友愛数の平行移動

飯高 茂

平成 31 年 6 月 8 日

1　友愛数

友愛数はピタゴラスの時代にすでに知られていた.

友愛数を大量に生産するアルゴリズムも工夫されそれを使ったプログラムを使うと 1 晩で 100 万個もの友愛数がみつかることもあるという. それにもかかわらず, 友愛数が無数にあることの証明はできていない.

2019 年 5 月現在では 10 億個以上発見されているそうである. (Total known amicable pairs: 1,223,393,792 By wiki).

[1]

私は喜寿を迎えた高齢者であるが現役の大学生 (放送大学学園 東京多摩学習センター所属) でもある. 学内に多摩数学クラブというサークルを作り活動している. 4 月には新入生に対し新部員を獲得するため勧誘活動をすることになった.

興味深い数学の話題を提供してクラブの例会を盛り上げる手はないかいろいろ考えた結果, 例会で友愛数を紹介することにした. 「友愛数から派生した結婚数や婚約数もありますよ」, とクラブ紹介の催しで宣伝したところ, 4 月にある例会い女子学生も参加してくれた.

私の完全数研究ははじめて 6 年になるが完全数の平行移動を考えることが研究の上で大切な鍵の一つであった. そこで友愛数についても平行移動を考えることにした.

定義 1 $F_k(a) = \sigma(a) - a + k$ とおく. $b = F_k(a), a = F_k(b), a \neq b$,(a, b) を $k-$ 友愛数という.

あるいは (a, b) を 平行移動 k の友愛数と呼んでもいい. k が小さい場合は先行研究がある.

- $k = 0$ のとき (a, b) を 元祖友愛数
- $k = -1$ のとき (a, b) を婚約数. (婚約したが破談).
- $k = 1$ のとき (a, b) を結婚数. (友情から結婚にいたって 1 子誕生).
- $k = 2$ のとき (a, b) を子だくさん数.

maxima による友愛数の素因数分解のプログラムにより次の結果が得られた.

[1] Amicable Pairs, a Survey (2003)
By 1) Mariano Garcia(11802 SW 37th Terrace, Miami, Florida 33175, USA), 2) Jan Munch Pederse (Vitus Bering CVU, Chr. M. Ostergaardsvej 4, DK-8700 Horsens, Denmark) 3) Herman te Riele (1090 GB Amsterdam, The Netherlands)

表 1: $k = 0$ すなわち友愛数

a	素因数分解	型	b	素因数分解
$k = 0$				
284	$2^2 * 71$	A	220	$2^2 * 5 * 11$
6368	$2^5 * 199$	A	6232	$2^3 * 19 * 41$
18416	$2^4 * 1151$	A	17296	$2^4 * 23 * 47$
66992	$2^4 * 53 * 79$	D	66928	$2^4 * 47 * 89$
76084	$2^2 * 23 * 827$	D	63020	$2^2 * 5 * 23 * 137$
123152	$2^4 * 43 * 179$	D	122368	$2^9 * 239$
153176	$2^3 * 41 * 467$	D	141664	$2^5 * 19 * 233$
176336	$2^4 * 103 * 107$	D	171856	$2^4 * 23 * 467$
180848	$2^4 * 89 * 127$	D	176272	$2^4 * 23 * 479$
203432	$2^3 * 59 * 431$	D	185368	$2^3 * 17 * 29 * 47$
365084	$2^2 * 107 * 853$	D	280540	$2^2 * 5 * 13^2 * 83$
389924	$2^2 * 43 * 2267$	D	308620	$2^2 * 5 * 13 * 1187$
399592	$2^3 * 199 * 251$	D	356408	$2^3 * 13 * 23 * 149$
455344	$2^4 * 149 * 191$	D	437456	$2^4 * 19 * 1439$
514736	$2^4 * 53 * 607$	D	503056	$2^4 * 23 * 1367$
669688	$2^3 * 97 * 863$	D	600392	$2^3 * 13 * 23 * 251$
686072	$2^3 * 191 * 449$	D	609928	$2^3 * 11 * 29 * 239$
691256	$2^3 * 71 * 1217$	D	624184	$2^3 * 11 * 41 * 173$
712216	$2^3 * 127 * 701$	D	635624	$2^3 * 11 * 31 * 233$
796696	$2^3 * 53 * 1879$	D	726104	$2^3 * 17 * 19 * 281$
901424	$2^4 * 53 * 1063$	D	879712	$2^5 * 37 * 743$
980984	$2^3 * 47 * 2609$	D	898216	$2^3 * 11 * 59 * 173$
1043096	$2^3 * 23 * 5669$	D	998104	$2^3 * 17 * 41 * 179$

表 2: $k=0$ すなわち友愛数

a	素因数分解	型	b	素因数分解
2924	$2^2*17*43$	D	2620	$2^2*5*131$
5564	$2^2*13*107$	D	5020	$2^2*5*251$
10856	$2^3*23*59$	D	10744	$2^3*17*79$
168730	$2*5*47*359$	F	142310	$2*5*7*19*107$
202444	$2^2*11*43*107$	F	196724	$2^2*11*17*263$
430402	$2*7*71*433$	F	319550	$2*5^2*7*11*83$
652664	$2^3*17*4799$	F	643336	$2^3*29*47*59$
783556	$2^2*31*71*89$	F	667964	$2^2*11*17*19*47$
1210	$2*5*11^2$	F	1184	2^5*37
486178	$2*7^2*11^2*41$	F	469028	2^2*7^2*2393
88730	$2*5*19*467$	F	79750	$2*5^3*11*29$
14595	$3*5*7*139$	H	12285	$3^3*5*7*13$
71145	$3^3*5*17*31$	H	67095	$3^3*5*7*71$
87633	$3^2*7*13*107$	H	69615	$3^2*5*7*13*17$
124155	$3^2*5*31*89$	H	100485	$3^2*5*7*11*29$
139815	$3^2*5*13*239$	H	122265	$3^2*5*11*13*19$
525915	$3^2*5*13*29*31$	H	522405	$3^2*5*13*19*47$
863835	$3*5*7*19*433$	H	802725	$3*5^2*7*11*139$
1125765	$3^3*5*31*269$	H	947835	$3^3*5*7*17*59$

これらの素因数分解を観察すると次のことが見て取れる.

A 型 (すなわち素因数分解が $2^e p$), D 型 (素因数分解: $2^e qr$) 　のペアが多い.

