総合政策論集　第6巻第1号　2007年

自然数 67993 は合同数である

河本　進 *

67993 is a congruent number

KOMOTO Susumu

1．はじめに

自然数 n が合同数であるとは，面積が n となる3辺の長さが有理数の直角三角形が存在することをいう．例えば，3辺の長さが $3,4,5$ の直角三角形の面積は 6 なので，6 が合同数であることは直ちにわかる．また，3辺の長さが $3/2, 20/3, 41/6$ の直角三角形の面積は 5 なので，5 が合同数になることが，フィボナッチによって示されている．一方，フェルマーによって $1,2,3$ は合同数でないことが示されている．このように，自然数が合同数か否かを調べることは，昔から考えられてきた問題である．ここで，ある自然数が合同数か否かを統一的に判定する方法があるかどうかが問題となる．例えば，8 で割った余りが 5 または 7 となる素数は合同数であり，余りが 3 となる素数は合同数でないなどの条件が知られている．1983 年には，J. B. Tunnell [1] によって合同数になるための必要条件が与えられた．J. B. Tunnell による必要条件は，クレイ数学研究所がミレニアム懸賞問題の1つとしてあげた Birch and Swinnerton-Dyer 予想の弱形式が解決すれば必要十分条件となるが，この予想は解決されていない．つまり，与えられた自然数が合同数か否かを完全に決定する方法は，未だ確立されていない．そこで，計算機を利用した数値計算によって，合同数を小さな数から決定していく試みがなされている．

その結果，1993 年に K. Noda and H. Wada [2] によって1万以下の合同数がすべて決定された．次に，1998 年に F. R. Nemenzo [3] によって 42,552 以下の合同数がすべて決定された．そして，2005 年に開催された 6-th Symposium on Algebra and Computation で，S. Komoto, T. Watanabe and H. Wada は「42553 が合同数であること」と「71473, 90697, 98242 を除く10万以下の合同数がすべて決定したこと」の報告を行った（42553 が合同数であることを確かめた計算結果は [4] を参照）．

本稿では，8 で割った余りが 1 となる素数を考察して，67993 が合同数であることを具体計算によって確かめた．また，同じ計算方法を用いて 90697 が合同数であることも確かめた．なお，98242 が合同数であることは，すでに他の自然数を調べた方法で確かめられている．

* 東北文化学園大学講師　Lecturer of Tohoku Bunka Gakuen University
e-mail: komoto@pm.tbgu.ac.jp

最後に，この研究のご指導をして下さった上智大学名誉教授の和田秀男先生，この研究を共に行ってきた渡辺透氏に深い感謝の意を表します．

2．合同数と楕円曲線

3辺の長さが $L_1 < L_2 < L_3$ で，面積が n となる直角三角形が存在するとき，

$$(x, y) = \left(\frac{L_3^2}{4} , \frac{(L_2^2 - L_1^2)L_3}{8} \right) \tag{1}$$

とすると，(x, y) は楕円曲線 $y^2 = x^3 - n^2 x$ 上の点となることが簡単な計算によって確認できる．例えば，面積が 6 となる3辺の長さが $3, 4, 5$ の直角三角形に対して，$(x, y) = (25/4, 35/8)$ が楕円曲線 $y^2 = x^3 - 36x$ 上の点となることは直ちにわかる．実は，与えられた自然数 n が合同数になることと，楕円曲線 $y^2 = x^3 - n^2 x$ 上に $(x, y) = (0, 0), (-n, 0), (n, 0)$ 以外に有理点を持つこととが同値になることが知られている．この同値条件によって，合同数という素朴な研究対象が，楕円曲線という現代数学の研究テーマと結びつく．

