高校生もわかる新しい数論研究
第3期　予稿1
我々はどこから来たのか 我々は何者か
我々はどこへ行くのか

飯高 茂

2017 年 5 月 14 日

1. 我々はどこから来たのか

(元祖) 完全数がこの研究の源泉である. いろいろな完全数がでてきて分かりにくい. 一度整理してほしいという要望がありそれに応えるべくまとめた次第である.

今まで考えてきた完全数を列挙してみる：

究極の完全数, フェルマ完全数, 桐山の完全数, 劣完全数 (これはニューフェース), オイラーの φ 完全数, オイラーの $(+)$ 完全数, オイラーの $(*)$ 完全数, オイラーの $(**)$ 完全数, オイラーの劣完全数, 重完全数, 半完全数, これだけで 11 個あり 2 桁になっていたではないか.

これらに対して乗数をつけることができ, 乗数つき究極の完全数, 乗数つき劣完全数, 実は乗数つきは I 型と II 型 (alternative :いかにも怪しい) がある. これを加えると 4 つ増える.

ゴーギャンのように南の島に行って島の生活をしながら完全数を大きく育ててみたいものだ.

「我々はどこへ行くのか」これに答えることは難しい. 分かりません.

1　元祖完全数

$q = 2^{e+1} - 1$ が素数のとき $a = 2^e q$ をユークリッドの完全数 (または 狭義の完全数) という.

これは方程式 $\sigma(a) = 2a$ を満たす.

方程式 $\sigma(a) = 2a$ の解を広義の完全数という. これが元祖完全数である.

広義の完全数が実はユークリッドの完全数になるという予想がある. 2300 年たっても証明できない強者であり数学界でもっとも困難な問題と言ってもよい.

1.1 完全数の数表

完全数の数表は何度見ても美しい.

紀元前に得られた 4 つの完全数は 6,28,496,8128 である. 1800 年経ってから発見された完全数は 33550336. これは 8 桁の数で末尾の数は 6. 2015 年には, 49 番目の完全数が Curtis Cooper により発見された.

表 1: 完全数 a の数表, $p = 2^{e+1} - 1$:メルセンヌ素数

$e \bmod 4$	e	$2^e * p$	a	$a \bmod 10$	$p \bmod 10$
1	1	$2 * 3$	6	6	3
2	2	$2^2 * 7$	28	8	7
0	4	$2^4 * 31$	496	6	1
2	6	$2^6 * 127$	8128	8	7
0	12	$2^{12} * 8191$	33550336 (1456 年)	6	1
0	16	$2^{16} * 131071$	8589869056 (Cataldi,1588 年)	6	1
2	18	$2^{18} * 524287$	137438691328 (Cataldi,1588 年)	8	7
2	30	A	B (Euler, 1772 年)	8	7
0	60	C	D (Pervushin, 1883 年)	6	1
0	88	E	F (Powers, 1911)	6	1
2	106	G	H (Powers, 1914)	8	7
2	126	I	J (Lucas, 1876)	8	7

$A = 2^{30} * 2147483647$

$B = 2305843008139952128$

$C = 2^{60} * 2305843009213693951$

$D = 265845599156983174465469261595384217 6$

$E = 2^{88} * 6189700196426901374495621 11$

$F = 191561942608236107294793378084303638130997321548169216$

$G = 2^{106} * 162259276829213363391578010288127$

$H = 13164036458569648337239753460458722910223472318386943117783728128$

$I = 2^{126} * 170141183460469231731687303715884105727$

$J = 14474011154664524427946373126085988481573677 49$

$- - 14748358890663534349131199152128.$

$a > 10$ のとき次の結果が観察される. 証明は容易.
$e \equiv 0 \bmod 4 \Longrightarrow a \equiv 6 \bmod 10, p \equiv 1 \bmod 10,$
$e \equiv 2 \bmod 4 \Longrightarrow a \equiv 8 \bmod 10, p \equiv 7 \bmod 10.$

ユークリッドの完全数の末尾 1 桁は 6 または 8 であり, 完全数のもつ簡単だが美しい性質として古くから注目されてきた.

2. 我々は何者か

2　完全数の水平展開

$q = 2^{e+1} - 1 + m$ が素数のとき $a = 2^e q$ を m だけ平行移動した狭義の完全数という. 素数条件によって, m : 偶数になる.

これは方程式 $\sigma(a) = 2a - m$ を満たす.

この方程式 $\sigma(a) = 2a - m$ の解を m だけ平行移動した広義の完全数という.

m : 奇数の場合を含めて m だけ平行移動した広義の完全数を研究することは大きな課題である.

解の形が $a = 2^e q, (q$: 素数) となるとき正規解という. 一般に A 型の解ともいう.

解の形が $a = 2^e rq, (r < q$: 素数) となるとき第二正規解という. 一般に D 型の解という.

解の形が素数のべき $a = q^e$,(e : 任意) の場合は C 型の解という. $m = 1, a = 2^e$: がその例であり, 素数べきの一般解ともいう.

m_0 : 完全数のとき, $a = m_0 q (q$: が素数) は $m = -2m_0$ だけ平行移動した広義の完全数になり, 通常解という. これを一般に B 型の解という.

m_0 を完全数として $a = m_0 p$ とおき (ただし $m_0 \not\equiv 0 \mod p$), $\sigma(a) - 2a$ を計算する.

$$\sigma(a) - 2a = \sigma(m_0 p) - 2m_0 p = 2m_0(p+1) - 2m_0 p = 2m_0.$$

$\sigma(a) > 2a$ を満たす場合 a を過剰数という. $a = m_0 p$ は過剰数.

m : 奇数の場合は解が少ないがそれにもまして興味深いことが多い. 適当に E,F,G 型の解という.

