...that is, ...RY OF RESULTS AND PROOFS ON FERMAT'S LAST THEOREM (SIXTH PAPER)

BY H. S. VANDIVER

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS

Communicated October 26, 1931

In a re...nt paper[1] the writer proved a number of results concerning Fermat's ...st Theorem. In another article[2] he gave a number of side-lights an...mments on the contents of that paper, as well as extensions of the ...rems therein. In the present paper further results will be given along these lines.

As noted in N, Theorem IV of T is quite complicated and in the former paper another proof is indicated. I give here, however, a method for proving the statement which is far simpler than either of those just referred to. We shall assume the relation (27) of T, that is

$$\omega + \zeta\theta \equiv 0 \pmod{\mathfrak{P}} \tag{1}$$

omitting the superscripts in ω and θ. Hence the relation (27a) of T takes the form

$$\begin{gathered}(\omega + \zeta^a\theta)^c \equiv (\zeta^a\omega + \theta)^c \pmod{\mathfrak{P}} \\ a = 0, 2, 3, \ldots, l-2.\end{gathered} \tag{2}$$

$$\text{Set } f(a) = (\omega + \zeta^a\theta)^c, \text{ and } g(a) = (\zeta^a\omega + \theta)^c.$$

Expansion of (2) gives

$$\begin{gathered}\omega^c + c\omega^{c-1}\zeta^a\theta + \binom{c}{2}\omega^{c-2}\zeta^{2a}\theta^2 + \ldots + \zeta^{ac}\theta^c \equiv \\ \zeta^{ac}\omega^c + c\zeta^{a(c-1)}\omega^{c-1}\theta + \binom{c}{2}\zeta^{a(c-2)}\omega^{c-2}\theta^2 + \ldots\end{gathered} \tag{3}$$

As noted before this is true for $a = 0, 2, 3, \ldots, l-2$. Noting that $f(1) \equiv g(-1) \equiv 0 \pmod{\mathfrak{P}}$ we then obtain

$$-f(-1) + \sum_{i=0}^{l-1} f(i) \equiv -g(1) + \sum_{i=0}^{l-1} g(i) \pmod{\mathfrak{P}}.$$

Using $(\zeta^k)^{l-1} + (\zeta^k)^{l-2} \ldots + 1 = 0$ for $k \not\equiv 0 \pmod{l}$, and noting that $c < l$, this gives

$$l\omega^c - (\omega + \zeta^{-1}\theta)^c \equiv l\theta^c - (\zeta\omega + \theta)^c \pmod{\mathfrak{P}},$$

and using $\omega \equiv -\zeta\theta \pmod{\mathfrak{P}}$ this reduces to

$$-\zeta^c l \equiv (1 - \zeta^2)^c \pmod{\mathfrak{P}}. \tag{4}$$

In the same way we have

$$-\zeta f(-1) + \sum_{i=0}^{l-1} \zeta^{-i} f(i)$$
$$\equiv -\zeta^{-1} g(1) + \sum_{i=0}^{l-1} \zeta^{-i} g(i) \pmod{\mathfrak{P}}$$

and this gives $lc\zeta^c(\zeta^{c-2} - 1) \equiv (\zeta^{c-2} - 1)(1 - \zeta^2)^c$.

Now if $c \neq 2$ we have $lc \equiv (1 - \zeta^2)^c \pmod{\mathfrak{P}}$ and comparison with (4) gives $c \equiv -1 \pmod{\mathfrak{P}}$, which is impossible.

For $c = 2$, we obtain from (1) and (2)

$$(\zeta - \zeta^a)^2 \equiv (\zeta^{a+1} - 1)^2.$$

Set $a = 2$, this gives

$$\zeta - \zeta^2 \equiv \pm(\zeta^3 - 1) \pmod{\mathfrak{P}}, \tag{5}$$

and the plus sign gives

$$\zeta^3 + \zeta^2 \equiv \zeta + 1$$

and

$$(\zeta^2 - 1)(\zeta + 1) \equiv 0 \pmod{\mathfrak{P}},$$

which is impossible, since $(\zeta + 1)$ is a unit and $(\zeta^2 - 1)$ is a prime ideal factor of (l), which is prime to p. The minus sign in (5) gives

$$(\zeta^2 + 1)(\zeta - 1) \equiv 0 \pmod{\mathfrak{P}},$$

which is likewise impossible.

