奇数の完全数の諸命題から、代数方程式，楕円曲線へ関連させる試み

高 橋 鋼 一

Ⅰ．はじめに

正の整数aが完全数とは、aの約数全体の和をS(a)で表すと、S(a)＝2aが満たす整数aのことである。偶数の完全数については、ユークリッドの「原論」九巻命題36で、$a=2^{n-1}(2^n-1)$ （ただし、nは2以上の素数）の形で、2^n-1が素数ならば、aは完全数であることはわかっていたが、この命題の逆（「偶数の完全数aは,この形に限る。」）は、200年ほど前にEulerによって証明され、偶数の完全数の形は解決した。偶数の完全数が無限にあるのかどうかは、2^n-1型の素数が無限にあるのかどうかに依存する。この型の素数をメルセンヌ素数と言うが、現在、計算機を用いてメルセンヌ素数が発見されているが、まだ50個に満たない。

他方、奇数の完全数は、まだ1個も発見されていない。先ずはじめに、次のⅡ章以降で、奇数の完全数が存在すると仮定した場合、どのような命題が成り立つのかという研究結果を述べる。これについて、学生時代に、「数と図形」(ラーデマッヘル・テップリッツ著)の本を読んで考え、その中で、命題1～命題5までは、既に18世紀にEulerが既に示したことを最近インターネットで知りました。その次のⅢ章では、Euler以後の「奇数の完全数についての数学史」の概略を簡単に述べることにします。Ⅳ章以降は、「奇数の完全数の存在を仮定すると、どのような命題が成り立たねばならないか？」ということについて、私の考察を展開することにします。Ⅴ章は、奇数の完全数と代数的方程式との関連を述べ、第Ⅵ章以降で、奇数の完全数と楕円曲線との関連の試みを述べることにします。

Ⅱ．奇数の完全数Nの素因数分解表示(Eulerによる)

以下に述べる命題1から命題30(ただし、[命題29]を除く)までは、私が学生時代から「奇数の完全は存在するのだろうか？」という研究課題に取り組んで得た結果である。命題1から命題5までは、Eulerが既に取り組んだ研究があることを前述した通り。Eulerの原論文が入手してないので、私が辿った証明の過程を載せることにします。

正の奇数の完全数Nの存在を仮定して、その素因数分解を、

$$N=p_1^{\ell_1}\,p_2^{\ell_2}\cdots\cdots\,p_k^{\ell_k}\,p_{k+1}^{\ell_{k+1}}$$ （ただし、p_i ($i=1,2,3,\cdots,k,k+1$)はすべて奇素数で互いに素とする。各指数ℓ_iはすべて自然数とする）……(1)

とする。Sは自然数を入力とし、その自然数のすべての約数の総和を出力とする作用(関数)とする。

完全数の定義(条件)より、

$$S(N)=2N \qquad \cdots\cdots(2)$$

を満たさなければならない。(2)より、

$$S(p_1^{\ell_1}\,p_2^{\ell_2}\cdots\cdots\,p_k^{\ell_k}\,p_{k+1}^{\ell_{k+1}})=2p_1^{\ell_1}\,p_2^{\ell_2}\cdots\cdots\,p_k^{\ell_k}\,p_{k+1}^{\ell_{k+1}} \qquad \cdots\cdots(2)^*$$

となる。一般に、a，bを任意の互いに素となる自然数とすると、S(ab)＝S(a)S(b)が成り立つから、

(2)*より、

$\therefore S(p_1^{\ell_1})\,S(p_2^{\ell_2})\cdots\cdots S(p_k^{\ell_k})S(p_{k+1}^{\ell_{k+1}})=2p_1^{\ell_1}\,p_2^{\ell_2}\cdots\cdots\,p_k^{\ell_k}\,p_{k+1}^{\ell_{k+1}}$ ……(3)

が成り立たねばならない。ここで、$i=1,2,3,\cdots\cdots$, k,k+1について、

$$S(p_i^{\ell_i})=1+p_i+p_i^2+p_i^3+\cdots\cdots+p_i^{\ell_i-1}+p_i^{\ell_i}=\sum_{u=1}^{\ell_i}p_i^u=\frac{p_i^{\ell_i+1}-1}{p_i-1}\quad\cdots\cdots(4)$$

である。等式(3)の右辺は、素因数分解の形をしていて、素因数の2が一回だけ含まれている。

したがって、(3)の左辺の因数 $S(p_i^{\ell_i})$ (ただし、$i=1,2,3,\cdots\cdots,k,k+1$))の中の一つだけが偶数で、残りのすべての因数は奇数でなければならない。(3)の左辺の一つだけの因数$S(p_{k+1}^{\ell_{k+1}})$を偶数としても一般性をそこなわないので、$S(p_{k+1}^{\ell_{k+1}})$を偶数とする。さらに、$S(p_{k+1}^{\ell_{k+1}})$は2で1回だけ割り切れなければならない。

$$S(p_{k+1}^{\ell_{k+1}})=1+p_{k+1}+p_{k+1}^2+\cdots\cdots+p_{k+1}^{\ell_k}+p_{k+1}^{\ell_{k+1}}\quad\cdots\cdots(5)$$

であり、(5)の右辺は$(\ell_{k+1}+1)$個の奇数$1,p_{k+1},p_{k+1}^2,\cdots\cdots,p_{k+1}^{\ell_k},p_{k+1}^{\ell_{k+1}}$の和である。(5)が2で1回だけ割り切れるためには、項の個数$(\ell_{k+1}+1)$が偶数で、かつ$(\ell_{k+1}+1)/2$は奇数なければならない。

$\therefore \ell_{k+1}+1=2h$ (ただし、hは適当な自然数で奇数) ……(6)

とおける。つまり、

$\ell_{k+1}=2h-1$ (奇数) ……(7)

とならなければならない。さらに、(3)の左辺の$S(p_{k+1}^{\ell_{k+1}})$以外の因数$S(p_i^{\ell_i})$(ただし、$1\leqq i\leqq k$)は、すべて奇数でなければならない。したがって、次の命題1(証明は上述通り),命題2が成り立つ。

[命題1] 奇数の完全数 $N=p_1^{\ell_1}p_2^{\ell_2}\cdots\cdots p_k^{\ell_k}p_{k+1}^{\ell_{k+1}}$が存在すると仮定すると、Nの素因数分解のある一つの素数 p_{k+1}のべき指数ℓ_{k+1}のみ、奇数である。

[命題2] (3)を満たす$S(p_i^{\ell_i})$ $(i=1,2,3,\cdots\cdots,k)$はすべて奇数で、各p_iの指数ℓ_iはすべて偶数である。

(証明) 命題1の結果より、(3)の等式の両辺は2で1回だけ割り切れ、$S(p_{k+1}^{2h-1})$は偶数より、

$$S(p_1^{\ell_1})S(p_2^{\ell_2})S(p_3^{\ell_3})\cdots\cdots S(p_k^{2\ell_k-1})\left\{\frac{S(p_{k+1}^{2h-1})}{2}\right\}=p_1^{\ell_1}\,p_2^{\ell_2}\,p_3^{\ell_3}\cdots\cdots p_k^{\ell_k}\,p_{k+1}^{2h-1}\quad\cdots\cdots(8)$$

(8)の右辺は奇数より、(8)の左辺のすべての因数$S(p_1^{\ell_1}),S(p_2^{\ell_2}),S(p_3^{\ell_3}),\cdots\cdots,S(p_k^{\ell_k}),\left\{\frac{S(p_{k+1}^{2h-1})}{2}\right\}$は、奇数でなければならない。$i=1,2,3,\cdots\cdots,k$において、$S(p_i^{\ell_i})=1+p_i+p_i^2+\cdots\cdots+p_i^{\ell_i}$ の各項は奇数で、項数は(ℓ_i+1)個だから、項数ℓ_i+1は奇数でなければならない。したがって、

$\ell_i+1=2m_i+1$ (ただし、m_iは適当な自然数 $(1\leqq i\leqq k)$) ……(9)

とおける。(9)より、各$\ell_i=2m_i$ (偶数)となる。

(証終)

[命題3] (3)の式において、$p_{k+1}\equiv 1 \pmod 4$である。

(証明) 命題1より、ℓ_{k+1}は奇数であるから、$\ell_{k+1}=2h-1$(ただし、hは適当な自然数))とおく。ここで、奇

数の完全数の素因数p_{k+1}をqで表すことにする。

$$S(p_{k+1}^{\ell_{k+1}})=S(q^{2h-1})=1+q+q^2+q^3+q^4+q^5+q^6+\cdots\cdots+q^{2h-2}+q^{2h-1}$$

$$=(1+q)+q^2(1+q)+q^4(1+q)+\cdots\cdots+q^{2h-2}(1+q)$$

$$=(1+q)(1+q^2+q^4+q^6+\cdots\cdots+q^{2h-2})$$

右辺の因数$(1+q)$が偶数であることを考慮して、この両辺を2で割ると、

$$\{\frac{S(q^{2h-1})}{2}\}=(\frac{1+q}{2})\{1+q^2+q^4+q^6+\cdots\cdots+q^{2(h-1)}\} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(10)$$

が成り立つ。(10)を(8)の左辺の式に代入した等式の右辺が奇数であることより、$\frac{S(q^{2h-1})}{2}$は奇数となり、(10)の右辺も奇数で、したがって、(10)の右辺の2つの因数$(\frac{1+q}{2})$,$\{1+q^2+q^4+q^6+\cdots\cdots+q^{2(h-1)}\}$は、ともに奇数でなければならない。$\frac{1+q}{2}=2t-1$(ただし、tは適当な自然数)とおける。

$\therefore \quad q=4t-3$

となるから、$p_{k+1}=q\equiv -3\equiv 1 \pmod 4$が成り立つ。　　(証終)

[命題4] 奇数の完全数Nの素因数$p_{k+1}^{\ell_{k+1}}=q^{\ell_{k+1}}$のべき指数について、$\ell_{k+1}\equiv 1 \pmod 4$ が成り立つ。

(証明) 命題3の証明の中で、式(10)の右辺の因数$\{1+q^2+q^4+q^6+\cdots\cdots+q^{2(h-1)}\}$は奇数で、各項は奇数からなる$(h-1)+1=h$個の和であるから、項数hは奇数でなければならない。したがって、

$h=2n-1$ (ただし、nは適当な自然数)とおける。命題1より、$\ell_{k+1}=2h-1$だから、

$\ell_{k+1}=2h-1=2(2n-1)-1=4n-3$となり、

$\ell_{k+1}\equiv -3\equiv 1 \pmod 4$

が成り立つ。(註:式(5)の後の文章の中で、$(\ell_{k+1}+1)/2$が奇数であることからも、命題が導ける。)

(証終)

[命題5] 奇数の完全数Nが存在すると仮定すると、次の(ⅰ),(ⅱ)が成り立つ。

(ⅰ)　$N=p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots\cdots p_k^{2m_k}q^{4n-3}$　(ただし、命題3より、qは素数で、$4t-3=q$とおいた。)

(ⅱ)　Nは、$N\equiv 1 \pmod 4$型の整数である。

(証明) (ⅰ)の証明は、命題2, 3, 4より明らか。

(ⅱ)の証明について。(ⅰ)の右辺の式で、$i=1,2,3,\cdots,k$ において、p_iは互いに素な奇素数で、各指数$2m_i$が偶数である。$p_i^2\equiv 1 \pmod 4$型の整数より、各$p_i^{2m_i}=(p_i^2)^{m_i}\equiv 1 \pmod 4$が成り立つ。

さらに、$q^{4n-3}=(4t-3)^{4n-3}\equiv 1 \pmod 4$が成り立つから、これらの因数の積からなるNについて、$N\equiv 1 \pmod 4$が成立する。　　(証終)

(註:命題5より、次のⅢ章の①で述べられた事柄(Nは2個の平方数の和で表される。)が成立する。)

Ⅲ. Euler以後、「奇数の完全数について」の考察

Ⅱ章の命題1～命題5の結果より、「奇数の完全数Nが存在する」と仮定すると、Nの素因数分解(乗法的分解)は、次のように表される。

$$N=p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}q^{\ell_{k+1}} \quad (\text{ただし、} q\equiv 1(\text{mod } 4), \ell_{k+1}\equiv 1 \ (\text{mod } 4)) \quad \cdots\cdots\cdots\cdots (11)$$

Euler以後の「奇数の完全数」についての考察の結果を列挙してみる。

⓪J.シルヴェスター(1888年)奇数の完全数は、少なくとも3つの異なった素因数をもつ。

①(Stuyavaert(1896年))Nは2個の平方数の和でなければならない。(註:Euler&Gaussの命題:「2平方和の定理」から得られる。)

②(O.Grun(1952年))(11)のNの素因数$p_1,p_2,\cdots,p_k$の中で、一番を小さい素因子をp_iとすれば、

$p_i<\frac{2k}{3}+2$である。

③(Touchard(1953年)&Satyanarayana(1959年))Nは、12m+1または36m+9の形をしている。

④Joseph B.Muskat(1966年) 奇数の完全数は、p^k (ただし、$k>10^{12}$,pは素数)で割り切れる。

⑤(MacDaniel(1970年))(11)のNの式において、$m_1\equiv m_2\equiv m_3\equiv\cdots m_k\equiv 1(\text{mod } 3)$ではない。

⑥P.Hagis and Wayne McDaniel(1973年) 奇数の完全数の最大素因数は、100110より大きい。

⑦C.Pomerance(1975年) 奇数の完全数の2番目に大きい素因数は、138より大きい。

⑧(Steuerwald, Hagis(1975年), Cohen(1985年))$m_1=m_2=m_3=\cdots=m_{k-1}=m_k=\beta$とすると、$\beta$は1,2,3,5,6,8,11,12,14,17,18,24,62ではない。

⑨P.Hagis(1975年), E.Z.Chein(1979年) 奇数の完全数が、もし存在するとものならば、少なくとも8個の異なる素因数を持つ。

⑩J.T.Condict(1978年) ,P.Hagis 奇数の完全数の最大素因数は300000より大きく、その次に大きい素因数は1000より大きい。

⑪C.Pomerance(1970年代(?)) せいぜいK個の異なる因数しか持たない奇数の完全数は、

$$(4K)^{(4K)^{2^{K^2}}}$$

より小さい。

⑫M.D.Sayers(1986年) 奇数の完全数は、必ずしも異なるとは限らない、少なくとも29個の素因子がある。

⑬G.L.Cohen(1987年) 奇数の完全数は、10^{20}より大きい成分(素数べきの約数)をもつ。

⑭R.P.Brent,G.L.Cohen &H.J.J.te Riele (1991年)奇数の完全数の下からの限界は、10^{300}である。

⑮D.E.Iannucci & R.M.Sorli (2003年)奇数の完全数は、かならずしも異なるとはかぎらない37個の素因子をもつ。

⑯＊Iannucci(1999年) 奇数の完全数の2番目に大きい素因数は、10^4より大きい。

＊Iannucci (2000年) 奇数の完全数の3番目に大きい素因数は、100より大きい。

＊(Hare(2005年)) Nは重複も数えて少なくとも75個の素因数をもつ。

＊(大野泰生, 後藤文志(2006年)) Nは10^8より大きい素因数をもつ。

⑰＊奇数の完全数は少なくとも9個の相異なる素因数をもつ。(Nielsen(2007年))

＊ Nが3で割り切れない場合、12個の相異なる素因数を持つ。

＊ Nが3でも5でも割り切れない場合、15個の相異なる素因数を持つ。

＊ Nが3でも5でも7でも割り切れない場合は、27個の相異なる素因数をもつ。

⑱Paolo Starni(1993年) $N=M^2q^{4n-3}$(ただし、$M=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$)で、4n-1は素数である。

⑲奇数の完全数Nの素因数分解を、$N=p_1^{2\ell_1}p_2^{2\ell_2}\cdots p_k^{2\ell_k}q^{4n-3}$ (ただし、qは、$q\equiv1(\mathrm{mod}\ 4)$を満たす素数)で表し、相異なる素因子$p_1,p_2,p_3,\cdots\cdots,p_k$について、$p_1<p_2<p_3<\cdots<p_k$としても、一般性を失わない。

＊(M.Kishore(1981年)) $i=2,3,4,5,6$のとき、$p_i<2^{2^{i-1}}(k-i+1)$である。

＊(山田智宏(2005年))もし、$\ell_1=\ell_2=\ell_3=\cdots=\ell_{k-1}=\ell_k=\beta$と仮定すると、$k\leq4\beta^2+2\beta+2$である。

＊山田智宏(2005年), M.Satyanarayama(1959年), J.A.Holdener(2002年), T.Roberts(2008年)

$N\equiv1(\mathrm{mod}\ 12)$かまたは

$N\equiv0.5\times3^{2\ell_1}(3^{2\ell_1+1}-1)\ (\mathrm{mod}\ 2\times3^{2\ell_1}(3^{2\ell_1+1}-1))$である。

＊(Nielsen(2003年)

$$N<2^{4^{K+1}}$$

である。

⑳(「オイラー入門」W. ダンハム著 Springer)p.30の註から。(Klee andWagon,pp212-213)

＊ 奇数の完全数は$105=3\times5\times7$では割り切れない。

＊すべての奇数の完全数の逆数の和は有限である。式で表すと、

$$\sum_{n\text{は奇数の完全数}}\frac{1}{n}<\infty\text{が成り立つ。}$$

Ⅳ．奇数の完全数の存在を仮定すると、どのような命題が成り立たねばならないか？

Ⅱ章～Ⅲ章の数学史をふまえて、これ以降、私が取り組んだ結果を述べることにする。奇数の完全数については、ユークリッド以来、一つも見つかっていない。この問題に取り組む方法は、演繹だけでは不可能であろうと思われる。代数学が、定義⇒公理⇒命題（定理）という形で整理され、学習するには容易になったとはいえ、数学が演繹のみ依拠してでは何も新しい事柄は生まれないだろう。高木貞治が「近世数学史談」の中で、Gaussの”書かれなかった楕円関数”にふれた最後の箇所で、「帰納の一途に精進すべき」ことを提唱している。（ここでの帰納とは、狭い意味の数学的帰納法ではない。）高木貞治の提唱をどう受け止めたら良いのか、若い頃から暗中模索してきた。（現在も暗中模索中である。）個人的な私見を述べれば、既存の数学の殿堂から少し距離をおいて、時には定義を意味のある変更をし、公理を削ったり、増やしたり、定理の仮定条件を変更したり、場合によっては、現象学的には判断中止（エポケ）にして、依拠している立場や方法を検証し直して、アプローチの方法を変えて、数学の殿堂に無い、かつ、未だ命題や定理に昇格していない例題や問題，予想と取り組む中で特殊から一般へと進めて、最も根本的かつ本質的と思われることに関連する事象そのものに依拠することではないか、･･･と考えて、このような方法論で拙文を先に進めることにします。

[**命題6**] 奇数の完全数が存在すると仮定する。[命題5]の（ｉ）で、Nの因数q^{4n-3}以外の素因数の積 $p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}$ の約数の総和、および、Nのq^{4n-3}以外の素因数の積の2倍をそれぞれ

$$A=S(p_1^{2m_1}p_2^{2m_2}\cdots p_k{}^{2m_k})=S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots\cdots S(p_k^{2m_k}),$$

$$B=2p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots\cdots p_k^{2m_k}$$

とおくと、A＜Bが成り立たなければならない。

（証明） 奇数の完全数Nの存在の仮定から、(3)の等式が成り立つ。(3)の等式と[命題5]を使うと、

$$A\times S(q^{4n-3})=B\times q^{4n-3} \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(12)$$

が成り立たなければならない。ところで、$S(q^{4n-3})>q^{4n-3}$が成り立つから、(12)の等式より、A＜Bでなければならない。（ただし、qは、$q\equiv1\pmod 4$を満たす素数）

（証終）

[**命題7**] 奇数の完全数Nが存在すると仮定する。命題6より、(12)の等式、

$$A\times S(q^{4n-3})=B\times q^{4n-3}$$

が成り立つが、この等式から、$q^{4n-3}\mid A$が成り立つ。したがって、Aをq^{4n-3}で割った商は自然数で、Rとおくと、$A=q^{4n-3}R$ と表される。ただし、$R=Aq-B+B$と表され、$q\nmid R$となる。

さらに、$S(q^{4n-3})$は、$B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$ の素因数のうち、2と重複を含めて幾つかの奇数の素因数の積の形で表される。

（証明） 奇数の完全数Nが存在すると仮定すると、$N=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}$ (ただし、$p_1,p_2,\cdots,p_k$ は奇素数、奇素数qは、$q\equiv 1 \pmod 4$) の型をなすことが[命題3]で示された。(12)を満たすAおよびB,$S(q^{4n-3})$は、それぞれ

$$A=S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k}),$$

$$B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k},$$

$$S(q^{4n-3})=1+q+q^2+q^3+\cdots+q^{4n-3}=\frac{q^{4n-2}-1}{q-1}$$ （註:$S(q^{4n-3})$は偶数）

である。(12)の右辺の相異なる素因数は、$2,p_1,p_2,p_3,\cdots,p_k,q$だから、左辺に含まれる素因数も同じである。したがって,(12)の左辺に現れる因数は、$2,p_1,p_2,\cdots,p_k,q$の一部分の重複を許した素因数を含む。Aは奇数だから、奇数の素因数$p_1,p_2,\cdots,p_k,q$の重複を許して幾つかを含まねばならない。

(12)の左辺に、因数$S(q^{4n-3})=\frac{q^{4n-2}-1}{q-1}$を代入すると、

$$A\times\frac{q^{4n-2}-1}{q-1}=B\times q^{4n-3} \quad \cdots\cdots(13)$$

（ただし、qは4を法として1と合同の奇素数だから、$q\geq 5$である。$\Rightarrow\ \therefore\ q-1\neq 0$）

が成立する。(13)の両辺に$(q-1)$を掛けると、

$$A\times(q^{4n-2}-1)=B\times q^{4n-3}(q-1)$$

$$Aq^{4n-2}-A=Bq^{4n-2}-Bq^{4n-3}$$

$$\therefore\ q^{4n-3}(Aq-Bq+B)=A \quad \cdots\cdots(14)$$

(14)の右辺は自然数だから、左辺の因数$(Aq-Bq+B)$は自然数となり、Aの約数の中に、q^{4n-3}が存在する。したがって、Rを$R=Aq-Bq+B$とおくと、$R>0$で、$Aq>B(q-1)$を満たし、(14)より、$A=q^{4n-3}R$と表される。(13)の左辺にある因数qのべき指数は$(4n-3)$だから、右辺にある因数Aに含まれるqのべき指数は、(12)の両辺を比較すると、$(4n-3)$を超えることはできない。したがって、$q\nmid R$である。$A=q^{4n-3}R$を(12)の 左辺に代入すると、

$$q^{4n-3}R\,S(q^{4n-3})=Bq^{4n-3}$$

となり、両辺をq^{4n-3}で割ると、

$$RS(q^{4n-3})=B$$

となる。$S(q^{4n-3})$は偶数（Bも偶数である。Rは奇数である。）より、$S(q^{4n-3})$は,2とBの奇数の素因数の重複も含めて幾つかの指数乗どうしの積に等しいことになる。 （証終）

（註:(14)の右辺$A>0$より、左辺の因数$R=Aq-Bq+B>0$だから、$B>(B-A)q$が成り立つ。）

(別証) qとS$(q^{4n-3})=1+q+q^2+q^3+\cdots+q^{4n-3}$は、互いに素である。さらに、$1\leq^{\forall} j\leq 4n-3$を満たす任意の$j$について、$q^j$とS$(q^{4n-3})$とは互いに素となる。なぜならば、$q^j$ を法として、S$(q^{4n-3})-q^{4n-3}$を考えると、

$$S(q^{4n-3})-q^{4n-3}=(1+q+q^2+\cdots+q^{4n-3})-q^{4n-3}=1+q+\cdots+q^{4n-4}\equiv 1+q+q^2+\cdots+q^{j-1}(\mathrm{mod}\ q^j)\quad\cdots(15)$$