3　第 2 完全数 28

3.1　$m = -56$ の場合

表 2: $m = -56$

a	factor
84	$2^2 * 3 * 7$
140	$2^2 * 5 * 7$
224	$2^5 * 7$
308	$2^2 * 7 * 11$
364	$2^2 * 7 * 13$
476	$2^2 * 7 * 17$
532	$2^2 * 7 * 19$
644	$2^2 * 7 * 23$
812	$2^2 * 7 * 29$
868	$2^2 * 7 * 31$
1036	$2^2 * 7 * 37$
1148	$2^2 * 7 * 41$
1204	$2^2 * 7 * 43$
1316	$2^2 * 7 * 47$
1372	$2^2 * 7^3$
1484	$2^2 * 7 * 53$
1652	$2^2 * 7 * 59$
1708	$2^2 * 7 * 61$

$28p$: (p は 2,7 以外の素数) は $\sigma(a) - 2a = 56$ の解でありこれを通常解という.

この表で $28p$ 以外の解を探すと

$a = 224 = 2^5 * 7$, $a = 1372 = 2^2 * 7^3$

がある.

この 2 つの解は予期できる解といってよい.

通常解である $2^2 * 7p$ において p が擬素数 2^3 に変身してできた $2^5 * 7$ と p が擬素数 7^2 に変身してできた $2^2 * 7^3$ があり, これらは擬素数解とみなすことができる.

擬素数解は素性の確かな変わり者である.

通常解は無限にあるのでこれらを排除した解の表を求めてみた.

これらの解は正規形 $2^e q$ および 第二正規形 $2^e rq$ である.

表 3: $m = -56, a : 28$ で割れない解

a	factor
4544	$2^6 * 71$
9272	$2^3 * 19 * 61$
14552	$2^3 * 17 * 107$
25472	$2^7 * 199$
74992	$2^4 * 43 * 109$
495104	$2^9 * 967$
6019264	$2^6 * 163 * 577$

$\sigma(a) = 2a + 56$ が正規形の解 $2^e q$ を持つなら, $q = 2^{e+1} - 1 - 56$: 素数という条件を満たす. 通常型の解が非常に多いので, 28 で割れない解に制限して正規形の解だけを求めた.

得られた表は次の通り:

表 4: $m = -56$ のとき正規形の解

a	factor
224	$2^5 * 7$
4544	$2^6 * 71$
25472	$2^7 * 199$
495104	$2^9 * 967$
2145615872	$2^{15} * 65479$
137424011264	$2^{18} * 524231$
8795973484544	$2^{21} * 4194247$
36028789368553472	$2^{27} * 268435399$
38685626227417444939464704	$2^{42} * 8796093022151$
2475880078568755040589185024	$2^{45} * 70368744177607$

$e \equiv 1 \mod 4, q \equiv 7 \mod 10, a \equiv 4 \mod 10,$
$e \equiv 2 \mod 4, q \equiv 1 \mod 10, a \equiv 4 \mod 10,$
$e \equiv 3 \mod 4, q \equiv 9 \mod 10, a \equiv 2 \mod 10.$

$2^e rq$ $(2 < r < q$: 素数) の解をアルゴリズムでさがしてみたら次のようになった.

表 5: $m = -56$, 第二正規形の解

a	factor
14552	$2^3 * 17 * 107$
9272	$2^3 * 19 * 61$
74992	$2^4 * 43 * 109$
35019968	$2^6 * 131 * 4177$
15317696	$2^6 * 137 * 1747$
6019264	$2^6 * 163 * 577$
53032832	$2^7 * 317 * 1307$
3365232128	$2^9 * 1277 * 5147$
26882784256	$2^{10} * 2557 * 10267$
17374747648	$2^{10} * 3691 * 4597$
125619603976192	$2^{12} * 8209 * 3736003$
12659380301824	$2^{12} * 8377 * 368947$
2306054088064335872	$2^{15} * 65539 * 1073790961$

4 究極の完全数

$2^{e+1} - 1 = \sigma(2^e)$ はユークリッドの公式であるが, $q = \sigma(2^e) - 1 + m$ が素数のとき $a = 2^e q$ を m だけ平行移動した狭義の完全数という.

P を素数とし, 整数 m に関して $\sigma(P^e) + m$ が素数 q のとき $a = P^e q$ を m だけ平行移動した底が P の狭義の究極の完全数と呼ぶ.

m だけ平行移動した場合を考えることは重要であり, これによって問題が奥深くなった.

この場合の方程式も比較的シンプルである.

$$\overline{P}\sigma(a) - Pa = (P-2)\mathrm{Maxp}(a) - m(P-1). \tag{1}$$

$\mathrm{Maxp}(a)$ は a の最大素因子を指している.

この式を満たす a を m だけ平行移動した底が P の広義の究極の完全数と呼ぶ.

5 完全数の垂直展開

$P = 3, 5, 7, 11, \cdots$ のおのおのに関して水平展開をする.

これらについて, $P=2$ の場合の解の型がどの程度維持されるかを調べることが興味ある課題である.

6　桐山の完全数

高専 2 年生桐山君は 完全数で使われる 2 を一般化することを試み素数 P をとりある自然数 n に対して $\sigma(P^n)$ がまた素数の場合を調べることにした. そして $q=\sigma(P^n)$ とおいた.

$\overline{P}=P-1$ を使うと

$$\overline{P}q=(P-1)\sigma(P^n)=P^{n+1}-1.$$

そこで $a=P^nq$ とおくとき $\sigma(a)=\sigma(P^n)\sigma(q)$ に $\overline{P}$ をかけて,

$$\begin{aligned}\overline{P}\sigma(a)&=(P^{n+1}-1)(q+1)\\&=P^{n+1}q+P^{n+1}-(q+1)\\&=Pa+P^{n+1}-1-q\\&=Pa+(P-2)\sigma(P^n).\end{aligned}$$

かくて,

$$\overline{P}\sigma(a)-Pa=(P-2)\sigma(P^n) \tag{2}$$

ができた.

