5-1940

A study of Fermat's last theorem.

Jerome L. Krumpelman
University of Louisville

UNIVERSITY OF LOUISVILLE

A STUDY OF FERMAT'S LAST THEOREM.

A Dissertation

Submitted to the Faculty

Of the Graduate School of the University of Louisville

In Partial Fulfillment of the

Requirements for the Degree

Of Master of Arts.

Department of Mathematics.

By

Jerome L. Krumpelman.

Year

1940

NAME OF STUDENT: Jerome L. Krumpelman

TITLE OF THESIS: A Study of Fermat's Last Theorem

APPROVED BY READING COMMITTEE COMPOSED OF THE FOLLOWING MEMBERS:

Walter L. Moore

Guy Stevenson

NAME OF DIRECTOR: Charles Loewner

DATE: May 24, 1940.

TO

HELEN EMILY SHERMAN

CONTENTS

		Page
Purpose of Treatise		1
Chapter		
I.	Introduction	3
II.	Method of Infinite Descent and its Application when $n = 3, 4, 5$.	9
III.	An Introduction to the Nature of Ideals	26
IV.	Resumés of Articles Published on Fermat's Last Theorem from 1919 to 1938.	34
V.	Books Published from 1919 to 1938	66
VI.	Bibliography	70

PURPOSE OF TREATISE

This work is intended primarily for the student of mathematics who may not necessarily wish to delve into the complete theory of the problem, but who may wish to get a picture of the work necessary to study and understand it. For a complete history of the problem until 1919, refer to Chapter XXVI of Dickson'S History of the Theory of Numbers, II, and for the work primarily connected with Irregular Cyclotomic Fields and Fermat's Last Theorem through part of 1927, refer to Algebraic Numbers, II, National Research Council Bulletin, # 62. For a short presentation of the problem refer to Mordell, Three Lectures on Fermat's Last Theorem. For a more detailed analysis of the methods used to work on this problem refer to Bachmann, Das Fermatproblem.

The author of this treatise has attempted to cover certain points. First, to give the nature of Fermat's Last Theorem. Second, an introduction, which will contain some historical facts of the Last Theorem, a reference to the mathematical development which resulted from this problem, and its status at the present. Third, a detailed account of the method of infinite descent. The cases $n = 3, 4, 5$ are used to show this method of attack. For $n = 5$ the procedure is that of Dirichlet.(1) In order that a better understanding may be secured of various steps in his proof, all the theorems of his article are reproduced without proof. Fourth, an introduction to the theory of ideals. This is not an exhaustive study of ideals but an attempt to aid the beginner to understand them.

Fifth, this treatise will also give a detailed account of the work done on this problem from 1919 to 1938 presented in two parts: first, resumes of all papers (2) published during that time; and second, a list of books published in the same period.

.....

(1) Dirichlet, G. L. : Mémoire sur l'impossibilité de quelques équations indéterminees du cinquieme degré; Journal für Mathematik, 3, 1828, pp. 354-75.

(2) The author was unable to give the results of two papers; the first by Georgikopulas, 1931, he was unable to secure, the second by Niewiadomski, 1938, he was unable to translate.

CHAPTER I

INTRODUCTION

Fermat, about 1637, stated that "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 this margin is too small to contain." [6] This theorem is known as Fermat's Last Theorem. This problem may be more simply stated by the equation $x^n + y^n = z^n$, where x, y, z, and n are rational integers.

Since Fermat made this statement concerning the problem which bears his name there have been published over 350 papers which have contributed toward the advancement of the solution of this problem. P. Wolfskehl, in 1908, bequeathed to the K. Gesellschaft der Wissenschaften zu Gottigen one-hundred-thousand marks to be offered as a prize for a complete proof of Fermat's Last Theorem. It may be noted that Wolfskehl was the author of a paper on the related subject of the class number for complex numbers formed of eleventh and thirteenth roots of unity. Following the announcement of this prize over one-thousand false proofs were published, mostly as pamphlets. This retarded the work on the problem as eminent mathematicians were spending their time disproving the claims. The printers were the ones who benefited by these false proofs as the prize stipulated they must be published.

The attempts to prove that the equation $x^n + y^n = z^n$ has no solutions in positive rational integers, none zero, has probably contributed more to the development of the theory of algebraic numbers than any other one problem. "Fermat's Last Theorem is not of special importance in itself, and the publication of a

complete proof would deprive it of its chief claim to attention for its own sake. But the theorem has acquired an important position in the history of mathematics on account of its having afforded the inspiration which led Kummer to his invention of his ideal numbers out of which grew the general theory of algebraic numbers, which is one of the most important branches of modern mathematics."(2)

In attacking Fermat's Last Theorem it is convenient to break it up into two cases and treat each separately. "If

$$x^p + y^p + z^p = 0$$

is satisfied in rational integers x, y, z prime to the odd prime p, this will be referred to as Case I of Fermat's Last Theorem; and if one of these integers is divisible by p with x, y, z prime to each other this will be referred to as Case II of the theorem."(3) This method of approach does not lose any generalization as $x^4 + y^4 = z^4$ has been disproved, and if n is a multiple of 4 it is a special case of $x^4 + y^4 = z^4$. If n is composite it can be made to rest on the solution of its prime factors. Also there is no loss of generality in assuming the symmetric equation $x^p + y^p + z^p = 0$ instead of $x^p + y^p = z^p$ for p an odd prime. A $(-z)$ will do as well as a $(+z)$ since it will be raised to an odd power.

"Writing the equation (p an odd prime)

$$x^p + y^p = z^p$$

in the form

$$(x + y)(x + \zeta y)(x + \zeta^2 y) \ \ldots \ (x + \zeta^{p-1} y) = z^p$$

where ζ is a complex p-th root of unity, the attention of

mathematicians was drawn to the study of expressions of the form

$$a + b\zeta + c\zeta^2 + \ldots\ldots + k\zeta^{p-1},$$

where a, b, c, ... , are integers, and to inquire if the ordinary laws of arithmetic applied to such expressions.

"Many of the most important developments of arithmetic depend upon the definition of a prime number and the so called factor theorem, namely that every number can be resolved into prime factors in one way only. It follows from this fact that if positive integers A, B, C, ... , K, L, of which no two have a common factor, satisfy the condition

$$ABC \ldots K = L^p,$$

then each of the numbers A, B, ... , K must be a perfect p-th power. Should any of the quantities A, B, ... have a common factor, this result must be slightly modified: for example A now will be a perfect p-th power multiplied by a constant depending on the common factors mentioned above. Particular cases of this theorem have already been used. The question immediately suggests itself - Can this theorem be extended to apply to the equation $x^p + y^p = z^p$, and can we deduce that the factors $(x + \zeta y)$, $(x + \zeta^2 y)$, ... , are each p-th powers of the expression of the form

$$a + b\zeta + c\zeta^2 \ldots$$

or perhaps multiples of such p-th powers? If so, a proof of Fermat's Last Theorem would be fairly easy." (4)

"Lamé essayed to prove Fermat's Last Theorem but assumed without proof that integers in the field $\Omega(\alpha)$, where α is a primitive n-th root of unity, n being an odd prime, decomposed

uniquely into prime factors in the field. This error was pointed out by Liouville in commenting on Lamé's first article. Lamé recognized this lacuna but showed that this theorem was true for the case n = 5, and affirmed that it was also true for n general. He proved that the equation

$$A^5 + B^5 + C^5 = 0$$

is impossible for integers A, B, C in the field $\Omega(\alpha)$, $\alpha^5 = 1$, $\alpha \neq 1$." [5]

That the unique factorization law did not hold in all cases led Kummer to the development of the theory of ideals. This revolutionized the study of algebraic numbers." In this connection it may be noted that although many contributions have been made to the first case of the theorem no paper has been published on the second case since Kummer's 1857 memoir which is proved to represent an advance over his results of that paper." [6] Kummer was interested in the solution of $x^n + y^n + z^n = 0$ and would have given up the study of ideal theory if he could have found another means of solving the general problem. The theory of ideals as it is now known is not that of Kummer but of Dedekind who advanced Kummer's work to the more general form. Kummer also worked on the general law of reciprocity.

Besides Kummer, the mathematicians usually connected with this problem are Sophie Germain, Wendt, Wieferich, Mirimanoff, Furtwängler, Pollaczek, Dickson, and Vandiver.

At the present Case I has been proved for p > 41,000,000. Case II, by an intensive study of Bernoulli's numbers and their application to Fermat's Last Theorem by Vandiver, has been

extended to $p < 617$. At the present the study of Irregular Cyclotomic Fields and Bernoulli Numbers may lead to a possible solution of the general case. That Case I has not been proved is one of the most amazing facts in present-day mathematics. Everything indicates that it is true. As for Case II, several specialists in the theory of numbers think that it is quite possible that there exist odd prime integers ℓ and integers x, y, z prime to each other, $z \equiv 0 \pmod{\ell}$ such that

$$x^{\ell} + y^{\ell} + z^{\ell} = 0 .$$

.....

(1) Dickson, L. E., History of the Theory of Numbers, vol. 2, p.731.

(2) Dickson, L. E., History of the Theory of Numbers, vol. 2, p. xix.

(3) National Research Council Bulletin, No. 62, p.28.

(4) Mordell, L. J., Three Lectures on Fermat's Last Theorem, p. 10.

(5) National Research Council Bulletin No. 62, p. 29.

(6) National Research Council Bulletin, No. 62, p.28.

CHAPTER II

METHOD OF INFINITE DESCENT AND ITS APPLICATION WHEN $n = 3, 4, 5$.

Among the methods that have been used in working on Fermat's Last Theorem the simplest one is that of infinite descent. This method is only applicable to the smaller values of n, where n is the exponent of the equation $x^n + y^n = z^n$. This method is characterized by first assuming a smallest solution and then showing that there is a still smaller solution of the same form. This leads to an infinite set of decreasing integers, none zero, which is impossible. The easiest case to prove is for n equal to 4. For this we develop the conditions for primitive solutions of $x^2 + y^2 = z^2$. Then we apply these results to n equal to 4. For the case n equal to 5 the proof is that of Dirichlet. The theorems he develops to give his proof will be found reproduced at the end of the case where n equals 5. Dirichlet's proof of the case n equal to 5 is a special case of a more general fifth degree equation of the form $x^5 \pm y^5 = 2^m 5^n Az^5$ when z is even, and of $x^5 \pm y^5 = 5^n Az^5$ when z is odd.

.....

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

A solution in which x, y, z have no common factor is called a primitive solution. It will be sufficient to find all the primitive solutions, for every non-primitive solution can be deduced from some primitive solution by multiplying all its numbers by the proper factor.

Our first step is to see what form x, y, and z will have in the primitive solutions. We will show that one of x and y will be even the other odd. For (a) if x and y were both even, z would also be even; the common factor, 2, would be present and

the solution would not be primitive. (b) If x and y were both odd (that is, of the form $2n + 1$), x^2 and y^2 would both be of the form $4n + 1$; and hence z^2 would be of the form $4n + 2$. But this is impossible, since the square of every even number is of the form $4n$, and that of every odd number is of the form $4n + 1$. Since suppositions (a) and (b) are both incorrect one of the numbers x and y must be even, the other odd. Let x denote the even one. Then y and z are odd.

