $F_5 = 4294967297$ はオイラーにより素因数分解された:

$$4294967297 = 641 \times 6700417$$

皮肉なことに $n \geq 5$ のとき素数になるフェルマー数 (すなわち、フェルマー素数) は今に至るまで 1 つも発見されていない。

5.1 フェルマー数の積

フェルマー数の積を a_n , すなわち $a_n = F_0 F_1 F_2 \cdots F_n$ とおく。すると、定義から

$$a_{n+1} = F_0 F_1 F_2 \cdots F_n F_{n+1} = a_n F_{n+1}$$

なので $a_{n+1} = a_n F_{n+1}$ 。

5.2 補題

補題 1 $a_n = f_{n+1} - 1$.

これを帰納法で示す.

$n = 0$ なら成立. 実際, $a_0 = F_0 = 2^1 + 1 = 3, f_1 - 1 = 4 - 1 = 3$.

$n > 0$ のとき, $n - 1$ の場合を仮定すると, $a_{n-1} = f_n - 1, F_n = f_n + 1$ に注意して

$$a_n = a_{n-1}F_n = (f_n - 1)(f_n + 1) = (f_n)^2 - 1 = f_{n+1} - 1.$$

5.3 $a_n - 2\varphi(a_n) = -1$ の証明

$n \leq 4$ について F_n は素数なので $\varphi(F_n) = f_n$ により $b_n = \varphi(a_n)$ とおくと

$$b_n = \varphi(a_{n-1})\varphi(F_n) = \varphi(a_{n-1})f_n = f_0f_1f_2 \cdots f_n$$

となる. このとき

$$b_n = 2^{1+2+2^2+\cdots+2^n} = 2^{2^{n+1}-1}$$

により

$$2 \times b_n = 2^{2^{n+1}} = f_{n+1} = a_n + 1$$

を満たす. よって,

$$a_n - 2\varphi(a_n) = a_n - 2b_n = -1.$$

表 4: フェルマー素数の積

n	a_n	素因数分解	b_n
0	3	[3]	2
1	15	[3,5]	8
2	255	[3,5,17]	128
3	65535	[3,5,17,257]	32768
4	4294967295	[3,5,17,257, 65537]	2147483648

6 未解決の課題

研究課題

$$a - 2\varphi(a) = -1 \tag{1}$$

を満たす a は上の表に載っているものだけか?

これは難しい問題であろう. しかし分かることが少しある.

式 (1) を満たすとき, a の素因子の指数は 1 である. このことを示そう.

実際, a の素因子 p について a の p での指数を e と書く. $e > 1$ とすると $\varphi(a)$ も p の倍数なので $a - 2\varphi(a)$ も p の倍数になり式 (1) に矛盾する.

さて $a = 2\varphi(a) - 1$ なので a は奇数である. したがって, a は異なる素数 $p_1, p_2, \dots, p_r$ の積であり $a = \prod_{j=1}^r p_j$, $\varphi(a) = \prod_{j=1}^r (p_j - 1)$ と書ける. これらが $a = 2\varphi(a) - 1$ を満たすという条件をうまく使うことが難しい.

練習課題 $a = p_1 p_2 (p_1 < p_2)$ が $a = 2\varphi(a) - 1$ を満たすとき $(p_1 - 2)(p_2 - 2) = 3, p_1 = 3, p_2 = 5$ を示せ.

$a = p_1 p_2 p_3 (p_1 < p_2 < p_3)$ の場合はどうか.

6.1 証明への一步一步

i. a は 3 を素因数に持つと仮定する.

$a = 3k_0$ と書くとき, k_0 は 3 で割れないから式 (1) に注意して $2\varphi(a) = 2\varphi(3k_0) = 4\varphi(k_0)$.

