DIOPHANTINE EQUATIONS

L. J. MORDELL

DIOPHANTINE EQUATIONS

L. J. MORDELL

ST. JOHN'S COLLEGE
CAMBRIDGE, ENGLAND

1969

ACADEMIC PRESS London and New York

ACADEMIC PRESS INC. (LONDON) LTD.
Berkeley Square House, Berkeley Square, London, W1X 6BA

U.S. Edition published by
ACADEMIC PRESS INC.
111 Fifth Avenue, New York, New York 10003

Second Printing 1970

LIBRARY OF CONGRESS CATALOG CARD NUMBER: 68-9112
SBN: 12-506250-8

PRINTED IN GREAT BRITAIN BY WILLIAM CLOWES AND SONS LT
LONDON AND BECCLES

Preface

Most books on number theory treat with more or less detail various aspects of Diophantine analysis, a subject which can be described briefly by saying that a great part of it is concerned with the discussion of the rational or integer solutions of a polynomial equation $f(x_1, x_2 \ldots, x_n) = 0$, with integer coefficients. It is well known that for many centuries, no other topic has engaged the attention of so many mathematicians, both professional and amateur, or has resulted in so many published papers. Nevertheless, apart from reports or surveys, there are very few books dealing only with Diophantine equations, and sometimes these are either very elementary or deal only with special aspects of the subject. It seems therefore desirable to produce a more representative account, and an attempt is now made to do this. I have tried to preserve the old spirit and traditions of Diophantine analysis, and to these I attach great importance.

It is hoped that all readers will find herein some results which are of interest to them and which do not require too much knowledge. Some well known elementary results have been included for the sake of completeness. Accounts have been given without undue generality of many results which seemed to me of greatest significance, and most representative of the subject. Note has been taken of various Diophantine problems, both classical and recent ones, which seemed worthy of special attention. I have included a number of results, really part of the subject but not usually found in accounts of Diophantine equations, and indicating something about their role in number theory. The material is arranged in a systematic way such that a basic idea runs through each chapter, and it is hoped that the presentation is reasonably self-contained.

The proofs of the results vary considerably. Some are very elementary and others are rather simple, making little demand upon specialized knowledge. This does not apply to the demonstration of the really important theorems. Many require a knowledge of the fundamental results for an algebraic number field, for example, the basis for the integers, the finite generation of the units and the finiteness of the number of classes of ideals. When more knowledge of algebraic numbers is required as for Fermat's last theorem, I state the results assumed in the proof. Occasionally a brief introductory account is given of relevant results or principles required, for example, of some algebraic geometry and the invariants and covariants of binary cubic and biquadratic forms, and also for local or p-adic applications.

This book had its origin in the lectures on Diophantine equations given at Cambridge (England), Toronto (Canada), Varenna (Italy), and Urbana (Illinois), and so the reader must not expect an exhaustive treatise. However, it seemed desirable to enlarge the scope of the book and in particular some mention is made of the more important and worthwhile results, especially recent ones.

A great deal of number theory also arises from the study of the solution in integers of a polynomial equation $f(x_1, x_2, \ldots, x_n) = 0$, and so our subject is coextensive with most of number theory. Hence it becomes necessary to make a choice of material, both classical and modern.

There is no need in this book to go into detail about general Diophantine problems whose study forms part of a general theory to be found in the usual treatises such as the representation of number by quadratic forms in several variables, or by norm forms in algebraic number fields.

No account has been given of theorems whose proofs are of an advanced analytical character such as the applications of the Hardy-Littlewood-Vinogradoff circle method, though many interesting and important results have been found in this way, for example, Waring's theorem on the representation of an integer as a sum of powers, and Davenport's theorem that every homogeneous cubic equation in at least 16 variables has an infinity of integer solutions.

Unless the results are of fundamental importance, arithmetical proofs have also been usually omitted when they are lengthy and complicated, or involve considerable details, or excessive numerical work, or are out of place in this book. Among such instances are Linnik's proof of Waring's theorem, and Siegel's theorem on the solution of the binomial equation $ax^l + by^l = c$. Many striking results on the solution of equations of the form $ax^m + by^n = c$ can be stated very simply but, unfortunately, their proofs require a surprisingly large amount of calculation and so are not discussed here. This applies to proofs of many simple and long sought results given by Ljunggren. An outline, however, is given of some of the specially interesting ones.

