# オイラーの数論

高瀬正仁

目次



## 緒言

1621年，フランスの数学者バシェ(Claude Gaspar Bachet de Méziriac，1581-1638)は，三世紀のギリシアの人ディオファントスの作品と伝えられる数学書「アリトメチカ」をラテン語に翻訳し，ギリシア語の原文とともに配列した対訳書を作り，刊行した．バシェと同じフランスの数学者フェルマ(Pierre de Fermat，1601年8月17日-1665年1月12日)はバシェの翻訳書を入手し，欄外に48個の命題を記入した．これが名高い「欄外ノート」である．1637年ころと推定される出来事である．

フェルマの「欄外ノート」が実際に書き込まれている書物そのものは失われたが，1670年，フェルマの息子のサミュエル・ド・フェルマ(Samuel de Fermat, 1630-1690)がバシェの翻訳書を復刊し，その際，父フェルマの「欄外ノート(marginal note)」を収録した．オイラー(Leonhard Euler, 1707-1783)もラグランジュ(Joseph-Louis Lagrange, 1736-1813)もこの復刻版を読んでフェルマの書き込みを認識したのである．

数論に寄せるフェルマの関心は「欄外ノート」以降も失われず，友人知人に宛てた書簡の中で幾度も繰り返して数論に言及した．その様子をフェルマ全集から拾うと，一番日付の早い手紙は1640年12月25日付のメルセンヌ宛書簡で，ここには「直角三角形の基本定理」，すなわち

《4の倍数よりも1だけ大きい素数はどれもみな二つの平方数で作られる．》

という命題と，

《フェルマ数，すなわち$2^{2^x}+1$，$x=0$，1，2，3 … という形の数はどれもみな素数である．》

という命題が記されている．数論の命題が読み取れる最後の手紙は歿年の7年前の1658年6月付のデグビィ宛書簡で，ここには再び「直角三角形の基本定理」が登場する．主な文通相手は下記の6名である．

カルカヴィ(Pierre de Carcavi, ?-1684)

ディグビィ(Kenelm Digby, 1603-1665)

フレニクル(Bernard Frenicle de Bessy, 1605-1675)

メルセンヌ(Marin Mersenne, 1588-1648)

パスカル(Blaise Pascal, 123-1662)

ロベルヴァル(Gilles Personier de Roberval, 1602-1675)

数論を語るフェルマの言葉には命題の言明が認められるのみで，証明は附されていない．この状勢を受けて，オイラーは証明の欠如したフェルマの諸言明に証明を与えようと試みるとともに，フェルマを越えて新たな地平を切り開こうとする息の長い試みを続けた．近代数論はこのオイラーの営為の中から生れたのである．

オイラーの全集は全88巻の予定で企画され，刊行が続けられているが，現在もなお未完結である．全体は5系列に分かれ，第一系列(全29巻，30冊)が数学著作集で，これは完結した．この第一系列の巻２から巻５までの全４冊が「アリトメチカ論文集」に割り当てられていて，数論に関するオイラーのすべての論文が集められている．エネストレームによる番号付けに従って数えると，収録されている論文は全部で99篇．ただし，そのうち２篇はオイラーの息子アルブレヒト・オイラーが書いたものである．また論文[708]aは[708]に準じるのでひとまず除外すると，残るのは96篇になる．各論文のテーマに応じて区分けすると，概要は次のようになる．

Ⅰ．　不定解析(1)　一次不定方程式の解法

論文1篇

[E 36]

Ⅱ．　不定解析(2)　二次不定方程式の解法

論文7篇

[E 29] [E 279] [E 323] [E 452] [E 454] [E 556] [E 559]

Ⅲ．　不定解析(3)　一般の不定方程式の解法

論文37篇

[E 98] [E 167] [E 253] [E 255] [E 270] [E 405] [E 427] [E 428] [E 451] [E 466] [E 474]

[E 515] [E 523] [E 560] [E 696] [E 702] [E 713] [E 716] [E 732] [E 739] [E 753] [E 754] [E 755] [E 763] [E 764] [E 769] [E 772] [E 773] [E 774] [E 775] [E 776] [E 777] [E 778] [E 793] [E 796] [E 797] [E 799]

不定解析の論文だけで45篇になり，オイラーのアリトメチカの全論文のほぼ50パーセントに達する．

Ⅳ．　素数の形状理論

論文8篇

[E 164] [E 228] [E 241] [E 256] [E 272] [E 598] [E 610] [E 744]

Ⅴ．　冪剰余の理論(1)　フェルマの小定理とその一般化

論文4篇

[E 26] [E 54] [E 271] [E 54]

Ⅵ．　冪剰余の理論(2)　冪剰余の一般的考察

論文8篇

[E 134] [E 242] [E 262] [E 449] [E 552] [E 554] [E 557] [E 792]

Ⅶ．　数の表示理論

論文3篇

[E 445] [E 566] [E 586]

Ⅷ．　親和数

論文3篇

[E 100] [E 152] [E 798]

Ⅸ．　数の分割の理論

論文8篇

[E 158] [E 175] [E 191] [E 243] [E 244] [E 394] [E 541] [E 542]

Ⅹ．　素数の判定法

論文10篇

[E 283] [E 369] [E 467] [E 498] [E 699] [E 708] [E 715] [E 718] [E 719] [E 725]

Ⅺ．　その他の諸論文

論文7篇

[E 461] [E 558] [E 591] [E 596] [E 683] [E 748] [E 758]

冪剰余の理論は冪指数が2の場合には平方剰余の理論になるが，この領域においてオイラーは平方剰余相互法則を発見した．ただし証明は欠けている．一般の二次不定

方程式の解法は，$A+Bt^2=u^2$ ($A$，$B$ は定量を表し，$t$，$u$ は不定量を表す)という特別のタイプの方程式の解法に帰着されていく．オイラーはこの後者の方程式を整数の範囲で解こうと試みた．素数の形状理論は直角三角形の基本定理を雛形とする理論である．今，$p$ は「4の倍数よりも1だけ大きい素数」とすると，$p=4n+1$ という形に表示される．これは $p$ の線型的形状である．そうして直角三角形の基本定理によれば $p=x^2+y^2$ という形に表示される．これは $p$ の平方的形状である．すなわち，同一の素数 $p$ の線型的形状 $4n+1$ と平方的形状 $x^2+y^2$ が比較され，等値されたのである．このような比較と等値の姿が組織的に解明されて，素数の形状理論が形成された．この呼称の背景にはピタゴラスの定理が控えていて，直角三角形の基本定理は通約可能な三辺をもつ直角三角形の形を教えている．答は，「斜辺の長さが4で割ると剰余が1になる素数」であること．不定解析の見地から見ると，二次不定方程式

$$x^2+y^2=n$$

が整数の範囲で解けるために $n$ に課される条件が明らかにされたと言える．答は「$n$ を4で割ると剰余が1になる素数」であること．すなわち，素数の形状理論は不定解析の一区域を形成すると言えるのである．

オイラーの数論研究を継承したのはラグランジュとルジャンドルである．ラグランジュはオイラーの研究を補足改訂し，オイラーが開いた数論的世界を大きく拡大した．ルジャンドルはオイラーとラグランジュの数論研究の成果を集大成する役割を担い，1798年の著作「数論の試み」の中で全容の描写を試みた．オイラー，ラグランジュ，ルジャンドルへの手により，フェルマが表明した個々の諸命題を結ぶ有機的な相互関連が次第に明らかにされて，「数論」が形成されたのである．フェルマの「欄外ノート」が現れたと推定される1637年ころから，ルジャンドルの著作「数論のエッセイ」が刊行された1798年まで，おおよそ160年ほどの間に繰り広げられた小さな物語である．

本稿では平方剰余の理論と平方剰余相互法則，フェルマの小定理，$A+Bt^2=u^2$ というタイプの二次不定方程式の解法理論，それに素数の形状理論の描写に主眼を置いてオイラーの数論を叙述する．高次冪剰余の理論がオイラーの数論的世界の中で占める位置は特異である．この理論の意味を解明するためには，ガウスによる高次冪剰余相互法則の究明との関連のもとで精密に考察しなければならないが，他の機会を俟ってもう一篇の大きな論説を書き，ガウスの数論との対比のもとで詳細に論じることにしたいと思う．

## 1. フェルマの言葉より

オイラーの数論の叙述の契機を，数論に関するフェルマの言葉に求めたいと思う．不定解析，ペルの方程式，フェルマの小定理，二次形式の約数の形状の観察，素数の

形状理論に分けて，数論を語るフェルマの言葉を紹介する．

不定解析

不定解析の領域で語られたフェルマの言葉は三つ記録されている．一つは後に「フェルマの大定理」「フェルマの最後の定理」などと呼ばれることになった命題で，今日のいわゆるフェルマ方程式 $x^n+y^n=z^n$ の整数解は，$n\geqq 3$ の場合，自明な解のほかには存在しないことを主張する命題である．「欄外ノート2」(フェルマ全集，巻1，p.291)の記事がこれは該当する．もう一つは「不定方程式 $x^4-y^4=x-y$ は解ける(数域は有理数域)」という高次不定方程式論の命題で，これは「欄外ノート11」(同上，p.300-301)の記事である．

第三番目の言葉はいわゆる「ペルの方程式」に関するもので，

> 《与えられた非平方数を $a$ とし，求めたい平方数を $y^2$ で表すとき，量 $ay^2+1$ が平方数になるようにしたい．》(この主旨の言葉はフェルマ全集，巻2，p.335に出ている．フェルマの言葉をそのまま写すと次の通り．「ある任意の非平方数が与えられたとせよ．このとき，その与えられた数にある平方数を乗じて1を加えると，その積がまた平方数になることがある．そのような性質を備えた平方数は無数に存在する．」)

というのである．ここで要請されている平方数を $x^2$ で表すと，結局，問題は，ペルの方程式と呼ばれる不定方程式

$$ay^2+1=x^2 \quad (a>0)$$

を解くこと，すなわちこの方程式を満たす二つの整数 $x$ と $y$ を求めることに帰着する．

フェルマはイギリスの数学者たちに向けてペルの方程式を提示し，解法を求めて挑戦した．フェルマ自身の解答は伝わっていない．この問題は1657年2月(推定)に書かれた第二番目の挑戦状に記されていたもので(フェルマ全集，巻2，p.334-335)，すでにフェルマの最晩年の出来事である．1658年6月(月は推定)のディグビィ宛書簡(同上，p.402-408)．1658年4月7日付のディグビィ宛書簡(同上，p.374-378)．1659年8月のカルカヴィ宛書簡(同上，p.431-436)．

フェルマの小定理

フェルマの小定理というのは，

> 《$p$ は素数，$a$ は $p$ で割り切れない整数とすると，合同式 $a^{p-1}\equiv 1 \pmod{p}$ が成立する．》

という命題のことで，1640年10月18日付フレニクルのフェルマ宛書簡(同上，p.206-212)に記録されている．「フェルマの小定理」という呼称は「フェルマの大定理」

と対をなすものだが，後年の呼称である．

フェルマ数

$2^{2^x}+1$，$x=0$，1，2，3 ･･･という形の数，すなわち

3，5，17，257，65537，4294967297，18446744073709551617 ･･･

と続いていく数はどれもみな素数である．1640年8月(月は推定)のフレニクル宛書簡(同上，p.205-206)．1640年10月18日付フレニクル宛書簡(同上，p.206-212)．1640年12月25日付メルセンヌ宛書簡(同上，p.212-217)．1654年8月29日付パスカル宛書簡(同上，p.307-310)．今日，$2^{2^x}+1$という形の数は「フェルマ数」と呼ばれることがある．オイラーは，すべてのフェルマ数は素数であるというフェルマの言葉はまちがっていることを，反例を挙げて明らかにした([E 54]．オイラーは4294967297の約数641を発見した)．

二次形式の約数の形状の観察

命題三つ．

1°．$a^2+2b^2$という形の平方数の平方根はやはり$x^2+2y^2$という形である．「欄外ノート45」(フェルマ全集，巻1，p.340-341)．

2°．互いに素な二つの平方数の和として書き表わされる数は，$4x-1$型のいかなる素数でも割り切れない．1640年8月のロベルヴァル宛書簡(フェルマ全集，巻2，p.202-205)．

これによれば，互いに素な二つの平方数の和でありうる数の約数は，2は別にすると，$4x+1$型でしかありえないことになる．この事実はオイラーが証明した([E 134])

3°．$a^2-2$という形の数は$x^2+2$という形のいかなる素数でも割り切れない．1640年10月18日付のフレニクル宛書簡(フェルマ全集，巻2，p.206-212)．

これは二次形式の約数の平方的形状について語る言葉であり，二次形式$a^2-2$の素因子の線型的形状が確立されれば明らかになる事実である．ラグランジュが示したように(ラグランジュ全集，巻3，p.714-715)，一般に二次形式$t^2-2u^2$の約数の平方的形状は同じく$y^2-2z^2$であるから，$a^2-2$の平方的約数は$x^2+2$という形ではありえない．

オイラーとラグランジュにより明らかにされたことによれば，「二次形式の約数の形状」の観察は素数の形状理論と親密な関係で結ばれている．しかしフェルマの段階では，このような関連が存在することはまだわからない．

