高校生もわかる数学の研究 (書泉での講義)
完全数超入門

飯高 茂

2020/2/21

1　はじめに

今回は新入生がいることを期待して, 初めから説明することにした. しかしベテランの方からみても興味のあるような導入にする予定である.

2　完全数の定義

自然数 a に対しその約数の和を $\sigma(a)$ と書き, これを関数と見てユークリッド関数という.
$\sigma(a) = 2a$ を満たす a を完全数という.

命題 1 $a = 2^e$ とおく. $q = \sigma(a) = 2^{e+1} - 1$ を素数と仮定すると, $\alpha = aq$ は完全数になる.

Proof
$\sigma(a) = 2^{e+1} - 1$ を素数としてこれを q とおき, $\alpha = aq$ と書くと

$$\sigma(\alpha) = \sigma(a)\sigma(q) = q(q+1) = q(2^{e+1}) = 2q2^e = 2\alpha.$$

よって,$\sigma(\alpha) = 2\alpha$.
q.e.d.

メルセンヌ素数

$q = 2^{e+1} - 1$ が素数のとき, メルセンヌ素数という.
したがって, 完全数は 2 べきとメルセンヌ素数の積に分解される.
4 世紀の人, ヤンブリコスはこの逆, 完全数はユークリッドの完全数に限るのではないか, と考えた.
18 世紀になって, オイラーは偶数の完全数はユークリッドの完全数になることの証明に成功した.

2019 年現在 51 個もの完全数が発見されているが奇数の完全数は見つかっていない. それゆえ奇数完全数は存在しないだろうと想像されているが, 証明はできていない.

2000 年以上に亘って解決がつかない問題はほかにはない. 完全数に関しては, 定義はわかりやすいが証明ができない問題が数限りなくあるというところに大きな魅力がある.

3　完全数の定理

オイラーの定理の証明に入る前に次の結果に注目する.

分数について

Euler は次の事実に注目する.

補題 1 (既約分数の原理) $\frac{a}{b}=\frac{c}{d}$ について, $\frac{a}{b}$ が既約分数形と仮定する, 言い換えれば a,b は互いに素. ある 自然数 k があり, $c=ak, d=bk$ となる

通常は $\frac{a}{b}$ が既約分数と仮定するのだが, . 既約分数の概念は分数については定められないことに今回初めて気がついた.

定義 1 分数が等しい $\frac{a}{b}=\frac{c}{d}$ とは $ad=bc$ のことである.

したがって $\frac{c}{d}$ が 既約分数である, は意味をなさない.

そこで, 記号は同じだが, 分数形という概念を導入する.

定義 2 分数形が等しい $\frac{a}{b}=\frac{c}{d}$ とは $a=c, b=d$ のことと定義する.

分数形 $\frac{a}{b}$ の分母は b で分子は a である. これは, 分母, 分子は分数形に関して定義される概念である.

数学教育上分数の概念が難しい理由の 1 つは, 分数と分数形を区別してこないことにあったのであろう.

例えば, 始点が定まっている以上位置ベクトルは単なる有向線分であって, ベクトルとは言えない.

束縛ベクトルは有向線分, 自由ベクトルは本物のベクトル.

ベクトルを中国語では向量という. 向きと量としての数が組み合わされた造語である.

既約分数の原理の証明は一見にして簡単である. に代入すると

Proof 1) 分数形 $\frac{c}{d}$ の分母, 分子の GCD= δ で割ると, $c'=c/\delta, d'=d/\delta$. $\frac{a}{b}=\frac{c'}{d'}$. 左右の分数形が既約分数形なので, $a=c', b=d'$. そこで $k=\delta$ とおけばよい.

2) (別の証明)

$ad = bc$ かつ a, b は互いに素. 仮定により $a|bc$ より $a|c$. ゆえに $c = ak$. $ad = bc$ に代入すると $d = bk$.

q.e.d.

3.1 Euler

定理 1 (Euler) 偶数の完全数 a は素数 $p = 2^{e+1} - 1$ によって $a = 2^e p$ と書ける.

Proof

$\sigma(a) = 2a$ に対して a:偶数 を仮定する.

$a = 2^e L, (L : odd)$ と書くと, $N = \sigma(2^e) = 2^{e+1} - 1$ を使って, $\sigma(a) = \sigma(2^e L) = N\sigma(L), 2a = 2^{e+1}L = (N+1)L$ なので,

$\sigma(a) = 2a$ を用いると, $N\sigma(L) = (N+1)L$.

$N\sigma(L) = (N+1)L$ を分数に直す. $\dfrac{N+1}{N} = \dfrac{\sigma(L)}{L}$

$\dfrac{N+1}{N}$ は既約分数形なので ある 自然数 k があり, $\sigma(L) = k(N+1), L = kN$ となる.

$L = kN$ は k, N が L の約数を意味する.

1. $k = 1$ とすると, $L = kN = N$ かつ $\sigma(L) = k(N+1) = N + 1 = L + 1$. よって, L は素数だから, p とおくと,$L = N$ により, $p = L = N = 2^{e+1} - 1$. $a = 2^e L = 2^e p$.

2. $k > 1$ とすると, L の約数には, $1, k, L(= kN)$. があるので, かつ $\sigma(L) \geq 1 + k + L = k(N+1) = N + 1 = L + 1 + k$.

一方 $\sigma(L) = k(N+1) = L + k$ だったので矛盾.

q.e.d.

3.2 高木貞治

高木は初等整数論講義で, オイラーの証明をほめて「 味のある証明」と言っている.

Proof

$N\sigma(L) = (N+1)L$ を N で割って, $\sigma(L) = L + \dfrac{L}{N}$ を得る.

