

1932

# Fermat's last theorem

---

<https://hdl.handle.net/2144/17543>

*"Downloaded from OpenBU. Boston University's institutional repository."*

rgent, L. D.

378.744

B0

A.M. 1932

Boston University  
College of Liberal Arts  
Library

THE GIFT OF the Author

378.744

B0

A.M. 1932

2

P7249

BOSTON UNIVERSITY  
GRADUATE SCHOOL

Thesis

HERBERT'S LAST THEMES

by

Laura Driver Sargent

(A.B., Mount Holyoke, 1922)

submitted in partial fulfilment of the  
requirements for the degree of  
Master of Arts

1932

BOSTON UNIVERSITY  
COLLEGE OF LIBERAL ARTS  
LIBRARY

Oct.

p7249

378.744  
B0  
A.M. 1932  
S

Outline of Thesis  
Fermat's Last Theorem

	Page
I. Statement of Theorem	1
II. Relation of Diophantus to the Problem	2
1. His life	2
2. His works, and translations of his works	2
3. Type of problem he solved, and his methods for solving them	3
III. Fermat	5
1. His life	5
2. His place in the history of mathematics	5
3. Possibility of his having a proof for $x^m + y^m = z^m$	5
4. Type of proofs he used in his work on theory of numbers	7
IV. Present Status of the Problem	8
1. What has been done	8
2. Prizes offered for the solution	8
V. Important Proofs for Special Cases	10
1. When $n=4$	10
a. Importance of having a proof when $n=4$	10
b. Euler's proof	10
c. Fermat's proof that the area of a right triangle can never be a square	11
d. Use of this proof to show that $x^4 + y^4 \neq z^4$	13
e. Mordell's proof	14
2. When $n=3$	16
a. Euler's proof	16



	Page
b. Mordell's comment on Euler's proof	18
c. Carmichael's proof of part not proved by Euler	19
3. Sophie Germain's contribution to the problem	24
4. Dickson's proof for $n < 6857$	26
5. Kummer's invention of ideal numbers the most important development of the theory of the problem	28
VI. Other Methods Applicable to Fermat's Last Theorem	30
1. Use of O. Schmiedel's theorem to prove Fermat's Last Theorem for all values of $n$ and all values of $x, y, z$ , except when one of $x, y, z$ is even.	31
2. Use of this same theorem to prove the equation $x^m + y^m = z^m$ is impossible if $z = x + y$ or if $z > x + y$	32
VII. Summary	34
VIII. Bibliography	35



FERMAT'S LAST THEOREM

1. Statement of Theorem

The equation  $x^n + y^n = z^n$  has an interesting place in the history of the theory of numbers. Fermat in the seventeenth century stated without proof the following theorem which is known as Fermat's Last Theorem.

Carmichael  
p.86

If n is an integer greater than two, there do not exist integers x,y,z, all different from zero, such that  
 $x^n + y^n = z^n$ .

Smith  
(2)  
p.213

This theorem appears beside the eighth proposition of Fermat's copy of the second book of Diophantus. "To divide a square number into two other square numbers". Fermat stated in the margin beside this proposition. "It is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into two powers of like degree; I have discovered a truly remarkable proof which the margin is too small to contain".

Fermat  
p.61

Dickson  
(1)  
p.731

No general proof has yet been given for this theorem, though it has been attempted by the greatest of mathematicians including Euler, Legendre, Gauss, Abel, Dirichlet, Cauchy, and Kummer. The theorem is not of special importance in itself. It has acquired an important position in the history of mathematics, because it afforded the inspiration which led Kummer to his invention of ideal numbers.

Lordell  
p.1

Dickson  
(1)  
p.XIX



II. Relation of Diophantus to the Problem

1. His life

Heath  
(1)  
p.243

The only facts of the personal history of Diophantus are found in an arithmetical epigram, the solution of which gives the following: his boyhood lasted 14 years, he had a beard at 21, married at 33, had a son born 5 years later who died at 42 when his father was 80. and he himself died 4 years later at the age of 84.

Diophantus' dates are not certain. It is probable that he lived somewhere in the second half of the third century. The title of his work shows that he lived at Alexandria.

2. His works and translations of his works

Heath  
(1)  
p.17

The neglect of Diophantus' works by his contemporaries show they were not appreciated or understood.

Smith  
(1)  
p.423

The most ancient manuscript of Diophantus' "Arithmetica" was written in the thirteenth century, about a thousand years after the original one appeared. The works on which the fame of Diophantus rests are:

Heath  
(2)  
p.448

a. The Arithmetica (originally in 13 books)

b. A tract On Polygonal Numbers

c. A collection of propositions under the title of Porisms

We have only six books of The Arithmetica left and only a fragment of the tract On Polygonal Numbers.

A translation of Diophantus was written by Xylander in 1575, based upon a manuscript found about the mid-



dle of the sixteenth century in the Vatican Library, where it had probably been carried from Greece when the Turks took possession of Constantinople.

Lagrange  
p.50

A new translation of Diophantus was published with a commentary by Bachel de Meziriac, Paris, in 1621. It was on a copy of this edition of Diophantus that Fermat wrote his notes, including Fermat's Last Theorem. From the brevity of the notes they must have been intended for experts, or they may have been written just for Fermat's own pleasure.

Gow  
p.102

A reproduction of Diophantus by Heath in modern notation with introduction and notes, published in 1910, is the most complete and up-to-date edition.

Heath  
(1)  
p.54

3. Type of problem he solved, and his methods for solving them

The theory of Diophantine Analysis has been cultivated for many centuries. The extent to which the works of Diophantus are original is not known; but whether his Arithmetica is original or not, he has had a great influence on the development of the theory of numbers.

Carmichael  
p.4

The most of the work of Diophantus on the theory of numbers consists of problems leading to indeterminate equations. The general type of problem is to find a set of numbers, usually 2,3, or 4 in number, such that different expressions involving them in first, second, or third degrees are squares or cubes, or otherwise have a preassigned form.

Hankel says that in 130 indeterminate equations which Diophantus treats, there are more than 50 different classes.....Almost more various than the problems are their



solutions.....Each calls for a quite distinct method,  
 which is often useless for the most closely-related problems.  
 It is therefore difficult for a modern, after studying 100  
 Diophantine equations, to solve the 101<sup>st</sup>.

Gow  
 p.113



### III. Fermat

#### 1. His life

Pierre Fermat was born in 1601 near Montauban. He was the son of a leather merchant. He was educated at home. In 1631 he became councillor for the local parliament at Toulouse. He was distinguished for his legal knowledge and for his integrity of conduct. He spent the remainder of his life at Toulouse, devoting most of his leisure to mathematics. He died at Toulouse on January 12, 1665.

Ball  
(2)  
p.260

#### 2. His place in the history of mathematics

Fermat published nothing except for a few isolated papers. But the remarks, method, and results of Fermat written on the margin of his copy of Diophantus show that he is the greatest master of Diophantine Analysis who has yet appeared. These notes by Fermat gave the fundamental initial impulse to the great work in the theory of numbers that has brought the subject to its present state of advancement.

Carmichael  
p.3

Fermat made use of infinitesimals, and he was probably in possession of the general idea of his method for finding maxima and minima as early as 1628.

Ball  
(2)  
p.265

The rise of the theory of probability may be dated practically from the correspondence of Fermat and Pascal, 1654.

Ball  
(2)  
p.266

3. Possibility of his having a proof for  $x^n + y^n \neq z^n$ , if  $n > 2$ .

Fermat was a mathematician of first rank, and he made a special study of the theory of numbers. It took more than a century before some of the simpler results of



Fermat were proved, and most of them required the skill of Euler, Lagrange, and Cauchy. It is not surprising that a proof of the theorem which he proved only towards the close of his life should present great difficulties. Many centuries elapsed between the solution of the quadratic and of the cubic, but now the solution of the cubic seems simple.

Ball  
1,  
p.42

Mordell  
p.3

There is evident at present among some mathematicians a growing opinion that Fermat's Last Theorem is not true. The case where x,y, and z are not divisible by n seems true, and it has been proved to be true for a great many cases. But for the case where one of the integers x,y,z is divisible by n, no result has been published to show any advance over Kummer's work. Kummer proved  $x^n + y^n + z^n = 0$  impossible for all values of  $n < 100$ .

Encyc.  
Brit.

A proof of the theorem can be given on the assumption that every number can be resolved in one and only one way into the product of primes and their powers. This is true of real numbers, but not true when complex factors are admitted. As example  $10 = (3+i)(3-i) = (3+2i)(3-2i) = 2(2+i)(2-i)$  It is possible that Fermat made such a false assumption, but it is just as probable that he discovered a rigorous proof.

Ball  
(1)  
p.41

No theorem on the subject which Fermat stated he could prove has been shown to be false. Every one but this theorem has been proved to be true. From what is known of Fermat's character it is quite certain that he at least thought he had a proof. He thought  $2^{2^n} + 1$  was a prime number for all positive integral values of n. but he said he could not prove it. Later Euler showed this to be false.

Ball  
(1)  
p.41

Mordell  
p.2



4. Type of proofs he used in his work on theory of numbers

The method used most often by Fermat seems to be one of induction, or as he calls it "la méthode de la descente infinie". It is described in a letter written by Fermat to Carcevi and now in the university library at Leyden. It is undated. It seems from the letter that at the time, Fermat had proved the case only when  $n=3$ .

Ball  
(2)  
p.263

"J'ay ensuite considéré certaines questions qui bien que negatives ne restent pas de recevoir tres-grande difficulté la methode pour y pratiquer la descent estant tout a fait diuerse des precedentes comme il sera aise d'esprouer. Telles sont les suivantes. Il n'y a aucun cube diuisible en deux cubes."

Ball  
(2)  
p.264

Such proofs by Fermat as are extant involve only elementary algebra and geometry, but he used other methods. He proposed, as a problem to the English mathematicians, to show that there was only one integral solution of  $x^2 + 2=y^3$ , the solution being  $x=5, y=3$ . On this he had a note, that there was no trouble in finding a solution of rational fractions, but that he had discovered an entirely new method which made it possible for him to solve such questions in integers. It is Ball's opinion that continued fractions played an important part in Fermat's researches. Ball says that Fermat's theorem that a prime of form  $4n+1$  is expressible as the sum of two squares, may be proved fairly easily by properties of such fractions.