一方 $2\varphi(a) = a + 1 = 3k_0 + 1$. ゆえに

$$3k_0 + 1 = 4\varphi(k_0). \quad (2)$$

$k_0 = 1$ のとき, $a = 3, 2\varphi(a) - 1 = 4 - 1 = 3$ なので $a = 3$ は解.

ii. k_0 が 5 を素因数に持つと仮定する. $k_0 = 5k_1$ とおくと,

$$4\varphi(k_0) = 4\varphi(5k_1) = 4^2\varphi(k_1)$$

と $3k_0 + 1 = 15k_1 + 1$ により

$$15k_1 + 1 = 4^2\varphi(k_1).$$

$k_1 = 1$ のとき, $a = 15, 2\varphi(a) - 1 = 2 \times 2 \times 4 - 1 = 15$ なので $a = 3 \times 5$ は解.

ゆえに $a_1 = 15, f_2 = 4^2$. ここで $a_1 = f_2 - 1$.

$k_1 > 1$ のとき, k_1 の最小素因数を p とすると $k_1 = pk_2$ と書けて $15k_1 + 1 = 15pk_2 + 1$. さらに

$$15k_1 + 1 = 4^2\varphi(k_1) = 4^2\varphi(pk_2) = 4^2 \times (p-1)\varphi(k_2) \leq 4^2 \times (p-1)k_2$$

によって

$$15pk_2 + 1 < 4^2 \times (p-1)k_2.$$

これを变形して

$$1 < (4^2 \times (p-1) - 15p)k_2 = (p-16)k_2.$$

iii. p は 16 以上の素数なので $p = 17$ とおいてみる. すると $k_1 = 17k_2, a = 3 \times 5 \times 17 \times k_2$ によって,

$$2\varphi(a) = 2\varphi(3 \times 5 \times 17 \times k_2) = 2 \times 2 \times 4 \times 16 \times \varphi(k_2).$$

よって $a - 2\varphi(a) = -1$ を思い出すと

$$3 \times 5 \times 17 \times k_2 = 2 \times 2 \times 4 \times 16 \times \varphi(k_2) - 1.$$

ゆえに $a_2 = 3 \times 5 \times 17, f_3 = 4^2 \times 16$ を思い出せば

$$a_2 k_2 = f_3 \varphi(k_2) - 1$$

と書ける.

$k_2 = 1$ のとき $a_2 = f_3 - 1 = 255$. これより $2\varphi(a_2) = f_3 = a_2 + 1$ になり $a_2 = 15 \times 17$ が解になる.

iv. $k_2 > 1$ のとき k_2 の最小素因数を p とすると $k_2 = pk_3$ と書けて

$$a_2 k_2 = a_2 p k_3 = f_3 \varphi(k_2) - 1 = f_3 \varphi(pk_3) - 1 = f_3(p-1)\varphi(k_3) - 1 < f_3(p-1)k_3 - 1.$$

これより

$$1 < -a_2 p k_3 + f_3(p-1)k_3 = (-a_2 p + f_3(p-1))k_3 = (p - f_3)k_3. \quad (3)$$

$256 = f_3 < p$ であり $F_3 = 257$ は素数なので $p = F_3$ とおく. $a_3 = a_2 \cdot F_3$ なので

$$a_3 k_3 = a_2 F_3 k_3 = (f_3)^2 \varphi(k_3) - 1 = f_4 \varphi(k_3) - 1.$$

$k_3 = 1$ のとき a_3 が解.

v. $k_3 > 1$ のとき k_3 の最小素因数を p とすると $k_3 = pk_4$ と書けて

$$a_3 p k_4 = f_4 \varphi(pk_4) - 1 = f_4(p-1)\varphi(k_4) - 1 < f_4(p-1)k_4 - 1.$$

$$1 < -a_3 p k_4 + f_4(p-1)k_4 = (-a_3 p + f_4(p-1))k_4 = (p - f_4)k_4. \quad (4)$$

$p - f_4 > 0$ により $p \geq f_4 + 1$. $F_4 = f_4 + 1$ は素数なので $p = F_4$ とおけば

$$a_4 k_4 = a_3 F_4 k_4 = f_4(p-1)\varphi(k_4) - 1.$$

$k_4 = 1$ とおけば $a_4 = F_0 F_1 F_2 F_3 F_4$ が解になる.