$\dfrac{L}{N}$ は整数なので, $d = \dfrac{L}{N}$ とおくと,$L = Nd$.

$\sigma(L) = L + \dfrac{L}{N} = L + d$. L の約数は d, L しかないことを意味するので, $d = 1, L = N$. L は素数 p.

3.3 オイラーもどきの証明

Proof

$N\sigma(L) = (N+1)L$ を N で整理する.

$N(\sigma(L)-L)=L.$ となるので $co\sigma(L)=\sigma(L)-L$ に注意して $d=co\sigma(L)$ とおく.

$d=1$ なら $co\sigma(L)=1$ なので, L:素数.

$d>1$ なら $1,d,L$ は L の約数なので, $\sigma(L)\geq 1+d+L.$ $d=co\sigma(L)=\sigma(L)-L$ により $d;L=\sigma(L)\geq 1+d+L.$ 矛盾.

q.e.d.

私は, 高校のとき先生にすすめられ「数と図形」(ラーデマッヘルとテプリッツ) の本にある 完全数の章 でオイラーの定理の証明を知った. かなりわかりにくい, 難解な証明であった.

今にして思えば, 1930 年代に入って, ドイツの市民向けの公開講座で現代数学を紹介する試みの中でなるべく数式を使わない証明だったので却って分かりにくいものとなったと思う.

表 1: $h = 1, m = 0$ 完全数のとき

$h = 1$			
e	a 完全数		q メルセンヌ素数
1	6	$2 * 3$	3
2	28	$2^2 * 7$	7
4	496	$2^4 * 31$	31
6	8128	$2^6 * 127$	127
12	33550336	$2^{12} * 8191$	8191
16	8589869056	$2^{16} * 131071$	131071
18	137438691328	$2^{18} * 524287$	524287
30	2305843008139952128	$2^{30} * 2147483647$	2147483647

次のことは周知の事実である.

命題 2 $e > 1$ のとき メルセンヌ素数の末尾の数は *1,7.*
完全数の末尾の数は *6,8.*

証明もできる.

乗数付きメルセンヌ素数

h が素数のとき, $q = h * 2^{e+1} - 1$ が素数のとき, 乗数 h のメルセンヌ素数という.
完全数のときと同様に, $\alpha = 2^e q$ を乗数 h の完全数という.
完全数のときと同様の性質がは 2 べきとメルセンヌ素数の積に分解される.

表 2: $h = 3, m = 0$ 完全数のとき

$h = 3$			
e	α		q :乗数 3 のメルセンヌ素数
1	22	$2 * 11$	11
2	92	$2^2 * 23$	23
3	376	$2^3 * 47$	47
5	6112	$2^5 * 191$	191
6	24512	$2^6 * 383$	383
10	6290432	$2^{10} * 6143$	6143
17	103079084032	$2^{17} * 786431$	786431
33	442721857760439304192	$2^{33} * 51539607551$	51539607551
37	113336795588734046175232	$2^{37} * 824633720831$	824633720831
42	116056878683000002725281792	$2^{42} * 26388279066623$	26388279066623

命題 3 $e > 1$ のとき 乗数 *3* のメルセンヌ素数の末尾の数は *1,3,7.*
乗数 *3* の完全数の末尾の数は *2.*

表 3: $h = 5, m = 0$ 完全数のとき

$h = 3$			
e	a		q
1	38	$2 * 19$	19
3	632	$2^3 * 79$	79
7	163712	$2^7 * 1279$	1279
9	2620928	$2^9 * 5119$	5119
11	41940992	$2^{11} * 20479$	20479
13	671080448	$2^{13} * 81919$	81919
17	171798560768	$2^{17} * 1310719$	1310719
31	4611686018212639539 2	$2^{31} * 21474836479$	21474836479

命題 4 $e > 0$ のとき 乗数 *5* のメルセンヌ素数の末尾の数は *9.*
乗数 *5* の完全数の末尾の数は *2,8.*

表 4: $h = 7, m = 0$ 完全数のとき

e	a		q
4	3568	$2^4 * 223$	223
8	917248	$2^8 * 3583$	3583
16	60129476608	$2^{16} * 917503$	917503
20	15393161740288	$2^{20} * 14680063$	14680063
28	1008806316262555648	$2^{28} * 3758096383$	3758096383
44	433279013749881336996089036 8	$2^{44} * 246290604621823$	246290604621823

命題 5 *e は 4 の倍数*

乗数 7 のメルセンヌ素数の末尾の数は 3.

乗数 7 の完全数の末尾の数は 8.

4 平行移動 m の完全数

そしてこれらを一般に考えることにした. $\sigma(a) = 2a - m$ を満たすとき, a を平行移動 m の完全数 (m だけ平行移動した完全数) という.