Ball  
(1)  
p.13



IV. Present Status of the Problem

1. What has been done

The greatest mathematicians of the last three centuries have attempted to solve the theorem. Euler, Lagrange, Kummer, and Riemann have all tried, but none of them has been able to give a general proof.

Euler has left a proof when  $n=3$ , but it is incomplete at one point. He had a good proof when  $n=4$ . Legendre in 1823 proved the theorem when  $n=5$ . In 1832 Dirichlet proved it for  $n=14$ ; and in 1840 Lamé and Lebesgue gave a proof when  $n=7$ .

Ball  
(1)  
p.42

In 1849 Kummer, by means of ideal primes, proved the theorem true for all numbers except those, if any, which satisfy three conditions. It is not known whether any numbers can be found to satisfy these conditions. It has been proved that no number less than 100 does.

Sophie Germain attacked the problem on other lines, showing that it was true for all numbers except those, if any, which satisfied certain conditions.

L.E. Dickson has made a study of Fermat's Last Theorem, giving reports in his "Theory of Numbers" for more than 300 papers on the subject. Dickson himself has done a great deal of work on the theorem. He has proved it for integers prime to  $n$  if  $n$  is less than 6857.

Dickson  
(1)  
ch.26

Carmichael  
p.99

In 1925 Feeger proved  $x^n + y^n + z^n = 0$  impossible in integers  $x,y,z$  prime to  $n$  for all primes  $n < 14000$ .

Encyc.  
Brit.

2. Prizes offered for the solution

At different times during the past century,



Dickson  
(1)  
p.742

scientific academies have offered prizes for a proof of the theorem. The French Academy of Sciences offered a gold medal valued at 3000 francs for a proof. The date fixed for the award was postponed several times, and finally the medal was given to Kummer for his work on complex numbers, though he had not been a competitor. Kummer created his famous theory of ideal numbers while trying to prove Fermat's Last Theorem.

Lantzig  
p.55

In 1908 a prize was offered, consisting of

Lantzig  
p.54

100,000 marks, bequeathed to the Academy of Sciences of Göttingen by a Dr. Wolfsköel who had himself devoted a great deal of time to the problem. This prize is to be given before 2007.

Hall  
(1)  
p.42

It is estimated that over 1000 "complete" solutions were sent to the committee on award between 1908-1911.

Lantzig  
p.50

"It is characteristic of all such efforts that their authors completely ignore the tremendous amount of work already done; nor are they interested in learning wherein the difficulty lies."



V. Important Proofs for Special Cases

1. When n=4

a. Importance of having a proof when n=4

Carmichael  
p.87

Since n is greater than 2, it must contain 4 or an odd prime factor p. If n contains the factor 4, we may write  $n=4m$ . Then  $x^n + y^n = z^n$  becomes  $(x^m)^4 + (y^m)^4 = (z^m)^4$ .

If we can prove the case impossible when the exponent is 4, it will be impossible when the exponent is any multiple of 4.

Then it will be sufficient to prove the impossibility of the equation  $x^p + y^p = z^p$  when p is an odd prime.

b. Euler's proof that  $x^4 + y^4 \neq z^4$ , if  $xy \neq 0$

$x^4 + y^4 = z^4$  is the same as  $x^4 + y^4 = \square$

If any 2 of the numbers x,y,z have a common factor p, then the third one is divisible by p. Thus if any equation  $x^4 + y^4 = \square$  exists, there exists one in which x,y and z are relatively prime.

Carmichael  
p.17

If  $(x^2)^2 + (y^2)^2 = \square$ , where x and y are relatively prime, then  $x^2 = p^2 - q^2$ ,  $y^2 = 2pq$  where p and q are relatively prime, one even and the other odd,  $p > q$ . The derivation of this formula for primitive Pythagorean triangles as given by Diophantus is found in Carmichael's "Diophantine Analysis", p.10.

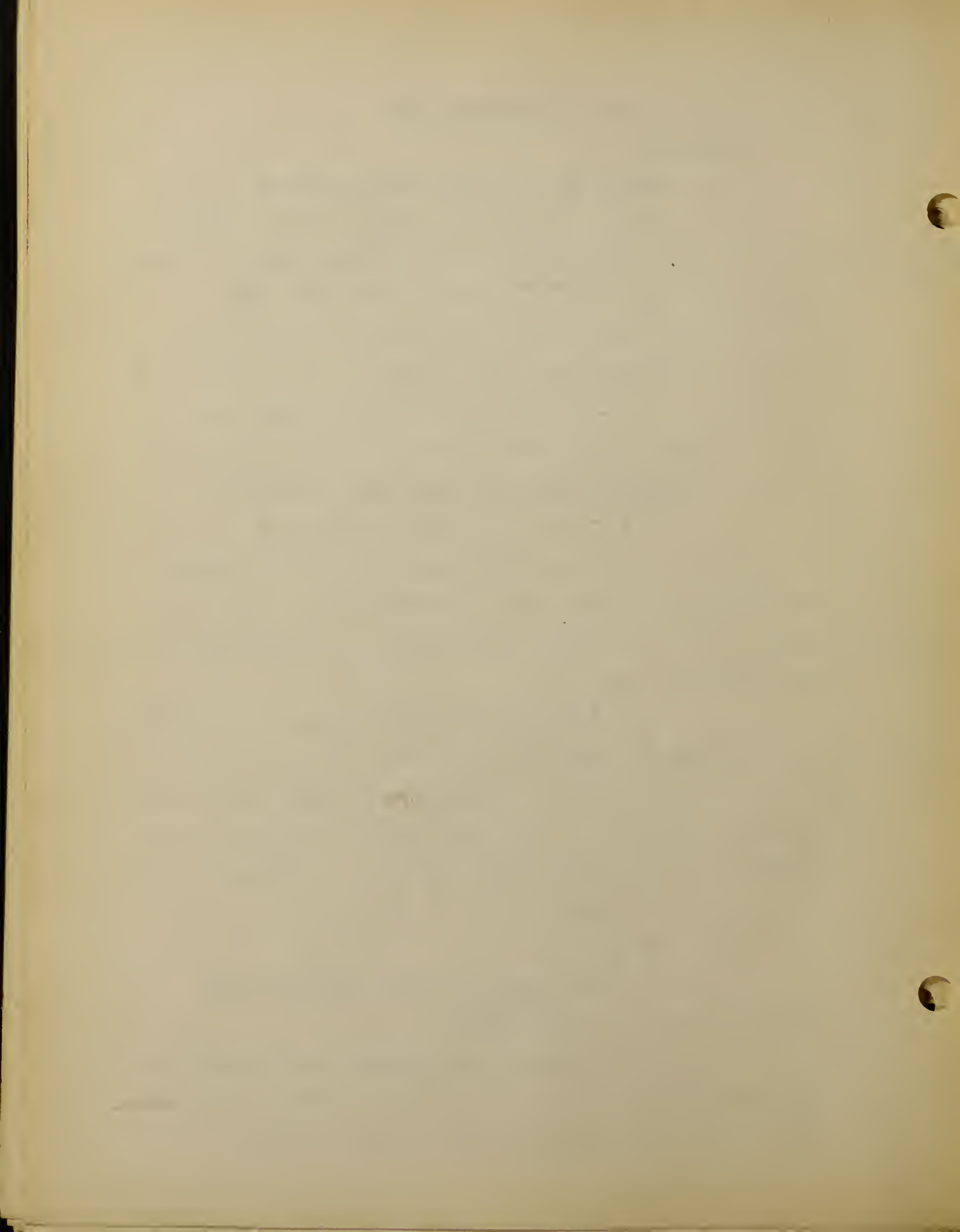
Dickson  
(1)  
p.618

$p^2 - q^2 = x^2$

$p^2 = q^2 + x^2$

x is odd, because x and y are relatively prime, and  $y^2 = 2pq$ , an even number.

Hence, applying the formula for primitive Pythagorean triangles again,  $p = m^2 + n^2$ ,  $x = m^2 - n^2$ ,  $q = 2mn$ ,  $m > n$ , where m and n are relatively prime. Thus q is even.



$p(2q) = y^2$ , so  $p$  and  $2q$  are squares.

$2q = \square$ ,  $2q = 4mn$ , so  $mn = \square$ ,  $m = a^2$ ,  $n = b^2$

Thus  $a^4 + b^4 = \square$ , and  $a$  and  $b$  are less than  $x, y$ .

Proof that  $a$  and  $b$  are less than  $x, y$

$$a^2 = m$$

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

Hence,  $a$  is less than  $x$ , and in like manner we may prove  $b$  less than  $y$ .