となる。(15)の最右辺の値$\left(1+q+q^2+\cdots+q^{j-1}=\dfrac{q^j-1}{q-1}\right)$について、$q^j$と大小を比較すると

$$q^j-\frac{q^j-1}{q-1}=\frac{q^j(q-1)-q^j+1}{q-1}=\frac{q^{j+1}-2q^j+1}{q-1}=\frac{q^j(q-2)+1}{q-1}$$

で、qは5以上かつ$q\equiv 1\ (\mathrm{mod}\ 4)$を満たす素数だから、$\dfrac{q^j(q-2)+1}{q-1}>0$となる。したがって、

$$q^j>1+q+q^2+\cdots+q^{j-1}\quad\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(16)$$

(15)の等式をq^jを法として考えると、

$$S(q^{4n-3})-0\equiv 1+q+q^2+\cdots+q^{j-1}\not\equiv 0(\mathrm{mod}\ q^j)$$

となる。したがって、(16)より、

$$S(q^{4n-3})\not\equiv 0\ (\mathrm{mod}\ q^j)\ (\text{ただし、}1\leq^{\forall} j\leq 4n-3)\quad\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(17)$$

(17)から、S(q^{4n-3})とq^{4n-3}は互いに素となる。

(12)の等式で、

$$A\times S(q^{4n-3})=B\times q^{4n-3}$$

が成り立ち、S(q^{4n-3})とq^{4n-3}が互いに素であるから、q^{4n-3}は、$A=S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_k^{2m_k})$を割り切らなければならない。このことと(12)より、S(q^{4n-3})は偶数だから、Bの因数2と2以外のBのいくつかの奇数の素因数の指数乗どうしの積からなる。　　(証終)

(註:$q^{4n-3}\mid A$であるが、$q^{4n-3}=A$(この場合、$R=1$である。)か、あるいは$A\neq q^{4n-3}$(この場合、$R\neq 1$で、q^{4n-3}はAの真の約数で、Rは$p_1,p_2,\cdots,p_k$の幾つかの指数乗の積となる)のどちらかである。))

「命題7」の証明過程で得た式を変形すると、興味ある等式が得られる。計算を再度繰り返すと、奇数の完全数の定義を変形して、等式$A\times S(q^{4n-3})=B\times q^{4n-3}$を得たが、命題7より$q^{4n-3}\mid A$が成り立ち、さらに、Aを$q^{4n-3}$で割った商を$R$とすると、$A=q^{4n-3}R$と表された。

これを(12)の等式 :AS$(q^{4n-3})=Bq^{4n-3}$ に代入して、両辺をq^{4n-3}で割ると、

$$Rq^{4n-3}S(q^{4n-3})=Bq^{4n-3}\ \Rightarrow\ RS(q^{4n-3})=B$$

を得た。この等式を変形すると次のページの(19)の興味ある等式が得られる。

$R\mathrm{S}(q^{4n-3})=\mathrm{B} \Rightarrow R\dfrac{q^{4n-2}-1}{q-1}=$Bの両辺に$(q-1)$を掛けて、

$$R(q^{4n-2}-1)=\mathrm{B}(q-1) \quad \cdots\cdots(18)$$

$$\therefore q(\mathrm{B}-Rq^{4n-3})=\mathrm{B}-R \quad \cdots\cdots(19)$$

が成り立つ。

(註:命題6より、$\mathrm{B}>\mathrm{A}=q^{4n-3}R$ が成り立つから、(19)の左辺の因数$\mathrm{B}-Rq^{4n-3}>0$が成り立つ。したがって、右辺$\mathrm{B}-R>0$が成り立つ。さらに、(19)より、$q \mid (\mathrm{B}-R)$が成り立つ。)

命題7で、$\mathrm{A}=q^{4n-3}R$の右辺の因数Rについて、$R\neq 1$の場合と$R=1$の場合とに分けて、考えることにする。

[命題7からのLemma I]

(ⅰ)$R\neq 1$の場合(つまり、Aがq^{4n-3}を真の約数にもつ場合)Aはq^{4n-3}以外の素因数 $p_1,p_2,\cdots,p_k$の幾つかの中から重複を許してそれらの積を因数にもつ。実は、q^{4n-3}以外のAに含まれるすべての重複を許した素因数の積はRである。さらに、(19)より、$q(\mathrm{B}-Rq^{4n-3})=\mathrm{B}-R$ が成り立ち、$\mathrm{S}(q^{4n-3})$は、$\mathrm{B}=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$の素因数2とその他のいくつかの奇数の素因数の各指数乗どうしの積に等しい。

(註:$\mathrm{S}(q^{4n-3})$とRに含まれるそれぞれの$p_1,p_2,\cdots,p_k$の幾つかの素因数の重複を許した積どうしの積は、$p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}$になる。)

(ⅱ)$R=1$の場合、 $q^{4n-3} \mid \mathrm{A}$が成り立ち、$\mathrm{A}=q^{4n-3}R$で、かつ$R=1$のとき、$\mathrm{A}=q^{4n-3}$が成り立ち、次の**(ア),(イ),(ウ)**が成り立つ。

(註:奇数の完全数は、$\mathrm{N}=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}$ (ただし、qは、$q\equiv 1 \pmod 4$の奇素数))

(ア) $\mathrm{S}(q^{4n-3})=\mathrm{B}$である。

(イ) $q \mid (\mathrm{B}-1)$かつ$(\mathrm{B}-\mathrm{A}) \mid (\mathrm{B}-1)$が成り立ち、さらに$\mathrm{B}>q^{4n-3}$である。

(ウ) $\mathrm{A}\geq\dfrac{4\mathrm{B}+1}{5}$が成り立つ。

(証明)

(ⅰ)$R\neq 1$の場合、RはAの真の約数で、式(19)から、

$$q(\mathrm{B}-Rq^{4n-3})=\mathrm{B}-R$$

が成り立つ。

また、命題7の結果から、$\mathrm{S}(q^{4n-3})$とq^{4n-3}は互いに素だから、等式(12)の左辺の因数と右辺の素因数に注目すると、奇数$\mathrm{A}=q^{4n-3}R$は,$\mathrm{B}=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$の2以外の素因数の重複を許して幾つかの積の因数を含む。したがって、Rは、Bの2以外の素因数の幾つかの重複を許した積として表される。

(ii) $R=1$の場合

(ア)について。

$A=q^{4n-3}R$で$R=1$より、$A=q^{4n-3}$となる。(つまり、$S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})=q^{4n-3}$である。)

したがって、$A=q^{4n-3}$を奇数の完全数の定義式:$AS(q^{4n-3})=Bq^{4n-3}$に代入して、

$q^{4n-3}S(q^{4n-3})=Bq^{4n-3}$となる。この等式の両辺を$q^{4n-3}$で割ると、

$$S(q^{4n-3})=B$$

が得られる。

(イ)について。

前頁の(19)の等式に、$R=1$を代入すると、

$$Bq-q^{4n-2}=B-1 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(20)$$

(20)より、$q(B-q^{4n-3})=B-1$だから、$q \mid (B-1)$で、かつ$(B-q^{4n-3}) \mid (B-1)$(つまり、$(B-A) \mid (B-1)$)が成立する。

また、$q(B-q^{4n-3})=B-1$で、Bは正の偶数より、$B-1>0$となり、

$$B-q^{4n-3}>0$$

が成り立つから、$B>q^{4n-3}$を得る。(つまり、前述した「命題6」の結果($B>A$)が成り立っている。)

(ウ) 命題7の(14)の等式で、左辺の因数Rについて、$R=Aq-Bq+B$とおいた。この場合、$R=1$より、

$$Aq-Bq+B=1$$

となる。この等式より、

$$q=\frac{B-1}{B-A}$$

が得られる。qは$q\equiv 1 \pmod 4$を満たす素数だから、$q\geq 5$が成り立つ。したがって、

$$q=\frac{B-1}{B-A}\geq 5 \text{より、} A\geq\frac{4B+1}{5}$$

が成り立つ。 (証終)

＊昨年(20012年)の10月13日に、津田塾大学・数学史シンポジウムで発表したレジュメの中で、命題番号順からはずして、「私にとって興味ある意外な3つの命題([**命題 λ**],[**命題 μ**],[**命題 ν**])を載せました。なぜ、命題の番号順からはずしたかというと、一つの理由は、私が研究中の思いつきの発想で得た結果が意外であったこと、二つ目の理由は、註の箇所で述べたように、検証の過程を経ていなかったので、検証を待たねばならないと思ったからです。再度、計算を見直したところ、[**命題 λ**]($R\neq 1$の場合)にミスが見つかったこと、この命題に関連した[**命題 μ**](奇数の完全数の存

在は$R=1$の場合に限る)が削除に至りました。したがって、問題のミスの箇所を簡単に説明します。[**命題λ**]のミスの箇所は、証明の中の(③)が成立しないことです。以下、直線で囲った部分がもとのレジュメの命題(ミスである)で、それ以外はミスの解説部分です。

([**命題λ**]**のミスの解説**):「用いた命題は、命題1から命題7のLemma Ⅰまでの初等整数論の範囲である。まず、$R\neq 1$の場合、矛盾が起こるプロセスを紹介する。」とした点にミスがあり、$R\neq 1$の場合、矛盾がないことが言える。

[**命題λ**] 命題7および命題7のLemma Ⅰから、「$R\neq 1$の場合、奇数の完全数は存在しない。」ことが言える。

(**証明の中でミスに至るプロセスについて**): 命題7の結果から、$A=q^{4n-3}R$となり、$q\nmid R$が成り立つことが得られた。等式(奇数の完全数Nの必要十分条件$(S(N)=2N\Leftrightarrow S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots\cdots\cdots S(p_k^{2m_k})S(q^{4n-3})=2p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}q^{4n-3}))\Leftrightarrow AS(q^{4n-3})=Bq^{4n-3}$のこと。(ただし、ここで、$A=S(p_1^{2m_1})S(p_2^{2m_2})\cdots S((p_k^{2m_k}),\ B=2p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots\cdots\cdots p_k^{2m_k}$とおいた。)

この等式に$A=q^{4n-3}R$を代入し、両辺をq^{4n-3}で割ると、命題7のLemma Ⅰの(ⅰ)の$R\neq 1$の場合の(19)の式となり、

$$q(B-Rq^{4n-3})=B-R \quad (\text{ただし、}q\text{は、}q\equiv 1(\mathrm{mod}\ 4)\text{を満たす素数}) \quad \cdots\cdots\cdots(①)$$

が成り立つことが示された。この等式(①)の左辺と右辺を比較すると、$B-R$は、奇素数qを因数に持たねばならない。

$$\therefore\ q\mid(B-R) \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(②)$$

(註:ところで、命題7の註より、$B-q^{4n-3}R>0$かつ$B-R>0$が成り立つ。したがって、$B-R\neq 0$である。)

命題7のLemma Ⅰの(ⅰ)$R\neq 1$の場合は,Rの素因数分解で現れる素数たちは、$p_1,p_2,\cdots,p_k$の中の一部分である。$A=q^{4n-3}R$であるから、(12)の式に代入すると、$AS(q^{4n-3})=Bq^{4n-3}\ \Rightarrow\ Rq^{4n-3}S(q^{4n-3})=Bq^{4n-3}\ \Rightarrow\ RS(q^{4n-3})=B$の左辺と右辺にある素因数分解で現れる素数たちは、Bの素因数たち$2,p_1,p_2,p_3,\cdots p_k$に限られ、左辺の$S(q^{4n-3})$は偶数で、Aは奇数より、Rは奇数である。したがって、Rは命題7のLemma Ⅰの(ⅰ)より、$p_1,p_2,p_3,\cdots,p_k$のいくつかの指数乗どうしの積からなる。$B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$だから、Bと$R$の最大公約数は$R$となり、その約数は、$p_1,p_2,\cdots,p_k$の幾つかの指数乗どうしの積(つまり、$R=p_{j_1}^{w_1}p_{j_2}^{w_2}\cdots p_{j_g}^{w_g}\cdots p_{j_z}^{w_z}$ (ただし、$1\leq^{\exists}j_g\leq k,\ 1\leq^{\forall}g\leq z,\ 1\leq^{\exists}w_g\leq 2m_{j_g}$))になる。Bと$R$の公約数は、$R$の約数となる。

(ここまでは、正しいと考える。)

(B $-R$)とRの最大公約数がRで、かつ$q\nmid R$なので、ここから、

$q\nmid(\mathrm{B}-R)$ ・・(③)

を導き出したことがミスの原因でした。(③)が成立すれば、(②)と(③)が矛盾して[**命題λ**]が成立するのですが、(③)が誤りなので[**命題λ**]が成立しません。

そのミスの根拠は、B-Rの因数はR以外に、因数$\frac{\mathrm{B}-R}{R}$(これをUとおくことにする。)が存在し、このUは素因数qを因数に持つことを見落としていました。命題7および命題7のLemma I から、$R\neq1$の場合、A$=Rq^{4n-3}$ かつB$=R\mathrm{S}(q^{4n-3})$が成り立つことが言えた。この2番目の式の両辺からRをそれぞれ引くと、

$$
\begin{aligned}
\mathrm{B}-R&=R\mathrm{S}(q^{4n-3})-R\\
&=R(\mathrm{S}(q^{4n-3})-1)\\
&=R\,\{(1+q+q^2+\cdots\cdots+q^{4n-3})\ -1\}\\
&=R(q+q^2+q^3+\cdots\cdots+q^{4n-3})\\
&=Rq\,(1+q+q^2+\cdots\cdots+q^{4n-4})
\end{aligned}
$$

(註:この式は、後述する(53)で再び現れます。)

となるから、(B-R)のR以外の因数$\frac{\mathrm{B}-R}{R}$=Uは、$q(1+q+q^2+q^3+\cdots\cdots+q^{4n-4})$となり、素因数$q$を必ず持つことが言える。したがって、$q\nmid(\mathrm{B}-R)$ ・・・・・・・・・・・・(③)は誤りで、この点が、[**命題λ**]が成立しない根拠です。 **(以上、[命題λ]の誤りの説明終わり)**

以上述べたことより、[**命題λ**]を削除します。また、[**命題μ**]は[**命題λ**]に関連して導き出したので、ここでも削除します。[**命題μ**]は、以下の通り。

[**命題μ**] 奇数の完全数が存在すると仮定すると、$R=1$でなければならない。さらに、A$=q^{4n-3}$かつS(q^{4n-3})=Bが成り立つ。(つまり、2つの等式の連立になる。)

*この[**命題μ**]のミスの箇所は、「$R=1$でなければならない。」という点である。$R\neq1$であっても、奇数の完全数となる可能性がある。 **(以上、もとのレジュメのミスの箇所の説明終わり)**

津田塾大学で発表後、Rが1であるのか、そうでないのかという課題に取り組んできたが、現段階では、$R\neq1$であるのか、または、$R=1$であるのか、決定する結果が得られず、未定のままである。したがって、[**命題μ**]が成り立つ可能性は否定できない。したがって、これから論じる場合、一般的($R=1$の場合、および、$R\neq1$の場合)にも成立するように、あるいは、Rの値のままでの場合の形で、これから論理を展開することにする。これから述べる[**命題η**],[**命題k**],[**命題ν**],[**命題τ**],[**命題υ**]は、レジュメを書き直す途中で考え付いた命題で、検証されることを望む。

[**命題 η**] 奇数の完全数が存在すると仮定すると、命題7から、

$\mathrm{A}=\boldsymbol{R}q^{4n-3}$かつ$\boldsymbol{R}\mathrm{S}(q^{4n-3})=\mathrm{B}$が成立した。この2つの式から、$\boldsymbol{R}=\mathrm{A}q-\mathrm{B}q+\mathrm{B}$が成り立つ。

したがって、$q=\dfrac{\mathrm{B}-\boldsymbol{R}}{\mathrm{B}-\mathrm{A}}$ となる。

(証明) 命題7から、

$$\boldsymbol{R}\mathrm{S}(q^{4n-3})=\mathrm{B}$$

$$\therefore \boldsymbol{R}\times\frac{q^{4n-2}-1}{q-1}=\mathrm{B}$$

両辺に$(q-1)$を掛けると、

$$\boldsymbol{R}(q^{4n-2}-1)=\mathrm{B}(q-1)$$

$$\boldsymbol{R}q^{4n-2}-\boldsymbol{R}=\mathrm{B}q-\mathrm{B} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(④)$$

命題7より、$\mathrm{A}=\boldsymbol{R}q^{4n-3}$だから、$\boldsymbol{R}q^{4n-2}=\mathrm{A}q$となる。これを(④)上の式に代入すると、

$$\therefore \mathrm{A}q-\boldsymbol{R}=\mathrm{B}q-\mathrm{B}$$

この等式を変形すると、$\boldsymbol{R}=\mathrm{A}q-\mathrm{B}q+\mathrm{B}$が得られる。この式から、

$$q=\frac{\mathrm{B}-\boldsymbol{R}}{\mathrm{B}-\mathrm{A}}$$

が得られる。　(証終)

ここでついでに、代数幾何、数論幾何の見地から思いついた[**命題 κ**]を述べる。レジュメの内容の進め方としては、奇数の完全数を代数幾何、数論幾何に関連させることは、表題の楕円曲線との関連以外はふれるつもりはいなく、次回の発表の機会にと思っていたが、ここでふれた方が、レジュメの進め方として良いと思い、載せることにする。

[**命題 κ**]$\boldsymbol{R}$を定数とする。奇数の完全数が存在すると仮定すると、その個数は高々有限個である。

この命題を証明するための準備としての解説を述べる。

(証明の準備のための解説)：まず、20世紀に証明された2つの定理といくつかの定義を挙げよう。

ジーゲルの定理(1929年)：有理数体上の2変数の多項式f(x, y)で、f(x, y)＝0の種数が1以上であるとき、f(x, y)＝0を満たす整数の組(x, y)は有限個しか存在しない。

ファルティングスの定理(モーデル予想)：f(x, y)を有理数係数の2変数の多項式で、種数が2以上ならば、f(x, y)＝0を満たす有理数の組(x, y)は有限個しか存在しない。

(註：加藤和也氏の本「素数の歌が聞こえる」ぷねうま舎(2012年6月出版)によると、ファルティングス

の定理を代数幾何的な言葉遣いにすると、次のように言い換えられると述べている。

「有理数体上の種数が2以上の代数曲線は、有理点を有限個しかもたない。」)

次に、種数についての定義を述べる。

この「ファルティングスの定理(モーデル予想」)の応用から、次の命題が得られる。(上記の加藤和也氏の本より抜粋する。)

(ⅰ):「$h(x)$が有理係数の次数が5以上である多項式で、重根を持たないものなら、方程式$y^2=h(x)$を満たす有理数の組(x, y)は有限個しか存在しない。」

(ⅱ):「n≥4で、a,b,cが0でない有理数なら、$ax^n+by^n=c$を満たす有理数の組(x, y)は有限個しか存在しない。」

(種数について(上記の本からの抜粋))

(あ):a,b,cは0でない複素数とするとき、代数曲線$ax^n+by^n=c$の種数は、$\frac{(n-1)(n-2)}{2}$である。

(い):$h(x)$を複素数係数の1変数のn次多項式で、重根をもたないものとするとき、

$y^2=h(x)$の種数は、

nが偶数ならば、$\frac{n-2}{2}$である。

nが奇数ならば、$\frac{n-1}{2}$である。　　(以上、抜粋終わり)

(註:種数については、複素数係数で定義されているが、$Q\subset C$であるから、(ⅰ)および(ⅱ)について、**(い)**の定義はそのまま使える。)

ここで、奇数の完全数が存在すると仮定すると、その個数は有限個なのか、あるいは、無限個なのかという問題に解答を与えよう。

奇数の完全数$N=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}$(ただし、n≥2(註:後述する[命題16]より)で、qは、$q\equiv 1 \pmod 4$の素数)について、

$$A=S(p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k})=S(p_2^{2m_1})S((p_2^{2m_2})\cdots S(p_k^{2m_k})$$

$$B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$$

とおくと、命題7より、$A=Rq^{4n-3}$かつ$RS(q^{4n-3})=B$が成立した。この2つの式から、[**命題 η**](つまり、$R=Aq^{-B}q^{+B}$)が成り立つことが言えた。

ここで、$A=Rq^{4n-3}$および$RS(q^{4n-3})=B$に現れる自然数A,B,R,qのうちのいくつかを不定元に置き換えて(あるいは変数と見做して)、その他を定数として、それらの不定元からなる連立の多項式(代数曲線あるいは代数多様体とも見做すことができる)ので、この連立多項式に有理数解、あるいは整数解が存在するのかどうか、そして、それらの解は有限個なのかどうか論じることは可能である。

例えば、$RS(q^{4n-3})=B$について、Bは定数としてあつかい、R,qをそれぞれ不定元Y,X,に置きかえ

ると、

$$YS(X^{4n-3})=B \quad \cdots\cdots\cdots\cdots\cdots\cdots (⑤)$$

が得られる。例えば、この(⑤)の式を満たす整数解が有限個であることが示されれば、奇数の完全数は高々有限個であることが言える。さらに、整数解$(X,Y)=(\boldsymbol{q},\boldsymbol{R})$があるならば、もう一つの式

$A=\boldsymbol{R}\boldsymbol{q}^{4n-3}$も同じように不定元を使って、

$$S(\frac{B}{2})=YX^{4n-3} \quad (註:A=S(p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k})=S(\frac{B}{2})である。) \quad \cdots\cdots (⑥)$$

と表されて、(⑥)の代数曲線上に整数解$(X,Y)=(\boldsymbol{q},\boldsymbol{R})$があれば、奇数の完全数の存在が言えた事になる。また、そのような整数解が存在しなければ、奇数の完全数は存在しないことが言える。

$A,B,\boldsymbol{R},\boldsymbol{q}^{4n-3}$の中のある整数を代表する文字の一部分の因数を定数とし、残りの因数を不定元として表した代数曲線あるいは代数多様体についても、上で説明したことが言える。

例えば、$A=\boldsymbol{R}\boldsymbol{q}^{4n-3}$において、$A=S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_k^{2m_k})$だから、$S(p_1^{2m_1})$を不定元としてYで表し、残りの因数の積を定数と見做して$\boldsymbol{W}_1$とおく。(つまり、$\boldsymbol{W}_1=S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_k^{2m_k})$とおく。)$\boldsymbol{R}$を定数と見做し、$\boldsymbol{q}$を不定元Xで置きかえると、$A=\boldsymbol{R}\boldsymbol{q}^{4n-3}$は、2変数の多項式(代数曲線)$Y\boldsymbol{W}_1=\boldsymbol{R}X^{4n-3}$と表される。この式に整数解$(X, Y)=(\boldsymbol{q},S(p_1^{2m_1}))$が存在するのかどうか。もし、仮に整数解$(\boldsymbol{q},S(p_1^{2m_1}))$が存在しないならば、奇数の完全数が存在しないことになる。

([命題 κ]の証明の準備のための解説終わり)

([命題 κ]の証明) 奇数の完全数が存在すると仮定すると、**命題7**から、$A=\boldsymbol{R}\boldsymbol{q}^{4n-3}$かつ$\boldsymbol{R}S(\boldsymbol{q}^{4n-3})=B$が成立しなければならない。したがって、これらの2つの式を下記に述べるように不定元化(変数化)して、2つの2変数多項式のうちの一つが有理数の組(有理点)、あるいは、整数の組(整数点)の存在の個数が有限個ならば、奇数の完全数の個数は、高々有限個であることが言える。