まずは，楕円曲線に関して必要な性質をいくつか述べる．なお，証明等の詳細は楕円曲線に関する文献を参照のこと．

$4a^3 + 27b^2 \neq 0$ を満たす有理数 a, b に対して，

$$E : y^2 = x^3 + ax + b \tag{2}$$

で定義される曲線 E を $\mathbb{Q}$ 上の楕円曲線という．この定義式を射影空間の同時座標で考えると，

$$Y^2 Z = X^3 + aXZ^2 + bZ^3 \tag{3}$$

となるので，楕円曲線 E と 射影空間内の無限遠直線 $Z = 0$ とは，$[X : Y : Z] = [0 : 1 : 0]$ で3重に接することが分かる．この点を無限遠点とよび $\mathcal{O}$ で表す．次に，集合 $E(\mathbb{Q})$ を

$$E(\mathbb{Q}) = \{P = (x, y) \in E \mid x, y \in \mathbb{Q}\} \cup \mathcal{O} \tag{4}$$

と定義をして，$E(\mathbb{Q})$ の各元を有理点とよぶ．このとき，$E(\mathbb{Q})$ 上に $\mathcal{O}$ を単位元とする二項演算 $(+)$ が，$P_1, P_2, P_3 \in E(\mathbb{Q})$ に対して，

$$P_1, P_2, P_3 \text{ は一直線上にある} \iff P_1 + P_2 + P_3 = \mathcal{O} \tag{5}$$

という特徴付けによって定義でき，$E(\mathbb{Q})$ は Abel 群になる．なお，座標を与えたときの具体的な演算は簡単な計算で与えられるが，ここでは，$P = (x, y)$ に対して，$2P = P + P$ の x 座標が

$$\frac{(x^2 - a)^2 - 8bx}{4y^2} \tag{6}$$

になることのみを記述する．なお，$y = 0$ のときは，$2P = \mathcal{O}$ となる．

$E(\mathbb{Q})$ に関して Mordell の定理と呼ばれる，次の定理が成り立つ．

Mordell の定理. $E(\mathbb{Q})$ は，有限生成 Abel 群である．

したがって，Abel 群の基本定理より

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}} \tag{7}$$

となる．ここで，$E(\mathbb{Q})_{\text{tors}}$ で $E(\mathbb{Q})$ の位数有限の元全体のなす部分群を表す．また，r を $E(\mathbb{Q})$ のランクという．

ここからは， N. Koblitz [5] より，合同数と楕円曲線の関係についての結果を引用する．

自然数 n に対して，楕円曲線 E_n を

$$E_n : y^2 = x^3 - n^2x \tag{8}$$

と定義する．このとき，次の２つの命題が成り立つ．

命題 1. $E_n(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0,0), (-n,0), (n,0)\}$.

命題 2. 次は同値である．
(1) 自然数 n が合同数になる．
(2) rank $E_n(\mathbb{Q}) \geqq 1$.

命題 1, 2 より，次の系が成り立つ．

系. 次は同値である．
(1) 自然数 n が合同数になる．
(2) $E_n(\mathbb{Q})$ に $\{\mathcal{O}, (0,0), (-n,0), (n,0)\}$ 以外の有理点が存在する．

３辺の長さが $L_1 < L_2 < L_3$ で面積が n となる直角三角形と，楕円曲線 $y^2 = x^3 - n^2x$ 上の有理点との間には，次の対応がある．

命題 3. 面積が n の３辺の長さが有理数の直角三角形全体と $2E_n(\mathbb{Q}) - \{\mathcal{O}\}$ は，３辺の長さを $L_1 < L_2 < L_3$ でと表すとき，次の写像により１対１に対応する．

$$(x, \pm y) \mapsto L_1 = \sqrt{x+n} - \sqrt{x-n},\ L_2 = \sqrt{x+n} + \sqrt{x-n},\ L_3 = 2\sqrt{x} \tag{9}$$

$$L_1 < L_2 < L_3 \mapsto \left(\frac{L_3^2}{4},\ \pm \frac{(L_2^2 - L_1^2)L_3}{8} \right) \tag{10}$$