Put $x^2 + y^2 = z^2$ in the form $x^2 = z^2 - y^2 = (z + y)(z - y)$. Since z and y are both odd we may put

$$z + y = 2k$$
$$z - y = 2l$$
$$x^2 = 4kl.$$

Since x, y, z are relatively prime, k and l must also be relatively prime; for, from the equations

$$z = k + l \qquad \text{and} \qquad y = k - l;$$

it is clear that if k and l had a common factor y and z would have that factor in common also.

Since $4kl$ is a square, it follows that k and l must be squares. We therefore put:

$$k = m^2$$
$$l = q^2 \qquad (m,q \text{ relatively prime}).$$

Consequently, in any primitive solution of $x^2 + y^2 = z^2$, x, y, z must be of the following form:

$$x = 2mq$$
$$y = m^2 - q^2$$
$$z = m^2 + q^2 \qquad \text{from the above values of } x, y, z.$$

$$x^4 + y^4 = z^4$$

To disprove this consider the equation $x^4 + y^4 = z^2$ in the form $(x^2)^2 + (y^2)^2 = z^2$. In this form $x^2 = 2mq$, $y^2 = m^2 - q^2$, $z = m^2 + q^2$, where m, q are prime to each other and not both odd. From $y^2 = m^2 - q^2$ we see that q must be even since y^2 is odd, and if m^2 is even $m^2 - q^2$ would be of the form $4K+3$ which is impossible. In $y^2 + q^2 = m^2$ q is even, m is odd and prime to q. Also, y, q, and m are relatively prime. Hence

$$\left.\begin{aligned} y &= a^2 - b^2 \\ q &= 2ab \\ m &= a^2 + b^2 \end{aligned}\right\}$$ where a and b are prime to each other and both not odd.

From $x^2 = 2mq$

$$x^2 = 2(a^2 + b^2)(2ab) = 4ab(a^2 + b^2).$$

Since a and b are relatively prime both are relatively prime to $(a^2 + b^2)$ and hence all three must be perfect squares. Put then $a = r^2$, $b = s^2$, $a^2 + b^2 = t^2$

from which $r^4 + s^4 = t^2$.

Now the values of x, y, z in terms of r, s, t are given by

$y = r^4 - s^4$, $x = rst$, $z = m^2 + q^2 = (r^4 + s^4)^2 + 4(r^4 s^4)$

$z = r^8 + 2r^4 s^4 + s^8 + 4r^4 s^4 = r^8 + 6r^4 s^4 + s^8$

so that $z > (r^4 + s^4)^2 > t^4$ or $t < \sqrt[4]{z}$.

Given then one solution of $x^4 + y^4 = z^2$ for which x, y, z are not zero then another solution (r, s, t) can be found such that none are zero and $t < \sqrt[4]{z}$. This process can be continued, so that an infinite number of positive integers $t, t_1, t_2, \ldots$, can be found such that $t_1 < \sqrt[4]{t}$, $t_2 < \sqrt[4]{t_1}$, which is clearly absurd.

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

Our first step in attacking this problem is to determine the form of x, y, z. If x, y, and z are all even then the factor of a power of 2 can be factored out. Two of the unknowns x, y, z must be odd and as any of the unknowns may be negative if we put the equation in the form $x^3 + y^3 + z^3 = 0$ there is no loss of generality in assuming z even and x and y odd. The numbers x, y, z can take the form 3k, $3k \pm 1$. When cubed $(3k \pm 1)^3 = 27k^3 \pm 27k^2 + 9k \pm 1$, and $(3k)^3 = 27k^3$. These numbers will then be congruent to +1, -1, 0 (mod 9). From this we will show that solutions of Case I are impossible. That is, when (x, y, z) = 1, (xyz, p) = 1. This symbol means that 1 is the greatest common divisor of the numbers in the parenthesis. The p in the second parenthesis is the prime exponent of $x^p + y^p = z^p$. The proof of the impossibility of solutions of Case I is easy. Assume that none of the numbers x, y, z is divisible by 3. Then their residues $\pm 1 \pm 1 \equiv 0$ or $\equiv \pm 2$ (mod 9) which is impossible.

Since we are letting x and y be odd numbers then

$$x + y = 2p \qquad x = p + q$$

$$x - y = 2q \qquad y = p - q \quad .$$

If we substitute the values of x and y in the original equation we will find that $2p(p^2 + 3q^2) = z^3$. p and q are prime and cannot both be odd for then x and y would not be prime to each other. p must be even and q odd otherwise z would be divisible by 2 but not by 8. Then $(p^2 + 3q^2)$ is odd. As p and q are prime to each other

$2p$ and $p^2 + 3q^2$

are either relatively prime or have a common factor of 3. In the first case p and z are prime to 3; in the latter case both are divisible by 3.

First case: As $2p$ and $(p^2 + 3q^2)$ are prime to each other, each must be a perfect cube. We can write

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

Values of p, q, r can be found by taking

$$*(\ r = m^2 + 3n^2\ )$$

where m and n are integers and writing

$$p + q\sqrt{-3} = (m + n\sqrt{-3})^3 .$$

$$p^2 + 3q^2 = r^3 = (p + q\sqrt{-3})(p - q\sqrt{-3})$$
$$= (m + n\sqrt{-3})^3 \cdot (m - n\sqrt{-3})^3 .$$

By equating real and imaginary parts of $p + q\sqrt{-3}$, $(m + n\sqrt{-3})^3$

$$p = m^3 - 9mn^2 , \quad q = 3m^2n - 3n^3$$

and if m and n are prime to each other and not both odd, and m is not divisible by 3, then p and q are prime to each other and p is not divisible by 3. This method gives suitable values of p, q, r, satisfying $(p^2 + 3q^2) = r^3$.

Since $2p$ is a cube, m and n must be such that $2m(m + 3n)(m - 3n)$ is a perfect cube.

Since $q = 3n(m + n)(m - n)$, n is odd and m is even. Since m is prime to 3, no two of $2m$, $m + 3n$, $m - 3n$ can have a common factor; each must be a perfect cube

$$m + 3n = a^3 , \quad m - 3n = b^3 , \quad 2m = c^3$$

and adding the above we get

$$a^3 + b^3 = c^3 .$$

This equation has the same form as $x^3 + y^3 = z^3$ with the same conditions as x, y, z. We will show that the values of a, b, c are less than x, y, z. Also we will have here another application of case I where we can continue this process and find integers less than a, b, c which will satisfy the same equation.

Continuing the above we find

$$z^3 = 2p(p^2 + 3q^2) = a^3 \cdot b^3 \cdot c^3 \cdot (m^2 + 3n^2)^3 ,$$

or $$z = abc(m^2 + 3n^2) = 1/3abc(a^6 + a^3b^3 + b^6)$$

and as a and b cannot both be unity, z is numerically greater than c. Then as for n = 4 we get a set of numerically decreasing integers, none zero, which is impossible.

Second case: As 2p and $(p^2 + 3q^2)$ have a factor of 3

$$p = 3p_1 = 3^2 p_2 .$$

Since $2p(p^2 + 3q^2) = z^3$ it can be put in the form

$$2 \cdot 3^2 p_2 (3^2 p_1^2 + 3q^2) = z^3$$

or, by taking out 3^3

$$2p_2(q^2 + 3p_1^2) = z_1^3 .$$

From here the proof is that of the first case.

.....

* Every odd divisor of $x^2 + 3y^2$ (x and y relatively prime) is of that form. (Dickson, L. E., Introduction to the Theory of Numbers, page 96, problem 4).

$$x^5 + y^5 = z^5$$

x, y and z can have one of the following forms: 5k, (5k ± 1), (5k ± 2). Raising these forms to the fifth power x, y, z would be congruent to 0, ± 1, or ± 7, modulus 5^2. Hence we get the following possibilities:

$$\pm 1 \pm 1 = 0, \pm 2$$
$$\pm 1 \pm 7 = \pm 6, \pm 8$$
$$\pm 7 \pm 7 = \pm 14, \quad 0 .$$

Since these possibilities must conform to one of the residues when added, the only possibilities are:

$$+1 - 1 = 0 \qquad +7 - 7 = 0$$
$$-1 + 1 = 0 \qquad -7 + 7 = 0 .$$

From this we find that one of the numbers x, y, z must be of the form 5k, i. e., divisible by 5. Therefore Case I of the theorem, x,y, z, p being relatively prime in pairs, is impossible. There will be no loss of generality in assuming z divisible by 5. This will lead to two cases, first, when z is even; second, when z is odd.

Case I. x odd, y odd, z even and divisible by 5.

Case II. x odd, y even, z odd and divisible by 5.

Case I. $x + y = 2p, \qquad x = p + q$

$x - y = 2p, \qquad y = p - q$

where p and q are relatively prime integers, one even, the other odd. This can be seen from the above values of x and y, for if p and q were both odd x and y would both be even.

Substituting for x and y we get

$$(p + q)^5 + (p - q)^5 = z^5$$

which gives after multiplying out and collecting terms

$$2p(p^4 + 10p^2q^2 + 5q^4) = z^5 .$$

Although we know that p and q are relatively prime one even, the other odd, we can show that p is even and q is odd. Let us first suppose p odd and q even and see what results. Then we will suppose p even and q odd. By this method we will be able to determine the nature of p and q. If p is odd and q is even we would have $(p^4 + 10p^2q^2 + 5q^4)$ odd and 2p two times an odd number. But since z is even z^5 would be divisible by at least 2^5, our hypothesis above is incorrect and p must be even and q odd.

Our next problem is to determine whether p is divisible by 5. We will now show that it is. If p is not divisible by 5 then $(p^4 + 10p^2q^2 + 5q^4)$ is not divisible by 5. But since z is divisible by 5, z^5 must be divisible by 5^5 and this can only hold if we have p divisible by 5. Hence p has the form such that

$$2p = 2^5 \cdot 2^{5k_1} \cdot 5^4 \cdot 5^{5k_2} \cdot \alpha^5$$

where k_1 and k_2 may both be zero. We can also write

$$p^4 + 10p^2q^2 + 5q^4 = 5\beta^5 .$$

Hence

$$z^5 = 2^5 \cdot 2^{5k_1} \cdot 5^5 \cdot 5^{5k_2} \cdot \alpha^5 \cdot \beta^5 \quad \text{or} \quad x^5 + y^5 = 2^{5(k_1+1)}\, 5^{5(k_2+1)}\, z_1^5 .$$

In $p^4 + 10p^2q^2 + 5q^4 = 5\beta^5$ let $p = 5p_1$.

From this we get

$$5^4 \cdot p_1^4 + 2 \cdot 5^3 \cdot p_1^2 q^2 + 5q^4 = 5\beta^5$$

or

$$5^3 \cdot p_1^4 + 2 \cdot 5^2 \cdot p_1^2 q^2 + q^4 = \beta^5$$

which can be written as

$$(q^2 + 5^2 p_1^2)^2 - 5^4 p_1^4 + 5^3 p_1^4 = \beta^5$$

or $$(q^2 + 5^2 p_1^2)^2 - 5^3 4 \cdot p_1^4 = \beta^5 .$$

If we set $$P = q^2 + 5^2 p_1^2$$

and $$Q = 2 \cdot 5 \cdot p_1$$

then we will get $$P^2 - 5Q^2 = \beta^5$$

where P and Q are relatively prime.