ここで、$\boldsymbol{q}$を変数Xに置き換える。また、$p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$を変数Yに置き換える。残りの$\boldsymbol{R}$は定数として扱うことになる。$\boldsymbol{q}^{4n-3}$は$X^{4n-3}$と変数化され、$A=S(p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k})$は$S(Y^2)$と変数化される。したがって、$A=\boldsymbol{R}\boldsymbol{q}^{4n-3}$は、次のような2変数多項式

$$S(Y^2)=\boldsymbol{R}X^{4n-3} \quad \cdots\cdots\cdots\cdots (⑦)$$

得られる。(註:$S(Y^2)$がYの多項式で表されることは後述する。) $(X,Y)=(\boldsymbol{q},p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k})$ は、(⑦)の整数解の一つである。$\boldsymbol{R}S(\boldsymbol{q}^{4n-3})=B$は、変数化(不定元で表すと)すると、2変数の多項式

$$\boldsymbol{R}S(X^{4n-3})=2Y^2 \quad (ただし、n\geq 2) \quad \cdots\cdots\cdots (⑧)$$

となる。(註:$\boldsymbol{R}S(X^{4n-3})=2Y^2$の(⑧)の整数解の一つに、$(\boldsymbol{q},p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k})$がある。)

この2変数多項式(⑧)の左辺は、$\boldsymbol{R}S(X^{4n-3})=\boldsymbol{R}(1+X+X^2+\cdots+X^{4n-3})$となる。

したがって、この(⑧)の両辺を2で割ると、2変数多項式(代数曲線)

$$Y^2=\frac{R}{2}(1+X+X^2+\cdots+X^{4n-3}) \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (⑨)$$

が得られる。右辺のXの多項式は、**複素数体上で重根をもたない。**

なぜならば、(⑨)の右辺の(4n-3)次の多項式を0とする複素数の根は、複素平面上で半径1,原点(0,0)を中心とする円周上にX＝1を除いて、等分的に(離散的に)存在して重複していないから。

(註:円分方程式:$X^{4n-3}-1=(X-1)(X^{4n-3}+X^{4n-4}+\cdots+X^2+X+1)=0$の根のうち、X＝1以外のすべての根が, $1+X+X^2+\cdots+X^{4n-3}=0$の根であり、重根は存在しない。)

(⑨)の右辺のXの多項式:$\frac{R}{2}(1+X+X^2+\cdots+X^{4n-3})$の次数については、後述するⅣ章の命題16より、n≥2が示されるから、次数(4n-3)は、4n-3≥5となり、上記**(い)**の定義より、種数は$\frac{(4n-3)-1}{2}=2n-2$≥2である。したがって、ファルティングスの定理の(モーデル予想)の応用(ｉ)より、有理数体上の2変数の多項式(⑨)は、有限個の有理点(X, Y)しか持たない。

さらに、この有限個の有理点のうち、奇数の完全数が存在すると仮定すると、整数点でなければならない。さらにまた、この整数点は(⑦)の代数曲線の式(註:$S(Y^2)=RX^{4n-3}$)を満たさなければならない。さらに、整数点のX座標は4で割ると1余る素数でなければならず、Yは奇数でなければならない。したがって、奇数の完全数が存在すると仮定すると、その個数は高々有限個である。

次に、この命題は(⑨)を満たす代数曲線の右辺のXの多項式の次数(4n-3)に限った制限下での「奇数の完全数が存在すれば高々有限個である。」ことを上記で示したのである。この多項式の次数:(4n-3)が、5,9,13,17,21,25,29,・・・・・が考えられ、各次数の場合について、それぞれ(⑨)を満たす代数曲線上に有理点が高々有限個(したがって、整数点も高々有限個である)であるが、次数が4を法として1余り、かつ、5以上の(⑨)を満たす代数曲線は、次数に関して無限にあるわけではない。後述するp.31の命題11の証明後の註の中で、$AS(q^{4n-3})=Bq^{4n-3}$において、qをxに置き換えて未知数化した代数方程式:$(B-A)x^{4n-2}-Bx^{4n-3}+(B-R)=0$ について、次数(4n-2)に上界M_0(自然数)が存在することを示した。また、p.25の**[命題❸]**でも、得られた代数方程式の次数について上界があることを示した。したがって、各代数曲線上の有理点が有限個で代数曲線(⑨)の右辺の次数も有限である制限下にあるので、「奇数の完全数が存在すれば、高々有限個である。」ことが成り立つ。(証終)

(別証) $f(X, Y)=Y^2-\frac{R}{2}(1+X+X^2+\cdots+X^{4n-3})$とおく。**ジーゲルの定理**を応用すると、$f(X, Y)=0$(⑨と同値な式)の種数は1以上だから、この2変数の代数曲線を満たす整数点は、有限個である。(⑨)の右辺のXについての多項式の次数の制限について、上記の(証明)と同じである。

(証終)

(註:(⑦)の代数曲線は、X, Yの2変数の多項式型である。その理由を述べる。

$A=S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_k^{2m_k})$だから、各$p_i$ $(0\leq i\leq k)$が変数化したYを使った有理数体上で式に表せればよい。

$$p_i=\frac{p_1^{m_1}p_2^{m_2}\cdots p_{i-1}^{m_{i-1}}p_i^{m_i}p_{i+1}^{m_{i+1}}\cdots p_k^{m_k}}{p_1^{m_1}p_2^{m_2}\cdots p_{i-1}^{m_{i-1}}p_i^{m_i-1}p_{i+1}^{m_{i+1}}\cdots p_k^{m_k}}$$

だから、$c_i=\dfrac{1}{p_1^{m_1}p_2^{m_2}\cdots p_{i-1}^{m_{i-1}}p_i^{m_i-1}p_{i+1}^{m_{i+1}}\cdots p_k^{m_k}}$とおくと、$p_i$は変数化され、$p_i$は$c_iY$で表される。

したがって、(⑦)の式:$S(Y^2)=RX^{4n-3}$は、

$$S((c_1Y)^{2m_1})S((c_2Y)^{2m_2})S((c_3Y)^{2m_3})\cdots S((c_kY)^{2m_k})=RX^{4n-3}$$

となる。つまり、(⑦)を変数化(不定元化とでも言うことができるが)すると、

$$\prod_{i=1}^{k}\{1+(c_iY)+(c_iY)^2+(c_iY)^3+\cdots\cdots+(c_iY)^{2m_i}\}=RX^{4n-3}$$

が得られる。ここで、$g(X,Y)=\prod_{i=1}^{k}\{1+(c_iY)+(c_iY)^2+(c_iY)^3+\cdots+(c_iY)^{2m_i}\}-RX^{4n-3}$

とおく。ここで、有理数係数の代数多様体$V(g)=\{(X,Y)\mid g(X,Y)=0\}$とおく。奇数の完全数が存在すると仮定すると、$(q,p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k})\in V(g)$でなければならない。また、(別証)の中でふれたf(X, Y)について、有理数係数の代数多様体$V(f)=\{(X,Y)\mid f(X,Y)=0\}$とする。

また、$V(f,g)=\{(X,Y)\mid f(X,Y)=0 \text{ and } g(X,Y)=0\}$とすると、f(X,Y)とg(X,Y)が共通因子を持たなければ、

$$V(f,g)=V(f)\cap V(g)$$

は、有限個の点からなる。(註:「代数曲線入門」(梶原　健著, 日本評論社)p. 42の**2.5.1の命題**の参照)

ここで、f(X, Y)とg(X, Y)の共通因子がないことは、示さなければならないが、終結式が0なのか、あるいは、0でないのか、計算すればわかることである。しかし、S(N)=2Nが、**命題7**により、2つの$A=Rq^{4n-3}$ and $RS(q^{4n-3})=B$に分解されたことが示されているので、変数化されたf(X,Y)とg(X,Y)は、定数Rを除けば互いに素であることが推察される。その理由は、

$$f(X,Y)=Y^2-\frac{R}{2}(1+X+X^2+\cdots+X^{4n-3})=Y^2-\frac{R}{2}(1+X)\{1+X^2+(X^2)^2+\cdots+(X^2)^{(2n-2)}\}$$

は有理数体上で(Y-(Xの多項式))(Y-(Xの多項式))型に因数分解できない。

なぜならば、もし、$f(X,Y)=(Y-Q_1(X))(Y-Q_2(X))$のように、有理数体上で因数分解すると仮定すると、恒等式として、

$$Y^2-\frac{R}{2}(1+X)\{1+X^2+(X^2)^2+\cdots+(X^2)^{2n-2}\}=(Y-Q_1(X))(Y-Q_2(X))$$

が成立しなければならない。左辺と右辺のYの一次の項およびYを含まない項を較べると、

$$-\frac{R}{2}(1+X)\{1+X^2+(X^2)^2+\cdots+(X^2)^{2n-2}\}=Q_1(X)Q_2(X) \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{(⑩)}$$

$$Q_1(X)+Q_2(X)=0 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \text{(⑪)}$$

でなければならない。(⑩)と(⑪)(註:$Q_2=-Q_1$)より、

$$-\frac{R}{2}(1+X)\{1+X^2+(X^2)^2+\cdots+(X^2)^{2n-2}\}=-Q_1(X)^2 \quad \cdots\cdots\cdots\cdots\cdots\cdots (⑫)$$

ところで、(⑫)の左辺のXについての最高次の次数は奇数(註:(4n-3)次)であるが、右辺は完全平方式の(-1)倍なので、その最高次の次数は偶数でなければならない。これは、矛盾である。したがって、f(X, Y)は有理数体上で既約である。

したがって、もし仮にf(X, Y)とg(X, Y)が共通因数をもつと仮定すると、g(X,Y)は、f(X,Y)を因数をもつことになる。つまり、適当な2変数多項式h(X,Y)が存在して、

$$g(X, Y)=f(X,Y)h(X,Y)$$

$$\therefore S(Y^2)-RX^{4n-3}=\{Y^2-\frac{R}{2}(1+X+X^2+\cdots+X^{4n-3})\}h(X,Y) \quad \cdots\cdots\cdots\cdots\cdots\cdots (⑬)$$

と表されなければならない。

つまり、(⑬)の右辺と左辺のXの最高次数を比較すると、両方とも(4n-3)次であるから、h(X,Y)はXを含まないYだけの1変数多項式(この多項式をH(Y)とおくことにする。)になる。このH(Y)の次数は右辺と比較すると、左辺はYについて$(2m_1+2m_2+\cdots+2m_k)$次の多項式で、右辺のH(Y)は、Yの$(2m_1+2m_2+\cdots+2m_k-2)$次の多項式になるが,(⑬)の左辺は$RX^{4n-3}$の項のみ存在するが、右辺には左辺には無いXの(4n-3)次以下の項$\frac{1}{2}H(Y)X^i$ (ただし、$0\leq i\leq 4n-4$)があるので、恒等式として(⑬)は矛盾する。したがって、f(X,Y)とg(X,Y)は互いに素で共通因数が存在しないことがいえる。したがって、V(f,g)は、有限個の点からなることが言える。

なお、私には、「V(f,g)が有限個の点からなる」という考えの背景に、ベズーの定理が関係していると考える。

したがって、終結式が0であることが成立することが推察されるが、「奇数の完全数の個数は、高々有限個である」という別証に続く3番目の証明が可能であると考える。)　　(註の説明終わり)

命題7より、$A=Rq^{4n-3}$かつ$RS(q^{4n-3})=B$が成り立つ。ここで、$R=1$の場合、

$$A=q^{4n-3} \quad \cdots\cdots\cdots\cdots\cdots\cdots (⑭)$$

$$S(q^{4n-3})=B \quad \cdots\cdots\cdots\cdots\cdots\cdots (⑮)$$

が同時に成り立つ。$A=S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_j^{2m_j})\cdots S(p_k^{2m_k})$ だから、これを(⑭)に代入すると、

$$S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_j^{2m_j})\cdots S(p_k^{2m_k})=q^{4n-3} \quad \cdots\cdots\cdots\cdots (⑯)$$

(⑯)の右辺は、素数qの(4n-3)乗だから、$^{\forall}j$ (ただし、$1\leq j\leq k$)に対して、左辺と比較すると、

$S(p_j^{2m_j})=q^{i_j}$　（ただし、i_jは適当な自然数で、$1\leq i_j\leq 4n-3$　かつ　$\sum_{j=1}^{k} i_j = 4n-3$）　・・・・・・・(⑰)

となる。

[命題τ]　上記の素数p_jについて、

(a)　$p_j\equiv 1 \pmod 4$ならば、m_jは偶数である。

(b)　$p_j\equiv 3 \pmod 4$ならば、m_jは適当な自然数である。

(証明) (a)について。(⑰)より、

$$1+p_j+p_j^2+p_j^3+p_j^4+p_j^5+\cdots+p_j^{2m_j}=q^{i_j} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(⑱)$$

$q\equiv 1 \pmod 4$だから、(⑱)の右辺について、$q^{i_j}\equiv 1 \pmod 4$となる。一方、(⑱)の左辺の各項p_j^r（ただし、$1\leq r\leq 2m_j$)は、$p_j\equiv 1 \pmod 4$だから、$p_j^r\equiv 1 \pmod 4$である。(⑱)の左辺は初項の1を含めて、mod 4で考えると、

$$\overbrace{1+1+1+1+1+1+\cdots\cdots+1}^{2m_j個}\equiv 1 \pmod 4$$

が成立しなければならない。

$\therefore (2m_j+1)\equiv 1 \pmod 4$

が成り立つためには、m_jは偶数でなければならない。

(b)について。

$p_j\equiv 3 \pmod 4$だから、$p_j^2\equiv 1 \pmod 4$である。したがって、p_jの偶数乗$p_j^{2s}=(p_j^2)^s\equiv 1 \pmod 4$が成り立つ。（ただし、$1\leq s\leq m_j$)

一方、p_jの奇数乗$p_j^{2s-1}=p_j^{2(s-1)}\cdot p_j\equiv 1\cdot 3\equiv 3 \pmod 4$となる。(⑱)の左辺の項の数は、$2m_j+1$個であるが、$p_j$の偶数乗となる項の個数は、$m_j$個である。したがって、$p_j$の奇数乗となる項数も$m_j$個である。初項の1を含めると、(⑱)の左辺は、mod 4で考えると、

$$\overbrace{(1+1+1+1+1+\cdots+1)}^{m_j個}+\overbrace{(3+3+3+\cdots+3)}^{m_j個}=(m_j+1)+3m_j=4m_j+1\equiv 1 \pmod 4$$

だから、(⑱)の右辺をmod 4で考えると1だから、m_jが適当な自然数ならば整合して、一致する。　(証終)

[命題ν] [命題7]より、次のことが言えた。

つまり、奇数の完全数を$N=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}$とすると、

$$A=S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k}) \text{ かつ } B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$$

とおいて、$A=q^{4n-3}R$（ただし、$R=Aq-Bq+B$)が成り立った。

さらに、[命題7からのLemma Ⅰ]より、$R=1$の場合、$A=q^{4n-3}$ かつ $B=S(q^{4n-3})$が成り立つことを示した。これらのことから、$R=1$の場合、次の事柄が成り立つ。

$\forall j$（ただし、$1\leq j\leq k$）に対して、

$p_j^{2m_j+1} - q^{i_j} p_j + q^{i_j} - 1 = 0$が成り立つ。このことから、$p_j^{2m_j+1} \equiv 1 \pmod{q^{i_j}}$, $q^{i_j} \equiv 1 \pmod{p_j}$

(証明) (⑰)の式から、

$S(p_j^{2m_j}) = q^{i_j}$ より、$\dfrac{p_j^{2m_j+1}-1}{p_j-1} = q^{i_j}$ が成り立つ。

$\therefore p_j^{2m_j+1} - 1 = q^{i_j}(p_j - 1)$

したがって、

$$p_j^{2m_j+1} - q^{i_j} p_j + q^{i_j} - 1 = 0 \quad \cdots\cdots (⑲)$$

等式(⑲)を$(\bmod\ q^{i_j})$で考えると、

$p_j^{2m_j+1} - 1 \equiv 0 \pmod{q^{i_j}}$

となる。また、等式(⑲)を$(\bmod\ p_j)$で考えると、

$q^{i_j} - 1 \equiv 0 \pmod{p_j}$

が成り立つ。 (証終)

命題7において、奇数の完全数Nの定義:S(N)＝2Nは、
$A = Rq^{4n-3}$ and $RS(q^{4n-3}) = B$が成立することと同値になった。ここで、$R \neq 1$の場合、$A = Rq^{4n-3}$の式に着目すると、Rは命題7からのLemma I より、Rは$B = 2p_1^{2m_1} p_2^{2m_2} \cdots p_k^{2m_k}$の2以外の幾つかの素因数を持つから、$R = p_{j_1}^{w_1} p_{j_2}^{w_2} \cdots p_{j_g}^{w_g} \cdots p_{j_z}^{w_z}$ (ただし、$1 \leq {}^\forall g \leq z, 1 \leq {}^\exists j_g \leq k, 1 \leq {}^\exists w_g \leq 2m_{j_g}$)と表される。
$A = S(p_1^{2m_1}) S(p_2^{2m_2}) S(p_3^{2m_3}) \cdots S(p_i^{2m_i}) \cdots S(p_k^{2m_k}) = Rq^{4n-3} = \left(\prod_{g=1}^{z} p_{j_g}^{w_g}\right) q^{4n-3}$ だから、${}^\forall p_i$ (ただし、

$1 \leq i \leq k$)に対して、$S(p_i^{2m_i})$がRの素因数をもつか、あるいはもたないかということについて考える。

$S(p_i^{2m_i})$が、Rの素因数の重複を数えた任意の積$p_{j_g}^{s_g}$ (ただし、s_gは最大にとる。)で割り切れる場合、

$U_g = \dfrac{R}{p_{j_g}^{s_g}}$とおくと、$U_g$の重複を数えた素因数の中で、$S(p_i^{2m_i})$に含まれる素因数たちの積を
V_gとおく。

$S(p_i^{2m_i}) = p_{j_g}^{s_g} q^{t_g} V_g$ (ただし、$1 \leq s_g \leq w_g$, $0 \leq t_g \leq 4n-3$,)

と表される。

$$\therefore \frac{p_i^{2m_i+1}-1}{p_i-1} = p_{j_g}^{s_g} q^{t_g} V_g$$

この両辺に$(p_i - 1)$を掛けてまとめると、

$$p_i^{2m_i+1} - p_i p_{j_g}^{s_g} q^{t_g} V_g + p_{j_g}^{s_g} q^{t_g} V_g - 1 = 0 \quad \cdots\cdots (⑳)$$

が成り立つ。(⑳)を(mod p_{j_g})で考えると、

$$p_i^{2m_i+1}-1\equiv 0 \pmod{p_{j_g}}$$

p_iとp_{j_g}はともに素数だから、

$p_{j_g}\nmid p_i$ が言える。つまり、$p_i\neq p_{j_g}$が成り立つ。つまり、p_iは、$\boldsymbol{R}$に含まれるどの素因数とも一致しない。

$S(p_i^{2m_i})$が$\boldsymbol{R}$の素因数を含まない場合、[**命題 ν**]と同じような結果が得られる。

したがって、この前半の結果のみ,[**命題 υ**]として、挙げておきます。

[**命題 υ**] $\boldsymbol{R}\neq 1$で、Aのある因数$S(p_i^{2m_i})$が$\boldsymbol{R}$のある素因数p_{j_g}を持つ場合、(⑳)を満たすp_i ,p_{j_g}について、$p_i\neq p_{j_g}$である。

＊以上5つの[命題 η], [命題 κ],[命題 τ],[命題 ν],[命題 υ]が正しいのかどうか、再び検証を待たねばならないが、ここでレジュメを終えないで、奇数の完全数の世界への旅($\boldsymbol{R}=1$ or $\boldsymbol{R}\neq 1$)の場合、あるいは、Aそのままの形か、または$A=q^{4n-3}\boldsymbol{R}$の一般的な形にして考察する)を続けることにします。

したがって、これから、もとの命題順の進め方に戻ります。

[**命題8**] [命題5]の(ｉ)の形の$N=p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}q^{4n-3}$において、

(ｉ)k＝0の場合(つまり、$N=q^{4n-3}$の場合)⇒Nは完全数ではない。

(ⅱ)k＝1の場合(つまり、ここで、$p_1=p,2m_1=2m$とおくと、$N=p^{2m}q^{4n-3}$の場合)⇒Nは完全数ではない。

(証明)(ｉ)について。

この形の$N=q^{4n-3}$が奇数の完全数であると仮定すると、S(N)＝2Nより、

$$S(q^{4n-3})=2q^{4n-3}\quad(\text{ただし、nは自然数})\quad\cdots\cdots\cdots\cdots\cdots\cdots(21)$$

が成り立たねばならない。(21)の左辺は、

$$S(q^{4n-3})=1+q+q^2+q^3+\cdots\cdots+q^{4n-3}$$

$$=\frac{q^{4n-2}-1}{q-1}\qquad\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(22)$$

(21)と(22)より、

$$\frac{q^{4n-2}-1}{q-1}=2q^{4n-3}$$

となる。この両辺に$(q-1)$を掛けて分母を払うと、

$\therefore q^{4n-2}-1=2(q-1)q^{4n-3}$

$q^{4n-2}-1=2q^{4n-2}-2q^{4n-3}$

$\therefore -1=q^{4n-2}-2q^{4n-3}$

$-1=q^{4n-3}(q-2)$ ……(23)

$q\equiv 1 \pmod 4$より、qは5以上の素数であるから、(23)の右辺は、正の整数となるから、左辺の値が(-1)に等しくなることはない。矛盾である。したがって、$N=q^{4n-3}$型の奇数の完全数は存在しない。

(ⅱ)について。

$N=p^{2m}q^{4n-3}$が奇数の完全数であると仮定すると、$S(N)=2N$より、

$S(p^{2m})S(q^{4n-3})=2p^{2m}q^{4n-3}$

$$\frac{p^{2m+1}-1}{p-1}\cdot\frac{q^{4n-2}-1}{q-1}=2p^{2m}q^{4n-3}$$

両辺に$(p-1)(q-1)$を掛けると、

$(p^{2m+1}-1)(q^{4n-2}-1)=2p^{2m}q^{4n-3}(p-1)(q-1)$

$p^{2m+1}q^{4n-2}-p^{2m+1}-q^{4n-2}+1=2p^{2m}q^{4n-3}(pq-p-q+1)$

$1-p^{2m+1}-q^{4n-2}=2p^{2m}q^{4n-3}(pq-p-q+1)-p^{2m+1}q^{4n-2}$

$1-p^{2m+1}-q^{4n-2}=p^{2m}q^{4n-3}(pq-2p-2q+2)$

$1-p^{2m+1}-q^{4n-2}=p^{2m}q^{4n-3}\{(p-2)(q-2)-2\}$ ……(24)

pは3以上の奇素数，qは「命題3」より、$q\equiv 1 \pmod 4$を満たすので5以上の素数となり、(24)の右辺は正の整数となり、(24)の左辺は負の整数となる。これは矛盾である。したがって、$N=p^{2m}q^{4n-3}$型の奇数の完全数は存在しない。 (証終)

(註:k=3,4,・・・・・, 9,10,・・・・・・の場合、上述した証明方法が、k=1,2の場合と同じ様に適用できるのかどうか未定である。k=5の場合でも、計算はかなり複雑になるのではないだろうか。この点については、奇数の完全数Nの素因数分解に現れる素因数の個数(k個)との関係は、Ⅲ章の「Euler以後の奇数の完全数についての考察」の中で言及した⑨のHagis,⑩のPomerance,⑪のNielsen等の結果と関連する。)