I have also omitted a discussion of results which require too much previous preparation and knowledge such as the modern developments linking Diophantine analysis with the new algebraic geometry and homological algebra. These have led to many new points of view as can be seen from Lang's book and Cassels' recent report.

Most of the book is concerned with the classical theory of the subject, in which the unknowns were in general elements of the rational field Q, and the solution of the equation involved only operations in this field. Occasionally solutions were considered in some quadratic and cubic fields, and more importantly in cyclotomic fields in connection with Fermat's last theorem. Further developments led to emphasis on solutions in fields other than Q, and in particular, in finite fields. This required a discussion of the solvability and the number of solutions of a polynomial congruence,

$$f(x) = f(x_1, x_2, \ldots, x_n) = 0 \pmod{p^r},$$

where p is a prime number. Such congruences had previously arisen in the solution of some equations $f(x) = 0$, and in particular in the Hardy-Littlewood analytic solution of Waring's problem that every positive integer n can be expressed as a sum of k r-th powers of non-negative integers where k is independent of n.

Great advances have recently been made by the association of congruences with types of zeta-functions, and many important and suggestive results have been found. In particular, this has led to highly probable conjectures when $f(x) = 0$ is a plane cubic curve of genus one, and a new field of research has been opened up.

Sufficient has been said to show that Diophantine analysis draws upon resources from many branches of mathematics, for example, the higher arithmetic, algebra, geometry, analysis; not only the classical aspects of these subjects but also the most recent developments.

I have much pleasure in acknowledging my great indebtedness to the many writers on Diophantine equations, both ancient and modern, many of whom are not mentioned here. From these, I have learnt much and also derived inspiration. In fact, my interest in the subject was aroused in my school days by reading the chapters on Diophantine equations usually to be found in many of the algebra books of the first half of the nineteenth century. These except for Euler's algebra have long since been forgotten.

Among the writers on Diophantine Equations whom I have studied are Borevich and Shafarevich, Carmichael, Delone and Faddeev, Dickson, Lang, Nagell, Skolem. Many books on number theory also contain useful sections on Diophantine analysis. There may be mentioned those by Bachmann, Hardy and Wright, Landau, Le Veque, Nagell, Sierpenski, Uspensky-Heaslet. I have also consulted many papers and memoirs, in particular those by Billings, Birch and Swinnerton-Dyer, Cassels, Erdös, Fueter, Ljunggren, Nagell, Pocklington, Roth, Selmer, Skolem, Siegel. Many references have been given but the list is by no means complete, especially for the older results. For these Dickson's invaluable "History of the Theory of Numbers" may be consulted.

Nov. 1968 L. J. MORDELL

Acknowledgments

I have much pleasure in acknowledging my very great indebtedness to many colleagues for their numerous comments and suggestions. Among these are Dr A. Baker, Prof. Cassels, Prof. Chalk, Prof. Davenport, Mr Makowski, Mr H. Montgomery, Prof. Nagell, Dr M. Newman, Dr A. Rotkiewicz, Prof. Schinzel, Prof. de Witte. I am very grateful to all of them for their valuable assistance with the manuscript and proof sheets and the resulting clarification in the exposition. Prof. de Witt and Mr Montgomery should be given special mention.

Mr Montgomery also prepared the list of equations.

The book has profited from the great knowledge and the generous help of Prof. Nagell in reading the proof sheets.

I am especially indebted to Prof. Schinzel who made a most painstaking reading and careful scrutiny of the proof sheets. He corrected many errors, noted many obscurities, and suggested numerous improvements.

Finally, I should like to thank the Academic Press for the great help they have given me in preparing my manuscript for publication and for meeting my every wish. It has been a great pleasure to deal with them.