$F_5 = f_5 + 1$ は素数ではない. したがってここで終わらざるを得ない.

6.2 反省

ここでは, 各段階で最小の素数を選ぶことにしたらうまく行った. これしかできないことを言いたい.

たとえば最初に 5 を選んだら議論が進まないことを言え良いのである. ここで著者は再び冷温停止状態に至った. この困難をのり超える力を読者に期待する.

7 $x = 2, 4, 8$ のとき

先月号において $x = 2^e$ の場合 が扱われていて、そのときの解は $a = 2^e p$ (p は奇素数). したがって無限個の分かりやすい解があり、しかもそれだけが解なのである.

7.1 $x = 6$ のとき

$a = 2(\varphi(a) + 3)$ なので $k = \varphi(a) + 3$ とおくと, $a = 2k$.

したがって,

$$\varphi(a) = \varphi(2k) = k - 3.$$

$a = 2k, k = 2^e L (L : \text{奇数})$ と書く.

$$\varphi(2k) = \varphi(2^{e+1}L) = 2^e \varphi(L) = 2^{e+1}L - 3.$$

によって

$$3 = 2^{e+1}L - 2^e \varphi(L) = 2^e (2L - \varphi(L)).$$

したがって $e = 0$. よって $k = L$ は奇数で $\varphi(2k) = k - 3$ を満たす. 乗法性によって $\varphi(2k) = \varphi(k)$ を得るから $\varphi(k) = k - 3$. よって,

$$k - \varphi(k) = 3.$$

k が素数でも素数の平方でもない場合は, 5月号で扱った $k - \varphi(k)$ の値の研究結果を使う. これによれば $k - \varphi(k) = 3$ なら $k = 9$ になる. よって, $a = 2 \times 9 = 18$.

油田を掘る話でたとえば $x = 6$ の地点では $a = 18$ しか出ないことが証明されたので, もう掘る価値がない, ということになる.

8 $x = 5, 3$ のとき

$x = 5$ のときは 解 $a = 165$ があることはわかっている. しかしそれを証明しようと私は試みたが手も足も出ない. 証明できない以上, 別の解が出てくるかもしれないと思ってパソコン君に探索を続けてもらったら $a = 64005 = 3 \times 5 \times 17 \times 251$ が解であることがわかった.

$x = 3$ の場合は解 $a = 195$ がある. $x = 5$ のときより大きな解なので, 他の解があるかどうかの問題は困難さが増しているようだ.

9 $x = 1$ のとき

$a - 2\varphi(a) = 1$ の解があるとすればそれは相異なる素数の積である. パソコン君によれば解は多分存在しない. しかし証明ができない. 読者への重い課題としよう.

$a - 2\varphi(a) = -1, 0, 1; \sigma(a) - 2a = -1, 0, 1$ についての既知の結果を表にしてみた.

表 5: $a - 2\varphi(a) = -1, 0, 1; \sigma(a) - 2a = -1, 0, 1$

$a - 2\varphi(a)$	a	$\sigma(a) - 2a$	a
-1	フェルマー素数に関連	-1	多分 2^e
0	2^e	0	完全数
1	多分無い	1	多分無い

$\sigma(a) - 2a = -1, 0, 1$ に応じて a をそれぞれ 概完全数 (almost perfect number), 完全数 (perfect number) 準完全数 (pseudo perfect number) と呼ぶ.

準完全数は無い, というのが予想なのだそうです.

10 歯を食いしばって 9 から 16 まで

$a - 2\varphi(a) = x$ の解を探すことを $x = 9, 10, 11, \dots, 15$ の場合に試みた.

$x = 9$ の解は面白そうである.