命題7の結果の$q^{4n-3}\mid A$より、$q^{4n-3}\leq A$であるから、$A=q^{4n-3}$の場合($R=1$の場合)と$q^{4n-3}<A$の場合(つまり、$R\neq 1$で、$A=Rq^{4n-3}$の場合)の二通りに分類されるが、これからは、Rは1以上のAの約数として、広く一般的に考察することにする。

[**命題9**]奇数の完全数Nが存在すると仮定すると、次の事柄が成り立つ。

$$(\mathrm{i})\ S(q^{4n-3}) \leq B \qquad (\mathrm{ii})\ S\left(\frac{RS(q^{4n-3})}{2}\right)=A \qquad (\mathrm{iii})\ S\left(\frac{S\left(\frac{RS(q^{4n-3})}{2}\right)}{R}\right)=S(q^{4n-3})$$

(証明)(ⅰ)について

命題5より、奇数の完全数Nの存在を仮定すると、$N=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}$となり、$q$は、$q\equiv 1 \pmod 4$を満たす素数でなければならなかった。そして、Sを約数の総和を求める作用とすると、Nは、完全数の定義により、次の等式

$$S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})S(q^{4n-3})=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3} \quad \cdots\cdots(25)$$

が成り立たねばならなかった。ここで、$A=S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})$,$B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$とおいた。(25)の等式は、

$$AS(q^{4n-3})=Bq^{4n-3} \quad \cdots\cdots(26)$$

この(26)の式(以前に言及した命題7の証明の(12)の式に該当した式)は、不思議な等式である。

その理由は、命題7より、Aはq^{4n-3}を約数にもち、$A=Rq^{4n-3}$ ($^{\exists}R\in Z$)とおいて、(26)に代入して両辺をq^{4n-3}で割ると、

$$RS(q^{4n-3})=B \quad \cdots\cdots(27)$$

$$\therefore S(q^{4n-3})=\frac{B}{R}\ (R\text{はAとBの公約数でもあるから、}\frac{B}{R}\text{は、Bの約数}) \quad \cdots\cdots(28)$$

となる。$R\geq 1$だから、$S(q^{4n-3}) \leq B$が成り立つ。

(ⅱ)について

(27)の等式に、$B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$を代入し、両辺を2で割ると、

$$\frac{RS(q^{4n-3})}{2}=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$$

となる。この両辺にさらに約数の和を出力させるSを作用させると、

$$S\left(\frac{RS(q^{4n-3})}{2}\right)=S(p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}) \quad \cdots\cdots(29)$$

(29)の右辺はAとなるから、

$$S\left(\frac{RS(q^{4n-3})}{2}\right)=A \quad \cdots\cdots(30)$$

が成り立つ。

(ⅲ)について

$A=Rq^{4n-3}$だから、これを(30)代入し、

$$S\left(\frac{\boldsymbol{R}S(q^{4n-3})}{2}\right)=\boldsymbol{R}q^{4n-3}$$

この両辺を$\boldsymbol{R}$で割り、にさらにSを作用させると、

$$S\left(\frac{S\left(\frac{\boldsymbol{R}S(q^{4n-3})}{2}\right)}{\boldsymbol{R}}\right)=S(q^{4n-3}) \quad \cdots\cdots(31)$$

となり、この右辺は(28)の左辺に戻ってしまった。つまり、約数の和を出す作用によって、4を法として1と合同な素数qの冪q^{4n-3}はA,Bと関係し、無限に再帰性とも言える入れ子の関係になっている。

(ただし、$\boldsymbol{R}$は1か$p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$の約数である。) (証終)

＊:約数の和を出力する作用Sについて、無限の入れ子のような再帰性をもつ素数がはたして存在するのであろうか？

V．奇数の完全数が存在すると仮定すると、どのような代数方程式が成立しなければならないか？

Ⅱ章とⅣ章は、主に単なる代数的計算によって得られた命題である。この章では、奇数の完全数$N=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}$において、$A=S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})$, $B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$とおいて、奇数の完全数の定義式: $A\times S(q^{4n-3})=B\times q^{4n-3}$を中心に据えて、奇数の完全数の素因数の中で、4を法として1に合同な素数qについて、そのべき指数も他の素因数よりは比較的に詳しくわかっているので、qを未知数xと置き換えて代数方程式と関連させて述べることにする。代数方程式の解は、関数とy＝0(x軸)との交点のx座標と考えられるので、関数の場合は、xを変数とみなして論を進めることにする。命題6の証明の中の(12)の等式にqを変数xに置き換えて代入すると、

$$A\times S(x^{4n-3})=B\times x^{4n-3} \quad \cdots\cdots(32)$$

となる。ここで、$f(x)=AS(x^{4n-3})-Bx^{4n-3}$とおくと、(32)は,代数方程式 f(x)＝0と同値である。この方程式の次数は、一見すると、(4n-3)次の代数方程式f(x)＝0と見なして、実数解xが存在するのか、あるいは、存在しないのか論じたくなる。しかし、命題7より、$q^{4n-3}\mid A$なので、qをx と置き換えたので、Aの約数$\boldsymbol{R}$ (命題7で言及した$\boldsymbol{R}$のこと)を選んで、Aは変数化されて、$\boldsymbol{R}x^{4n-3}$と表される。

これをf(x)＝$AS(x^{4n-3})-Bx^{4n-3}$＝0に代入すると、

$$f(x)=AS(x^{4n-3})-Bx^{4n-3}=\boldsymbol{R}x^{4n-3}\frac{(x^{4n-2}-1)}{x-1}-Bx^{4n-3}=0 \quad (\text{ただし、nは正の整数})$$

となり、両辺に(x－1)を掛けると、$(x-1)f(x)=\boldsymbol{R}x^{4n-3}(x^{4n-2}-1)-Bx^{4n-3}(x-1)=0$となる。変形して、

$$\boldsymbol{R}x^{8n-5}-Bx^{4n-2}+(B-\boldsymbol{R})x^{4n-3}=0 \quad \cdots\cdots(33)$$

(33)の解 $x=q$は、$q\equiv 1 \pmod 4$の奇素数であるから、$x\neq 0,1$より、(33)の両辺をx^{4n-3}で割ると、

$\boldsymbol{R}x^{4n-2}-Bx+(B-\boldsymbol{R})=0$ (この式の左辺をF(x)とおき、関数とみなす。) ‥‥(34)

となる。(34)から、次の代数方程式が得られる。

$F(x)=\boldsymbol{R}x^{4n-2}-Bx+(B-\boldsymbol{R})=0$ (註:F(1)=0より、$\boldsymbol{Q}$上で既約ではない。)‥‥‥‥‥‥‥‥(35)

ところで、Bと$\boldsymbol{R}$を固定した定数として、(35)の代数方程式の1以外の実数解があるのかどうか、また、実数解があった場合、それが有理数なのかどうか、あるいは整数解があるのかどうか、さらにその整数解が素数なのかどうか、また、その素数は4を法として1に合同なのかどうか調べてみる必要がある。

(註:(35)を満たす実数解$x=\boldsymbol{q}$(ただし、$\boldsymbol{q}$は、$\boldsymbol{q}\equiv 1 \pmod 4$を満たす素数)が存在すれば、(35)から逆に(34)、そして(33) ⇒ (32)が成り立ち、奇数の完全数の定義に辿りつくことができる。)

しかし、例えBと$\boldsymbol{R}$を固定した定数と仮定しても、命題7, 命題7のLemma Ⅰ により、Aは$\boldsymbol{q}^{4n-3}$ の倍数となり、$S(\boldsymbol{q}^{4n-3})$はBの約数を因数にもち、さらに、$\boldsymbol{q}^{4n-3}$は、命題9よりSに関して再帰性があるので、AとBと$\boldsymbol{q}$は、複雑に関係している。したがって、Aを定数とするのかどうか、またBを定数にするのかどうか、$\boldsymbol{q}$を変数化(あるいは、不定元と見做す)とするのかどうかが問題ではあるが、(35)の代数方程式を代数曲線または代数曲面の式として考えた方が、一般的な命題が得られることだろう。Bと$\boldsymbol{R}$を定数と仮定しても、この(35)の代数方程式で、論を進めても次の結果(命題❶ ,命題❷,命題❸)を得ることができるが、後述するようにAをその因数$\boldsymbol{R}$ を使った表し方をしないでAとBを定数として固定し、$G(x)=\{Bx^{4n-3}-AS(x^{4n-3})\}\times(x-1)$とおいて、$G(x)=0$の代数方程式を考えることも同じような結果を得るので、$F(x)=0$の実数解についての証明を簡略して載せることにします。

[命題❶] 奇数の完全数が存在すると仮定すると、$x>0$の範囲で、(35)の代数方程式

$F(x)=\boldsymbol{R}x^{4n-2}-Bx+(B-\boldsymbol{R})=0$

を満たす$x=1$以外の実数解は存在してもただ1個で、それは、$x=\boldsymbol{q}$でなければならない。

(証明) (34)の左辺の関数をF(x)を使って、$y=F(x)$とおく。この関数の定義域を$0<x$で考える。後述する[命題16]の(ⅰ),(ⅱ)より、$n=1$のとき、奇数の完全数が存在しないので、$n\geq 2$でなければならない。したがって、$y=F(x)$のついては、$(4n-2)$次関数で、ただし、$(4n-2)\geq 6$でなければならない。

奇数の完全数が存在すると仮定すると、$y=F(x)$のグラフを描くと、次の(あ),(い),(う)のうち、(あ),(い)は成立せず、(う)のみが成り立つことを説明する。$y=F(x)$を微分すると、

$F'(x)=\boldsymbol{R}(4n-2)x^{4n-3}-B$

$F'(x)=0$の実数解は、$x=\sqrt[4n-3]{\dfrac{B}{\boldsymbol{R}(4n-2)}}$ のみである。この実数解をαとおく。$y=F(x)$は区間$0<x\leq\alpha$では単調減少し、$\alpha\leq x$では単調増加である。したがって、$y=F(x)$は、$x=\alpha$

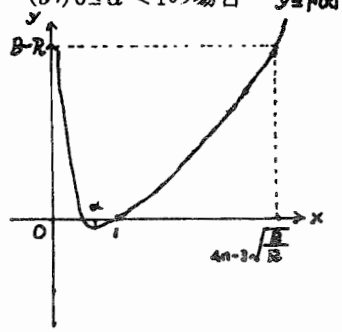
で唯一の極小値をとる。ところで、F(0)＝B－R＞0である。(なぜなら、B＞A＞Rだから。さらに、F′(0)＝0である。)

また、y＝F(x)とy＝B－Rとの交点は,連立させて、F(x)＝B－Rより、

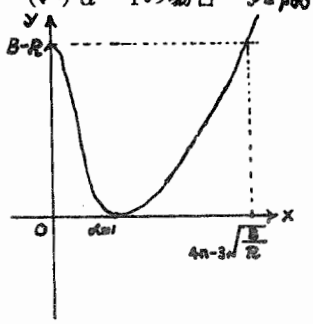
$Rx^{4n-2}-Bx+(B-R)=B-R$

を解くと、x＝0以外の実数解は、$\sqrt[4n-3]{\frac{B}{R}}$ が得られる。F(1)＝0を考慮して、y＝F(x)のグラフを以下の(あ),(い),(う)の3通りが考えられる。

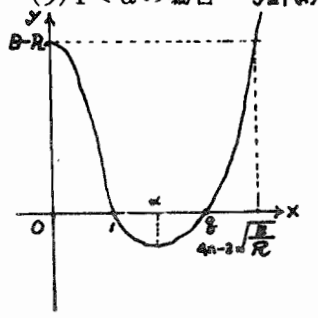
(あ) $0\leq\alpha<1$の場合



(い) $\alpha=1$の場合



(う) $1<\alpha$の場合



なお、上記3つのグラフについて、極小値F(α)＜0でなければならない。なぜならば、F(α)＞0と仮定すると、0＜x の範囲に極小値が唯一つあることになるが、$\lim_{x\to\infty}F(x)=\infty$なの で、0＜x の範囲で最小値はF($\alpha$)＞0となるが、F(1)＝0と矛盾する。また、0＜xでF′(x)＞0なので、F(α)＝0とすると、$\alpha=q=1$となって、矛盾である。(註:この場合、(い)のグラフに該当する。)

(あ)の場合、F(x)＝0を満たすx＝1以外の実数解は0＜x＜1の範囲にあり、x＝q≥5と矛盾する。

(い)の場合、F(x)＝0を満たす実数解は、x＝1のみで、これも矛盾する。

(う)の場合、F(x)＝0を満たすx＝1以外の実数解は、1＜xの範囲に唯一つ存在し、その解はx＝qでなければならない。この場合、F(α)＜0となる。　　(証終)

[**命題❷**] $F(x)=Rx^{4n-2}-Bx+(B-R)=0$を満たすx＝1以外の実数解(x＝$q$)は、区間

$\alpha=\sqrt[4n-3]{\frac{B}{R(4n-2)}}<x<\sqrt[4n-3]{\frac{B}{R}}$ の範囲に1個ある。(ただし、αは$(\frac{dF}{dx})_{x=\alpha}=0$となるx座標)

(**証明**)命題❶の結果より、F(α)＜0かつF$(\sqrt[4n-3]{\frac{B}{R}})>0$であるから、中間値の定理より、開区間 $\alpha=\sqrt[4n-3]{\frac{B}{R(4n-2)}}<x<\sqrt[4n-3]{\frac{B}{R}}$ の範囲に少なくとも実数解が少なくとも一つあるが、極値がただ一つしか存在しないから,この区間で実数解(x＝q)が唯一つ存在しなければならない。　　(証終)

[**命題❸**] F(x)＝0を満たすx＝1以外の実数解(x＝q)が存在するならば、次数(4n-2)に上限がある。

(**証明**)[**命題❷**]で述べた開区間について、右端の数値について、$\lim_{n\to\infty} \sqrt[4n-3]{\frac{B}{R}}=1$であり、さらに、左端の数値について、$\lim_{n\to\infty} \sqrt[4n-3]{\frac{B}{R(4n-2)}}=1$となる。このことはF(x)の次数が増加すると、区間の幅は0に近く小さくなり、F(x)＝0を満たすx＝1以外の実数解x＝q(ただし、qは$q\equiv 1(\mathrm{mod}\ 4)$を満たす素数)は、この開区間に属さないことになる。これは、奇数の完全数の存在の仮定に矛盾する。したがって、ある自然数M_0があって、次数(4n-3)＜M_0でなければならない。実際に、M_0の候補を求めてみる。

$q\geq 5$で、$\sqrt[4n-3]{\frac{B}{R}}>q$だから、$\sqrt[4n-3]{\frac{B}{R}}>5$でなければならない。この不等式の両辺の常用対数をとると、

$$\log\left(\sqrt[4n-3]{\frac{B}{R}}\right)>\log 5$$

$$\therefore\ \frac{1}{4n-3}\log\left(\frac{B}{R}\right)>\log 5$$

$$4n-3<\frac{\log B-\log R}{\log 5}$$

となるから、F(x)の次数(4n-2)について、$\left(\frac{\log B-\log R}{\log 5}+1\right)$より大で最小な自然数を$M_0$とすればよい。尚、上記の命題❶,❷,❸は、$R$＝1の場合にも成立する。この場合、

$F(x)=x^{4n-2}-Bx+(B-1)$ となり、F(x)＝0を満たすx＝1以外の実数解は、

$$\sqrt[4n-3]{\frac{B}{4n-2}}<x<\sqrt[4n-3]{B}$$

の区間に唯一つ存在する。ただし、F(x)の次数(4n-2)については、$\left(\frac{\log B+\log 5}{\log 5}\right)$より大でかつ最小な自然数を$M_0$とすれば、F(x)の次数に関して、奇数の完全数が存在すると仮定すると、と、(4n-2)＜M_0という制限下にある。　　(証終) ⇒(以上で、命題❶,❷,❸の説明終わり)

上で述べことがらは、奇数の完全数の定義と命題7および命題7のLemma Ⅰから、y＝F(x)のグラフで、y＝0とおいて、F(x)＝0のx＝1以外の実数解(その中の整数解)について考えてきた。命題7および命題7のLemma Ⅰを用いずに、これからは、奇数の完全数の定義:

$$S(N)=2N\Leftrightarrow A\times S(q^{4n-3})=B\times q^{4n-3}$$

において、qを変数化してxと置き換えて、AとBを固定した定数として扱い、次の式で考えるこ

とにする。(註:したがって、Rも定数として扱うことになる。)

$$A\times S(x^{4n-3})=Bx^{4n-3}$$

$$\therefore Bx^{4n-3}-A\times\frac{x^{4n-2}-1}{x-1}=0 \quad \cdots\cdots(36)$$

となる。ここで、$g(x)=Bx^{4n-3}-AS(x^{4n-3})$とおくことにする。(36)の両辺に$(x-1)$をかけてまとめると、

$$\therefore (B-A)x^{4n-2}-Bx^{4n-3}+A=0 \quad \cdots\cdots(37)$$

(37)の左辺は、$(x-1)g(x)$だから、この関数を$G(x)$とおく。(37)の代数方程式は、

$$(x-1)g(x)=Bx^{4n-3}(x-1)-A(x^{4n-2}-1)=0$$

となる。

$$G(x)=(B-A)x^{4n-2}-Bx^{4n-3}+A \quad (\text{註:[命題6]より、}(B-A)>0\text{である。}) \quad \cdots\cdots(38)$$

奇数の完全数の存在を仮定すると、代数方程式$G(x)=0$を満たす1以外の実数解が存在しなければならない。そして、その実数解は、$x=q$(ただし、qは、$q\equiv 1\pmod 4$の素数)の型の整数解なのかどうか、出来うるところまで調べることにする。

まず、(38)の式を用いて、$G(x)=(B-A)x^{4n-2}-Bx^{4n-3}+A=0$

の実数解について考える。

初めに、$G(x)=0$の次数$(4n-2)$のnについて、$n=1$の場合と$n\geq 2$の場合に分類して述べる。

[命題10] 命題5の(ⅰ)において、n=1の場合(つまり、$4n-2=2$の場合)、奇数の完全数

$N=p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}q$が存在すると仮定すると、(38)の関数は、$G(x)=(B-A)x^2-Bx+A$の型になる。$G(x)=0$の実数解は、2個あり、それらは、$x=1,\frac{A}{B-A}$ である。

さらに、$\frac{A}{B-A}$は5以上の素数より、$q=\frac{A}{B-A}$(ただし、qは$q\equiv 1\pmod 4$を満たす素数)でなければならない(註)。したがって、$B>A\geq\frac{5}{6}B$が 成り立つ。

(註:後述する命題15により、$\frac{A}{B-A}$は整数にならない。⇒Nは奇数の完全数ではない。)

(証明) $G(x)$の最高次の係数$(B-A)$は、命題6より、$(B-A)>0$である。$n=1$の場合、次数$4n-2=2$で、

$$G(x)=(B-A)x^2-Bx+A=(x-1)\{(B-A)x-A\} \quad \cdots\cdots(39)$$

となり、$G(x)=0$とおくと、その実数解(実は有理数解)は、

$x=1,\ \frac{A}{B-A}$である。$x=1$以外の実数解は、$x=\frac{A}{B-A}$である。$n=1$の場合、奇数の完全数が存在するためには、$\frac{A}{B-A}\neq 1$かつ$\frac{A}{B-A}$が4を法として1と合同なの素数でなければならない。

まず、$\frac{A}{B-A}\neq 1$を示す。

$\frac{A}{B-A}=1$と仮定すると、$2A=B$となる。

この等式($2A=B$)は、すなわち、$2S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$ であるから、

$$\therefore 2(1+p_1+p_1^2+\cdots+p_1^{2m_1})(1+p_2+p_2^2+\cdots+p_2^{2m_2})\cdots\cdots(1+p_k+p_k^2+\cdots+p_k^{2m_k})=2p_1^{2m_1}p_2^{2m_2}\cdots\cdots p_k^{2m_k}$$

この両辺を2で割ると、

$$(1+p_1+p_1^2+\cdots+p_1^{2m_1})(1+p_2+p_2^2+\cdots+p_2^{2m_2})\cdots\cdots(1+p+p_k^2+\cdots+p_k^{2m_k})=p_1^{2m_1}p_2^{2m_2}\cdots\cdots p_k^{2m_k}$$

この等式は、左辺の値が右辺の値よりも大きいから、明らかに矛盾である。したがって、

$\frac{A}{B-A}\neq 1$でなければならない。したがって、奇数の完全数が存在すると仮定すると、$x=\frac{A}{B-A}$は4を法として1と合同な素数より、5以上でなければならない。つまり、$\frac{A}{B-A}\geq 5$となり、命題6と組み合わせると、$B>A\geq\frac{5}{6}B$となる。 (証終)

[命題11] 奇数の完全数が存在すると仮定すると、nは2以上の整数として、次の開区間

$$\alpha=\frac{B(4n-3)}{(B-A)(4n-2)}<x<\frac{B}{B-A}$$

内に、ただ1個の$x=\gamma$(実数)が存在し、$G(\gamma)=0$となる。さらに、$\gamma=q$で、qは$q\equiv 1\pmod 4$を満たす素数でなければならない。

(証明) $n\geqq 2$のとき、xの関数 $y=G(x)$のグラフを調べる。$G(x)$をxで微分する。

$$G'(x)=(B-A)(4n-2)x^{4n-3}-B(4n-3)x^{4n-4}=(B-A)(4n-2)x^{4n-4}\{x-\frac{B(4n-3)}{(B-A)(4n-2)}\}$$

$G'(x)=0$より、$x=0,x=\frac{B(4n-3)}{(B-A)(4n-2)}$が得られる。ここで、$\alpha=\frac{B(4n-3)}{(B-A)(4n-2)}$とおくことにする。

命題6より、$A<B$より、$B-A>0$である。したがって、$\alpha>0$となる。

$$G''(x)=(B-A)(4n-2)(4n-3)x^{4n-4}-B(4n-3)(4n-4)x^{4n-5}$$

$$\therefore G''(x)=(B-A)(4n-2)(4n-3)x^{4n-5}\{x-\frac{B(4n-4)}{(B-A)(4n-2)}\}$$

となる。$G''(0)=0$である。また、

$$G'(\alpha)=G'(\frac{B(4n-3)}{(B-A)(4n-2)})=(B-A)(4n-2)(4n-3)\{\frac{B(4n-3)}{(B-A)(4n-2)}\}^{4n-5}\{\frac{B}{(B-A)(4n-2)}\}$$

より、

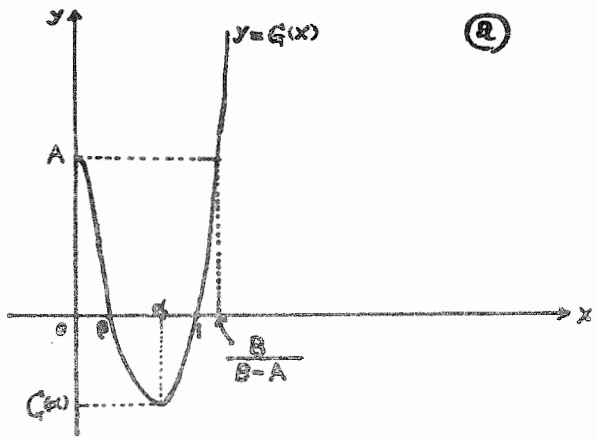
$G''(\alpha)=G''(\frac{B(4n-3)}{(B-A)(4n-2)})>0$となる。したがって、$x=\alpha$で極小となり、$y=G(x)$はただ1個の極小値$G(\alpha)$をとる。また、$G(0)=A$,$G(1)=0$である。また、