Feb. 1969 L. J. MORDELL

Contents

CHAPTER 1

Introduction

Preliminary

1. Let $x_1, x_2, \ldots, x_n$, say $\mathfrak{x}$, be n variables, and let $f(x_1, x_2, \ldots, x_n)$, say $f(\mathfrak{x})$, be a polynomial in these variables with rational coefficients. There will be no loss of generality in supposing that the coefficients are integers since we shall be concerned with equations $f(\mathfrak{x}) = 0$. An obvious question is the

Problem. To find some or all of the solutions of $f(\mathfrak{x}) = 0$ *in*

I. *rational numbers, i.e. in the field Q;*
II. *rational integers, i.e. in the ring Z.*

Suppose first that $f(\mathfrak{x})$ is a homogeneous polynomial. We ignore the trivial solution $\mathfrak{x} = 0$. Then the questions I and II are clearly† equivalent, and we can confine ourselves to integer solutions with $(x_1, x_2, \ldots, x_n) = 1$.

Suppose next that $f(\mathfrak{x})$ is a non-homogeneous polynomial. On putting

$$x_1 = y_1/y_{n+1}, \ldots, x_n = y_n/y_{n+1},$$

we have a homogeneous equation

$$g(y_1, y_2, \ldots, y_n, y_{n+1}) = 0.$$

There is now a 1–1 correspondence between the rational values of $\mathfrak{x}$, and those integer values of $\mathfrak{y}$ with $y_{n+1} \neq 0$, and $(y_1, y_2, \ldots, y_{n+1}) = 1$.

We may also have simultaneous equations of the type $f(\mathfrak{x}) = 0$, e.g.

$$f_1(\mathfrak{x}) = 0, \ldots, f_r(\mathfrak{x}) = 0.$$

These can be written as the single equation

$$f_1^2(\mathfrak{x}) + \cdots + f_r^2(\mathfrak{x}) = 0.$$

More generally we can impose restrictions upon the variables. Thus we can require them to be positive integers. The simplest significant problem then arising is $x_1 x_2 = n$, and the solutions of the natural questions arising from this lead in due course to the classical results on the divisor problem and the theory of prime numbers. We are also led to Waring's problem on the representation of integers as sums of rth powers. We can require variables to be prime numbers and then problems associated with Goldbach's theorem arise. We may also allow the variables to be algebraic integers, for example, Gaussian integers of the form $x + yi$ where x and y are rational integers.

† This statement due to Gauss is disputed by Dickson.[1,2]

The general problem suggests many questions. Can we find reasonably simple necessary conditions for the solvability of $f(x) = 0$? Are these conditions sufficient? Can we, having found some solutions, deduce from these others or an infinity of others, or all the solutions? What can be said about the number of solutions or their magnitudes in terms of the coefficients of $f(x)$? Questions may also be asked about the arithmetical properties of solutions.

2. *Necessary conditions for solvability.*

Theorem 1

Rational or integer solutions of $f(x) = 0$ can exist only if $f(x) = 0$ can be satisfied by real values of x.

Proof. Obvious.

Theorem 2

Integer solutions of the inhomogeneous equation $f(x) = 0$ can exist only if the congruence

$$f(x) \equiv 0 \pmod{M}$$

has solutions for all integers M.

Proof. Obvious.

The elementary properties of congruences show that we need only consider $M = p^\alpha$ where p runs through the primes and $\alpha = 1, 2, \ldots$.

Theorem 3

Integer solutions $x \neq 0$ of the homogeneous equation $f(x) = 0$ can exist only if the congruence

$$f(x) \equiv 0 \pmod{M},$$

has solutions for which $(x_1, x_2, \ldots, x_n, M) = 1$ for all integers M; and if in particular when $M = p^\alpha$, it has solutions for which not all x are divisible by p.

This is obvious since we may suppose $(x_1, x_2, \ldots, x_n) = 1$ in a homogeneous equation, and this x must satisfy $f(x) \equiv 0 \pmod{M}$.

It is also obvious that if an inhomogeneous equation $f(x) = 0$ implies that $x_1 \equiv x_2 \equiv \cdots \equiv x_n \equiv 0 \pmod{p^\alpha}$, for given p and arbitrary large α, then $x = 0$ is the only solution.

Finally, if the equation $f(x) = 0$ implies that one variable, say x_1, is divisible by p for an infinity of primes p, then there can only be solutions with $x_1 = 0$.