表 6: $a - 2\varphi(a) = 9$ の解

a	素因数分解	$\varphi(a)$
105	$[3, 5, 7]$	48
585	$[3^2, 5, 13]$	288
15561	$[3^2, 7, 13, 19]$	7776

$a < 200000$ の範囲の解は上記の通り. 何となく素性のわかりそうな解である. わかることを列挙してみる.

〈1〉 a は奇数

〈2〉 a の 3 の指数は 2 以下

〈3〉 a の 3 以外の奇素数の指数は 1 以下

研究課題

上のことを証明せよ.

少しでもわかることがあるとうれしい. だからこれらのどれかができれば研究へ意欲が沸くことであろう.

10.1 $a - 2\varphi(a) = 10$ を満たす a

$x = 10$ のとき $a < 200000$ における解は $a = 50$ だけだとパソコン君が言うのでその証明を試みた.

$a = 2\varphi(a) + 10$ なので a は偶数. $a = 2^e k, (k : \text{奇数})$ とおけば

$$2^e k = 2^e \varphi(k) + 10.$$

これより, $e = 1$ になり $k = \varphi(k) + 5$.

$k - \varphi(k) = 5$ を満たす k は 25 のみ. よって $a = 50$.

10.2 $a - 2\varphi(a) = x$ を満たす $x = 11, 13$

$x = 11, 13$ のとき $a - 2\varphi(a) = x$ を満たす a は見つかっていない. しかし, 証明はまだ.

10.3 $a - 2\varphi(a) = 12$ を満たす場合

$x = 12$ のとき $a < 200000$ の範囲で 解は $a = 36$ のみ.

この場合は, $x = 10$ のときと同様にして $a = 2^e k, (k : \text{奇数})$ とおけば

$$2^e k = 2^e \varphi(k) + 12.$$

をえる. ここで $e = 2$ のみ. すると $k - \varphi(k) = 3$. k は素数でないから $3 = k - \varphi(k) \geq \sqrt{k}$ が成り立つ. よって $k \leq 9$. これより $k = 9$ がわかり $a = 2^e \times 9 = 36$ となる.

10.4 $a - 2\varphi(a) = 14$ を満たす場合

表 7: $a - 2\varphi(a) = 14$ を満たす a

a	素因数分解	$\varphi(a)$
30	$[2, 3, 5]$	8
98	$[2, 7^2]$	42

$x = 14$ の場合, $x = 10$ のときと同様にして $a = 2k$ と書けば $k - \varphi(k) = 7$.

k は素数でないから, $7 = k - \varphi(k) \geq \sqrt{k}$.

よって $k \leq 7^2$. 素数べきが最大値となる可能性があり, 49 が 1 つの解でこのとき $a = 98$.

これ以外なら k は奇数で, $k < 47$. $k = 15$ が残りの解.

10.5 $a - 2\varphi(a) = 15$ を満たす a

$x = 15$ では 解が急にたくさん出てきた.

表 8: $a - 2\varphi(a) = 15$ を満たす a

a	素因数分解	$\varphi(a)$
495	$[3^2, 5, 11]$	240
975	$[3, 5^2, 13]$	480
61455	$[3, 5, 17, 241]$	30720
192015	$[3^2, 5, 17, 251]$	96000

10.6 省察

$a - 2\varphi(a) = x$ の解の決定問題では $x = 2^e$ なら解はすべて求まる.
 x が偶数 $2L$ なら $a = 2^e k$ ($e > 0, k$: 奇数) とおけて

$$2^e k = 2^e \varphi(k) + 2L.$$

与えられた具体的な L に対して k を求めることは個々にできるだろう.
 しかしながら x が奇数のとき, 超えがたい障壁の存在を感じる.