与えられた素数 P と自然数 n に対し式

$$(P-1)\sigma(a)-Pa=(P-2)\sigma(P^n)$$

を a についての方程式とみなす. この解として出てくる数は完全数の一般化になると桐山君は考えた.

ここではこの解を桐山の完全数ということにする.

7　m だけ平行移動した桐山の完全数

桐山の完全数の場合も平行移動を考えてみた.

$q=\sigma(P^e)+m$(q は素数) と仮定する.

$a=P^eq$ とおくとき $\overline{P}(q-m)=P^{e+1}-1$ および $q-m=\sigma(P^e)$ なので

$$\begin{aligned}\overline{P}\sigma(a) &= (P^{e+1}-1)(q+1)\\ &= Pa + P^{e+1} - q - 1\\ &= Pa - q + (q-m)\overline{P}\\ &= Pa - q + (q-m)(P-2+1)\\ &= Pa + (q-m)(P-2) - m\\ &= Pa - m + (P-2)\sigma(P^e)\end{aligned}$$

ゆえに次の式ができるがこれを a についての方程式とみる.

$$\overline{P}\sigma(a) - Pa = (P-2)\sigma(P^n) - m.$$

この方程式の解を与えられた P, n, m に対し m だけ平行移動した桐山の完全数という.

7.1 m だけ平行移動した桐山の完全数の計算例

表 6: $[P=3, n=2, m=-2](a < 2\times 10^6)$; m だけ平行移動した桐山の完全数

e	a	素因数分解
2	99	$3^2 * 11$
	147	$3 * 7^2$
4	18387	$3^4 * 227$
	100347	$3 * 13 * 31 * 83$
	145915	$5 * 7 * 11 * 379$

$a = 99 = 3^2 * 11$ と $a = 18387 = 3^4 * 227$ は正規形の解.

さらに非正規形の解がいくつかでてきた.

$a = 147 = 3 * 7^2$ は尾の部分が持ち上がって 2 つに割れた twin tail (ウルトラマンの怪獣) を連想させる.

$a = 100347 = 3 * 13 * 31 * 83$ と $a = 145915 = 5 * 7 * 11 * 379$ はオビの拡張形.

$m = 0$ の場合は非正規形の解は未発見.

ここで出てきた解はいろいろあってまことに興味深い.

$a = 153 = 3^2 * 17$, $a = 1917 = 3^3 * 71$, $a = 18873 = 3^4 * 233$, $a = 174717 = 3^5 * 719$. これらは正規形の解

表 7: $[P=3,n=2,m=4](a<2\times10^6)$; m だけ平行移動した桐山の完全数

e	a	素因数分解
2	153	3^2*17
	957	$3*11*29$
3	1917	3^3*71
4	18873	3^4*233
	24957	$3^2*47*59$
	29637	$3^2*37*89$
	67077	$3^2*29*257$
	138237	$3*11*59*71$
5	174717	3^5*719
	201597	$3*11*41*149$

$a=957=3*11*29$, $a=24957=3^2*47*59$, $a=29637=3^2*37*89$, $a=67077=3^2*29*257$. これらは 3^eqr 型の解

$a=138237=3*11*59*71, a=201597=3*11*41*149$. これらはオビの拡張形.

8 フェルマ完全数

2 だけ平行移動した狭義の完全数は, $q=2^{2^m}+1$ が素数のとき $a=2^{2^m-1}q$ になる. ここにおいて, $q=F_m=2^{2^m}+1$ はフェルマ素数なので $a=2^{2^m-1}q$ をフェルマ完全数という.

フェルマ素数は 5 個しか知られていないので素数条件をはずして, フェルマ数について考えた場合 $a=2^{2^m-1}q$ をフェルマー弱完全数という.

P が奇素数のとき $L_m=\dfrac{P^{2^m}+1}{2}$ が素数のとき, $a_m=P^{2^m-1}L_m$ を底が P のフェルマ完全数という. 素数条件をはずして底が P のフェルマ弱完全数を考えてもよい. この場合, フェルマ完全数の方程式は考えなくてもよい.

8.1 例

表 8: $P = 2$; Fermat　弱完全数

m	2^m	a_m	(F_m)=素因数分解
0	1	3	(3)=3
1	2	10	(5)=5
2	4	136	(17)=17
3	8	32896	(257)=257
4	16	2147516416	(65537)=65537
5	32	9223372039002259456	$(4294967297) = 641 * 6700417$
6	64	A	B

$A = 170141183460469231740910675752738881536$
$B = (18446744073709551617) = 274177 * 67280421310721$

9　P を底とするフェルマの (弱) 完全数

Fermat 完全数を底の概念を導入して一般化しよう.

P を奇素数とし $E > 0$ について $R = P^E + 1$ とおく. これ は偶数なので $L_E = \frac{R}{2}$ とする. L_E を素数とすると, E は 2 のべきになるので $E = 2^m, (m > 0)$ とかける.

一般に $E = 2^m$ とかけるとき L_E は奇数であることが証明できる.

実際,L_E は偶数であると仮定する. すなわち $L_E = \frac{R}{2} = 2L'$ とすると $R = 4L'$ なので

$$R = P^E + 1 = 4L' \equiv 0 \mod 4.$$

ゆえに, $P^E \equiv -1$. 一方, $P = 2k + 1$ とおくとき

$$P^E = (2k + 1)^{2^m} \equiv 1 \mod 4.$$

これで前の式に矛盾した.