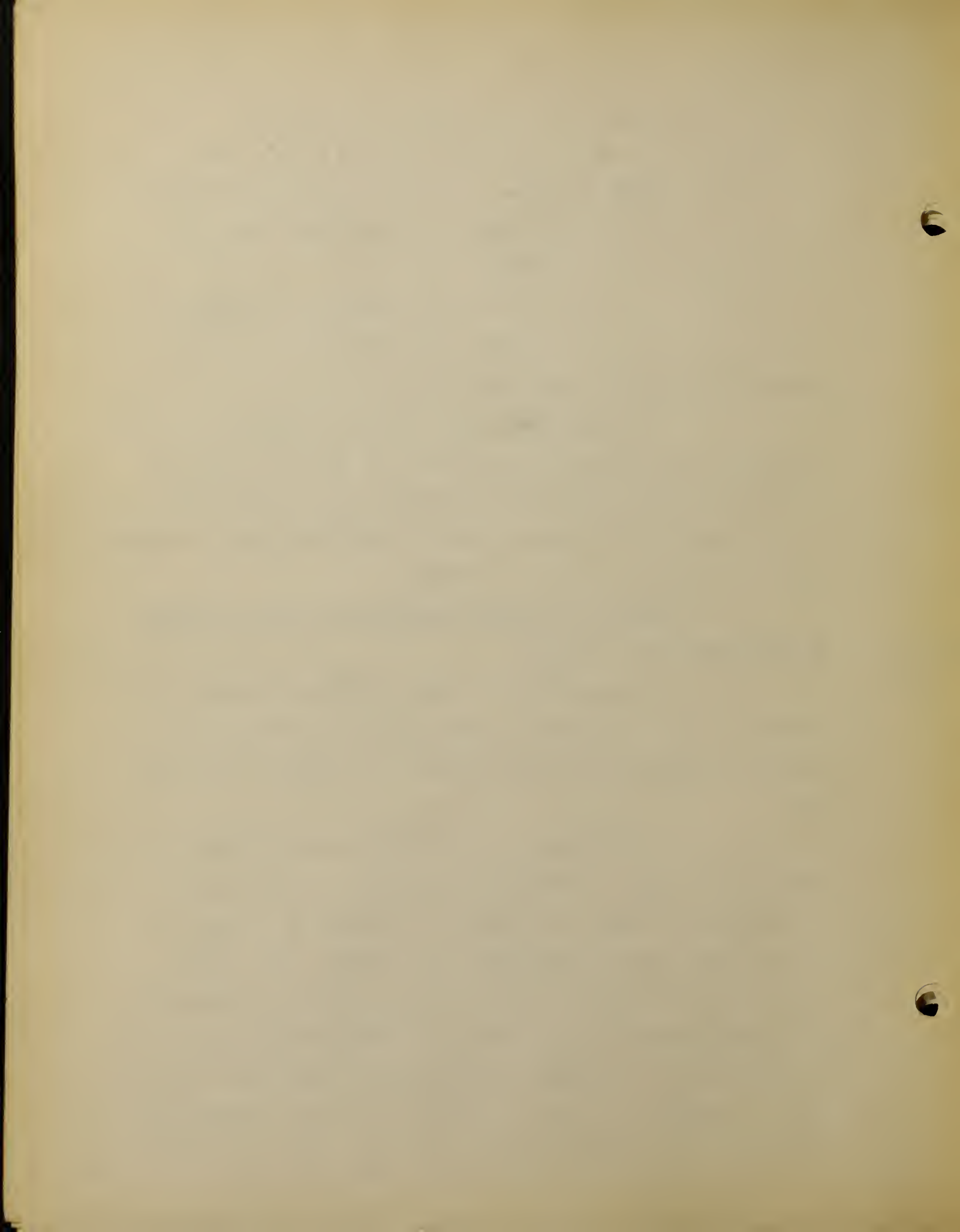
By continuing the process, we can get an infinite number of numbers less than  $x, y$ . such that in each case the fourth power of one plus the fourth power of the other equals a square. But there is not an infinite number of integers less than  $x, y$ . Hence  $x^4 + y^4 \neq \square$ .

c. Fermat's proof that the area of a right triangle is never equal to a square.

Dickson  
(1)  
p. 615

This proof is of great interest, because it illustrates in detail Fermat's method of infinite descent and because it presents the only instance of a detailed proof by him.

A translation of the proof is as follows: "If the area of a right triangle were a square, there would be two biquadrates whose difference is a square, and hence two squares whose sum and difference are squares. Thus there would be a square equal to the sum of a square and the double of a square, such that the sum of the two component squares is a square. But if a square is the sum of a square and the double of a square, its root is likewise the sum of a square and the double of a square, which I can easily prove. It follows



that this root is the sum of the two legs of a right triangle, one of the squares forming the base and the double of the other square the height. This right triangle will therefore be formed from two squares whose sum and difference are squares. But both of these squares can be shown to be smaller than the squares of which it was assumed that the sum and difference are squares. Similarly we would have smaller and smaller integers satisfying the same conditions. But this is impossible, since there is not an infinitude of positive integers smaller than a given one. The margin is too narrow for the complete demonstration and all its developments."

The detailed proof of the statements made here by Fermat is given by Dickson as follows.

Dickson  
(1)  
p.615

If the sides of a right triangle have a common factor, the area has a square factor which may be removed. Now we may assume the sides  $x, y, z$  relatively prime. Then applying the rule of Diophantus,  $x = 2mn$ ,  $y = m^2 - n^2$ , where  $m$  and  $n$  are relatively prime integers, one even and one odd,  $m > n$ .

$$\text{Then } mn(m^2 - n^2) = \square$$

$$m = a^2, n = b^2, m^2 - n^2 = a^4 - b^4 = \square$$

$a$  and  $b$  are relatively prime, one even and one odd. Thus  $a^2 + b^2$  and  $a^2 - b^2$  are relatively prime.

Hence  $a^2 + b^2 = k^2$ ,  $a^2 - b^2 = l^2$ ,  $k$  and  $l$  are odd integers.

$$a^2 = k^2 - b^2, \quad a^2 = l^2 + b^2$$

$$k^2 - b^2 = l^2 + b^2$$

$$k^2 = l^2 + 2b^2$$



$$k^2 - l^2 = 2b^2$$

$$(k+l)(k-l) = 2b^2$$

$$\text{Let } e = \frac{k+l}{2} \text{ and } f = \frac{k-l}{2}$$

$$ef = \frac{k^2 - l^2}{4} = \frac{2b^2}{4} = \frac{b^2}{2}$$

$e$  and  $f$  are integers, because  $(k+l)$  is even, since  $k$  and  $l$  are both odd, and thus  $k+l$  can be divided by 2. A common factor of  $e$  and  $f$  would divide  $l, k, b^2$ , and  $a^2$ . Hence,  $e$  and  $f$  are relatively prime. We may take  $e$  odd, changing if necessary the sign of  $l$ . Thus  $e=r^2$ ,  $f=2s^2$ ,  $2rs=b$ , where  $r$  and  $s$  are integers.

$$\text{Hence } k=e+f=r^2+2s^2$$

$$l=r^2-2s^2$$

$$a^2=b^2+l^2=r^4+4s^4$$

Now we have a right triangle with legs  $r^2$  and  $2s^2$ .  $r^2 = m_1^2 - n_1^2$ ,  $2s^2 = 2m_1n_1$ . The area is  $r^2s^2$ .

$$r^2s^2 = m_1n_1(m_1^2 - n_1^2), \quad m_1 = a_1, \quad n_1 = b_1$$

$$a_1^2b_1^2 = m_1n_1 = s^2$$

$$a_1b_1 = s. \quad s \text{ is a factor of } b = 2rs$$

Hence  $a_1$  and  $b_1$  are each less than  $b$  and hence less than  $a$ .

d. Use of Fermat's theorem that the area of a right

Carmichael triangle is never a square to prove  $x^4 + y^4 \neq z^4$   
p.18

Carmichael states without proof the following corollary: there exist no integers  $x, y, z$  all different from zero such that  $x^4 + y^4 = z^4$ .

$$x^4 = z^4 - y^4$$

$$(z^4 - y^4)z^2y^2 = x^4z^2y^2$$

$$(z^4 - y^4)^2 + (2z^2y^2)^2 = (z^4 + y^4)^2$$

We see that the Pythagorean triangle de-



terminated here has its area  $(z^4 - y^4)(z^2 y^2)$  equal to the square number  $x^4 y^2 z^2$ . But this is impossible. Hence no equation of form  $x^4 + y^4 = z^4$  exists.

e. Mordell's proof that  $x^4 + y^4 \neq z^4$

Mordell  
p.5

It is sufficient to consider  $x^4 + y^4 = z^4$ , when  $x, y, z$  are all relatively prime. It may be assumed that they are all positive. As all numbers are odd or even,  $x$  is of form  $2m$  or  $2m+1$ , where  $m$  is an integer.  $x^2$  is of form  $4m^2$  or  $4m^2 + 4m + 1$ , that is, of form  $4l$  or  $4l+1$ . A number of form  $4l+2$  or  $4l+3$  cannot be a square.  $x$  and  $y$  cannot both be odd, for the sum of their fourth powers would be of form  $4l+2$ , and this cannot be a square. So either  $x$  or  $y$  is even. Let  $y$  be even.

$$(x^2)^2 + (y^2)^2 = z^2$$

$x^2 = a^2 - b^2$ ,  $y^2 = 2ab$ ,  $z = a^2 + b^2$ , where  $a$  and  $b$  are relatively prime, and not both odd, ~~and~~ from  $x^2 = a^2 - b^2$  we see that  $a$  cannot be even, for then  $b$  would be odd, and  $x^2$  would be of form  $4l+3$ . This is impossible.

$$\text{Then } x^2 + b^2 = a^2 \quad b \text{ is even, } a \text{ is odd.}$$

$a$  and  $b$  are relatively prime; so  $a, b$  and  $x$  are relatively prime.

$$\text{Hence } x = p^2 - q^2$$

$$b = 2pq$$

$$a = p^2 + q^2 \quad p \text{ and } q \text{ are relatively}$$

prime and not both odd,  $p > q$

$$\text{From } y^2 = 2ab \text{ we have } y = 4pq(p^2 + q^2)$$

Since  $p$  and  $q$  are relatively prime, each of them must be prime to  $p^2 + q^2$ , hence all three are perfect squares.

$$p = r^2, q = s^2, p^2 + q^2 = t^2, \text{ from which}$$



$$r^4 + s^4 = t^2$$

Now  $x = (r^4 - s^4)$ ,  $y = 2rst$ ,  $z = a^2 + b^2$

$z = a^2 + b^2 = r^8 + 6r^4s^4 + s^8$ , so that

$$z > (r^4 + s^4)^2 > t^4. \quad t \ll z$$

It follows that if one solution of  $x^4 + y^4 = z^2$  is known for which none of the unknowns is zero, another solution  $(r,s,t)$  can be found for which none of the unknowns is zero and such that  $t \ll z$ .

This process can be continued, so that an infinite number of positive integers  $t, t_1, t_2, \dots$  can be found such that  $t_1 \ll t, t_2 \ll t_1, \dots$  but there is not an infinitude of numbers  $\ll t$ . So  $x^4 + y^4 = z^2$  is not possible.



2. When n=3

a. Euler's proof

Euler stated in 1753 that he had proved the problem impossible. His proof is good, but incomplete at one point.

$$x^3 + y^3 = z^3$$

Two of the unknowns  $x, y, z$  must be odd. Suppose  $x$  and  $y$  odd and  $z$  even.

$$x+y=2p, \quad x-y=2q, \quad x=p+q, \quad y=p-q$$

$$x^3 + y^3 = z^3 \text{ becomes } (p+q)^3 + (p-q)^3 = z^3$$

$$p^3 + 3p^2q + 3pq^2 + q^3 + p^3 - 3p^2q + 3pq^2 - q^3 = z^3$$

$$2p(p^2 + 3q^2) = z^3$$

Since  $x$  and  $y$  are relatively prime,  $p$  and  $q$  must be relatively prime.  $p$  and  $q$  cannot both be odd, for then  $x$  and  $y$  would both be even.  $p$  cannot be odd and  $q$  even; for then  $p^2 + 3q^2$  would be odd, and  $z^3$  would be divisible by 2 but not by 8. Hence  $p$  must be even and  $q$  odd, and  $p^2 + 3q^2$  is odd.