REFERENCES

1. L. E. Dickson. Fallacies and misconceptions in diophantine analysis. A new method in diophantine analysis. *Bull. Amer. Math. Soc.*, 27 (1921), 312–319.
2. L. E. Dickson. "Modern Elementary Theory of Numbers". Univ. Chicago Press, Chicago (1939), Chapter IX.

CHAPTER 2

Equations Proved Impossible by Congruence Considerations

1. We now consider the

Problem. To find by congruence considerations, equations $f(x) = 0$, *with either no integer solutions or only the solution* $x = 0$.

This requires the application of some elementary results in number theory. Many of the results now given are classical. We begin with a preliminary discussion of the equation

$$x_1^r = a + bx_2, \tag{1}$$

where r is an integer > 1. First, let $r = 2$ and so

$$x_1^2 = a + bx_2. \tag{2}$$

This is solvable if and only if the congruences

$$x_1^2 \equiv a \pmod{2^\alpha}, \quad x_1^2 \equiv a \pmod{p^\beta}, \quad x_1^2 \equiv a \pmod{q^\gamma}, \ldots$$

are solvable, where $2^\alpha \parallel b$, i.e. 2^α is the highest power of 2 occurring in b, $p^\beta \parallel b \ldots$. For simplicity, we suppose $(a, b) = 1$. When $\alpha = 1$, the congruence is always solvable; when $\alpha = 2$ only if $a \equiv 1 \pmod 4$; when $\alpha = 3$ only if $a \equiv 1 \pmod 8$, and then it is also solvable for $\alpha > 3$. The congruence is solvable for all β if it is solvable for $\beta = 1$. Then a is called a quadratic residue of p, i.e. $(a/p) = 1$. If the congruence is insoluble, a is called a quadratic non-residue of p, i.e. $(a/p) = -1$. From these results, it follows that every prime divisor p of $x^2 - a$ for integer x is either a divisor of a, or can be represented by a finite number of arithmetic progressions. Thus if $p \mid (x^2 + c^2)$ and $p \neq 2$, then if $(p, c) = 1$, $p \equiv 1 \pmod 4$, but if $p \equiv 3 \pmod 4$, $p \mid c$.

Theorem 1

The equation

$$f(x_1, x_2, \ldots, x_n) = g(x) \tag{3}$$

is impossible in integers if $f(x_1, x_2, \ldots, x_n)$ *has a prime factor* p *which cannot be a divisor of* $g(x)$, *e.g.* $g(x) = x^2 - a$ *where* $(a/p) = -1$.

Proof. Obvious.

Suppose next that $r = 3$ in (1). Then

$$x_1^3 = a + bx_2, \tag{4}$$

and for simplicity we suppose that $(a, b) = 1$. Let $3^\alpha \parallel b, p^\beta \parallel b, \ldots$. Then (4) is solvable if and only if

$$x_1^3 \equiv a \pmod{3^\alpha}, \quad x_1^3 \equiv a \pmod{p^\beta}, \quad x_1^3 \equiv a \pmod{q^\gamma}, \ldots \tag{5}$$

are solvable. When $\alpha = 1$, the first congruence is always solvable. When $\alpha = 2$, it is solvable only when $a \equiv \pm 1 \pmod 9$, and then it is solvable for all α. Take next the second congruence. When $p \equiv 2 \pmod 3$, it is solvable for all β. When $p \equiv 1 \pmod 3$, the condition for solvability is not so simple and it is not easy to specify the values of a for which the congruence is solvable. Then a is called a cubic residue of p and we write $(a/p)_3 = 1$. It might be noted that $(2/p)_3 = 1$ if and only if p can be represented in the form $p = x^2 + 27y^2$ with integers x and y. Similar remarks apply for other values of r.

2. *Congruences* mod M.

We now apply to various equations, congruences mod M, where M is a prime power. We commence with $M = 2^\alpha$.

$M = 4$.

The equation

$$x_1^2 + x_2^2 = 4x_3 + 3 \tag{6}$$

has no integer solutions.

For $x_1^2 \equiv 0, 1$, $x_2^2 \equiv 0, 1$, $x_1^2 + x_2^2 \equiv 0, 1, 2$.

The equation

$$x_1^2 + x_2^2 = (4a + 3)x_3^2 \tag{7}$$

has only the integer solution $x_1 = x_2 = x_3 = 0$.