以上を踏まえて, $E = 2^m$ のとき $L_m = \frac{P^E+1}{2}$ とおく.
これは奇数であり, P を底とするフェルマ数と理解する.
ただし,$P = 2$ のとき $E = 2^m, L_m = F_m = P^E + 1$ とおく.

補題 1 $e > 1$ について L_m の素因子 Q は $P - 1$ の因子にならない.

$a_m = P^{2^m-1}L_m$ を P が **底のフェルマの弱完全数**と定義する.
L_m が素数の場合なら, a_m を P が**底のフェルマの完全数**と呼ぶ.

フェルマの弱完全数はフェルマの完全数に比べて豊富な例を持っている. しかも, フェルマの完全数で言えたことは弱完全数でも成り立つ事がある.

一般の底の場合でもフェルマの完全数は数が少ない. 研究対象が少ないのは研究上不利だ.

一方, 弱完全数は無限にあるので研究材料として有利である.

9.1 $P = 3$

$P = 3$ のときの Fermat 弱完全数を計算してみよう.
ここで面白い例が出なければ, 底を一般化する試みは失敗したとも言える.

表 9: $P = 3$; Fermat 弱完全数

m	2^m	a	(L_m)=素因数分解
1	2	15	(5)=5
2	4	1107	(41)=41
3	8	7175547	$(3281) = 17 * 193$
4	16	308836705316427	(21523361)=21523361
5	32	A	B
6	64	C	D
7	128	E	F

$A = 572280636715419056279672990187$
$B = (926510094425921) = 926510094425921$
$C = 196503076295643052858681214356932539158308401746008315969770 7$
$D = (171684191014625624232892454464 1) = 17168419101462562423289245446 41$
$E = 231680753961907887941566311316[62digits]771379200003876302731668088747$
$F = (589509228886929158576043643070625933283910579613792055454848 1)$
$= 257*275201*138424618868737*391378628151452492 9*153849834853910661121$

10　真正 Fermat 完全数

P : 奇素数, 平行移動 m の真正 (第二種) Fermat 完全数を次のように定義する.
$q = \dfrac{P^e + 1}{2} + m$: 素数と仮定する. すると, $2(q - m) = P^e + 1$.
$a = P^{e-1}q$ を狭義の真正 Fermat 完全数という.
$N = P^e - 1$ とおくとき, $a = P^{e-1}q$ について,

$$\sigma(a) = \sigma(P^{e-1}q) = \frac{P^e - 1}{\overline{P}}(q + 1)$$

なので分母を払い,

$$\overline{P}\sigma(a) = N(q + 1) = (N + 1)q + N - q.$$

$(N + 1)q = Pa, 2(q - m) - 1 = P^e = N + 1$ によれば, $N = 2(q - m - 1)$.

ゆえに,

$$\overline{P}\sigma(a) - Pa = (N+1)q + N - q - (N+1)q = N - q = q - 2(m+1).$$

$q =$Maxp(a) を用いて

$$\overline{P}\sigma(a) - Pa = Maxp(a) - 2(m+1).$$

これを真正 Fermat 完全数の方程式といい, これを満たす a を広義の真正 Fermat 完全数という.

10.1 計算結果

表 10: $P = 3, m = -5$, のときの解

a	factor
147	$3 * 7^2$
3185	$5 * 7^2 * 13$
50373	$3^2 * 29 * 193$

表 11: $m = -3$, のときの解

a	factor
99	$3^2 * 11$
759	$3 * 11 * 23$
795339	$3^6 * 1091$

表 12: $m = -2$, のときの解

a	factor
27755	$5 * 7 * 13 * 61$
218225	$5^2 * 7 * 29 * 43$

表 13: $m = 0$ のときの解

a	factor
15	$3 * 5$
741	$3 * 13 * 19$
1107	$3^3 * 41$
14883	$3 * 11^2 * 41$
38781	$3^2 * 31 * 139$

$15 = 3 * 5$

$1107 = 3^3 * 41$

正規形以外の解が意外に多い.
第二正規形もそこそこある.

表 14: $P = 3, m = 1$ のときの解

a	factor
3	3
9	3^2
27	3^3
81	3^4
243	3^5
729	3^6
2187	3^7
6561	3^8
19683	3^9
59049	3^{10}
99807	$3 * 17 * 19 * 103$
177147	3^{11}
531441	3^{12}
603681	$3 * 13 * 23 * 673$
1594323	3^{13}

$m = 1$ のときは 3^e は直ちにわかるように解である.
しかしそれ以外の解がでてきた. どれもオビである.

$$\overline{P}\sigma(a) - Pa = Maxp(a) - 2(m+1).$$

において, $a = P^e$
が解と仮定すると $\overline{P}\sigma(a) - Pa = (P^{e+1} - 1) - P^{e+1} = -1$ なので

$$-1 = P - 2(m+1).$$

ゆえに, $m = \frac{P+1}{2} - 1 = m = \frac{P-1}{2}$
$P = 3, m = 1$
$P = 5, m = 2$
$7^2 * 13$ は正規解ではない.
$P = 7m = 3$ のときの解は $a = 7^e$ の他の解は未発見.

表 15: $P = 5, m = 2$ のときの解

a	factor
25	5^2
125	5^3
625	5^4
637	$7^2 * 13$
3125	5^5
15625	5^6

表 16: $P = 3, m = 2$ のときの解

a	factor
21	$3 * 7$
1161	$3^3 * 43$
89181	$3^5 * 367$

正規解がある.