Since  $p$  and  $q$  are relatively prime,  $2p$  and  $p^2 + 3q^2$  are either prime to each other or have a common factor 3. In the first case,  $p$  is prime to 3, and hence  $z$  is prime to 3. In the latter case,  $p$  and  $z$  are both divisible by 3.

Case 1.  $p$  and  $q$  have the common factor 1.

$2p$  and  $p^2 + 3q^2$  are relatively prime

$$2p(p^2 + 3q^2) = z^3$$

$2p$  and  $p^2 + 3q^2$  must each be a cube.

Euler stated without rigorous proof



Lickson  
(1)  
p.546

that since  $p^2 + 3q^2$  is a cube, it is the cube of a number of form  $t^2 + 3u^2$  and  $p + q\sqrt{-3}$  is the cube of  $t + u\sqrt{-3}$

$$p + q\sqrt{-3} = (t + u\sqrt{-3})^3$$

$$p + q\sqrt{-3} = t^3 + 3t^2u\sqrt{-3} - 9tu^2 - 3u^3\sqrt{-3}$$

Mordell  
p.7

By equating real and imaginary parts,

$$p = t^3 - 9tu^2, \quad q = 3t^2u - 3u^3, \quad t \text{ and } u \text{ must be}$$

relatively prime and not both odd.

$t$  is not divisible by 3.  $p$  and  $q$  are relatively prime, and  $p$  is not divisible by 3.

Lickson  
(1)  
p.546

$$2p = 2t(t^2 - 9u^2)$$

$2p$  is a cube, so  $2t$  must be a cube, and

$(t+3u), (t-3u)$  must be cubes.

$(t+3u)$  and  $(t-3u)$  are relatively prime since  $p$  and hence  $t$  is not divisible by 3.

$$t+3u = f^3, \quad t-3u = g^3$$

$$2t = f^3 + g^3, \quad 2t \text{ is a cube}$$

Thus we have 2 cubes  $f^3$  and  $g^3$  much smaller than  $x^3, y^3$ , whose sum is a cube  $2t$ .

Lickson  
(1)  
p.546

A similar method of descent is used in the case where  $p=3r$ , when the product of the relatively prime numbers  $\frac{9r}{4}$  and  $3r^2 + q^2$  is a cube.

Case 2.  $2p$  and  $p^2 + 3q^2$  have a common factor 3.

$p$  is divisible by 3, and hence  $z$  is divisible by 3.  $2p(p^2 + 3q^2) = z^3$

Let  $p=3r$

$$\frac{2p(p^2 + 3q^2)}{8} = \frac{z^3}{8}$$

$$\frac{p}{4}(p^2 + 3q^2) = \frac{z^3}{8}$$

$$\frac{3r}{4}(9r^2 + 3q^2) = \frac{z^3}{8}$$

$$\frac{9r}{4}(3r^2 + q^2) = \frac{z^3}{8}$$



$\frac{9r}{4}$  and  $3r^2 + q^2$  must be relatively prime.  
 Hence  $\frac{9r}{4}$  and  $3r^2 + q^2$  must each be a cube. Since  $q^2 + 3r^2$  is a  
 cube, it is the cube of a number of form  $t^2 + 3u^2$ , and  $q + r\sqrt{-3}$   
 is the cube of  $t + u\sqrt{-3}$ .

$$q + r\sqrt{-3} = (t + u\sqrt{-3})^3$$

$$q + r\sqrt{-3} = t^3 + 3t^2u\sqrt{-3} - 9tu^2 - 3u^3\sqrt{-3}$$

$$q = t^3 - 9tu^2$$

$$r = 3t^2u - 3u^3, \quad r = 3u(t^2 - u^2)$$

$$\frac{8 \cdot 9r}{27 \cdot 4} = \frac{2r}{3} = 2u(t+u)(t-u)$$

$\frac{9r}{4}$  is a cube, so  $2u(t+u)(t-u)$  is a cube.

$2u, t+u, t-u$  must be cubes.  $t+u$  and  $t-u$

are relatively prime.

$$t+u = f^3, \quad t-u = g^3$$

$2u = f^3 - g^3$ . Since  $2u$  is a cube,  $f^3 - g^3$  is a  
 cube. Thus we have 2 cubes,  $g^3$  and  $2u$  whose sum is a cube  $f^3$ .  
 We have 2 cubes smaller than  $x^3, y^3$  whose sum is a cube.

#### b. Mordell's comment on Euler's proof

Euler stated that by equating real and imagin-  
 ary parts in  $p + q\sqrt{-3} = (t + u\sqrt{-3})^3$ ,  $p = t^3 - 9tu^2$ ,  $q = 3t^2u - 3u^3$

Mordell explains that though this method does  
 give suitable values of  $p, q, r$  satisfying  $p^2 + 3q^2 = r^3$ , it is not  
 obvious that all the values of  $p, q, r$  can be found in this way,  
 though it is a fact in this particular case. If the equation  
 had been  $p^2 + 11q^2 = r^3$ , all the values of  $p$  and  $q$  would not be  
 given by putting  $p + q\sqrt{-11} = (m + n\sqrt{-11})^3$ .

"The removal of this difficulty involves the  
 study of the arithmetical theory of the binary quadratic form  
 or of ideal numbers."



c. Carmichael's proof of the part not proved by Euler

Euler did not have a rigorous proof for finding the general solution of  $p^2 + 3q^2 = s^3$ , where  $p$  and  $q$  are relatively prime integers and  $s$  is odd. Carmichael has a result which he gets by means of 3 lemmas.

Carmichael  
p.67

Lemma 1. If a number is expressible in the form  $d^2 + 3B^2$ , and if the quotient  $\frac{d^2 + 3B^2}{a^2 + 3b^2}$  is an integer  $m$ , where  $d, B, a, b$  are integers and  $a^2 + 3b^2$  is a prime number, then  $m$  is expressible in the form  $r^2 + 3d^2$ , where  $r$  and  $d$  are integers.

Proof (not given in Carmichael, but based on a similar one of his on p.39.)

$$m = \frac{d^2 + 3B^2}{a^2 + 3b^2} = \frac{(d^2 + 3B^2)(a^2 + 3b^2)}{(a^2 + 3b^2)^2} = \frac{(da \pm 3Bb)^2 + 3(db \mp Ba)^2}{(a^2 + 3b^2)^2} = \left(\frac{da \pm 3Bb}{a^2 + 3b^2}\right)^2 + 3\left(\frac{db \mp Ba}{a^2 + 3b^2}\right)^2$$

Since  $a^2 + 3b^2$  is a prime, if it is a factor of the product of the numbers  $(da \pm 3Bb)$  it is a factor of one of the numbers.

$$d^2 a^2 - 9B^2 b^2 = a^2 (d^2 + 3B^2) - 3B^2 (a^2 + 3b^2) = (ma^2 - 3B^2)(a^2 + 3b^2)$$

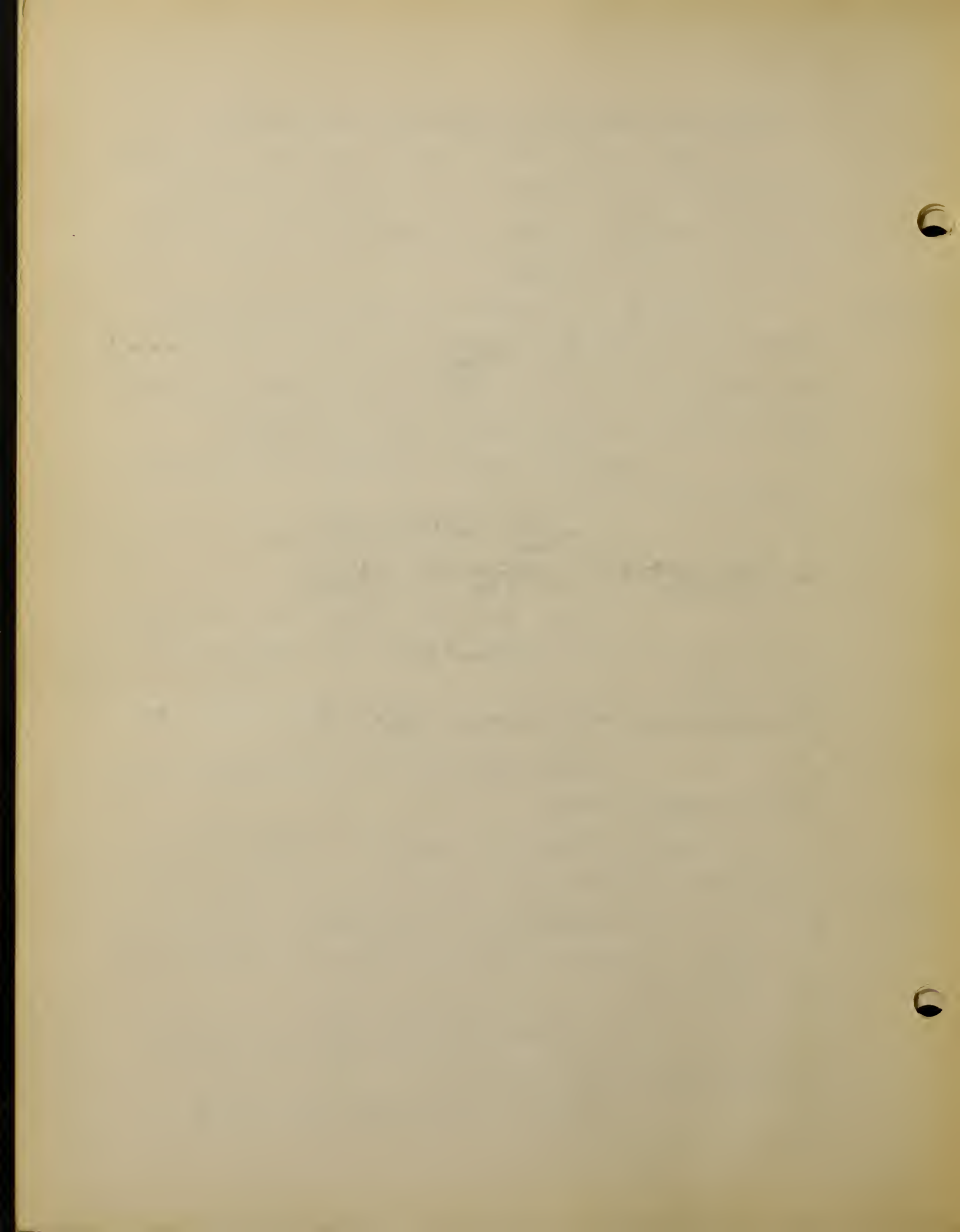
Thus we see that  $a^2 + 3b^2$  is a factor of either  $da + 3Bb$  or  $da - 3Bb$ .