D 型 と D 　型のペアもある. 　奇数 (H 型) 同士のペアも散見する.

A 型 と D 　型 のペアは有限個しかないようだ. これらを決定出来たら面白い.

偶数 と奇数のペアが存在しないことは奇数の完全数の不存在問題と同様の難問らしい.

奇数の友愛数は 3 の倍数が多いが, 6 で割れないが 5 の倍数の例はある.

友愛数の素因数分解の表を詳しく検討した結果 $a = 2^e r, b = 2^f pq$ という形の解を求めてみたいという気になった.

$e = f$ の場合はオイラーにより深く研究されていた.

2　Euler の結果

Euler は友愛数について次の結果をえていた.

定理 1 (p,q,r) は次式で定義された素数とする. ここで $n,m(n>m)$ は自然数.
$K=2^{n-m}+1$ とおくとき $p=2^mK-1, q=2^nK-1, r=2^{n+m}K^2-1$.
$A=2^npq, B=2^nr$　について, $co\sigma(A)=B$.　さらに $co\sigma(B)=A$.
すなわち (A,B) は友愛数.

Euler は偶数完全数 a について, $a=2^np,(p=2^{n+1}-1$:メルセンヌ素数) と書けることを示していた.

定理 1 は友愛数についてもメルセンヌ素数と類似したさらに複雑な形の素数を与えるとそれから D 型と A 型からなる友愛数ができることを示している. なかなか興味のある結果といえるだろう.

私は定年後の仕事の 1 つとして, 京王永山駅近くにあるカルチャースクールで数学を教えている. 参加者は大人 2 人と小学生である. 実際にはゼミ形式でしている.

ゼミの課題としてオイラーの結果を確認するため $A=2^npq, B=2^nr$　について, $co\sigma(A)=B$ を計算で確かめることにした. 私も含めて 4 人で議論しながら計算したが複雑な計算に時間を取られ時間内にできなかった.

帰宅してから時間をかけて計算しようやくできた. それが次の証明である.
$N=2^{n+1}-1$ とおくとき $co\sigma(A)=co\sigma(2^npq)=N(p+1)(q+1)-2^npq$.
$p+1=2^mK, q+1=2^nK, pq=2^{n+m}K^2-K(2^n+2^m)+1$ に注意する.

$$\begin{aligned}
N(p+1)(q+1)-2^npq &= N(2^{n+m}K^2)-2^n(2^{n+m}K^2-K(2^n+2^m)+1)\\
&=(2^{n+1}-1)(2^{n+m}K^2)-2^n(2^{n+m}K^2-K(2^n+2^m)+1)\\
&=2^{2n+m+1}K^2-2^{n+m}K^2-2^n(2^{n+m}K^2-K(2^n+2^m)+1)\\
&=2^n(2^{n+m}K^2-2^mK^2+K(2^m+2^n)-1)\\
&=2^nX.
\end{aligned}$$

$r=K^22^{n+m}-1$ を用いると, $X=2^{n+m}K^2-1-2^mK^2+K(2^m+2^n)=r+L$ となる.
ここで, $L=-2^mK^2+K(2^m+2^n)=KL_0$ とおくと $L_0=-2^mK+(2^m+2^n)=-(2^m+2^n)+(2^m+2^n)=0$.
したがって, $co\sigma(A)=N(p+1)(q+1)-2^npq=2^nr=B$. よって, $co\sigma(A)=B$
同様にして $co\sigma(B)=A$ も示される.

そののち, 参加者の一人である小学 5 年生の梶田光君から証明ができたとのメールがあり添付ファイルに見事な証明が書かれていた. その後半を紹介する.

2.1 $co\sigma(B) = A$, 梶田君の証明

$A = 2^n pq, B = 2^n r$　について,$\sigma(A) - A = co\sigma(A) = B$ は示されたので $\sigma(A) = A + B$. $\sigma(B) = A + B$ を示せばよい.

上記にある証明で $co\sigma(A) = B$ はできている. $\sigma(A) = N(p+1)(q+1) = N(r+1) = \sigma(B)$ が成り立つから, $\sigma(B) = \sigma(A) = A + B$.

3 オイラーの式の導出

オイラーの式は複雑ではあるが計算してみると味わいのある式である. オイラーは次の２つの解

1).$B = 284 = 2^2 * 71, A = 220 = 2^2 * 5 * 11$, 2)$B = 18416 = 2^4 * 1151, A = 17296 = 2^4 * 23 * 47$

をもとに友愛数の例を与える式を作った, という仮説のもとで議論を進める.

Proof

$A = 2^n pq, B = 2^n r$　について, $co\sigma(A) = B$, $co\sigma(B) = A$ が成り立つと仮定する.

$B = co\sigma(A) = \sigma(A) - A, A = co\sigma(B) = \sigma(B) - B$ により, $\sigma(A) = A + B = \sigma(B)$.

$N = 2^{n+1} - 1$ とおくとき $\sigma(A) = N(p+1)(q+1), \sigma(B) = N(r+1)$ により,$N(p+1)(q+1) = N(r+1)$. 整理して, $(p+1)(q+1) = (r+1)$.

例２について試みる. $p = 23, q = 47, r = 1151$ なので $p + 1 = 24 = 2^3 * 3, q + 1 = 48 = 2^4 * 3, r + 1 = 1151 + 1 = 2^7 * 3^2$.

そこで「仮定 $(*)$: $p + 1 = 2^n K, q + 1 = 2^m K, (K$: 奇数)」を使う. すると $r + 1 = (p+1)(q+1) = 2^{n+m} K^2$, $r = 2^{n+m} K^2 - 1$. ここで, p, q の式の対称性により $n \geq m$ を仮定する.

$2^n pq = A = co\sigma(B) = \sigma(B) - B = N(r+1) - 2^n r = 2^n r + N - r$ により

$r = 2^n r + N - 2^n pq = 2^n (r - pq) + N$. ゆえに $r = N + 2^n (r - pq)$.

$p = 2^n K - 1, q = 2^m K - 1, r = 2^{n+m} K^2 - 1$ によって, $r - pq = -2 + K(2^n + 2^m)$.

$$\begin{aligned} 2^{n+m} K^2 - 1 &= r \\ &= N + 2^n (r - pq) \\ &= N + 2^n (-2 + K(2^n + 2^m)) \\ &= -1 + 2^n K(2^n + 2^m)). \end{aligned}$$

ゆえに $2^{n+m} K^2 = 2^n K(2^n + 2^m)$.

