フェルマ 完全数とは何か

飯高 茂

平成 31 年 5 月 28 日

1　フェルマ 完全数

完全数の定義を参考にして

$$\sigma(a) = 2a - 2$$

を満たす a を調べよう. a を偶数と仮定して $a = 2^e q, (q = 2^{e+1} + 1 : \text{素数})$ の形になることを示したい. しかしこれが難しい.

実際, $a = 2^e L, (L\text{:奇数})$ と表し $\sigma(a) = (2^{e+1} - 1)\sigma(L)$ と書き, $N = 2^{e+1} - 1$ とおくと, $\sigma(a) = N\sigma(L)$, $2a - 2 = 2^{e+1}L - 2 = (N + 1)L - 2$.

$$\sigma(a) = N\sigma(L) = (N + 1)L - 2$$

ゆえに, $N(\sigma(L) - L) = L - 2$.

完全数の場合なら, $\sigma(a) = 2a$ を満たすので $N(\sigma(L) - L) = L$ になる. よって, $d = \sigma(L) - L$ が L の約数になり, 議論が進む.

しかし今の場合は $N(\sigma(L) - L) = L - 2$ を満たすので d が $L - 2$ の約数になるだけでこれ以上議論が進まない. いわゆるデッドロックである.

そこで $\sigma(a) = 2a - 2$ を満たすとき ,$a = 2^e q, (q : \text{素数})$ の形をしていると仮定しよう.

定義から

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

となりこれより $q = 2^{e+1} + 1$ をえる.

$q = 2^{e+1} + 1$ が素数のとき $e + 1$ は 2 のべき, すなわち 2^m とかける.

そこで $F_m = 2^{2^m} + 1$ と書ける数 F_m を フェルマ 数. とくに素数になるときフェルマ 素数という.

$m = 0, 1, 2, 3, 4$ のとき F_m は素数になる. これら以外のフェルマ 素数は知られていない. 6 番目のフェルマ 素数はあるかどうかまったく分からない. もし見つかれば, ニューヨークタイムズのトップ記事になったとしても不思議ではない.

そこでユークリッドの完全数にならって,$e = 2^m - 1$ とするとき

- F_m がフェルマ 素数のとき $2^e F_m$ をフェルマ 完全数
- F_m がフェルマ 数のとき $2^e F_m$ をフェルマ 弱完全数

と言うことにする.

フェルマ 完全数は 5 個しか知られていないが, フェルマ 弱完全数なら無限にある. したがって研究しやすい.

1.1 数値例

表 1: $P = 2$; フェルマ 弱完全数

m	2^m	$e = 2^m - 1$	$a_m = 2^e F_m$	(F_m)=素因数分解
0	1	0	3	(3)=3
1	2	1	10	(5)=5
2	4	3	136	(17)=17
3	8	7	32896	(257)=257
4	16	15	2147516416	(65537)=65537
5	32	31	9223372039002259456	(4294967297)=641*6700417
6	64	63	A	B
7	128	127	C	D

A= 170141183460469231740910675752738881536

B= (18446744073709551617)=274177*67280421310721

C= 57896044618658097711785492504343953926805133516280751251460479307672448925696

D= (340282366920938463463374607431768211457)=59649589127497217*5704689200685129054721

1.2 フェルマ の弱完全数

普通の完全数 (ユークリッドの完全数) の最初の 4 つは 6,28,496,8128 であり, その末尾 1 桁の数は 6 または 8. この性質はユークリッドの発見による.

フェルマ の弱完全数ではどうか.

最初の 4 つは 3,10,136,32896 であり, その末尾 1 桁の数は (1,2 番を無視して)3 番目からに限ると, 6 である. フェルマ数の末尾 1 桁の数は 3 番目からに限ると, 7 である.

何となく 完全数に近い性質を持っているではないか.

フェルマ の完全数という言い方がすでにあるかどうかわからないが, 新しい用語フェルマ の完全数 をここで提案する次第である. そこで読者もフェルマ の完全数 の宣伝, 広報の仕事に参加してほしい.

10 を街で見かけたら, フェルマ の完全数を見つけた, と叫ぼう.

Windows 10 という命名の背後に 10 は 2 番目のフェルマ の完全数だからこの名前がついた, と勝手に思い込むことにしよう.

2　オイラーの結果

フェルマ 数 F_m の素因子を Q とおく.$E = 2^m$ を用いると

$$F_m = 2^E + 1 \equiv 0 \mod Q.$$

$E = 2^m$ によって

$$2^E = 2^{2^m} \equiv -1 \mod Q.$$

ゆえに

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

Q を法とすると 2 の位数は 2^{m+1} の約数であるが $2^E = 2^{2^m} \equiv -1$ によって Q を法とする 2 の位数は 2^{m+1}.

$2^E = 2^{2^m} \equiv -1 \mod Q$ により $Q \neq 2$. フェルマの小定理によって

$2^{Q-1} \equiv 1 \mod Q$. $Q_1 = Q - 1$ は位数 2^{m+1} の倍数なので, $Q_1 = 2^{m+1}K$ と整数 K で表せる.