表 17: $P = 3, m = 3$ のときの解

a	factor
5	5
153	$3^2 * 17$
27639	$3^2 * 37 * 83$
51417	$3^2 * 29 * 197$
799713	$3^6 * 1097$
965007	$3^3 * 103 * 347$

表 18: $P = 3, m = 5$ のときの解

a	factor
7	7
171	$3^2 * 19$
10287	$3^4 * 127$

10.2 正規形の解

表 19: $P = 3, m = 0$ のときの解

a	factor
15	$3 * 5$
1107	$3^3 * 41$
308836705316427	$3^{15} * 21523361$
572280636715419056279672990187	$3^{31} * 926510094425921$
A	B

A=19650307629564305285868121435693253915830840174600831596977
B=$3^{63} * 1716841910146256242328924544641$

表 20: $P = 3, m = 2$ のときの解

a	factor
21	$3 * 7$
1161	$3^3 * 43$
89181	$3^5 * 367$
581179941	$3^9 * 29527$
C	D

C= 2995017166524052017355299716202601385179261075182205454 01
$D = 3^{59} * 211955791376081017571472166 03$

10.3　真正フェルマ完全数の B 型解

$$\overline{P}\sigma(a) - Pa = Maxp(a) - 2(m+1).$$

これを真正 Fermat 完全数の方程式といい, これを満たす a を広義の真正 Fermat 完全数という.

表 21: $P = 5, m = -9, a < 200$ のときの解

a	factor
15	$3 * 5$
21	$3 * 7$
33	$3 * 11$
39	$3 * 13$
51	$3 * 17$
57	$3 * 19$
69	$3 * 23$
87	$3 * 29$
93	$3 * 31$
111	$3 * 37$
123	$3 * 41$
129	$3 * 43$

$a = 3p$ が解でありこれを通常解という.
これを一般にすることを考えてみた.
$Q = P - 2$ は素数と仮定して, $a = Qq$ は次の方程式の解と仮定する.

$$\overline{P}\sigma(a) - Pa = Maxp(a) - 2(m+1).$$

Maxp$(a) = q$ に注意する.

$$\overline{P}\sigma(a) - Pa = q - 2(m+1).$$

$\sigma(a) = (Q+1)(q+1) = (P-1)(q+1)$ により
$\overline{P}\sigma(a) - Pa = \overline{P}^2 q + \overline{P}^2 - P(P-2)q$ なので

$$\overline{P}^2 q + \overline{P}^2 - P(P-2)q = q - 2(m+1).$$

$\overline{P}^2 q - P(P-2)q$ なので, q が消えて

$$\overline{P}^2 = -2(m+1).$$

これを m について解くと

$$m+1=-\frac{\overline{P}^2}{2}.$$

$P=5$ なら $Q=3$, $m+1=-8$. よって, $m=-9$.

$Q=P-2$:素数, $m=-\frac{\overline{P}^2}{2}-1$ とおくとき, $a=Qq$ が解であり, B 型の解である.

$Q, P=Q+2$ はともに素数であり (Q,P) はいわゆる双子素数である. 双子素数は無数にあるという予想があるが未解決.

表 22: $P=5$ のときの B 型解を与える P

a	factor			
twin	P	$Q=P$	$(P-1)^2/2$	m
	5	3	8	-9
	7	5	18	-19
x	9	7	32	-33
x	11	9	50	-51
	13	11	72	-73
x	15	13	98	-99
x	17	15	128	-129
	19	17	162	-163
x	21	19	200	-201
x	23	21	242	-243
x	25	23	288	-289
x	27	25	338	-339
x	29	27	392	-393
	31	29	450	-451
x	33	31	512	-513

twin に x が書かれているのは双子素数にならない場合.

11 劣完全数

ユークリッドの完全数の定義 $p=2^{e+1}-1$ の 2 を奇素数 P に変更し $2^{e+1}-1$ の代わりに $P^{e+1}-1$ としさらに平行移動を考えることは十分意義のあることである.

$q=P^{e+1}-1+m$ が素数のとき $a=P^eq$ を底 P, 平行移動 m の狭義の劣完全数 (subperfect number) といい, このときの q をサブ素数 (subprime number) という.

ここで劣完全数の方程式の導入を行う.

劣完全数 $a = P^e q$ について

$$\overline{P}\sigma(a) = \overline{P}\sigma(P^e q) = (P^{e+1} - 1)(q + 1) = Pa - (q + 1 - P^{e+1})$$

$q = P^{e+1} - 1 + m$ によれば $q + 1 - P^{e+1} = m$ なので

$$\overline{P}\sigma(a) = Pa - m.$$

究極の完全数の場合と比べて簡明な式になった. この方程式の解を底 P, 平行移動 m の広義の劣完全数 (subperfect number with translation parameter m) というのである.

広義の劣完全数を簡単に劣完全数という.

$P > 2$ なら, $m = 0$ のとき $P^{e+1} - 1 + m$ は素数にならない. これを克服するために $\sigma(P^e)$ を使うことになり $q = \sigma(P^e) - 1 + m$ が素数のとき $a = P^e q$ を究極の完全数という.

しかし, m によっては $P^{e+1} - 1 + m$ は素数なのでこのようにしても一向構わない.

劣完全数の研究は現在進行中であり, 興味ある結果が多数得られている.

12 $P \geq 3$, 平行移動 $m = 0$ の劣完全数

狭義の劣完全数の場合は, $q = P^{e+1} - 1 + m$ が素数なので, $P \geq 3$ であれば, m : 奇数になる.

広義の劣完全数ではあえて, m : 偶数でも考える. とくに $m = 0$ の場合は興味があり, 次の結果が得られている.

(これは平行移動 m の 完全数の場合, その解の完全決定にはどれも成功しないことに比べるとまことに著しい結果である)

命題 1 $P = 3, a = 2$ 以外なら $P \geq 3$, 平行移動 $m = 0$ の広義の劣完全数は存在しない.

Proof.