This is obvious if $a < 0$, and so we need only consider $a \geqslant 0$. From (6), $x_3 \not\equiv 1 \pmod 2$, and so $x_3 \equiv 0 \pmod 2$, and then $x_1 \equiv x_2 \equiv 0 \pmod 2$. Since we may suppose $(x_1, x_2, x_3) = 1$, we have a contradiction unless $x_1 = x_2 = x_3 = 0$.

$M = 8$.

The equations

$$\begin{aligned} & x_1^2 + 2x_2^2 = 8x_3 + 5 \quad \textit{or} \quad 8x_3 + 7, \\ \textit{and} \quad & x_1^2 - 2x_2^2 = 8x_3 + 3 \quad \textit{or} \quad 8x_3 + 5 \end{aligned} \tag{8}$$

have no solutions.

For to mod 8, $x_1^2 \equiv 0, 1, 4$ and so $x_1^2 + 2x_2^2 \not\equiv 5, 7$, $x_1^2 - 2x_2^2 \not\equiv 3, 5$.

The equation

$$x_1^2 + x_2^2 + x_3^2 = 4^\alpha (8x_4 + 7) \tag{9}$$

has no solutions.

If $\alpha \geqslant 1$, $x_1 \equiv x_2 \equiv x_3 \equiv 0 \pmod{2}$, and so we need only consider $\alpha = 0$. But then $x_1^2 + x_2^2 + x_3^2 \not\equiv 7 \pmod{8}$.

The equation

$$ax_1^2 + bx_2^2 + cx_3^2 = 0, \qquad abc \neq 0, \qquad (x_1, x_2, x_3) = 1 \tag{10}$$

has only the trivial solution $x_1 = 0$, $x_2 = 0$, $x_3 = 0$ *if either*

$$a \equiv b \equiv c \equiv 1 \pmod{2} \quad \textit{and} \quad a \equiv b \equiv c \pmod{4},$$

or

$$a/2 \equiv b \equiv c \equiv 1 \pmod{2} \quad \textit{and} \quad b + c \equiv a \textit{ or } 4 \pmod{8}.$$

The result is obvious in the first case since

$$x_1^2 + x_2^2 + x_3^2 \not\equiv 0 \pmod{4}.$$

In the second case, we write

$$ax_1^2 + bx_2^2 + cx_3^2 \equiv 0 \pmod{8}.$$

Clearly x_1, x_2, x_3 are not all odd since $a + b + c \not\equiv 0 \pmod{8}$. Also two of the x cannot be even and so only one can be even. This cannot be x_1 since $b + c \not\equiv 0 \pmod{8}$, nor x_2 since cx_3 is odd, nor x_3 since bx_2 is odd.

The equation

$$z^2 = (ax^2 + by^2)^2 - 2k(cx^2 + dy^2)^2 \tag{11}$$

has no integer solutions $\neq (0, 0, 0)$ *if* $a + b \equiv 0 \pmod{2}$, $cd \equiv 1 \pmod{4}$, $k \equiv 1 \pmod{2}$.

Suppose first that $x \equiv 1 \pmod{2}$, $y \equiv 0 \pmod{2}$. Then

$$z^2 \equiv a^2 - 2c^2 \equiv -1 \text{ or } 2 \pmod{4},$$

and this is impossible. Similarly if $x \equiv 0 \pmod{2}$, $y \equiv 1 \pmod{2}$.

Suppose next that $x \equiv y \equiv 1 \pmod{2}$. Then

$$\left(\frac{z}{2}\right)^2 \equiv \left(\frac{a+b}{2}\right)^2 - 2k\left(\frac{c+d}{2}\right)^2 \pmod{4}$$
$$\equiv -1 \text{ or } 2 \pmod{4},$$

since $c + d \equiv 2 \pmod{4}$.

M = 16.

The equation

$$ax_1^4 + bx_2^4 + cx_3^4 + dx_4^4 = 0, \quad (x_1, x_2, x_3, x_4) = 1 \tag{12}$$

has only the trivial solution $x = 0$ *if*

I. $a \not\equiv 0 \pmod{16}$, *etc.*
II. $a + b \not\equiv 0$, $a + c \not\equiv 0 \pmod{16}$, *etc.*
III. $a + b + c \not\equiv 0$, $a + b + d \not\equiv 0 \pmod{16}$, *etc.*
IV. $a + b + c + d \not\equiv 0 \pmod{16}$.