$2^m K = 2^n + 2^m$ によって,$K = 2^{n-m} + 1$. これで証明が完了.

3.1 仮定 $(*)$ を使わない場合

さらに検討を続けた結果, 仮定 $(*)$ はいらないことが分かった. (わたくしは 2019 年現在 76 歳になりオイラーの没年齢にならんだ. オイラーの結果を検討し計算していると偉大

なオイラーを身近に感じる.)

$(p+1)(q+1) = (r+1)$ により, $p+1, q+1$ は偶数なので, 奇数 K_1, K_2 を用いて $p+1 = 2^n K_1, q+1 = 2^m K_2$ としてみると $r+1 = (p+1)(q+1) = 2^{n+m} K_1 K_2$.

$2^n pq = A = co\sigma(B) = \sigma(B) - B = N(r+1) - 2^n r = 2^n r + N - r$ により

$r = 2^n r + N - 2^n pq = 2^n(r-pq) + N$.

ゆえに $r = N + 2^n(r-pq)$.(これは前の議論のまま)

$p = 2^n K_1 - 1, q = 2^m K_2 - 1, r = 2^{n+m} K_1 K_2 - 1$ によって,

$r - pq = -2 + (2^n K_1 + 2^m K_2)$.

2^n を掛けると $2^n(r-pq) = -2^{n+1} + 2^n(2^n K_1 + 2^m K_2)$.

$r = N + 2^n(r-pq), -2^{n+1} = -N - 1$ を用いて

$r - N = 2^n(r-pq) = -2^{n+1} + 2^n(2^n K_1 + 2^m K_2) = -1 - N + 2^n(2^n K_1 + 2^m K_2)$.

それゆえ

$$r + 1 = 2^n(2^n K_1 + 2^m K_2).$$

一方 $r + 1 = (p+1)(q+1) = 2^{n+m} K_1 K_2$ により,

$$2^{n+m} K_1 K_2 = 2^n(2^n K_1 + 2^m K_2).$$

よって, $2^m K_1 K_2 = 2^n K_1 + 2^m K_2$. これより $2^m K_2(K_1 - 1) = 2^n K_1$.

$n \geq m$ を用いて式を整理し $K_2(K_1 - 1) = 2^{n-m} K_1$.

ここで $K_1 - 1, K_1$ は互いに素なので整数 α により $(K_1 - 1)\alpha = 2^{n-m}$ と書ける.

とくに $\alpha > 1$ なら α は偶数.

$K_2(K_1 - 1) = 2^{n-m} K_1$ によって, $K_2 = \alpha K_1$. α 　は奇数となるので $\alpha = 1$.

$(K_1 - 1)\alpha = 2^{n-m}$ によると　　$K_1 - 1 = 2^{n-m}$. ゆえに $K_1 = 2^{n-m} + 1$.

$K_2(K_1 - 1) = 2^{n-m} K_1$ を用いると $K_2 = K_1$.

End.

$m < n < 40$ の範囲でオイラーの式の与える友愛数をパソコンで求めたところ, $(n, m) = (2, 1), (4, 3), (7, 6), (8, 1)$ のときのみ (p, q, r) は素数.(がっかりさせられる)

表 3: $k = 0$ 友愛数,Euler の式で (p, q, r) 素数の場合

$m = 1, n = 2$			
220	$2^2 * 5 * 11$	284	$2^2 * 71$
$m = 3, n = 4$			
17296	$2^4 * 23 * 47$	18416	$2^4 * 1151(Fermat)$
$m = 6, n = 7$			
9363584	$2^7 * 191 * 383$	9437056	$2^7 * 73727(Descartes)$
$m = 1, n = 8$			
2172649216	$2^8 * 257 * 33023$	2181168896	$2^8 * 8520191$

4　婚約数と結婚数の素因数分解

表 4: $k = -1$ 婚約数

a	素因数分解	型	b	素因数分解
75	$3 * 5^2$	H	48	$2^4 * 3$
195	$3 * 5 * 13$	H	140	$2^2 * 5 * 7$
75495	$3 * 5 * 7 * 719$	H	62744	$2^3 * 11 * 23 * 31$
2295	$3^3 * 5 * 17$	H	2024	$2^3 * 11 * 23$
16587	$3^2 * 19 * 97$	H	8892	$2^2 * 3^2 * 13 * 19$
20735	$5 * 11 * 13 * 29$	H	9504	$2^5 * 3^3 * 11$
1925	$5^2 * 7 * 11$	H	1050	$2 * 3 * 5^2 * 7$
1648	$2^4 * 103$	A	1575	$3^2 * 5^2 * 7$
6128	$2^4 * 383$	A	5775	$3 * 5^2 * 7 * 11$

偶数 と奇数のペアばかりらしい.

表 5: $k = 1$ すなわち結婚数

a	素因数分解	型	b	素因数分解
11697	$3 * 7 * 557$	H	6160	$2^4 * 5 * 7 * 11$
16005	$3 * 5 * 11 * 97$	H	12220	$2^2 * 5 * 13 * 47$
28917	$3^5 * 7 * 17$	H	23500	$2^2 * 5^3 * 47$
76245	$3 * 5 * 13 * 17 * 23$	H	68908	$2^2 * 7 * 23 * 107$
339825	$3 * 5^2 * 23 * 197$	H	249424	$2^4 * 7 * 17 * 131$
570405	$3 * 5 * 11 * 3457$	H	425500	$2^2 * 5^3 * 23 * 37$
871585	$5 * 11 * 13 * 23 * 53$	H	434784	$2^5 * 3 * 7 * 647$
697851	$3^2 * 7 * 11 * 19 * 53$	H	649990	$2 * 5 * 11 * 19 * 311$
678376	$2^3 * 19 * 4463$	D	660825	$3^3 * 5^2 * 11 * 89$

偶数 と奇数のペアばかりらしい. しかも素因数分解の型が複雑なのでわからないまま H 型にしてある.