From Theorem I of Dirichlet's proof we can set

$$P = q^2 + 5^2 p_1^2 = t(t^4 + 2 \cdot 5^2 t^2 s^2 + 5^3 s^4)$$

and $$Q = 10 p_1^2 = 5s(t^4 + 10 t^2 s^2 + 5s^4)$$

where s and t are relatively prime, the first even the second odd and not divisible by 5. Since p_1 is divisible by 5 then s must be divisible by 5.

If in $2 \cdot 5^2 p_1 = 2^{5(k_1+1)} \, 5^{5(k_2+1)} \, \alpha^5$ we square both sides we will have

$$2^2 5^4 p_1^2 = \lambda^5 = 2 \cdot 5^4 s(t^4 + 10 t^2 s^2 + 5s^4)$$

in which $2 \cdot 5^4 s$ and $(t^4 + 10 t^2 s^2 + 5s^4)$ are relatively prime since t is not divisible by 5. Hence

$$t^4 + 10 t^2 s^2 + 5s^4 = \lambda_1^5$$

which can be written as

$$(t^2 + 5s^2)^2 - 5(2s^2)^2 = \lambda_1^5 .$$

From Theorem I of Dirichlet's proof, $(t^2 + 5s^2)$ can be written as

$$t^2 + 5s^2 = t'(t'^4 + 10 t'^2 s'^2 + 5 s'^4)$$

$$2s^2 = 5s'(t'^4 + 10 t'^2 s'^2 + 5 s'^4)$$

or $2s^2 > 5s' \cdot 5s'^4$ or $s' < \sqrt{2s^2/25}$ hence $s' < s$.

Here if t' and s' are relatively prime we can set

$$(t'^4 + 10 t'^2 s'^2 + 5 s'^4) = \lambda_2^5$$

which can be written in the same form as above with numbers

t'' and s'' . This can be shown in the following manner:

Let $t^4 + 10t^2s^2 + 5s^4 = \lambda_1^5$

$t'^4 + 10t'^2s'^2 + 5s'^4 = \lambda_2^5$ etc.

Then $(t'\lambda_2^5)^2 - 5(5s'\lambda_2^5)^2 = \lambda_1^5$

$(\lambda_2^5)^2 \cdot (t'^2 - 5^3 \cdot s'^2) = \lambda_1^5$

$t'^2 - 5(5s')^2 = \lambda_3^5$.

From this we get a series of decreasing integers $t, t', t'', \ldots$, and $s, s', s'', \ldots$, such that the preceding one is greater than the succeeding one and as zero is not included in this series it is impossible.

.....

Case II. x odd, y even, z odd and divisible by 5.

Let us consider the equation

$$x^5 + y^5 = 5^{5n} z^5 \tag{1}$$

and place $x + y = p$, $2x = p + q$

$x - y = q$, $2y = p - q$

where p and q are relatively prime, both odd. Substituting for x and y in (1) we get

$$\left(\frac{p+q}{2}\right)^5 + \left(\frac{p-q}{2}\right)^5 = 5^{5n} z^5$$

which gives

$$p(p^4 + 10p^2q^2 + 5q^4) = 2^4 \cdot 5^{5n} \cdot z^5 .$$

We can show that p is divisible by 5, hence $p = 5r$, or

$$5^2 \cdot r(q^4 + 2 \cdot 5^2 \cdot q^2 r^2 + 5^3 \cdot r^4) = 2^4 \cdot 5^{5n} \cdot z^5$$

which gives

$$r(q^4 + 2 \cdot 5^2 \cdot q^2 r^2 + 5^3 \cdot r^4) = 2^4 \cdot 5^{5n-2} \cdot z^5 .$$

Since p and q are relatively prime we can readily see that r is

divisible by 5. This makes

r and $(q^4 + 2\cdot 5^2 q^2 r^2 + 5^3 r^4)$ relatively prime.

Hence $(q^4 + 2\cdot 5^2 q^2 r^2 + 5^3 r^4)$ is equal to 2^4 times a fifth power, and as a consequence of Theorem VII, can be set into

$$\left(\frac{q^2 + 5^2 r^2}{2}\right)^2 - 5(5r^2)^2$$

where $\frac{q^2 + 5^2 r^2}{2}$ and $5r^2$ are relatively prime, both odd, and the latter is divisible by 5. Hence

$$\frac{q^2 + 5\cdot r^2}{2} = \frac{t(t^4 + 2\cdot 5^2 t^2 s^2 + 5^3 s^4)}{2^4}$$

$$5r^2 = \frac{5s(t^4 + 10t^2 s^2 + 5s^4)}{2^4}$$

where t and s are relatively prime, both odd, and t is not divisible by 5. Since r is divisible by 5, s must also be. Above we find that $5^2 r = 5^{5n}$. Hence $5^4 r^2 = 5^{10n} z_i^{10}$ or

$$5^4 r^2 = \frac{5^4 s(t^4 + 10t^2 s^2 + 5s^4)}{2^4} = 5^{10n} z_i^{10}$$

which can be put in the form

$$5r^2 = \frac{5s(t^4 + 10t^2 s^2 + 5s^4)}{2^4} = 5^{10n-3} z_i^{10}$$

which gives

$$s(t^4 + 10t^2 s^2 + 5s^4) = 2\cdot 5^{4\,10n-4} \cdot z_i^{10} .$$

Since t and s are relatively prime, both odd, and t not divisible by 5, we can set

$$(t^4 + 10t^2 s^2 + 5s^4) = 2^4 z_j^5$$

where z_j is not divisible by 5. The above equation can be placed in the following form

$$\left(\frac{t^2 + 5\cdot s^2 s^2}{2}\right)^2 - 5(s^2)^2$$

where $\frac{t^2 + 5^2 s^2}{2}$ and $5s^2$ are relatively prime, both odd, and the latter divisible by 5. Hence

$$\frac{t^2 + 5^2 s^2}{2} = \frac{t'(t'^4 + 2\cdot 5^2 t'^2 s'^2 + 5^3 s'^4)}{2^4}$$

$$s^2 = \frac{5s'(t'^4 + 10t'^2 s'^2 + 5s'^4)}{2^4}$$

where t' and s' are relatively prime, both odd, and t' not divisible by 5. As s is divisible by 5 and t' is not then s' must be divisible by 5.

We see that $s^2 > 25/16\ s'^5$ and that s is much larger than s'. From the fact that we get a series of trinomial factors of the same form in which $t > t' > t''$ etc., and $s > s' > s''$ etc., and that zero is excluded from this set we can say that the theorem for $n = 5$ is impossible.

Theorem I.

Given l, an odd prime, which is not a factor of a, and suppose that we have the equation

(1) $$\delta^2 - a\varepsilon^2 = l$$

which satisfies

(2) $$d^2 - ae^2 = l^n$$

the numbers d and e being given by the expression

(3) $$(\delta + \varepsilon\sqrt{a})^n = d + e\sqrt{a} = l(d' + e'\sqrt{a})$$

and

(3a) $$(\delta - \varepsilon\sqrt{a})^n = d - e\sqrt{a}$$

then if we equate the rational parts and the coefficient of $\sqrt{a}$, then the numbers d and e thus obtained are relatively prime.

Theorem II.

Let l be an odd prime and not a divisor of a, and suppose that

(4) $$d^2 - ae^2 = l^n,$$

(5) $$d'^2 - ae'^2 = l^n,$$

the numbers d and e, d′ and e′ being relatively prime, then there exists two numbers t and u which satisfy the equation

(6) $$t^2 - au^2 = 1$$

which can be put in the following form

(7) $$(d' \pm e'\sqrt{a})(t \pm u\sqrt{a}) = d + e\sqrt{a}$$

the signs being conveniently chosen and the rational parts and the coefficients of $\sqrt{a}$ equated separately.

Theorem III.

Given l, an odd prime, not dividing a, and k an odd number relatively prime to a, which satisfy the following equations

$$D^2 - aE^2 = \ell^n k,$$
$$d^2 - ae^2 = \ell^n,$$

Where D and E, d and e are relatively prime, then there exists two numbers D' and E', relatively prime, which will satisfy the equation

$$D'^2 - 5E'^2 = k$$

and also

$$(D' \pm E'\sqrt{a})(d \pm e\sqrt{a}) = D + E\sqrt{a}$$

the signs being suitably chosen and the rational parts and the coefficients of $\sqrt{a}$ equated separately.

Theorem IV.

If P and Q afe relatively prime numbers, the one even, the other odd, and if the last one is divisible by 5, then in order to set $P^2 - 5Q^2$ equal to a fifth power in the most general manner, it will be sufficient to set

$$P + Q\sqrt{5} = (\varphi + \psi\sqrt{5})^5$$

where the indeterminants φ and ψ are relatively prime, the one even, the other odd, and the first moreover not divisible by 5.

Theorem V.

If the numbers m and n are positive, n being different from 2, and the number A not divisible by 2 or 5, nor by any prime of the form $10k + 1$, then it will be impossible to find two relatively prime numbers x and y, such that $x^5 \pm y^5 = 2^m 5^n Az^5$.

Theorem VI.

If the numbers m and A are subjected to the same restrictions given in Theorem V, and if the number $2^m A$, when divided by 25, gives one of the following eight residues, 3, 4, 9, 12, 13, 16, 21, 22, it will be impossible to find two relatively prime numbers x and y, such that $x^5 \pm y^5 = 2^m A z^5$.

Theorem VII.

If the numbers P and Q are relatively prime, both odd, the last divisible by 5, then in order to equate the binomial $P^2 - 5Q^2$ to the quadruple of a fifth power in the most general form, it will be sufficient to set:

$$P + Q\sqrt{5} = \frac{(\varphi + \psi\sqrt{5})}{2^4}$$

where the indeterminant numbers φ and ψ are relatively prime, both odd, and the first moreover, not divisible by 5.

Theorem VIII.

If n designates a postive number other than 0 and 2, and if the number A is neither divisible by 2 nor 5, neither by any prime of the form $10k + 1$, then it will be impossible of finding two numbers x and y which are relatively prime, such that

$$x^5 \pm y^5 = 5^m A z^5 .$$

Theorem IX.

If A is subjected to the same restrictions given in Theorem VIII, and is divided by 25 and gives the following eight residues, 3,4,

9, 12, 13, 16, 21, 22, then it will be impossible to find two relatively prime numbers x and y such that $x^5 \pm y^5 = Az^5$.

CHAPTER III

AN INTRODUCTION TO THE NATURE OF IDEALS

In Chapter I we stated that Kummer invented the ideal theory and that Dedekind advanced this theory to a more general form. In this chapter it is intended to give an introduction to the nature of ideals. It will be shown why ideals must be introduced in order to extend unique factorization to all number fields of finite order. For the study of ideals as applied to the field $K(\sqrt{-5})$ and the quadratic fields refer to Reid[1], for the general theory refer to Hancock[2], and for the need of ideals and its theory as applied to Fermat's Last Theorem refer to Dickson[3], and to Bachmann[4]. The above books develop all the necessary theory of ideals which the reader will need. This chapter will attempt to help the beginner understand the makeup of an ideal and the notation used.

We will begin our discussion by stating that in the rational integral number system any number can be represented as a product of primes in one and only one way. This is called unique factorization. The theorem which substantiates this property is called the Unique Factorization Theorem. Our next step then is to see whether or not this property is true of complex numbers of the form $a + bi$. Following this the next step is to determine whether or not this property is applicable to algebraic numbers in general. Before we give this we must define an algebraic number and a number field.