Since $x_1^4 \equiv 0$ or $1 \pmod{16}$, these conditions exclude in turn one odd value, two odd values etc. for the variables. A simple instance occurs if we take a, b, c, d to be congruent mod 16 to any distinct four of 1, 2, 3, 4, 5, 6.

$M = 2^\alpha$.

The equation

$$ax_1^2 + bx_2^2 + cx_3^2 = 2dx_1x_2x_3, \tag{13}$$

where $a \equiv b \equiv c \equiv \pm 1 \pmod 4$ has only the solution $x_1 = x_2 = x_3 = 0$.

Obviously x_1, x_2, x_3 cannot all be odd, for if one is even, so are the others since then

$$x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod 4.$$

Put $x_1 = 2X_1$, $x_2 = 2X_2$, $x_3 = 2X_3$. Then

$$aX_1^2 + bX_2^2 + cX_3^2 = 4dX_1X_2X_3.$$

Similarly X_1, X_2, X_3 are all even. Hence all the x must be zero since they are divisible by 2^α where α is arbitrary.

$M = 32$.

The equation

$$(a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2)(b_1x_1^2 + b_2x_2^2 + b_3x_3^2 + b_4x_4^2)$$
$$= 2k(c_1x_1^2 + c_2x_2^2 + c_3x_3^2 + c_4x_4^2)(d_1x_1^2 + d_2x_2^2 + d_3x_3^2 + d_4x_4^2) \tag{14}$$

has only the trivial solution $x = 0$ if the a, b, c, d are all odd, and

$$a_1 \equiv a_2 \equiv a_3 \equiv a_4 \pmod 8, \qquad b_1 \equiv b_2 \equiv b_3 \equiv b_4 \pmod 8,$$
$$(c_1 + c_2 + c_3 + c_4)(d_1 + d_2 + d_3 + d_4) \equiv 0 \pmod{16}.$$

We may suppose without loss of generality that

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \equiv 0 \pmod 2.$$

Then either

I. $x_1 \equiv x_2 \equiv x_3 \equiv x_4 \equiv 1 \pmod 2$,

or, say,

II. $x_1 \equiv x_2 \equiv 1 \pmod 2$, $x_3 \equiv x_4 \equiv 0 \pmod 2$.

For I, $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \equiv 4 \pmod 8$, and so the left-hand side of (14) is $\equiv 16 \pmod{32}$. The right-hand side is $\equiv 0 \pmod{32}$, i.e. a contradiction. For II, $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \equiv a_1 + a_2 \equiv 2 \pmod 4$, and so the left-hand side of (14) is $\equiv 4 \pmod 8$. The right-hand side is $\equiv 0 \pmod 8$, i.e. a contradiction.

$M = 3^\alpha$.

$M = 3$.

The equation

$$(3a + 1)x_1^2 + (3b + 1)x_2^2 = 3c, \quad c \not\equiv 0 \pmod 3 \tag{15}$$

has no integer solutions.

Here $x_1^2 + x_2^2 \equiv 0 \pmod 3$, and since $x_1^2 \equiv 0, 1 \pmod 3$, $x_1 \equiv x_2 \equiv 0 \pmod 3$, and this is impossible.

$M = 9$.

The equation

$$x_1^3 + x_2^3 + x_3^3 = 9x_4 \pm 4 \tag{16}$$

has no integer solutions.

This is obvious since $x_1^3 \equiv 0, \pm 1 \pmod 9$.

The equation

$$x_1^3 + 2x_2^3 + 4x_3^3 = 9x_4^3, \qquad (x_1, x_2, x_3, x_4) = 1 \tag{17}$$

has only the trivial solution $x = 0$.

Here $x_1^3 + 2x_2^3 + 4x_3^3 \equiv 0 \pmod 9$. The only solution of this is $x_1 \equiv x_2 \equiv x_3 \equiv 0 \pmod 3$, and then $x_4 \equiv 0 \pmod 3$.

