早稲田大学大学院理工学研究科

博 士 論 文 概 要

論 文 題 目

Some exponential Diophantine equations

いくつかの指数型不定方程式

申 請 者

寺井 伸浩

Nobuhiro Terai

数学専攻・代数学研究

平成4年12月

Diophantine problems（不定方程式の整数解や有理数解を求める問題）は、幾何学と同様、ギリシャ時代以来の長い歴史をもち、現在まで多くの研究者を引きつけてきた。特に、Fermat 方程式 $x^n+y^n=z^n$ や Catalan 方程式 $x^m-y^n=1$ などの指数型方程式については、詳細に研究されてきた。

本論文では、次の3つの指数型不定方程式；

(1) $q_p(m)=x^l$

(2) $x^2+q^m=p^n$

(3) $x^4+dy^4=z^p$

について研究する。本論文は、3章より構成されている。以下に、各章の概要を述べる。

第1章では、不定方程式(1)について考察する。p を奇素数とし、m を p で割り切れない正の整数とする。このとき、Fermat 商 $q_p(m)$ を、$q_p(m)=(m^{p-1}-1)/p$ で定義する。Fermat 商 $q_p(m)$ は、Fermat の小定理より整数であり、整数論では非常に興味深い数である。例えば、Fermat の大定理の Case I が素指数 p に対して誤りならば、$m \leqq 103$ のすべての素数 m に対して $q_p(m)\equiv 0 \pmod p$ が成り立つことが知られている。Lucas は、$q_p(2)$ が平方数となるのは $p=3$、7 に限ることを証明した。この Lucas の定理を一般化するために、不定方程式(1)（l：素数）が解（p, m, x, l）を持つかどうか考察した。この章の主要な結果は、以下の通りである。

［定理1］不定方程式 $q_p(m)=x^2$ $(p>3)$ は、m が奇数ならば唯一つの解 $(p, x, m)=(5, 3, 4)$ を持つ。

［定理2］Catalan 予想が成り立つと仮定する。このとき、$p>3$ かつ m が偶数ならば、不定方程式 $q_p(m)=x^l$ は唯一つの解 $(p, m, x, l)=(7, 2, 3, 2)$ を持つ。

［定理3］m を奇数（$\geqq 3$）とする。

(a) $m<50$ ならば、不定方程式 $q_p(m)=x^3$ は唯一つの解 $(p, m, x)=(3, 5, 2)$ を持つ。

(b) $m\pm 1 \not\equiv 0 \pmod{2^{l-2}}$ ならば、不定方程式 $q_p(m)=x^l$ $(l>3)$ は解を持たない。

定理1の証明は、ある2次の不定方程式に関する Ljunggren, Nagell の定理と2次体の類数に関してよく知られた結果を用いる。Catalan 予想に関する結果と定理1, 2より、$q_p(m)=x^2$ $(p>3)$ は完全に解けたことになる。Catalan 方程式の解の個数が高々有限個であることは、Tijdemen により Baker 理論（代数的数の対数の1次形式の絶対値の評価に関する理論）を用いて示された。従って、定理2より不定方程式 $q_p(m)=x^l$ ($p>3$, m：偶数）の解の個数は高々有限個である。

定理3の(a), (b)は、各々ある3次の不定方程式に関する Ljunggren, Nagell の定理と Störmen の定理を用いて示される。定理3の(a), (b)の結果を合わせれば、不定方程式 $q_p(m)=x^l$ ($m\equiv 3, 5 \pmod 8$ かつ $m<50$) の解は $(p, m, x, l)=(3, 5, 2, 3)$ であることがわかる。定理3の系として、不定方程式 $q_p(r)=x^r$ (r：奇数 $\geqq 3$) は解を持たないことを得る。

第2章では、不定方程式(2)について考察する。1956年に、Sierpinski は、不定方程式 $3^x+4^y=5^z$ の唯一つの正の整数解は $(x, y, z)=(2, 2, 2)$ であることを示した。また、Jeśmanowicz は、

$$5^x+12^y=13^z,\quad 7^x+24^y=25^z,\quad 9^x+40^y=41^z,\quad 11^x+60^y=61^z$$

の各方程式の唯一つの正の整数解は $(x, y, z)=(2, 2, 2)$ であることを示し、a, b, c が Pythagorean triples, つまり $a^2+b^2=c^2$ を満たす正の整数解ならば、不定方程式 $a^x+b^y=c^z$ の唯一つの正の整数解は $(x, y, z)=(2, 2, 2)$ であることを予想した。

Jeśmanowicz の予想の類似として、次のような予想を考える。

［予想］正の整数 a, b, c は $a^2+b^2=c^2$ を満たし、$(a, b, c)=1$ で a は偶数とする。この時、$x^2+b^m=c^n$ の唯一つの正の整数解は $(x, m, n)=(a, 2, 2)$ である。

この章では、b、c が奇素数 p, q、つまり $q^2+1=2p$ のとき、$x^2+q^m=p^n$ が、$(p-1, 2, 2)$ 以外に正の整数解を持つかどうかを考える。その時、次の定理を得た。

［定理］奇素数 p、q は次の条件を満たすとする。

(i) $q^2+1=2p$　　(ii) $q\equiv 1 \pmod 4$ ならば、$d=1$ または偶数

ここに、d は虚2次体 $\mathbb{Q}(\sqrt{-q})$ の ideal 類群における (p) の prime divisor の位数である。この時、不定方程式