ここで $K = 1$ なら $Q = Q_1 + 1 = 2^{m+1} + 1$ これもフェルマ素数. この結果はオイラーによる.

$\frac{Q-1}{2} = 2^m K$ によれば

$$2^{\frac{Q_1}{2}} = 2^{2^m K} \equiv (-1)^K \mod Q.$$

オイラーの基準にしたがい $\left(\frac{2}{Q}\right) = 2^{\frac{Q-1}{2}} \mod Q$.

$$\left(\frac{2}{Q_1}\right) = 2^{\frac{Q_1}{2}} \equiv (-1)^K \mod Q.$$

次のようにまとめる.

定理 1 $Q = 1 + 2^{m+1}K$ において

- K が奇数なら *($Q-1$ の 2 の指数は $m+1$ のとき)* $\left(\frac{2}{Q}\right) = -1$. すなわち, Q を法とするとき 2 は平方非剰余.
- K が偶数なら *(Q_1 の 2 の指数は $m+2$ 以上のとき)* $\left(\frac{2}{Q}\right) = 1$. すなわち, Q を法とするとき 2 は平方剰余.

$m = 5, 6, 7$ のフェルマ数について各素因子 Q について $Q_1 = Q - 1$ を素因数分解した結果を次に述べる. これは美しい性質をもっている. Q_1 の素因数 2 の指数 e は m 以上である.

表 2: 素因子 Q

m	Q	$Q_1 = Q - 1$	Q_1 の素因数分解
5	641	640	$[2^7, 5]$
5	6700417	6700416	$[2^7, 3, 17449]$
6	274177	274176	$[2^8, 3^2, 7, 17]$
6	67280421310721	67280421310720	$[2^8, 5, 47, 373, 2998279]$
7	59649589127497217	59649589127497216	A

ここで $A = [2^9, 116503103764643]$

そこで $m = 5$ のとき素因子の 1 つは $Q = 641$ という例外的に小さい値を持っていることに注意しよう. このため F_5 の素因数として 641 がオイラーによって発見されたのである. まさに僥倖としかいいようがない. しかも $Q_1 = Q - 1 = 640 = 2^7 * 5$ という美しい構造を持っている.

3　フェルマ の弱完全数の末尾２桁

$f_m = 2^{2^m}, F_m = f_m + 1, B_m = 2^{2^m - 1}$ とおくと, $B_{m+1} = B_m \times f_m, a_m = B_m \times F_m$.

これを 100 を法として計算すると次の表ができる.

表 3: $P = 2$;, 法は 100

m	2^m	f_m	F_m	B_m	a_m
2	4	16	17	8	36
3	8	56	57	28	96
4	16	36	37	68	16
5	32	96	97	48	56
6	64	16	17	8	36
7	128				96

m と 2^m には周期性がないが, この表により 100 を法とすると f_m , F_m , B_m , a_m には周期 4 の周期性があることがこの表により分かる.

- $m \equiv 2 \mod 4$ ならば $F_m \equiv 17, a_m \equiv 36 \mod 100$.
- $m \equiv 3 \mod 4$ ならば $F_m \equiv 57, a_m \equiv 96 \mod 100$.
- $m \equiv 0 \mod 4$ ならば $F_m \equiv 37, a_m \equiv 16 \mod 100$.
- $m \equiv 1 \mod 4$ ならば $F_m \equiv 97, a_m \equiv 56 \mod 100$.

3.1　フェルマ の弱完全数の末尾３桁

$m = 2$ の行の 3 項以後の 16,17,8,136 が $m = 22$ の行の 3 項以後の 16,17,8,136 と同じなので以後繰り返しがおこる.

$22 - 2 = 20$ なので周期 20 である.

4　P を底とするフェルマの弱完全数

フェルマ 完全数の概念を一般化しよう.

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.

表 4: $P=2$ 法は 1000

m	2^m	f_m	F_m	B_m	a_m
2	4	16	17	8	136
3	8	256	257	128	896
4	16	536	537	768	416
5	32	296	297	648	456
6	64	616	17	808	736
7	128	456	457	728	696
8	256	936	937	968	16
9	512	96	97	48	656
10	1024	216	217	608	936
11	2048	656	657	328	496
12	4096	336	337	168	616
13	8192	896	897	448	856
14	16384	816	817	408	336
15	32768	856	857	928	296
16	65536	736	737	368	216
17	131072	696	697	848	56
18	262144	416	417	208	736
19	524288	56	57	528	96
20	1948576	136	137	568	816
21	2097152	496	497	248	256
22	4194304	16	17	8	136

実際,$L_E = \frac{R}{2} = 2L'$ 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.

5　オイラーの結果の一般化

L_E は奇数なのでその素因子を Q とおくと

$$P^E + 1 = 2L_E \equiv 0 \mod Q.$$

$E = 2^m$ によって

$$P^E = P^{2^m} \equiv -1 \mod Q.$$

ゆえに

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

Q を法とすると P の位数は 2^{m+1} 以下であるが $P^E = P^{2^m} \equiv -1$ によって 2^m より大なので, P の位数は 2^{m+1}.