An algebraic number is a number that satisfies an algebraic equation with rational coefficients. An algebraic

integer is a number which satisfies an algebraic equation with integral coefficients, the coefficients of the highest power of x being unity.

A number-field can be defined as follows: "A set of complex numbers is called a field, or, more specifically, a number-field, if the set contains at least two distinct numbers, and the sum, difference, product, and quotient of any two numbers of the set is in the set, division by 0 being always excluded. The numbers of the field are called its elements.

Example 1. The rational numbers form a field: for the sum, difference, product, and quotient of any two rational numbers is a rational number.

Example 2. The real numbers form a field.

Example 3. The complex numbers form a field.

Example 4. The numbers of the form $a + b\sqrt{2}$, where a and b range independently over the field of rational numbers, form a field."(5)

The totality of all algebraic numbers form a field. Every subfield of this field is therefore called an algebraic field. We will now introduce a definition of linear dependence and linear independence of algebraic numbers. The algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ are said to be linearly independent if a linear combination of them with rational coefficients vanishes only if all coefficients are zero. They are linearly dependent if there exists a linear combination of them with rational coefficients which vanishes

without all the coefficients being zero. An algebraic field is called a finite algebraic field if there exists a positive rational integer k so that more than k numbers of the field are linearly dependent. The smallest value of k is called the degree of the number field. The field generated by the roots of an algebraic equation of the form $x^2 + a = 0$ where a is a positive or negative integer, not a perfect square, is called a quadratic field. For this field the value of k is 2. The simplest case of a quadratic field is when $a = 1$.

When $a = 1$ we have the field $K(\sqrt{-1})$. The integers in this field are of the form $u + ti$. For other values of a, say 3 or 5, we would write a number in these fields as $x + y\sqrt{-3}$, or $x + y\sqrt{-5}$. We would like now to define a prime in these fields. Before we do this we must define a unit, a norm, and an associate. The norm of $a + bi$ is found by multiplying it by its conjugate $a - bi$. The units in the quadratic fields where the number in the radical defining the field is negative are those integers in that field whose norms are 1. Two integers in a field are associated when they differ by only a unit factor.

We are now ready to define a prime number of K(i). An integer of K(i) that is not a unit and that has no divisors other than its associates and the units, is called a prime number of K(i). The definition of a prime in each of the other fields is similar to that of K(i). We also find that in the fields K(i), $K(\sqrt{2})$, $K(\sqrt{-3})$, a number may be represented as a product of primes in one and only one way.

This means that the Unique Factorization Theorem is valid in these fields. But this is not true in $K(\sqrt{-5})$. This is the simplest case where the Unique Factorization Theorem does not hold. We find here that

$$\begin{aligned} 6 &= 2\cdot 3 &&= (1+\sqrt{-5})(1-\sqrt{-5}) \\ 21 &= 3\cdot 7 &&= (1+2\sqrt{-5})(1-2\sqrt{-5}) \\ & &&= (4+\sqrt{-5})(4-\sqrt{-5}) \\ 9 &= 3^2 &&= (2+\sqrt{-5})(2-\sqrt{-5}) \\ 49 &= 7^2 &&= (2+3\sqrt{-5})(2-3\sqrt{-5}) \end{aligned}$$

the factors in the above products can easily be proved primes of $K(\sqrt{-5})$. This means that the above numbers can be factored into primes in more than one way. By this breakdown of unique factorization we are faced with a new problem. This problem is to determine whether or not we can by any new ideas or concepts reintroduce unique factorization.

In our attack on this problem we want to define a set. A set is a totality of things of any kind which are considered as a unit. The things of the set are the elements of the set. The set may be finite or infinite according as the number of the elements of the set is finite or infinite. In the latter case the definition of the set cannot be given unless we give a law by which we can decide whether or not any given thing is an element of the set. The following are examples of sets.

Example 1. A set consisting of integers from 1 to 100.

Example 2. The even numbers.

Example 3. The odd numbers.

Example 4. Numbers of the form $4n + 1$ where $n = 1, 2, 3, \ldots$ The first set is finite, the other three are infinite. We are going to use the notion of a set to define ideals.

If in Example 4 we let the numbers $4n + 1$ form a set, we find that the product of any two numbers in the set is a number in the set. That is, $(4p + 1)(4q + 1) = (4m + 1)$ where p, q, m, are integers. We may also want to find the primes in this set. They can be defined as those numbers which can only be expressed as the product of themselves and unity. In this set, 1, $\underline{5}$, $\underline{9}$, $\underline{13}$, $\underline{17}$, $\underline{21}$, 25, $\underline{29}$, $\underline{33}$, $\underline{37}$, $\underline{41}$, 45, $\underline{49}$, $\underline{53}$, $\underline{57}$, $\underline{61}$, 65, ... , we find that all the numbers which are prime in the rational number field are prime in this set, and in addition, some numbers which are composite in the field of rational numbers are prime here. The underlined are the primes. If we take the number 10857 of this set we find that it can be factored in primes in two different ways in this set. That is,

$$10857 = 141 \cdot 77 = 21 \cdot 517.$$

We also find another example of this type, as follows

$$693 = 9 \cdot 77 = 21 \cdot 33.$$

We find above that we do not have unique factorization, but if we extend our set to include all positive integers we would find that this difficulty would be overcome. This principle is employed in the study of ideals. That is, we extend the field of factorization. The numbers above would be factored in the (ideal) field as follows:

$$10857 = 3 \cdot 7 \cdot 11 \cdot 47$$

$$693 = 3 \cdot 3 \cdot 7 \cdot 11.$$

An ideal is defined as follows: An ideal of a number field (e. g. $K(\sqrt{-5})$ is a set of integers $\alpha_1, \alpha_2, \ldots, \alpha_m$ of the field infinite in number and such that every linear combination $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots$ of them, where $\lambda_1, \lambda_2, \lambda_3, \ldots,$ are any integers of the field, is an integer of the set. It would be sufficient to say that a finite number of numbers could represent an ideal, as the linear combination of these finite number will give the infinite set. The integers of the infinite set which sonstitute the ideal are called the numbers of the ideal. The ideals of the rational integral number field are the primes. Every number in this field can be represented as a linear combination of the primes. The ideals in any number field where the Unique Factorization Theorem holds are the primes in that field.

We shall now state some properties of ideals without proofs.

I. Equality of Ideals. Two ideals $\mathcal{U} = (\alpha_1, \alpha_2, \cdots, \alpha_m)$ and $\mathfrak{b} = (\beta_1, \beta_2, \cdots, \beta_m)$ are equal when the two infinite systems of integers that constitutes these ideals are the same.

II. Multiplication of Ideals. By the product of two ideals $\mathcal{U} = (\alpha_1, \alpha_2, \cdots, \alpha_m)$ and $\mathfrak{b} = (\beta_1, \beta_2, \cdots, \beta_m)$, we understand the ideal defined by all possible products of a number defining $\mathcal{U}$ by a number defining $\mathfrak{b}$; that is,

$$\mathcal{U}\mathfrak{b} = (\alpha_1\beta_1, \alpha_1\beta_2, \cdots, \alpha_1\beta_m, \cdots, \alpha_m\beta_1, \cdots, \alpha_m\beta_m).$$

III. Divisibility of Ideals. An ideal, $\mathcal{U}$, is said to be divisible by an ideal, $\mathfrak{b}$, when there exists an ideal, $\mathcal{N}$,

such that

$$\mathfrak{a} = \mathfrak{b}\mathfrak{N};$$

$\mathfrak{b}$ and $\mathfrak{N}$ are then said to be divisors or factors of $\mathfrak{a}$.

It can now be pointed out that by means of ideals unique factorization can be restored to all algebraic number fields. The work of Kummer in trying to solve Fermat's Last Theorem led to the development of Ideals and opened a whole field of mathematics. Most of the work done recently on this theorem contains the theory of ideals or an extension of that theory.

.....

(1) Reid, L. W. . The Elements of the Theory of Algebraic Numbers. Chapter VIII, Chapter XI.

(2) Hancock, Harris. Foundations of the Theory of Algebraic Numbers.

(3) Dickson, L. E.. On Fermat's Last Theorem., Annals of Mathematics, 18, page 161.

(4) Bachmann, P.. Das Fermatproblem.

(5) Weisner, L.. Introduction to the Theory of Equations. page 20.

CHAPTER IV

RESUMÉS OF ARTICLES PUBLISHED ON FERMAT'S LAST THEOREM FROM 1919 TO 1938

The following is a chronological list of articles published from 1919 to 1938 concerning Fermat's Last Theorem. (For articles prior to 1919 refer to Dickson: History of the Theory of Numbers, II, Chapter 26.)

Vandiver, H. S. (English)

A Property of Cyclotomic Integers and its Relation to Fermat's Last Theorem.

Ann. of Math., II, 21, 1919-20, p. 73.

The author takes the criterion of Furtwängler

$$\frac{r^{p-1}}{p} = q(r) \equiv 0 \pmod{p},$$

the criterion of Kummer

$$B_n \left[\frac{d^{p-2n} \log(x + e^v y)}{dv^{p-2n}} \right]_{v=0} \equiv 0 \pmod{p},$$

and the criterion of Mirimanoff

$$B_n f_{p-2n}\left(-\frac{x}{y}\right) \equiv 0 \pmod{p} \quad \left(n = 1, 2, 3, \ldots, \frac{p-3}{2}\right),$$

and derives these results by methods a bit different from those employed by the above mentioned. He shows that the criteria of Kummer and Furtwängler may be derived from one relation. He also derives some other criteria in reference to $x^p + y^p + z^p = 0$.

.....

Vandiver, H. S. (English)

On Kummer's Memoir of 1857 Concerning Fermat's Last Theorem

Proc. Nat. Acad. Sci., 6, 1920, p. 266. (First Paper)

In an article in the Mathematische Abhandlungen of the Berlin Academy for the year 1857, pages 41-74, Kummer essayed to prove that the relation

(1) $$x^p + y^p + z^p = 0$$

could not be satisfied in integers, when p is an odd prime not satisfying three given conditions. Based on this result, the conclusion that (1) is impossible for all p's less than 100 was derived by him. In the present paper it is pointed out that Kummer made several errors in his argument, which vitiate his results.

.....

Vandiver, H. S. (English)

On the Class Number of the Field $\Omega\left(e^{\frac{2\pi i}{p^m}}\right)$ and the Second Case of Fermat's Last Theorem.

Proc. Nat. Acad. Sci., 6, 1920, p. 416.

In the present paper an analogous expression for the residue of the first factor of the class number of $\Omega\left(e^{\frac{2\pi i}{p^m}}\right)$ modulo p, was obtained and the result used to show that certain results due to Bernstein on Fermat's Last Theorem do not have the generality stated by him. The author shows that the criterion given by Bernstein in the Göttigen Nachrichten, in 1910 (507-16) constitutes no extension over the one given by Kummer.

.....

Vandiver, H. S. (English)

Bachmann on Fermat's Last Theorem.

Bull. Am. Math. Soc. , 27, May 1921, p. 373.