ここで，$2E_n(\mathbb{Q})$ で，$P \in E_n(\mathbb{Q})$ の２倍点，すなわち，$2P$ で表される元全体を表す．

3．ランクの計算方法

ここでは，有理数体上の楕円曲線のランクを計算する方法を，J. H. Silverman and J. Tate [6] 第3章より本稿で必要な形で引用をする．

整数 $a \neq 0$ に対して，楕円曲線 E, E' を

$$E : y^2 = x^3 + ax, \quad E' : y^2 = x^3 - 4ax \tag{11}$$

と定義する．E, E' の無限遠点をそれぞれ $\mathcal{O}, \mathcal{O}'$ で表す．このとき，次の2つの命題が成り立つ．

命題 4. (1) 写像 $\phi : E(\mathbb{Q}) \to E'(\mathbb{Q})$ を

$$\phi(P) = \begin{cases} (\frac{y^2}{x^2}, \frac{y(x^2-a)}{x^2}) & \text{if } P = (x,y) \neq \mathcal{O},\ (0,0) \\ \mathcal{O}' & \text{if } P = \mathcal{O},\ (0,0) \end{cases} \tag{12}$$

で定義すると準同型写像になる．このとき，$\ker \phi = \{\mathcal{O}, (0,0)\}$ となる．
(2) 写像 $\psi : E'(\mathbb{Q}) \to E(\mathbb{Q})$ を

$$\psi(P) = \begin{cases} (\frac{y^2}{4x^2}, \frac{y(x^2+4a)}{8x^2}) & \text{if } P = (x,y) \neq \mathcal{O}',\ (0,0) \\ \mathcal{O} & \text{if } P = \mathcal{O}',\ (0,0) \end{cases} \tag{13}$$

で定義すると準同型写像になる．このとき，$\ker \psi = \{\mathcal{O}', (0,0)\}$ となる．
(3) 合成写像 $\psi \circ \phi : E \to E$ は2倍写像になる．すなわち，$\psi \circ \phi(P) = 2P$ となる．これより，

$$(E(\mathbb{Q}) : 2E(\mathbb{Q})) = (E(\mathbb{Q}) : \psi(E'(\mathbb{Q}))) \cdot (\psi(E'\mathbb{Q})) : \psi \circ \phi(E(\mathbb{Q}))) \tag{14}$$

となる．

命題 5. (1) 写像 $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ を

$$\alpha(P) = \begin{cases} 1 \pmod{(\mathbb{Q}^\times)^2} & \text{if } P = \mathcal{O} \\ a \pmod{(\mathbb{Q}^\times)^2} & \text{if } P = (0,0) \\ x \pmod{(\mathbb{Q}^\times)^2} & \text{if } P = (x,y) \text{ with } x \neq 0 \end{cases} \tag{15}$$

で定義すると準同型写像になる．

このとき，$\alpha(E(\mathbb{Q}))$ の各元の代表元として，$1, a$ または（$1 \equiv a$ となることもある），

$$dX^4 + \frac{a}{d}Y^4 = Z^2 \tag{16}$$

が $X \neq 0$, $\gcd(X, \frac{a}{d}YZ) = \gcd(Y, dXZ) = 1$ を満たす整数解を持つ整数 $d \mid a$ を採ることができる．また，このような整数 d と (16) の解に対して，

$$(x, y) = \left(\frac{dX^2}{Y^2}, \frac{dXZ}{Y^3}\right) \tag{17}$$

は $E(\mathbb{Q})$ 上の点となる．

(2) 写像 $\alpha' : E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ を

$$\alpha'(P) = \begin{cases} 1 \pmod{(\mathbb{Q}^\times)^2} & \text{if } P' = \mathcal{O}' \\ -4a \equiv -a \pmod{(\mathbb{Q}^\times)^2} & \text{if } P' = (0,0) \\ x \pmod{(\mathbb{Q}^\times)^2} & \text{if } P' = (x,y) \text{ with } x \neq 0 \end{cases} \tag{18}$$