11 2 と 3 のべきの場合

a が 2 と 3 のべきの場合, すなわち $a = 2^\varepsilon \times 3^\eta$ ($\varepsilon > 0, \eta > 0$) と書けるとしよう.
 $\varphi(a) = \varphi(2^\varepsilon 3^\eta) = 2^{\varepsilon-1} 3^{\eta-1}$ によって

$$3\varphi(a) = 3 \times 2^{\varepsilon-1} 3^{\eta-1} = 2^{\varepsilon} 3^{\eta} = a.$$

よってオイラー関数の 1 次関係式が次のように得られた.

$$3\varphi(a) = a.$$

この式を a について解こう.

a は 3 の倍数なので $a = 3^f L$ (L は 3 で割れない) とおく.

$$3\varphi(a) = 3\varphi(3^f L) = 3\varphi(3^f)\varphi(L) = 2 \times 3^f \varphi(L).$$

一方 $a = 3^f L$ なので条件式 $3\varphi(a) = a$ によって $2 \times 3^f \varphi(L) = 3^f L$ なので $2\varphi(L) = L$ を得る. 前項の結果によって $L = 2^e$. 結局 $a = 3^f L = 2^e 3^f$ となって次の定理が証明された.

定理 1 $a = 2^e 3^f$ ($e, f > 0$) とかける必要十分条件は $3\varphi(a) = a$.

12 $a - 3\varphi(a) = x$

今度は $a - 3\varphi(a) = 0$ を平行移動してみよう. どんな結果が出るだろうか. 見当もつかないのでパソコン君に頼んで次の表を作ってもらった.

表 9: $a - 3\varphi(a) = x$

a	素因数分解	$a - 3\varphi(a)$
6	[2,3]	0
30	[2,3,5]	6
42	[2,3,7]	6
66	[2,3,11]	6
78	[2,3,13]	6
102	[2,3,17]	6
60	[2,2,3,5]	12
84	[2,2,3,7]	12
132	[2,2,3,11]	12
156	[2,2,3,13]	12
204	[2,2,3,17]	12
90	[2,3,3,5]	18
126	[2,3,3,7]	18
198	[2,3,3,11]	18
234	[2,3,3,13]	18
306	[2,3,3,17]	18
120	[2,2,2,3,5]	24
168	[2,2,2,3,7]	24
264	[2,2,2,3,11]	24
312	[2,2,2,3,13]	24
408	[2,2,2,3,17]	24

12.1 24 までが幸福な時

$x = 0$ のとき a は 2 と 3 のべきなので代表的な 6 だけあげておいた. 解のある場合の x は 6, 12, 18, 24, $\dots$ である. 解のある場合には

$$6 = 2 \times 3, 12 = 2^2 \times 3, 18 = 2 \times 3^2, 24 = 2^3 \times 3$$

なのでこれらは 2 と 3 のべきである.

研究課題

$x \leq 24$ で 2 と 3 のべきの場合, $a - 3\varphi(a) = x$ の解は xp と書けることは正しいか. 正しければ証明を, 誤りなら反例を与えよ.

13 2 と 3 のべき

$m = 2^\varepsilon 3^\zeta$, ($\varepsilon > 0, \zeta > 0$) とおく. p は 2, 3 と異なる素数とすると $a = mp$ とおけば

$$3\varphi(a) = 3\varphi(mp) = 3\varphi(m)\varphi(p) = m\varphi(p) = m(p-1) = a - m.$$

そこで、2 より大きい自然数 a が

$$a - 3\varphi(a) = 2^\varepsilon 3^\zeta \quad (\varepsilon > 0, \zeta > 0). \quad (5)$$

を満たすとしよう.

$a > 2$ ならばオイラー関数 $\varphi(a)$ は偶数なので $a = 3\varphi(a) + 2^\varepsilon 3^\zeta$ も偶数. そこで $a = 2^e L$, ($L > 1$: 奇数) とおくと $3\varphi(a) = 3\varphi(2^e L) = 3 \times 2^{e-1} \varphi(L)$,

$$a - 3\varphi(a) = 2^e L - 3 \times 2^{e-1} \varphi(L) / 2 = 2^\varepsilon 3^\zeta.$$

$\varphi(L)/2$ は整数なので

$$L - 3\varphi(L)/2 = 2^{\varepsilon-e} 3^\zeta.$$

i. $\varepsilon - e = 0$ のとき.