表 5: $h = 1, m = 2$ 完全数のとき

e	a		q
1	10	$2 * 5$	5
3	136	$2^3 * 17$	17
7	32896	$2^7 * 257$	257
15	2147516416	$2^{15} * 65537$	65537

命題 6 $e > 1$ のとき乗数 *1,*$m = 2$ のメルセンヌ素数の末尾の数は *7.*
乗数 *1,*$m = 2$ の完全数の末尾の数は *6.*

表 6: $h = 1, m = 4$ 完全数のとき

e	a		q
1	14	$2 * 7$	7
2	44	$2^2 * 11$	11
3	152	$2^3 * 19$	19
5	2144	$2^5 * 67$	67
6	8384	$2^6 * 131$	131
11	8394752	$2^{11} * 4099$	4099
14	536920064	$2^{14} * 32771$	32771
15	2147581952	$2^{15} * 65539$	65539
17	34360131584	$2^{17} * 262147$	262147
27	36028797421617152	$2^{27} * 268435459$	268435459
29	576460753914036224	$2^{29} * 1073741827$	1073741827

命題 7 $e > 1$ のとき乗数 *1,*$m = 4$ のメルセンヌ素数の末尾の数は *1,7,9.*
乗数 *1,*$m = 4$ の完全数の末尾の数は *2,4.*

表 7: $h = 1, m = -2$ 完全数のとき

e	a		q
2	20	$2^2 * 5$	5
3	104	$2^3 * 13$	13
4	464	$2^4 * 29$	29
5	1952	$2^5 * 61$	61
8	130304	$2^8 * 509$	509
9	522752	$2^9 * 1021$	1021
11	8382464	$2^{11} * 4093$	4093
13	134193152	$2^{13} * 16381$	16381
19	549754241024	$2^{19} * 1048573$	1048573
21	8796086730752	$2^{21} * 4194301$	4194301
23	140737463189504	$2^{23} * 16777213$	16777213
28	144115187270549504	$2^{28} * 536870909$	536870909

この定義は次の結果により正当性をえる.

命題 8 $p = \sigma(2^e) + m$ が素数のとき $a = 2^e p$ は $\sigma(a) = 2a - m$ を満たす.

Proof

$N = \sigma(2^e) = 2^{e+1} - 1$ を使って,$p = \sigma(2^e) + m = N + m$ に注意する. $\sigma(a) = \sigma(2^e)\sigma(p) = N(p+1) = Np + N = (2^{e+1} - 1)p + N = 2a - p + N = 2a - m$.

$$\begin{aligned}
\sigma(a) &= \sigma(2^e)\sigma(p) \\
&= N(p+1) \\
&= Np + N \\
&= (2^{e+1} - 1)p + N \\
&= 2a - p + N \\
&= 2a - m.
\end{aligned}$$

q.e.d.

これを観察すると面白い.

$\sigma(a) = 2a - 1$ を満たすとき, a を概完全数という. 2^e は概完全数である. この逆, 則ち, 概完全数は 2 べき : 2^e になるという主張を概完全数予想という.

奇数完全数の問題と並び概完全数予想も未解決の難問とされている.

退職後広尾学園に出入りするようになり, 高校生に数学研究の助言をすることとなった. 高校生 (大学生も) には完全数は人気のあるテーマである.

完全数は世界的も人気のあるテーマなのでこれを高校生に勧めることはできない. そこで Wikipedia で調べると,

$\sigma(a) = 2a - 1$ を満たすとき, a を概完全数という. 2 のべき以外の概完全数は存在するかどうか不明.

$\sigma(a) = 2a + 1$ を満たすとき, a を pseudo perfect number(疑似完全数) という. するかどうか不明.

そこで概完全数, 完全数, 疑似完全数と合わせてこれらを 3 点セットと呼ぶことした.

さらに $\sigma(a) = 2a \pm 2$ も含めて 5 点セットで考えたらさらに研究対象が広がるだろう.

5　完全数 m, a:偶数, $a = 2^e L$

$\sigma(a) = 2a - m$ の解を a:偶数の場合に $a = 2^e L, (2 \not| L)$ として探すアルゴリズムを使う.

これは能率よく求められる.

$N = 2^{e+1} - 1$ とおき $a = 2^e L$ を定義式 $\sigma(a) = 2a - m$ に代入すると

$\sigma(a) = \sigma(2^e L) = N * \sigma(L), 2a - m = 2^{e+1} L - m = (N+1)L - m$ になり, $L_m = L - m$ とおくと,

$N\sigma(L) = (N+1)L - m$ により, $N(\sigma(L) - L) = L_m$.

ユークリッドの余関数 $\mathrm{co}\sigma(L) = \sigma(L) - L$ を用いると $N\mathrm{co}\sigma(L) = L_m$.

ここで最初の関門は $L_m > 0$.

第 2 の関門は $W_0 = L_m / \mathrm{co}\sigma(L)$ が整数となる. L が素数なら,$\mathrm{co}\sigma(L) = 1$ なのですぐ突破.

第 3 の関門は $W = W_0 + 1$ は 2 べき すなわち $W = 2^f$ とかける.

最後に, $f = e + 1$ なので, $2^{f-1} L$ は解になる.

表 8: 完全数 $m = -10$:偶数, $a = 2^e L$

a	素因数分解
1696	$2^5 * 53$
518656	$2^9 * 1013$
34358296576	$2^{17} * 262133$
	$m = -8$
368	$2^4 * 23$
128768	$2^8 * 503$
11096	$2^3 * 19 * 73$
2087936	$2^{10} * 2039$
836	$2^2 * 11 * 19$
17816	$2^3 * 17 * 131$
77744	$2^4 * 43 * 113$
2291936	$2^5 * 67 * 1069$
8589344768	$2^{16} * 131063$
13174976	$2^6 * 139 * 1481$
35021696	$2^7 * 419 * 653$
45335936	$2^7 * 337 * 1051$
45356	$2^2 * 17 * 23 * 29$
91388	$2^2 * 11 * 31 * 67$
254012	$2^2 * 11 * 23 * 251$
388076	$2^2 * 13 * 17 * 439$

表 9: 完全数 $m=-6$:偶数, $a=2^eL$

a	素因数分解
8925	$3*5^2*7*17$
32445	$3^2*5*7*103$
442365	$3*5*7*11*383$
	$m=-4$
70	$2*5*7$
1888	2^5*59
32128	2^7*251
521728	2^9*1019
4030	$2*5*13*31$
5830	$2*5*11*53$
8378368	$2^{11}*4091$
34359083008	$2^{17}*262139$
1848964	$2^2*13*31^2*37$