素数の形状理論

素数の形状理論に所属するフェルマの言葉は五つある．

1°．　直角三角形の基本定理．「欄外ノート7」(フェルマ全集，巻2，p.293-297)．1640年12月25日付のメルセンヌ宛書簡(同上，p.212-217)．1641年6月15日付のフレニクル宛書簡(同上，p.221-226)．1658年6月(月は推定)のディグビィ宛書簡(同上，p.402-408)．1659年8月のカルカヴィ宛書簡(同上，p.431-436)．

1641年6月15日付のフレニクル宛書簡の中に，

「直角三角形の基本定理というのは，4の倍数よりも1だけ大きい素数はどれもみな二つの平方数で作られる，というものです．」(同上，p.221)

という言葉が出ている．「直角三角形の基本定理」という呼称はこのフェルマの言葉に由来するのである．逆は明らかである．すなわち，二つの平方数の和の形に表される素数は必ず「4の倍数よりも1だけ大きい」．また，ここに挙げたフェルマの言葉には明記されていないが，「4の倍数よりも1だけ大きい素数」すなわち$4n+1$型の素数を二つの数の和として表示する仕方がただひと通りに限定されることも重要な事実である．

直角三角形の基本定理に関連して，次に挙げる二つの言葉も重要である．

(1-1) 3で割り切れるが9では割り切れない数，すなわち$9n\pm3$という形の数は二つの平方数の和ではありえない．一般に有理数の平方数を許容することにしてもなお不可能である．「欄外ノート25」(フェルマ全集，巻1，p.312-313)．

(1-2)　$4n-1$という形の数は決して二つの平方数の和ではありえない．一般に有理数の平方数を許容することにしてもなお不可能である．1640年8月(月は推定)のロベルヴァル宛書簡(フェルマ全集，巻2，p.202-205)．「欄外ノート7」(フェルマ全集，巻1，p.293-297)．

2°．$8n+1$型および$8n-1$型の素数は$y^2-2z^2$という形に書き表わされる．1641年8月2日付および同年9月6日付のフレニクルのフェルマ宛書簡(二通の手紙の全文はそれぞれフェルマ全集，巻2　，p.226-232およびp.232-242)．この二通の手紙はフェルマが書いたものではないが，ここに見られる記述を通じて，フェルマ自身もまた上記の命題に気づいていた様子がうかがわれる．

3°．$3n+1$型の素数(それは必然的に$6n+1$型である)はどれもみな$y^2+3z^2$という形である．1654年9月25日付パスカル宛書簡(同上，p.310-314)．1658年のディグビィ宛書簡(同上，p.402-408)．

4°．$8n+1$型もしくは$8n+3$型の素数はどれもみな$y^2+2z^2$という形である．1654年9月25日付パスカル宛書簡．1658年のディグビィ宛書簡．

5°．$20n+3$もしくは$20n+7$という形の二つの素数の積は$y^2+5z^2$という形である．1658年のディグビ宛書簡．

6°．$4n+3$という形であって，しかも末尾の数が3もしくは7であるような二つの素数の積はつねに$y^2+5z^2$という形である．特に，そのような数の各々の平方もまた$y^2+5z^2$という形である．1658年のディグビィ宛書簡．

$4n+3$型の数であって，しかも末尾の数字が3もしくは7であるものは必ず

$20n+3$ もしくは $20n+7$ 型であるから，この言葉6°は前の言葉5°と同等である．実際，$4m+3$ において次々と $m=5n$，$5n+1$，$5n+2$，$5n+4$ を代入すると，$4m+3$ は

$$20n+3,\ 20n+7,\ 20n+11,\ 20n+15,\ 20n+19$$

となる．これらのうち，末尾の数字が3もしくは7であるものは $20n+3$ と $20n+7$ のみである．

命題2°から5°までの四つの命題は，直角三角形の基本定理から派生した変奏曲である．直角三角形のような図形的な意味合いはもう失われ，純粋に数の形状にのみ関心が寄せられている．

## 2. 二次不定方程式と平方剰余の理論

二次不定方程式の解法理論は，ペルの方程式 $x^2-Ay^2=1$ を語るフェルマの言葉とともに端緒が開かれていった．フェルマの挑戦を受けて，イギリスの数学者ブラウンカー(William Brouncker, 1620- 1684)が解答を与えることに成功し，ウォリス(John Wallis, 1616- 1703)が著作『代数学』(*Treatise on Algebra,* 1685)の中でブラウンカーの解答を公表した．オイラーの著作『代数学』(*Vollständige Anleitung zur Algebra,* 1770, 全2巻)巻2にもほぼそのまま引用されている．したがって本当は「ペルの方程式」ではなく「フェルマの方程式」「ブラウンカーの方程式」または「ウォリスの方程式」と呼ぶほうがよいと思われるが，オイラーの論文[E 29]「あるディオファントス問題の整数による解決について」([L.Euler 2])には「ペルとフェルマの方法」への言及があるし(オイラー全集 I -2, p.12)，論文は[E323]「ペルの問題に解決を与える新しいアルゴリズムについて」([L.Euler 14])には「ペルの問題」「ペルの解法」という言葉が見られる．これが「ペルの方程式」という用語の由来であろう．ペル(John Pell, 1611- 1685)はイギリスの数学者である．オイラーはブラウンカーの解答をペルの解答と勘違いしたのではないかと推測されている．フェルマ自身，独自の解法をもっていたようで，1659年8月のフレニクル宛書簡に，「一般的な証明は無限降下法を適切に適用することにより見いだされる」(フェルマ全集，巻2, p.433)という言葉が出ているが，その証明の実体は伝わっていない．

ラグランジュは1769年の論文「アリトメチカの一問題の解決」([J. L.Lagrange 1])においてペルの方程式を取り上げてウォリスの解法に言及し，評価するとともに批判を加えた．この論文のタイトルに出ている「一問題」というのは，ペルの方程式を解く問題のことである．ラグランジュの見るところ，ブラウンカーの方法は一種の手探りにすぎず，確実に目的地に達するという保証はないし，はたして到達するかどうかも実はわからない．それに何よりも，大前提として解の存在証明を確立しなければなら

ないが，この論点は未解決である．そこでラグランジュは，方程式$x^2 - Ay^2 = 1$にはつねに整数解が存在することを証明するとともに，実際に解を求める確実な方法を提示したのである．それは，非有理量$\sqrt{A}$を連分数に展開する方法である．連分数展開のアイデアを導入したのはオイラーであり，ラグランジュはこれを踏襲した．

ラグランジュの数学全体の中で数論の占める割合は決して大きいとは言えないが，どの一篇を見ても完成度の高さは無類である．フェルマは二，三のスケッチを除いて証明を書き残さなかった．オイラーはフェルマの言明のいくつかを正しく証明し，機能的考察を通じて新たに発見した大量の命題を，証明を与えないまま公正に伝えた．ルジャンドルは証明の現場においてしばしば粗雑であった．これに対し，ラグランジュはガウスに匹敵するほどの洗練された理論構成を誇っている．

ラグランジュの不定方程式論は連分数展開の理論の上に築かれている．この理論は，数値方程式に関する二論文「数値方程式の解法について」([J. L. Lagrange 3])とその補足([J. L. Lagrange 4])，特に後者の論文において一般的な様式で記述されている．これらの二論文のテーマは整係数代数方程式の近似的解法であり，それ自体は数論とは無縁だが，不定方程式論と並んで，連分数展開の理論の土台の上に建設されるもう一つの理論である．

論文「数値方程式の解法に関する論文への補足」([J. L. Lagrange 4])において，ラグランジュはこう言っている．

> 周期的連分数はどれもみな，いつでも，ある二次方程式に帰着されるが，この事実はずっと以前から注目されてきた．だが，この命題の逆，すなわち，二次方程式の根はどれもみないつも必ず周期的な連分数の形に変形できることを証明した人は，私の知る限り皆無である．オイラー氏はペテルブルク科学アカデミー新紀要，巻11，に掲載されたすばらしい論文の中で，ある整数の平方根はつねに周期的な連分数の形に変形されることに気づいた．ただし，そうではあるが，この我々の定理の特別の場合にすぎない定理は，オイラー氏の手では証明されなかった．この定理は，我々が上に確立した諸原理の助けを借りてはじめて証明が可能になるのである．(ラグランジュ全集，巻2，p.615)

二次不定方程式の解法に連分数展開の理論を応用するというアイデアは，元来オイラーに胚胎していたことを明示する言葉である．言及されているオイラーの論文は[E323]を指す．

不定方程式の解はディオファントスの段階ではまだ有理数の範囲で探し求められていた．バシェはこの点を一歩を進めて整数解の探究を試みた．ただし，その対象は一次方程式に限定されていた．オイラーは二次不定方程式の整数による解法を探究し，可解条件を見つけようと試みた．オイラーの研究を踏まえ，ラグランジュは二次不定方程式の有理数による解法を求め，平方剰余の理論との関係を明らかにした．

一般の二次不定方程式

$$a x^2+b x y+c y^2+d x+e y+f=0$$

が提示されたとしよう．ここで$x$と$y$は不定量，$a$，$b$，$c$，$d$，$e$，$f$は正または負の与えられた整数である．この方程式から，まずはじめに

$$2 a x+b y+d=\sqrt{\left(b y+d\right)^2-4 a\left(c y^2+e y+f\right)}$$

が取り出される．表記を簡単にするために，右辺の平方根を$t$で表し，$b^2-4 a c=B$，$b d-2 a e=g$，$d^2-4 a f=h$と置くと，二つの方程式

$$2 a x+b y+d=t$$

$$B y^2+2 g y+h=t^2$$

が得られる．後者の方程式に$B$を乗じ，新たに$B y+g=u$，$g^2-B h=A$と置くと，提示された方程式は

$$A+B t^2=u^2$$

という形の方程式に変換されることがわかる．逆に，この変換方程式$A+B t^2=u^2$の有理数解$u$と$t$が見つかったなら，それらの値から，提示された方程式の有理数解$x$と$y$の値が取り出される．すなわち，

$$y=\frac{u-g}{B},\quad x=\frac{t-b y-d}{2 a}$$

となる．

ラグランジュはオイラーの二論文[E29][E279]に手がかりを得て，論文「二次不定問題の解決について」([J. L.Lagrange 2])において不定方程式$A+B t^2=u^2$の整数もしくは有理数による解法を究明した．不定方程式論には二つの本質的な論点がある．一つは，解が存在するか否かの判定をアプリオリに可能にしてくれる存在定理である．ラグランジュは，オイラーにはこの点の究明が不十分と指摘し，批判した．もう一つは，解の存在が保証された場合について，解を見つける具体的な手順を与えることである．ラグランジュはこれらの二論点を申し分なく追究した．

$A$，$B$のいずれかが平方数の場合には，簡単な因数分解を考えることにより，方程式$A+B t^2=u^2$の有理数解がすぐに見つかる．ただし整数解を求めるのはむずかしい．この場合の考察はすでにディオファントスの著作『アリトメチカ』に現れている．一般の場合，$A$が正で$B$が負の場合には試行錯誤を繰り返すことにより整数解を見つけることができる．というのは，$A+B t^2$は正であるから$|t|<\sqrt{-\frac{A}{B}}$．そこで$\sqrt{-\frac{A}{B}}$よりも小さい絶対値をもつ整数$t$(有限個しかない)をすべて書き並べ，それらの各々に対して，$A+B t^2$が平方数になるか否かを試せばよいからである．これで整数解は見つかるが，有理数解を求めようとすると，試すべき$t$の個数が無限になってしまうので，この方法は効果がない．すなわち，今度は整数解を求めることのほうが有理数解を求めることよりもむずかしくなってしまう．$A$と$B$がともに正の場合には，この手探りの手段も失われてしまう．二次不定方程式の解法をめぐって，オイラー以前に知られていた事柄はこれで全部である．

オイラーは二篇の論文[E29][E279]において方程式 $A = u^2 - Bt^2$ の整数解を探索したが，オイラーの考察は $B$ が正の場合に限定されていた．議論の根拠は $\sqrt{B}$ の連分数展開である．ディオファントスの方法は $B$ が平方数の場合に限定されていたから，オイラーは一歩を越えたと言えることになる．ラグランジュはなお一歩を進めて $B$ が負の場合へと踏み込んだ．

オイラーの論文[E279]を見ると，方程式 $A = u^2 - Bt^2$ が整数解をもつための条件が与えられている．それは，$A$ が

$$4nB + a^2 \quad \text{もしくは} \quad 4nB + a^2 - B$$

($n$ と $a$ は任意の整数)という形の素数であること，あるいは $A$ の素因子がそれぞれみなこれらのいずれかの形状であること，という条件である．この $A$ と $B$ に課された条件が方程式 $A = u^2 - Bt^2$ の整数解の存在を保証するというのがオイラーが書き留めた命題だが，証明は与えられなかった．そればかりか，オイラーは証明を見つけることはできなかったと打ち明けてさえいる．これを受けてラグランジュは証明を試みた末に，オイラーの命題が成立しないことを示す例を発見し，論文「整数により不定問題を解くための新しい方法」([J. L.Lagrange 5])において報告した (ラグランジュ全集，巻2，p.657)．それは，

$$101 = u^2 - 79t^2$$

という方程式である．この方程式を観察すると，101 は素数であり，$B = 79$，$a = 38$ および $n = -4$ と取れば，たしかに $4nB + a^2 - B$ という形になっている．ところがこの方程式は整数解をもたないのである．