Hence we have proved that $\omega + \theta$ is divisible by p in (26a) of T.

The above proof applies in connection with Theorem IV but not in connection with the proof of Theorem V of T, since in the latter case the p we are using is not necessarily less than $(l^2 - l)$. The argument for the proof of $\theta + \omega = 0 \pmod{p}$ which was used in T in connection with the proof of Theorem IV is necessary to supply a similar step in the proof of Theorem V of T, since that part of the argument in the proof of Theorem IV does not depend upon the fact that p is less than $(l^2 - l)$.

We now consider the relation

$$\alpha^l + \beta^l + \eta\gamma^l = 0 \tag{6}$$

where l is a regular prime; α, β and γ are integers in the field $k(\zeta)$ none zero, and η is a given unit in this field. Let us assume first that γ is prime to $\lambda = (1 - \zeta)$. Since we may take α and β each in the form $f(\text{mod } \lambda^2)$, it follows that $\alpha^l \equiv a(\text{mod } \lambda^l)$, $\beta^l \equiv b(\text{mod } \lambda^l)$ and $\gamma^l \equiv c \pmod{\lambda^l}$, where a, b and c are rational integers. Reducing our equation $(\text{mod } \lambda^l)$ we obtain,

$$a^l + b^l + \eta c^l \equiv 0 \pmod{\lambda^l}.$$

Since γ is prime to λ it follows that

$$c \not\equiv 0 \pmod{\lambda},$$

hence we have,

$$\eta \equiv -\frac{a^l + b^l}{c^l} \pmod{\lambda^l}$$

Hence η is congruent to a rational integer, (mod λ^l), and hence is primary

Since the field is regular, however,[3] it follows by a known result that η is the lth power of a unit in $k(\zeta)$. Hence our relation (6) becomes

$$\alpha^l + \beta^l + \gamma_1{}^l = 0 \tag{7}$$

where γ_1 is an integer in $k(\zeta)$. This relation is known[4] to be impossible, hence (6) is impossible for γ prime to λ.

Consider now the case where γ is divisible by λ in (6). In both the known[4] proofs that

$$\alpha^l + \beta^l + \gamma^l = 0$$

is impossible where γ is divisible by λ; the arguments include a proof that (6) is impossible for γ divisible by λ. For the first steps in these arguments take the equation in the general form (6). Hence we may state the

THEOREM. *The equation*

$$\alpha^l + \beta^l + \eta\gamma^l = 0$$

is impossible for α, β and γ integers in the field $k(\zeta)$ none zero where η is a given unit in this field and l is a regular prime.

So far in connection with known proofs of Fermat's Last Theorem for regular primes the discussion has been divided into two quite distinct parts. The first part is confined to the case where x, y and z are prime to each other and $xyz \not\equiv 0 \pmod{l}$, called case I, in the relation

$$x^l + y^l + z^l = 0. \tag{7a}$$

The second part of the proof considers the case where one of the integers is divisible by l, called case II. The treatments of case II have always involved some form of Fermat's famous method of infinite descent. The writer has constructed a proof that (6) is impossible in the special case where α, β and γ belong to the field $\Omega(\zeta + \zeta^{-1})$ prime to each other, in which the treatment of case I, that is when α, β and γ are prime to λ, also involves the method of infinite descent. In fact, the argument is so

constructed that the two cases are treated simultaneously during the descent. The equation is taken in the form

$$\theta^l + \omega^l + \delta\gamma^l = 0. \tag{7b}$$

For the case γ prime to λ we have

$$\theta + \omega\zeta^a = \eta_a^l \sigma_a^l \; ; \qquad a = 0, 1, \ldots, l-1.$$

We deduce from this by known methods the relation $\theta \equiv \omega \pmod{\lambda^l}$ and this gives

$$\theta + \omega\zeta^a = (1 + \zeta^a)\eta_a\sigma_a^l$$

where η_a is a real unit in $k(\zeta)$.