Lemma 2. Every prime number of the form  $6n+1$  can be represented in one and in only one way in the form  $a^2 + 3b^2$  where  $a$  and  $b$  are integers. No prime number of the form  $6n-1$  is a divisor of a number of the form  $a^2 + 3b^2$  where  $a$  and  $b$  are relatively prime.

Proof (not given in Carmichael, but based on a similar one of his on p.39.)

We start from the fact that  $-3$  is a

Carmichael  
p.67  
p.68



quadratic residue of primes of form  $6n+1$  and of no other primes.

This means that every prime number of form  $6n+1$  is a factor of a number of form  $t^2+3$ , where  $t$  is a positive integer, while no prime of form other than  $6n+1$  is a factor of  $t^2+3$ .

If we take for  $t$  the least integer such that a prime number  $p$  of form  $6n+1$  is a factor of  $t^2+3$ , then  $t^2+3=pk$ ,  $k < p$ .

Now consider set of numbers

$$1^2+3, 2^2+3, 3^2+3, 4^2+3, \dots \quad (1)$$

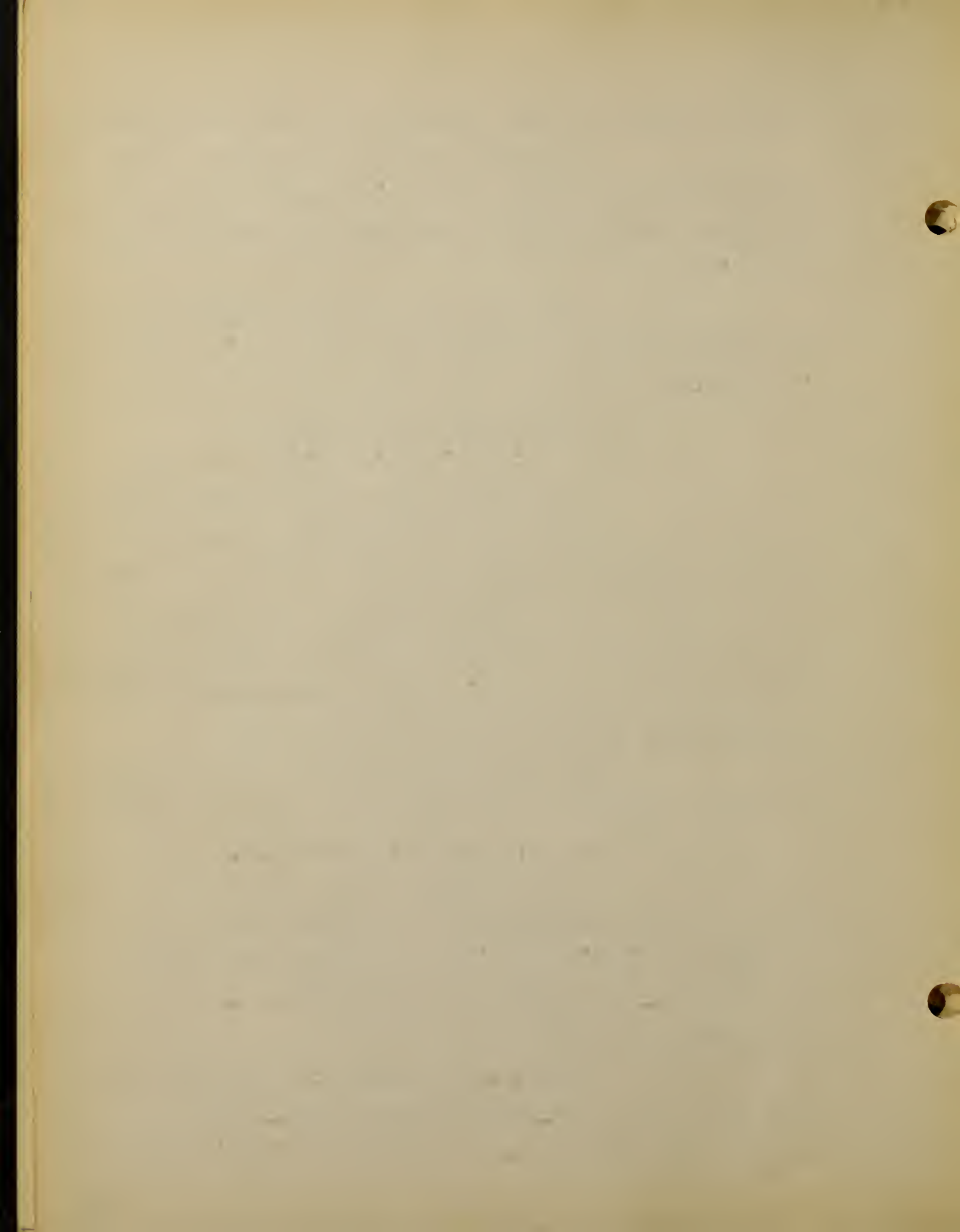
It is obvious that if any of these numbers contains 2 prime factors, one of the prime factors must be a factor of a preceding number of the set. For if one of the numbers contains 2 prime factors neither of which is a factor of a preceding number of the set, the smaller of these primes must be a factor of a number  $t^2+3$  with a complementary factor less than itself and hence less than the other prime.

Arrange all prime numbers of form  $6n+1$  in the order in which they occur as factors of numbers in set (1).

$$p_1=7, p_2=19, p_3=13, p_4=67, p_5, p_6, \dots \quad (2)$$

This set contains every prime of form  $6n+1$ . Suppose  $p_m$  is a prime number of set (2) which is not expressible as  $a^2+3b^2$ . Let  $t^2+3$  be the first number of set (1) of which  $p_m$  is a factor and by means of which  $p_m$  was assigned its place in (2).

Then  $p_m k_m = t^2 + 3$ , where  $k_m$  is such that every prime factor of  $k_m$  appears earlier than  $p_m$  in set (2). If every prime factor of  $k_m$  is expressible as  $a^2 + 3b^2$ , then a



repeated use of Lemma I in connection with  $k_m = t^2 + 3$  would lead to the conclusion that  $p_m$  is expressible as  $a^2 + 3b^2$ . But this is contrary to the hypothesis concerning  $p_m$ . Hence there is some prime factor of  $k_m$  which is not expressible as  $a^2 + 3b^2$ .

Thus we have proved, that if any prime of set (2) is not expressible as  $a^2 + 3b^2$ , then there is an earlier prime likewise not expressible as  $a^2 + 3b^2$ . This contradicts the fact that the first primes of this set are each expressible as  $a^2 + 3b^2$ . Hence every prime in set (2) is expressible as  $a^2 + 3b^2$ .

Now we must show that no prime  $p$  can be represented in 2 ways as  $a^2 + 3b^2$ .

$$\text{Assume } p = a^2 + 3b^2 = c^2 + 3d^2 \quad (3)$$

$a$  and  $c$  are even,  $b$  and  $d$  are odd.

Now prove  $a^2 = c^2$ ,  $b^2 = d^2$

$$p^2 = (ac + 3bd)^2 + 3(ad - bc)^2 = (ac - 3bd)^2 + 3(ad + bc)^2 \quad (4)$$

$$p(a^2 - c^2) = a^2(c^2 + 3d^2) - c^2(a^2 + 3b^2) = 3ad^2 - 3cb^2 = 3(ad - cb)(ad + cb)$$

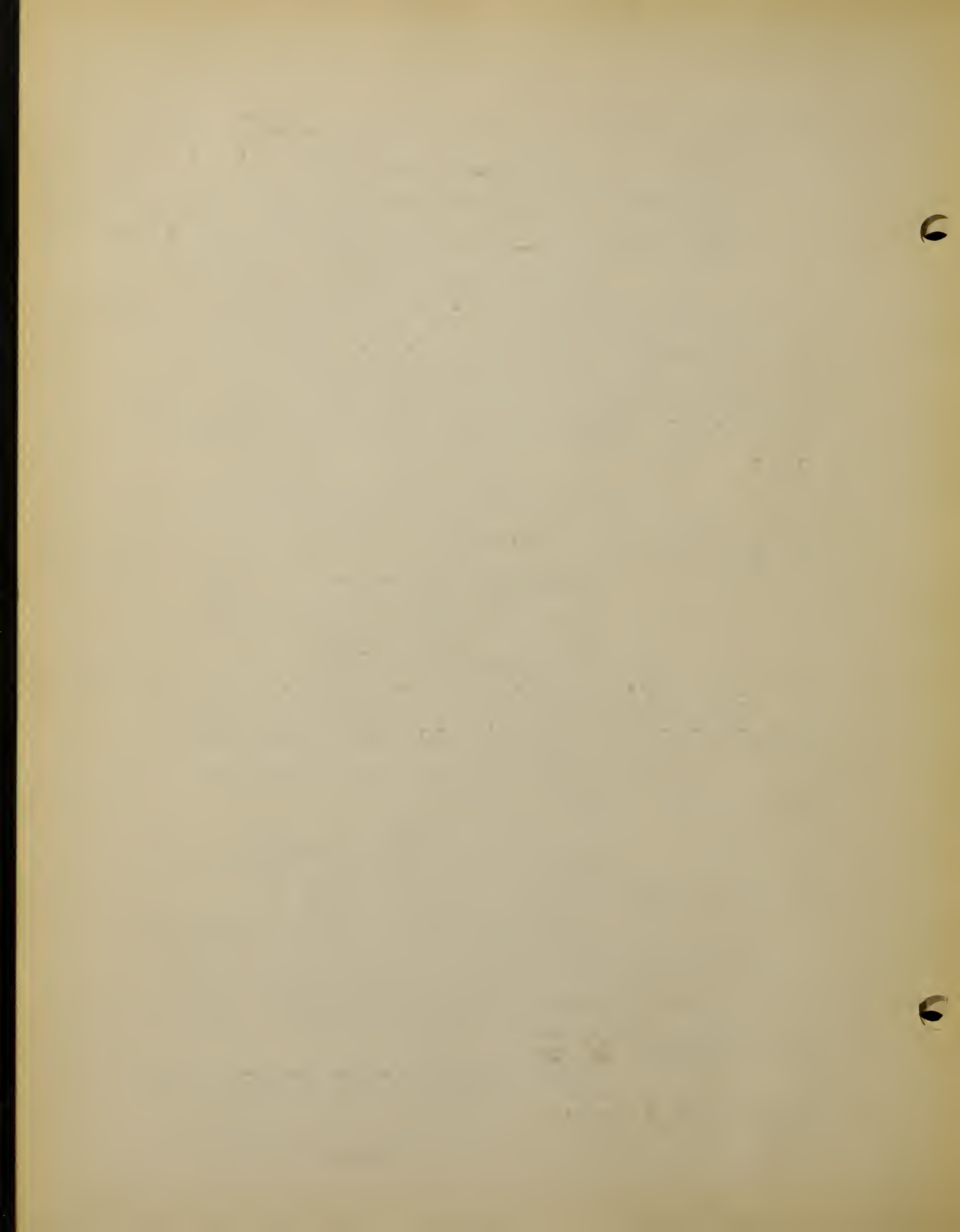
$p$  is a factor of one of the numbers  $ad - cb$ ,  $ad + cb$ .