素因数分解の一意性から, $\sigma(a)$ は P で割れるので,$\sigma(a) = P^\varepsilon L$($L$ は P で割れない) とかける.

$$\overline{P}\sigma(a) = \overline{P}P^\varepsilon L = Pa.$$

これより, $a = P^{\varepsilon-1}L\overline{P}$. $N = P^\varepsilon - 1, M = \overline{P}L$ とおけば $a = P^{\varepsilon-1}M, Pa = (N + 1)M$. M は P で割れないから,

$$\sigma(a) = \sigma(M)\sigma(P^{\varepsilon-1}).$$

$$\overline{P}\sigma(a) = \sigma(M)(P^{\varepsilon} - 1) = N\sigma(M).$$

$\overline{P}\sigma(a) = Pa$ によって,

$$N\sigma(M) = (N+1)M.$$

これより

$$\frac{N}{N+1} = \frac{M}{\sigma(M)}.$$

$\dfrac{N}{N+1}$ は既約分数なので, $M = kN, \sigma(M) = k(N+1)$ を満たす整数 k が存在する. 2 つの式を引いて,

$$\sigma(M) - M = k.$$

$M = kN$ により, k も M の約数なので, $\sigma(M) = M + k$ から M は素数で,$k = 1$ となる.

$M = \overline{P}L$ が素数なので $\overline{P} = 2, L = 1$.

書き直すと $P = 3, L = 1$ のとき $a = 2$. これ以外なら $M = \overline{P}L$ は素数ではないので矛盾.

(この証明は オイラーが行った, 偶数完全数はユークリッドの完全数の証明と類似している)

注意. $P = 2$ でも同じ論法がある程度使える. しかし

$a = 2^{\varepsilon-1}L$ になり, a : 奇数とすると, $\varepsilon - 1 = 0$. $a = L = M$, になり $\sigma(L) = 2L$. ここから矛盾はでない.

13 $P \geq 3$, 平行移動 $m = P - 1$ の劣完全数

定理 1 $P \geq 3$, 平行移動 $m = \overline{P}$ の劣完全数は存在しない.

Proof.

$\overline{P}\sigma(a) - Pa = -\overline{P}$ によって, $\overline{P}(\sigma(a) + 1) = Pa$ になるので, 素因数分解の一意性から, $\sigma(a) + 1 = P^{\varepsilon}L$ (L は P で割れない) と書ける.

$\overline{P}P^{\varepsilon}L = Pa$ になり, $M = L\overline{P}, N = P^{\varepsilon}-1$ とおくとき $Pa = P^{\varepsilon}M = (N+1)M$.

$$\sigma(a) = \sigma(M)\sigma(P^{\varepsilon-1}) = \sigma(M)\frac{P^{\varepsilon} - 1}{\overline{P}}.$$

これを変形して

$$\overline{P}\sigma(a) = \sigma(M)(P^{\varepsilon} - 1) = \sigma(M)N.$$

$\overline{P}\sigma(a) + \overline{P} = Pa = (N+1)M$ によって,

$$\sigma(M)N + \overline{P} = (N+1)M.$$

1. $L \neq \overline{P}, L \geq 2$ のとき.
$P \geq 3$ なので $M = L\overline{P}$ により, $M, L, \overline{P}, 1$ は M の相異なる約数である.
$N = P^{\varepsilon} - 1, \sigma(M) \geq M + L + \overline{P} + 1 = M + L + P$ を使うと,

$$\sigma(M)N \geq (M + L + P)N.$$

$$\begin{aligned}(N+1)M - \overline{P} &= \sigma(M)N \\ &\geq (M + L + P)N \\ &= M(N+1) - M + (L+P)N\end{aligned}$$

これより, $N \geq \overline{P}$ を用いると

$$L\overline{P} - \overline{P} = M - \overline{P} \geq (L+P)N \geq L\overline{P} + PN.$$

しかし $-\overline{P} > PN$ は矛盾.

2. $L = \overline{P}$ のとき.
$\sigma(M) \geq M + L + 1$ を得るので

$$\begin{aligned}(N+1)M - \overline{P} &= \sigma(M)N \\ &\geq (M + L + 1)N \\ &= M(N+1) - M + LN + N\end{aligned}$$

これより, $M = L\overline{P} = \overline{P}^2$ に留意して

$$M - \overline{P} \geq LN + N \geq L\overline{P} + \overline{P}.$$

これも矛盾.

3 . $L = 1$ のとき. $M = \overline{P}$.

$$\sigma(M)N + \overline{P} = \sigma(\overline{P})N + \overline{P}, (N+1)M = (N+1)\overline{P}.$$

これより

$$\sigma(\overline{P})N + \overline{P} = (N+1)\overline{P}.$$

$\sigma(\overline{P})N = N\overline{P}$ により $\sigma(\overline{P}) = \overline{P}$. よって $\overline{P} = 1; P = 2$. 仮定に反する.

14 $P \geq 3$, 平行移動 $m = -\overline{P}$ の劣完全数

定理 2 $P \geq 3$, 平行移動 $m = -\overline{P}$ の劣完全数は $P = 3, a = 2^2$.

Proof.

$\overline{P}\sigma(a) - Pa = \overline{P}$ によって, $\overline{P}(\sigma(a) - 1) = Pa$ になるので, 素因数分解の一意性から, $\sigma(a) - 1 = P^{\varepsilon}L$ (L は P で割れない) と書けるので,

$$\sigma(a) = \sigma(M)\sigma(P^{\varepsilon-1}) = \sigma(M)\frac{P^{\varepsilon} - 1}{\overline{P}}.$$

これを変形して

$$\overline{P}\sigma(a) = \sigma(M)(P^{\varepsilon} - 1) = N\sigma(M).$$

$\overline{P}\sigma(a) - \overline{P} = Pa = (N+1)M$ によって,

$$\sigma(M)N - \overline{P} = (N+1)M.$$

1. $L \neq \overline{P}, L > 1$.