$G(\frac{B}{B-A})=(B-A)(\frac{B}{B-A})^{4n-2}-B(\frac{B}{B-A})^{4n-3}+A=(\frac{B}{B-A})^{4n-3}\{(B-A)\frac{B}{B-A}-B\}+A=A$

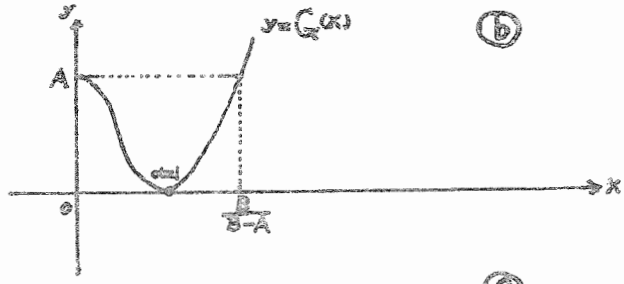
となる。さらに、$\lim_{x\to\infty} G(x)=\infty$である。

$y=G(x)$は、$0<x$の範囲で極小値が1個だけで、$G(x)=0$のtrivialな実数解$x=1$以外の実数解を持つためには、中間値の定理より、$G(\alpha)<0$でなければならない。$y=G(x)$のグラフの概形を、αと1の大小と関連させて述べる。

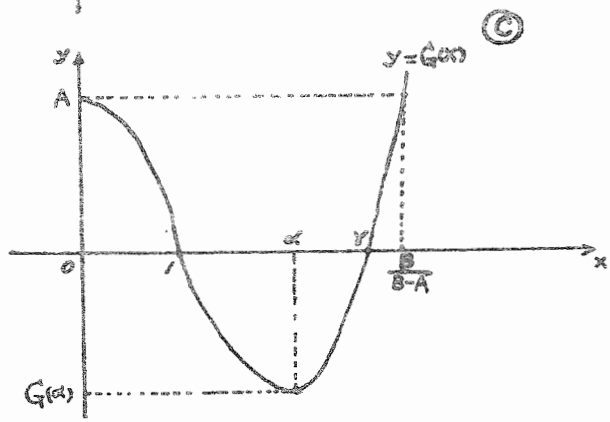
ⓐ$0<\alpha<1$の場合、$y=G(x)$は、$0<x<\alpha$で単調減少、$x=\alpha$で極小、$\alpha<x$で単調増加である。したがって、もう一つの実数解が存在するためには、中間値の定理より、$G(\alpha)<0$でなければならない。$x=1$以外の$G(x)=0$の実数解$x=\beta$は、$0<\beta<\alpha<1$で、βが整数とならないから、この場合は奇数の完全数は存在しない。



ⓑ $\alpha=1$の場合、$G(\alpha)=G(1)=0$で極小値をとるから、$y=G(x)$は、$x=\alpha=1$で、x軸と接する。したがって、$x=\alpha=1$は重解となるから、この場合は奇数の完全数は存在しない。



ⓒ $1<\alpha$の場合、$y=G(x)$は、$0<x<\alpha$で単調減少、$x=\alpha$で極小、$\alpha<x$で単調増加である。$G(x)=0$を満たす$x=1$以外の実数解をもつためには、$G(\alpha)<0$でなければならない。この場合、$x=1$以外の実数解を$x=\gamma$とおくと、$1<\alpha<\gamma$となり、$x=\gamma$が素数となる可能性があることが言える。さらに、$\frac{B}{B-A}=1+\frac{A}{B-A}>1$で、$G(\frac{B}{B-A})=A>0, G(\alpha)<0$だから、中間値の定理より、



開区間$\alpha<x<\frac{B}{B-A}$

に、G(x)＝0の実数解x＝γが1個だけある。それは、γ＝qでなければならない。　　(証終)

(註:開区間$\alpha=\frac{B(4n-3)}{(B-A)(4n-2)}<x<\frac{B}{B-A}$において、$\lim_{n\to\infty}\alpha=\frac{B}{B-A}$となるから、nが増加するとx＝$q$が存在する区間の幅が限りなく0に収束する。さらに、$F(\frac{B}{B-A})\neq 0$となるから、nに上界M_1があるといえる。実際に、F(x)の次数(4n-2)の上界M_1について、$\alpha=\frac{B(4n-3)}{(B-A)(4n-2)}<q<\frac{B}{B-A}$より、この不等式を解くと、$4n-2<\frac{B}{B-q(B-A)}$かつ $q=\frac{B-R}{B-A}$(註:命題7より)となるから、$4n-2<\frac{B}{R}$が成り立つ。この右辺の値をM_1とおけばよい。つまり、p.27の[**命題❸**] と同様な命題が成り立つことが言える。)

[**命題12**] 奇数の完全数$N=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}$において、nが2以上の整数とする。(38)の関数G(x)において、$G(\frac{A}{B-A})<0$である。

(証明) $G(\frac{A}{B-A})=(B-A)(\frac{A}{B-A})^{4n-2}-B(\frac{A}{B-A})^{4n-3}+A$

$$=(B-A)(\frac{A}{B-A})(\frac{A}{B-A})^{4n-3}-B(\frac{A}{B-A})^{4n-3}+A$$

$$=(\frac{A}{B-A})^{4n-3}(A-B)+A=-A(\frac{A}{B-A})^{4n-4}+A$$

$$=A\{1-(\frac{A}{B-A})^{4n-4}\}\quad\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(40)$$

ところで、命題11より、$\frac{B}{B-A}>q$ が成り立ち、$q\geqq 5$を満たす素数であるから、

$\frac{B}{B-A}-1>q-1\geqq 4$が成り立つ。ところで、$\frac{B}{B-A}-1=\frac{B-(B-A)}{B-A}=\frac{A}{B-A}\geq 4$が成立する。したがって、(40)の因数$\{1-(\frac{A}{B-A})^{4n-4}\}$は負の値になり、A＞0より、$G(\frac{A}{B-A})<0$となる。

(証終)

[**命題13**] 奇数の完全数が存在すると仮定する。$G(x)=(B-A)x^{4n-2}-Bx^{4n-3}+A=0$(ただし、nは2以上の整数とする)の2個の実数解のうち、x＝1以外の実数解x＝qは、

開区間$\frac{A}{B-A}<x<\frac{B}{B-A}$内にただ1個存在しなければならない。

(証明) 命題12より、$G(\frac{A}{B-A})<0$ である。さらに、$G(\frac{B}{B-A})=A>0$だから、中間値の定理より、開区間$\frac{A}{B-A}<x<\frac{B}{B-A}$内に、方程式G(x)＝0の実数解は、1個だけ存在する。その実数解は、

x＝q($q\equiv 1\pmod 4$を満たす)となる素数でなければならない。

(証終)

[命題14] 奇数の存在を仮定すると、$\frac{B}{B-A}$は、有理数ではあるが、整数ではない。

(証明) $\frac{B}{B-A}$が整数であると仮定する。

$$\frac{B}{B-A}=1+\frac{A}{B-A} \quad \cdots\cdots(41)$$

が整数より、$\frac{A}{B-A}$もまた整数でなければならない。

したがって、$A=(B-A)s$ を満たす適当な自然数sが存在する。この式を(41)に代入して、

$$(s+1)A=sB \quad \cdots\cdots(42)$$

が成り立つ。sと(s+1)は互いに素であるから、

$$(s+1)\mid B,\ \ s\mid A$$

が成り立たねばならない。つまり、

$$(s+1)\mid 2p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k} \quad \cdots\cdots(43)$$

$$s\mid S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_k^{2m_k}) \quad \cdots\cdots(44)$$

(42)において、$s\neq 1$である。(また、Aは奇数であり、Bは偶数だから、(44)より、sは奇数である。)

なぜならば、$s=1$と仮定すると、(42)の式は、

$$2A=B$$

が成り立たねばならない。この式を変形すると、$\frac{A}{B-A}=1$となる。しかし、

$\frac{A}{B-A}=\frac{B}{B-A}-1$で、命題12の証明の中で示した不等式$\frac{B}{B-A}\geq 5$だから、$\frac{A}{B-A}\geq 4$より、矛盾が起こる。

したがって、sは、2以上の奇数である。(42)の両辺にq^{4n-3}を掛けると、

$$(s+1)Aq^{4n-3}=sBq^{4n-3} \quad \cdots\cdots(45)$$

奇数の完全数の存在を仮定しているから、

$$Bq^{4n-3}=AS(q^{4n-3}) \quad \cdots\cdots(46)$$

が成り立つ。(46)を(45)に代入すると、

$$(s+1)Aq^{4n-3}=sAS(q^{4n-3})$$

$$\therefore (s+1)q^{4n-3}=sS(q^{4n-3}) \quad \cdots\cdots(47)$$

sと(s+1)は互いに素であるから、$s\mid q^{4n-3}$,$(s+1)\mid S(q^{4n-3})$となる。したがって、

$s=q^j$ (ただし、$1\leqq {}^{\exists}j\leqq 4n-3$を満たす適当な自然数)となる。

これを(47)に代入して両辺を$s=q^j$で割ると、

$$S(q^{4n-3})=\frac{(q^j+1)q^{4n-3}}{q^j}=q^{4n-3}+q^{4n-j-3} \quad \cdots\cdots(48)^{(注)}$$

(48)の式は、$S(q^{4n-3})=1+q+^2+q^3\cdots+q^{4n-3}$であることに矛盾する。したがって、$\frac{B}{B-A}$は整数ではない。

(証終)

(註:(48)が成立するのは、n＝1かつj＝1の場合に限るが、n＝1の場合、後述する[命題16]より、Nは奇数の完全数にならない。)

[命題15] $\frac{A}{B-A}$も整数ではない。

(証明) $\frac{A}{B-A}=\frac{B}{B-A}-1$と命題14より、あきらかである。 (証終)

[命題16] 奇数の完全数が存在するならば、$G(x)=0$(ただし、最高次の次数$(4n-2)$)の$x=1$以外の実数解について、

(ⅰ)n＝1の場合、$x=1$以外の実数解は、$x=\frac{A}{B-A}$(命題10より)であるが、この場合、命題15より

$N=p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}q^{4n-3}=p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}q$ 型の奇数の完全数は存在しない。

(ⅱ)n≧2の場合、$x=1$以外の実数解は、$x=q=[\frac{B}{B-A}]$である。

(証明) (ⅰ)について、n＝1の場合は、命題10と命題15よりあきらかである。

(ⅱ)について、$G(x)=0$の$x=1$以外の実数解は、命題13で述べた開区間$(\frac{A}{B-A},\ \frac{B}{B-A})$内にある。この区間の幅は$\frac{B}{B-A}-\frac{A}{B-A}=1$で、命題13,14,15より、$x=1$以外の$G(x)=0$の実数解$x=\gamma$は、Gauss記号を使うと、$x=\gamma=[\frac{B}{B-A}]$となる。この$\gamma$が$q$に等しく、$q\equiv1\pmod 4$を満たす素数でなければならない。 (証終)

[命題17] 奇数の完全数$N=p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}q^{4n-3}$(ただし、$q\equiv1\pmod 4$を満たす素数)が存在すると仮定する。

n≧2のとき、$N=p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}([\frac{B}{B-A}])^{4n-3}$である。

(証明) 命題16の(ⅱ)より、明らかである。 (証終)

[命題18] 奇数の完全数が存在すると仮定すると、次の等式が成り立たねばならない。

$$S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_k^{2m_k})S([\frac{B}{B-A}])^{4n-3}=2p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}([\frac{B}{B-A}])^{4n-3}$$

(証明) 命題17と完全数の定義から、明らかである。 (証終)

[命題19] $G(x)=0$を満たす$x=1$以外の整数解$x=q=[\frac{B}{B-A}]$について、$\frac{q-1}{q}B<A<\frac{q}{q+1}B$である。

(証明) 命題13より、

$\frac{A}{B-A}<q<\frac{B}{B-A}$が成立することから、明らか。 (証終)

[命題20]V章の(32)の式を変形して、$Bx^{4n-3}-AS(x^{4n-3})=0$が得られ、この式の左辺をg(x)で表した。つまり、$g(x)=Bx^{4n-3}-AS(x^{4n-3})=Bx^{4n-3}-A(1+x+x^2+x^3+\cdots\cdots+x^{4n-3})=Bx^{4n-3}-A\dfrac{x^{4n-2}}{x-1}$とおいて、$G(x)=g(x)(x-1)$で表した。代数方程式$g(x)=0$は有理数体$Q$上で、唯一つの整数解$x=q=[\dfrac{B}{B-A}]$をもつから、$\dfrac{g(x)}{x-q}=\dfrac{G(x)}{(x-1)(x-q)}$は$Q$上で既約である。

(証明) 命題13および命題16の(ii)より、$G(1)=0$ かつ$G(q)=0$で、$G(x)=0$は、$x=1$, q以外に有理数解は存在しないから、$\dfrac{g(x)}{x-q}=\dfrac{G(x)}{(x-1)(x-q)}$は、$Q$上で既約である。 (証終)

[命題21] $G(x)=0$を満たす$x=1$以外の実数解$x=q=[\dfrac{B}{B-A}]$について、

$$\frac{B}{B-A}=q+\frac{q-1}{q^{4n-3}-1}$$

が成り立つ。

(証明) 奇数の完全数Nの定義:S(N)=2Nより、

$$AS(q^{4n-3})=Bq^{4n-3} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (49)$$

(註:(12)の式と同じである。)
が成り立つ。

$BS(q^{4n-3})=BS(q^{4n-3})$から、(49)の辺々を引くと、

$$BS(q^{4n-3})-AS(q^{4n-3})=BS(q^{4n-3})-Bq^{4n-3}$$

$$\therefore (B-A)\times\frac{q^{4n-2}-1}{q-1}=B\{S(q^{4n-3})-q^{4n-3}\} \quad (\text{註:}S(q^{4n-3})=\frac{q^{4n-2}-1}{q-1}\text{だから})$$

$$(B-A)\times\frac{q^{4n-2}-1}{q-1}=B\{(1+q+q^2+q^3+\cdots q^{4n-4}+q^{4n-3})-q^{4n-3}\}$$

$$(B-A)\times\frac{q^{4n-2}-1}{q-1}=B\times\frac{q^{4n-3}-1}{q-1}$$

分母をはらって、式を変形すると、

$$\frac{B}{B-A}=q+\frac{q-1}{q^{4n-3}-1}$$

を得る。

(証終)

(別証) $G(x)=(B-A)x^{4n-2}-Bx^{4n-3}+A$だから、$G(q)=0$より、

$$(B-A)q^{4n-2}-Bq^{4n-3}+A=0$$

が成り立つ。この両辺に$S(q^{4n-3})=1+q+q^2+q^3\cdots\cdots+q^{4n-3}=\dfrac{q^{4n-2}-1}{q-1}$を掛けると、

$$(B-A)q^{4n-2}S(q^{4n-3})-Bq^{4n-3}S(q^{4n-3})+AS(q^{4n-3})=0$$

となる。命題6の証明の中の式(12)より、$AS(q^{4n-3})=Bq^{4n-3}$だから、上式に代入して、

$$(B-A)q^{4n-2}S(q^{4n-3})-Bq^{4n-3}S(q^{4n-3})+Bq^{4n-3}=0$$

$$\therefore\ (B-A)q^{4n-2}\frac{q^{4n-2}-1}{q-1}-Bq^{4n-3}\frac{q^{4n-2}-1}{q-1}+Bq^{4n-3}=0$$

両辺をq^{4n-3}で割り、$q-1\neq 0$より、分母を払うと、

$$(B-A)q(q^{4n-2}-1)-B(q^{4n-2}-1)+B(q-1)=0$$

$$(B-A)q(q^{4n-2}-1)-B\{(q^{4n-2}-1)-(q-1)\}=0$$

$$(B-A)q(q^{4n-2}-1)-Bq(q^{4n-3}-1)=0$$

この両辺をqで割って、

$$(B-A)(q^{4n-2}-1)-B(q^{4n-3}-1)=0$$

$$\therefore\ (B-A)(q^{4n-2}-1)=B(q^{4n-3}-1)$$

$$\frac{q^{4n-2}-1}{q^{4n-3}-1}=\frac{B}{B-A}$$

$$\frac{q(q^{4n-3}-1)+q-1}{q^{4n-3}-1}=\frac{B}{B-A}$$

$$q+\frac{q-1}{q^{4n-3}-1}=\frac{B}{B-A}$$

$$\therefore\ \frac{B}{B-A}=q+\frac{q-1}{q^{4n-3}-1}\qquad\cdots\cdots(50)$$

となる[註]。 (証終)

(註:$q=[\frac{B}{B-A}]$を上の等式(50)の右辺に代入して、$\frac{B}{B-A}=[\frac{B}{B-A}]+\frac{q-1}{q^{4n-3}-1}$ ・・・・・(51)
を得る。

命題16の(ⅱ)より、n≥2でなければならないから、$\frac{q-1}{q^{4n-3}-1}\leq\frac{q-1}{q^{5}-1}$である。$q\geq 5$より、

$\frac{q-1}{q^{4n-3}-1}\leq\frac{5-1}{5^5-1}=\frac{4}{3124}=\frac{1}{781}=0.0012804\cdots$となる。つまり、$q=[\frac{B}{B-A}]$と$\frac{B}{B-A}$との差は、$\frac{1}{781}$以下である。)

(註:命題21の結果の等式

$$\frac{B}{B-A}-q=\frac{q-1}{q^{4n-3}-1}$$

が成り立ち、n≥2より、$q^{4n-3}-1>q-1$より、$0<\frac{q-1}{q^{4n-3}-1}<1$となるから、$[\frac{q-1}{q^{4n-3}-1}]=0$である。)

奇数の完全数$N=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}$について、完全数の定義より、

S(N)=2Nが成り立たねばならない。この等式を書き直すと、

$$S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})S(q^{4n-3})=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}$$

となり、$A=S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})$,$B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$とおくと、上の等式は、

$AS(q^{4n-3})=Bq^{4n-3}$となり、[命題7]の結果より、$q^{4n-3}\mid A$であった。この結果から、$A=\boldsymbol{R}q^{4n-3}$となる自然数(Aの約数$\boldsymbol{R}$)があることが解かったが、$\boldsymbol{R}$が1か1でないかのどちらかであった。

ここでまず、$\boldsymbol{R}$の上界について述べる。[命題7]の証明過程の(14)の等式から、$\boldsymbol{R}=B-(B-A)q$であった。[命題16]の(ⅱ)の結果より、$q\equiv 1 \pmod 4$を満たす奇素数qは、$[\frac{B}{B-A}]$であった。

$\frac{B}{B-A}-1\leq[\frac{B}{B-A}]<\frac{B}{B-A} \Rightarrow -(\frac{B}{B-A}-1)\geq -[\frac{B}{B-A}]> -\frac{B}{B-A}$だから、これらの不等式の辺々に(B-A)を掛けてBを加えると、

$B-(B-A)(\frac{B}{B-A}-1)\geq B-(B-A)q>B-(B-A)(\frac{B}{B-A}) \Rightarrow B-A\geq \boldsymbol{R}>0$

$\therefore\ 0<\boldsymbol{R}\leq B-A \Rightarrow 1\leq \boldsymbol{R}$より、$1\leq \boldsymbol{R}\leq B-A$

が得られる。これも命題として、載せることにする。

[命題22] $1\leq \boldsymbol{R}\leq B-A$が成り立つ。

[命題23] $\frac{B}{B-A}-[\frac{B}{B-A}]=\frac{\boldsymbol{R}}{B-A}$が成り立つ。

(証明) [命題7]の証明過程の式(19):$q(B-\boldsymbol{R}q^{4n-3})=B-\boldsymbol{R}$が成り立つ。$A=\boldsymbol{R}q^{4n-3}$だから、(19)に代入すると、命題7より、

$q(B-A)=B-\boldsymbol{R}$

だから、両辺を(B-A)で割ると、度々現れる式:$q=\frac{B-\boldsymbol{R}}{B-A}$が得られる。

この式(註:[**命題** η]の結果の式でもある。)$\Rightarrow\therefore[\frac{B}{B-A}]=\frac{B}{B-A}-\frac{\boldsymbol{R}}{B-A}$

となり、この式を変形すると、$\frac{B}{B-A}-[\frac{B}{B-A}]=\frac{\boldsymbol{R}}{B-A}$が得られる。 (証終)

(註:この式の意味は、$\frac{B}{B-A}$とG(x)=0の1以外の整数解x=qとの誤差は、$\frac{\boldsymbol{R}}{B-A}$となることである。)

[命題24] $\frac{\boldsymbol{R}}{B-A}=\frac{q-1}{q^{4n-3}-1}$ が成り立つ。

(証明) $q=[\frac{B}{B-A}]$だから、命題23と命題21より、明らかである。 (証終)

[命題25] 次の等式(ⅰ),(ⅱ)が成り立つ。

(ⅰ)$B-A=\boldsymbol{R}(1+q+q^2+\cdots+q^{4n-4})$ (ⅱ)$B=\boldsymbol{R}S(q^{4n-3})$ (註:(ⅰ)の結果から得らる。)

(証明) (ⅰ)命題24で示した等式の両辺の逆数を求めると、$\frac{B-A}{\boldsymbol{R}}=\frac{q^{4n-3}-1}{q-1}$となり、この右辺は、$1+q+q^2+\cdots+q^{4n-4}$だから、分母を払って、

$$B-A=\boldsymbol{R}(1+q+q^2+\cdots+q^{4n-4}) \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(52)$$

(ⅱ)命題7より、$A=\boldsymbol{R}q^{4n-3}$だから、これを(52)の左辺に代入すると、

$$B-Rq^{4n-3}=R(1+q+q^2+q^3+\cdots+q^{4n-4}) \quad \cdots\cdots(53)$$

$$\therefore\ B=R(1+q+q^2+\cdots+q^{4n-4}+q^{4n-3})$$

となり、この右辺は、$RS(q^{4n-3})$に等しい。(註:命題7の証明過程の等式が再度現れた。) (証終)

(註:式(52)より、(B-A)の素因数は、Rの素因数か、または、$(1+q+q^2+\cdots+q^{4n-4})$の素因数に限る。)

VI. 奇数の完全数と楕円曲線との関係について

[1] 奇数の完全数と合同数との関係(「奇数の完全数は、合同数になり得ない」こと)

まず初めに、合同数について、その歴史をふりかえる事にする。その後、合同数と楕円曲線との関係を述べる。「奇数の完全数は、合同数になりえない。」という否定文の命題(文脈)であるが、これをきっかけに奇数の完全数と楕円曲線へと思いついたので、レジュメの内容に加えることにする。

1):等差数列をなす3つの平方数と楕円曲線との関連について

13世紀のイタリアの数学者フィボナッチは、「等差数列をなす3つの平方数」について研究している。実は、この問題は楕円曲線を扱っているのである。「数学七つの未解決問題」(森北出版株式会社)の本(著者は、10名)の中で、バーチ&スウィナートン・ダイアーの予想の章で、橋本喜一朗氏が、「等差数列をなす3つの平方数」について言及している。この部分の概略を本の中から抜粋することにする。

Z^2,X^2,Y^2が公差dで等差数列をなすとする。(ただし、$X,Y,Z\in Q$とする。)

$Z^2=X^2-d$, X^2, $Y^2=X^2+d$ と表される。Z^2とY^2を辺々加えると、

$$\therefore Z^2+Y^2=2X^2 \quad \cdots\cdots(54)$$

この両辺をX^2で割ると、

$$\left(\frac{Z}{X}\right)^2+\left(\frac{Y}{X}\right)^2=2 \quad \cdots\cdots(55)$$