Also by known methods we have for the case where γ is divisible by λ the relation

$$\frac{\theta + \zeta^a\omega}{1 - \zeta^a} = \eta''_a\rho_a^l.$$

The last two relations may be combined into the statement

$$\frac{\theta + \omega\zeta^a}{1 \pm \zeta^a} = \eta_a\sigma_a^l \; ; \qquad a = 1, 2, \ldots, l-1. \tag{8}$$

From this relation we obtain

$$\sigma_{-a}^{\,l}\,\frac{\theta + \omega\zeta^a}{1 \pm \zeta^a} = \frac{\theta + \omega\zeta^{-a}}{1 \pm \zeta^{-a}}\,\sigma_a^{\,l}$$

where σ_{-a} is obtained from σ_a by the substitution ζ/ζ^{-1}. This is considered (mod $\mathfrak{P}$) where $\mathfrak{P}$ is a prime ideal divisor of $\theta + \omega\zeta$. Using power characters we infer as in a former paper by the writer[4a]

$$\left\{\frac{E_n}{\mathfrak{P}}\right\} = 1; \quad n = 1, 2, \ldots, \frac{l-3}{2}.$$

Hence

$$\left\{\frac{E_n}{\sigma_1}\right\} = 1,$$

where

$$E_n = \prod_{i=0}^{(l-3)/2} \epsilon(\zeta^{ri})^{r^{-2in}}$$

$$\epsilon = \left(\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}\right)^{1/2},$$

r being a primitive root of l. By taking the known expressions for power

characters of units in a cyclotomic field we find after some transformations, the relation

$$\sigma_1 \equiv \sigma_{-1} \pmod{\lambda^{l-1}}.$$

Using (8) we have

$$\theta + \omega\zeta = (1 \pm \zeta)\eta_1\sigma_1^l$$
$$\theta + \omega\zeta^{-1} = (1 \pm \zeta^{-1})\eta_{-1}\sigma_{-1}^l$$
$$\lambda^t(\theta + \omega) = \eta_0\sigma_0^l$$

where the exponent $t = 0$ or (-1), according as γ is not or is divisible by λ. Eliminating θ and ω from the last three equations we obtain

$$\sigma_1^l \pm \sigma^l{}_{-1} = \eta_0^1\sigma_0^l$$

where η_0^1 is a unit in $k(\zeta)$. This leads to

$$\sigma_1 \pm \zeta^a\sigma_{-1} = (1 \pm \zeta^a)\xi_a\tau_a^l, \tag{9}$$

the ambiguous sign being positive or negative according as γ is not or is divisible by λ. Using the relation obtained from (9) by substituting $(-a)$ for a throughout and employing $\sigma_a \equiv \sigma_{-a} \pmod{\lambda^{l-1}}$, we find that ξ_a/ξ_{-a} is primary, and hence, since the field is regular, it is the lth power of a unit in said field. Taking $a = 1, -1$, in (9) together with

$$\lambda^t(\sigma_1 + \sigma_{-1}) = \xi_0^1\tau_0^l,$$

and eliminating σ_1 and σ_{-1} from the three resulting equations we have

$$\tau_1^l + \frac{\xi_{-1}}{\xi_1}\tau_{-1}^l + \delta_1\tau_0^l = 0.$$

Using the fact that ξ_{-1}/ξ is an lth power we obtain

$$\theta_1^l + \omega_1^l + \delta_1\gamma_1^l = 0, \tag{10}$$

which is the same form as (7b), since θ_1, ω_1 and γ_1 each belong to $\Omega(\zeta + \zeta^{-1})$ and are prime to each other. We may now employ the same transformations on (10) as were used in connection with (7b) and we shall obtain the relation

$$\theta_2^l + \omega_2^l + \delta_2\gamma_2^l = 0.$$

Proceeding in this way we find that we get an infinite series of equations of this type with the successive γ's each containing less ideal prime factors than the preceding, which is impossible unless a certain γ is a unit in $k(\zeta)$. But this is easily shown to lead to a contradiction.

An extension of this method leads to the proof of the impossibility of (7b) where δ is replaced by given types of integers in $k(\zeta)$.