表 6: $k=2$ 子だくさん数

a	素因数分解	b	素因数分解
38	$2*19$	24	2^3*3
92	2^2*23	78	$2*3*13$
7928	2^3*991	6954	$2*3*19*61$
2528	2^5*79	2514	$2*3*419$
34688	2^7*271	34674	$2*3*5779$
1358	$2*7*97$	996	2^2*3*83
826	$2*7*59$	616	2^3*7*11
286	$2*11*13$	220	2^2*5*11
494	$2*13*19$	348	2^2*3*29
2678	$2*13*103$	1692	2^2*3^2*47
1178	$2*19*31$	744	2^3*3*31
9082	$2*19*239$	5320	$2^3*5*7*19$
27626	$2*19*727$	16056	2^3*3^2*223
48662	$2*29*839$	26940	$2^2*3*5*449$
30938	$2*31*499$	17064	2^3*3^3*79
17114	$2*43*199$	9288	2^3*3^3*43
61946	$2*47*659$	33096	$2^3*3*7*197$
5434	$2*11*13*19$	4648	2^3*7*83
8648	$2^3*23*47$	8634	$2*3*1439$
12008	$2^3*19*79$	11994	$2*3*1999$
36518	$2*19*31^2$	23064	2^3*3*31^2
38828	$2^2*17*571$	33246	$2*3^2*1847$
53966	$2*11^2*223$	35412	$2^2*3*13*227$
65588	$2^2*19*863$	55374	$2*3*11*839$

これは理学部数学科で講義をしている頃, 友愛数のほかに結婚数, 婚約数もあるらしい. と話すと学生がおおいに興味あるというのでついでに子だくさん数も考えて紹介した思い出がある.

すべて偶数らしいが素因数分解の型が分かりやすい点で興味がある.

$a=38, b=24$ のペアが最も簡単な数なのでこれの特徴を与える結果は次の通り.

命題 1 $k=2$ のとき $a=2p, b=2^eq, (p,q)$: 奇素数, と仮定すると, $a=2p=38, b=2^eq=24$.

Proof

$F_2(a)=F_2(2p)=3(p+1)-2p+2=p+5$, $F_2(a)=b=2^eq$ により, $p+5=2^eq$.

$2p=a=F_2(b)=F_2(2^eq)=(2^{e+1}-1)(q+1)-2^eq=2^eq-(q+1)+2^{e+1}+2$

$p=2^eq-5$ を代入して

$$2(2^e q - 5) = 2^e q - (q+1) + 2^{e+1} + 2.$$

$$2 * 2^e q = 2^e q - (q+1) + 2^{e+1} + 12 = 2^e(q-2) - q + 11.$$

ゆえに $2^e q = 2 * 2^e - q + 11$ となり $(2^e + 1)q = 2 * 2^e + 11$.

$q \geq 3$ によって,

$$2^{e+1} + 11 \geq 2^e 3 + 3.$$

$8 \geq 2^e$.

よって, $3 \geq e$.

1. $e = 3$ なら $2^e q = 2 * 2^e - q + 11$ に代入して $8q = 16 - q + 11$. よって, $9q = 27$ によって, $q = 3$. これより $p = 2^e q - 5 = 24 - 5 = 19$. $a = 2 * 19 = 38, b = 8q = 24$.

2. $e = 2$ なら $2^e q = 2 * 2^e - q + 11$ に代入して $4q = 8 - q + 11$. これは矛盾.

3. $e = 1$ なら $2^e q = 2 * 2^e - q + 11$ に代入して $2q = 4 - q + 11$. よって, $q = 5$. $p = 2^e q - 5$ に注意すると, $p = 2^e q - 5 = 10 - 5 = 5$. これより $a = 10, b = 10$. $a = b$ となり矛盾.

End

以前のスーパー完全数の研究において m だけ平行移動を考えた．その結果 $m=-18,-58,-14$ などの場合に解としてスーパー双子素数が組織的な形を取りながら現れた．

これは私にとって大きな成功体験であった．そこで k 友愛数の k をいろいろ変えながら分かりやすい形の解を探してみた．

$k=-16$ のとき特に美しい結果が出てきた．これは望外の成功であった．

5　$k=-16$ でのスーパー双子素数解

表 7: $k=-16$

	a	素因数分解	b	素因数分解
$k=-16$				
	92	2^2*23	60	2^2*3*5
	124	2^2*31	84	2^2*3*7
	188	2^2*47	132	2^2*3*11
	284	2^2*71	204	2^2*3*17
	316	2^2*79	228	2^2*3*19
	508	2^2*127	372	2^2*3*31
	604	2^2*151	444	2^2*3*37
	668	2^2*167	492	2^2*3*41
	764	2^2*191	564	2^2*3*47
	956	2^2*239	708	2^2*3*59
	1436	2^2*359	1068	2^2*3*89
	1724	2^2*431	1284	$2^2*3*107$
	1756	2^2*439	1308	$2^2*3*109$
	1084	2^2*271	804	2^2*3*67
	2396	2^2*599	1788	$2^2*3*149$
	2428	2^2*607	1812	$2^2*3*151$
	2524	2^2*631	1884	$2^2*3*157$
	2876	2^2*719	2148	$2^2*3*179$
	2908	2^2*727	2172	$2^2*3*181$

ここで主な解として $a=4p, b=12q, (p,q)$:奇素数, の解が多いことに注意する．

$F(a)=F_{-16}(a)$ とおくとき $F(a)=\sigma(a)-a-16$ となる．

$a=4p, b=12q, (p,q$:奇素数) を解と仮定する．

$a=4p$ のとき　$F(a)=\sigma(a)-a-16=7(p+1)-16=3p-9=b=12q$ により $p-3=4q$.

次に $p-3=4q$ を用いると $b=12q$ のとき　$F(b)=28(q+1)-12q-16=16q+12=4(4q+3)=4p=a$ となる．

定理 2 (a,b) は -16 友愛数とする． $F(a)=F_{-16}(a)=\sigma(a)-a-16$ とおくとき $b=F(a), a=F(b), a\neq b$ と仮定する．

そこで解は $a=2^ep, b=2^eqr, (p,q,r<q$:奇素数) の形になると仮定すると, $e=2, r=4, a=4p, b=12q$ さらに $p=4q+3$ を満たす．

ここで $(q, p=4q+3)$ を満たすので (q,p) はスーパー双子素数.

Proof.