Neither of the numbers  $ac + 3bd$  or  $ac - 3bd$  is equal to zero, since both of them are odd.

Hence from (4) we see that  $3(ad - bc)$  and  $3(ad + bc)$  are both less than  $p$  in absolute value. But one of them is divisible by  $p$ , and hence that one is equal to zero. Therefore,  $\frac{a^2}{c^2} = \frac{b^2}{d^2}$

From this and  $p = a^2 + 3b^2 = c^2 + 3d^2$ , it follows that  $a^2 = c^2$ ,  $b^2 = d^2$ .

From the first statement we see that no



prime number of form  $6n-1$  is a divisor of a number of form  $a^2+3b^2$ , where  $a$  and  $b$  are relatively prime.

Carmichael  
p.67

Lemma 3. Let  $p$  be a prime number of form  $6n+1$  and write  $p=a^2+3b^2$ , where  $a$  and  $b$  are integers. Let  $m$  be any integer such that  $pm=\alpha^2+3\beta^2$ , where  $\alpha$  and  $\beta$  are integers. Then there exists a representation of  $m$  as a sum of 4 integral squares,

$$m = \left( \frac{a\alpha + 3b\beta}{a^2+3b^2} \right)^2 + 3 \left( \frac{\alpha b + a\beta}{a^2+3b^2} \right)^2$$

such that the representation  $\alpha^2+3\beta^2$  of  $pm$  is obtained from the foregoing representation of  $p$  and  $m$  by multiplication in accordance with the formula

$$(a^2+3b^2)(c^2+3d^2) = (ac+3bd)^2 + 3(ad-bc)^2$$

Proof

Carmichael  
p.42

We showed in Lemma 1 that  $m$  has the value given here. That this representation has the further property specified may be seen by direct computation.

Carmichael  
p.67

Corollary. If  $h$  is a composite number all of whose prime factors are of the form  $6n+1$  and if we write  $h=h_1h_2$ , where  $h_1$  and  $h_2$  are positive integers, then every representation of  $h$  in the form  $a^2+3b^2$  is obtained by taking every representation of  $h_1$  and  $h_2$  and multiplying these expressions in accordance with the formula

$$(a^2+3b^2)(c^2+3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2$$

Now we use these lemmas to find the general solution of  $p^2+3q^2=s^3$ , where  $p$  and  $q$  are relatively prime integers and  $s$  is odd.

$s$  must have form  $t^2+3u^2$ ,  $t$  and  $u$  are integers.



$$(t^2+3u^2)(t^2+3u^2)=(t^2\pm 3u^2)^2+3(tu\mp ut)^2$$

$$[(t^2\pm 3u^2)^2+3(tu\mp ut)^2][(t^2+3u^2)]=[(t^2\pm 3u^2)t\pm 3(tu\mp ut)u]^2$$

$$+[(t^2\pm 3u^2)u\mp (tu\mp ut)t]^2$$

Use lower signs, as  $tu-ut=0$ .

$$[(t^2-3u^2)t-3(tu+ut)u]^2+3[(t^2-3u^2)u+(tu+ut)t]^2=p^2+3q^2$$

$$p=t^3-3u^2t-6tu^2=t^3-9tu^2$$

$$q=t^2u-3u^3+2t^2u=3t^2u-3u^3$$

$$\text{Hence } p=t^3-9tu^2, \quad q=3u(t^2-u^2)$$

These are the same results as Euler had for values of  $p$  and  $q$ .



3. Sophie Germain's contribution to the problem

All writers on the subject of Fermat's Last Theorem have found it necessary to separate the case where no one of the integers  $x, y, z$  is divisible by the prime  $n$ , from the case where at least one of them is divisible by  $n$ . For the first case Sophie Germain (1778-1831) invented a simple method.

Dickson  
(2)  
p.14

She proved that if  $n$  is an odd prime  $< 100$ ,  $x^n + y^n + z^n = 0$

Dickson  
(1)  
p.734

has no integral solutions each prime to  $n$ .

Consider  $x, y, z$  as relatively prime.

Let  $\frac{y^n + z^n}{y+z} = \phi(y, z) = y^{n-1} - y^{n-2}z + y^{n-3}z^2 - \dots + z^{n-1}$

Then  $y+z$  and  $\phi(y, z)$  are relatively prime.

Proof for this fact:

Dickson  
(2)  
p.14  
p.15

Suppose  $x^n + y^n + z^n = 0$  has integral solutions  $x, y, z$ , without a common divisor and no one a multiple of the odd prime  $n$ .

Since  $(-x)^n = y^n + z^n = (y+z)\phi$ ,  $\phi(y, z) = y^{n-1} - y^{n-2}z + \dots + z^{n-1}$  a common prime factor of  $y+z$  and  $\phi$  would divide  $x$  and

$\phi(y, -y) = ny^{n-1}$ , contrary to our assumptions.

Hence  $y+z$  and  $\phi$  are exact  $n^{\text{th}}$  powers whose product is  $(-x)^n$ .

Let $y+z = a^n$	$\phi(y, z) = \lambda^n$	$x = -a\lambda$	(1)
$z+x = b^n$	$\phi(z, x) = \mu^n$	$y = -b\mu$	
$x+y = c^n$	$\phi(x, y) = \nu^n$	$z = -c\nu$	

Hence  $2x = b^n + c^n - a^n$

$2y = a^n + c^n - b^n$

$2z = a^n + b^n - c^n$

Theorem; If there exists an odd prime  $p$  such that  $q^n + r^n + s^n \equiv 0 \pmod{p}$  has not a set of integral solutions  $q, r, s$



each not divisible by  $p$ , and such that  $n$  is not the residue of the  $n^{\text{th}}$  power of any integer modulo  $p$ , then  $x^n + y^n + z^n = 0$  has no integral solutions each prime to  $n$ .  $n \not\equiv 0 \pmod{p}$

For, if  $x, y, z$  are integers satisfying  $x^n + y^n + z^n = 0$ , they satisfy  $q^n + r^n + s^n \equiv 0 \pmod{p}$  so that one of them, say  $x$ , is divisible by  $p$ . Then by  $2x = b^n + c^n - a^n$

$$2y = a^n + c^n - b^n$$

$$2z = a^n + b^n - c^n$$

$$b^n + c^n + (-a)^n \equiv 0 \pmod{p}$$

Hence  $a, b$ , or  $c$  is divisible by  $p$ . But if  $b$  were divisible by  $p$ , then  $y = -ba$  would be divisible by  $p$ . Hence by  $x^n + y^n + z^n = 0$  also  $z$  would be divisible by  $p$ . But  $x, y, z$  have no common factor. Similarly  $c$  is not divisible by  $p$ .

$$\text{Hence } a \equiv 0, x \equiv 0, z \equiv -y, \varphi(x, y) \equiv y^n, \varphi(y, z) \equiv ny^{n-1} \pmod{p}$$

$$\text{Thus by (1) } v^n \equiv y^n, x^n \equiv ny^{n-1}$$

$$\text{Hence } n \cdot v^{n-1} \equiv x^n \pmod{p}$$

By the final equation of (1),  $v$  is prime to  $p$ .

Hence we can determine an integer  $r$ , such that  $vr \equiv 1 \pmod{p}$

$$\text{Thus } n \equiv (vr)^n \pmod{p} \text{ contrary to hypothesis.}$$

The theorem applies if  $n=7$ ,  $p=29$ , since the residues of the  $7^{\text{th}}$  powers modulo 29 are  $\pm 1, \pm 12$ , no two of which differ by unity, and no one of which is congruent to 7.

Similarly for each odd prime  $n < 100$ , Sophie Germain gave a  $p$  for which the theorem applies.



#### 4. Dickson's proof for $n < 6857$

We have seen that Sophie Germain proved the impossibility of  $x^n + y^n + z^n = 0$  for integers not divisible by the odd prime  $n$  for every odd prime  $n < 100$ .

Legendre proved it for  $n < 200$ .

Maillet extended the limit to 223, Dirimanoff to 257.

Dickson in his paper on the subject which appeared in volume 38 of "Messenger of Mathematics" still further extended the limit to  $n < 1700$ .

The theorem as stated by Sophie Germain is: if there exists an odd prime  $p$  such that  $q^n + r^n + s^n \equiv 0 \pmod{p}$  has not a set of integral solutions  $q, r, s$  each not divisible by  $p$ , and such that  $n$  is not the residue of the  $n^{\text{th}}$  power of any integer modulo  $p$ , then  $x^n + y^n + z^n = 0$  has no integral solutions each prime to  $n$ .

Dickson showed restrictions on the selection of the prime  $p$  required here. He showed  $3n$  must not divide  $p-1$ . Hence  $p = mn + 1$  ( $m$  is an even integer prime to 3)

In his first paper Dickson investigated the values  $m \leq 32$  and  $m = 40, 56, 64$ . The earlier values were treated simultaneously, and the aim was to avoid a sub-division into cases.