(2) $x^2+q^m=p^m$

の唯一つの正の整数解は $(x, m, n)=(p-1, 2, 2)$ である。

定理の証明の方針は、以下の通りである。まず、証明は次の3つの場合：

(a) n：偶数　(b) m：偶数かつ n：奇数　(c) m, n：奇数

に分かれる。(a)の場合には、Störmen と Ljunggren の定理より、不定方程式(2)は唯一つの正の整数解 $(x, m, n)=(p-1, 2, 2)$ を持つことがすぐに従う。(b)の場合には、(2)の両辺を虚2次体 $\mathbb{Q}(i)$ で分解して得られる式を、ある数を法として考え、その両辺の実部又は虚部を比較することによって容易に矛盾を得る。一方、(c)の場合には、いくつかの技巧を必要とする。このとき、$q\equiv 1 \pmod 4$ となる。(2)の両辺を虚2次体 $\mathbb{Q}(\sqrt{-q})$ で分解し、ある二次の線型の数列に関する結果と仮定(ii)を用いることにより、次の命題を得る。

［命題］r は固定された正の整数とする。不定方程式 $x^2+q^{2r+1}=p^n$ が解 (x, n) を持つならば、不定方程式 $x^2+q^{2r-1}=p^n$ もまた解 (x, n) を持つ。

しかし、条件(i)より、不定方程式 $x^2+q=p^n$ は解 (x, n) を持たない。従って、不定方程式(2)は解を持たない。（この証明法は、一種の（条件付）"降下法"である。）

条件(ii)に関して注意しておくと、$q^2+1=2p$, $q\equiv 1 \pmod 4$, $\left(\frac{-q}{p}\right)=1$ を満たす (p, q) の組は、$q<2000$ の範囲で10組あるが、これらはすべて $d=1$ または偶数である。

最後に、予想における b, c が $b^2+1=2c$, $b<20$, $c<200$, b, c：奇数であるとき，これらすべての場合に、予想がすべて成り立つことを確かめた。

第3章では、不定方程式(3)について考察する。dを平方因子を持たない正の整数，pを奇素数とし、$p^*=(-1)^{(p-1)/2}\cdot p$とおく。Powellは、次を示した。

［定理1］ (a) $p \not\equiv \pm 1 \pmod 8$ ならば、不定方程式 $x^4+y^4=z^p$ は，$(x, y)=1$ $p \nmid xy$ なる整数解 x, y, z を持たない。

(b) 不定方程式 $x^4-y^4=z^p$ は、$(x, y)=1$, $p \nmid xyz$ なる整数解を持たない。

(a)はGauss整環 $\mathbb{Z}[i]$ を、(b)はTerjanianによる偶数冪に対するFermatの大定理の第一の場合の証明に用いられたJacobi symbolに関するある結果を用いて証明される。

定理1, (a)を一般化するために，TeraiとOsadaの共著の論文では不定方程式 $x^4+dy^4=z^p$ が整数解を持つかどうかを考え、次を得た。

［定理2］ pを奇素数，$d \not\equiv 3 \pmod 4$ を平方因子を持たない正の整数、$h(-d)$を虚2次体 $\mathbb{Q}(\sqrt{-d})$ の類数とする。$p \not\equiv \pm 1 \pmod 8$ かつ $p \nmid h(-d)$ ならば、不定方程式

$$x^4+dy^4=z^p \tag{3}$$

は，$(x, y)=1$, $p \nmid xy$, y：偶数なる整数解 x, y, z を持たない。

(3)で $d=1$ ならば、$p \nmid h(-1)$ で y：偶数としてよい。従って，定理2は定理1の(a)の一般化を与える。定理2の証明は，次の2つの事実に基づいている：

(i) a, b を互いに素な反対の偶奇数をもつ整数，cを整数とする。この時，

$$a^2+db^2=c^p \Longrightarrow a+b\sqrt{-d}=(u+v\sqrt{-d})^p \tag{4}$$

がある整数 u, v に対して成り立つ。

(ii) 奇数の平方数 $\equiv 1 \pmod 8$。

一般には、(4)が成立すること（特に、$d<0$ に対して）を示すのは難しい。Adachiは、ある条件のもとで(4)が $d=-p^*$ に対して成立することを示した。このAdachiの結果とTerjanianのアイデアを応用して得られるRotkiewiczの結果を用いて，次の定理を得た。

［定理3］ $p \equiv 1 \pmod 4$ かつ $B_{(p-1)/2} \not\equiv 0 \pmod p$ ならば、不定方程式

$$x^4-py^4=z^p \tag{5}$$

は、$(x, y)=1$、$p \mid y$, x：偶数なる整数解 x, y, z を持たない。

［定理4］不定方程式 $x^4+3y^4=z^3$ は、$(x, y)=1$ なる整数解 x, y, z を持たない。

$B_{(p-1)/2} \equiv 0 \pmod p$ の例は，$p<6270713$ に対しては知られていない。不定方程式(5)は，$p \nmid y$ かつ x：奇数なら解を持つことがある。例えば，$(x, y, z, p)=(3, 2, 1, 5)$ である。また，不定方程式 $x^4+3y^4=z^3$ は、$(x, y) \neq 1$ ならば多くの解を持つ。例えば、$(x, y, z)=(2a^3, 2a^3, 4a^4)$, $(7a^3, 14a^3, 49a^4)$ である。

定理3の証明法を用いれば、$x^4-p^3y^4=z^p$ に対しても定理3と同様な定理が成立することが分かる。