This paper analyzes Bachmann's book DAS FERMATPROBLEM. He states that this book will constitute a valuable aid to anyone attempting a serious study of Fermat's Last Theorem. He points out, however, that a numbef of references to articles bearing directly on some of the work given in the text have been omitted. He notes some results given which are not found elsewhere except in the original articles. He also notes some omissions in proof by both Kummer and Bachmann, and that the works of Frobenius are not treated in the correct perspective.

.....

Nagel, T. (Norwegian)

Fermats Problem. En Oversigt.

Norsk matem. Tidsskrift, 3, 1921, p. 7-21.

A summary of the most important results of the theory of Fermat's Last Theorem.

.....

Fueter, R. (French)

Le critère de Kummer relatif au dernier théorème de Fermat.

Ens. Math., 22, 1922, p. 62.

A resumé of the transformation necessary to put Fermat's equation in terms of cyclotomic numbers.

.....

Fueter, R. (German)

Kummer's Kriterium zum letzten Theorem von Fermat.

Math. Ann., 85, 1922, p. 11-20.

The author, using methods and symbolism due to Hilbert, develops a relation by means of which he proves the theorems

of Furtwängler. He also obtains a transformation of an equation of Vandiver which he uses to deduce the Kummer criteria

$$\begin{cases} B_{\frac{(p-i)}{2}} \quad f_i(t) \equiv 0 \pmod{p} \\ f_{p-1}(t) \equiv 0 \pmod{p} \end{cases}$$

$i = 3, 5, \ldots, p-2$; $-t = x/y, y/x, x/z, z/x, y/z, z/y$.

.....

Vandiver, H. S. (English)

Note on Some Results Concerning Fermat's Last Theorem.

Bull. Am. Math. Soc., 28, 1922, p. 258.

This article is confined to statements of new results obtained by the writer for both cases of the problem. The proofs are not given. Among other indicated results, Vandiver, by the use of new developments in the theory of cyclotomic fields derives the following for Case I:

$$B_S \equiv 0 \pmod{p^2}$$

$$S = \frac{hp+1}{2}, \quad h = p-4, p-6, p-8, p-10.$$

.....

Vandiver, H. S. (English)

On Kummer's Memoir of 1857 Concerning Fermat's Last Theorem.

Bull. Am. Math. Soc., 28, 1922, p. 400-407. (Second Paper)

"1. Introduction. In a previous paper under the same title (Proc. Nat. Acad. 1920), the writer considered an article by Kummer, (Math. Abhand. Berlin Acad. 1857), and pointed out that the argument there used for proving certain results regarding

the equation $x^\lambda + y^\lambda + z^\lambda = 0$, where x, y, z are integers and λ is an odd prime, is deficient and incorrect in several respects. Kummer attempts to prove four theorems which in my first paper were numbered I to IV. I pointed out that the proofs of Theorems I and IV are incomplete, and that the proofs of II and III are inaccurate. In the present paper additions to and modifications of Kummer's arguments will be given, by means of which the demonstrations Theorems I and IV will be completed."

.....

Pomey, Léon. (French)

Sur le dernier théorème de Fermat.

c. r. Acad. Sci. Paris, 177, 1923, p. 1187-1190.

An abstract of an article in Journ. de Math., 1925, p. 1-22.

.....

Vandiver, H. S. (English)

A New Type of Criteria for the First Case of Fermat's Last Theorem.

Ann. of Math., II, 26, 1924-1925, p. 88.

By transforming the criteria of Kummer, the author shows that if $x^p + y^p + z^p \equiv 0$ is satisfied in integers x, y, and z, not zero, and prime to the odd prime p, then

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{u^2} \equiv 0 \pmod{p}$$

where u is the greatest integer in p/3.

.....

Vandiver, H. S. (English)

A Property of Cyclotomic Integers and its Relation to Fermat's Last Theorem.

Ann. of Math., II, 26, 1924-25, p. 217. (Second Paper)

In this paper extensions of the Kummer criteria are obtained by the use of $\prod_{\gamma=1}^{k-1} \prod_{r=1}^{[\frac{\gamma p}{k}]} \left(x + \alpha^{[1:r]} y\right)^2 = \alpha^{\frac{-2kyg(k)}{x+y}} \omega^{2p}$ and the conditions $B_s \equiv 0 \pmod{p^2}$, $s = \left(\frac{lp+1}{2}\right)$, $l = p-4, p-6, p-8, p-10$, derived therefrom. For the modulus p, these congruences reduce to the relations of Mirimanoff. (i. e., If $x^p + y^p + z^p = 0$ is satisfied in integers $xyz \not\equiv 0 \pmod{p}$, then $B_{\mu-1} = B_{\mu-2} = B_{\mu-3} = B_{\mu-4} \equiv 0 \pmod{p}$, $\mu = \left(\frac{p-1}{2}\right)$.

.....

Vandiver, H. S. (English)

Note on Trinomial Congruences and the First Case of Fermat's Last Theorem.

Ann. of Math., II, 27, 1925-26, p. 54.

This note contains the proofs of some theorems concerning the relation

(1) $$x^p + y^p + z^p = 0$$

x, y, and z being integers prime to the odd prime p, that depends on the possibility of finding prime integers q such that

(2) $$\xi^p + \eta^p + \zeta^p \equiv 0 \pmod{q}$$

has no solutions in integers ξ, η, ζ prime to q. In particular the following result is obtained: If (2) has no solutions under the conditions above mentioned, $q = 1 + mp$, and $m < 10p$, then (1) has no solutions in integers prime to p.

.....

Vandiver, H. S. (English)

Transformations of the Kummer Criteria in Connection with Fermat's Last Theorem.

Ann. of Math., II, 27, 1925-26, p. 171. (First Paper)

In this paper transformations of $B_m f_{p-m}(t) \equiv 0$, $f_{p-1}(t) \equiv 0 \pmod{p}$ are obtained which are useful in deriving criteria for the solution of $u^p + v^p + w^p = 0$, where u, v, and w are rational integers prime to p of the type $m^{p-1} \equiv 1 \pmod{p^2}$.

.....

Pomey, Léon (French)

Sur le dernier théorème de Fermat.

Journal de Mathematiques, 90, II, 4, 1925, p. 1-22.

Using elementary methods he proved Fermat's Last Theorem in Case I for eleven prime exponents between 9048 and 10000, as well as for twenty-four other exponents between 5,000,000 and 5,003,250.

.....

Ore, O. (Norwegian)

Fermats Theorem.

Norsk Mat. Tidsskrift, 7, 1925, p. 1-10.

A summary of the progress made in the theory of Fermat's

Last Theorem up to the year 1924.

.....

Vandiver, H. S. (English)

Laws of Reciprocity and the First Case of Fermat's Last Theorem. Proc. Nat. Acad. Sci., 11, 1925, p. 292.

This paper contains the proof of the following theorem: Suppose $x^p + y^p + z^p = 0$ is satisfied in integers, none zero, and all prime to the odd prime p, also, let the primcipal ideal $(\omega(\alpha))$ be the p-th power of any ideal in the field defined by $\alpha = e^{\frac{2\pi i}{p}}$ which is prime to (z) and (p); then

$$f_{p-n}(t)\left[\frac{d^n \log \omega(e^{-v})}{dv^n}\right]_{v=0} \equiv 0 \pmod{p};$$

$$f_k(t) = \sum_{s=1}^{p-1} s^{k-1} t^s \; ; \quad t \equiv -x/y \pmod{p};$$

$n = 1, 2, \ldots, p-2$, and e is the Naperian base. A number of corollaries are obtained to this theorem, including the criteria

$$f_{p-n}(t)\, f_n(1-t) \equiv 0 \pmod{p},$$

$n = 1, 2, \ldots, p-1$.

.....

Vandiver, H. S. (English)

Summary of Results and Proofs Concerning Fermat's Last Theorem. Proc. Nat. Acad. Sci., 12, 1926, p. 106. (First Paper)

This paper contains several results regarding Fermat's Last Theorem obtained by the author within the last ten years and not hitherto published. The Proofs are indicated.

.....

Vandiver, H. S. (English)

Application of the Theory of Relative Cyclic Fields to Both Cases of Fermat's Last Theorem.

Trans. Am. Math. Soc., 28, 1926, p. 554.

In this paper the author attacks the Last Theorem by a new method based on the theory of power characters in the field $\Omega(\theta)$, where θ is a primitive (p^k)-th root of unity, k prime to the odd prime p. The following result among others is obtained: If $x^p + y^p + z^p = 0$ is satisfied in integers none zero and all prime to the odd prime p, v is any number in the set t, $1 - t$, $1/t$, $1/(1 - t)$, $t/(t - 1)$, $(t - 1)/1$, and $-x/y = t$, then if $\alpha = e^{\frac{2\pi i}{p}}$, $\beta = e^{\frac{2\pi i}{n-1}}$,

$$q(n) \prod_{a=1}^{n-2} ((1 - v)\mathrm{ind}(\alpha\beta^a - 1) - q(n)) \equiv 0 \pmod{p},$$

where $\mathfrak{f} = (\beta - r, rv)$, r is a primitive root of n,

$$(\alpha\beta^a - 1)\frac{(N(\mathfrak{q}) - 1)}{p} \equiv \alpha^i \pmod{\mathfrak{f}},$$

$$i = \mathrm{ind}(\alpha\beta^a - 1), \qquad q(n) = \frac{(n^{p-1} - 1)}{p},$$

n is any prime $\not\equiv 0$ or $1 \pmod{p}$, and $N(\mathfrak{f})$ is the norm of $\mathfrak{f}$.

.....

Vandiver, H. S. (English)

Summary of Results and Proofs Concerning Fermat's Last Theorem.

Proc. Nat. Acad. Sci., 12, 1926, p. 767. (Second Paper)

In this note, among other results, the author indicates the proofs of the following theorems: If p is an odd prime, and $u^p + v^p + w^p = 0$ is satisfied in non-zero integers in the

field $\Omega(\alpha + \alpha^{-1})$, $\alpha = e^{\frac{2\pi i}{p}}$, then the class number of the field $\Omega(\alpha)$ is divisible by p^2. Under the assumptions (1) none of the Bernoulli Numbers B_k, $k = (sp + 1)/2$, $B_1 = 1/6$, $B_2 = 1/30$, etc., ($s = 1, 3, \ldots, p - 4$) are divisible by p^2, for p an odd prime and (2) the second factor of the class number of the field $\Omega(\alpha)$ is prime to p, the equation $x^p + y^p + z^p = 0$ is not solvable in rational integers, none zero.

.....

Ciuropajlowicz, Thomas (Interlingua)

Duo Demonstrationes de Magno Theorema de Fermat.

Boll. di Mat., II, 5, 1926, p. 123-125.

The author here uses the substitutions $y = x + a$, $z = x + b$, $b - a = z - y = c$, and treats the equation $ck + bh = z^n$. He develops certain inequalities between x, y, z, a, b, and n. In $ck + bh = z^n$, $x^n = z^n - y^n = (z - y)k = ck$, $y^n = z^n - x^n = (z - x)h = bh$.

.....

Vandiver, H. S. (English)

Transformations of the Kummer Criteria in Connection with Fermat's Last Theorem.

Ann. of Math., II, 28, 1926-27, p. 451.