オイラーが予測した命題の形を少し変型して，

> 《$4nB + \alpha$ という形の素数はどれもみな $u^2 - Bt^2$ という形である．ただし，$\alpha$ もまた $u^2 - Bt^2$ という同じ形の素数とする．》

というふうに表明したとしても，上記の同じ例 $101 = u^2 - 79t^2$ が教えてくれるように，まだ正しいとは言えない．なぜなら，$n = -2$ および $B = 79$ と取ると，素数 101 は

$$101 = 4nB + 733$$

という形に表示される．しかも 733 は，$p = 38$ および $q = 3$ と取れば $u^2 - Bt^2$ という形になっている．ところが 101 は決して $u^2 - Bt^2$ という同じ形にはならないのである．

この一例によりオイラーの命題は間違っていることが判明したが，素数の形状理論の視点に立つと，この命題の形はそれ自体において真に注目に値する．なぜなら，オイラーの元の命題では $4nB + a^2$ や $4nB + a^2 - B^2$，あるいはラグランジュが変形した命題では $4nB + \alpha$ などにより数 $A$ の線型的形状が指定され，それが $u^2 - Bt^2$ という平方的形状と等値されると主張されている．ところが，これは素数の形状理論と同じ様式の命題である．二次不定方程式 $A = u^2 - Bt^2$ の整数による可解条件を追い求めたオイラーは，素数の形状理論の一般理論に導かれたと言えると思う．あるいはむしろ，オイラーは直角三角形の基本定理など，フェルマに見られる素数の形状理論の断片に示唆を受けて，二次不定方程式の可解条件(まちがっていたが)に到達したのであろう．

二次不定方程式論はこんなふうにして素数の形状理論に結びついていく．

今度は方程式 $A+Bt^2=u^2$ の有理数解 $t$ と $u$ が見つかったとしよう．それらを共通の分母をもつ分数の形に変形して $u=\frac{x}{z}$，$t=\frac{y}{z}$ と置くと，解くべき方程式は

$$x^2-By^2=Az^2$$

という形になり，この変換方程式の整数解 $x$，$y$，$z$ を求めることが問題になる．

そこであらためて方程式 $x^2-By^2=Az^2$ が提示されたとしよう．状勢を整えるため $A$ と $B$ はともに正で，しかも平方因子をもたないと仮定しよう．これに加えて $A>B$ も仮定して考察する．求める整数解 $x$，$y$，$z$ は公約数をもたないものに限定してさしつかえないが，このとき $x$ と $y$，$x$ と $z$，$y$ と $z$ はそれぞれ互いに素になることがわかる．これより明らかになるように，$y$ と $A$ もまた互いに素である．なぜなら，もし $y^2$ と $A$ が公約数 $\theta$ をもつなら，$x^2$ もまた $\theta$ で割り切れなければならず，$x^2$ と $y^2$ は互いに素ではないことになってしまうからである．ところが，$y$ と $A$ は互いに素なのであるから，提示された方程式が解けるとして，$x$ と $y$ の定まった値を見つけることができるなら，二つの適切な不定数 $n$，$y'$ を見つけて $x=ny-Ay'$ という形に設定することができる．この値を提示された方程式に代入して，$A$ で割ると，方程式

$$\left(\frac{n^2-B}{A}\right)y^2-2nyy'+Ay'^2=z^2$$

が得られるが，$y$ と $A$ は互いに素なのであるから，$\frac{n^2-B}{A}$ は必ず整数である．すなわち，ガウスの表記法にならうなら，二次合同式 $n^2\equiv B\left(\mathrm{mod}.A\right)$ が成立する．あるいは，$A$ が素数の場合についてルジャンドルの記号を用いるなら，等式 $\left(\frac{B}{A}\right)=+1$ が成立する．これが，方程式 $x^2-By^2=Az^2$ の可解条件(必要条件)である．これを指摘したのはラグランジュである([J. L.Lagrange 2]参照)．

そこで一般に合同式 $n^2\equiv B\left(\mathrm{mod}.A\right)$ の可解条件を見いだして，$B$ は与えられた数として，もう一つの与えられた数 $A$ が $\alpha^2-B$ という形の数の約数でありうるか否かを判別する方法を見つけることが問題になる．二次不定方程式の解法理論と平方剰余の理論がこうして出会う．この出会いの状勢をはっきりと観察したのはラグランジュであり，オイラーも気づかなかった事柄である．そもそもオイラーには有理数解を求めようとした形跡は見られない．ただし，合同式 $n^2\equiv B\ \ \left(\mathrm{mod}.A\right)$ の可解条件それ自体については別で，オイラーはすでにこの条件を発見していた．$A$ が素数の場合を考えれば十分である．オイラーの論文[E134]「数の約数に関する諸定理」の「定理11」は次の通り．

《$a$ は $a=ff\pm\left(2m+1\right)\alpha$ という形とし，しかも $2m+1$ は素数とすると，$a^m-1$ は $2m+1$ で割り切れる．》

$p=2m+1$ と置いてこれを言い換えると，次のように言える．

《$a$は奇素数$p$の平方剰余とすると，$a^{\frac{p-1}{2}}-1$は$p$で割り切れる．》

この逆も言える．オイラーのもう一つの論文[E262]「冪の割り算を遂行して残される剰余に関する諸定理」の「定理19」は次の通り．

《$a^m-1$が素数$p=mn+1$で割り切れるなら，適当な数$x,y$を与えて，$ax^n-y^n$が同じ素数$p=mn+1$で割り切れるようにすることができる．》

しかも，つねに$x=1$と取れることもオイラーは示している．そこで今これを承認して，この定理において$n=2$，$x=1$と取ると，この定理の言明は次のようになる．

《$p=2m+1$は素数とし，$a^{\frac{p-1}{2}}-1$が$p$で割り切れるなら，適当な数$y$を与えて，$a-y^2$が同じ素数$p=2m+1$で割り切れるようにすることができる．言い換えると，$a$は$p$の平方剰余になる．》

これらの二定理は平方剰余の概念とフェルマの小定理の間の架橋であり，今日ではしばしば「オイラーの基準」という名で呼ばれる．このあたりの事情をもう少し詳しく説明すると，フェルマの小定理により$a^{p-1}\equiv 1 \pmod{p}$．よって合同式

$$\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)\equiv 0 \pmod{p}$$

が成立するが，これより$a^{\frac{p-1}{2}}\equiv \pm 1 \pmod{p}$となること，すなわち$a^{\frac{p-1}{2}}$を$p$で割ると，剰余は1または$-1$のいずれかであることが明らかになる．ルジャンドルはこの点に着目してルジャンドル記号$\left(\frac{a}{p}\right)$を定義した．すなわち，

$$a^{\frac{p-1}{2}}\equiv +1 \pmod{p}\text{のとき，}\left(\frac{a}{p}\right)=+1,$$

$$a^{\frac{p-1}{2}}\equiv -1 \pmod{p}\text{のとき，}\left(\frac{a}{p}\right)=-1$$

と定義した(このアイデアは1785年の論文[A. M. Legendre 1]で表明されたが，実際にルジャンドル記号$\left(\frac{a}{p}\right)$が考案され，導入されたのは1789年の著作 [A. M. Legendre 2]においてである)．ルジャンドル記号そのものはフェルマの小定理の簡単な書き換えにすぎないが，このような書き換えを行うことにより平方剰余の理論との関係が明瞭になる．オイラーの基準の意味合いはそこに認められるのである．

オイラーの二論文[E134][E262]では，平方剰余を越えて一般的な冪剰余に関する抽象的な考察が展開されているのであるから，そこに「オイラーの基準」と二次不定方程式$A=u^2-Bt^2$との関連を見るのは不可能である．オイラーは気づいていなかったのである．だが，ラグランジュは

この偉大な幾何学者が，$A = u^2 - Bt^2$ という形の方程式の解法において，これらの定理(註．複数形になっているのは，「オイラーの基準」が二分されて，二つの命題提示されているからである)を利用できることにまったく思いいたらなかったとは思えない．([J. L. Lagrange 3]; 全集2, p.491)

と言っている．このラグランジュの言葉が正鵠を射ていると思う．オイラーは冪剰余に関する抽象的な探究を通じて，二次不定方程式論の根幹を作る原理に期せずして近接していたことになる．

フェルマの言葉の時点に立ち返ると，二次不定方程式論の端緒を開いたペルの方程式，素数の形状理論の雛形と見られる直角三角形の基本定理，それに平方剰余の理論と結ばれているフェルマの小定理とは完全に別個に表明されたのであり，親密な内的関係で相互に結ばれていることを示す徴候はどこにも見あたらなかった．この相互関連は，オイラーを経てラグランジュにいたる過程で次第に明らかになっていった．一見して無縁のように見えたフェルマの三つの言葉が，オイラーの二次不定方程式論により開かれた場において繋がり合い，有機的なまとまりのある「オイラーの数論の世界」を作り始めたのである．

無関連に言明された個々の命題が，証明の探索を受けたり，一般化をめざされたりしているうちに，長い時間をかけて手足を伸ばし，つながれていく．このプロセスが数学の形成史であり，数学史叙述の眼目である．

## 3. 平方剰余相互法則

平方剰余の理論の根幹を作るのは平方剰余相互法則である．この法則はルジャンドルの1785年の論文「不定解析研究」([A. M. Legendre 1])で「異なる二つの奇素数の間に存在する相互法則」という形で表明された．ルジャンドルとは別にガウスもまた独自にこの法則を発見し，1801年の著作"Disquisitiones arithmeticae"([Gauss 1])において「平方剰余の理論における基本定理」として表明し，しかも異なる二通りの様式で正確に証明した．ルジャンドルが与えた呼称から「相互法則」の一語を採り，ガウスの呼称から「平方剰余」の一語を採って組み合わせると，今日流布している「平方剰余相互法則」という言葉が作られる．

今日の平方剰余相互法則には二つの補充法則が伴っている．ルジャンドルの記号を用いると，それらは，$p$ は奇素数として，

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \text{(第一補充法則)}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \qquad \text{(第二補充法則)}$$

というふうに表明される．ルジャンドルの数論的世界にも，論理的に見て二つの補充

法則と同等の命題は見られるが，ルジャンドルがそれらを相互法則の補充法則と認識していた形跡はない．

ルジャンドルもガウスも独立に同じ法則を発見したことになるが，クロネッカーが論文「相互法則の歴史について」([L. Kronecker])において精密に考証したところによれば，この法則を最初に発見したのはオイラーである．ただしオイラーは観察を通じて到達した諸命題を書き留めるのみで，証明は欠如している．

しばらくクロネッカーの考証をたどりたいと思う．オイラーの論文　(E　164)「$paa \pm qbb$ という形状に包摂される数の約数に関する諸定理」([L. Euler 5])には，平方剰余相互法則と同等の一連の命題がすでに記述されている．「註釈14」の内容は次の通り．

> それゆえ，今 $4Nm \pm \alpha$ は式 $aa - Nbb$ に包摂されている数の一般の約数のひとつの形状とすると，文字 $\alpha$ は一般に多くの数を表わすことになる．それらの数の間にはつねに1が含まれている・・・．それゆえ，$\alpha$ のさまざまな値は，$2N$ よりも小さくて，しかも $N$ と素な奇数である．そうしてそのような数，すなわち $2N$ よりも小さくて，しかも $N$ と素であるようなあらゆる奇数のうち，半分だけを採れば，それだけですでに $\alpha$ に適合する値が与えられる．残る半分の値が提供する諸式には，式 $aa - Nbb$ の約数はまったく包摂されない．(オイラー，全集Ⅰ-2, p.216)

「註釈16」には次のような記述がある．

> そのような $\alpha$ のさまざまな値の間にはつねに数1が見られるが，$4N$ と素な各々の平方数もまた，$\alpha$ に対し，適合する値を与えてくれるであろう．(オイラー，全集Ⅰ-2, p.216-217)

式 $a^2 + Nb^2$ もしくは式 $a^2 - Nb^2$ の素因子と非素因子とは，線形的形状 $4Nm \pm \alpha$ により二分されるとオイラーは語っている．しかも，$\alpha$ のさまざまな値と $N$ の平方剰余との関係がはっきりと強調されている点も，注目に値する．ある整数 $N$ に対し，はじめの $\frac{1}{2}(N-1)$ 個の奇平方数は $N$ を法として互いに非合同なのであるから，オイラーによれば，それらの奇平方数は $\alpha$ に対し，一般に必要とされるだけの個数の適切な値を与えている．この観察事項は相互法則とほぼ同等であり，ここから即座に相互法則が導かれるとクロネッカーは言う．実際，そのようにするとき $N$ は，正または負に取るとき $4N$ を法としてある平方数と合同になるという性質を備えたある素数，しかもただ一つのそのような素数の平方剰余でなければならないからである．

オイラーの論文(E　552)「素数による平方数の割り算に関連するさまざまな観察」([L. Euler 9])の末尾を見ると，ガウスの"Disquisitiones arithmeticae"に見られるものとまったく同じ文脈で平方剰余相互法則が記述されている．すなわち，この論文の§38に挙

げられている四つの定理は，全体として単一の相互法則を明示しているのである．クロネッカーは「それらのひとつひとつの内容が相互法則のいろいろな場合を示す四定理」と言っているが，オイラーの次のような言葉も書き添えられた．