$L - 3\varphi(L)/2 = 3^\zeta$ なので L は 3 の倍数. そこで $L = 3^f M$, $3 \nmid M$ とおくと

$$3^f M - 3^f \varphi(M) = 3^\zeta.$$

これから $\eta = \zeta - f$ とおけば

$$M - \varphi(M) = 3^\eta.$$

$0 < \eta, M > 1$ なら $\eta \geq 4$. これは $a - \varphi(a)$ の値の評価からすぐ証明できる.

$\eta = 0$ なら $M - \varphi(M) = 1$. よって M は素数 p であって $a = 2^e L = 2^e 3^f p$.

ii. $\varepsilon - e > 0$ のとき.

$u = \varepsilon - e$ とおけば $L - 3\varphi(L)/2 = 2^u 3^\zeta$.

L は奇数で、 $2^u 3^\zeta$ は偶数なので $3\varphi(L)/2$ は奇数. したがって $\varphi(L)/2$ は奇数なので、 L の素因子はすべて奇数で素因子はただ 1 つである.

よって、 $L = p^g$ と書ける. ここで $\varphi(L)/2 = p^{g-1}(p-1)/2 = p^{g-1}v$, ($p = 1 + 2v$, v : 奇数,) となる. したがって

$$p^g - 3p^{g-1}v = 2^u 3^\zeta.$$

よって、 p^g は 3 の倍数なので、 $p = 3$. 故に $a = 2^e L = 2^e 3^g$. このとき $a - 3\varphi(a) = 0$. これは矛盾. これを定理とする.

定理 2 $x = 2^e 3^f$ ($e, f > 0, f \leq 3$) $a = 3\varphi(a) + x$ の解は xp . ここで $p \geq 5$ は素数.

13.1 計算例

$x = 2 \times 3^3, 2 \times 3^4$ の場合の計算をパソコン君にしてもらった.

* はエイリアン解を示す.

表 10: $a - 3\varphi(a) = 2 \times 3^3$ の解

a	素因数分解	$\varphi(a)$
270	$[2, 3^3, 5]$	72
378	$[2, 3^3, 7]$	108
594	$[2, 3^3, 11]$	180
702	$[2, 3^3, 13]$	216
918	$[2, 3^3, 17]$	288
1026	$[2, 3^3, 19]$	324
1242	$[2, 3^3, 23]$	396
1566	$[2, 3^3, 29]$	504
1674	$[2, 3^3, 31]$	540
1998	$[2, 3^3, 37]$	648

表 11: $a - 3\varphi(a) = 2 \times 3^4$ の解

a	素因数分解	$\varphi(a)$
690 *	$[2, 3, 5, 23]$	176
810	$[2, 3^4, 5]$	216
1122 *	$[2, 3, 11, 17]$	320
1134	$[2, 3^4, 7]$	324
1782	$[2, 3^4, 11]$	540
2106	$[2, 3^4, 13]$	648
2754	$[2, 3^4, 17]$	864
3078	$[2, 3^4, 19]$	972
3726	$[2, 3^4, 23]$	1188
4698	$[2, 3^4, 29]$	1512

14 25 を超えると荒野が

パソコン君は 24 までは幸福な時でそれを過ぎると例外が多数出てくる荒野になると言う.

$a < 2001$ までは情報として不完全なので $x = 26$ から $x = 41$ について $a = 100000$ までの解を調べた.

表 12: $a - 3\varphi(a) = x, x \geq 26, x \neq 36, 48$

a	素因数分解	$\varphi(a)$	$a - 3\varphi(a) = x$
1610	[2,5,7,23]	528	26
4060	[2,2,5,7,29]	1344	28
150	[2,3,5,5]	40	30
1330	[2,5,7,19]	432	34
1190	[2,5,7,17]	384	38
8680	[2,2,2,5,7,31]	2880	40