で定義すると準同型写像になる．

このとき，$\alpha'(E'(\mathbb{Q}))$ の各元の代表元として，$1, -a$ または（$1 \equiv -a$ となることもある），

$$dX^4 - \frac{4a}{d}Y^4 = Z^2 \tag{19}$$

が $X \neq 0$, $\gcd(X, \frac{4a}{d}YZ) = \gcd(Y, dXZ) = 1$ を満たす整数解を持つ整数 $d\,|4a$ を採ることができる．また，このような整数 d と (19) の解に対して，

$$(x,y) = \left(\frac{dX^2}{Y^2}, \frac{dXZ}{Y^3}\right) \tag{20}$$

は $E'(\mathbb{Q})$ 上の点となる．

(3) $r = \operatorname{rank} E(\mathbb{Q})$ とする．このとき，

$$2^{r+2} = \#\alpha(E(\mathbb{Q})) \cdot \#\alpha'(E'(\mathbb{Q})) \tag{21}$$

となる．

以上より，n を自然数とするとき，楕円曲線 $E_n : y^2 = x^3 - n^2x$, $E'_n : y^2 = x^3 + 4n^2x$ に対して，命題 5 を使って不定方程式を解き，$E_n(\mathbb{Q})$ に自明でない有理点が存在すれば n は合同数であり，自明でない有理点が存在しなければ n は合同数でないことがわかる．なお，有理点が存在したときは，求めた点の 2 倍点から三角形の 3 辺を計算できる．

次の節以降は，$p \equiv 1 \pmod 8$ となる素数が合同数になるか否かを考察する．

4．楕円曲線 $\mathbf{y^2 = x^3 - p^2x}$

p を $p \equiv 1 \pmod 8$ となる素数とする．ここでは，楕円曲線 $E : y^2 = x^3 - p^2x$ と楕円曲線 $E' : y^2 = x^3 + 4p^2x$ を考察して，$E(\mathbb{Q})$ のランクを計算する方法を与える．

(1) $\alpha(E(\mathbb{Q}))$ を求める

命題 5 より，$\alpha(E(\mathbb{Q})) \subset \{1, p, -p, -p^2 \pmod{(\mathbb{Q}^\times)^2}\}$ となる．ここで，$\alpha(\mathcal{O}) \equiv 1 \pmod{(\mathbb{Q}^\times)^2}$, $\alpha((0,0)) \equiv -p^2 \pmod{(\mathbb{Q}^\times)^2}$ より，$d = \pm p$ について考えると，不定方程式

$$\pm pX^4 \mp pY^4 = Z^2 \text{（複合同順）} \tag{22}$$

は，$(X,Y,Z)=(1,1,0)$ を解に持ち，この解から有理点を求めると $(x,y)=(\pm p,0)$ となる．以上より，

$$\alpha(E(\mathbb{Q}))=\{1,p,-p,-p^2\ (\mathrm{mod}(\mathbb{Q}^{\times})^2)\} \tag{23}$$

となる．なお，ここで求めた楕円曲線 $E:y^2=x^3-p^2x$ の有理点は，すべて自明な点である．

(2) $\alpha'(E'(\mathbb{Q}))$ を求める

命題 5 より，$\alpha'(E'(\mathbb{Q}))\subset\{1,2,p,2p,-1,-2,-p,-2p\ (\mathrm{mod}(\mathbb{Q}^{\times})^2)\}$ となる．ここで，$d<0$ のとき $dX^4+\frac{4p^2}{d}Y^4\leqq 0$, $Z^2\geqq 0$ となるので，不定方程式

$$dX^4+\frac{4p^2}{d}Y^4=Z^2 \tag{24}$$

の解は $(X,Y,Z)=(0,0,0)$ しか持たない．よって，$\alpha'(E'(\mathbb{Q}))\subset\{1,2,p,2p\ (\mathrm{mod}(\mathbb{Q}^{\times})^2)\}$ となる．また，$\alpha(\mathcal{O})\equiv 1\ (\mathrm{mod}\ (\mathbb{Q}^{\times})^2)$ より，$d=2,p,2p$ から定まる 3 つの不定方程式