> 私はこれらの定理を書き添えるが，そのようにするわけは，人々がこのような諸々の観察に心を寄せて，それらの証明を探し求めるようになってほしいのである．そのようにすることにより数の理論は著しい進歩が達成されるであろう．これは決して疑わしいことではない．(オイラー，全集 I -2, p.512)

オイラーは平方剰余相互法則を発見したが，証明を見つけることはできなかったのである．

オイラーの言葉に具体的に耳を傾けてみよう．クロネッカーの言う「四つの定理」に先立って次に挙げる二命題が出ている．

> もし除数 $P$ が $4q+3$ という形の素数なら，そのとき $-1$ もしくは $P-1$ は非剰余の系列の間にみいだされる．(定理4．オイラー，全集 I -3, p.504)
> もし除数 $P$ が $4q+1$ という形の素数なら，そのとき $-1$ もしくは $P-1$ はたしかに剰余の系列の間にみいだされる．(定理5．オイラー，全集 I -3, p.505)

これらの二命題を合わせると，平方剰余相互法則の第一補充法則そのものになる．この引用文において単に剰余，非剰余と言われているものは，それぞれ $P$ の平方剰余，$P$ の平方非剰余のことである．続いて，クロネッカーの言う「それらのひとつひとつが相互法則の種々の場合をその内容とする四定理」が列挙される．それらは次の通り．

> 1°．$s$ は素数として，もし素除数が $4ns+(2x+1)^2$ という形なら，そのとき $+s$ と $-s$ は剰余の間に現われる．
> 2°．$s$ は素数として，もし素除数が $4ns-(2x+1)^2$ という形なら，そのとき $+s$ は剰余の間に現われるが，$-s$ は非剰余の間にとどまる．
> 3°．$s$ は素数として，$4ns-(2x+1)^2$ という形状に包摂されるあらゆる値を取り除いたうえで，もし素除数が $4ns-4z-1$ という形なら，そのとき $-s$ は剰余の間に現われるが，$+s$ は非剰余である．
> 4°．$s$ は素数として，$4ns+(2x+1)^2$ という形状に包摂されるあらゆる値を取り除いたうえで，もし素除数が $4ns+4z+1$ という形なら，そのとき $+s$ と $-s$ は非剰余の間に現われる．　(これらはオイラーの論文の§38に記されている．オイラー，全集 I -3, p.511-512)

続いてオイラーは，これらの四定理を書き直し，言葉を変えて提示した．ここには平方剰余相互法則の姿が明瞭に現れている．同じ論文(E552)の§39からの引用である．

$s$はいたるところで素数を表わすものとする．奇平方数$1,9,25,49\cdots$のみを除数$4s$で割って剰余を書き留めていく，それらはすべて$4q+1$という形になる．それらの各々を文字$\alpha$で表わす．一方，$4q+1$型の数のうち，残されている数，すなわちそれらの剰余の間に現われない数を，どれもみな文字$\mathfrak{A}$で表わす，このようにしておくとき，もし除数が

$4ns+\alpha$　という形の素数なら，そのとき　$+s$は剰余であり，しかも$-s$も剰余である．

$4ns-\alpha$　という形の素数なら，そのとき　$+s$は剰余であり，しかも$-s$は非剰余である．

$4ns+\mathfrak{A}$　という形の素数なら，そのとき　$+s$は非剰余であり，しかも$-s$も非剰余である．

$4ns-\mathfrak{A}$　という形の素数なら，そのとき　$+s$は非剰余であり，しかも$-s$は剰余である．(オイラー，全集Ⅰ-3, p.512)

この状勢は次のように理解するとよい．まず$s$は素数である．次に，ある奇平方数$(2x+1)^2$を$4s$で割ると0と$4s$の間にとどまる剰余が得られるが，そのような剰余を一般に文字$\alpha$で表わすことにする．奇平方数はつねに$4q+1$型であることに留意すると，$\alpha$で表わされる数はどれもみなやはり$4q+1$型であることがわかる．そうして0と$4s$の間にとどまるあらゆる$4q+1$型の奇数のうち，$\alpha$で表わされるもの以外の数を一般に文字$\mathfrak{A}$で表わすことにするのであるから，$\mathfrak{A}$はつねに$4s$の平方非剰余である．特に$s$が奇素数なら，$\alpha$と$\mathfrak{A}$の差は決して$s$で割り切れない．よってこの場合には，$\mathfrak{A}$はつねに$s$自身の平方非剰余でもある．また，$4q+1$型のあらゆる奇数が二つの式$4ns+\alpha$, $4ns+\mathfrak{A}$のいずれかで表わされることは明らかである．したがって$4q+3$型の奇数はどれもみな必ず二つの式$4ns-\alpha$, $4ns-\mathfrak{A}$のいずれかで表わされる($\alpha$, $\mathfrak{A}$は$4n+1$型なので$4s-\alpha$, $4s-\mathfrak{A}$は$4n+3$型であることに留意する)．こうしてこれらの四つの式を全部集めると，どのような奇数もこれらの式のどれかで表わされることになる．

一例として$s=2$の場合を考えよう．この場合，奇平方数$1^2,3^2,5^2,7^2\cdots$を$4s$で割ると，剰余はつねに1である．よって文字$\alpha$, $\mathfrak{A}$で表わされる数はいずれもただひとつしか存在しない．すなわち$\alpha=1$, $\mathfrak{A}=5$である．したがって四つの形状$4ns+\alpha$, $4ns-\alpha$, $4ns-\mathfrak{A}$, $4ns+\mathfrak{A}$はそれぞれ$8n+1, 8n+7, 8n+3, 8n+5$という形状にほかならない．それゆえオイラーの定理によれば次のように言える．

1°．2と$-2$は$8n+1$型の素数の平方剰余である．

2°．2は$8n+7$型の素数の平方剰余であり，$-2$はそのような素数の平方非剰余である．

3°．$-2$は$8n+3$型の素数の平方剰余であり，2はそのような素数の平方非剰余である．

4°．2と−2は$8n+5$型の素数の平方非剰余である．

これらを要約すると，

2は$8n+1$型および$8n+7$型の素数の平方剰余であり，$8n+3$型および$8n+5$型の素数の平方非剰余である．また，$-2$は$8n+1$型および$8n+3$型の素数の平方剰余であり，$8n+5$型および$8n+7$型の素数の平方非剰余である．

となる．平方剰余相互法則の第一補充法則に留意すると，$+2$に関する言明と$-2$に関する言明は同義である．するとここに与えられているのは偶素数2がどのような奇素数の平方剰余であるか，またどのような奇素数の平方非剰余であるかという問いに対する完全な解答である．ところが，これは平方剰余相互法則の第二補充法則そのものにほかならない．

さて，あらためて任意の奇素数$p$を取り上げよう．$s$も奇素数として，しかも$p$と$s$は異なるとする．上述の事柄から諒解されるように，$p$の線型的形状は$4ns+\alpha$，$4ns-\alpha$，$4ns+\mathfrak{A}$，$4ns-\mathfrak{A}$のいずれかである．これらはそれぞれ，

$p$は$4n+1$型であり，しかも$s$の平方剰余である．

$p$は$4n+3$型であり，しかも$-p$は$s$の平方剰余である．

(これらの二言明は「$\left(-1\right)^{\frac{1}{2}(p-1)}p$は$s$の平方剰余である」と要約される．)

$p$は$4n+1$型であり，しかも$s$の平方非剰余である．

$p$は$4n+3$型であり，しかも$-p$は$s$の平方非剰余である．

(これらの二言明は「$\left(-1\right)^{\frac{1}{2}(p-1)}p$は$s$の平方非剰余である」と要約される．)

ということと同義である．オイラーの言葉によれば，これらの各々の場合に対応して，

$+s$は剰余であり，$-s$も剰余である．

$+s$は剰余だが，$-s$は非剰余である．

$+s$は非剰余であり，$-s$も非剰余である．

$+s$は非剰余だが，$-s$は剰余である．

というふうに言えることになる．ここで「剰余」というのは「$p$の平方剰余」のことで，「非剰余」は「$p$の平方非剰余」を意味する．このオイラーの言葉から$+s$に関する部分のみを取り出すと，

$\left(-1\right)^{\frac{1}{2}(p-1)}p$ が$s$の平方剰余なら，$+s$は$p$の平方剰余である．また，

$\left(-1\right)^{\frac{1}{2}(p-1)}p$が$s$の平方非剰余なら，$+s$は$p$の平方非剰余である．

と要約される($-s$に関する部分も同様に要約されるが，第一補充法則を考慮に入れると，両者は同等であることがわかる)．

今日の通有の意味合いにおいてルジャンドルの記号を用いると，上記のオイラーの定理は

$$\left(\frac{(-1)^{\frac{p-1}{2}}p}{s}\right)\left(\frac{s}{p}\right)=\left(\frac{(-1)^{\frac{p-1}{2}}}{s}\right)\left(\frac{p}{s}\right)\left(\frac{s}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{s-1}{2}}\left(\frac{p}{s}\right)\left(\frac{s}{p}\right)=1$$

と記述される．ここで$\left(\frac{(-1)^{\frac{p-1}{2}}}{s}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{s-1}{2}}$という関係を用いたが，これは平方剰余相互法則の第一補充法則にほかならない．この結果，

$$\left(\frac{p}{s}\right)\left(\frac{s}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{s-1}{2}}$$

という関係式が得られるが，これは今日の平方剰余相互法則そのものである．

ガウスの著作"Disquisitiones arithmeticae"([Gauss 1])の第131節には，

> $p$が$4n+1$という形の素数なら$+p$が，$p$が$4n+3$という形なら$-p$が，正に取るときに$p$自身の剰余もしくは非剰余であるような素数の剰余もしくは非剰余である．(「剰余」「非剰余」はそれぞれ「$p$の平方剰余」「$p$の平方非剰余」の意)

と「平方剰余の理論の基本定理」が記述されている．これを適宜言葉を補って要約すると次のようになる．

> 二つの異なる正の奇素数$p$，$s$に対し，もし$s$が$p$の平方剰余もしくは平方非剰余なら，それぞれの状勢に対応して，$(-1)^{\frac{1}{2}(p-1)}p$は$s$の平方剰余もしくは平方非剰余である．

今，$p$，$s$　は二つの異なる正の奇素数としよう．ガウスの基本定理によれば，$p$　が$4n+1$型の素数のとき，もし$s$が$p$の平方剰余もしくは平方非剰余であれば，$p$はそれぞれの場合に応じて$s$の平方剰余もしくは平方非剰余になる．$p$が$4n+3$型の素数のときは，もし$s$が$p$の平方剰余もしくは平方非剰余であれば，今度は$-p$が，それぞれの場合に応じて$s$の平方剰余もしくは平方非剰余になる．これを要約すると，

$$\left(\frac{s}{p}\right)\left(\frac{(-1)^{\frac{p-1}{2}}p}{s}\right)=1$$

という等式が得られる．ここで$\left(\frac{(-1)^{\frac{p-1}{2}}}{s}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{s-1}{2}}$に留意すると，この等式は

$$\left(\frac{p}{s}\right)\left(\frac{s}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{s-1}{2}}$$

という形になり，上述のオイラーの命題とぴったり一致する．オイラーはガウスと同じく平方剰余の理論の範疇において，すでに相互法則を発見していたのである．　オ

イラーとガウスとは別にルジャンドルもまた平方剰余相互法則を発見したが，ルジャンドルの場合，出発点は平方剰余の理論ではなく，フェルマの小定理であった．$p$と$q$は異なる二つの奇素数とすると，二つのルジャンドル記号$\left(\frac{q}{p}\right)$と$\left(\frac{p}{q}\right)$が同時に考えられるが，ルジャンドルはそれらの相互関係を指摘したのである．論理的に見ればオイラー，ガウスの相互法則とルジャンドルの相互法則は同等であり，それを保証するのが「オイラーの基準」なのであった．

## 4. フェルマの小定理

オイラーの「アリトメチカ論文集」(全集，第一系列，巻2-5)にはフェルマの小定理に関する諸論文が散見する．論文[E 26]「フェルマの一定理および素数に注目して得られる他の諸定理の観察」は数論の領域におけるオイラーの第一論文であり，17...年に執筆され，ペテルブルク科学アカデミー紀要，巻6(1732/3年)に掲載された．この学術誌が実際に刊行されたのは1738年であり，このときオイラーは38歳であった．数論の諸定理が列挙され，フェルマの小定理も出ているが，証明はついていない．

オイラーはまず，

《フェルマ数$2^{2^m}+1$，$m=0,1,2,3\cdots$はすべて素数である．》

というフェルマの言明を否定した．$m=5$のときに反例が生じ，$2^{32}+1=4294967297$は因子641をもつことをオイラーは発見したのである．次に，フェルマ数に対応して$2^n-1$という形の数が考えられるが，一般に次の定理が成立する．

《$n+1$は素数とし，二つの数$a$と$b$はいずれも$n+1$で割り切れないとしよう．このとき，$a^n-b^n$はつねに$n+1$で割り切れる．》

この命題はフェルマの小定理の一つの表現様式だが，証明は記されていない．この定理によれば，特に，もし$n+1$が素数なら，$2^n-1$はつねに$n+1$で割り切れることが判明する．論文の末尾に6個の定理が列挙されていて，それらのうち定理1はフェルマの小定理であり，定理2と定理3はその一般化である．