$\frac{Z}{X}$および$\frac{Y}{X}$をuを用いたパラメータ表示をすると、

$$\frac{Z}{X}=\frac{u^2+2u-1}{u^2+1},\qquad \frac{Y}{X}=\frac{u^2-2u-1}{u^2+1}$$

となる。これらの式から

$$d\left(\frac{u^2+1}{2X}\right)^2=-u(u^2-1) \quad \cdots\cdots(56)$$

が導かれ、(56)の両辺にd^3を掛けると、

$$d^4\left(\frac{u^2+1}{2X}\right)^2=-du(d^2u^2-d^2) \quad \cdots\cdots(57)$$

ここで、$\frac{d^2(u^2+1)}{2X}=y$, $-du=x$とおくと、(57)の等式は、次の式になる。

$$y^2=x(x^2-d^2) \quad \cdots\cdots(58)$$

この(58)の型の式は、楕円曲線(判別式$\Delta=4d^6\neq0$である。)の方程式である。

2):合同数に関するTunnellの定理について

まず、合同数の定義から述べる。

(定義)合同数とは、3辺の長さが有理数の直角三角形の面積として表される有理数のことをいう。

Mが合同数ならば、直角三角形の3辺をx,y,zとおくと、合同数の定義より、

$$x^2+y^2=z^2,\ \frac{xy}{2}=M \quad (\text{ただし、}x,\ y,z\text{は有理数})$$

で表される。$xy=2M$より、

$$(x-y)^2+4M=z^2,\ (x+y)^2-4M=z^2 \quad \cdots\cdots(59)$$

が成り立つから、$(x-y)^2$, z^2, $(x+y)^2$は、3つの平方数からなる等差数列(公差dは4M)となる。

(59)の各等式を4で割れば、$(\frac{x-y}{2})^2,(\frac{z}{2})^2,(\frac{x+y}{2})^2$は、公差Mの等差数列になる。したがって、1)で述べた楕円曲線と関連がある。

1983年、J.B.Tunnellは、合同数の問題を保型形式の理論に結び付けて、興味深い研究をした。その研究論文は、J.B.Tunnell, "A classical Diophantine problem and modular forms of weight3/2", Invent.Math 72, 323-334(1983)である。

Tunnellの「合同数の条件」についての定理を載せる。

[Tunnellの定理(合同数の条件)]

合同数の定義より、x, y, Mが満たす代数曲線(それは、楕円曲線で表される)について、自然数Mが合同数であるための必要十分条件は、

$$\text{楕円曲線}:y^2=x(x^2-M^2) \quad \cdots\cdots(60)^{\text{註}}$$

が、無限に多くの有理点をもつことである。　　(以上、抜粋の概略終わり)

(註:(54)から(58)までと同様に計算をたどれば、楕円曲線(60)の方程式式が得られる。また、逆に辿れる。)

奇数の完全数と関連させるために、この定理の対偶を載せておく。

[Tunnellの定理の対偶]

自然数Mが合同数ではない必要十分条件は、

楕円曲線:$y^2=x(x^2-M^2)$

が、高々有限個の有理点しかもたないことである。

3) 合同数であることについての同値の命題

(a) Mが合同数であるためには、$E_M(Q)=\{(x,y) \mid x,y\in Q$で、$y^2=x(x^2-M^2)$を満たす。$\}$の階数が0でないことが必要十分である。(註:「楕円曲線と保型型式」(Springer;N. コブリッツ著のp. 63の命題1.18参照)

(b) Aを平方因子をもたない正の整数とし、Eは楕円曲線:$y^2=x(x^2-A^2)$とする。方程式

$$x^2+Ay^2=z^2$$
$$x^2-Ay^2=t^2$$

が自明でない解($y\neq 0$)を有理数体Qでもつのは、Eの階数$r_Q(E)>0$のとき、そのときに限る。

(註:「数論入門講義-数と楕円曲線-」(共立出版;J.F.Chahal著のp.184の「定理7.24」参照)

(c) dを正の有理数とするとき、次の条件(ⅰ)-(ⅲ)は同値である。

(ⅰ)3辺の長さが有理数で面積がdの直角三角形が存在する。

(ⅱ)有理数の平方となる3つの数で、公差dの直角三角形が存在する。

(ⅲ)楕円曲線$y^2=x(x^2-d^2)$の有理数解が、$(x,y)=(0,0),(\pm d,0)$の他にも存在する。

(註:「数論1(岩波講座　現代数学の基礎)Fermatの夢」(加藤和也・黒川信重・斎藤毅著)のp.20の補題1.3参照)

(ⅰ)⇔(ⅱ)⇔(ⅲ)より、それらの対偶命題が成り立つが、あらためて書き表さないことにする。

以上の命題を使って、奇数の完全数について、合同数との関係を述べることにする。

[命題26] 奇数の完全数が存在すると仮定すると、それは合同数ではない。

(証明) この命題の証明は、いくつか考えられるので、証明に番号をふることにする。

(証明1) Nを奇数の完全数とする。命題5の(ⅰ)より、

$N=p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}q^{4n-3}$ (ただし、qは、$q\equiv 1 \pmod 4$を満たす素数)

の型で表される。奇数の完全数の定義により、

$$S(N)=2N \qquad \cdots\cdots(61)$$

が成り立たねばならない。この等式の両辺を2で割ると、

$$N=\frac{S(N)}{2} \Leftrightarrow S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_k^{2m_k})\left\{\frac{S(q^{4n-3})}{2}\right\}=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3} \qquad \cdots\cdots(62)$$

$S(N)=S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_k^{2m_k})S(q^{4n-3})$を素因数分解した場合、(62)の右辺の式の2倍にな

るが、それを2個の有理数X，Yに分けて、$2N=S(N)=XY$と表すことにする。したがって、$N=\frac{XY}{2}$と表したことになる。(註：すぐ下で、ふれるようにX,Yは整数としても一般性を失わない。)

奇数の完全数Nを合同数だと仮定してみよう。$X^2+Y^2=Z^2$かつ$N=\frac{XY}{2}$を満たす有理数がX,Y,Zが存在し、適当な有理数sを選んでs^2Nを平方因子を含まない整数にすることができる。

その理由は、3辺sX,sY,sZをもつ三角形の面積は、$\frac{sX\cdot sY}{2}=s^2N$(整数)となるから、一般性を失わないで合同数を平方因子をもたない自然数としてよい。つまり、その逆に、整数の範囲で合同数を考察して、その後、$Q^+/(Q^+)^2$に戻して考えてもよい。奇数の完全数Nは平方因子をもつが、このままの形で整数の範囲で、これから考えることにする。Yは2を因数に含む自然数(ただし、XとYは互いに素として選ぶ。)としても、一般性を失わない。つまり、直角三角形をs倍に拡大または縮小して、各辺を自然数となる相似形で考える。S(N)は、2の因数を1個のみ含み、残りの因数はすべて奇素数である。(註：$S(q^{4n-3})$が偶数である。)
奇数の完全数が合同数であると仮定したから、

$$N=\frac{XY}{2}=X(\frac{Y}{2}) \quad \cdots\cdots(63)$$

と表される。

つまり、ある整数Zが存在して3つの平方数X^2，Y^2，Z^2が等差数列をなし、さらに$X^2+Y^2=Z^2$が成り立ち、X,Y,Zは互いに素であると仮定する。(実際に、2つの整数XとYは互いに素として選んである。)
(X，Y，Z)はピタゴラス数より、ある適当な自然数m，nをパラメータとして用いると、
$X=m^2-n^2$,$Y=2mn$ (Yは偶数より)，$Z=m^2+n^2$で表される。Xは奇数、Yは偶数より、

$$N=X(\frac{Y}{2})=(m^2-n^2)mn \quad \cdots\cdots(64)$$

となり、この左辺Nは奇素数の積$p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}q^{4n-3}$だから、右辺と比較すると、Xおよび$\frac{Y}{2}$は、ともに奇数である。したがって、$\frac{Y}{2}=mn$より、$m$と$n$は、両方とも奇数である。

ところで、ピタゴラス数(X，Y，Z)において、mとnのうち、両方とも奇数、あるいは、偶数になることはない。

なぜならば、mとnがともに奇数の場合、$X=m^2+n^2$および$Z=m^2-n^2$はともに偶数となる。だから、Zが偶数になり、Yはもともと偶数としたから、X,Y,Zは公約数として2があることになる。このことは、X,Y,Zは互いに素であるという仮定に矛盾する。

したがって、Nは合同数ではない。　　(証終)

(証明2) 証明1の途中で、mとnが両方とも奇数だから、Nが合同数と仮定すると,$X=m^2-n^2$が偶数であることが導かれるが、このことは、S(N)＝2N＝XYとして、Xは奇数(Yは偶数に選んである)であったことから、矛盾する。　(証終)

(証明3) 証明1の途中の式(64)において、$N=(m^2-n^2)mn=(m+n)(m-n)mn$より、Nは奇数の完全数だから、最右辺の因数$(m+n)$,$(m-n)$, m,nはすべて奇数でなければならない。したがって、この場合、m,nは両方とも奇数だから、Nの因数$(m+n)$,および$(m-n)$がともに偶数になり、$(m+n)$,$(m-n)$が奇数でなければならないことに矛盾する。　(証終)

[Lemma Ⅱ] Nを奇数の完全数とすると、非特異楕円曲線:$y^2=x(x^2-N^2)$のrankは0である。

(証明)命題26より、Nは合同数ではない。Tunnellの定理の対偶より、この楕円曲線の有理点は有限個である。したがって、有理点の群はTorsion Groupだけとなるから、楕円曲線:$y^2=x(x^2-N^2)$のrankは0である。　(証終)

[2] 奇数の完全数と楕円曲線との関連についての試み

これから論じる[2]以降の内容は、奇数の完全数の諸命題を楕円曲線へと関連させる試みである。S.Langが「楕円曲線については、いくらでも論文が書ける。」と言われた。この言葉をふまえると、私は楕円曲線を学び・研究する上で、いつもスタート地点に立たされていて、心もとない感がある。

したがって、これから述べることは、奇数の完全数を楕円曲線に関連させる途中の段階で留めて、次回の機会に奇数の完全数を楕円曲線へと関連付ける一つのアプローチから、どのような命題が引き出されるのという問題提起したいと思います。

このアプローチの方法が、Frey曲線(楕円曲線)⇒Ribetの定理⇒Wilesによる「半安定な楕円曲線による谷山－志村予想の解決」(Fermatの最終定理」を肯定的に解決)のように辿るかどうか、私にとって未知の段階です。さらに、これから幾つかの構成する楕円曲線の中に、半安定ではない楕円曲線が含まれます。まず、楕円曲線を幾つか構成するところから始めます。

この節以降では、合同数と異なる視点から奇数の完全数と楕円曲線との関連を考えることにする。奇数の完全数が存在すると仮定すると、Ⅴ章の(38)の$y=G(x)$の式において、$G(x)=0$を満たす$x=1$以外の実数解は、$x=q=[\frac{B}{B-A}]$であることを示した。つまり、

$$G(q)=(B-A)q^{4n-2}-Bq^{4n-3}+A=0 \quad (\text{ただし、}n\geq 2) \quad \cdots\cdots\cdots\cdots\cdots\cdots(65)$$

(ただし、$A=S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})=(1+p_1+p_1^2\cdots p_1^{2m_1})(1+p_2+p_2^2+\cdots+p_2^{2m_2})\cdots(1+p_k+p_k^2+\cdots+p^{2m_k})$,

$B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$)　$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(66)$ となる。)

(65)より、

$$(B-A)q^{4n-2}+A=Bq^{4n-3} \quad \cdots\cdots (67)$$

が成り立たねばならない。(67)の左辺の各項を使って、次の新たな楕円曲線

$$\boldsymbol{E}_1 : y^2=x(x-A)\{x+(B-A)q^{4n-2}\} \quad \cdots\cdots (68)$$

をつくると、この楕円曲線$\boldsymbol{E}_1$について、どのような事柄が成り立つであろうか？

この楕円曲線の判別式$\Delta(\boldsymbol{E}_1)$はminimalとは限らないが、(68)より判別式は、

$$\Delta(\boldsymbol{E}_1)=A^2\{(B-A)q^{4n-2}\}^2\{(B-A)q^{4n-2}+A\}^2$$

$$=A^2(B-A)^2q^{8n-4}(Bq^{4n-3})^2 \quad (\text{註:(67)より})$$

$$=\{AB(B-A)\}^2q^{16n-10} \quad \cdots\cdots (69)$$

$$=\{S(p_1^{2m_1})\cdots S(p_k^{2m_k})2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}(2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}-S(p_1^{2m_1})\cdots S(p_k^{2m_k}))\}^2q^{16n-10} \quad \cdots\cdots (70)$$

となる。判別式$\Delta(\boldsymbol{E}_1)\neq 0$であるから、楕円曲線$\boldsymbol{E}_1$は非特異楕円曲線であり、その種数$g$は1である。種数1の楕円曲線については、有理点が無限個あるのか、あるいは有限個あるのかを判定する命題は、重要な問題の一つである。

[命題27] (68)の楕円曲線$\boldsymbol{E}_1$は、mod$q$で3重解をもつ。(つまり、良い還元をもたず、かつ半安定でない。つまり、mod qで、additive reductionをもつ。)

(証明) 命題6の証明過程で現れる奇数の完全数となる条件の等式(12)は、以下の通り。

$$AS(q^{4n-3})=Bq^{4n-3} \Leftrightarrow (B-A)q^{4n-2}+A=Bq^{4n-3}$$

(ただし、$S(q^{4n-3})=\dfrac{q^{4n-2}-1}{q-1}$だから。)

(68)の楕円曲線$\boldsymbol{E}_1$の方程式について考える。(70)より、$q \mid \Delta(\boldsymbol{E}_1)$であり、さらに[命題7]より、

$$q^{4n-3} \mid A \quad \cdots\cdots (71)$$

である。また、$q \mid (B-A)q^{4n-2}$が成り立つ。したがって、楕円曲線$\boldsymbol{E}_1$は、mod qで還元すると、

$$y^2=x(x-A)\{x+(B-A)q^{4n-2}\} \Rightarrow y^2=x^3 (\text{mod } q) \quad \cdots\cdots (72)$$

となり、(72)の最後の合同式はmod qで3重根をもつ。 (証終)

ところで、奇数の完全数が存在するための条件式(12):$AS(q^{4n-3})=Bq^{4n-3}$に$A=Rq^{4n-3}$(命題7より)を代入して、

$$Rq^{4n-3}\frac{q^{4n-2}-1}{q-1}=Bq^{4n-3} \Leftrightarrow Rq^{4n-3}(q^{4n-2}-1)=Bq^{4n-3}(q-1)$$

の両辺をq^{4n-3}で割ってまとめると、等式

$$Rq^{4n-2}-Bq+(B-R)=0 \Rightarrow Rq^{4n-2}+(B-R)=Bq \quad \cdots\cdots (73)$$

が得られる。ここでは、Rが1でない場合か、または、$R=1$場合の分類分けに拘泥せず、$R=1$、ま

たは、$R\neq 1$、あるいはRの値のまま、等式(73)の左辺の各項を使って、次のような楕円曲線

$$E_2: y^2 = x(x - Rq^{4n-2})\{x + (B-R)\} \quad \cdots\cdots(74)$$

を構成する。

(74)より、E_2の判別式$\Delta(E_2)$は、

$$\Delta(E_2) = (Rq^{4n-2})^2(B-R)^2\{Rq^{4n-2}+(B-R)\}^2 = R^2(q^{4n-2})^2(B-R)^2(Bq)^2 = R^2B^2(B-R)^2q^{8n-2} \neq 0$$

となる。

(註:このE_2に関して、$R=1$ or $R\neq 1$にかかわらず、$q \mid (B-R)$なので、判別式を割り切る素数qによる還元では、additive reductionである。)

楕円曲線(74)において、$R=1$の場合、楕円曲線(74)に$R=1$を代入すると、楕円曲線

$$E^*: y^2 = x(x - q^{4n-2})\{x + (B-1)\} \quad \cdots\cdots(75)$$

を得る。判別式$\Delta(E^*) = B^2(B-1)^2q^{8n-2}$である。まず、楕円曲線$E_1$の有理点について述べる。

[命題28] 楕円曲線E_1の有理点は、y座標が0の点に限る。つまり、有理点からなる群は、$\{\infty,(0,0),(A,0),((B-A)q^{4n-2},0)\}$である。(註:$\infty$を$O$で表すこともある。)

(証明) 証明は背理法による。

もし仮に楕円曲線E_1上に有理点のy座標が0でない点P(a,b)が存在したと仮定する。

したがって、$a\neq 0$かつ$b\neq 0$である。点P(a,b)と(0,0)を通る直線の方程式は、

$$y = \frac{b}{a}x \quad \cdots\cdots(76)$$

である。傾き$\frac{b}{a} \in Q$となる。(76)を(68)の式に代入すると、代数方程式

$$(\frac{b}{a}x)^2 = x(x-A)\{x + (B-A)q^{4n-2}\} \quad \cdots\cdots(77)$$

を得る。この式を変形して、

$$x^3 + \{(B-A)q^{4n-2} - A - (\frac{b}{a})^2\}x^2 - A(B-A)q^{4n-2}x = 0 \quad \cdots\cdots(78)$$

$$\therefore\ x[x^2 + \{(B-A)q^{4n-2} - A - (\frac{b}{a})^2\}x - A(B-A)q^{4n-2}] = 0 \quad \cdots(79)$$

したがって、(79)の解は、$x=0$と2次方程式

$$x^2 + \{(B-A)q^{4n-2} - A - (\frac{b}{a})^2\}x - A(B-A)q^{4n-2} = 0 \cdots\cdots(80)$$

の2個の解である。(80)の判別式をD_1とおき、$(\frac{b}{a})^2 = \omega$おくと、

$$D_1 = \{(B-A)q^{4n-2} - A - \omega\}^2 + 4A(B-A)q^{4n-2} \quad \cdots\cdots(81)$$

$$= \omega^2 - 2\{(B-A)q^{4n-2} - A\}\omega + \{(B-A)q^{4n-2} - A\}^2 + 4A(B-A)q^{4n-2}$$

$$= \omega^2 - 2\{(B-A)q^{4n-2} - A\}\omega + \{(B-A)q^{4n-2} + A\}^2 \quad \cdots\cdots(82)$$

となり、(81)より、$D_1>0$となる。(註:つまり、相異なる実数解となる。)

(80)の2つの実数解は、

$$x=\frac{-\{(B-A)q^{4n-2}-A-\omega\}\mp\sqrt{D_1}}{2} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(83)$$

である。(83)の分母は2で、分子の始めの項:$-\{(B-A)q^{4n-2}-A-\omega\}$は有理数だから、この2つの実数解が有理数であるためには、$D_1\in\boldsymbol{Q}$ではあるが、D_1が平方数の型でなければならない。(82)はωの2次式だから、ωについて完全平方式になるためには、ωについて(82)の判別式$\overline{D_1}=0$でなければならない。

$$\overline{D_1}=4\{(B-A)q^{4n-2}-A\}^2-4\{(B-A)q^{4n-2}+A\}^2=-16A(B-A)q^{4n-2}=0 \quad \cdots\cdots\cdots(84)$$

(84)において、命題6より、$B-A>0$だから、$-16A(B-A)q^{4n-2}<0$となり、矛盾である。

したがって、$\omega=(\frac{b}{a})^2$は有理数ではない。つまり、点P(a,b)は有理点ではあり得ない。楕円曲線$\boldsymbol{E}_1$上には、有理点がなす群は$\{\infty,(0,0),(A,0),((B-A)q^{4n-2},0)\}$のみである。 (証終)

(註:楕円曲線$\boldsymbol{E}_2$および$\boldsymbol{R}=1$の場合の楕円曲線$\boldsymbol{E}^*$も同様に、y座標が0でない有理点は存在しないことが、上と同様な計算で確かめられる。したがって、Nagell-Lutzの定理のy座標が0でないことがらについての検証は、応用できないであろう。このことは、Torsion Groupを計算するのではなく、楕円曲線$\boldsymbol{E}_1$, $\boldsymbol{E}_2$、$\boldsymbol{E}^*$については、L-function,L-series,modular elliptic curve,modular form, modular representation,Galois表現,Ribetの定理、・・・・・の方に視点を移した方が良いと考える。)

[3] 奇数の完全数Nに関する楕円曲線の型([2]の$\boldsymbol{E}_1$,$\boldsymbol{E}_2$と異なる)について

奇数の完全数について、**Ⅲ**章の①の中で、Stuyavaertが1896年、「奇数の完全数は2個の平方数の和でなければならないこと。」に言及した。このことは、命題5の(ⅱ)より、「Nの素因数の一つqが$q\equiv1\pmod 4$が成り立つ」ことと、下で述べる「**2平方和定理**」を使って、Nが2つの自然数の平方和になることが示される。つまり、「**2平方和定理**」の2条件((a)か、または、(b)において、奇数の完全数Nについて、条件(a)を満たされているので、適当な自然数2個を選んで、Nをそれらの平方和に表される。「**2平方和定理**」を書き表すと、

「2平方和定理」

mを自然数とする。

(a) mを、$m=p_1p_2\cdots p_rM^2$と相異なる素数$p_1,p_2,\cdots,p_r$の積とM^2(ただし、Mは自然数)に分解する。このとき、mが2つの平方数の和で表せるのは、各p_i $(i=1,2,3,\cdots,r)$は2であるか、または、$p_i\equiv1\pmod 4$のときである。

(b) 自然数mが2つの平方数の和$m=a^2+b^2$かつ$\gcd(a,b)=1$に表せる必要十分条件は、以下の2条件のうちの一つが満たされることである。

（ｉ）mは奇数かつmの各素因数はすべて4を法として1に合同である。

（ⅱ）mは偶数で$\frac{m}{2}$が奇数であり、$\frac{m}{2}$の各素因数はすべて4を法として1に合同である。

（以上の定理は、シルヴァーマン著「はじめての数論」(p. 175)からの抜粋による。）

奇数の完全数Nについて、命題5より、

$N=p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}=q^{4n-3}(p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k})^2=q^{4n-3}(M_1)^2$ （ただし、$M_1=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$） ・・・(85)

$=q(p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}q^{2n-2})^2=q(M_2)^2$ （ただし、$M_2=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}q^{2n-2}$） ・・・・・・・・・・・・・・・・・(86)

と表される。

(註：$N=q^{4n-3-2w}(p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}q^{w})^2=q^{4n-3-2j}M_w^2$ (ただし、$1\leq{}^{\forall}w\leq 2n-2$, $M_w=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}q^{w}$)とおくと、「2平方和定理」の条件(a)を満たすので、(ｉ)より、$N=a_w^2+b_w^2$ （ただし、$1\leq{}^{\forall}w\leq 2n-2$）の表し方がある。したがって、これらの$a_w$と$b_w$を使って、楕円曲線：$y^2=x(x-a_w^2)(x-b_w^2)$が構成される。$a_w$と$b_w$は互いに素ではないので、これらの楕円曲線を$q$で還元すると、additive reductionとなる。上記の等式(85), (86)は、これらの楕円曲線の中に含まれている。)

ここで、(85)および(86)について、「**2平方和定理**」の条件(a)にMに該当する因数は、それぞれM_1およびM_2で、かつ、qは$q\equiv 1 \pmod 4$の素数であるから、条件(a)を満たしている。nは命題16の（ⅱ）より、$n\geq 2$を満たす自然数である。