Determination of Some Properly Irregular Cyclotomic Fields.—The integer h which represents the number of classes of ideals in a cyclotomic field defined by $e^{2i\pi/l}$, where l is an odd prime, can be written in the form h_1h_2, where h_1 and h_2 are both integers.[10] If $h \equiv 0 \pmod{l}$ the field is called irregular. The necessary and sufficient condition that h_1 be divisible by l is that one of the first $(l-3)/2$ Bernoulli numbers be divisible by l. A necessary, but not a sufficient, condition that h_2 be divisible by l is that h_1 be divisible by l. A cyclotomic field in which h_1 is divisible by l, but h_2 is prime to l, is called a *properly irregular cyclotomic field.*

In a former paper I showed that this definition of a properly irregular cyclotomic field is equivalent to the statement[5] that none of the units E_n already defined, are lth powers of units in $k(\zeta)$. In another paper by Miss Elizabeth T. Stafford and myself[6] it was found that all the irregular fields, defined by primes $l < 211$, were also properly irregular.

In order to determine if a given cyclotomic field is properly irregular for an $l > 210$, it is first necessary to test the same as to regularity. As noted in another article,[7] this test was made by Miss E. M. Badger, for all primes l; $210 < l < 269$. All were found regular between these limits except 233, 257 and 263; for each l the only B's divisible by l in the set

$$B_1, B_2, \ldots, B_{(l-3)/2} \tag{11}$$

are as follows:

$$233, B_{42}; \quad 257, B_{82}; \quad 263, B_{50}$$

These tests were continued by Mr. M. M. Abernathy who examined the regularity of all primes l; $268 < l < 307$, this work being included in his M.A. thesis at the University of Texas. All were found regular within the limits just mentioned except 271, 283 and 293. The Bernoulli numbers were congruent to 0 (mod l) as follows:

$$271, B_{42}; \quad 283, B_{10}; \quad 293, B_{78}.$$

On page 145 of a former article[6] a method was described for testing the regularity of the prime $l = 127$. We depended primarily on the formula

$$\sum_{s=[l/6]+1}^{[l/4]} s^{2a-1} \equiv \frac{1 - 3^{l-2a} - 4^{l-2a} + 6^{l-2a}}{4a} (-1)^a B_a \pmod{l},$$

where $2a < (l-1)$ and [x] denotes the greatest integer in x. For a particular s the expressions s^{2a-1} were computed for the successive values starting with $a = 12$. The tests of Mr. Abernathy referred to above were the same as just indicated, except, in order to apply certain checks on the accuracy of the computations, the columns were included corresponding to all the integers $a = 1, 2, \ldots, \frac{l-1}{2}$. It was then easy to

show that the sum of the integers that were congruent to s^{2a-1} for a particular s, gives an integer divisible by l. Also, after the totals of all columns were made, the sum of these totals must be congruent to zero.[7a] For the cases 271 and 283 the corresponding Bernoulli numbers were found in Adams' *Tables*, and the numerators divided by the respective primes gave remainders of zero in each case.

Having determined that the primes 233, 257, 263, 271, 283 and 293 are all irregular, each one was tested as to being properly irregular, by considering the unit E_n and the possibility of its being the lth power of a unit in $k(\zeta)$ for the values of n corresponding to the subscripts of the Bernoulli numbers divisible by l in each case. The method used for the irregular primes < 211 is described on page 148 of another article.[6] The method employed for the primes now under discussion was the same, aside from the fact that these computations were carried out much more systematically and a number of new devices for shortening the calculations were used. If

$$E_i = \delta^l \tag{11a}$$

where δ is an integer in $k(\zeta)$ let p be the smallest rational prime, such that $p \equiv 1 \pmod{l}$. Then p decomposes in $k(\zeta)$ into the product of $(l-1)$ distinct ideal factors. Let d be an integer such that $d^l \equiv 1 \pmod{p}$. Then one of the ideal factors mentioned is $\mathfrak{P} = (\zeta - d, p)$, which gives $\zeta \equiv d \pmod{\mathfrak{P}}$. Consider the expression (11a) as a congruence (mod $\mathfrak{P}$); in view of the fact that $\zeta \equiv d \pmod{\mathfrak{P}}$ we obtain