This paper contains other transformations of the same type as was considered in a previous paper by the same title (Ann. of Math., 1925-26). There are also developed here methods for extending the known criteria for $u^p + v^p + w^p = 0$, of the type

$$B_{\mu-1} \equiv B_{\mu-2} \equiv B_{\mu-3} \equiv B_{\mu-4} \equiv 0 \pmod{p}$$

where $\mu = (p-1)/2$ and the B's are Bernoulli numbers.

.....

Pomey, Léon (French)

Sur le dernier théorème de Fermat.

c. r. du l'Ass. fran., 1926, p. 67-68.

A proof of a proposition stated previously by Pomey. (c. r. Acad. Sci., 1923, p. 1187).

.....

Vandiver, H. S. (English)

Application of the Theory of Relative Cyclic Fields to Both Cases of Fermat's Last Theorem.

Trans. Am. Math. Soc., 29, 1927, p. 154. (Second Paper)

In this paper several theorems are obtained, including the following: If $x^p + y^p + z^p = 0$ is satisfied in integers none zero and each prime to the odd prime p, then

$$\left(\frac{(n^{p-1} - 1)}{p}\right) D_o \equiv 0, \quad \left(\frac{(n^{p-1} - 1)}{p}\right) B_{\frac{s+1}{2}} D_s \equiv 0 \pmod{p},$$

$s = 1, 3, \ldots, p-4$. $I(\alpha^d - \beta^a)$ is defined by

$$\left\{\frac{\theta}{\mathfrak{P}}\right\} = \alpha^{I(\theta)}, \qquad \theta = \alpha^a - \beta^d;$$

$\mathfrak{P}$ is a prime ideal divisor of the ideal (n), n being a rational odd integer $\not\equiv 0$ or $1 \pmod{p}$; $\alpha = e^{\frac{2\pi i}{p}}$, $\beta = e^{\frac{2\pi i}{n-1}}$; a is some integer in the set $1, 2, \ldots, n-2$, other than $((n-1)/2)$; the B's are the numbers of Bernoulli, $B_1 = 1/6$, $B_2 = 1/30$, etc, and $\left\{\frac{\theta}{\mathfrak{P}}\right\}$ is defined as

the power of α such that $\theta^{N(\mathfrak{p})-\frac{1}{\mathfrak{p}}} \equiv \left\{\frac{\theta}{\mathfrak{p}}\right\} \pmod{p}$, $N(\mathfrak{p})$ being the norm of $\mathfrak{p}$.

.....

Morishima, Taro (German)

Ueber die Fermatsche Vermytung I.

Proc. Imp. Acad. Jap., 4, 1928, p. 590-592.

The following theorem is given: If $x^p + y^p + z^p = 0$ $(x, y, z) = 1$, $p \nmid xyz$, $p > 5$, then $5^{p-1} \equiv 1 \pmod{p^2}$. The author gives a simple proof of this theorem in a case where $2^{p-1} \not\equiv 1 \pmod{p^4}$.

.....

Pérez-Cacho, L. (Spanish)

Sobre el ultimo teorema de Fermat.

Revista Mat. hisp-amer., (2) 3, 1928, p. 147-153.

The author makes a study of a work of W. Meissner (Sitzungber. der Kőnigl. Pruess. Akad. der Wiss., 1913).

.....

Steen, S. W. P. (English)

On Fermat's Last Theorem.

Proc. London Math. Soc., 29, 1928, p. 331.

"The object of this paper is to give formulae for $\sum \nu^2 \mu^2$ summed over the solutions of $a^n = \nu^n + \mu^n$ where a is a fixed integer and ν and μ are positive integers. In the course of the paper it soon becomes apparent that there is considerable simplification if $n = 2$, and that there is a difference between n even and n odd. The final formulae are given for n odd and greater than one.

"The method employed consists in forming the function

$$f_n(\xi) = \sum_{r=0}^{\infty} \frac{2\xi r^2}{\xi^2 - r^{2n}},$$

and finding a second expression for it by the Euler sum formula. The function

$$g_n(\xi) = f_n(\xi) f_n(a^n - \xi) \sin 2\pi\xi$$

is then formed."

.....

Vandiver, H. S. (English)

On the First Case of Fermat's Last Theorem.

Ann. of Math., II, 30, 1928-29, p. 552.

In this paper the author examines the equation $x^l + y^l + z^l = 0$, where x, y, and z are rational integers prime to the odd prime l and none zero. The special case $x \equiv y \pmod{l}$ is discussed, and among other results the following theorem is obtained: If the above equation is satisfied under the conditions mentioned, and $x \equiv y \pmod{l}$, then there exists no prime integers in the set $(1 + 2l), (1 + 4l), \ldots, 1 + (l - 1)l$.

.....

Vandiver, H. S. (English)

An Algorithm for Transforming the Kummer Criteria in Connection with Fermat's Last Theorem.

Ann. of Math., II, 30, 1928-29, p. 559.

In this paper the author applies the theory of power characters in the field $k(\zeta_l)$, $\zeta = e^{\frac{2\pi i}{l}}$, l an odd prime, to the equation $x^l + y^l + z^l = 0$, where x, y, and z are rational

integers prime to l and none zero. By means of this method various combinations of the well known Kummer criteria for the solution of this equation are obtained, including new derivations of the congruences

$$2^{l-1} \equiv 3^{l-1} \equiv 1 \pmod{l^2}.$$

.....

Vandiver, H. S. (English)

On Fermat's Last Theorem.

Trans. Am. Math. Soc., 31, 1929, p.613.

In various papers published during the last fifteen years the writer has obtained a number of results concerning Fermat's Last Theorem. In the present paper all these results are obtained from two general methods of approaching the problem. Some new criteria are also derived by the use of these methods. When applied to special exponents they yield the result that if $n > 2$, $x^n + y^n + z^n = 0$ is impossible in rational integers x, y, and z, none zero, for every n less than 211.

.....

Vandiver, H. S. (English)

Summary of Results and Proofs Concerning Fermat's Last Theorem.

Proc. Nat. Acad. Sci., 15, 1929, p. 43. (Third Paper)

In this paper, among other results, a proof is indicated for the following theorem: Under the assumption (1) none of the Bernoulli numbers $B_{\nu p}$ ($\nu = 1, 2, 3, \ldots, (p-3)/2$) is divisible by p^3 and (2) the second factor of the class number of the field $k(\alpha)$, $\alpha = e^{\frac{2\pi i}{p}}$, is prime to p, it follows that $x^p + y^p + z^p = 0$ is not satisfied in rational

integers x, y, and z, prime to each other, none zero, if $xyz \equiv 0 \pmod{p}$, and p is an odd prime.

.....

Vandiver, H. S. (English)

Summary of Results and Proofs Concerning Fermat's Last Theorem.

Proc. Nat. Acad. Sci., 15, 1929, p. 108. (Fourth Paper)

A summary of a paper the details of which appear in Trans. Am. Math. Soc., 31, 1929.

.....

Morishima, Taro. (German)

Ueber die Fermatsche Vermutung, II.

Proc. Imp. Acad., 5, 1929, p. 183-185.

The author proves the theorem:

"Let $x^p + y^p + z^p = 0$ $(x, y, z) = 1$, $xyz \not\equiv 0 \pmod{p}$ then

$$\sum_{h=1}^{p-1} h^{p-1} \cdot t^h \equiv 0 \pmod{p^2}$$

where $-t \equiv y/x, x/y, y/z, z/y, z/x, x/z \pmod{p^2}$ and moreover when $p > 3$ we have

$$\sum_{i=1}^{p-1} \frac{t^i}{i} \equiv 0 \pmod{p^2} . "$$

.....

Morishima, Taro (German)

Ueber die Fermatsche Vermutung, III.

Proc. Imp. Acad., 5, 1929, p. 263-264.

The author proves that $\sum_{i=1}^{p-1} \frac{t^i}{i} \equiv 0 \pmod{p^2}$ holds where $t = -x/y$, etc., for the first case of Fermat's Last

Theorem where $p > 3$.

.....

McDonnell, John (English)

Note on Fermat's Last Theorem.

Bull. Am. Math. Soc., 35, 1929, p. 769.

The author proves that if $x^p + y^p + z^p = 0$, then (1) if $yz + zx + xy \not\equiv 0 \pmod{p}$, and r be any factor of $x^2 - y^2$, then $r^{p-1} \equiv 1 \pmod{p^2}$, and (2) if $x(x - z)(x^2 + y^2) \not\equiv 0 \pmod{p}$ and r be any factor of $x^2 + yz$, then $r^{p-1} \equiv 1 \pmod{p^2}$. The proof resembles a proof of Furtwängler for a similar result.

.....

Turner, J. S. (English)

Some Identities Connected with Fermat's Last Theorem.

Bull. Am. Math. Soc., 36, 1930, p. 204.

In this paper, the equation $a^n + b^n = c^n$ (a, b, c, n positive integers, $n > 2$) is transformed by various trigonometrical formulas. Attempts are made to find the highest powers of 2 and n contained in the non-zero members of the resulting equations. In this way many interesting identities are discovered.

.....

McDonnell, John (English)

New Criteria Associated with Fermat's Last Theorem.

Bull. Am. Math. Soc., 36, 1930, (August)

"Furtwängler has obtained by means of Eisenstein's law of reciprocity for residues of p-th powers, p an odd prime, certain criteria in connection with the solution of the equation

$x^p + y^p + z^p = o$ where x, y, z are relatively prime rational integers, and these criteria involve the rational factors of x, y, z, y - z, z - x, x - y.

"It is the object of the present article to employ the same method to derive similar criteria for the factors of $x^2 - yz$, $y^2 - zx$, $z^2 - xy$, $x^2 + y^2$, $y^2 + zx$, $z^2 + xy$."

.....

Vandiver, H. S. (English)

Summary of Results and Proofs on Fermat's Last Theorem.

Proc. Nat. Acad. Sci., 16, 1930, p. 298. (Fifth Paper)

In this article Vandiver gives a number of sidelights and comments on the contents of his article in Trans. Am. Math. Soc., 31, 1929, and also extends some of the theorems therein.

.....

Morishima, Taro (German)

Ueber die Fermatsche Vermutung, IV.

Proc. Imp. Acad., 6, 1930, p. 243-244.

The author gets two kinds of equations of the Fermat type which have no integral solution with respect to the particular field. This results from the following theorem which he proves. For $n \geq 3t + 2$, $x^l + y^l + z^l = 0$, $(x, y) = 1$, l/z, $l + h$ where h_o is the class number of k_o, k_o is the real subfield of degree $(l - 1)/2$ of k, k is the cyclotomic field of $\zeta_j = e^{\frac{2\pi i}{l^t}}$, and l^t is the highest power contained in the class number of k.

.....

Morishima, Taro (German)

Ueber die Fermatsche Vermutung, V.

Proc. Imp. Acad., 6, 1930, p. 303-305.

The author proves the following theorem: For $n \geqq \sigma + t$

(1) $\alpha^{\ell} + \beta^{\ell} = \varepsilon \gamma^{\ell^n}$, $(\alpha, \beta, \gamma, \ell) = 1$

has no solutions in integers of k_o where ε is a unit of this field. $\sigma = (\ell - 3)/2$, $\ell > 31$. If $\ell \leqq 31$ he can also prove that (1) has no solution in k_o when $n = 1$.

.....

Massoutié, L. (French)

Sur le dernier théorème de Fermat.

c. r. Acad. Sci. Paris, 193, 1931, p. 502-504.