$a=2^ep$ について, $N=2^{e+1}-1$ とおいて

$F(a)=\sigma(a)-a-16=N(p+1)-2^ep-16=Np-2^ep+N-16=2^ep-p+N-16.$

$F(a)=b=2^eqr$ により, $2^ep-p+N-16=2^eqr.$

ゆえに $2^ep=p-N+16+2^eqr.$

整理して $(2^e-1)p=-N+16+2^eqr.$

$b=2^eqr$ について, $\Delta=q+r$ とおくと

$$\begin{aligned}
F(b)&=\sigma(b)-b-16\\
&=N(q+1)(r+1)-2^eqr-16\\
&=Nqr-2^eqr-16+N(\Delta+1)\\
&=2^eqr-qr+N(\Delta+1)-16\\
&=a\\
&=2^ep.
\end{aligned}$$

$2^eqr-qr-16+N(\Delta+1)=2^ep$ を得る.

$2^ep=p-N+16+2^eqr$ を代入して

$$2^eqr-qr-16+N(\Delta+1)=p-N+16+2^eqr.$$

これより

$$p=2^eqr-qr-16+N(\Delta+1)-(-N+16+2^eqr)=-32-qr+N\Delta+2N.$$

$p=-32-qr+N\Delta+2N$ を $(2^e-1)p=-N+16+2^eqr$ に代入すると

$$(2^e-1)(-32-qr+N(\Delta+2)=-N+16+2^eqr.$$

$-32(2^e-1)-(2^e-1)qr+(2^e-1)N(\Delta+2)=-N+16+2^eqr$

$-(2^e-1)qr$ を移項して

$$-32(2^e-1)+(2^e-1)N(\Delta+2)=-N+16+2^eqr+(2^e-1)qr=-N+16+Nqr.$$

$-32(2^e-1)=-16*2(2^e-1)=-16(N-1)$ と直すと

$$-16(N-1)+(2^e-1)N(\Delta+2)=-N+16+Nqr.$$

N を除して

$$-16+(2^e-1)(\Delta+2)=-1+qr.$$

$\Delta=q+r$ によって,$\eta=2^e-1, q_0=q-\eta, r_0=r-\eta,$ とおくと, $-15+\eta(\Delta+2)=qr.$

$$q_0r_0=qr-\eta\Delta+\eta^2=\eta^2+2\eta-15.$$

$\Theta=\eta^2+2\eta-15$ を導入すると $q_0r_0=\Theta.$

$e=2,3,4,\cdots$ と場合を分けて詳しく調べよう.

1. $e=2.$ $\eta=2^e-1=3, N=7, q_0=q-3, r_0=r-3, \Theta=\eta^2+2\eta-15=0.$ $q_0>r_0$ により, $r_0=0, r=3,$ $b=6q.$

$$\begin{aligned}
p&=-32-qr+N\Delta+2N\\
&=-32-3q+7*(q+3)+7*2\\
&=4q-32+35\\
&=4q+3.
\end{aligned}$$

$a=4*p, b=2^2*q*r=12q.p=4q+3$ となりこれは既に示した.

2. $e=3.$ $\eta=2^e-1=7, N=15, q_0=q-7, r_0=r-7, \Theta=\eta^2+2\eta-15=7(7+9)-15=63-15=48.$

$q_0r_0=\Theta=48$ により, $r_0=4, q_0=12.$ $r=11, q=19.$

$p=-32-qr+N\Delta+2N=-32-11*19+15(11+19)+30=239.$

よって, $a=1912=2^3*239, b=1672=2^3*q*r=2^3*11*19.$

3. $e=4.$ $\eta=2^e-1=15, N=31, q_0=q-15, r_0=r-15, \Theta=\eta^2+2\eta-15=15*17-15=15*16.$ $q_0r_0=\Theta=2^4*3*5$ により, $r_0=3*2=6, q_0=5*4=20.$ $r=21;$ 素数でないから矛盾.

$r_0=5*2=10, q_0=3*8=24.$ $r=25;$ 矛盾.

これ以上解はないらしい.

このように素因数分解の型を決めて A 型,D 型 と決めて簡単な場合の平行移動 -16 の友愛数の決定に成功したのである. これはオイラーの友愛数の構成式を連想させるものがある.

6 一般な場合の平行移動

$m = -16$ の場合はうまくできたので一般に平行移動 m の場合を扱ってみよう.

(a, b) は m 友愛数とする.

$F(a) = F_m(a) = \sigma(a) - a - 16$ とおくとき $b = F(a), a = F(b), a \neq b$ となる.

解は AD 型 と仮定する. すなわち $a = 2^e p, b = 2^e qr, (p, q, r < q$:奇素数) の形になると仮定する.

$a = 2^e p$ について, $N = 2^{e+1} - 1$ とおいて $F(a) = \sigma(a) - a + m = N(p+1) - 2^e p + m = Np - 2^e p + N + m = 2^e p - p + N + m$.

$F(a) = b = 2^e qr$ により, $2^e p - p + N + m = 2^e qr$.

ゆえに $2^e p = p - N - m + 2^e qr$.

整理して $(2^e - 1)p = -N - m + 2^e qr$.

$b = 2^e qr$ について, $\Delta = q + r$ とおくと

$$
\begin{aligned}
F(b) &= \sigma(b) - b + m \\
&= N(q+1)(r+1) - 2^e qr + m \\
&= Nqr - 2^e qr + m + N(\Delta + 1) \\
&= 2^e qr - qr + N(\Delta + 1) + m \\
&= a \\
&= 2^e p.
\end{aligned}
$$

ゆえに $2^e qr - qr + m + N(\Delta + 1) = 2^e p$ を得る.

$2^e p = p - N - m + 2^e qr$ を代入して

$$2^e qr - qr + m + N(\Delta + 1) = p - N - m + 2^e qr.$$

これより

$$p = 2^e qr - qr + m + N(\Delta + 1) - (-N - m + 2^e qr) = 2m - qr + N\Delta + 2N.$$

$p = 2m - qr + N\Delta + 2N$ を $(2^e - 1)p = -N - m + 2^e qr$ に代入すると

$$(2^e - 1)(2m - qr + N(\Delta + 2) = -N - m + 2^e qr.$$

$2m(2^e - 1) - (2^e - 1)qr + (2^e - 1)N(\Delta + 2) = -N - m + 2^e qr$

$-(2^e - 1)qr$ を移項して

$$2m(2^e - 1) + (2^e - 1)N(\Delta + 2) = -N + 16 + 2^e qr + (2^e - 1)qr = -N + -m + Nqr.$$

$2m(2^e - 1) = 2m(2^e - 1) = m(N - 1)$ と直すと

$$m(N-1)+(2^e-1)N(\Delta+2)=-N-m+Nqr.$$

N を除して

$$m+(2^e-1)(\Delta+2)=-1+qr.$$

$\Delta=q+r$ によって,$\eta=2^e-1, q_0=q-\eta, r_0=r-\eta$, とおくと, $m+1+\eta(\Delta+2)=qr$.

$$q_0r_0=qr-\eta\Delta+\eta^2=\eta^2+2\eta+m+1.$$

$\Theta=\eta^2+2\eta+m+1=(2^e-1)(2^e+1)+m+1=2^{2e}+m$ とおくとき $q_0r_0=\Theta$. これを基本等式という.