表 10: 完全数 m:偶数, $a=2^eL$

a	2^e	L	
$m=-6$	$-2*3$		
8925	2^0	8925	$3*5^2*7*17$
32445	2^0	32445	$3^2*5*7*103$
151115727449904501489664	2^{38}	549755813881	549755813881
	2^{714}	X	X

$X=$ 72364133221937103085272756482216056112753534658909761028039668631756215232006744379020625060744018369805777923479247838020220755974022884986972234404720831691332769255536872593544438018353486799545737272878084128761

$a=2^eQ,(Q$ 奇素数) の形の解を A 型解という. m が偶数なら A 型解は必ずあるに違いない.

しかし $m=-6$ のときは A 型解がごく少ない.

$e=38$ の場合があることは旧知の事実であるが $e=714$ のときもあった.

表 11: 完全数 $m = -10$:偶数, $a = 2^e L$

a	素因数分解
1696	$2^5 * 53$
518656	$2^9 * 1013$
34358296576	$2^{17} * 262133$
	$m = -8$
368	$2^4 * 23$
128768	$2^8 * 503$
11096	$2^3 * 19 * 73$
2087936	$2^{10} * 2039$
836	$2^2 * 11 * 19$
17816	$2^3 * 17 * 131$
77744	$2^4 * 43 * 113$
2291936	$2^5 * 67 * 1069$
8589344768	$2^{16} * 131063$
13174976	$2^6 * 139 * 1481$
35021696	$2^7 * 419 * 653$
45335936	$2^7 * 337 * 1051$
45356	$2^2 * 17 * 23 * 29$
91388	$2^2 * 11 * 31 * 67$
254012	$2^2 * 11 * 23 * 251$
388076	$2^2 * 13 * 17 * 439$

表 12: 完全数 $m = -6$:偶数, $a = 2^e L$

a	素因数分解
8925	$3 * 5^2 * 7 * 17$
32445	$3^2 * 5 * 7 * 103$
442365	$3 * 5 * 7 * 11 * 383$
	$m = -4$
70	$2 * 5 * 7$
1888	$2^5 * 59$
32128	$2^7 * 251$
521728	$2^9 * 1019$
4030	$2 * 5 * 13 * 31$
5830	$2 * 5 * 11 * 53$
8378368	$2^{11} * 4091$
34359083008	$2^{17} * 262139$
1848964	$2^2 * 13 * 31^2 * 37$

表 13: 完全数 $m = -2$:偶数, $a = 2^e L$

a	素因数分解
464	$2^4 * 29$
1952	$2^5 * 61$
130304	$2^8 * 509$
522752	$2^9 * 1021$
8382464	$2^{11} * 4093$
134193152	$2^{13} * 16381$
650	$2 * 5^2 * 13$

表 14: 完全数 $m = 0$:偶数, $a = 2^e L$

a	素因数分解
6	$2 * 3$
28	$2^2 * 7$
496	$2^4 * 31$
8128	$2^6 * 127$
33550336	$2^{12} * 8191$
8589869056	$2^{\mid}16 * 131071$
137438691328	$2^{18} * 524287$

表 15: 完全数 $m = 2$:偶数, $a = 2^e L$

a	素因数分解
3	3
10	$2 * 5$
136	$2^3 * 17$
32896	$2^7 * 257$
2147516416	$2^{15} * 65537$
	$m = 4$
152	$2^3 * 19$
110	$2 * 5 * 11$
2144	$2^5 * 67$
8384	$2^6 * 131$
8394752	$2^{11} * 4099$
536920064	$2^{14} * 32771$
2147581952	$2^{15} * 65539$
34360131584	$2^{17} * 262147$
884	$2^2 * 13 * 17$
18632	$2^3 * 17 * 137$
116624	$2^4 * 37 * 197$
15370304	$2^6 * 137 * 1753$
73995392	$2^7 * 293 * 1973$

表 16: 完全数 $m = 6$:偶数, $a = 2^e L$

a	素因数分解
592	$2^4 * 37$
315	$3^2 * 5 * 7$
2102272	$2^{10} * 2053$
1155	$3 * 5 * 7 * 11$
	$m = 8$
184	$2^3 * 23$
130	$2 * 5 * 13$
2272	$2^5 * 71$
33664	$2^7 * 263$
527872	$2^9 * 1031$
1012	$2^2 * 11 * 23$
18904	$2^3 * 17 * 139$
85936	$2^4 * 41 * 131$
70564	$2^2 * 13 * 23 * 59$
100804	$2^2 * 11 * 29 * 79$
1090912	$2^5 * 73 * 467$
2147713024	$2^{15} * 65543$
34360655872	$2^{17} * 262151$
391612	$2^2 * 13 * 17 * 443$

表 17: 完全数 $m = 10$:偶数, $a = 2^e L$

a	素因数分解
21	$3 * 7$
656	$2^4 * 41$
2336	$2^5 * 73$
8768	$2^6 * 137$
133376	$2^8 * 521$
528896	$2^9 * 1033$
34360918016	$2^{17} * 262153$

6 概完全数

$a = 2^e$ のとき, $\sigma(a) = 2^{e+1} - 1 = 2a - 1$ となる.

そこで, $a = 2^e$ とおいたことを忘却の彼方におき, $\sigma(a) = 2^{e+1} - 1 = 2a - 1$ を a についての方程式とみなした場合この解を概完全数という.

$a = 2^e$ なら概完全数になる. この逆は正しいか?