The equation

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3 = z^3 \tag{18}$$

has no integer solutions if

$$a \equiv d \equiv 4 \pmod 9, \qquad b \equiv 0 \pmod 3, \qquad c \equiv \pm 1 \pmod 3.$$

We may suppose $(x, y, z) = 1$. Clearly $xy \not\equiv 0 \pmod 3$, since $4x^3 \equiv z^3 \pmod 9$ requires $x \equiv z \equiv y \equiv 0 \pmod 3$. From (18), $z \equiv ax + dy \pmod 3$,

$$z^3 \equiv a^3x^3 + 3a^2dx^2y + 3ad^2xy^2 + d^3y^3 \pmod 9,$$

and so

$$\left(\frac{a - a^3}{3}\right) x^3 + (b - a^2d)x^2y + (c - ad^2)xy^2 + \left(\frac{d - d^3}{3}\right) y^3 \equiv 0 \pmod 3.$$

Since to mod 3, $x^3 \equiv x$, $x^2 \equiv 1$, we have

$$x + (b - 1)y + (c - 1)x + y \equiv 0 \pmod 3, \quad \text{or} \quad x \equiv 0 \pmod 3,$$

and this has been excluded.

The result implies that the equation

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3 = 1$$

has no rational solutions.

$M = 7.$

The equation

$$(7a + 1)x_1^3 + (7b + 2)x_2^3 + (7c + 4)x_3^3 + (7d + 1)x_1x_2x_3 = 0, \qquad (x_1, x_2, x_3) \equiv 1, \quad (19)$$

has only the trivial solution $x = 0$.

Here $$x_1^3 + 2x_2^3 + 4x_3^3 + x_1x_2x_3 \equiv 0 \pmod 7.$$

Also $x_1^3 \equiv 0, \pm 1 \pmod 7$. It suffices to show that $x_1 \equiv x_2 \equiv x_3 \equiv 0 \pmod 7$; if $x_3 \equiv 0$, $x_1^3 + 2x_2^3 \equiv 0$ and then $x_1 \equiv x_2 \equiv 0$: if $x_3 \not\equiv 0$, we can put $x_1 \equiv X_1x_3$, $x_2 \equiv X_2x_3$, and then

$$X_1^3 + 2X_2^3 + X_1X_2 + 4 \equiv 0.$$

Clearly $X_1X_2 \not\equiv 0$, and so $X_1^3 \equiv \pm 1$, $X_2^3 \equiv \pm 1$. This leads to four impossible cases since

1. $X_1^3 \equiv X_2^3 \equiv 1$ gives $X_1X_2 \equiv 0$,
2. $X_1^3 \equiv X_2^3 \equiv -1$ gives $X_1X_2 \equiv -1$, i.e. $X_1^3X_2^3 \equiv -1$,
3. $X_1^3 \equiv -X_2^3 \equiv 1$ gives $X_1X_2 \equiv 4$, i.e. $X_1^3X_2^3 \equiv 1$,
4. $X_1^3 \equiv -X_2^3 \equiv -1$ gives $X_1X_2 \equiv 2$, i.e. $X_1^3X_2^3 \equiv 1$.

$M = 7^2.$

The equation

$$x_1^3 + 2x_2^3 = 7(x_3^3 + 2x_4^3), \quad (x_1, x_2, x_3, x_4) = 1 \qquad (20)$$

has only the trivial solution $x = 0$.

Here $x_1^3 + 2x_2^3 \equiv 0 \pmod 7$ and so $x_1 = 7X_1$, $x_2 = 7X_2$. Then

$$7^2(X_1^3 + 2X_2^3) = x_3^3 + 2x_4^3.$$

This gives $x_3 = 7X_3$, $x_4 = 7X_4$ and then $(x_1, x_2, x_3, x_4) \geqslant 7$.

An obvious deduction is that the equation

$$x^3 + 2y^3 = 7(z^3 + 2) \qquad (21)$$

has no rational solutions.

$M = p^\alpha$, p a prime.

The equation

$$x_1^2 + 1 = px_2, \qquad p \equiv 3 \pmod 4 \qquad (22)$$

is impossible.

Obvious since $(-1/p) = -1$.

The equation

$$x_1^2 + 1 = ax_2, \qquad (23)$$

is impossible if a has a prime factor $\equiv 3 \pmod 4$.