論文[E54]「素数に関する二，三の定理の証明」に移ると，フェルマの小定理がはじめて正しく証明された．証明は二項定理に基づいている．

オイラーの証明法をたどってフェルマの小定理を証明しよう．すなわち，$p$は素数とし，$N$は$p$で割り切れない任意の数とするとき，$N^{p-1}\equiv 1\pmod{p}$となること，言い換えると$N^{p-1}-1$は$p$で割り切れることを証明しよう．

$x$は任意の整数とすると，二項定理により，

$$(1+x)^p=1+px+\frac{p(p-1)}{1\cdot 2}x^2+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}x^3+\cdots+px^{p-1}+x^p$$

となる．二項係数の性質により，右辺の諸項は，一番初めの項と一番最後の項を除いて，すべて$p$で割り切れる．それゆえ$(1+x)^c-1-x^c$は，$x$が何であっても$p$で割り切れる．

そこで$1+x=N$と置くと，$(1+x)^p-1-x^p=N^c-(N-1)^c-1$．これが$p$で割り切

れるのであるから，合同式 $N^p-1\equiv(N-1)^p\,(\mathrm{mod.}\ p)$ が成立する．すなわち，

$$N^p-N\equiv(N-1)^p-(N-1)\,(\mathrm{mod.}\ p).$$

ここで $N$ を $N-1$ に置き換えると，

$$(N-1)^p-(N-1)\equiv(N-2)^p-(N-2)\,(\mathrm{mod.}\ p)$$

となる．この手順を続けていくと，最後に $(N-N)^p-(N-N)$ という剰余に到達する．これは明らかに0であるから，合同式 $N^p\equiv N\,(\mathrm{mod.}\ p)$ が成立することが明らかになる．すなわち $N^p-N$ は $p$ で割り切れる．ところが $N^p-N$ は $N$ と $N^{p-1}-1$ の積であり，$N$ は $p$ で割り切れないと仮定されたから，$N^{p-1}-1$ は $p$ で割り切れなければならないことになる．これでフェルマの小定理が証明された．

論文[E271]「新しい方法で証明されたアリトメチカの諸定理」ではフェルマの小定理の一般化が試みられた．

(a) 任意の数 $N$ に対し，「$N$ よりも小さくて，しかも $N$ と互いに素な数の個数」の決定．この問題は，等差数列

$$a,\ a+b,\ a+2b,\ a+3b\cdots$$

の各項を，公差 $b$ と互いに素な数 $n$ で次々と割っていくときの剰余を調べることに由来する．しかし，この個数を表すために特定の記号が導入されたわけではない．今日流布している記号 $\varphi(N)$ はガウスの著作D.A.ではじめて登場した．

(b) 一般化されたフェルマの小定理．すなわち，《互いに素な二つの数 $x$，$N$ に対して，$x^{\varphi(N)}-1$ はつねに $N$ で割り切れる》という定理の証明．

既述のように，ルジャンドルはフェルマの小定理から相互法則を取り出した．フェルマの相互法則は平方剰余の理論とは無関係なのであるから，「異なる二つの奇素数間の相互法則」という言葉が真に相応しい．

フェルマの小定理はオイラーの数論的世界の扉を開いた命題である．見たところ，不定方程式論とも素数の形状理論とも無関係としか思われないが，後に報告するように，オイラー，ラグランジュの数論を継承したルジャンドルの数論の構想によれば，フェルマの小定理は素数の形状理論において重要な役割を果すことになる．観念的に考えるなら，これもまた予想を越えた出来事であり，数学という学問が生い立っていく姿をよく示しているように思う．

## 5. 素数の形状理論(1) オイラーによる直角三角形の基本定理の証明

素数の形状理論はオイラーの数論の中核を作る理論である．この方面でのオイラーの究明は直角三角形の基本定理の証明から始まっている．まずはじめに論文[E228]「二

つの平方数の和になるような数について」を概観しよう．「命題4」は，

《互いに素な二つの平方数の和は，それ自身が二つの平方数の和ではないような数では割り切れない．》

というものである．これによれば，互いに素な二つの平方数の和として書き表される数の素因子は，どれもみなやはり二つの平方数の和の形に書き表されることになる．そうして二つの平方数の和の形に表示される二つの素数の積は，やはり二つの平方数の和の形に表示される．これは，等式

$$\left(a^2+b^2\right)\left(c^2+d^2\right)=\left(a\,c+b\,d\right)^2+\left(a\,d-b\,c\right)^2$$

が示す通りである．したがって，平方的形状 $x^2+y^2$ をもつ数は，約数もまた同じ形状をもつと主張されていることになる．

「命題4」の証明は無限降下法によって行われる．オイラーはこの証明法をフェルマに学んだのであろう．オイラーにならって「命題4」の証明の粗筋を再現してみよう．「命題4」に先立っていくつかの命題が並んでいる．まず「命題1」は次の通り．

《積 $p\,q$ は二つの平方数の和の形に表示されるとし，一方の因子 $p$ はやはり二つの平方数の和としよう．このとき，もう一つの因子 $q$ もまた二つの平方数の和として表示される．》

「命題1」に基づいて，次に挙げる「命題2」が証明される．

《積 $p\,q$ は二つの平方数の和の形に表示されるとし，一方の因子 $q$ は二つの平方数の和として表示されないとしよう．このとき，もう一つの因子 $p$ は，もし素数なら，二つの平方数の和にはならない．もし素数ではないなら，二つの平方数の和にならない素因子を少なくとも一つもつ．》

続いて「命題3」が証明される．

《互いに素な二つの平方数の和 $a^2+b^2$ が数 $p$ で割り切れるとしよう．このとき，二つの平方数の和として表示される数 $c^2+d^2$ で，$p$ で割り切れて，しかも $\frac{1}{2}p^2$ よりも小さいものが必ず存在する．》

この命題の証明は次の通り．$a$ と $b$ を $p$ で割り，$a=m\,p\pm c$，$b=n\,p\pm d$ と置こう．ここで数 $m$，$n$ を適切に定めて，$c$ と $d$ が $\frac{1}{2}p$ を越えないようにする．すると，

$$a^2+b^2=m^2\,p^2\pm 2\,m\,c\,p+c^2+n^2\,p^2\pm 2\,n\,d\,p+d^2$$

となる．これが $p$ で割り切れるのであるから，必然的に $c^2+d^2$ は $p$ で割り切れることになる．しかも $c<\frac{1}{2}p$ かつ $d<\frac{1}{2}p$ であるから，$c^2+d^2<\frac{1}{4}p^2+\frac{1}{4}p^2=\frac{1}{2}p^2$ となる．

これで「命題4」の証明の準備ができた．今，「命題4」は正しくないとすれば，互いに素な二つの平方数の和の形に表示される何らかの数 $a^2+b^2$ と数 $p$ が存在し，$a^2+b^2$ は $p$ で割り切れて，しかも $p$ は二つの平方数の和の形には表示されえないということが起る．命題3により，二つの平方数の和 $c^2+d^2$ で，$p$ で割り切れて，しかも $\frac{1}{2}p^2$ よりも小さいものが見つかる．$c^2+d^2=p\,q$ と置くと，$p$ 自身は二つの平方

数の和ではないのであるから，命題2により，$q$もまたそのような形ではないか，あるいは少なくとも$q$の因子の中にそのような形ではないものが必ず存在する．その因子を$r$とする．$pq<\frac{1}{2}p^2$より$q<\frac{1}{2}p$．よって$r<\frac{1}{2}p$．ここで$c^2+d^2$と$r$に対して命題3を適用すると，$r$で割り切れる数$e^2+f^2$で，$\frac{1}{2}r^2<\frac{1}{8}p^2$より小さいものが見つかる．この手順をどこまでも続けていくと，どこまでも限りなく小さくなっていく自然数の無限系列ができることになる．ところが，そのような系列が存在しえないのは明らかである．これで「命題4」の証明が完成した．

この「命題4」の観察事項に基づいて直角三角形の基本定理が証明されるが，この時点では証明の基本方針が指示されているのみに留まっている．証明の細部は論文[E 241]で記述された．「命題6」と「命題7」は次の通り．

《ある$4n+1$型の数について，もしその数を互いに素な二つの平方数の和として書き表す仕方がただ一通りしか存在しないなら，その数は素数である．》

《ある$4n+1$型の数について，もしその数を互いに素な二つの平方数の和として二通りの仕方で書き表すことができるなら，その数は合成数である．》

これらの二命題を利用して，ある数が与えられたとき，それが相当に大きな数であっても，素数か否かの判定が可能になる．オイラーは6個の計算例を挙げている．たとえば，100981は$100981=215^2+234^2$と一意的に分解され，215と234は互いに素であるから100981は素数である．1000009は，

$$1000009=1000^2+3^2=235^2+972^2$$

というふうに，二つの平方数の和の形に二通りの仕方で分解される．よって1000009は素数ではない．233033は$4n+1$型だが，二つの素数の和の形に表示することはできない．よって素数ではない．実際，$233033=467\times499$と分解される．32129は$32129=95^2+152^2$と二つの平方数の和の形に一意的に分解されるが，95と152は互に素ではなく，共通因子19をもっている．よって32129は素数ではない．実際，$32129=19^2\times89$と分解される．

論文[E 241]「$4n+1$という形のあらゆる素数は二つの平方数の和であるというフェルマの定理の証明」では，論文[E 228]で表明された方針に基づいて「直角三角形の基本定理」，すなわち「$4n+1$型の素数はつねに$a^2+b^2$という形に表示される」という定理の証明が完成する．これに先立って，論文[E 134]「数の約数に関する諸定理」では，「$a$と$b$は互いに素とするとき，$a^2+b^2$という形の数の奇約数はつねに$4n+1$という形である」という定理が証明されている．オイラーの証明には，素数の形状理論の歩むべき道筋が具体的に指し示されている．

論文[E 228]に立ち返ると，「命題4」に続いて，「証明の試み」という小見出しのもとで，直角三角形の基本定理の証明の粗筋が描写されている．

証明の試み

$p=4n+1$は素数として，$a$と$b$は$p$で割り切れない数とする．フェルマの小定理に

より，$a^{4n}-1$ と $b^{4n}-1$ はいずれも $p$ で割り切れる．それゆえ，それらの差，すなわち $a^{4n}-b^{4n}$ もまた $p$ で割り切れるが，

$$a^{4n}-b^{4n}=\left(a^{2n}-b^{2n}\right)\left(a^{2n}+b^{2n}\right)$$

となるから，二つの数 $a^{2n}-b^{2n}$，$a^{2n}+b^{2n}$ のどちらか一方は必ず $p$ で割り切れるそこで，もし $a^{2n}-b^{2n}$ が $p$ で割り切れないなら，すなわちそのような二つの数 $a$，$b$ が存在するなら，それらの数 $a$，$b$ に対し，$a^{2n}+b^{2n}$ は $p$ で割り切れることになる．ところが，その場合，$p$ は二つの平方数 $a^{2n}$，$b^{2n}$ の和の約数なのであるから，「証明の試み」に先立って証明された命題，すなわち命題4により，$p$ 自身もまた二つの平方数の和の形に書き表されるのである．(「証明の試み」終)

このスケッチでは「$a^{2n}-b^{2n}$ が $p$ で割り切れないような二つの数 $a$，$b$ が存在する」という論点が証明を欠いたまま残されているが，論文[E241]で次のように補填された．$4n$ 個の数の系列

$$1,\ 2^{2n},\ 3^{2n},\ 4^{2n}\cdots\left(4n\right)^{2n}$$

を考えて，隣り合う二つの数の差を次々と作っていくと，

$$(a_1)\quad 2^{2n}-1,\ 3^{2n}-2^{2n},\ 4^{2n}-3^{2n}\cdots\left(4n-1\right)^{2n}-\left(4n-2\right)^{2n},\ \left(4n\right)^{2n}-\left(4n-1\right)^{2n}$$

という，$4n-1$ 個の数の系列が得られる．次に，今度はこの系列 $(a_1)$ から出発して同様の手順を繰り返すと，

$$(a_2)\qquad 3^{2n}-2\cdot 2^{2n}+1,\ 4^{2n}-2\cdot 3^{2n}+2^{n}\cdots\left(4n\right)^{2n}-2\cdot\left(4n-1\right)^{2n}+\left(4n-2\right)^{2n}$$

という系列が得られる．以下，同様の手続きを繰り返していくと，$2n$ 回目には同一の数 $(2n)!$ が $2n$ 個並んでいる系列

$$(2n)!,\ (2n)!,\ (2n)!\cdots(2n)!$$

が出現する．オイラーはこれを証明した．さて，もし第一系列 $(a_1)$ を作る $4n-1$ 個の数がすべて素数 $p=4n+1$ で割り切れるなら，第二系列 $(a_1)$，第三系列 $(a_1)$ ・・・についても同様である．したがって，特に第 $2n$ 系列に現れる数 $(2n)!$ は $p$ で割り切れることになるが，明らかにこのようなことはありえない．それゆえ，第一系列 $(a_1)$ を作る $4n-1$ 個の数のうち，少なくとも一つは $p$ で割り切れないことになる．これで，論文[E228]の段階で仮定されていた事柄が証明された．