If p is a prime of the form 6n - 1, then it is necessary that one of the unknowns of the equation $x^p + y^p + z^p = 0$ be divisible by 3. The proof is by means of the theory of rational numbers.

.....

Pomey, Léon (French)

Nouvelles remarques relatives au dernier théorème de Fermat.

c. r. Acad. Sci. Paris, 193, 1931, p. 563-564.

Another and shorter proof of the theorems of Massoutié.

.....

Morishima, Taro (German)

Ueber den Fermatschen Quotienten.

Japanese Journal of Mathematics, 8, 1931, p. 159-173.

An extension of some results of Wieferich, Mirimanoff, Vandiver, Frobenius, and Pollaczek. This is, that for a solution of

(1) $$x^p + y^p + z^p = 0$$

in integers, not divisible by p, it is necessary that

(2) $$q(m) = \frac{m^p - m}{p} \equiv 0 \pmod{p}$$

is fulfilled for m = 2, 3, 5, 11, 17 and if p = 6k + 5 it must be fulfilled for 7, 13, 19, and except for a finite number of primes p the congruence will hold for all prime numbers $m \leqq 31$. The author generalizes this result for other possibilities of p and m.

.....

Georgikopulos, Const. Ch.

Zum letzen Fermatschen Satz.

Delt. Hellen. math. Hetair, 12, 1931, p. 109-122.

.....

Netanjahu Mileikowsky, E. (German)

Elementorer Beitrag zur Fermatschen Vermutung.

J. Reine agnew. Math., 166, 1931, p. 116-117.

The author gives elementary proofs of the following: If $x < y < z$ are three relatively prime positive integers and $n > 2$, and $x^n + y^n = z^n$, then z is not a power of a prime. If n is not prime, then x and y are not powers of primes.

.....

Vandiver, H. S. (English)

Summary of Results and Proofs on Fermat's Last Theorem.

Proc. Nat. Acad. Sci., 17, 1931, p. 661-673. (Sixth Paper)

This article is an extension of the fifth paper of the same title. Besides this he simplifies Theorem IV of Trans. Am. Math. Soc., 31, 1929.

.....

Bussi, Carlo (Italian)

Sull'ultimo teorema di Fermat.

Boll. Un. Mat. Ital., 11, 1932, p. 267-269.

The author concludes that $a^{\varphi(k)} + b^{\varphi(k)} = c^{\varphi(k)}$ is impossible if a, b, c are all relatively prime to k, and some simple consequences of this fact.

.....

Morishima, Taro (German)

Ueber die Fermatsche Vermutung, VII.

Proc. Imp. Acad., 8, 1932, p. 63-66.

The author extends some results given by Vandiver and Kummer for the equation $x^{\ell} + y^{\ell} + z^{\ell} = 0$ where $(x, y, z, \ell) = 1$.

.....

Morishima, Taro (German)

Ueber die Fermatsche Vermutung, VIII.

Proc. Imp. Acad., 8, 1932, p. 67-69.

The author proves the theorem: If $x^{\ell} + y^{\ell} + z^{\ell} = 0$ is satisfied in Case I, then the six ratios $-t = x/y$, etc. must satisfy

$$b_{2i} \cdot f_{2i}(t) \left[\frac{d^{\ell(\ell-2i)}}{dv^{\ell(\ell-2i)}} \log(1 - e^{v}(1 - t)) \right]_{v=0} \equiv 0 \pmod{\ell^2}.$$

Morishima, Taro (German)

Ueber die Fermatsche Vermutung, IX.

Proc. Phys. Math. Soc. Jap., III, 14, 1932, p. 451-464.

The author extends a result given by Kummer for the equation $x^{\ell} + y^{\ell} + z^{\ell} = 0$ having the integral solutions x, y, z not divisible by ℓ and relatively prime.

.....

Vandiver, H. S. (English)

On the Method of Infinite Descent in Connection with Fermat's Last Theorem for Regular Prime Exponents.

Comment. Math helv., 4, 1932, p. 1-8.

In this paper regular primes are defined together with a list of all those less than 307. Kummer in Crelle's Journal 1850, proved that

$$\alpha^{\ell} + \beta^{\ell} + \gamma^{\ell} = 0$$

is impossible if α, β and γ are non-zero integers in the field $k(\zeta)$ prime to each other; $\zeta = e^{\frac{2\pi i}{\ell}}$ and ℓ is an odd prime greater than 3 such that $B_1, B_2, \ldots, B_{\left(\frac{\ell-3}{2}\right)}$ have numerators which are Bernoulli numbers, expressed in theor lowest terms. The prime 3 is defined as regular. The proof of Kummer was divided into two distinct parts. Vandiver gives a somewhat similar method of descent to cover both cases of Fermat's Last Theorem.

.....

Lehmer, D. H. (English)

A Note on Fermat's Last Theorem.

Bull. Am. Math. Soc., 38, 1932, p. 723-724.

The author extends Morishima's improvement on a theorem by Vandiver and ends with the lemma given as Theorem 4; If $x^p + y^p + z^p = 0$ has a solution for which xyz and p are coprime, then the first factor of the class number of the cyclotomic field $K(e^{\frac{2\pi i}{p}})$ is divisible by p^{12}.

.....

Moriya, M. (German)

Uber die Fermatsche Vermutung.

J. reine angnew. Math., 169, 1933, p. 92-97.

The author attacks the same problem as Maillet (Ass. fran. pour l'avan. Sci., St. Etienne, 1897; Fortschritte d. Math., 29, 1898) by a different method, one used by Landau (Vorlesungen uber Zahlentheorie).

.....

Matoušek, J. (Czeckish)

Une prauve de la théorème de M. Fermat pour la 4^e puissance.

Rozhl. mat. přirod., 13, 1933, p. 4-7.

This periodical compares to the "The Mathematics Teacher" and is an exposition of Fermat's Last Theorem for the case n = 4.

.....

Kapferer, H. (German)

Über die diophantischen Gleichungen $z^3 - y^2 = 3^3 \cdot 2^\lambda \cdot X^{\lambda+2}$ und deren Abhängigkeit von der Fermatschen Vermutung.

s. B. Heidelberg Akad. Wiss. Abh., 2, 1933, p. 32-37.

For an application of these equations to Fermat's Last Theorem, see Lubelski, Prace mat-fiz., 1935.

.....

Morishima, Taro (German)

Ueber die Fermatsche Vermutung, X.

Proc. Imp. Acad., 9, 1933, p. 577-579.

The following theorem is proved. Let t and t_o be the orders of the groups of q-th powers of the classes of the cyclotomic field $R(\zeta)$, respectively, of the real subfield $R(\zeta + \zeta^{-1})$ of $R(\zeta)$ where R represents the field of the rational numbers. If $t_1 < t_o < 6$ then $x^\ell + y^\ell + z^\ell = 0$ $(x, y, z, \ell) = 1$ has no integer solutions.

.....

Gravé, D. (Ukrainian)

Les méthods de la lutte contre les difficulties du grand probleme de Fermat.

J. Cycle math. Acad. Sci., Ukraine 1, Fasc. 4, 1934, p. 33-44.

Several well known methods are reviewed by means of which Fermat's Last Theorem is attacked. It has to be stressed that

$$\frac{(x + y + z)^n - x^n - y^n - z^n}{n(x + y)(y + z)(z + x)}$$

has been computed not by P. Bachmann, but by E. Catalan (Mein. Soc. Sc. Liége (2) (12) 1885, p. 179-185, 403).

.....

Vandiver, H. S. (English)

Fermat's Last Theorem and the Second Factor in the Cyclotomic Class Number.

Bull. Am. Math. Soc., 40, 1934, p. 118.

The author gives a sketch of a proof of a theorem which appears to him to be the principal result he has found so far concerning the first case of Fermat's Last Theorem. The work of this paper deals with this theorem given as Theorem 1, and with another given as Theorem 2, which extends some previous results. These theorems are:

Theorem 1. If $x^\ell + y^\ell + z^\ell = 0$ is possible in Case I, then the second factor of the class number of the cyclotomic field defined by $\zeta = e^{\frac{2\pi i}{\ell}}$ is divisible by ℓ.

Theorem 2. If $x^\ell + y^\ell + z^\ell = 0$ is satisfied in Case I, then, if η_j is a unit in $k(\zeta)$

$$E_{\ell-j} = \eta_j^\ell, \quad (j = 0, 1, 2, 3, 4, 5)$$

and

$$B_s \equiv 0 \pmod{\ell^2} \quad \begin{matrix} (i = 1, 2, 3, 4, 5, 6) \\ (s = n_i(\ell + 1) - i), \end{matrix}$$

where the n's each range independently over all positive integral values.

The author adds, "It may happen that Fermat's Last Theorem is true for rational integers, but for integers in the field $k(\zeta + \zeta^{-1})$ it is not true. Possibly the method of infinite descent properly belongs to the treatment of this generalization."

.....

James, Glenn (English)

On Fermat's Last Theorem.

Am. Math. Monthly, 41, 1934, p. 419-424.

This paper considers the Fermat equation $x^n + y^n = z^n$, $z > y > x > 0$, for the so called first case and proves that $z - y > c^n n^n$ where c is a certain function of x, y, and z whose lower limit is 2. This work provides a simple, and what seems to be a new proof for the case $n = 3$, and suggests a point of attack on the general. problem.

.....

Krasner, Marc (French)

Sur le premier cas du théorème de Fermat.

c. r. Acad. Sci. Paris, 199, 1934, p. 256-258.

This paper ties up various results given by different authors on Kummer's criteria for the first case.

.....

Pomey, Léon (French)

Sur le dernier théorème de Fermat (Divisibilite par 3 et par 5).

c. r. Acad. Sci. Paris, 199, 1934, p. 1562-1564)

A study of the case where $n = 6h + 1$. He concludes

1. that $x_1^n + x_2^n + x_3^n = 0$ is impossible if one of x_1, x_2, x_3 is not divisible by 3.
2. that $x_1^n + x_2^n + x_3^n = 0$ is impossible if one of x_1, x_2, x_3 is not divisible by 5.

.....

Grün, Otto (German)

Zur Fermatschen Vermutung.

J. reine angew. Math., 170, 1934, p. 231-234.

Given ℓ an irregular prime, ζ a primitive ℓ-th root of unity, $k = k(\zeta)$, k_o the greatest real field contained in k. Using this he develops the following: The equation $x^\ell + y^\ell + z^\ell = 0$ is impossible in rational integers x, y, z with $xyz \equiv 0 \pmod{\ell}$ and $xyz \not\equiv 0$ for $\ell > 3$, if the class number of k_o is prime to ℓ and none of the Bernoulli numbers $B_{i\ell} \equiv 0 \pmod{\ell^3}$ for $i = 2, 4, \ldots, \ell - 3$. There can be an infinite number of Bernoulli numbers $B_i \equiv 0 \pmod{\ell}$ for $i = 2, 4, \ldots, \ell - 3$.

.....

Morishima, Taro (German)

Uber die Fermatsche Vermutung, XI.

Jap. Jour. of Math., 11, 1934, p. 241-252.

An extension of Morishima (Jap. Jour. Math., 8, 1931) and Vandiver (Bull. Amer. Math. Soc., 1934, p. 118-126).

.....

Morishima, Taro (German)

Ueber die Fermatsche Vermutung, XII.