7　$\Theta=0$ の場合

指数 $e>1$ に対して $m=-2^{2e}$ とおく. $\Theta=0$ になり基本等式は $q_0r_0=\Theta=0$.. ここで $q>r$ と仮定しておく. $r_0=0; r=\eta=2^e-1$. q_0 はとくに定まらないが $q=q_0+\eta>r=\eta$ は素数だけ確認する. さらに $b=2^erq=2^e(2^e-1)q$.

$a=2^ep, b=2^erq$ であるが公式 $p=2m-qr+N\Delta+2N$ により p が決定される.

$$p=2m-qr+N\Delta+2N=-2*2^{2e}-qr+(2^{e+1}-1)(q+r)+2.$$

この式の右辺を q で整理する.

$$\begin{aligned}
p&=-2*2^{2e}-qr+(2^{e+1}-1)(q+r)+2\\
&=-2*2^{2e}+(2^{e+1}-1-r)q+(2^{e+1}-1)r+2\\
&=-2*2^{2e}+(2^{e+1}-2^e)q+(2^{e+1}-1)(2^e-1)+2\\
&=-2*2^{2e}+2^eq+2^{2e+1}-2^e+2^{e+1}-1\\
&=2^eq+2^e-1
\end{aligned}$$

かくして得られた式は

$$p=2^eq+2^e-1.$$

1. $e=2$ のとき $m=-2^4=-16$, $p=4q+3, b=2^e(2^e-1)q=12q$.
2. $e=3$ のとき $m=-2^6=-64$, $p=8q+7, b=2^e(2^e-1)q=56q$.
3. $e=4$ のとき $m=-2^8=-256$, $p=16q+15, b=2^e(2^e-1)q=240q$.

念のため次の結果を示す.

命題 2 $p=2^eq+2^e-1, r=2^e-1, m=-2^{2e}$ を満たすとき, $a=2^ep, b=2^erq$ は 平行移動 $m=-2^{2e}$ の友愛数.

Proof.

$F(\alpha)=\sigma(\alpha)-\alpha+m$ とおくとき $a=2^e p, b=2^e rq$ について, $F(a)=b, F(b)=a$ を示せばよい.

$N=2^{e+1}-1$ とおくとき $\sigma(a)=N(p+1)=Np+N=2^{e+1}p-p+N$.

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

最右端の式 $(2^e-1)p-(2^e-1)^2$ を X とおく.

一方, $b=2^e rq=2^e(2^e-1)q=(2^e-1)2^e q$ を変形して.

$p=2^e q+2^e-1$ に 2^e-1 を乗じて $(2^e-1)p=(2^e-1)2^e q+(2^e-1)^2$.

ゆえに,

$$X=(2^e-1)p-(2^e-1)^2=(2^e-1)2^e q=b.$$

よって, $X=b$.

End.

このように素因数分解の型を決めて平行移動の友愛数の決定に成功したのである. これはオイラーの友愛数の構成式を連想させるものがある.

7.1 $m=0$ のとき

$\Theta=2^{2e}+m=2^{2e}$ なので $\eta=2^e-1, q_0r_0=2^{2e}$. これより , $q_0=2^s, r_0=2^t, s+t=2e$. ここで,$t>e>s$ としておく.

$q=2^s+\eta=2^s+2^e-1, r=2^t+2^e-1$. $K=2^{e-s}+1$ とおくと

$$q=2^s+2^e-1=2^sK-1, r=2^t+2^e-1=2^{t-e}K-1=2^t-2^{t-e}-1.$$

一方 $p+1=(q+1)(r+1)=(2^s+2^e)(2^t+2^e)$ によって,$p=(q+1)(r+1)-1=2^sK2^{t-e}K-1=2^{s+t-e}K^2-1$.

結局, $K=2^{e-s}+1$ を使うと, $q=2^sK-1, r=2^{t-e}K-1, p=2^{s+t-e}K^2-1$.

これはオイラーの式である.

表 8: $m = -44$

a	素因数分解	b	素因数分解	
$m = -44$				
	322	$2*7*23$	210	$2*3*5*7$
	406	$2*7*29$	270	$2*3^3*5$
	574	$2*7*41$	390	$2*3*5*13$
	742	$2*7*53$	510	$2*3*5*17$
	826	$2*7*59$	570	$2*3*5*19$
	994	$2*7*71$	690	$2*3*5*23$
	1246	$2*7*89$	870	$2*3*5*29$
	1582	$2*7*113$	1110	$2*3*5*37$
	1834	$2*7*131$	1290	$2*3*5*43$
	1864	2^3*233	1602	$2*3^2*89$
	1990	$2*5*199$	1566	$2*3^3*29$

$a = 14p, b = 30q, ((p > 2 \neq 7, q > 5)$:素数) という解がある．この場合を以下で詳しく調べる．

$F(a) = \sigma(a) - a - 44$ とおくと，

$F(a) = F(14p) = \sigma(14p) - 14p - 44 = 24(p+1) - 14p - 44 = 10p - 20 = b = 30q;$ $p - 2 = 3q.$

$F(b) = F(30q) = \sigma(30q) - 30q - 44 = 72(q+1) - 30q - 44 = 42q + 28 = 7(6q+4) = 14(3q+2) = 14p = a.$

$(q, p = 2 + 3q)$ がスーパー双子素数になる場合である．

$p = 29$ とすると，$p = 27 = 2 + 3q$ を解くと，$q = 9$．この場合だけはスーパー双子素数にならない．

表 9: $m=-34$

a	素因数分解	b	素因数分解	
$m=-34$				
	225	3^2*5^2	144	2^4*3^2
	246	$2*3*41$	224	2^5*7
	406	$2*7*29$	280	2^3*5*7
	790	$2*5*79$	616	2^3*7*11
	494	$2*13*19$	312	2^3*3*13
	498	$2*3*83$	476	2^2*7*17
	834	$2*3*139$	812	2^2*7*29
	1338	$2*3*223$	1316	2^2*7*47
	1506	$2*3*251$	1484	2^2*7*53
	638	$2*11*29$	408	2^3*3*17
	764	2^2*191	546	$2*3*7*13$

$a=6p, b=28q, ((p>3, q\neq 2,7)$:素数$)$ という解がある.
$F(a)=F(6p)=12(p+1)-6p-34=6p-22=b=28q;\ 3p-11=14q.$
$F(b)=F(28q)=56(q+1)-28q-34=28q+22=2(14q+11)=a=6p; 14q+11=3p.$
p,q:素数, $14q+11=3p$ を満たす場合である.