$P \geq 3$ なので $M = L\overline{P}$ により, $M, L, \overline{P}, 1$ は M の相異なる約数である.

$N \geq \overline{P}, \sigma(M) \geq M + L + \overline{P} + 1 = M + L + P$ を使うと, 基本方程式

$$\sigma(M)N - \overline{P} \geq (N+1)M$$

が得られる.

$$(\sigma(M) - M)N = \overline{P} + M.$$

これを次のように計算する.

$$\begin{aligned}\overline{P} + M &= (\sigma(M) - M)N \\ &\geq (L+P)N \\ &\geq (L + \overline{P} + 1)\overline{P} \\ &\geq M + (\overline{P} + 1)\overline{P}\end{aligned}$$

これより,

$$\overline{P} + M \geq M + (\overline{P} + 1)\overline{P}.$$

かくして $0 \geq (\overline{P} + 1)^2$.

2. $L = \overline{P}$.
このとき,$M = L\overline{P} = L^2$, $\sigma(M) - M \geq L + 1 =$.

$$\begin{aligned} \overline{P} + M &= (\sigma(M) - M)N \\ &\geq PN \\ &\geq P\overline{P} \\ &\geq \overline{P}^2 + \overline{P}. \end{aligned}$$

$M = \overline{P}^2$ なので　等号が成り立ち, $N = \overline{P}$.
$\alpha = P - 1$ とおくとき $M = \alpha^2$, $\sigma(M) = \sigma(\alpha^2) = 1 + \alpha + \alpha^2$.
$\sigma(\alpha^2) = 1 + \alpha + \alpha^2$ により, $\alpha = P - 1$ は素数. $P = 3, \alpha = 2, a = M = 4$.
3. $L = 1$.
$M = \overline{P}$ になるので基本方程式

$$(\sigma(\overline{P}) - \overline{P})N = \overline{P} + \overline{P} = 2\overline{P}$$

により $N \geq \overline{P}$ を用いて

$$2\overline{P} \geq (\sigma(\overline{P}) - \overline{P})\overline{P}.$$

$\overline{P}$ で除して

$$2 \geq \sigma(\overline{P}) - \overline{P}.$$

$\overline{P} = 2\alpha > 2$ とおくと

$$2 \geq \sigma(2\alpha) - 2\alpha \geq 1 + \alpha.$$

ゆえに $\alpha = 1, P = 2$; 矛盾.

15　$P=3$,m は 偶数の場合

$P=3$ とする.

$2\sigma(a)-3a=-m$ になる. m : 偶数の場合 $m \leq -40$ の範囲についてコンピュータで表を作ってみた.

```
"m="-40
factor(52)=2^2*13
"m="-38
"m="-36
factor(44)=2^2*11
factor(50)=2*5^2
"m="-34
"m="-32
"m="-30
factor(32)=2^5
"m="-28
factor(28)=2^2*7
"m="-26
"m="-24
factor(18)=2*3^2
factor(20)=2^2*5
"m="-22
"m="-20
factor(12)=2^2*3
"m="-18
"m="-16
"m="-14
factor(16)=2^4
"m="-12
"m="-10
```

$m=-6$ のとき $a=2p.\ p>$: 素数, の解が出てくる.

$\sigma(2p)=3p+3$ なので $2\sigma(a)-3a=6p+6-6p=6$.

これはいわゆる通常解で,B 型の解である.

```
"m="-4
"m="-2
factor(4)=2^2
"m="0
```

```
factor(2)=2
"m="2
"m="4
"m="6
"m="8
"m="10
"m="12
"m="14
"m="16
"m="18
"m="20
```

これから推察できることは $m>0$ なら解がなく, $m=0$ なら $a=2$　が解.

$m=-2$ なら $a=4$　が解. $m=-6$ を飛ばすと, $m=-14a=2^4$ まで解がなく次は $m=-20, a=12$.

これらのことを以下で証明する.

$$\overline{P}\sigma(a)=Pa-m$$

に $P=3, m=-2\nu$ を代入すると $2\sigma(a)=3a+2\nu$.

$2(\sigma(a)-\nu)=3a$ と整理すると,

$\sigma(a)-\nu=3^{\varepsilon}L$, ($L,3$ は互いに素) にできる.

これより, $3^{\varepsilon}L=3a$ が成り立ち, $a=2L3^{\varepsilon-1}$ とかける. $M=2L$ とおけば $a=3^{\varepsilon-1}M$.

$M=3^{\varepsilon 1-1}$ とおくとき,

$$3a=3^{\varepsilon}M=(N+1)M.$$

$$2\sigma(a)=N\sigma(M).$$

$2\sigma(a)=N\sigma(M), 3a=3^{\varepsilon}M=(N+1)M$ なので,

$2\sigma(a)=N\sigma(M), 3a+2\nu=(N+1)M+2\nu$. かくて次の基本方程式ができた.

$$N\sigma(M)=(N+1)M+2\nu.$$

1.　$L=1$ のとき.

$M=2L=2$ なので

$$3N=2(N+1)+2\nu.$$

$$2\nu N - 2 = 3^{\varepsilon} - 3.$$

これより $\nu = \dfrac{3^{\varepsilon}-3}{2}$.

逆に $\nu = \dfrac{3^{\varepsilon}-3}{2}$ として方程式 $2\sigma(a) - 3a = 2\nu = 3^{\varepsilon} - 3$ ができる.