これが正しいと思う人にとっては概完全数は 2 べきに限ることが自然である.

しかし, 奇数完全数の問題と同じく, 2 べき以外の概完全数の存在問題は未解決の難問である.

アルゴリズムで考える.

$a = 2^e L$ を定義式 $\sigma(a) = 2a - 1$ に代入すると

$\sigma(a) = \sigma(2^e L) = N * \sigma(L), 2a - 1 = 2^{e+1} L - 1 = (N + 1)L - 1$ になり, $L_1 = L - 1$ とおくと, $N(\sigma(L) - L) = L_1$.

ユークリッドの余関数 $\mathrm{co}\sigma(L) = \sigma(L) - L$ を用いると $N\mathrm{co}\sigma(L) = L_1$.

第 2 の関門は $W_0 = L_1/\mathrm{co}\sigma(L)$ が整数となる. L が素数べき p^e なら,$\mathrm{co}\sigma(L) = \sigma p^{e-1} = (p^e - 1)/(p - 1)$ なので $W_0 = L_1 \mathrm{co}\sigma(L) = p - 1$.

したがって, $W = W_0 + 1 = p$. これは 2 べきにはならない.

一般に p : 素数なら $\overline{p} = p - 1$ とおくとき

$a = p^e$ とすると, $\overline{p}\sigma(a) = p^{e+1} - 1 = pa - 1$ となる.

7　一般の概完全数

$\overline{p}\sigma(a) = pa - 1$ を満たす a を p を底とする一般の概完全数という.

p べき以外に概完全数があるというのは一見して意外な結果である.

$p = 2, 3$ のとき反例はみつからない.

$a = p^e L$ を定義式 $\overline{p}\sigma(a) = pa - 1$ に代入すると $W = p^{e+1} - 1$ とおく.

$\overline{p}\sigma(a) = \overline{p}\sigma(p^e L) = W * \sigma(L)/\overline{p}, pa - 1 = p^{e+1}L - 1 = (W+1)L - 1$ になり, $L_1 = L - 1$ とおくと, $W\mathrm{co}\sigma(()L) = L_1$.

第2の関門は $W_0 = L_1/\mathrm{co}\sigma(L)$ が整数となる条件である. L が素数べき p^e なら,$\mathrm{co}\sigma(L) = \sigma p^{e-1} = (p^e - 1)/(p - 1)$ なので $W_0 = L_1\mathrm{co}\sigma(L) = p - 1$.

したがって, $W = W_0 + 1 = p$. このとき $f = 1, e = 0$ により解が $a = L = p^e$ として求まる. これが一般の概完全数の解としての p べき.

しかし, L には素数べきにならない解があった.

$p = 5, L = 77$. のとき, $L_1 = 76, \mathrm{co}\sigma(()77) = 96 - 77 = 19$. $W_0 = L_1/\mathrm{co}\sigma(()77) = 4$. $W = W_0 + 1 = 5$. $f = 1$ なので解 $a = 5^0 * 77 = 77$.

組織的に反例をさがすことに成功したのは 新型コロナウイルス感染症の恐怖に怯えていた 2020 年 3 月 15 日, 放送大学の学習センターにおいて.

とりあえず結果を記録しよう.

表 18: p べき以外の概完全数

p^e	L	素因数分解
5^1	77	7*11
11^1	611	13*47
17^1	1073	29*37
17^1	2033	19*107
7^1	97783	7*61*229
7^2	13969	61*229
31^1	6031	37*163
37^1	5293	67*79
47^1	9983	67*149
41^1	25241	43*587
73^1	65017	79*823
89^1	50249	109*461
101^1	40301	191*211
101^1	49901	139*359
101^1	51101	137*373
101^1	99101	113*877

ここで概完全数は $a = p^{e-1}L$ となる
(7^1 , 97783, 7*61*229) と (7^2 , 13969 , 61*229) 同じ解を与える.
$p = 7$ のときは 3 素数の積, その他は半素数 (3 素数の積) になっている.
$p = 2, 3, 13, 23, 43$ などの場合はこれを満たす例が見えない.

表 19: 完全数 m:偶数, $a = p^{e-1}L$

p^e	L	素因数分解
131^1	142091	151*941
173^1	131237	263*499
173^1	791717	179*4423
181^1	259741	211*1231
197^1	213053	257*829
199^1	681319	211*3229
233^1	455417	269*1693
239^1	228719	439*521
257^1	938753	277*3389
347^1	718643	439*1637
431^1	743471	809*919
431^1	929231	593*1567

実はほぼ 6 年前に完全数の研究の途中で, $p = 5, 7, 11, 13$ などの場合に
反例があることに気づいた.
反例があるからこの問題は解決済み, とは言えない.
$p = 5$ の場合は 77 と　5 べき 以外の反例があるか
という形の問題を提起してもよい.

8　アルゴリズム

$\overline{p}\sigma(a) = pa - 1$ を満たす a を求める際に $a = p^e L, (p \not| L)$ の形とかけるとする.

しかしついでに, 一般化して 与えられた m に対して $\overline{p}\sigma(a) = pa - m$ を満たす a を求めることにしよう.

$a = p^e L, (p \not| L)$ の形とかけるとする. しかし $e = 0$ も許容する.

$W = p^{e+1} - 1$ とおくと,

$$\overline{p}\sigma(a) = W\sigma(L), pa - 1 = p^{e+1}L - m = (W+1)L - m.$$

これより $W\sigma(L) = (W+1)L - m$.