この証明は大きく二段構えになっている．

第一段階

互いに素な二つの平方数の和の奇約数は，やはり二つの平方数の和の形に書き表される．

第二段階

$4n+1$ 型の素数はつねに，二つの互いに素な平方数の和の形に書き表される何らかの数の約数になる．

第二段階の言明が意味をもちうるためには，一つの前提事項が準備されていなけれ

ばならない．それは，

《二つの互いに素な平方数の和の形に書き表される数の奇約数は，つねに $4n+1$ という形である．》

という事実を確認することである．これはフェルマの言葉の一つであり，オイラーはこの命題の証明をを論文[E 134]「数の約数に関する諸定理」で遂行した．この事実が確定してはじめて，その逆を問う問いが意味をもってくるのである．

この証明の構造を省察すると，第一段階のテーマは「二次形式 $t^2+au^2$ の奇約数の平方的形状の決定」である．オイラーは $a=1$，2，3 の場合にのみ，そのような決定に成功したにすぎないが，オイラーを継承したラグランジュはこれを完全に決定した．ラグランジュの論文「アリトメチカ研究」第一部がこのテーマに捧げられている．オイラーの証明は $a=1$ の場合については上述の通り．$a=2$ の場合には論文[E256]，$a=3$ の場合には論文[E 272]に出ているが，証明の基本方針は $a=1$ の場合と同じである．

次に，オイラーによる直角三角形の基本定理の証明の第二段階のテーマは「二次形式 $t^2+au^2$ の奇約数の線型的形状の決定」である．オイラーが $a=1$ の場合にそうしたように，このテーマはさらに二分される．まず，

《二次形式 $t^2+au^2$ の奇約数の線型的形状の候補者》

を列挙し，それから次に，

《逆に，そのような線型的形状をもつ素数は，実際に必ず二次形式 $t^2+au^2$ の約数である．》

という事実の確立をめざすのである．オイラーは前者については随所で一般的な言明を書き残している．後者はむずかしいが，これが素数の形状理論の鍵である．オイラーは $a=1$ の場合に対してこの証明に成功し，そのおかげで直角三角形の基本定理を確立することができた．さらに $a=2$ の場合にも成功し，それを梃子にして「$6n+1$ 型の素数は $a^2+3b^2$ という形である」という，フェルマの言葉を証明することもできた([E 272])．オイラーは $a=3$ の場合も成功した．ただしその先に難所があり，「$8n+1$ 型の素数と $8n+3$ 型の素数は $a^2+2b^2$ という形である」([E 256])というもう一つのフェルマの言葉は証明することができなかった．

このオイラーの方針を継承したラグランジュは一般的な証明には到達しなかったが，その代わり，「$4n+3$ 型の素数はどれもみな必ず，二つの二次形式 $t^2+au^2$，$t^2-au^2$ のいずれかの約数である」という事実に気づき，これを梃子として，$4n+3$ 型の素数を対象にする一般理論を構築した．ただし，$4n+1$ 型の素数に対しては，ラグランジュは一般理論を作ることができなかった．この困難を乗り越えたのがルジャンドルで，ルジャンドルは平方剰余相互法則を駆使することにより

《$4n+1$ 型の素数はどれも必ず，二つの二次形式 $t^2+au^2$，$t^2-au^2$ のいずれかの約数である．》

という命題の証明に首尾よく成功した．ルジャンドルが平方剰余相互法則を提案した

理由はこの点に認められるのである．素数の形状理論はこれで完成する．ただしルジャンドルは平方剰余相互法則の証明には失敗した．

オイラーによる直角三角形の基本定理の証明は素数の形状理論の雛形であり，オイラーがここで明らかにした証明の基本構想はそのままラグランジュに継承された．第二段階のテーマ「二次形式$t^2+au^2$の奇約数の線型的形状の決定」には平方剰余相互法則の契機がすでに現れていて，オイラーはこの論点を追究することにより実際に平方剰余相互法則に到達した．平方剰余相互法則は素数の形状理論の中に埋もれていたのである．もっと根源に立ち返るなら，直角三角形の基本定理のオイラーによる証明の中に，平方剰余相互法則はすでに芽生えていたとも言えるように思う．

ルジャンドルはオイラーが平方剰余相互法則をすでに発見していたという事実には気づかなかったが，フェルマの小定理に平方剰余相互法則の契機を発見し，そこから実際に相互法則を取り出すことにも成功した．ルジャンドルの意図は，素数の形状理論が直面した最後の困難を克服する鍵を平方剰余相互法則に求めようとしたところに認められる．このような着眼はオイラーにもないルジャンドルの独自のアイデアであり，素数の形状理論に寄せる創意に満ちた貢献である．それだけにいっそう証明の失敗が惜しまれるのである．

ガウスの著作"Disquisitiones arithmeticae"と同じタイトルをもつラグランジュの論文「アリトメチカ研究」([J. L. Lagrange 6])は，素数の形状理論に捧げられた長篇である．この論文は二つの部分に分けられていて，第一部は1773年，第二部は1775年に公表された．眼目は第二部にある．第一部は全体として第二部のための予備的考察であり，テーマは「二次形式$t^2\pm au^2$の約数の平方的形状の決定」である．ラグランジュはいくつかの例を挙げたが，冒頭の三つの例

$$t^2+u^2,\ t^2+2u^2,\ t^2+3u^2$$

の平方的約数をラグランジュにならって求めてみよう．

ラグランジュは一般に二次形式

$$Bt^2+Ctu+Du^2$$

の考察から出発する．ここで$B$，$C$，$D$は定量，$t$，$u$は変化量である．変化量$t$，$u$に互いに素な数を自由に代入してできる数の約数の一般的形状を求めようとして，

$$Pt^2+Qtu+Ru^2$$

という形状を得た．ここで$4BD-C^2=4PR-Q^2$．この共通の値を$K$で表す．新たな定量$P$，$Q$，$R$は，あらかじめ与えられた定量$B$，$C$，$D$から定められるが，その様子は次の通り．$K$の偶奇に応じて$Q$は偶数または奇数になることに留意する．$K$の正負に応じて二通りの場合を区別する．まず$K$が正のとき，$Q$は$\sqrt{\frac{K}{3}}$を越えない．これで$Q$の候補が有限個に限定される．次に，$PR=\frac{K+Q^2}{4}$．また$P$も$R$も$Q$より小さくなることはない．これで$P$，$R$の候補が限定される．

この結果を二次形式$t^2 \pm a u^2$に適用してみよう．ここで$a$は正の定量である．まず$t^2 + a u^2$を取り上げる．上記の一般的状勢にあてはめると，$B=1$，$C=0$，$D=a$．よって$K=4a$．これは偶数であるから$Q$も偶数である．しかも$Q$の大きさは$\sqrt{\frac{4a}{3}}$を越えない．そこで$Q=\pm 2q\ (q>0)$と置くと，$q$は$\sqrt{\frac{a}{3}}$を越えない．また，$PR=\frac{4a+4q^2}{4}=a+q^2$．そこで$a+q^2$の二つの約数$p$，$r$を$pr=a+q^2$，$|p| \geqq 2q$，$|r| \geqq 2q$となるように取る．このとき$p$と$r$は必然的に同符号になることに注意する．これで二次形式$t^2 \pm a u^2$の約数の平方的形状$py^2 \pm 2qyz + rz^2$の決定が可能になる．二次形式$t^2 - a u^2$についても同様の手順が進行する．

特に$a=1$の場合を考えよう．この場合，まず$q \leqq \sqrt{\frac{1}{3}}$より$q=0$．次に$pr=1$より$p=1$，$r=1$．それゆえ二次形式$t^2+u^2$の約数の平方的形状は$y^2+z^2$であることがわかり，オイラーの論文[E 228]の「命題4」が再現される．オイラーの証明に比して，非常に高い一般性を備えた証明である．$a=2$の場合には，$q \leqq \sqrt{\frac{2}{3}}$より$q=0$．よって$pr=2$．これより$p=1$，$r=2$となり，二次形式$t^2+2u^2$の約数の平方的形状は$y^2+2z^2$であることが判明する．$a=3$の場合にも議論は同様に進行する．この場合，$q \leqq \sqrt{\frac{2}{3}}=1$であるから，$q=0$または$q=1$となる．$q=0$のとき，$pr=3$．よって$p=1$，$r=3$となる．$q=1$のときは$pr=3+1=4$．しかも$p$も$r$も$2q=2$より小さくはないから，$p=2$，$r=2$．これで，二次形式$t^2+3u^2$の約数の平方的形状は$y^2+3z^2$または$2y^2 \pm 2yz + 2z^2$であることが明らかになった．ところが後者の形状が表す約数は偶数である．したがって$t^2+3u^2$の奇約数の平方的形状は$y^2+3z^2$であることになる．ラグランジュはこんなふうにして次々と例を挙げていき，$a=3$を越えて$a=12$に及んだ．ラグランジュの方法はオイラーの方法とはまったく異なっていて，はるかに強力である．実際のところ，オイラーの方法では$a=1$，2，3の場合を越えることはできなかったのである．

二次形式$t^2 - a u^2$において$a=2$の場合を考えると，$t^2-2u^2$の約数の平方的形状は同じく$y^2-2z^2$であることが明らかになる(ラグランジュ全集，巻3，p.714-715)．特に$a^2-2$の平方的約数は$x^2+2$という形ではありえないことが判明し，フェルマの言葉の一つが確立される．

二次形式$t^2+u^2$，$t^2+2u^2$，$t^2+3u^2$で表される数の約数の平方的形状に関する三命題をはじめて証明したのはオイラーだが，命題それ自体は「フェルマ氏に負うていると私は思う」(ラグランジュ全集，巻3，p.714)とラグランジュは言っている．二次形式の約数の平方的形状についてフェルマが述べたのは，実際には「$a^2+2b^2$という形の平方数の平方根はやはり$x^2+2y^2$という形である」(欄外ノート45)ということのみである．オイラーはこれだけを手がかりにして三つの命題を言明し，証明した．その証明法は一種の無限降下法であり，オイラーはこれをフェルマに学んだのではないかと思う．しかもオイラーはなお一歩を進め，直角三角形の基本定理と，「$6n+1$型のあらゆる素数は$y^2+3z^2$という形である」という定理を証明し，素数の形状理論の礎石を築くことに成功した([E 272])．オイラーは「二次形式の約数の平方的形状」の究明が素数の形状理論の基礎になりうることに気づき，フェルマの言葉が表明された段

階では無関係に見えた二つの事柄の相互関連を明るみに出したのであり，オイラーに独自のアイデアはこのようなところに明瞭に観察されるのである．

## 6. 素数の形状理論(2) オイラー，ラグランジュの理論

オイラーの論文[E 256]を見ると，素数の形状理論に所属するフェルマの言葉と，オイラーが発見して付け加えた諸命題が列挙されている．第56節に出ている8個の命題は次の通り．

Ⅰ． $4n+1$ 型のあらゆる素数は $a^2+b^2$ という形に表示される．(直角三角形の基本定理．フェルマの言葉)

Ⅱ． $8n+1$ 型および $8n+3$ 型のあらゆる素数は $2a^2+b^2$ という形に表示される．(フェルマの言葉)

Ⅲ． $12n+1$ 型もしくは $12n+7$ 型の素数，言い換えると $6n+1$ 型のあらゆる素数は $3a^2+b^2$ という形に表示される．

Ⅳ． $16n+1$，$16n+5$，$16n+9$，$16n+13$ 型の素数，言い換えると $4n+1$ 型のあらゆる素数は $4a^2+b^2$ という形に表示される．(この命題の証明は命題Ⅰに包摂されている．)

Ⅴ． $20n+1$，$20n+9$ 型のあらゆる素数は $5a^2+b^2$ という形に表示される．

Ⅵ． $24n+1$，$24n+7$ 型のあらゆる素数は $6a^2+b^2$ という形に表示される．

Ⅶ． $28n+1$，$28n+9$，$28n+11$，$28n+15$，$28n+23$，$28n+25$ 型の素数，言い換えると $14n+1$，$14n+9$，$14n+11$ 型のあらゆる素数は $7a^2+b^2$ という形に表示される．

Ⅷ． $24n+5$ 型および $24n+11$ 型のあらゆる素数は $3a^2+2b^2$ という形に表示される．(オイラー全集，巻2，p.486)

これらの命題のうち，オイラーが実際に証明に成功したのは命題Ⅰ(直角三角形の基本定理)のみにすぎないが，オイラーを継承したラグランジュは長篇「アリトメチカ研究」においてオイラーが予測した諸命題の証明を試みた．ラグランジュの理論は $4n+3$ 型の素数に対しては大きな成功をおさめ，オイラーが挙げた命題Ⅰ-Ⅷのうち，$4n+3$ 型の素数に関する部分はすべて証明された．これらはラグランジュの理論が成功した事例である．フェルマの言葉の中に，「$3n+1$ 型の素数(それは必然的に $6n+1$ 型である)はどれもみな $a^2+3b^2$ という形である」，「$8n+1$ 型および $8n-1$ 型の素数は $a^2-2b^2$ という形に書き表わされる」というのがあるが，前者の言葉のうち $n$ が奇数の部分と，後者の言葉のうち $8n-1$ 型の素数に関する部分はラグランジュ