ここで、(85)の式を使うと、「**2平方和定理**」より、適当な自然数a_1, b_1が存在して、

$N=q^{4n-3}M_1^2=a_1^2+b_1^2$ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・(87)

と表される。（ただし、a_1とb_1は、互いに素ではない。）(註)

（註：奇数の完全数Nを(87)のように、2平方和に表す仕方の個数については、命題29,30及び例の中で述べることにする。）

ここで、(87)の式について、a_1とb_1は互いに素ではないということを説明する。その理由は、

$N=q^{4n-3}M_1^2$

と置いたことによります。素数qは$q\equiv 1 \pmod 4$であるから、$q^{4n-3}\equiv 1 \pmod 4$となり、適当な自然数r_1とs_1があって、$q^{4n-3}=r_1^2+s_1^2$という型に表される。したがって、

$N=(r_1^2+s_1^2)M_1^2=r_1^2M_1^2+s_1^2M_1^2=(r_1M_1)^2+(s_1M_1)^2$ ・・・・・・・・・・・・・・・・・・・・・・・・(88)

となるから、$a_1=r_1M_1, b_1=s_1M_1$となり、a_1とb_1は1以外に公約数M_1があるからです。a_1, b_1を用いて

楕円曲線E_3：$y^2=x(x-a_1^2)(x+b_1^2)$ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・(89)

を構成する。

また、(85)の辺々をM_1^2で割ると、$\frac{N}{M_1^2}=q^{4n-3}=r_1^2+s_1^2$（この表し方の個数については、命題29,30の解説の例の中で述べることにする）となり、r_1とs_1は互いに素となるから、これら構成される楕円曲線

$$E_4: y^2=x(x-r_1^2)(x+s_1^2) \quad \cdots\cdots(90)$$

は、非特異半安定な楕円曲線になる。

また、(86)の両辺をM_2^2で割ると、

$$\frac{N}{M_2^2}=q=a_2^2+b_2^2 \text{（ただし、}a_2\text{と}b_2\text{は互いに素である。）} \quad \cdots\cdots(91)$$

と表せる。(91)の最右辺の表し方は、自然数の範囲では1通りで、a_2が奇数ならばb_2は偶数であり、a_2が偶数ならばb_2は奇数である。(91)を満たすa_2,b_2を用いて、楕円曲線E_5

$$E_5: y^2=x(x-a_2^2)(x+b_2^2) \quad \cdots\cdots(92)$$

を構成する。E_5は、a_2とb_2は互いに素であるから、種数1の半安定な非特異楕円曲線である。

[命題29](註) 奇数の完全数 $N=p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}q^{4n-3}$について、

$N=u_i^2+v_i^2$ （ただし、u_i,v_iは自然数の範囲ではなく、整数の範囲で選ぶ。）

と表す仕方の個数を$r_2(N)$とおくことにする。

$$\Rightarrow r_2(N)=4\sum_{d|N}\chi(d)\text{である。(ただし、}\chi(d)=\begin{cases}1 & d\equiv 1(\mathrm{mod}\ 4)\\ -1 & d\equiv 3(\mathrm{mod}\ 4)\\ 0 & d\text{が偶数のとき}\end{cases}$$

（註：この[命題29]は、Gaussによって証明済みである。）

（証明の概略）数学史上では、Fermatがディオファントスの本の余白に「Fermat予想」をはじめとする48のコメントを書いた中の一つに、$p\equiv 1(\mathrm{mod}\ 4)$の素数pは、$p=x^2+y^2$(x, yは整数)と表され、$p\equiv 3(\mathrm{mod}\ 4)$の素数は、2平方数の和で表せない事がコメントされていた。さらに、Fermatは、一般に自然数n(ただし、$n\geq 2$)に対して、$n=x^2+y^2$と表し方の個数を与えていますが、その証明は、ガウスによって1800年ごろに、2平方和に表される仕方の個数は、$r_2(n)=4\sum_{d|n}\chi(d)$の証明が与えられた。奇数の完全数Nは、「2平方和定理」の条件(a)を満たすので、整数の範囲で考えると、$r_2(N)(\neq 0)$個であることがわかる。このGaussによる証明は、

「$n=x_1^2+x_2^2+\cdots+x_k^2$ の表し方の個数$r_k(n)$について、kが偶数のとき、q 展開の

$q=e^{2\pi i}$(註:q は今まで使用してきた素数q($q\equiv 1 \pmod 4$ではない。)を用いて、

$\sum_{n=0}^{\infty} r_k(n)q^n$ $(=\sum q^{x_1^2+x_2^2+\cdots+x_k^2})$として、ここに和は、すべてk個の整数の組

$(x_1,x_2,\cdots,x_k)$についてのもの)が上半平面上の重み$\frac{k}{2}$の保型形式になる。」

という命題を用いて証明することができる。

(参考資料:「解決!フェルマーの最終定理」(日本評論社:加藤和也著(p.212〜p214参照),

「フェルマーの大定理(第2版)」(日本評論社:足立恒雄著(p.53〜p.54参照))

[命題30] 奇数の完全数をNする。2Nも「2平方和定理」の条件(a)を満たすから、

$r_2(2N)\neq 0$になる。

(証明略)(註) (註:命題29は、公式「$(U^2+V^2)(S^2+T^2)=(US+VT)^2+(VS-UT)^2$ の応用による。つまり、奇数の完全数Nについて、$N=a_1^2+b_1^2$ と表されるから、

$$2N=(1^2+1^2)(a_1^2+b_1^2)=(1a_1+1b_1)^2+(1a_1-1b_1)^2$$

のように、2つの整数の平方和で表されるからである。(ただし、(87)より、a_1とb_1は互いに素ではない。)

命題29,30より、$r_2(N)\neq 0, r_2(2N)\neq 0$から、Nおよび2Nは、整数の範囲でそれぞれ$r_2(N)$個及び$r_2(2N)$個の平方和に表される。Nについての平方和が、$N=a_i^2+b_i^2$(ただし、$a_i, b_i\neq 0$)と表された場合、これらの各項を使って、これから楕円曲線:$y^2=x(x-a_i^2)(x+b_i^2)$を構成するとしよう。a_iとb_iを置き換えることも考慮すると、整数の範囲で$N=a_i^2+b_i^2$を満たす(a_i,b_i)の組は、$(\mp a_i,\mp b_i)$, $(\mp b_i,\mp a_i)$の8個つづつ同じ表し方になり、それらから構成される楕円曲線は、まったく同じ(同値な)楕円曲線になる。奇数の完全数Nについて、(a_i,b_i)の組から構成できる異なる楕円曲線の個数について考察する。まず初めに、奇数の完全数にとらわれずに、一般の自然数n(n≥2)について、$n=t^2+s^2$(ただし、t, sは整数で、t≤sとする。つまり、tとsを置き換えても同一の表し方とみなす。)の表し方の個数を考える。まず、幾つかの例題で検証してみる。

例. ＊n=5のとき、$5=(\mp 1)^2+(\mp 2)^2=(\mp 2)^2+(\mp 1)^2$と表され、$(\mp 1,\mp 2),(\mp 2,\mp 1)$の8個の表し方がある。

Gaussが証明した命題を使うと、

$$r_2(5)=4\sum_{d\mid 5}\chi(d)=4(\chi(1)+\chi(5))=4(1+1)=8$$

で、初めの計算結果と一致する。

＊$n=5^2=25$の場合、$n=(\mp 3)^2+(\mp 4)^2=(\mp 4)^2+(\mp 3)^2=0^2+(\mp 5)^2=(\mp 5)^2+0^2$と表され、表し方は全部で12個ある。Gaussの計算方法を使うと、$r_2(5^2)=4(\chi(1)+\chi(5)+\chi(25))=4(1+1+1)=12$で、上の計算結果と一致する。しかし、$(t,s)=(0,\mp 5),(\mp 5,0)$から構成されるそれぞれの楕円曲線というよりは特異な代数曲線(重解型であるから)で(註:判別式が0となる$y^2=$(xの3次式)は楕円曲線の仲間ではな

い。)、

$$y^2=x(x-0^2)\{x+(\mp5)^2\}=x^2\{x+(\mp5)^2\}$$

$$y^2=x\{x-(\mp5)^2\}(x+0^2)=x^2\{x-(\mp5)^2\}$$

となり、それぞれの右辺の判別式が0となるから、非特異楕円曲線ではない。$n=t^2+s^2$の表し方のうち、tかsが0の場合を省くことにすると、12個から4個を差し引いて、8個となり、符号の違いとsとtを置き換えて交換した表し方を同一視すれば、$8\div8=1$で、1通りの楕円曲線

$y^2=x(x-3^2)(x+4^2)$ が得られたことになる。

＊$n=5^3$の場合、5のべき指数は奇数より、$n=5^2$の場合のようなt,sのうちの一方が0となることは起らない。$r_2(5^3)=4\{\chi(1)+\chi(5)+\chi(5^2)+\chi(5^3)\}=16$であるが、

$$5^3=125=(\mp2)^2+(\mp11)^2=(\mp11)^2+(\mp2)^2=(\mp5)^2+(\mp10)^2=(\mp10)^2+(\mp5)^2$$

となり、16通りの表し方がある。自然数の範囲で、tとsの置き換えを同一視すれば、(t,s)=(1,11)と(5,10)の 2通りであるが、$r_2(5^3)\div8=16\div8=2$で、一致する。

したがって、楕円曲線

$$y^2=x(x-2^2)(x+11^2)$$

$$y^2=x(x-5^2)(x+10^2)$$

が得られたことになる。

一般に、$q\equiv1\pmod4$の素数qの指数が奇数$(2k-1)$ならば、q^{2k-1}を2つの平方の和$(q^{2k-1}=t^2+s^2)$に表す仕方の個数は、$t\neq s$ (なぜならば、$t=s$と仮定すると、$q^{2k-1}=2t^2$となり、左辺は奇数で右辺は偶数という矛盾が起る。)なので、自然数の範囲でかつ$t<s$の条件下で、その表し方は、

$$\frac{r_2(q^{2k-1})}{8}=\frac{\sum_{d\mid q^{2n-1}}^{4}\chi(d)}{8}=\frac{4(\chi(1)+\chi(q)+\chi(q^2)+\cdots\chi(q^{2k-1}))}{8}=\frac{4\times(2k)}{8}=k\text{通りである。}$$

奇数の完全数$N=p_1^{2m_1}p_2^{2m_2}\cdots\cdots p_k^{2m_k}q^{4n-3}=q^{4n-3}M_1^2$(ただし、$M_1=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$,$q$は$q\equiv1\pmod4$の素数)より、Nの因数$q^{4n-3}$について、自然数の範囲で、かつ$t<s$の条件下で考えると、2平方和の表し方の個数は$\frac{r_2(q^{4n-3})}{8}=(2n-1)$個になる。したがって、$q^{4n-3}$を一つの2平方和に表わす仕方を$q^{4n-3}=t_h^2+s_h^2$とすると、$N=M_1^2q^{4n-3}=M_1^2(t_h^2+s_h^2)=(M_1t_h)^2+(M_1s_h)^2$という平方和であらわされるが、これから楕円曲線$E_{h,N}:y^2=x(x-a_h^2)(x+b_h^2)$ (ただし、$1\leq h\leq\frac{r_2(q^{4n-3})}{8}$,$a_h=M_1t_h$,$b_h=M_1s_h$である。)が構成される。

また、$2N=c_j^2+d_j^2$ (ただし、$1\leq j\leq\frac{r_2(q^{4n-3})}{8}$)から、楕円曲線 $E_{j,2N}:y^2=x(x-c_j^2)(x+d_j)$

(ただし、$1\leq j\leq\frac{r_2(q^{4n-3})}{8}$) が構成される。これらのすべての楕円曲線について、各a_hとb_h および

各c_jとd_jは、共通な因数をもつので、楕円曲線$E_{h,N}$および$E_{j,2N}$は半安定な楕円曲線ではない。

[**命題31**] 奇数の完全数Nが存在すると仮定すると、Nは連続した自然数の積を2個使って、それぞれの2倍の和に1を加えた整数である。

(**証明**)Nを奇数の完全数とすると、$2N=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}=2q^{4n-3}(p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k})^2$だから、「2平方和定理」の(a)の条件を満たしている。したがって、適当な自然数c,dを選んで、

$$2N=c^2+d^2 \quad \cdots\cdots(93)$$

と表される。

(93)の左辺は偶数より、右辺についてc^2とd^2が共に偶数の場合と共に奇数の場合に分けて考える。

(ア)cが偶数$2u$,dが偶数$2v$の場合(ただし、u,vはある適当な整数)

c^2とd^2は4の倍数だから、(93)の両辺を2で割ると

$$N=\frac{c^2}{2}+\frac{d^2}{2}=\frac{(2u)^2}{2}+\frac{(2v)^2}{2}=2u^2+2v^2 \quad \cdots\cdots(94)$$

(94)の右辺は偶数になり、左辺のNは奇数の完全数だから、矛盾が起る。

(イ)cが奇数$2u+1$で、かつdも奇数$2v+1$の場合(ただし、u,vはある適当な自然数)

$2N=(2u+1)^2+(2v+1)^2=4u^2+4v^2+4u+4v+2$ だから、両辺を2で割ると、

$$N=2u^2+2v^2+2u+2v+1$$
$$=2u(u+1)+2v(v+1)+1 \quad \cdots\cdots(95)$$

(95)の右辺の第1項の因数u(u+1)と第2項のv(v+1)は、それぞれ連続した自然数の積だから、両方とも偶数となり、2u(u+1)および2v(v+1)は4の倍数となるから、Nは4を法として1と合同であることがわかる。つまり、[命題5]の(ⅱ)の別証明が得られたことになる。

(註:この場合、(ア)のような矛盾は起きない。) つまり、奇数の完全数の存在を仮定すると、(イ)の(95)の式が成り立たねばならない。したがって、[命題31]が成立する。 (証終)

(95)の等式から、右辺の各項を使って、次のような楕円曲線E_6

$$E_6: y^2=x\{x-2u(u+1)\}\{x+2v(v+1)+1\} \quad \cdots\cdots(96)$$

を構成する。E_6の判別式$\Delta(E_6)=\{2u(u+1)\}^2\{2v(v+1)+1\}^2N^2\neq 0$だから、非特異楕円曲線である。

奇数の完全数$N=(p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k})^2q^{4n-3}$に対して、上で述べた楕円曲線$E_1,E_2,E_3,E_4,E_5,E_6$,および

$E_{h,N}$(ただし、$1 \leq h \leq \frac{r_2(q^{4n-3})}{8}$)、$E_{j,2N}$(ただし、$1 \leq j \leq \frac{r_2(q^{4n-3})}{8}$)について、楕円曲線の理論を使ってどのような事柄が成り立つであろうか？

Ⅶ. 構成した楕円曲線の夢(研究課題を含めて)を語る。

数学で「夢」を語るという最たる事例は、「クロネッカーの青春の夢」であろう。その後、この夢は、ヒルベルト、そして、高木貞治へと引き継がれて、大きな実り(類体論)として実現した。最近では、数十年前に、久賀道郎さんの「ガロアの夢」が出版され、読んだことがある。この本の最後の章は、確しか、ある流行歌の題名をもじって、"さよならは、ハッタリの後で！"だったと思うが、ガロアの理論をモノドロミー群を使って、微分方程式が与えられた関数の族の中で解けるのか解けないのか・・・という証明抜きの夢を語ったのだと思う。その後、「ガロアの夢」は、グロタンディックから影響を受けた人達によって、線型微分方程式方面で実を結んだと思う。この私も、奇数の完全数の夢を語ろうと思う。夢であるから、証明は脇に置いて、思いついた発想を中心に語る。

谷山－志村予想が完全に(つまり、楕円曲線が半安定or半安定ではないことにかかわらず、Breuil, Conrad,Diamond,Taylor,Wilesによる証明)肯定的に解決された現在、上述したこれらの楕円曲線がモジュラーかどうか検証することが、その重要な課題となることであろう。まず、最初に着手しなければならないことは、それぞれの導手(Conductor)を、計算して求める必要がある。しかし、その前に、Euler以後に見つけられた「奇数の完全数についての諸命題」と構成した楕円曲線が整合するのか、あるいは、異常な振る舞いが観られるのか・・・ということを検証しておく必要がある。

(ア) Torsion Groupについて

数学史上、4次のFermat予想は、無限降下法で解かれた。3次のFermat予想はEulerによって解決した。その後、3次のFermat予想は有理関数で変数変換して、楕円曲線:$y^2=x^3-432$へと変換され、また、4次のFermat予想は、同様に有理関数で、楕円曲線:$y^2=x^3-4x$に変換され、それぞれのTorsion Groupが限られたものしか存在しないことを示して、解決した事例がある。これらの楕円曲線のTorsion Groupの有理点(x,y)は、いずれも$y \neq 0$を満たす点であった。

楕円曲線E_1やE_2の各Torsion Groupの各点は、[命題28]より、∞(O)以外は、y座標が0に限るから、$E_1[2]=\{O,(0,0),(A,0),((B-A)q^{4n-2},0)\}$ (註:$E_1[2] \simeq Z_2 \oplus Z_2$である。)のみ用いて、何か情報を得ようとしても徒労に終わることだろう。

なぜならば、楕円曲線E_1は、奇数の完全数の条件式: $(B-A)q^{4n-2}+A=Bq^{4n-3}$の左辺の各項のみを使って構成した式であり、左辺＝右辺という奇数の完全数の条件が、Torsion GroupE_1[2]には反映していない。したがって、Torsion Groupを使って、前述した楕円曲線の情報を得たいと考えるならば、[命題28]の註で述べたように、Torsion Groupから離れて別の視点を持った方が良いと考える。楕円曲線E_1, E_2,およびE^*以外の「2平方和定理」から構成した楕円曲線E_3, E_4,E_5,E_6, $E_{h,N}$, $E_{j,2N}$ は、各Torsion Groupの中でy座標が0でないものが存在する可能性あるかもしれない。そのようなTorsion subroupを研究課題にすることが重要であろう。有理点からなるTorsion Groupの各座標は、Nagell-Lutzの定理より、整数座標になり、その整数点のy-座標が0で無いものを見つけるには、$y^2 \mid 16\Delta(E_1)$を満たすyを求め、楕円曲線の式に代入し、x座標が整数のものを求めればよいと考える。

そのような楕円曲線たちの判別式や導手は、各解の差積の2乗に関連した情報を含んでいるので、奇数の完全数になる条件式が反映していると考える。それらは、E_1[2]とは異なる 豊かな情報がもたらされるものと期待したい。

(㋑)Torsion Groupを用いない方法へ

上述した楕円曲線たち(それらを代表してEで表す)について、奇数の完全数の条件を考慮した概念や式は、判別式$\Delta(E)$やj-invariant、導手(conductor)、badな素数とgoodな素数の分類から構成する楕円曲線のL-series＝$L_E(s)$,modular form,・・・などであろう。GaLois representasionは、初めはTorsion Groupから出発するが、Froubenius automorphismやℓ-adic integersや$a_r=r+1-\#E(F_r)$・・・などが関係するから、奇数の完全数の条件が、これらの式の中に情報としてもたらされていると考える。したがって、この領域の研究が重要であると考える。

(㋒) Ⅱ章で言及した「Nielsen命題」,「Hareの命題」に関して

また、「Hareの命題: 奇数の完全数Nは、重複も数えて少なくとも75個の素因数をもつ」ことを考慮すると、Nの相異なる素因数の数が9個(つまり、k+1≥9のとき)以上であっても、素因数の数を重複も数えて、$2m_1+2m_2+2m_3+\cdots+2m_k+(4n-3)\leq 74$ならば、奇数の完全数ではあり得ないので、[2],[3]で構成した楕円曲線たちの中で、楕円曲線論の諸定理と矛盾する異常な兆候が観られるはずである。これらの兆候なり、傾向から上述した楕円曲線たちの性質から一般的な命題を引き出せるだろうか？

(㋓) 幾つかのコメント(導手も含めて)

＊ 再度、[2],[3]で構成した非特異楕円曲線E_1,E_2,E_3,E_4,E_5,E_6,$E_{h,N}$,$E_{j,2N}$ (ただし、h,j は上述した通り)について,楕円曲線を構成した過程を振り返ることにする。

(a) 式(67): $(B-A)q^{4n-2}+A=Bq^{4n-3}$ ⇒(68)の楕円曲線$E_1: y^2=x(x-A)\{x+(B-A)q^{4n-2}\}$

(註:判別式$\Delta(E_1)=A^2(B-A)^2B^2q^{16n-10}$である。$q \mid A$より、$E_1$は半安定な楕円曲線ではない。)

(b) 式(73):$\boldsymbol{R}q^{4n-2}+(B-\boldsymbol{R})=Bq$ ⇒ (74)の楕円曲線$\boldsymbol{E}_2$:$y^2=x(x-\boldsymbol{R}q^{4n-2})\{x+(B-\boldsymbol{R})\}$

(註:判別式$\Delta(\boldsymbol{E}_2)=\boldsymbol{R}^2B^2(B-\boldsymbol{R})^2q^{8n-2}$である。)

(c) 式(88):$N=(\boldsymbol{r}_1M_1)^2+(\boldsymbol{s}_1M_1)^2=\boldsymbol{a}_1^2+\boldsymbol{b}_1^2$ ⇒(89)の楕円曲線$\boldsymbol{E}_3$:$y^2=x(x-\boldsymbol{a}_1^2)(x+\boldsymbol{b}_1^2)$

(註:ただし、$\boldsymbol{r}_1M_1=\boldsymbol{a}_1$,$\boldsymbol{s}_1M_1=\boldsymbol{b}_1$とおいた。$\boldsymbol{a}_1$と$\boldsymbol{b}_1$は公約数$M_1^2$をもつから互いに素ではない。

判別式$\Delta(\boldsymbol{E}_3)=\boldsymbol{a}_1^4\boldsymbol{b}_1^4N^2$である。したがって、$\boldsymbol{E}_3$は半安定ではない。))

(d) 式(85)より、$\dfrac{N}{M_1^2}=q^{4n-3}=\boldsymbol{r}_1^2+\boldsymbol{s}_1^2$ ⇒(90)の楕円曲線$\boldsymbol{E}_4$:$y^2=x(x-\boldsymbol{r}_1^2)(x+\boldsymbol{s}_1^2)$

(註:$\boldsymbol{r}_1$と$\boldsymbol{s}_1$は互いに素である。判別式$\Delta(\boldsymbol{E}_4)=\boldsymbol{r}_1^4\boldsymbol{s}_1^4\dfrac{N^2}{M_1^4}$である。$\boldsymbol{E}_4$は半安定である。)

(e) 式(91):$\dfrac{N}{M_2^2}=q=\boldsymbol{a}_2^2+\boldsymbol{b}_2^2$ ($\boldsymbol{a}_2$と$\boldsymbol{b}_2$は互いに素) ⇒(92)の楕円曲線$\boldsymbol{E}_5$:$y^2=x(x-\boldsymbol{a}_2^2)(x+\boldsymbol{b}_2^2)$

(註:$\boldsymbol{a}_2$と$\boldsymbol{b}_2$は互いに素である。判別式$\Delta(\boldsymbol{E}_5)=\boldsymbol{a}_2^4\boldsymbol{b}_2^4\dfrac{N^2}{M_2^4}$となり、$\boldsymbol{E}_5$は半安定である。)

(f) 式(95):$N=2u(u+1)+2v(v+1)+1$ ⇒(96)の楕円曲線$\boldsymbol{E}_6$:$y^2=x\{x-2u(u+1)\}\{x+2v(v+1)+1\}$

(註:$2u(u+1)$と$\{2v(v+1)+1\}$は互いに素かどうか未定である。

判別式$\Delta(\boldsymbol{E}_6)=\{2u(u+1)\}^2\{2v(v+1)+1\}^2N^2$となる。)