$$2X^4+2p^2Y^4=Z^2 \tag{25}$$

$$pX^4+4pY^4=Z^2 \tag{26}$$

$$2pX^4+2pY^4=Z^2 \tag{27}$$

の解を求めることで，楕円曲線 $E:y^2=x^3-p^2x$ のランクが計算できる．以上より，次の補題を得る．

補題 6. p を $p\equiv 1\ (\mathrm{mod}\ 8)$ となる素数，E を楕円曲線 : $y^2=x^3-p^2x$ とする．このとき，

$$\mathrm{rank}\ E(\mathbb{Q})=\begin{cases}0 & \text{if 3つの不定方程式すべてが自明でない解を持たない}\\ 1 & \text{if 3つの不定方程式のうち，1つの式だけ自明でない解を持つ}\\ 2 & \text{if 3つの不定方程式すべてが自明でない解を持つ}\end{cases} \tag{28}$$

となる．

系. p を $p\equiv 1\ (\mathrm{mod}\ 8)$ となる素数とする．このとき，次は同値である．
(1) p が合同数．
(2) 3つの不定方程式のうち少なくとも1つの式で自明でない解を持つ．

注意. 命題 5 より，3つの不定方程式のうち，2つの式に自明でない解が存在することがわかれば，残りの1つの式にも自明でない解が存在することがわかる．

注意. 上で与えた3つの不定方程式は変数変換をすることにより，次の3つの不定方程式

$$X^4+p^2Y^4=2Z^2 \tag{29}$$

$$X^4+4Y^4=pZ^2 \tag{30}$$

$$X^4+Y^4=2pZ^2 \tag{31}$$

に置き換えることができる．

5．不定方程式 $\mathbf{X^4+p^2Y^4=2Z^2}$

p を $p\equiv 1 \pmod 8$ となる素数とする．ここでは，不定方程式 $X^4+p^2Y^4=2Z^2$ の解を探す方法を記述する．

不定方程式 $X^4+p^2Y^4=2Z^2$ に $\gcd(X,\,Y)=1$ を満たす解があれば，$X\equiv Y\equiv Z\equiv 1 \pmod 2$ となる．このとき，$Z=(A+Bi)(A-Bi)$ とおき，

$$(X^2+pY^2i)(X^2-pY^2i)=(1+i)(1-i)(A+Bi)^2(A-Bi)^2 \tag{32}$$

と Gauss 平面上で分解することができる．ここで，実部と虚部を比較することで，

$$\begin{aligned}
&\text{Case 1: } X^2=A^2-B^2-2AB, && pY^2=A^2-B^2+2AB\\
&\text{Case 2: } X^2=A^2-B^2-2AB, && pY^2=-(A^2-B^2+2AB)\\
&\text{Case 3: } X^2=-(A^2-B^2-2AB), && pY^2=A^2-B^2+2AB\\
&\text{Case 4: } X^2=-(A^2-B^2-2AB), && pY^2=-(A^2-B^2+2AB)
\end{aligned} \tag{33}$$

の4つのケースのいずれかが解を持つことになる．なお，単数倍に関しては A,B の役割を入れ替えたりすることで，これらのケースに集約できる．

次に，8で割った余りを考察することにより，Case 2, Case 3 は起こらないことがわかる．逆に，Case 1 または Case 4 を満たす整数 X,Y,A,B を見つければ，$X^4+p^2Y^4=2Z^2$ の解を見つけることができる．

まずは，Case 1 の解を考察する．$(A-B,B,X)=(-1,0,1)$ は $X^2=A^2-B^2-2AB=(A-B)^2-2B^2$ の解である．これより，あとで述べる補題 8 を用いて，$X^2=A^2-B^2-2AB$ 解をパラメーター I,J を使って，

$$A-B=I^2+2J^2,\ B=2IJ,\ X=I^2-2J^2\ (\Longrightarrow A=I^2+2IJ+2J^2) \tag{34}$$

と表示できる．さらに，(34) を $pY^2=A^2-B^2+2AB$ に代入すると，$pY^2=I^4+8I^3J+12I^2J^2+16IJ^3+4J^4$ となる．