Proc. Imp. Acad. Jap., 11, 1935, p. 307-309.

An extension of Theorem 5 of a previous work (Jap. Jour. Math, 11, 1934, p. 241-252).

.....

Niewiadomski, R. (German)

Zur Fermatschen Vermutung.

Prace mat-fiz., 42, 1935, p. 1-10.

This article contains an eight page table of all p-th power residues modulo p for each prime less than 200. The object of the table is to furnish, at least for $p = 6n - 1$, an elementary test for the solvability of $x^p + y^p = z^p$ where p is prime to xyz. In fact, it is easily seen that a sufficient condition for the non-existence of (x, y, z) is the non-existence of two p-th power residues which differ by unity. This simple test fails for all primes p of the form $6n + 1$ and also for $p = 53$, 83, and 179.

.....

Lubelski, S. (German)

Studien über den grossen Fermatschen Satz.

Prace mat-fiz., 42, 1935, p. 11-44.

The results of novelty in this paper concern the generalization of the criteria of Furtwängler, Kummer, and Kapferer to the case of the equation (1) $x^p + y^p = cz^p$. For example the author proves that in case (1) has a solution for which cxyz id prime to the odd prime p and if c is either a p-th power residue modulo p^2 or such a non-residue that c/2 is itself a residue and finally if c is divisible by no prime of the form $pn + 1$, then $2^p - 2$ is divisible by p^2. As an analogue of Kapferer's theorem we have: If c is a prime or a power of a prime the equation (1) with p merely odd

has solutions not zero if and only if the equation
$u^3 - v^2 = 3 \cdot 2 \cdot c \cdot w \cdot p$ is solvable.

.....

Lehmer, Emma (English)

On a Resultant Connected with Fermat's Last Theorem.

Bull. Am. Math. Soc., 41, 1935, p. 864-867.

This is an extension of Bachmann, DAS FERMATPROBLEM, page 59, and some of the results of Lubelski (Prace mat-fiz. 1935).

.....

Vandiver, H. S. (English)

On Trinomial Diophantine Equations Connected with the Fermat Relation.

Mh. Math. Phy., 43, 1936, p. 317.

In this paper the author considers the equation $x^\ell + y^\ell = cz^\ell$ where c is a given rational integer and ℓ is a given prime greater than 3 which is regular. The discussion is divided into three cases: (1) xyz prime to ℓ ; (2) $xy \equiv 0 \pmod{\ell}$; (3) $z \equiv 0 \pmod{\ell}$. Combining the results for the three cases the author gets the following theorem:
The equation

$$x^\ell + y^\ell = cz^\ell$$

where c is a given integer prime to the regular prime $\ell > 3$ and containing only prime factors belonging to even exponents, modulo ℓ , is impossible in non-zero integers, x, y, and z, provided $c^{\ell-1} \not\equiv 1 \pmod{\ell^2}$
and $2^{\ell-1} \not\equiv c^{\ell-1} \pmod{\ell^2}$.

.....

Yamada, Kaneo (English)

On the Necessary Condition for the Fermat's Last Theorem.

Proc. Imp. Acad. Japan., 12, 1936, p. 313-317.

Vandiver (Ann. of Math., 1924) proved that if

$$x^p + y^p + z^p = 0, \qquad p \nmid xyz,$$

then the following condition

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{\left[\frac{p}{3}\right]^2} \equiv 0 \pmod{p},$$

is necessary.

In the present paper the author gives a proof of H. Schwandt's condition (Jahresber. 1934)

(I) $$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{\left[\frac{p}{6}\right]^2} \equiv 0 \pmod{p}$$

and then shows that two analogous conditions

(II) $$\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{\left[\frac{p}{3}\right]} \equiv 0 \pmod{p}$$

and

(III) $$\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{\left[\frac{p}{6}\right]} \equiv 0 \pmod{p}$$

are necessary.

.....

Thébault, V. (French)

Sur une application du dernier théorème de Fermat.

Enseignement Math., 36, 1937, p. 222-228.

An interesting study of triangles which, incidentally, the author says, may be a new proof of the case where $n = 4$.

.....

James, Glenn (English)

On the First Case of Fermat's Last Theorem.

Bull. Am. Math. Soc., 43, 1937, p. 774.

In a previous paper limits were established for the parameters x, y, z of the Fermat equation $x^n + y^n = z^n$, beneath which this equation can have no solution. When $n = 3$ the limit was $21,147^+$ and when $n = 14,000$ the limit was $10^{112,300+}$ (14,000 is the limit for n beneath which the equation is known to have no solution). In the present paper these limits are raised to $26,855^+$ and $(10/7)10^{112,300}$, the general limit being raised from $n(2n^2 + 1)$ to

$$\left(\frac{1}{(2^{\frac{1}{n}} - 1) - 1}\right)$$

times that limit.

.....

Vandiver, H. S. (English)

On Bernoulli Numbers and Fermat's Last Theorem.

Duke Math. Jour., 3, 1937, p. 569-584.

This paper summarizes some of the results that have been found regarding Bernoulli numbers and simplifies and generalizes some previous results of congruences with Bernoulli numbers. Among other results it extends the results of Fermat's Last Theorem for special exponents particularly with a study of primes ℓ, regular and irregular, $306 < \ell < 617$.

.....

Gottschalk, Eugen (German)

Zum Fermatschen Problem.

Math. Ann., 115, 1938, p. 157-158.

The author develops the following: If the prime p or a multiple mp which is not divisible by p^2 is resolved into $mp = a \pm b$ so that

(I) a and b have no other prime factors than 2, 3, 5, 11, 17:

and

(II) if $p \equiv 5 \pmod 6$, a and b have no greater prime factor than 19,

then the Fermat problem has no solutions.

.....

Niewiadomski, R. (Polish)

Sur la grandeur absolue et relation mitelle des nombres entiers qui peuvent resomdre l'equation $x^p + y^p = z^p$.

Widdom. mat., 54, 1938, p. 113-127.

.....

CHAPTER V

BOOKS PUBLISHED FROM 1919 TO 1938

The following books have been published during the period 1919 to 1938 pertaining to Fermat's Last Theorem.

Algebraic Numbers - II, Bulletin 62. National Research Council. 1928.

Bachmann, Paul; Das Fermatproblem in seiner bisherigen Entwicklung. 1919.

Bruns, H. W. ; Über den Ursprung der Tatsache, die dem grossen Fermatschen Theorem zugrunde liegt. 1933.

Cashmore, M. ; Fermat's Last Theorem: Three Proofs by Elementary Algebra. Revised edition 1919, third edition 1921.

Chincin, A. J. ; Der grosse Fermatsche Satz.

Christof, P. ; Das Fermat'sche Problem und seine Losung. - Le probleme de Fermat et sa solution.

Dickson, L. E. ; History of The Theory of Numbers. Volume II, Chapter 26. 1919.

Franz, W. E. ; Fermat, $x^n + y^n \lesseqgtr z^n$.

Heil, J. ; Das letzte Fermatsche Theorem und seine Lösung.

Hennig, P. ; Meine Lösung des Fermat-Problems. 1926.

Junker, F. ; Der grosse Fermatsche Satz. Vollständiger Beweis des Satzes auf elementar-mathematischer Grundlage. 1921.

Keller, Ernst; Die Lösung des Problems von Fermats. 1929.

Lindemann, Ferdinand; Nachtrag zu meiner Shrift uber den Fermatschen Satz. 1928.

Lindemann, Ferdinand; Untersuchungen über den Fermatschen Satz. 1928.

Mordell, L. J. ; Three Lectures on Fermat's Last Theorem. 1921.

Muika,I. ; Das Fermatsche Theorem. 1926.

Muika,I. ; Das Fermatsche Theorem. 1927.

Muika,I. ; Théorème de Fermat. Fourth edition. 1924.

Nikalajew, B. ; Bedingungen der Möglichkeit der Gleichungen $x^n + y^n = z^n$ in ganzen zahlen. 1924.

Nogues, R. ; Théorème de Fermat. Son histoire. 1932.

Romert, J. ; Der elementare Beweis des Fermatschen Satzes $x^{2n+1} + y^{2n+1} = z^{2n+1}$ auf Grund der Zerlegung in Faktoren wid der Regeln der Potenzlehre. 1920.

Rupeika, Z. ; Didziosios P. Fermat'o teoremas irodynias. 1934.

Theiss, F. ; Zahlenbeispiele zum grossen Fermat'schen Satz. 1934.

Villani, N. ; L'equazione di Fermat $x^n + y^n = z^n$, con dimostrazione generale.

Walsh, C. M. ; An Attempted Proof of Fermat's Last Theorem by A New Method. 1932.

Weigel, H. W. ; $x^n + y^n = z^n$? Die elementare Lösung des Fermatprobleme. 1933.

CHAPTER VI

BIBLIOGRAPHY

BIBLIOGRAPHY

The following books will offer the beginner a very good approach to the problems concerning and incidental to Fermat's Last Theorem.

Algebraic Numbers - I - National Research Council. 1923.

Algebraic Numbers - II - National Research Council. 1928.

Bachmann, Paul. Das Fermatproblem in seiner bisherigen Entwicklung. 1919.

Carmichael, R. D. Diophantine Analysis. Chapter 5.

Dickson, L. E. . Fermat's Last Theorem. Annals of Mathematics. 18, 1917, page 161.

Dickson, L. E. . History of the Theory of Numbers. Volume II. Chapter 26. 1919.

Dickson, L. E. . Introduction to the Theory of Numbers. 1929.

Hancock, Harris. Foundations of the Theory of Algebraic Numbers, Volume I, 1931.

Mordell, L. J. . Three Lectures on Fermat's Last Theorem. 1921.

Reid, L. W. . The Elements of the Theory of Algebraic Numbers. 1910.

Weisner, Louis. Introduction to the Theory of Equation. 1938.

BIBLIOGRAPHY

In order to facilitate the securing of the full name of the publication in which various articles may appear, the following list is compiled.

Annals of Mathematics

Bollettino della Unione Matematica Italiana

Bollettino di Matematica

Bulletin of the American Mathematical Society

Commentarii Mathematici Helvetici

Comptes rendus du Congres de 1926 de l'Association Francaise pour L'Avancement Des Sciences. Lyon. 1926.

Comptes rendus hebdomadaires des seances de l'academie des sciences.

Duke Mathematical Journal

Japanese Journal of Mathematics

Journal de Mathematiques

Journal für die reine und angewandte Mathematik

L'Enseignement Mathématique

Mathematische Annalen

Monatshefte fur Mathematik und Physik

Norsk Mathematisk Tidsskrift

Prace Matematyczno-Fizyczne

Proceedings of the Imperial Academy of Japan

Proceedings of the London Mathematical Society

Proceedings of the National Academy of Science

Proceedings of the Physico-Mathematical Society of Japan

BIBLIOGRAPHY

Rozhledy matematicko-přírodovědecké.

Revista Matematica Hispano-Americana

Sitzungsberichte der Heidelberger Akademie der Wissenschaften

The American Mathematical Monthly

Transactions of the American Mathematical Society

.....

The following two periodicals, among others, contain a list of mathematical publications and articles which appear in those publications.

Jahrbuch Uber Die Fortschritte Der Mathematik

Zentralblatt Für Mathematik und Ihre Grenzgebiete

.....