In his second paper, by extending the range of the  $m$ 's to include all values  $< 74$  as well as 70 and 128, with a proof covering almost 20 pages Dickson proved Fermat's equation  $x^n + y^n + z^n = 0$  is impossible in integers prime to  $n$  for every odd prime  $n < 6857$  and for the larger primes  $< 7000$ . He says, "I have not taken the trouble to treat this case, which

Dickson  
(2)  
p.14

Dickson  
(2)  
p.10

Dickson  
(3)  
p.27

Dickson  
(1)  
p.763

Dickson  
(3)  
p.45



falls just below the limit 7000".

Dickson  
(1)  
p.763

Dickson states in his Theory of Numbers that he has proved the last theorem true for integers prime to  $n$  for  $n < 7000$ . In a footnote on the same page it is stated that the omitted value  $n=6857$  was later shown in MS. to be excluded, which apparently leaves 7000 as the limit reached by Dickson with the exception of the value  $n=6857$ .



5. Kummer's invention of ideal numbers the most important development of the theory of the problem.

A proof of Fermat's Last Theorem can be given on the assumption that every number can be factored into primes in one and only one way. I have pointed out on page 6 that this is true of real numbers, but not true when complex factors are admitted.

Example:  $21=3 \times 7=(4+\sqrt{-5})(4-\sqrt{-5})=(1+2\sqrt{-5})(1-2\sqrt{-5})$ .

Mordell p,14

Mordell gives a proof that  $4+\sqrt{-5}$  cannot be factored into factors of form  $a+b\sqrt{-5}$ ; so we call it a prime. he says. Hence we see that 21 can be factored into primes in 3 ways. Can the group of algebraic numbers of form  $a+b\sqrt{-5}$  be enlarged by joining a new group of numbers so that the factor law of arithmetic holds for this enlarged group?

Mordell p.16

Hilbert gives the following simple illustration to show that although in one set of numbers the laws of arithmetic may not hold, by adding another set to the first set, a third set of numbers may be produced in which the laws of arithmetic do hold. Consider the odd integers of form  $4n+1$ .

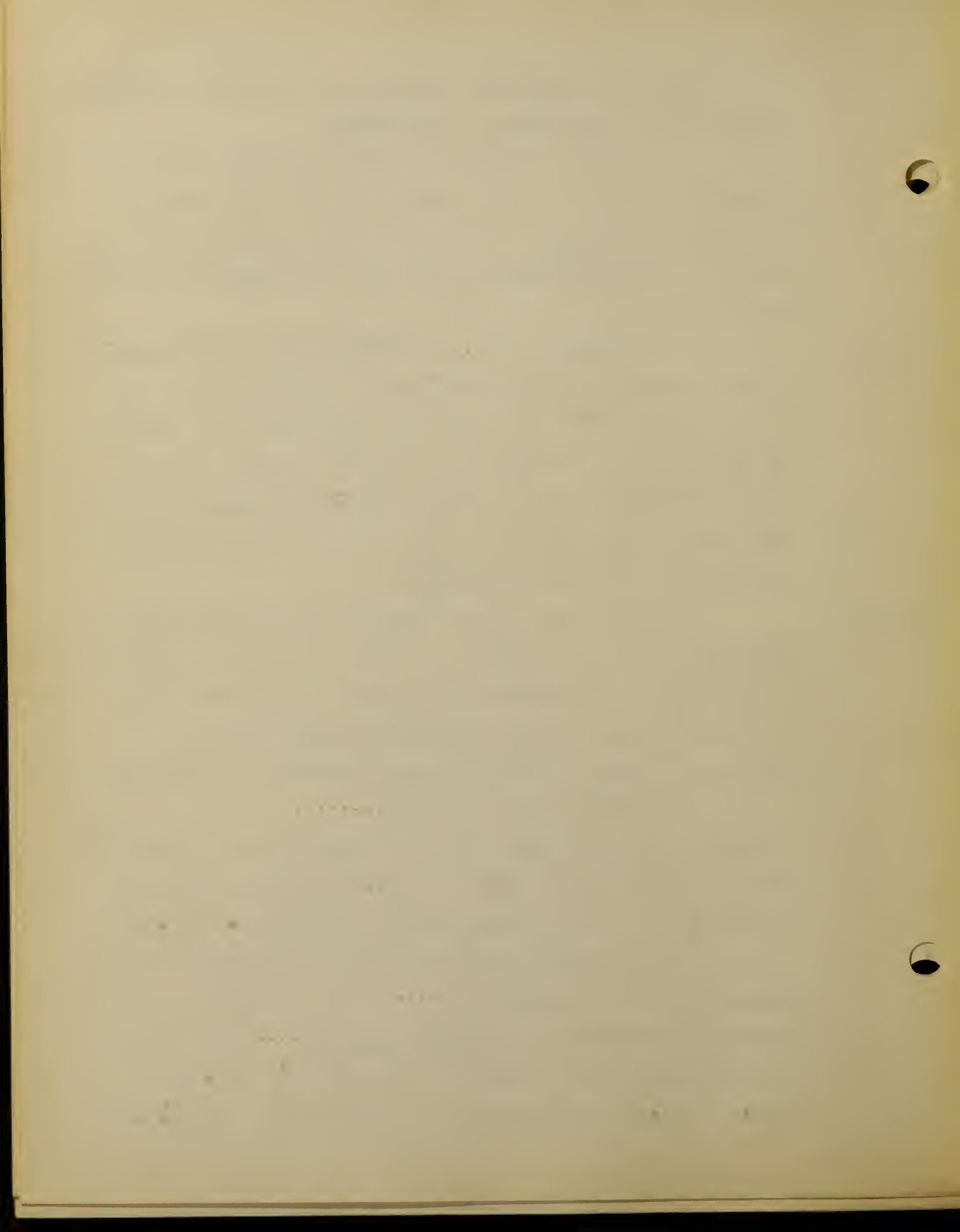
$1, 5, 9, 13, 17, 21, 25, 33, 37, 41 \dots \dots \dots$  (1)

A number a will be called a prime in this set if it cannot be written in form  $a=bc$ .  $b, c \neq 0$ .  $21=3 \times 7$ . Neither 3 nor 7 is in this set, so 21 is a prime number. Also  $693=9 \times 77=21 \times 33$ .

Now consider in addition the odd numbers of form  $4n+3$ .  $3, 7, 11, 15, 19 \dots \dots \dots$  (2)

Then in the new group of integers  $1, 3, 5, 7, 9 \dots \dots$  (3)

the ordinary laws of arithmetic hold, and  $9=3^2$ ,  $77=7 \times 11$ ,  $21=3 \times 7$ ,  $33=3 \times 11$ , so 693 factors in only one way.  $693=3^2 \times 7 \times 11$ .



In a like manner Kummer shows how all algebraic numbers can be enlarged by joining a new group of numbers so that the factor law of arithmetic holds for this enlarged group. As stated on page 8, by means of this new group of numbers which he called ideal numbers, Kummer proved the theorem true for all numbers except those, if any, which satisfy three conditions. It is not known whether any number can be found to satisfy these conditions, but Kummer proved that no number less than 100 does.

Note: A very good account of ideal numbers may be found in Foundations of The Theory of Algebraic Numbers by H. Hancock, published in December 1931 by Macmillan.



VI. Other Methods Applicable to Fermat's Last Theorem.

- Most of the work which has been done on Fermat's Last Theorem deals with the value of the exponent  $n$ . Much less seems to have been done with the  $x, y, z$ . disregarding the value of  $n$ . C. Jaquet (1651-1729) thought he had a proof which held regardless of the value of  $n$  if  $n > 2$ ; but his conclusion was shown by E. Lucas to be wrong. There have been other similar attempts. E. Laporte (1874) tried to prove the theorem from the fact that the series of powers higher than the second are formed by the summation of terms of arithmetical progressions preceded by extraneous terms. R. Sauer (1905) did succeed in proving that  $x^n + y^n = z^n$ ,  $n > 2$ , does not hold if  $x, y$ , or  $z$  is a power of a prime; and F. Borletti (1887) proved that if  $n$  is a prime  $> 2$ ,  $x^n + y^n = z^n$  has no positive integral solution if  $z$  is a prime.
- Dickson (1) p. 731
- Dickson (1) p. 747
- Dickson (1) p. 761
- Dickson (1) p. 754

It seems to me that much more might be done attacking the problem along these lines. It would seem that a theorem stated by O. Schmiedel might be of use in this connection. Schmiedel stated that any power of an integer may be expressed as the sum of consecutive odd numbers. thus;  $a^n = (a^n - a + 1) + (a^n - a + 3) + \dots + (a^n + a - 1)$ . If the integer is  $a$ , the sum consists of  $a$  consecutive odd numbers. I have used this theorem to prove  $x^n + y^n = z^n$ ,  $n > 2$ , is not true for all values of  $n$  and all values of  $x, y, z$ . except when one of the numbers  $x, y, z$  is even, and to prove the equation is not true if  $z = x + y$  or if  $z > x + y$ . Perhaps it is because they are quite obvious that I have not come across these results in my reading on the subject.

We might prove  $x^n + y^n = z^n$ ,  $n > 2$ , not true if  $x, y, z$  are



all odd by the fact that the  $n^{\text{th}}$  powers of  $x, y$ , and  $z$  would be odd, and the sum of 2 odd numbers cannot be an odd number. Likewise, we might as easily prove  $x^{\sim} + y^{\sim} = z^{\sim}, n > 2$ , not true if  $z = x + y$  or if  $z > x + y$ . But because I have been searching for different methods that might be applicable to Fermat's Last Theorem, I give the following results by use of O. Schriedel's theorem.

1. Use of O. Schriedel's theorem to prove  $x^{\sim} + y^{\sim} = z^{\sim}$   $n > 2$ , not true for all values of  $n$  and all values of  $x, y, z$ , except when one of the numbers  $x, y, z$  is even.

If any 2 of the numbers  $x, y, z$  are divisible by 2, the third one must be also. Then we may divide by  $2^{\sim}$ , getting an equation  $x_{\sim} + y_{\sim} = z_{\sim}$ . If any 2 of these numbers are divisible by 2, the third one must be, so divide by  $2^{\sim}$  again. Continue the process until we get an equation  $x_{\sim} + y_{\sim} = z_{\sim}$  in which no 2 of the numbers  $x, y, z$  are divisible by 2. Hence at least 2 of them are odd.