一方，Case 4 の場合は，$X^2=-(A^2-B^2-2AB)=(A+B)^2-2(-A)^2$ の解 $(A+B,-A,X)=(-1,0,1)$ を補題 8 に適用すると，$X^2=-(A^2-B^2-2AB)$ の解のパラメーター表示

$$A+B=I^2+2J^2,\ -A=2IJ,\ X=I^2-2J^2\ (\Longrightarrow B=I^2+2IJ+2J^2) \tag{35}$$

を得る．(35) を $pY^2=-(A^2-B^2+2AB)$ に代入すると $pY^2=I^4+8I^3J+12I^2J^2+16IJ^3+4J^4$ となる．以上より，次の補題を得る．

補題 7. p を $p\equiv 1 \pmod 8$ を満たす素数とする．このとき，

$$pY^2=I^4+8I^3J+12I^2J^2+16IJ^3+4J^4 \tag{36}$$

となる $I,\ J$ が求まることと，$X^4+p^2Y^4=2Z^2$ の解が求まることは同値である．

補題 8 (Elkies [7]). 不定方程式 $aX^2+2bXY+cY^2=dZ^2$（ここで，a, b, c, d は係数とする）が $z_0 \neq 0$ となる整数解 $(X,Y,Z)=(x_0,y_0,z_0)$ を持つとき，他の解は

$$\begin{cases} X &= -(ax_0+by_0)I^2-2cy_0IJ+cx_0J^2 \\ Y &= ay_0I^2-2ax_0IJ-(bx_0+cy_0)J^2 \\ Z &= az_0I^2+bz_0IJ+cz_0J^2 \end{cases} \tag{37}$$

と，パラメータ I,J を用いて表示できる．

以上より，I, J を動かして $(I^4+8I^3J+12I^2J^2+16IJ^3+4J^4)/p$ を計算して平方数になれば，$X^4+p^2Y^4=2Z^2$ の解が求まる．ここで，すべての I, J を動かしては効率が悪いので，I, J を動かす範囲を狭める方法を考える．

$p \mid \gcd(I,\ J)$ ならば $p \mid \gcd(X,\ Y)$ となるので，$p \nmid \gcd(I,\ J)$ としてよい．次に，$p \mid J$ とすると，$p \mid I^4+8I^3J+12I^2J^2+16IJ^3+4J^4$ ならば $p \mid I$ となる．よって，$p \nmid J$ としてよい．このとき，$p \mid I^4+8I^3J+12I^2J^2+16IJ^3+4J^4$ ならば，$\mathbb{F}_p$ 上で $J^4\{(I/J)^4+8(I/J)^3+12(I/J)^2+16(I/J)+4\}=0$ となる．ゆえに，$I/J \equiv \lambda$, $I \equiv \lambda J \pmod p$ となる λ が存在する．以上より，$I \equiv \lambda J \pmod p$ となる I, J を動かして計算をすればよい．また，次の補題を得る．

補題 9. I, J を $p \nmid \gcd(I,\ J)$ を満たす整数とする．$p \mid I^4+8I^3J+12I^2J^2+16IJ^3+4J^4$ を満たすならば，$\mathbb{F}_p$ 上の4次方程式 $X^4+8X^3+12X^2+16X+4=0$ の根の一つ λ を用いて $I \equiv \lambda J \pmod p$ となる．

系. p を $p \equiv 1 \pmod 8$ を満たす素数とする．このとき，$\mathbb{F}_p$ 上の4次方程式 $X^4+8X^3+12X^2+16X+4=0$ に解が存在しなければ，$X^4+p^2Y^4=2Z^2$ に自明でない解は存在しない．