$$E_n(d) \equiv c^l \pmod{p}$$

where c is a rational integer. Our problem is now reduced to determining if the index for $E_n(d)$ is divisible by l if we use a table of indices for the modulus p. In carrying this out, $E_n(d)$ was written in the following form

$$d^R \prod_{i=0}^{(l-3)/2} \left(\frac{d^{r^{i+1}} - 1}{d^{r^i} - 1}\right)^{r^{(l-1-2n)i}}$$

$$R = \frac{1-r}{2}\left(1 + r^h + r^{2h} + \ldots + r^{\frac{l-3}{2}h}\right)$$

$$h = l - 2n.$$

The exponent R in the first factor reduces immediately, modulo l, to

$$\frac{r-1}{r^{l-2n}-1}.$$

The computation of the index of d^R involves an obvious procedure, we now consider the determination of the index of the other factor, which

factor we shall call F. We shall describe the major part of the procedure in some detail as it is a bit elaborate. As an example take the case $l = 271$. Here $p = 1627$ and we take for the primitive root r of 271, the value 269 so that we may employ Jacobi's tables of indices for the prime 271. Also $n = 42$. A partial table of indices for the prime 1627 was then constructed by taking the primitive root 3 and finding the least positive residues of 3^k; $k = 1, 2, \ldots, 271$. A companion table giving the indices corresponding to all the least residues just mentioned, with blank spaces left for the indices of numbers not appearing in this set, was also made. Owing to the fact that only the indices reduced modulo l were required for the numbers involved in F, the partial tables just described readily yielded this information. For the prime being considered the integer d was taken as 3^6; the first ten rows and columns giving the computations in connection with our prime are exhibited below:

i	0	1	2	3	4	5	6	7	8	9
r^i	1	269	4	263	16	239	64	143	256	30
$6r^i$	6	1614	24	1578	96	1434	384	858	1536	180
$d^{r^i} - 1$	728	284	819	981	1479	1253	1507	826	1289	369
$\text{ind}(d^{r^i} - 1)$	39	78	167	154	146	13	138	26	193	118
$D(i)$	39	89	258	263	138	125	159	167	196	102
r^{186i}	1	166	185	87	79	106	252	98	8	244
$186i$	0	186	102	18	204	120	36	222	138	54
$K(i)$	39	140	34	117	62	242	231	106	213	227

Here

$$D(i) = \text{ind}\left[\frac{d^{r^{i+1}} - 1}{d^{r^i} - 1}\right]$$

$$K(i) = \text{ind}\left[\frac{d^{r^{i+1}} - 1}{d^{r^{i+1}} - 1}\right]^{r^{186i}}$$

The rows and columns are continued up to $i = 134$ inclusive. The elements of the second row are obtained from the tables of indices modulo 271. The third row is obtained immediately from the second and the multiplier 6 is used owing to the fact that $d = 3^6$. The elements of the fourth row are obtained from the partial table of indices modulo 1627, as well as those of the fifth row. The number in the sixth row are obtained by an obvious subtraction of certain elements in the preceding row. The elements in the eighth row are obtained by reducing $186i$ modulo 270, and from these numbers the data in the seventh row is obtained using a table of indices for the prime 271. The corresponding elements in the sixth and seventh rows are then multiplied together and reduced modulo 271 to give the numbers in the last row, which are then added together and this total is in turn added to the index for d^R to obtain the residue when the index of $E_n(d)$ is reduced modulo 271.