したがって,

$W\sigma(L) = (W+1)L - m$ になり

$$W(\sigma(L) - L) = L - m.$$

アルゴリズムは, 与えられた L について,$L_m = L - m$ とし L_m が $\mathrm{co}\sigma(L) = \sigma(L) - L$ で割れるとする.

$W_0 = \frac{L_m}{\mathrm{co}\sigma(L)} + 1$ を素因数分解すると, 素数べき p^{e+1} になれば $a = p^e * L$ が解になる.

$m=1$ で p べき, すなわち $L=p^{\varepsilon}$ のとき, $\mathrm{co}\sigma(L)=\sigma(p^{\varepsilon-1})=\frac{p^{\varepsilon}-1}{p-1}$ になる.

$W_0=\frac{L_1}{\mathrm{co}\sigma(L)}+1=p$ となる. したがって, $a=p^{\varepsilon}$ が解.

p べきの場合が解になり, これは通常解というべきものである.

L_1 が $\mathrm{co}\sigma(L)=\sigma(L)-L$ で割れて, W_0 が 2 個以上の素因子を持つという条件で探した結果得られたのが上記の表である.

表の数を見ると, L は 2 素数 p,q の積である.

次に, 2 素数 p,q の積 $L=pq$, $\Delta=p+q$ とする.

$L_1=pq-1$ $\Delta=p+q$ とすると, $L_1=pq-1$ が $\mathrm{co}\sigma(L)=\sigma(L)-L=\Delta+1$ で整除されると仮定する.

$cof=L_1/(\Delta+1)$ とおき $W_0=cof+1$ とおきこれを素因数分解する.

表 20: p べき以外の概完全数

$L=pq$	L_1	p	q	cof	W_0
77	76	7	11	4	5^1
611	610	13	47	10	11^1
1073	1072	29	37	16	17^1
2033	2032	19	107	16	17^1
5293	5292	67	79	36	37^1
6031	6030	37	163	30	31^1
9983	9982	67	149	46	47^1
13969	13968	61	229	48	7^2
15947	15946	37	431	34	$5*^1*7*^1$
23489	23488	83	283	64	$5*^1*13*^1$
25241	25240	43	587	40	$41*^1$

$L=15947, 23489$ は W_0 が 2 つの異なる素因数からなるので概完全数にならない

9 疑似完全数

$\sigma(a) = 2a$ を満たせば, 完全数 (perfect numbers).

$\sigma(a) = 2a - 1$ を満たせば, 概完全数 (almost perfect numbers) といい, それは 2 べきだけに限るという予想がある.

$\sigma(a) = 2a + 1$ を満たせば, 疑似完全数 (pseudo perfect numbers) という名前はついているがその例は知られていない.

ここでは 2 の代わりに素数 p について $\overline{p}\sigma(a) = pa + 1$ を満たす数を一般の疑似完全数と呼びこれを探す.

表 21: $a =$ p $^{e-1}L, \overline{p}\sigma(a) = pa + 1$, 一般の疑似完全数

p^e	L	素因数分解
3^1	21	$3 * 7$
5^1	115	$5 * 23$
7^1	329	$7 * 47$
13^1	731	$17 * 43$
3^1	2133	$3^3 * 79$
13^1	2171	$13 * 167$
19^1	6821	$19 * 359$
37^1	7379	$47 * 157$
43^1	8357	$61 * 137$
53^1	13987	$71 * 197$
3^1	19521	$3^4 * 241$
29^1	24331	$29 * 839$
79^1	24881	$139 * 179$
5^1	29491	$7 * 11 * 383$
103^1	46001	$157 * 293$

例 1 $p = 3, a = 21$ のとき $\overline{p}\sigma(a) = pa + 1$ を計算する.
$\overline{p}\sigma(a) = 2 * 4 * 8 = 64, pa + 1 = 3a + 1 = 3 * 21 + 1 = 64.$

例 2 $p = 5, a = 115 = 5 * 23$ のとき $\overline{p}\sigma(a) = pa + 1$ を計算する.
$\overline{p}\sigma(a) = 4 * 6 * 24 = 576, pa + 1 = 5a + 1 = 5 * 115 + 1 = 576.$

私は完全数の勉強を始めたころ, $\sigma(a) = 2a + 1$ を満たせば, 疑似完全数という名前はあるが, 実は存在しないという予想があると知って思わず笑ってしまった.

$\sigma(a) = 2a + 1$ を満たす数はもしかしたらあるかも知れない.

しかしせっかく発見しても, その数が 疑似完全数という芳しくない名称があると知ったらその数は憤慨するだろう. 大変な苦労の結果見つけたとき苦労は報われない.

今回はアルゴリズムがうまく働いて底を素数とするとき疑似完全数が続々と見つかった.

小さい素数 $p = 3, 5, 7, 13, 19$ などに対して 疑似完全数が発見できたことは 率直に言ってうれしい.

手計算も大変なので, wxmaxima で書いた次の関数で確認したら正しかった.

```
fpseudo(p,a):= block([p1], p1:p-1,b:p1*divsum(a)-a*p-1, return(b));
```

10 パワー完全数

$\overline{p}\sigma(a) = pa + 1$ を 一般に考えて与えられた m について $\overline{p}\sigma(a) = pa - m$ を満たす数を平行移動 m のパワー完全数と呼びこれらを探す.

20.2 群作用の例

群 G の部分群 H に対し H が集合 G に作用することを $a \in H$ と $x \in G$ に対して $a \cdot x = ax$ で定義する. これは部分群によるコセット分解で扱った場合である.

Hx が x での H 軌道であるが $H_x = \{e\}$ となる. よって, $|H| = |xH|$. この場合は軌道の長さがすべて等しくなり軌道の個数が $\dfrac{|G|}{|H|}$ となる. ここでは食パンの原理が成立する. 軌道の長さが変化する場合もある.