この先，$\mathbb{F}_p$ 上の4次方程式 $X^4+8X^3+12X^2+16X+4=0$ に解が存在する条件を考察する．

v,w を $p=w^2-2v^2$ を満たす自然数とすると，$(A+B,B,Y)=(w,v,1)$ は $pY^2=A^2-B^2+2AB=(A+B)^2-2B^2$ の解となる．補題8を適用すると，$pY^2=A^2-B^2+2AB$ の解をパラメーター K,L を用いて，

$$A+B=-wK^2+4vKL-2wL^2,\ B=vK^2-2wKL+2vL^2,\ Y=K^2-2L^2 \tag{38}$$

と表示でき，$v(A+B)+wB=-2pKL \equiv 0 \pmod p$ となる．ここで，K, L を用いた解と I, J を用いた解とで同じ解を求めることができるので，I, J を用いたパラメータ表示でも $v(A+B)+wB \equiv 0 \pmod p$ を満たす．これより，$v(I^2+4IJ+2J^2)+w(2IJ) \equiv 0 \pmod p$ となる．さらに，$p \nmid v$ より，両辺を v 倍して，$p=w^2-2v^2$ を用いて整理すると

$$\{vI+(2v+w)J\}^2-4(v^2+vw)J^2 \equiv 0 \pmod p \tag{39}$$

を得る．よって，$(\frac{v^2+vw}{p})=1$ のとき (39) の左辺は1次式に分解できる．なお，$(—)$ で平方剰余記号を表すとする．次に，$p=(-w)^2-2v^2$ を用いて同じ議論を繰り返すと，

$$\{vI+(2v-w)J\}^2-4(v^2-vw)J^2 \equiv 0 \pmod p \tag{40}$$

を得る．ここで，$(\frac{v^2+vw}{p}) = 1$ となるとき，$(\frac{v^2+vw}{p})(\frac{v^2-vw}{p}) = (\frac{v^4-v^2w^2}{p}) = (\frac{-v^4}{p}) = 1$ より，$(\frac{v^2-vw}{p}) = 1$ となり，(39) の左辺も1次式に分解できる．よって，$(\frac{v^2+vw}{p}) = 1$ のとき，q_1, q_2 を $q_1^2 \equiv 4(v^2+vw) \pmod p$, $q_2^2 \equiv 4(v^2-vw) \pmod p$ とすると，

$$\begin{aligned}
&\{vI+(2v+w+q_1)J\}\{vI+(2v+w-q_1)J\}\{vI+(2v+w+q_1)J\}\{vI+(2v-w-q_2)J\}\\
\equiv&\{v^2I^2+(4v^2+2vw)IJ+2v^2J^2\}\{v^2I^2+(4v^2-2vw)IJ+2v^2J^2\}\\
\equiv&v^4(I^4+8I^3J+12I^2J^2+16IJ^3+4J^4) \pmod p
\end{aligned}$$

が成り立つ．以上より，次の補題を得る．

補題 10. p を $p \equiv 1 \pmod 8$ を満たす素数，v, w を $p = w^2 - 2v^2$ を満たす自然数とする．$(\frac{v^2+vw}{p}) = 1$ となるときに限り，$\mathbb{F}_p$ 上の4次方程式 $X^4+8X^3+12X^2+16X+4=0$ の解

$$-v^{-1}(2v+w \pm q_1),\ -v^{-1}(2v-w \pm q_2) \tag{41}$$

が存在する．なお，q_1, q_2 を $q_1^2 \equiv 4(v^2+vw) \pmod p$, $q_2^2 \equiv 4(v^2-vw) \pmod p$ とする．

注意. 4次剰余や $\mathbb{Z}(\sqrt{2})$ 上の相互法則を利用して $(\frac{v^2+vw}{p}) = 1$ となる条件を考察すると，$p = c^2+64d^2$ ($c \equiv \pm 1 \pmod 8$) または $p = c^2+16d^2$ ($c \equiv \pm 3 \pmod 8, d$: odd) のとき，$\mathbb{F}_p$ 上 $X^4+8X^3+12X^2+16X+4$ は1次式の積に分解されることがわかる．