の理論の守備範囲である．

素数の形状理論を語るもう一つのフェルマの言葉，すなわち「$20n+3$ もしくは $20n+7$ という形の二つの素数の積は $y^2+5z^2$ という形である」という命題もラグランジュの理論により証明が可能になる．実際，$20n+3$ もしくは $20n+7$ という形の数が素数なら，ラグランジュの理論によりどちらも $2y^2+2yz+3z^2$ という形である(ラグランジュ全集，巻3，p.784)．そうして，式

$$\left(2y^2+2yz+3z^2\right)\left(2y'^2+2y'z'+3z'^2\right)=\left(2y'^2+2y'z'+3z'^2\right)^2+5\left(yz'-zy'\right)^2$$

が示しているように，そのような二つの数の積は $y^2+5z^2$ という形である．

ラグランジュの理論は $4n+1$ 型の数に対しては無力である．ラグランジュ自身，次のように語っている．

> 第45節の諸定理が視圏にとらえているのは $4n-1$ という形の素数のみである．$4n+1$ という形の素数に関して同様の諸定理を獲得するためには，「$4na+b$ という形の素数は，$b$ が $4m+1$ という形のときにはつねに，$t^2+au^2$ もしくは $t^2-au^2$ という形の何らかの数の約数でありうること」が証明できなければならない．というのは，我々はすでに，$t^2\pm au^2$ の約数であるような $4n+1$ 型の素数はこれもみな $t^2\mp au^2$ の約数でもあることを示したからである．ところで，帰納的考察によれば，$t^2\pm au^2$ の約数に適合する形状の素数はいつでも実際にそのような数の約数でありうる，ということを明示しているように思われる．だが，それにもかかわらず，この命題は $4n+1$ 型の素数に関しては，ごくわずかな場合についてだけ厳密に証明できるにすぎない．少なくとも，この証明を為し遂げるべく私が行ったあらゆる試みは，今のところ実りのないままに終始している．そこで，私はここでは若干の特別の場合における研究の諸結果を報告するだけにとどめることにする．それらの場合については，私はいま話題になっている命題の証明を首尾よく発見したのである．それらの場合というのは，$b=1$ で，しかも $a=1,2,3,5,7$ もしくは $a$ がこれらの数のいくつかの積に等しい場合，あるいは $b=9$ で，しかも $a=5,10$ の場合である．([J. L. Lagrange 6]．ラグランジュ全集，巻3, p.789)

ラグランジュは $4n+1$ 型の素数に対しては一般的な形状理論を作ることはできなかったが，個々の場合について工夫を凝らし，若干の結論を得た．それらの中には，オイラーが挙げている諸命題のうち $4n+1$ 型の素数に関する部分は，$24n+5$ 型の素数と $28n+9$ 型の素数に関する命題のほかはすべて証明された．フェルマの言葉でいうと，「$3n+1$ 型の素数(それは必然的に $6n+1$ 型である)はどれもみな $a^2+3b^2$ という形である」という命題のうち，$n$ が偶数の部分，それに「$8n+1$ 型の素数は $a^2-2b^2$ という形に書き表わされる」という命題も証明された．こうしてラグランジュの論文「アリトメチカ研究」により，素数の形状理論に所属するフェルマの言葉はすべて証

明されたうえ，はるかに広い世界に出ることも可能になったのであるから，ラグランジュの所期の目的はおおよそ達成されたと言えるのである．だが，「$4n+1$型の素数に対する一般理論の確立」という課題が残された．ルジャンドルはこれを引き継いだのである．

ラグランジュの理論に向けられたルジャンドルの批判も興味深い．ルジャンドルは1785年の論文「不定解析研究」の中で，$20x+1$，$20x+9$型の素数は$y^2+5z^2$という形であること，および$20x+3$，$20x+7$型の素数は$2y^2+2yz+3z^2$という形であることを示した後に，次のように述べている．

> これらの二命題はラグランジュ氏がベルリン科学アカデミー紀要，1775年(註．ラグランジュの論文「アリトメチカ研究」第二部を指す)の中で見いだした命題と一致している．しかしラグランジュ氏が$20x+1$型と$20x+9$型の素数に関する前者の命題にようやく到達したのは，他の場合に対しては適用できないように見えるある解く別の方法の支援を受けてのことであった．一般に，我々の表の中に出ている$4n+1$型素数に関する定理はことごとくみな，先ほど引用した命題と式$t^2+3u^2$，$t^2+7u^2$の約数に関する命題を除いて，まったく新しい．それに比して，$4n-1$型の素数がもたらす困難はずっと小さいように思われる．というのは，そのような数は必ず式$t^2+cu^2$，$t^2-cu^2$のどちらか一方を割り切る．したがって，これらの式の各々の約数の考察を通じて，$t^2-cu^2$を割り切らない形の数は必ず$t^2+cu^2$を割り切るという結論が下されるのである．ラグランジュ氏はそのようにして，$20x+3$，$20x+7$型の素数は必ず$t^2+5u^2$を割り切ること，したがって$2y^2+2yz+3z^2$ということを発見したのである．同様にして，$4n-1$型の素数を対象にして無限に多くの類似の定理を見つけることが可能である．だが，その方法は$4n+1$型の素数に関しては何事も教えてくれないのである．([A.M. Legendre 1])

ラグランジュの理論はもう一歩のところで完成にいたらなかった．この状勢を継承したルジャンドルは，「二つの異なる奇素数間の相互法則」に困難を乗り越える鍵を求め，素数の形状理論の完成を企図した．この試みは成功したが，鍵をにぎる平方剰余相互法則の証明には失敗した．われわれはここで，平方剰余相互法則の源泉もまたオイラーであるという事実にあらためて留意しておきたいと思う．

## 7. 高次冪剰余の理論への道

フェルマにもラグランジュにも見あたらず，オイラーにのみ独自の数論的交冊は冪剰余の理論において際立っている．ここでは冪剰余の一般的考察８篇の論文を挙げた

いと思う.

Ⅰ.　[E134]「数の約数に関する諸定理」

主な内容を列挙する.「定理3」の内容はフェルマの小定理であり，証明も与えられている.これは第二番目の証明である.第一証明は論文[E 54]で与えられた.

定理5　$a$ と $b$ は互いに素とするとき，$a^2+b^2$ という形の数の奇約数はつねに $4n+1$ という形である.

定理6　$a$ と $b$ は互いに素とするとき，$a^4+b^4$ という形の数の奇約数はつねに $8n+1$ という形である.

定理7　$a$ と $b$ は互いに素とするとき，$a^8+b^8$ という形の数の奇約数はつねに $16n+1$ という形である.

定理8　(上記の三定理の一般化) $a$ と $b$ は互いに素とするとき，$a^{2^m}+b^{2^m}$ という形の数の奇約数はつねに $2^{m+1}n+1$ という形である.

定理8において $a=2$，$b=1$ と置くと，次のように言える.

《フェルマ数 $2^{2^m}+1$ の約数はつねに $2^m n+1$ という形である.》

そこで特に $m=5$ の場合を考えると，フェルマ数 $2^{32}+1=4294967297$ の約数は $64n+1$ という形でしかありえないことが判明する.オイラーはこの事実に着目してこのフェルマ数の約数641を発見した.「すべてのフェルマ数は素数である」というフェルマの言葉に反例を与えることができたのである.

**定理11**　(「オイラーの基準」の半分)　$a=f^2\pm(2m+1)\alpha$ とし，$2m+1$ は素数とすると，$a^m-1$ は $2m+1$ で割り切れる.

言い換えると，$a$ が奇素数 $p=2m+1$ の平方剰余なら，$a^{\frac{p-1}{2}}-1$ は $p$ で割り切れる.もちろんオイラーは平方剰余という言葉を用いているわけではない.定理11は平方剰余の理論に所属するが，オイラーの考察はより高次の冪剰余へと進んでいく.

**定理12**　$a=f^3\pm(3m+1)\alpha$ とし，$3m+1$ は素数とすると，$a^m-1$ は $3m+1$ で割り切れる.

これを言い換えると，$a$ が奇素数 $p=3m+1$ の３次の冪剰余なら，$a^{\frac{p-1}{3}}-1$ は $p$ で割り切れる.

**定理13**　$a=f^n\pm(mn+1)\alpha$ とし，$mn+1$ は素数とすると，$a^m-1$ は $mn+1$ で割り

切れる.

これを言い換えると，$a$が奇素数$p=mn+1$の$n$次の冪剰余なら，$a^{\frac{p-1}{n}}-1$は$p$で割り切れる．論文[E262]ではこの定理の逆が証明されている.

一般化はさらに進行する.

**定理14**　$f^n-ag^n$が素数$mn+1$で割り切れるなら，$a^m-1$は$mn+1$で割り切れる.

**定理15**　$af^n-bg^n$が素数$mn+1$で割り切れるなら，$a^m-b^m$は$mn+1$で割り切れる.

Ⅱ.　[E242]「すべての整数もしくは分数は4個ないし4個以下の平方数の和であるというフェルマの定理の証明」

この論文には標題で言われている定理，すなわち「すべての整数または分数は4個ないし4個以下の平方数の和である」という定理も確かに見られるが，この論文の実質は平方剰余の基礎理論である．論文[E241]の続きとして書かれたものと考えられ，元来オイラー自身による標題は欠けていた.

Ⅲ.　[E 552]「平方数を素数で割ることに関連するさまざまな観察」

論文[E 242]を受けて，新たに平方剰余の理論の基礎が展開された．クロネッカーが考証したように，この論文には平方剰余相互法則が現れている.

Ⅳ.　[E 262]「冪の割り算を遂行して残される剰余に関する諸定理」

この論文は冪剰余の理論の基礎である．言及しなければならない事柄が多いが，なかでもフェルマの小定理の新証明は光彩を放っている．今，$p$は奇素数，$a$は$p$と互いに素な数として，等比数列

$$1, a, a^2, a^3, a^4 \cdots$$

の各項を次々と$p$で割っていこう．第二項から第$p-1$項までの諸項$a, a^2, \cdots a^{p-1}$を$p$で割るときに生じる$p-1$個の剰余の間には必ず数1が現れる．言い換えると，1と$p-1$の間の何かある数$\lambda$に対し，$a^\lambda-1$が$p$で割り切れる．このような$\lambda$のうち最小のものを取り，それをあらためて$\lambda$で表すことにする．このような状勢のもとで，オイラーは「$\lambda$は$p-1$の約数である」ことを示した．これより即座に$a^{p-1}-1$は$p$で割り切れることが明らかになる．すなわちフェルマの小定理が証明されたのである．注目に値するのは，このような証明法がすでにフェルマの言葉の中に見られるという事実である(1640年10月18日付のフェルマのフレニクル宛書簡参照．フェルマ全集，巻2，p.206-212)．フェルマの小定理は高次冪剰余の理論の世界を開く小さな扉であ

る.

V. [E449]「素数による冪の割り算を遂行して生じる剰余に関する諸証明」

この論文には原始根の概念が登場する. 論文[E262]におけるように, $p$ は奇素数, $a$ は $p$ と互いに素な数として, 等比数列

$$1, a, a^2, a^3 \cdots$$

の各項を次々と $p$ で割っていくものとする. そのようにして生じるさまざまな剰余の間に $p$ よりも小さい数がすべて姿を現す場合, オイラーは上記の等比数列を完全列と呼び, $a$ を $p$ に関する原始根と呼んだ. この定義によれば, $p$ に関する原始根とは, 「その $p-1$ 次以下のいかなる冪を $p$ で割っても, その剰余は決して $p$ ではありえないような数」のことにほかならない. 原始根の概念への道は, フェルマの小定理を踏まえて, その延長線上に伸びている.

オイラーは任意の奇素数 $p$ に対し, それに関する原始根の存在の証明を試みたが, 後年, ガウスは"Disquisitiones arithmeticae "においてオイラーの証明には二つの欠陥があることを指摘し, 独自の証明を与えた.

VI. [E554]「素数による平方数およびより高次の冪の割り算を遂行して残される剰余に関するいっそう精密な研究」

奇素数 $p$ に関する原始根の個数が探究されて, オイラー関数値 $\varphi(p-1)$ に等しいことが示されている. 根幹をなすテーマは高次冪剰余の考察である.

VII. [E 557]「冪の約数に関連して現れる二, 三の顕著な性質について」

さまざまな冪剰余に関する諸命題が列挙されている.

VIII. [E 792]「数に関する考究. 残存する16章」

オイラーの長大な遺稿であり, 標題はもともと欠けていた. 著作を企画していたものと思う. 各章の標題は次の通り.