21 共役

群 G の元 a と b はある元 $c \in G$ があって, $b = cac^{-1}$ とかけるとき, **共役** (conjugate) であるという. これは重要な概念である.

群 G の元 a が G の元 x に作用することを $a \cdot x = axa^{-1}$ で定義する. 実際, 簡単な計算により

$$b \cdot (a \cdot x) = b \cdot axa^{-1} = baxab^{-1} = ba \cdot x$$

となる.

x での G 軌道の元は axa^{-1} とかけるので x と共役な元である. したがって x での G 軌道は x の**共役類** (conjugacy class) と呼ばれ C_x と書かれる. x を C_x の代表という.

$a \cdot x = x$ を書き換えれば $ax = xa$. したがって, x での固定群 G_x は $\{a \in G \mid ax = xa\}$ とかける. これは中心化群 $Z_x(G)$ である. 故に $|C_x| = [G : Z_x(G)]$.

各々の共役類から代表 $x_1, x_2, \cdots, x_s$ を選ぶ. $g_j = |C_{x_j}|$ とおくと $g_j = [G : Z_{x_j}(G)]$ と書け, また

$$\sum_{j=1}^{s} g_j = |G|$$

が成立する. これを**類方程式** (class equation) という.

$Z_x(G) \subset G$ であるが, $Z_x(G) = G$ のとき x はすべての G の元と交換可能であり, このとき x は G の中心になる, すなわち $x \in Z(G)$.

22 p 群

有限群 G の位数が 1 ではなく素数 p のべきのとき p **群** (p group) という. クラインの 4 元群は 2 群の例である.

p 群 G の部分群の位数はやはり素数 p のべきなのでそれが単位群でない限り p の倍数である.

類方程式 $\sum_{j=1}^{s} g_j = |G|$ において $g_j = [G : C_G(x_j)]$ 素数 p のべきなので $C_G(x_j) = G$ でない限り g_j は p の倍数である.

$C_G(x_j) = G$ のとき x_j は中心 $Z(G)$ の元である. したがってそのとき $g_j = 1$ なので類方程式を mod p でみると $|Z(G)| \equiv 0 \mod p$. かくして次の重要な定理をえる.

定理 8 (中心存在定理) p 群 G の中心 $Z(G)$ は単位群でない.

23 Sylow の定理

有限群 G の部分群 H の位数は n の約数になることはラグランジュの定理の主張するところであるが, 逆は正しくない. すなわち n の約数を位数にもつ部分群がつねにあるわけではない.

約数が与えられたとき, それを位数にする部分群があるかはどうかは難しい問題である. しかし, n の素因数 p に対してそれを位数に持つ部分群があることはコーシーが証明した. G の位数 n を素因数分解をし, その p の指数を c とすると $n = p^c k$ と書ける. ここで k は p で割れない.

さらに素数べき p^f (ただし,$f \leq c$) にも部分群があることがシロウ (Sylow)[3] により証明された. とくに, 位数が p^c の部分群を $p-$ **Sylow 群**という.

$p-$ Sylow 群は存在し, それらは互いに共役でしかもその個数は mod p でみると 1 である. これを **Sylow の定理**という.

定理 9 (Sylow の 第 1 定理) 素数べき p^f *(ただし,$f \leq c$)* を位数に持つ部分群 P が存在する.

Proof

証明は G の 位数 n についての数学的帰納法による.

G の真部分群 H の位数 $m(m < n$ なので) の素因数 p の指数がやはり c なら, 帰納法の仮定により位数が p^f の部分群 P がある. これは G の部分群なのでこれでよい. したがって,G の真部分群 H の位数の素因数 p の指数はすべて c 未満であるとしてよい.

$a \in G$ に対してその中心化群 $C_G(a)$ が群 G でない限りその位数 m_a の素因数 p の指数はすべて c 未満なので $[G : C_G(a)]$ は p の倍数である. 共役類についての類方程式から

$$n \equiv |Z(G)| \mod p$$

が成り立つので $n > 1$ のとき中心 $Z(G)$ の位数は p の倍数になり単位群ではない.

[3]Peter Ludwig Mejdell Sylow, ノルウェーの数学者 (1832 – 1918), 彼は 60 代になるまで高校の教師であった.

中心 $Z(G)$ はアーベル群なので, アーベル群に関してのコーシーの定理により位数 p の元 z がある. そこで $C_0 = \langle z \rangle$ とおく. C_0 は正規部分群である. 実際, $a \in G$ に対して $z \in Z(G)$ だから中心の定義から $az = za$.

C_0 による商群 $G_0 = G/C_0$ の位数は n/p なので位数 p^{f-1} の部分群 P_0 がある. 自然準同型 $\psi : G \to G_0 = G/C_0$ による逆像 $\psi^{-1}(P_0)$ を P とおけばよい.

23.1 Sylow の第 2 定理

S を $p-$ Sylow 群とする. すなわち,S は位数が p^c の部分群である. さらに, 位数が p の累乗である部分群を P とおく.

$a \in G$ をとり, ダブルコセット $Sa \cdot P$ を考える. この元の (右コセット Hb らの) 個数は $[P : a^{-1}Sa \cap P]$ であるが, $|P|, |a^{-1}Sa| = |S|$ は p の累乗なので $[P : a^{-1}Sa \cap P]$ も p の累乗である. したがって,

1. $[P : a^{-1}Sa \cap P] \neq 1$ なら $[P : a^{-1}Sa \cap P]$ は p の倍数.
2. $[P : a^{-1}Sa \cap P] = 1$ なら $P = a^{-1}Sa \cap P \subset a^{-1}Sa$ になる.