注意. $p = 113$ $(= 7^2+64)$ のとき，$\mathbb{F}_p$ 上の4次方程式 $X^4+8X^3+12X^2+16X+4=0$ の解が存在するが，$p = 113$ は合同数でないことが知られている．

6．計算結果

この方法で合同数と確定したのは $p = 67993, 82793, 88721, 89897, 90697, 96329$ である．特に，$p = 67993$ と $p = 90697$ の場合の計算結果は，次のようになった．

$p = 67993$：不定方程式 $X^4+p^2Y^4 = 2Z^2$ の解は $I = 1609946, J = 7476759$ のとき，

$$X = -54605962082623, Y = 304767042623, Z = 4938388086514727907009866005$$

となる．このとき，面積 $p = 90697$ の直角三角形の3辺の長さ $L_1 < L_2 < L_3$ は，

$$L_1 = \frac{154964794869511991016364811212379267622458334369861633 84}{821851363916112011222191551321803663729075549559146 45}$$

$$L_2 = \frac{558801397867482039790304701490233965079310338411750445748 5}{774823974347559955081824056061896338112291671849308169 2}$$

$$L_3 = \frac{474688345994108801212424611421273538026149757673000254610200182190473225849975684763911946535388201584361834897}{6367901401124447342909307812553471765646252148364895278021279391488382780789387740895335680087804885641793 40}$$

となる．

$p = 90697$：不定方程式 $X^4 + p^2Y^4 = 2Z^2$ の解は，$I = 6347098, J = 55609047$ のとき，

$$X = -3072223281737407, Y = 12570268898441, Z = 12134025694162502899973688123925$$

となる．このとき，面積 $p = 90697$ の直角三角形の3辺の長さ $L_1 < L_2 < L_3$ は，

$$L_1 = \frac{581482422041543769038062251062579026771798898937220042662504 24}{468599967635178232454908061618885457685324423336910158201475}$$

$$L_2 = \frac{425006112646077601489627964646480543556858692233877406183991780 75}{290741211020771884519031125531289513385899449468610021331252 12}$$

$$L_3 = \frac{199874123785463492083705059193886160707546958785315628813358136213973626596819091936855051458442067219466375630946906415507 37}{136241322074546229918119117918228160268457338019388480433932954946666011387528197275806909351283400915310486134748980877 00}$$

となる．

7．その後の発展

松野一夫により，71,473が合同数であることの確認が，シドニー大学の計算代数グループによって開発が行われているソフトウェア Magma に搭載されている FourDescent コマンド等を用いることで行われた．その後の松野による計算で，百万以下の合同数を全て決定されている．なお，この結果の詳細は松野による Web サイト [8] に記載されている．

参考文献

[1] J. B. Tunnell: *A classical Diophantine problem and modular forms of weight 3/2*, Invent. math. **72** (1983), 323-334.

[2] K. Noda and H. Wada: *All congruent numbers less than 10000*, Proc. Japan Acad., **69A** (1993), 175–178.

[3] F. R. Nemenzo: *All congruent numbers less than 40000*, Proc. Japan Acad., **74A** (1998), 29–31.

[4] S. Komoto, T. Watanabe and H. Wada: *42553 is a congruent number*, Proceedings of the 6-th Symposium on Algebra and Computation, (2006), 1–6. (ftp://tnt.math.metro-u.ac.jp/pub/ac05/wada/wada.pdf).

[5] N. Koblitz: *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, GTM, 1984.

[6] J. H. Silverman and J. Tate: *Rational Points on Elliptic Curves*, Springer-Verlag, UTM, 1992.（足立恒雄，木田雅成，小松啓一，田谷久雄 訳：楕円曲線論入門，シュプリンガー・フェアラーク東京，1995）．

[7] N. D. Elkies: *On* $A^4 + B^4 + C^4 = D^4$, Math. Comp., **51** No. 184 (1988), 825–835.

[8] 松野 一夫：合同数について．(http://www.comp.metro-u.ac.jp/ matsuno/congr/congruent-j.htm).