1. 数の合成
2. 数の約数
3. 数の約数の和
4. 互いに素な数と互いに調和する数([註記] 互いに素ではない二つの数のことを「互いに調和する数」と呼ぶ.)
5. 割り算により生じる剰余

6. アリトメチカ的数列の諸項の割り算により生じる剰余
7. 幾何的数列の諸項の割り算により生じる剰余
8. 素数で割ると1が残る数の冪
9. $a^n \pm b^n$ という形の数の約数
10. 平方数を素数で割るときに生じる剰余
11. 三乗数を素数で割るときに生じる剰余
12. 四乗数を素数で割るときに生じる剰余
13. 五乗数を素数で割るときに生じる剰余
14. 平方数を合成数で割るときに生じる剰余
15. $xx+yy$ という形の数の約数
16. $xx+2yy$ という形の数の約数

こうして各章のタイトルを一瞥するだけでも，数論の領域でオイラーが何らかの体系的叙述を企図していたことは明らかである．第10-13章には平方剰余，三次剰余，四次剰余，五次剰余の理論への意志が垣間見える．一般に高次冪剰余への志向はオイラーに独自の視点であり，ラグランジュにもルジャンドルにもこれは見られない．

高次冪剰余の理論に向かったオイラーの真意は何だったのであろう．論文[E134]「数の約数に関する諸定理」を見ると，$a^4+b^4$，$a^8+b^8$，一般に $a^{2^m}+b^{2^m}$ という形の数の奇約数の形状が調べられている．次数が二次を越える形式で表される数に寄せるオイラーの関心は，すでに相当に早い時期から現れていたのである．素数の平方的形状と線型的形状の相互関連を究明する理論の形成過程をオイラー，ラグランジュ，ルジャンドルとたどっていくと，最後に平方剰余相互法則が決定的な役割を果して完成するが，その平方剰余相互法則の発見者もまたオイラーなのであった．まさしく同様に，オイラーは高次冪剰余の理論においても相互法則の存在を予測して，その土台の上に高次形式に関する素数の形状理論を建設する道筋を模索していたのではあるまいか．

オイラーの後，ガウスは平方剰余相互法則の発見と証明に契機を見いだして数論研究に入ったが，当初から高次冪剰余の理論に深い関心を寄せ，実際にガウス数域において二つの補充法則を伴う四次剰余相互法則を発見した．オイラーが指し示した数論の新たな到達点は，そのままガウスの出発点だったのである．機会があればもう一篇の論説「ガウスの数論」を書き，この間の消息をすっかり明らかにしたいと願っている．

## 参考文献

**Pierre de Fermat (1601-1665)** ピエール・ド・フェルマ

[P. de.Fermat] Œuvres de Fermat , Ⅰ-Ⅳ, eds., P. Tannery and C. Henry, Paris, 1891-1912; Supplément aux tomes Ⅰ-Ⅳ. Documents inédits publiés avec notices sur les nouveaux manuscrits, eds., m. C. de Waard, Paris, 1922.

[P. de Fermat ] Varia opera mathematica , ed, Samuel de Fermat, Tolosae, 1679.

フェルマは1601年8月17日，フランスの Beaumont-de-Lomagneに生れ，1665年1月12日，フランスのCastresで歿した．フェルマには二種類の全集がある．

1. Pierre de Fermat , Varia opera mathematica , Tolosae 1679

フェルマの子どものSamuel de Fermat (1630-1690)がフェルマの歿後，編纂した．1679年刊行．北陸先端科学技術大学院大学附属図書館がファクシミリ版を所蔵している．サミュエル・ド・フェルマには，

Remarques sur Diophante, 1670年刊行.

という著作もある．バシェが刊行したディオファントスのアリトメチカのギリシア語ラテン後対訳テキストを，フェルマの書き込みとともに再刊した書物である．

2. Œuvres de Fermat , Paris, 1891-1912

P. Tannery と C. Henry が編纂した．全4巻.

巻 1. Œuvres mathématiques diverses -- Observations sur diophante, 1891年

巻 2. Correspondance,

巻 3. Traductions par M. Paul Tannery,

巻 4. Compléments par M. Charles Henry,

普通，フェルマ全集というとこれを指すが，この4巻本の全集に，もう一冊，補足の巻がついている．これも全集のうちに含めると全5巻になる．

Supplément aux tomes Ⅰ-Ⅳ. Documents inédits publiés avec notices sur les nouveaux manuscrits, par m. C. de Waard.: Paris, Gauthier-Villars et cie, 1922.

**Leonhard Euler (1707-1783)** レオンハルト・オイラー

オイラー全集は未完結である．五系列で構成され，第一系列は数学著作集である．これは完結した．

Opera Omnia, Teubner, Birkhäuser, 1911- (未完結)

第一系列，数学著作集，全29巻，30冊(完結)

巻2-5(全4冊)=アリトメチカ論文集

[L.Euler 1] (E 26) Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus , Comm. Acad. Sci. Petropol. 6 (1732/3), 1738, p.103-107; Opera omnia, Ser. Ⅰ-2 , p.1-5.

[L.Euler 2] (E 29) De solutione problematum diophanteorum per numeros integros , Comm. Acad. Sci. Petropol. 6 (1732/3) 1738, p.175-188; Opera omnia, Ser. Ⅰ-2 , p.6-17.

[L. Euler 3] (E 54) Theorematum quorundam ad numeros primos spectantium demonstratio, Acad. Sci. Petropol. 8 (1736), 1741, p.141-146 ; Opera Omnia, Ser.I-2, p.33-37.

[L. Euler 4] (E 134) Theoremata circa divisores numerorum, Novi Comm. Acad. Sci. Petropol. 7 (1747/8), 1750, p.20-48 ; Opera Omnia , Ser. I-2, p.62-85.

[L. Euler 5] (E 164) Theoremata circa divisores numerorum in hac forma $paa \pm qbb$ contentorum, Comm. Acad. Sci. Petropol. 14 (1744/46) 1751, p.151-181; Opera Omnia, SerI-2, p.194-222.

[L. Euler 6] (E 228) De numeris, qui sunt aggregata duorum quadratorum, Novi Comm. Acad. Sci. Petropol. 4, (1752/3) 1758, p.3-40; Opera Omnia, Ser. I-2, p.5-8.

[L. Euler 7] (E241) Demonstratio theorematis Fermatiani omnem numerum primum formae $4n+1$ esse summam duorum quadratorum, Novi Comm. Acad. Sci. Petropol. 5 (1754/5), 1760, p.3-13; Opera Omnia, Ser. I-2, p.328 - 337.

[L. Euler 8] (E242) Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum, Novi Comm. Acad. Sci. Petropol. 5 (1754/5), 1760, p.13-58; Opera Omnia, Ser. I-2, p.338-372.

[L. Euler 9] (E 256) Specimen de usu observationum in mathesi pura, Novi Comm. Acad. Sci. Petropol. 6 (1756/7), 1761, p.185-230; Opera Omnia, Ser. I-2, p.459-492.

[L. Euler 10] (E 262) Theoremata circa residua ex divisione potestatum relicta, Novi Comm. Acad. Sci. Petropol. 7 (1758/9), 1761 , p.49-82 ; Opera Omnia , Ser.I-2, p.493-518.

[L. Euler 11] (E 271) Theoremata arithmetica nova methodo demonstrata, Novi Comm. Acad. Sci. Petropol. 8, (1760/1), 1763, p.74-104; Opera Omnia, Ser. I-2, p.531- 555.

[L.Euler 12] (E 272) Supplementum quorundam theorematum arithmeticorum quae in nonnullis demonstrationibus supponuntur, Novi Comm. Acad. Sci. Petropol. 8, (1760/1), 1763, p.105-128; Opera Omnia, Ser. I-2, p.556- 575.

[L.Euler 13] (E 279) De resolutione formularum quadricarum indeterminatarum per numeros integros, 1764 ; Opera omnia, Ser. I -2, p.576-611.

[L.Euler 14] (E323) De usu novi algorithmi in problemate Pelliano solvendo, Novi Comm. Acad. Sci. Petropol. 11, (1765), 1767, p.28-66; Opera Omnia, Ser. I-3, p.73-111.

[L.Euler 15] (E449) Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia, Novi Comm. Acad. Sci. Petropol. 18 (1773), 1774, p.85-135; Opera Omnia, Ser. I-3, p.240-281.

[L. Euler 16] (E 552) Observationes circa divisionem quadratorum per numeros primes, Opuscula analytica I , 1783, p.64-84 ; Opera Omnia , Ser. I-3, p.497-512.

[L. Euler 17] (E554) Disquisitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta, Opuscula analytica I , 1783, p.121-156; Opera Omnia , Ser. I-3,, p.513-543.

[L. Euler 18] (E 557) De quibusdam eximiis proprietatibus circa divisores potestatum occurrentibus, Opuscula analytica Ⅰ, 1783, p.242-295 ; Opera Omnia , Ser. I-4, p.25-64.

[L. Euler 19] (E 559) Nova subsidia pro resolutione formulae $axx+1=yy$, Opuscula analytica Ⅰ, 1783, p.310-328; Opera Omnia , Ser. I-4, p.76-90.

[L. Euler 20] (E 598) De insigni promotione scientiae numerorum, Opuscula analytica Ⅱ, 1785, p.275-314; Opera Omnia , Ser. I-4, p.163 - 196.

[L. Euler 21] (E 610) Novae demonstrationes circa divisores numerorum formae xx + nyy, Nova Acta Acad. Sci. Imperialis Petropol. 1(1787), p.47-74; Opera Omnia, Ser. Ⅰ-4, p. 197 - 220

[L. Euler 22] (E 744) De divisoribus numerorum in forma $mxx+nyy$ contentorum, Mém. de l'acad. des sci. de St.-Petersbourg 5(1812), 1815, p.3-23; Opera Omnia, Ser. Ⅰ-4, p.418-431.

三論文[E 598] [E 610] [E 744] はラグランジュの論文「アリトメチカ研究」の影響を受けて執筆された．オイラーが端緒を開いた素数の形状理論はラグランジュ，ルジャンドルに継承された大きく成長したが，オイラー自身はもう一つの別の道に踏み込んでいったように思う．

[L. Euler 23] (E 792) Tractatus de numerorum doctrina capita sedecim , quae supersunt, Comment. arithm. 2, 1849, p.503-575 ; Opera Omnia, Ser. Ⅰ-5, p.182-283.

**The Euler Archiev**

Web Site

http://www.math.dartmouth.edu/~euler/

本稿で引用したオイラーの諸論文すべてラテン語で書かれているが，このWeb Siteには原論文のタイトルの英語訳が出ている．

**Joseph-Louis Lagrange (1736 - 1813)** ヨセフ・ルイ・ラグランジュ

ラグランジュの全集は全14巻から成る．

Œuvres de Lagrange, 全14巻, Gauthier-Villars, 1867-92

[J. L. Lagrange 1] Solution d'un Problème d'Arithmétique, Miscellanea Taurinensia 4, 1766-1769; Œuvres Ⅰ, p.671-731.

[J. L. Lagrange 2] Sur la solution des Problèmes indéterminés du second dégré, Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin 23, 1769; Œuvres Ⅱ, p. 377-535.

[J. L. Lagrange 3] Sur la résolution des équations numériques, Mémoires de l'Académie. Royale des Sciences et Belles-Lettres de Berlin 23, 1769; Œuvres Ⅱ, p.539-578.

[J. L. Lagrange 4] Additions au Mémoire sur la résolution des équations numériques, Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin 24, 1770; Œuvres

Ⅱ, p.581-652

[J. L. Lagrange 5] Nouvelle méthode pour résoudre les Problèmes indéterminés en nombres entoers, Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin 24, 1770; Œuvres Ⅱ, p.655-726.

[J. L. Lagrange 6] Recherches d'Arithmétique, Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin 1773, 1775; Œuvres Ⅲ, p.695-795. 二回に分けて公表された. 第一部は1773年, 第二部は1775年公表.

**Adrien-Marie Legendre (1752-1833)** アドリアン・マリ・ルジャンドル

[A. M. Legendre 1] Recherches d'analyse indéterminée, Histoire de l'Académie Royale des Sciences , 1785, p.465-559.

[A. M. Legendre 2] Essai sur la théorie des nombres, 1st ed. Paris 1798; 2nd ed. Paris 1808; 3rd ed. Paris 1830.

ルジャンドルの著作『数論のエッセイ』"Essai sur la théorie des nombres"は改訂が重ねられ, 第三版に及んだ. 第二版には二回にわたり補遺が添えられた.

初版　1798年

第二版　1808年

補遺1, 1816年

補遺2, 1825年

第三版　1830年. ２巻本. 書名から"Essai"の一語がとれて"Théorie des nombres (数の理論)"になった.

**Claude Gaspar Bachet de Méziriac (1581-1638)** クロード・ガスパール・バシェ・ド・メジリアック

[O. G. Bachet] Diophanti Alexandrini Arithmeticorum libri sex, et de numeris multangulis liber unus. Nunc primum Graecè et Latinè editi, atque absolutismis commentariis illustrati, Lutetiae Parisiorum, 1621 ; 2nd ed. Tolosae, 1670.

**Leopold Kronecker (1823-1891)** レオポルト・クロネッカー

全集

Werke, Teubner, 1895-1931, 全5巻, 6冊.

[L. Kronecker] Ueber das Reciprocitätsgesetz, Monatsber. Berlin, 1876 , p.331-341; Werke II, p.11-23.

**Carl Friedrich Gauss (1777 - 1855)** カール・フリードリッヒ・ガウス

ガウス全集

Werke, Göttingen, 1863-1933(Olms, 1973), 全12巻, 14冊.

[Gauss 1] Disquisitiones arithmeticae 1801

**Diophantos** ディオファントス

Diophanti Alexandrini Opera Omnia cum graecis commentariis, ed. P. Tannery, Teubner, 2 vol., 1893-1895.

**André Weil (1906-1998)** アンドレ・ヴェイユ

Number Theory an approach through history: From Hammurapi to Legendre, Birkhäuser, 1983.

［平成19年(2007年)1月31日］