$P^E = P^{2^m} \equiv -1 \mod Q$ により $Q \neq P$. フェルマの小定理によって

$P^{Q-1} \equiv 1 \mod Q$. $Q-1$ は位数 2^{m+1} の倍数なので, $Q - 1 = 2^{m+1}K$.

この結果は $P = 2$ のときオイラーによる.

$\frac{Q-1}{2} = 2^m K$ によれば

$$P^{\frac{Q-1}{2}} = P^{2^m K} \equiv (-1)^K \mod Q.$$

オイラーの基準にしたがい

$$\left(\frac{P}{Q}\right) = P^{\frac{Q-1}{2}} \equiv (-1)^K \mod Q.$$

次のようにまとめる.

定理 2 $Q = 1 + 2^{m+1}K$ において K が奇数なら *($Q-1$ の 2 の指数は $m+1$ のとき)* $\left(\frac{P}{Q}\right) = -1$. すなわち, Q を法とするとき P は平方非剰余.

$Q = 1 + 2^{m+1}K$ において K が偶数なら *($Q-1$ の 2 の指数は $m+2$ 以上のとき)* $\left(\frac{P}{Q}\right) = 1$. すなわち, Q を法とするとき P は平方剰余.

5.1　$P = 3$

$P = 3$ のときのフェルマ 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.

$A = 57228063671541905627967299 0187$

$B = (926510094425921) = 926510094425921$

$C = 19650307629564305285868121435693253915830840174600831596977 07$

$D = (171684191014625624232892454464 1) = 171684191014625624232892454464 1$

表 5: $P=3$; フェルマ 弱完全数

m	2^m	a_m	(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

5.2 新素数５兄弟

$L_1=5, L_2=41, L_3$ は素数ではない, $L_4=21523361$

$L_5=926510094425921, L_6=1716841910146256242328924544641$

は新しい素数５兄弟である.

フェルマ 素数がフェルマ自身により５つ発見された. しかもフェルマ 数はすべて 素数 に違いないとフェルマは死ぬまで思い込んでいたそうである.

皮肉なことに彼の見出した５つのフェルマ 素数のほかにフェルマ 素数は発見されていない.

ガウス が素数 $p>2$ について正 p 角形の作図可能ならそれはフェルマ 素数であることを示した.

５つのフェルマ 素数をまとめて (フェルマ) 素数５兄弟と呼ぶ.

似たような美しい性質をもつ素数５兄弟がどこかに居てほしい, できたら自分で発見したいと思っていた.

$P=3$ を底とするフェルマ 素数を定義したら, 新しい素数５兄弟がでてきた. これには驚いた.

5.3 素因数 Q について $Q-1$ の素因数分解

$m=7$ に出てくる $L_7=589509228886929158576043643070625933283910579613792055454848 1$ の素因数 Q について $Q_1=Q-1$ の素因数分解をそれぞれ行う.

$Q_1=257-1=256=2^8$.

$Q_1=275201-1=275200=2^8*5^2*43$

$Q_1=138424618868737-1=138424618868736=2^{13}*3*2131*2643131$

$Q_1=3913786281514524929-1=3913786281514524928=2^8*31*787*3919*159898891$

$Q_1=153849834853910661121-1=153849834853910661120=$

$2^{11}*3*5*433*19801*584118287.$

この見所は 2 の指数が $m+1=8$ を超えるところである. これらは単なる数値例とはいえ, 見事な美しい結果である.

5.4 末尾２桁

L_m, a_m の末尾を調べるため, 次の数列を導入する.

$h_m=3^{2^m}, L_m=\frac{1+h_m}{2}, h_{m+1}=h_m^2, K_m=3^{2^m-1}$ とおく.

$h_m = 2L_m - 1, (h_m)^2 + 1 = 4{L_m}^2 - 4L_m + 1$. ゆえに $L_{m+1} = 2{L_m}^2 - 2L_m + 1$. $a_m = K_m L_m$ に注意して次の表を作る.

表 6: $P = 3$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	81	82	41	27	7
3	8	61	62	81	87	47
4	16	21	22	61	7	27
5	32	41	42	21	47	87
6	64	81	82	41	27	7

$6 - 2 = 4$ なので周期が 4.

表 7: $P = 3$

m	2^m	h_m	H_m	L_m	K_m	a_m
2	4	81	82	41	27	107
3	8	561	562	281	187	547
4	16	721	722	361	907	427
5	32	841	842	921	947	187
6	64	281	282	641	427	707
7	128	961	962	481	987	747
8	256	521	522	761	507	827
9	512	441	442	721	147	987
10	1024	481	482	241	827	307
11	2048	361	362	681	787	947
12	4096	321	322	161	107	227
13	8192	41	42	521	347	787
14	16384	681	682	841	227	907
15	32768	761	762	881	587	147
16	65536	121	122	561	707	627
17	131072	641	642	321	547	587
18	262144	881	882	441	627	507
19	524288	161	162	81	387	347
20	1048576	921	922	961	307	27
21	2097152	241	242	121	747	387
22	4194304	81	82	41	27	107

$22 - 2 = 20$ が周期なので案外短い.