(g) 上述した(c),(d),(e),(f)でふれた楕円曲線$\boldsymbol{E}_3$,$\boldsymbol{E}_4$,$\boldsymbol{E}_5$,$\boldsymbol{E}_6$は、前述した楕円曲線のグループ

$\boldsymbol{E}_{h,N}$ $(1\leq h\leq\dfrac{r_2(q^{4n-3})}{8})$に含まれている楕円曲線である。

また、$\boldsymbol{E}_{j,2N}$ (ただし、$1\leq j\leq\dfrac{r_2(q^{4n-3})}{8}$)は、$\boldsymbol{E}_{h,N}$ (ただし、$1\leq h\leq\dfrac{r_2(q^{4n-3})}{8}$)と双有理同値なのかどうか未定である。(註:$j$-invariantを$\overline{\boldsymbol{Q}}$で考えれば、双有理同値かどうか判定できる。)

上記(a)～(g)の楕円曲線たちの中で(90)の$\boldsymbol{E}_4$:$y^2=x(x-\boldsymbol{r}_1^2)(x+\boldsymbol{s}_1^2)$,(92)の$\boldsymbol{E}_5$:$y^2=x(x-\boldsymbol{a}_2^2)(x+\boldsymbol{b}_2^2)$

は、それぞれ半安定な非特異楕円曲線であるから、導手となる素因数のべき指数はすべて1であろうと予想される。$\boldsymbol{E}_4$の判別式$\Delta(\boldsymbol{E}_4)=(\boldsymbol{r}_1^2)^2(\boldsymbol{s}_1^2)^2(\boldsymbol{r}_1^2+\boldsymbol{s}_1^2)^2=\boldsymbol{r}_1^4\boldsymbol{s}_1^4\dfrac{N^2}{M_1^4}=\boldsymbol{r}_1^4\boldsymbol{s}_1^4q^{8n-4}$となる。同様に計算すると、$\boldsymbol{E}_5$の判別式$\Delta(\boldsymbol{E}_5)=\boldsymbol{a}_2^4\boldsymbol{b}_2^4(\boldsymbol{a}_2^2+\boldsymbol{b}_2^2)^2=\boldsymbol{a}_2^4\boldsymbol{b}_2^4\dfrac{N^2}{M_2^4}=\boldsymbol{a}_2^4\boldsymbol{b}_2^4q^2$である。

上述したことから、$\boldsymbol{E}_4$,$\boldsymbol{E}_5$は、それぞれ2平方和で表される自然数が互いに素であるから、当然両方の自然数が偶数ではないこと、さらにⅢ章の奇数の完全数について数学史⑳では、Nは$105=3\cdot5\cdot7$で割り切れないことから、Nは素因数3を持たないことから、楕円曲線$\boldsymbol{E}_4$,$\boldsymbol{E}_5$におけるp＝3による還元

は考慮しなくてても良いと考える。したがって、$\boldsymbol{E}_4,\boldsymbol{E}_5$の楕円曲線は、半安定非特異楕円曲線なので、p＝2の場合も含めて、導手(註:導手(Conductor)は、一般にNで表すことになっているが、文字Nは奇数の完全数で使っているので混同を避けるため、楕円曲線$\boldsymbol{E}$の導手をCon($\boldsymbol{E}$)で表すことにする。)は、多分、

$$\mathrm{Con}(\boldsymbol{E}_4)=(\Delta(\boldsymbol{E}_4)\text{の相異なる素因数の積})=q\prod_{p_u\mid r_1}p_u\prod_{p_v\mid s_1}p_v$$

$$\mathrm{Con}(\boldsymbol{E}_5)=(\Delta(\boldsymbol{E}_5)\text{の相異なる素因数の積})=q\prod_{p_c\mid a_2}p_c\prod_{p_d\mid b_2}p_d$$

となることが予想される。(註:たとえp＝3で2平方和の一方の自然数が割り切れても他の自然数およびNはp＝3を約数に持たない。p＝2の場合も同様である。)

一方、等式(67):$(B-A)q^{4n-2}+A=Bq^{4n-3}$から構成された(68)の

楕円曲線$\boldsymbol{E}_1:y^2=x(x-A)\{x+(B-A)q^{4n-2}\}$

について、この楕円曲線は半安定ではない楕円曲線で、判別式$\Delta(\boldsymbol{E}_1)=A^2B^2(B-A)^2q^{16n-10}\neq 0$である。Bの素因数の中に、2が含まれるので、導手を求める場合は、少し厄介である。しかし、命題25の証明過程の式(52)より、(B-A)の素因数は、$\boldsymbol{R}$か$(1+q+q^2+\cdots+q^{4n-4})$の素因数に限られるので、badな素数の候補は、$2,p_1,p_2,p_3,\cdots,p_k,q$の一部と(B-A)の素因数の一部であると考える。

Ⅵ章,Ⅶ章で構成した幾つかの非特異楕円曲線たち$\boldsymbol{E}_1,\boldsymbol{E}_2,\boldsymbol{E}_3,\boldsymbol{E}_4,\boldsymbol{E}_5,\boldsymbol{E}_6,\boldsymbol{E}_{h,N},\boldsymbol{E}_{j,2N}$について、奇数の完全数が存在するのか,あるいは非存在かという研究課題に関連について言及する。

[研究課題1]$\boldsymbol{E}_1,\boldsymbol{E}_2,\boldsymbol{E}_3,\boldsymbol{E}_4,\boldsymbol{E}_5,\boldsymbol{E}_6,\boldsymbol{E}_{h,N},\boldsymbol{E}_{j,2N}$を満たすそれぞれの有理点全体を、それぞれ$\boldsymbol{E}_1(\boldsymbol{Q})$, $\boldsymbol{E}_2(\boldsymbol{Q}),\boldsymbol{E}_3(\boldsymbol{Q}),\boldsymbol{E}_4(\boldsymbol{Q}),\boldsymbol{E}_5(\boldsymbol{Q}),\boldsymbol{E}_6(\boldsymbol{Q}),\boldsymbol{E}_{h,N}(\boldsymbol{Q}),\boldsymbol{E}_{j,2N}(\boldsymbol{Q})$とする。これらはアーベル群である。

①$\boldsymbol{E}_1,\boldsymbol{E}_2$以外のTorsion Groupを決定せよ。

②それぞれの導手、2分点、ℓ分点を決定せよ。また、ℓ分点はpで良いのだろうか?

③ これらの楕円曲線から考えられるGalois表現は、どのようなものか?

④これらの楕円曲線は、すべてモジュラーだろうか?

[研究課題2] BakerおよびSiegelの定理により、それぞれの楕円曲線$\boldsymbol{E}_3,\boldsymbol{E}_4,\boldsymbol{E}_5,\boldsymbol{E}_{h,N},\boldsymbol{E}_{j,2N}$を満たす各整数解は有限個である。各楕円曲線の整数解を決定せよ。

[研究課題3] 奇数の完全数Nについて、条件S(N)＝2Nより、(38)の関数G(x)を使うと、$G(q)=0$でなければならない。つまり、(13)の式が成り立ち、式を変形すると、

$$(B-A)q^{4n-2}-Bq^{4n-3}+A=0 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(97)$$

となる。ただし、$A=S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})$, $B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$, qは$q\equiv 1\pmod 4$を満たす素数である。ここで、qと$p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$を不定元のように変数化して、$q$をX, $p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$をYで表すと、

$B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$ は、$B=2Y^2$と表される。(97)の式をX, Y, Aを用いて表すと、

$$(2Y^2-A)X^{4n-2}-2Y^2X^{4n-3}+A=0 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(98)$$

となる。(98)より、式を変形すると、

$$Y^2=\frac{A(X^{4n-3}-1)}{2X^{4n-3}(X-1)} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(99)$$

となる。この(99)の代数曲線を双有理変換して、楕円曲線の型に変形できるであろうか？ もし、変形できなければ、高次元の代数幾何の領域で考えた方がよいか？

[研究課題4] 奇数の完全数Nの条件:

$$S(N)=2N\Leftrightarrow S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})S(q^{4n-3})=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}q^{4n-3}$$

において、$p_1,p_2,\cdots,p_k,q$をそれぞれ$X_1,X_2,\cdots X_k,Y$と変数変換すると、上の等式は、

$$S(X_1^{2m_1})S(X_2^{2m_2})\cdots S(X_k^{2m_k})S(Y^{4n-3})=2X_1^{2m_1}X_2^{2m_2}\cdots X_k^{2m_k}Y^{4n-3}$$

を満たす代数多様体として捉えて、その解集合を考察してはどうか？

また、$R=1$の場合、奇数の完全数の条件は、

$$A=q^{4n-3}\text{かつ}S(q^{4n-3})=B \quad \cdots\cdots\cdots\cdots\cdots\cdots(100)$$

であった。上で述べたようにNの素因数を上記と同様の変数に置き換えれば、(100)は、2つの等式

$$S(X_1^{2m_1})S(X_2^{2m_2})S(X_3^{2m_3})\cdots S(X_k^{2m_k})=Y^{4n-3}\text{かつ}S(Y^{4n-3})=2X_1^{2m_1}X_2^{2m_2}X_3^{2m_3}\cdots X_k^{2m_k} \quad \cdots\cdots(101)$$

の共通な解集合を考察し、その中に整数点が存在するのか、存在した場合、それらがすべて奇素数となる場合があるのか、さらに、YがY≡1(mod 4)となる奇素数であるのか？

この場合、[命題7]より、$1=R=Aq-B(q-1)$だから、A,Bの各素因数を変数に置き換えると、

$$1=S(X_1^{2m_1})S(X_2^{2m_2})\cdots S(X_k^{2m_k})Y-2X_1^{2m_1}X_2^{2m_2}\cdots X_k^{2m_k}(Y-1)$$

を同時に考慮しなくてもよいことは、[命題κ]の中で解説済みである。

＊(101)で使われている変数の個数は多すぎるので、以下の研究課題ではA,Bをひとまとめにして、定数、あるいは、変数に置き換えることにする。

[研究課題5] (38)の式から、代数方程式G(x)=0とおいて、$A=S(p_1^{2m_1})S(p_2^{2m_2})\cdots S(p_k^{2m_k})$を右辺の形にこだわらない変数Yで表し、$B=2p_1^{2m_1}p_2^{2m_2}\cdots p_k^{2m_k}$は、固定した定数として扱うことにする。xを変数Xと置き換えると、代数方程式G(x)=0は次のような2変数代数曲線G(X,Y)=0になる。

$$G(X,Y)=(B-Y)X^{4n-2}-BX^{4n-3}+Y=0 \quad \cdots\cdots\cdots\cdots\cdots\cdots(102)$$

(102)を満たす代数曲線について、どのようなことが成り立つであろうか？

(註:(102)より、$Y=\dfrac{BX^{4n-3}(X-1)}{X^{4n-2}-1}$となる。この代数曲線は、双有理変換で楕円曲線型になるであろうか？)

[研究課題6] **V章**では、$A=S(p_1^{2m_1})S(p_2^{2m_2})S(p_3^{2m_3})\cdots S(p_k^{2m_k}),B=2p_1^{2m_1}p_2^{2m_2}p_3^{2m_3}\cdots p_k^{2m_k}$として、命題10のSに関して入れ子のような再帰性があることに拘泥せず、定数のように扱ってきた。代数方程式$G(x)=(B-A)x^{4n-2}-Bx^{4n-3}+A=0$において、A,Bを定数と見做さず、またA,Bのそれぞれの右辺の形にこだわらず、Aを変数$\boldsymbol{Y}$,Bを変数$2\boldsymbol{Z}^2$(ただし、$\boldsymbol{Z}=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$とおく。),xを$\boldsymbol{X}$と置き換えると、$G(x)=0$は、次のような代数多様体$V(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z})=0$となる。

$$V(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z})=(2\boldsymbol{Z}^2-\boldsymbol{Y})\boldsymbol{X}^{4n-2}-2\boldsymbol{Z}^2\boldsymbol{X}^{4n-3}+\boldsymbol{Y}=0 \quad (\text{ただし、}n\geqq 2)^{\text{註}} \quad \cdots\cdots\cdots\cdots\cdots\cdots(103)$$

を満たす整数解$(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z})$(ただし、$\boldsymbol{X}\neq 1$)が存在すれば、奇数の完全数の存在の可能性がある。

この場合、諸命題とりわけ命題6のA,Bが満たさなければならない条件があることから、$\boldsymbol{Y}$, $\boldsymbol{Z}$の制約条件および$\boldsymbol{X}$の制約条件を満たすかどうか奇数の完全数の存在への鍵となる。一方、自明でない整数解$(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z})$が存在しない場合は、奇数の完全数は存在しない。

(ただし、自明な解は、$(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z})=(1,\boldsymbol{Y},\boldsymbol{Z})$である。)

(註:(103)の式で、$\boldsymbol{X}=\dfrac{X}{U},\boldsymbol{Y}=\dfrac{Y}{U},\boldsymbol{Z}=\dfrac{Z}{U}$と置き換えると、射影モデルとしての斉次方程式

$$(2Z^2-UY)X^{4n-2}-2Z^2UX^{4n-3}+U^{4n-1}Y=0 \quad \cdots\cdots\cdots\cdots\cdots\cdots(104)$$

となる。(104)の自明でない整数解(X,Y,Z,U)が存在するだろうか？)

[研究課題7]「2平方和定理」により、奇数の完全数Nは適当な自然数$\boldsymbol{a},\boldsymbol{b}$を選んで、

$$N=\boldsymbol{a}^2+\boldsymbol{b}^2 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(105)$$ (註:**VI章の[3]**で述べた事柄参照)

と表される。(105)とそれぞれ(85), (86)と組み合わせることによって、

$$\boldsymbol{a}^2+\boldsymbol{b}^2=\boldsymbol{q}^{4n-3}M_1^2 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(106)$$ (註:$M_1=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$とおいた。)

$$\boldsymbol{a}^2+\boldsymbol{b}^2=\boldsymbol{q}M_2^2 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(107)$$ (註:$M_2=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}\boldsymbol{q}^{2n-2}$とおいた。)

が成り立つ。(106)および(107)の等式から、次のようなそれぞれの不定方程式(108)および(109)を構成する。

(106)において、$\boldsymbol{a}$をXに、$\boldsymbol{b}$をYに、M_1をZに置き換えて、変数化(不定元とする)すると、

$$X^2+Y^2=\boldsymbol{q}^{4n-3}Z^2 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(108)$$

また、(107)において、$\boldsymbol{a}$をXに、$\boldsymbol{b}$をYに、M_2をZに置き換えて、変数化(不定元とする)すると、

$$X^2+Y^2=\boldsymbol{q}Z^2 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(109)$$

不定方程式(108)および(109)は、それぞれ種数0の代数曲面(2次曲面)であるから、それぞれの不定方程式において、(0,0,0)以外の整数解(X,Y,Z)が存在する。(108)の整数解の例として、

$$(X,Y,Z)=(\mp a,\mp b,\mp M_1)$$

がある。また、(109)の整数解の例として、$(X,Y,Z)=(\mp a,\mp b,\mp M_2)$が存在する。有理点をもつ2次曲面(108)および(109)は、Q上で双有理同値であることが予想される。それぞれの双有理同値写像全体はどのような構造をもっているのだろうか？

また、(108)および(109)を満たすそれぞれの整数解全体をS_1,S_2とする。それぞれのS_1,S_2は、それぞれどのような構造を持つであろうか(註)。

(註:(108)において、両辺をZ^2で割ると、

$$(\frac{X}{Z})^2+(\frac{Y}{Z})^2=q^{4n-3} \quad \cdots\cdots(110)$$

ここで、$(\frac{X}{Z})=U$, $(\frac{Y}{Z})=V$とおくと、(110)は、

$$U^2+V^2=q^{4n-3} \quad (\text{ただし、}q\text{は}q\equiv 1(\mathrm{mod}\ 4)\text{を満たす素数}) \quad \cdots\cdots(111)$$

(111)は、U-V平面では、幾何学的には半径$\sqrt{q^{4n-3}}$の円を表すが、この円周上に有理点(例えば、$(\frac{\mp a}{M_1},\frac{\mp b}{M_1})$で、(ただし、$q\nmid M_1$)が存在する。さらに、$q$は$q\equiv 1(\mathrm{mod}\ 4)$の奇素数なので、「2平方和定理」より、$(\frac{\mp a}{M_1},\frac{\mp b}{M_1})$と異なる整数点$(\mp c,\mp d)$が存在する。(111)を満たす有理点全体は、どのような構造をもつであろうか？

また、(109)の両辺をZ^2で割って、$\frac{X}{Z}=U$, $\frac{Y}{Z}=V$とおけば、

$$U^2+V^2=q \quad \cdots\cdots(112)$$

となる。(112)は、U-V平面では、幾何学的には半径$\sqrt{q}$の円を表すが、(112)を満たす有理点$(\frac{\mp a}{M_2},\frac{\mp b}{M_2})$以外に、「2平方和定理」より、整数解$(\mp e,\mp f)$がある。(112)を満たす有理点全体については、どのようなことが言えるであろうか。

また、p-進数体Q_pでは、(111)および(112)のそれぞれの解は、どのような構造があるだろうか。)

[研究課題8]VI章で述べた次の楕円曲線たち

$$E_1:y^2=x(x-A)\{x+(B-A)q^{4n-2}\}, \qquad E_2:y^2=x(x-Rq^{4n-2})\{x+(B-R)\}$$

$$E_3:y^2=x(x-a_1^2)(x+b_1^2), \qquad E_4:y^2=x(x-r_1^2)(x+s_1^2),$$

$$E_5:y^2=x(x-a_2^2)(x+b_2^2), \qquad E_6, E_{h,N}\text{および}E_{j,2N}$$

のそれぞれの整数解は、Siegelの定理により高々有限個であるが、各楕円曲線の整数解は、他の楕円曲線の整数解と互いにどのような関係があるのか？

また、これらの楕円曲線は、奇数の完全数Nと関連して構成した代数曲線なので、互いに関係があると考えられるが、その関係を見つけよ。例えば、適当な双有理変換で互いに同値になるものが存在するのであろうか？

[研究課題9] (105)の式 $a^2+b^2=N$において、$a=\frac{X}{U}, b=\frac{Y}{U}$とおいて、射影モデルの斉次方程式

$$(\frac{X}{U})^2+(\frac{Y}{U})^2=N \Rightarrow X^2+Y^2-NU^2=0 \quad \cdots\cdots(113)$$

が得られる。斉次方程式(113)は実数体R上では、解の一つ$(X,Y,U)=(3,4,\frac{5}{\sqrt{N}})$が存在する。さらに、p-進体$Q_p$で解が存在するであろうか。

(註:もし仮に、p-進体Q_p上で解が見つかれば、ハッセ(H,Hasse)の原理により、有理数体上で解が存在することが言える。また、もし仮に、p-進体Q_p上で解が無ければ、奇数の完全数Nは存在しないことが言えるだろう。)

[研究課題10] **[命題 ν]**が成り立つとして、その中で、

$$p_j^{2m_j+1}-q^{i_j}p_j+q^{i_j}-1=0 \quad \cdots\cdots(114)$$

(ただし、jは、$1\leq^{\forall} j\leq k$,i_j は,$1\leq^{\exists} i_j\leq 4n-3$を満たす自然数)

が成り立つことを示した。等式(114)をmod p_j およびmod$q$で考えると、

$$p_j^{2m_j+1}\equiv 1(\mathrm{mod}\ q) \quad \cdots\cdots(115)$$

$$q^{i_j}\equiv 1\ (\mathrm{mod}\ p_j) \quad \cdots\cdots(116)$$

ここで、Fermatの小定理との関連から、(115)より、

$(q-1)\mid(2m_j+1)$が成り立つことが言えるのではないだろうか。また、(116)から、

$(p_j-1)\mid i_j$ が成り立つことが言えるのではないだろうか。

(註:2つの素数p_jとqについて、$p_j\neq q$であるので、平方剰余の相互法則から、

$(\frac{p_j}{q})(\frac{q}{p_j})=1$が成り立つ。

なぜならば、平方剰余の相互法則より、

$$(\frac{p_j}{q})(\frac{q}{p_j})=(-1)^{\frac{1}{4}(p_j-1)(q-1)} \quad \cdots\cdots(117)$$

が成り立つ。(117)の右辺の(-1)の指数について、$q\equiv 1\ (\mathrm{mod}\ 4)$より、$(q-1)$は4の倍数で、$(p_j-1)$は偶数だから、$(p_j-1)(q-1)$は8の倍数になり、$\frac{1}{4}(p_j-1)(q-1)$は偶数となるから、$(-1)^{\frac{1}{4}(p_j-1)(q-1)}=1$となる。)

（註：奇数の完全数Nの素因数分解に現れる各素因数のべき指数においても、素因数のqやp_jにそれぞれ関係して、入れ子のような相互関係が読み取れるように思える。）

[研究課題11]命題7および命題7のLemma I より、$R=1$の場合、$A=q^{4n-3}$かつ $S(q^{4n-3})=B$ かつ $1=Aq-Bq+B$であることを示した。これらの等式から、次の楕円曲線が構成される。

$S(q^{4n-3})=B$より、$\dfrac{q^{4n-2}-1}{q-1}=B$となり、分母を払ってまとめると、$q^{4n-2}=B(q-1)+1$となる。右辺の各項を使って、$E_7: y^2=x(x-1)\{x+B(q-1)\}$を構成する。このルジャンドル型の楕円曲線の判別式は、

$$\Delta(E_7)=B^2(q-1)^2q^{8n-4}\neq 0$$

で、$q-1$は4の倍数であるから、$16 \mid \Delta(E_7)$が成り立つ。Bは偶数であるから、結局は、$64 \mid \Delta(E_7)$が成り立つ。また、$R\neq 1$の場合、$A=Rq^{4n-3}$かつ$RS(q^{4n-3})=B$ かつ$R=A(q-1)+B$だから、最後の等式：$R=A(q-1)+B$の右辺の各項を使って、次の楕円曲線

$$E_8: y^2=x(x-B)\{x+A(q-1)\}$$

を構成すると、この楕円曲線の判別式は、$\Delta(E_8)=B^2A^2(q-1)^2R^2=B^2(Rq^{4n-3})^2(q-1)^2R^2$
$=B^2R^4(q-1)^2q^{8n-6}$となる。E_7, E_8は、モジュラーだろうか？

（研究課題以上）

◎このレジュメの目的は、奇数の完全数が存在すると仮定して、それを数学史をふまえて代数方程式および楕円曲線や，できれば、代数幾何、代数多様体へと関連させる試みで中間報告の段階であり、このアプローチの方法が妥当なのかどうか・・・研究中である。

上述した楕円曲線たちの一つでもmodularでないことが示されれば、奇数の完全数が存在しないことが言えるのだが・・・。また、modularであることが示されたならば、さらに、奇数の完全数へのロマンの旅にかきたてられることだろう。また、命題η，命題κ，命題τ，命題ν，命題υの5つの命題が正しいかどうか検証の過程を経なければならない。

奇数の完全数の定義：$S(N)=2N$は、命題7より、2つの等式$A=Rq^{4n-3}$ かつ$RS(q^{4n-3})=B$に分解され、連立した型となることを示した。したがって、奇数の完全数の研究領域を連立型へと移さなければならないだろうと考える。

このレジュメは、あくまでも奇数の完全数についての数学史を背景にした「試み」であり、研究途上の中間報告である。（$R=1$であるのか、あるいは$R\neq 1$なのか未定のままである。）

また後日の発表の機会があれば、・・・と思う。この辺で、筆を置きます。　　（以上）