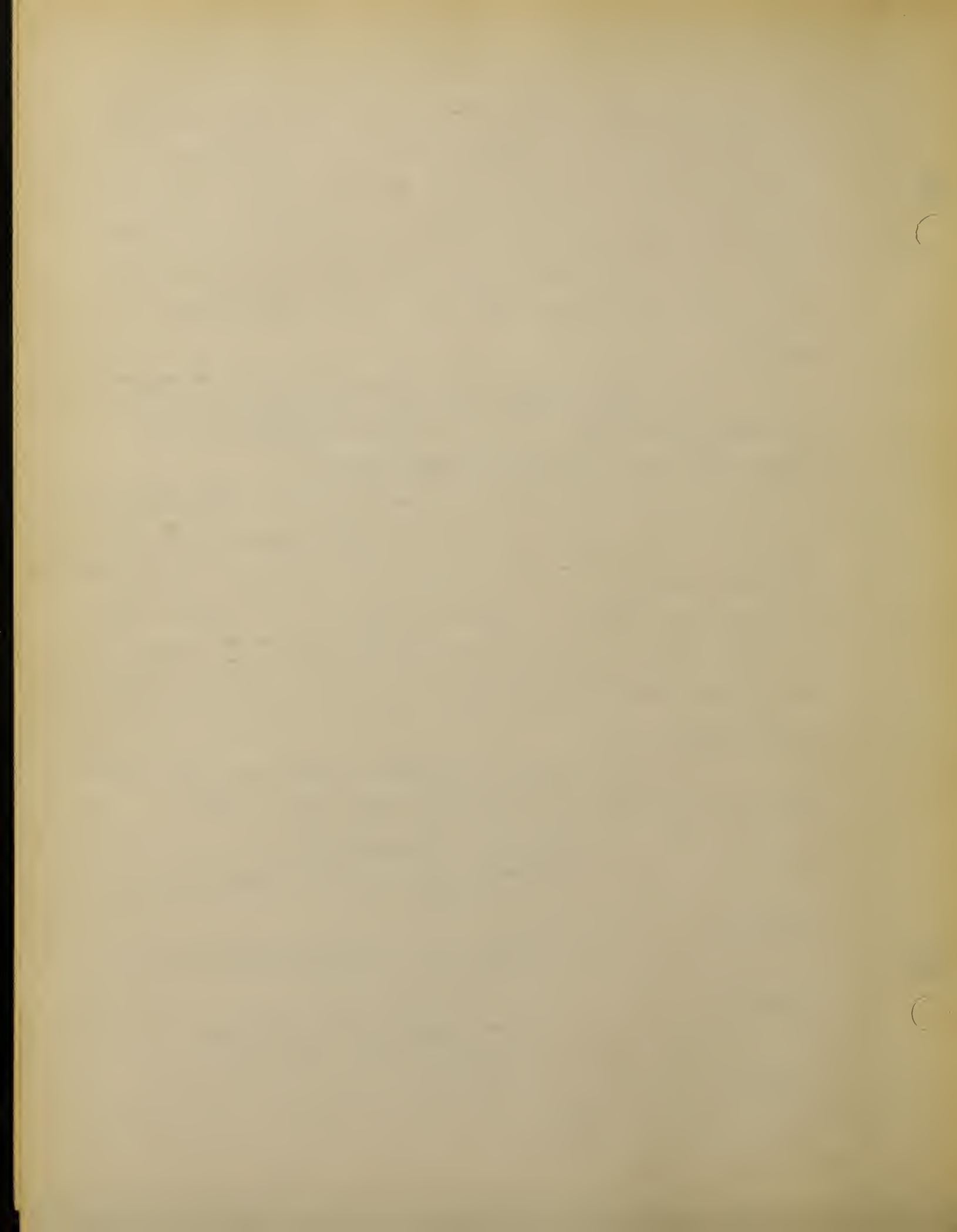
Now we have to consider the case only when  $x, y, z$  are all odd, or the case when one of them may be even.

Case 1.  $x, y, z$  all odd

$x^{\sim}$  is made up of  $x$  consecutive odd numbers.

$y^{\sim}$  is made up of  $y$  consecutive odd numbers.

$z^{\sim}$  is made up of  $z$  consecutive odd numbers.



$$\begin{aligned}
& [(x^{n-1} - x + 1) + (x^{n-1} - x + 3) + \dots + (x^{n-1} - x + 2x - 1)] + \\
& [(y^{n-1} - y + 1) + (y^{n-1} - y + 3) + \dots + (y^{n-1} - y + 2y - 1)] = \\
& [(z^{n-1} - z + 1) + (z^{n-1} - z + 3) + \dots + (z^{n-1} - z + 2z - 1)]
\end{aligned}$$

Cancel out x odd terms as indicated above. Then the remaining terms of the x series are all even, and their sum must be even. The y terms are odd, and there is an odd number of them, so their sum is odd. x of the z terms are now even. (z-x), which is even, of the z terms are still odd. So the sum of the z terms is even.

Hence even + odd = even Impossible

Case 2. One of x,y,z is even

I can get no proof to cover this case.

2. The equation  $x^n + y^n = z^n$  is impossible if  $z = x + y$  or if  $z > x + y$ .

Case 1. If  $z = x + y$

Let  $y > x$ . Then  $z > y$ .

If  $z = y$ ,  $z^n = y^n$ , and  $x^n = 0$

If  $z < y$ ,  $z^n < y^n$ , and  $z^n < y^n + x^n$ , but  $z^n = y^n + x^n$

Hence  $z > y$ .

Since x,y,z are all integers, z must be at least 1 greater than y. By O.Schmiedel's theorem,

$$y^n = (y^{n-1} - y + 1) + (y^{n-1} - y + 3) + \dots + (y^{n-1} + y - 1)$$

z might = (y+1) or > (y+1)

Let  $z = y + 1$

$$\begin{aligned}
\text{Then } z^n = & [(y+1)^{n-1} - (y+1) + 1] + [(y+1)^{n-1} - (y+1) + 3] + \dots + \\
& + [(y+1)^{n-1} + (y+1) - 1]
\end{aligned}$$

Thus we see that there are x odd numbers added to y odd numbers, giving at least y+1 odd numbers.

6

7

The largest number on the left side is  $y^{n-1} + y - 1$ . (1)

The least number on the right side is at least

$$(y+1)^{n-1} - (y+1) + 1.$$

$$(y+1)^{n-1} - (y+1) + 1 = [y^{n-1} + \frac{n-1}{1}(y)^{n-2} + \frac{(n-1)(n-2)}{2}(y)^{n-3} + \dots + 1] - (y+1) + 1 \tag{2}$$

Now compare (1) with (2). The second term of (2).

$$\frac{n-1}{1}(y)^{n-2} = \text{at least } 2y, \text{ since } n \text{ is at least } 3.$$

Hence we see that (2) > (1). i.e. The first term of  $z^n$  > the largest term of  $y^n$ .

Likewise the first term of  $y^n$  > last term of  $x^n$ .

Hence the sum of the  $z$  odd numbers > the sum of the  $x$  and the sum of the  $y$  odd numbers.

Case 2. If  $z > (x+y)$

Same proof as case 1. only there will be still more on the  $z$  side.

Case 3. If  $z < (x+y)$

I can get no proof for this case.



### Summary

The study of Fermat's Last Theorem has been for me a fascinating one. There is an endless amount of material available on the subject, so it was with some difficulty that I decided upon those parts which I have finally included in this paper.

I have given, perhaps, more than is necessary about Diophantus; but I did so because he was the one who was really responsible for the whole discussion.

Of the great many special proofs that have been made, I have included the case when  $n=4$  because of its importance in the resulting simplification of the problem. I have given in detail all the work necessary to prove the case when  $n=3$ , because by its complexity it helps to indicate how very difficult the general problem is.

Sophie Germain's contribution I have included, partly because her proof enabled Dickson to set 6857 as his limit for  $n$ , and partly because hers is the only woman's name I have come across in the history of the theorem.

Dickson's and Kummer's proofs are much too long to be reproduced in my paper, but I have attempted to give at least some idea of the greatness of the contribution of each.

Finally, I have pointed out that although most of the work which has been done on this famous theorem deals with the value of the exponent  $n$ , more attacks on the problem from the standpoint of the  $x,y,z$  might be valuable.

6

6

Bibliography

1. Ball, W.W.R.  
(1) Mathematical Recreations and Essays  
1914, Macmillan and Co.
2. Ball, W.W.R.  
(2) History of Mathematics  
1888, Macmillan and Co.
3. Carmichael, R.D. Diophantine Analysis  
1915, John Wiley & Sons
4. Dantzig, T. Number, the Language of Science  
1930, Macmillan and Co.
5. Dickson, L.E.  
(1) History of the Theory of Numbers  
Vol.2. Diophantine Analysis  
1920, Carnegie Institution of Washington
6. Dickson, L.E.  
(2) On the Last Theorem of Fermat  
1909, The Messenger of Mathematics, Vol.38  
Macmillan and Co.
7. Dickson, L.E.  
(3) On the Last Theorem of Fermat  
1908, Quarterly Journal of Pure and Applied Mathematics, Vol.40  
Longmans, Green, and Co. London
8. Fermat, P. Diophanti Alexandrini Arithmeti-  
corum libri sex, et de numeris multangulis  
liber unus. Cum commentariis C.G.  
Bacheti et observationibus D.P. de Fermat  
1670. Tolosae
9. Gow, J. History of Greek Mathematics  
1884, Cambridge, University Press
10. Heath, T.L.  
(1) Diophantos of Alexandria  
1885, Cambridge, University Press



11. Heath, T.H. (2) A History of Greek Mathematics (Vol.2)  
1921, Oxford, Clarendon Press

12. Lagrange, J.L. Elementary Mathematics  
1898, Open Court Publishing Co.

13. Mordell, L.J. Three Lectures on Fermat's Last Theorem  
1921, Cambridge, University Press

14. Schmiedel, Oscar The Theorem of Nicomachus  
1920, School Science and Mathematics, May  
Smith and Turton

15. Smith, D.E. (1) History of Mathematics (Vol.2)  
1925, Ginn and Co.

16. Smith, D.E. (2) Source Book in Mathematics  
1929, McGraw-Hill Book Co.

17. Encyclopaedia Britannica 14<sup>th</sup> Edition, 1929

Only those parts of the above books which dealt with the subject of the thesis were studied, with the exception of Carmichael's Diophantine Analysis which I have studied in detail. I found that part of Dickson's history which deals with Fermat's Last Theorem and Mordell's book especially valuable.



BOSTON UNIVERSITY



1 1719 02575 2785