表 10: $m = 12, 14$

a	素因数分解	b	素因数分解
$m = 12$			
428	$2^2 * 107$	340	$2^2 * 5 * 17$
664	$2^3 * 83$	608	$2^5 * 19$
$m = 14$			
398	$2 * 199$	216	$2^3 * 3^3$
23	23	15	$3 * 5$
190	$2 * 5 * 19$	184	$2^3 * 23$
754	$2 * 13 * 29$	520	$2^3 * 5 * 13$
1406	$2 * 19 * 37$	888	$2^3 * 3 * 37$
1390	$2 * 5 * 139$	1144	$2^3 * 11 * 13$
1364	$2^2 * 11 * 31$	1338	$2 * 3 * 223$
1990	$2 * 5 * 199$	1624	$2^3 * 7 * 29$

表 11: $m = 16, 18, 20$

a	素因数分解	b	素因数分解
$m = 16$			
94	$2 * 47$	66	$2 * 3 * 11$
122	$2 * 61$	80	$2^4 * 5$
382	$2 * 191$	210	$2 * 3 * 5 * 7$
310	$2 * 5 * 31$	282	$2 * 3 * 47$
1054	$2 * 17 * 31$	690	$2 * 3 * 5 * 23$
$m = 18$			
244	$2^2 * 61$	208	$2^4 * 13$
$m = 20$			
31	31	21	$3 * 7$
35	$5 * 7$	33	$3 * 11$
94	$2 * 47$	70	$2 * 5 * 7$
206	$2 * 103$	126	$2 * 3^2 * 7$
1034	$2 * 11 * 47$	714	$2 * 3 * 7 * 17$
2114	$2 * 7 * 151$	1554	$2 * 3 * 7 * 37$

8 $m = -64$ 友愛数, 計算例

表 12: $m = -64$

a	素因数分解	b	素因数分解
20344	$2^3 * 2543$	17752	$2^3 * 7 * 317$
23032	$2^3 * 2879$	20104	$2^3 * 7 * 359$
24952	$2^3 * 3119$	21784	$2^3 * 7 * 389$
26872	$2^3 * 3359$	23464	$2^3 * 7 * 419$
32632	$2^3 * 4079$	28504	$2^3 * 7 * 509$
35704	$2^3 * 4463$	31192	$2^3 * 7 * 557$
37624	$2^3 * 4703$	32872	$2^3 * 7 * 587$
38008	$2^3 * 4751$	33208	$2^3 * 7 * 593$
38392	$2^3 * 4799$	33544	$2^3 * 7 * 599$
39544	$2^3 * 4943$	34552	$2^3 * 7 * 617$
41848	$2^3 * 5231$	36568	$2^3 * 7 * 653$
42232	$2^3 * 5279$	36904	$2^3 * 7 * 659$
43768	$2^3 * 5471$	38248	$2^3 * 7 * 683$
53752	$2^3 * 6719$	46984	$2^3 * 7 * 839$
54904	$2^3 * 6863$	47992	$2^3 * 7 * 857$
55288	$2^3 * 6911$	48328	$2^3 * 7 * 863$
56824	$2^3 * 7103$	49672	$2^3 * 7 * 887$
60664	$2^3 * 7583$	53032	$2^3 * 7 * 947$
62584	$2^3 * 7823$	54712	$2^3 * 7 * 977$
64888	$2^3 * 8111$	56728	$2^3 * 7 * 1013$
74488	$2^3 * 9311$	65128	$2^3 * 7 * 1163$
76408	$2^3 * 9551$	66808	$2^3 * 7 * 1193$
77944	$2^3 * 9743$	68152	$2^3 * 7 * 1217$
70264	$2^3 * 8783$	61432	$2^3 * 7 * 1097$
70648	$2^3 * 8831$	61768	$2^3 * 7 * 1103$
78328	$2^3 * 9791$	68488	$2^3 * 7 * 1223$
78712	$2^3 * 9839$	68824	$2^3 * 7 * 1229$
104824	$2^3 * 13103$	91672	$2^3 * 7 * 1637$

表 13: $m = -64$

a	素因数分解	b	素因数分解
2802	$2 * 3 * 467$	2750	$2 * 5^3 * 11$
140	$2^2 * 5 * 7$	132	$2^2 * 3 * 11$
412	$2^2 * 103$	252	$2^2 * 3^2 * 7$
470	$2 * 5 * 47$	330	$2 * 3 * 5 * 11$
352	$2^5 * 11$	340	$2^2 * 5 * 17$
1012	$2^2 * 11 * 23$	940	$2^2 * 5 * 47$
1276	$2^2 * 11 * 29$	1180	$2^2 * 5 * 59$
1804	$2^2 * 11 * 41$	1660	$2^2 * 5 * 83$
2332	$2^2 * 11 * 53$	2140	$2^2 * 5 * 107$
3652	$2^2 * 11 * 83$	3340	$2^2 * 5 * 167$
3916	$2^2 * 11 * 89$	3580	$2^2 * 5 * 179$
4972	$2^2 * 11 * 113$	4540	$2^2 * 5 * 227$
5764	$2^2 * 11 * 131$	5260	$2^2 * 5 * 263$
7612	$2^2 * 11 * 173$	6940	$2^2 * 5 * 347$
7876	$2^2 * 11 * 179$	7180	$2^2 * 5 * 359$
8404	$2^2 * 11 * 191$	7660	$2^2 * 5 * 383$
10252	$2^2 * 11 * 233$	9340	$2^2 * 5 * 467$
10516	$2^2 * 11 * 239$	9580	$2^2 * 5 * 479$
11044	$2^2 * 11 * 251$	10060	$2^2 * 5 * 503$
12364	$2^2 * 11 * 281$	11260	$2^2 * 5 * 563$
12892	$2^2 * 11 * 293$	11740	$2^2 * 5 * 587$
15796	$2^2 * 11 * 359$	14380	$2^2 * 5 * 719$
18436	$2^2 * 11 * 419$	16780	$2^2 * 5 * 839$
19924	$2^2 * 17 * 293$	17056	$2^5 * 13 * 41$
18964	$2^2 * 11 * 431$	17260	$2^2 * 5 * 863$
19492	$2^2 * 11 * 443$	17740	$2^2 * 5 * 887$