ダブルコセット $Sa \cdot P$ は全体で右コセット空間 G/S をカバーするが G/S の元の個数は $n/p^c = k$ なのでこれは p で割れない. したがってある $a \in G$ がありそのダブルコセット $Sa \cdot P$ の元の個数は p でわれない. このとき $P \subset a^{-1}Sa$.

P も $p-$ Sylow 群ならその位数は $a^{-1}Sa$ の位数と同じになり結局 $P = a^{-1}Sa$. よってこのとき,P は最初に定めた $p-$ Sylow 群 S の共役群である.

$N = N_G(S)$ とおくとき,$p-$ Sylow 群の総数はコセット空間 G/N の元の個数である. よって $p-$ **Sylow 群の総数**を n_p と書くと $n_p = [G : N_G(S)]$. したがって n_p は $[G : S]$ の約数である. 次に n_p を G/N の部分集合であるダブルコセット $Na \cdot S$ を経由して数えよう.

23.2 Sylow の第 3 定理

$|Na \cdot S| = [S : a^{-1}Na \cap S]$ に注意して次のように場合分けを行う.

1. $[S : a^{-1}Na \cap S] = 1$ なら $|Na \cdot S| = 1$.
2. $[S : a^{-1}Na \cap S] > 1$ なら $|Na \cdot S| \equiv 0 \mod p$.

(2) のときは S が $p-$ 群 だから当然 $|Na \cdot S|$ は p の倍数.

(1) のときは $|Na \cdot S| = 1$ は定義通りだがこのようなダブルコセットは 1 つしかないことを次に証明する.

$S = a^{-1}Na \cap S \subset a^{-1}Na$. よって, $aSa^{-1} \subset N$ になるので S と aSa^{-1} は N の $p-$ Sylow 群と見なすことができ,

Sylow の第 2 定理によって, $b \in N$ があり,$aSa^{-1} = bSb^{-1}$ と書ける. $b \in N = N_G(S)$ なので $bSb^{-1} = S$. よって $aSa^{-1} = S$. これより $a \in N$. したがってダブルコセットは $Na \cdot S$ は $Ne \cdot S$ になり, ただ 1 つである.

以上により $p-$ Sylow 群の総数は $1+rp$ と書ける.

q.e.d.

24 位数 15 の群

G を位数 15 の群とする. Sylow の第 1 定理により, 位数 3 の部分群 H と位数 5 の部分群 N とがある. それぞれ $3-$ Sylow 群と $5-$ Sylow 群になる. これらは巡回群なので $H=\langle x\rangle, N=\langle y\rangle$ と生成元 x, y で表す.

N は正規部分群であることを最初に示す. $z\in G$ をとり $K=z^{-1}Nz$ とおくとこれも位数 5 であり $N\neq K$ と仮定すると $N\cap K=\{e\}$. このとき 写像 $\mu: H\times K\to G$ を $\mu(h,k)=hk$ で定義すると群の準同型になるとは限らないが単射である.

実際 $\mu(h,k)=\mu(h_1,k_1)$ とすると $hk=h_1k_1$ になり $kk_1^{-1}=h^{-1}h_1\in N\cap K=\{e\}$ だから $(h,k)=(h_1,k_1)$. したがって $\mu(H\times K)$ の元の個数は 25 になり G の位数は 15 に矛盾する.

$z=x$ に選ぶと $x^{-1}yx\in N=\langle y\rangle$.

N の元は生成元 y によって y^s と書けるので $x^{-1}yx=y^s$. ここで

$$x^{-2}yx^2=x^{-1}y^sx=y^{s^2}.$$

もう一回同じことをすると

$$x^{-3}yx^3=y^{s^3}.$$

しかし,$x^3=e$ なので $x^{-3}yx^3=y$. よって

$$y=y^{s^3}.$$

$y^5=1$ により $s^3=1 \mod 5$. 次の表によって計算すると $s=1$.

表 35: mod5 での計算

s	1	2	3	4
s^2	1	4	4	1
s^3	1	3	2	4

したがって, $xy=yx$. よって $G=H\times N=C_3\times C_5\cong C_{15}$. 以上によって, 位数 15 の群は巡回群 C_{15} に限ることがわかった. 位数 6 の群は巡回群 C_6 の他に D_3 があった. 位数 15 の方が簡単になったことは不思議なことといわざるをえない.

24.1 別証明

原田 [**?**] p148 には Sylow の第 3 定理を使う証明があるのでそれを紹介しよう.

G を位数 15 の群とする. その位数 3 と 5 の部分群はそれぞれ Sylow 群でありその総数を n_3, n_5 とおくと n_3 は $15/3=5$ の約数で,n_5 は $15/5=3$ の約数になる (p142).

Sylow の第 3 定理によれば $n_5 = 1 + 5k$. かつ 3 の約数だから $n_5 = 1$. よって位数 5 の部分群はただ 1 つしかない. それを S_5 と書く. 同様に $n_3 =$ となり位数 3 の部分群もただ 1 つなので S_3 と書く.

G の元 x の位数 r は 15 の約数なので 1,3,5,15 のいずれかである. $r = 3$ なら x は $S_3 \setminus \{e\}$ の元になり総計 2 個. 同様に位数 5 の元は総計 4 個. 単位元は 1 個なので $r = 1, 3, 5$ の元は総計 1+2+4=7 個. 残りの元は $15 - 7 = 8$ 個あることがわかった. これら残りの元の位数はどれも 15 なので G は巡回群になる.