$a = 2 \cdot 3^{\varepsilon-1}$ とおくとき,

$$2\sigma(a) - 3a = 3 \cdot (3^{\varepsilon} - 1) - 2 \cdot 3^{\varepsilon} = 3^{\varepsilon} - 3 = 0.$$

表 23: $P = 3$; $2\sigma(a) - 3a = 2\nu$ の解ひとつ

ε	1	2	3	4	5	6	7
ν	0	6	24	78	240	726	2184
$m = 2\nu$	0	12	48	156	480	1452	4368
a	2	6	18	54	162	486	1458

2. $L \geq 2, L \neq 2$ のとき.

M の約数として $M = 2L, L, 2, 1$ があるので $N \geq 2$ により

$$N(\sigma(M) - M) = M + 2\nu \geq 2(L + 3) = M + 6.$$

$\nu \geq 3$ になる.

$\nu = 3$ のとき, $N = 2, \sigma(M) - M = 3$. よって, $\varepsilon = 1$. L:素数 $p > 2$.

$a = 6p$ となる.

$\mathrm{co}\sigma(a) = \sigma(a) - a$ (ユークリッドの余関数) を使うと

$$N(co\sigma(M) - M) = M + 2\nu$$

これ以上続けるには時間がない.

16 ユークリッドの余関数の評価

$\mathrm{co}\sigma(a) = \sigma(a) - a$ はユークリッドの余関数の定義式である. これの評価式を作らないと劣完全数の決定問題が解けない.

$q = \mathrm{Maxp}(a)$ とおき $a = q^j\alpha, \alpha$ は p で割れないとする.

定理 3 $q = Maxp(a)$ とする. $a = q^j\alpha, (\alpha > 1, q \not| \alpha)$ のとき

$co\sigma(q^j\alpha) = \sigma(q^j)co\sigma(\alpha) + \alpha\sigma(q^{j-1})$.

$co\sigma(q^j\alpha) \geq \sigma(q^j) + \alpha\sigma(q^{j-1})$.

$co\sigma(q^j\alpha) = \sigma(q^j) + \alpha\sigma(q^{j-1})$ なら α は素数.

Proof.

$\sigma(q^j\alpha) = \dfrac{(q^{j+1}-1)\sigma(\alpha)}{\overline{q}}$ なので

$$\begin{aligned} co\sigma(q^j\alpha) &= \sigma(q^j\alpha) - q^j\alpha \\ &= \frac{(q^{j+1}-1)\sigma(\alpha) - q^j\alpha(q-1)}{\overline{q}} \\ &= \frac{(q^{j+1}-1)(co\sigma(\alpha)+\alpha) - q^j\alpha(q-1)}{\overline{q}} \\ &= \frac{(q^{j+1}-1)co\sigma(\alpha) + (q^j-1)\alpha)}{\overline{q}} \\ &= \sigma(q^j)co\sigma(\alpha) + \sigma(q^{j-1})\alpha \end{aligned}$$

以上によって,

$$co\sigma(q^j\alpha) = \sigma(q^j)co\sigma(\alpha) + \sigma(q^{j-1})\alpha.$$

$A = \sigma(q^j) + \alpha\sigma(q^{j-1})$ とおくとき

$$\begin{aligned} co\sigma(q^j\alpha) - A &= \sigma(q^j)co\sigma(\alpha) + \sigma(q^{j-1})\alpha - A \\ &= \sigma(q^j)(co\sigma(\alpha) - 1) \\ &\geq 0. \end{aligned}$$

$co\sigma(q^j\alpha) - A$ が成り立つなら,$co\sigma(\alpha) - 1 = 0$. このとき α が素数となる.

これは次の結果の類似である.

(小室慶太が研究したオイラー余関数の基本公式).

定理 4 $a = q^j\alpha, (\alpha > 1, q \not| \alpha)$ のとき

$$co\varphi(q^j\alpha) = q^{j-1}(\alpha + \overline{q}co\varphi(\alpha))$$

$$co\varphi(q^j\alpha) \geq q^{j-1}(\alpha + \overline{q}).$$

$co\varphi(q^j\alpha) = q^{j-1}(\alpha + \overline{q})$ なら α は素数.

Proof.
$co\varphi(\alpha) = \alpha - \varphi(\alpha)$ により $-\varphi(\alpha)$ を $co\varphi(\alpha) - \alpha$　で置き換える.

$$\begin{aligned} co\varphi(q^j\alpha) &= q^j\alpha - \varphi(q^j\alpha) \\ &= q^j\alpha - \overline{q}q^{j-1}\varphi(\alpha) \\ &= q^{j-1}(q\alpha + \overline{q}(co\varphi(\alpha) - \alpha))) \\ &= q^{j-1}(\alpha + \overline{q}co\varphi(\alpha)) \end{aligned}$$

よって,

$$co\varphi(q^j\alpha) = q^{j-1}(\alpha + \overline{q}co\varphi(\alpha)) \geq q^{j-1}(\alpha + \overline{q}).$$

$B = q^{j-1}(\alpha + \overline{q})$ とおき

$$co\varphi(q^j\alpha) - B = q^{j-1}(q-1)(co\varphi(\alpha) - 1) \geq 0.$$

$$co\varphi(q^j\alpha) \geq B = q^{j-1}(\alpha + \overline{q}).$$

$co\varphi(q^j\alpha) = q^{j-1}(\alpha + \overline{q})$ なら $co\varphi(\alpha) - 1 = 0$. よって, α は素数.

$\mathrm{co}\sigma(q^j) = \sigma(q^{j-1})$ が成り立つ. $\mathrm{co}\ \varphi(q^j) = q^{j-1}$ も便利な公式である.

次の公式を見比べてみよう.
$co\varphi(q^j\alpha) = q^{j-1}\overline{q}co\varphi(\alpha)) + \alpha q^{j-1}$,
$\mathrm{co}\sigma(q^j\alpha) = \sigma(q^j)\mathrm{co}\sigma(\alpha) + \alpha\sigma(q^{j-1})$
かなり類似性の高い公式とみてもよい.