表 14: $m=-64$

a	素因数分解	b	素因数分解
25048	$2^3*31*101$	23848	$2^3*11*271$
7192	$2^3*29*31$	7144	$2^3*19*47$
10792	$2^3*19*71$	10744	$2^3*17*79$
17848	$2^3*23*97$	17368	$2^3*13*167$
88946	$2*11*13*311$	68238	$2*3^2*17*223$
16286	$2*17*479$	9570	$2*3*5*11*29$
11488	2^5*359	11128	$2^3*13*107$
14042	$2*7*17*59$	11814	$2*3*11*179$
43492	$2^2*83*131$	34060	$2^2*5*13*131$
39652	$2^2*23*431$	32860	$2^2*5*31*53$
38114	$2*17*19*59$	26622	$2*3^3*17*29$
55106	$2*59*467$	29070	$2*3^2*5*17*19$
49996	$2^2*29*431$	40660	$2^2*5*19*107$
45410	$2*5*19*239$	40926	$2*3*19*359$
101230	$2*5*53*191$	85330	$2*5*7*23*53$
65186	$2*11*2963$	41454	$2*3^2*7^2*47$
59236	$2^2*59*251$	46540	$2^2*5*13*179$
94622	$2*11^2*17*23$	77682	$2*3*11^2*107$
71668	$2^2*19*23*41$	69388	$2^2*11*19*83$
115598	$2*7*23*359$	91698	$2*3*17*29*31$

表 15: $m = -64$

	a	素因数分解	b	素因数分解
$m = -64$				
	140	$2^2 * 5 * 7$	132	$2^2 * 3 * 11$
	352	$2^5 * 11$	340	$2^2 * 5 * 17$
	376	$2^3 * 47$	280	$2^3 * 5 * 7$
	412	$2^2 * 103$	252	$2^2 * 3^2 * 7$
	470	$2 * 5 * 47$	330	$2 * 3 * 5 * 11$
	1012	$2^2 * 11 * 23$	940	$2^2 * 5 * 47$
	1276	$2^2 * 11 * 29$	1180	$2^2 * 5 * 59$
	1804	$2^2 * 11 * 41$	1660	$2^2 * 5 * 83$
	248	$2^3 * 31$	168	$2^3 * 3 * 7$
	1528	$2^3 * 191$	1288	$2^3 * 7 * 23$
	1912	$2^3 * 239$	1624	$2^3 * 7 * 29$

$m = -64$ の解の型について 2019/april/25

$a = 44p = 2 - 2 * 11 * p, b = 20 = 2^2 * 5 * q, ((p > 3, p \neq 11, q \neq 2, 5)$:素数) という解がある．D 型同士の解.

$F(a) = F(44p) = 12 * 7(p + 1) - 44p - 64 = 40p + 20 = b = 20q; 2p + 1 = q$. ソフィーゲルマンの素数.

$F(b) = F(20q) = 42(q + 1) - 28q - 64 = 22q - 22 = 44p; q - 1 = 2p$.

$a = 8p = 2^3p, b = 56q = 2^3 * 7 * q, ((p > 3, p \neq 11, q \neq 2, 5)$:素数) という解がある.

$F(a) = F(8p) = 15(p + 1) - 8p - 64 = 7p + 49 = b = 56q; p + 7 = 8q$.

$F(b) = F(56q) = 120(q + 1) - 56q - 64 = 64q - 56 = 8p; 8q - 7 = p$.

$(p = 8q - 7, q)$ はスーパー双子素数.

$a = 8p, b = 56q, ((p > 3, p \neq 11, q \neq 2, 5)$:素数) という解がある.

9 社交数

$m = 0$ について，$F_0(a) = \sigma(a) - a$ とおくとき，相異なる a, b, c について，$F_0(a) = b, F_0(b) = c, F_0(c) = a$ となるとき社交数 (sociable number) というそうだ.

しかしこれを満たす 3 つ組は知られていない. 平行移動を入れると 3 つ組社交数はいろいろ出てくる.

$m = 2$ のとき $a = 6 = 2 * 3, b = 8 = 2^3, c = 9 = 3^2$ が最も簡単な例である.

表 16: k 社交数

a		b		c	
$m=-10$					
48	2^4*3	66	$2*3*11$	68	2^2*17
66	$2*3*11$	68	2^2*17	48	2^4*3
544	2^5*17	580	2^2*5*29	670	$2*5*67$
580	2^2*5*29	670	$2*5*67$	544	2^5*17
$m=-9$					
288	2^5*3^2	522	$2*3^2*29$	639	3^2*71
522	$2*3^2*29$	639	3^2*71	288	2^5*3^2
$m=2$					
6	$2*3$	8	2^3	9	3^2
8	2^3	9	3^2	6	$2*3$
$m=4$					
920	2^3*5*23	1244	2^2*311	944	2^4*59
6344	$2^3*13*61$	6680	$2^3*5*167$	8444	2^2*2111
6680	$2^3*5*167$	8444	2^2*2111	6344	$2^3*13*61$
$m=6$					
80	2^4*5	112	2^4*7	142	$2*71$
112	2^4*7	142	$2*71$	80	2^4*5
$m=7$					
8	2^3	14	$2*7$	17	17
14	$2*7$	17	17	8	2^3
$m=12$					
44	2^2*11	52	2^2*13	58	$2*29$
52	2^2*13	58	$2*29$	44	2^2*11
$m=13$					
21	$3*7$	24	2^3*3	49	7^2
24	2^3*3	49	7^2	21	$3*7$
$m=14$					
70	$2*5*7$	88	2^3*11	106	$2*53$
88	2^3*11	106	$2*53$	70	$2*5*7$