Checks were employed on the accuracy of the computations for each row excepting the fourth. Summing all the numbers in the first row and using the fact that they formed a geometric progression, the result should be congruent to

$$-\frac{2}{r-1} \pmod{271}.$$

Similarly we have obvious checks on the second, fifth, sixth and seventh rows. No check was employed on the fourth row but the accuracy of the numbers therein was involved in the check employed for the fifth row, which was more elaborate than the other checks referred to, and depends on the following transformations:

We have

$$(\zeta - 1)(\zeta^r - 1)(\zeta^{r^2} - 1) \ldots (\zeta^{r^{l-2}} - 1) = l$$

$$A = (\zeta - 1)(\zeta^r - 1)(\zeta^{r^2} - 1) \ldots (\zeta^{r^{\frac{l-3}{2}}} - 1), \tag{12}$$

then

$$AB = l,$$

where

$$B = (\zeta^{-1} - 1)(\zeta^{-r} - 1)(\zeta^{-r^2} - 1) \ldots (\zeta^{-r^{\frac{l-3}{2}}} - 1),$$

whence

$$B = (-1)^{\frac{l-1}{2}} \zeta^h A,$$

where $h = -1 - r \ldots - r^{\frac{l-3}{2}}$.

Now

$$h \equiv -\frac{r^{\frac{l-1}{2}} - 1}{r-1} \equiv \frac{2}{r-1} \pmod{l},$$

hence (12) gives

$$\zeta^{\frac{2}{r-1}} (-1)^{\frac{l-1}{2}} A^2 = l. \tag{13}$$

In A set d in place of ζ. Denote the result by $A(d)$. Then using $\zeta \equiv d \pmod{\mathfrak{P}}$ we have from (13), by taking indices

$$\left[\frac{2}{r-1}\right] \text{ind } d + \frac{l-1}{2} \cdot \frac{p-1}{2} + 2 \text{ ind } A(d) \equiv \text{ind } l \pmod{(p-1)}$$

where the symbol

$$\left[\frac{2}{r-1}\right]$$

denotes an integer i such that $i(r - 1) \equiv 2 \pmod{l}$, and this formula furnishes the check.

The table below gives the values of n, r, d, p and ? for each irregular prime l; $210 < l < 307$. The last column headed ind $E_n(d)$ gives the residue of this integer mod l in each case.

l	n	r	d	p	ρ	Ind $E_n(d)$
233	42	10	100	467	10	13
257	82	10	136	1543	10	123
263	50	10	729	1579	3	171
271	42	269	729	1627	3	4
283	10	273	729	1699	3	136
293	78	204	100	587	577	291

As the table shows, the computation established the fact that $E_n(d)$ is not divisible by l, and hence $E_n(\zeta)$ is not the lth power of a unit in the filed $k(\zeta)$ for any of the primes mentioned. It follows that the cyclotomic fields defined by each of these primes are properly irregular cyclotomic fields.

All the calculations of the type just mentioned were carried out by Mr. M. E. Tittle, Miss B. Bennett and Mr. M. M. Abernathy, with the aid of funds provided by the University of Texas. In particular, Mr. Tittle discovered some of the devices employed for shortening the computations.

Application of Properly Irregular Cyclotomic Fields to Fermat's Last Theorem.—In T I proved a number of theorems concerning Fermat's last theorem. In the present paper I shall consider the application to special exponents in the Fermat relation of the following theorems included in T (numbered as in T).

THEOREM I. *Under the following assumptions:*

(1) *the second factor of the class number of the field $k(\zeta)$ is prime to l;*

(2) *none of the Bernoulli numbers B_n, $n = 1, 2, \ldots, (l - 3)/2$, is divisible by l^3;*

the equation (7a) *is impossible in case II.*

THEOREM III. *If $l \equiv 1 \pmod 4$ and all the numbers in* (11) *which are divisible by l have even subscripts, then* (7a) *is impossible in rational integers none zero, provided*[8] *also that the second factor of the class number of $k(\zeta)$ is prime to l.*

THEOREM IV. *Under the following assumption:*

None of the units E_a, $a = a_1, a_2, \ldots, a_s$, is congruent to the lth power of an integer in the field $k(\zeta)$ mod $\mathfrak{P}$, where $\mathfrak{P}$ is a prime ideal divisor of p, p is a prime $< (l^2 - l)$ of the form 1 mod l, and $a_1, a_2, \ldots, a_s$ are the subscripts in the Bernoulli numbers in the set (11) *which are divisible by l;*

the relation (7a) *is impossible in case II.*

THEOREM V. *Under the following assumptions:*

(1) *there exists a rational prime integer p such that the congruence*

$$u^l + v^l + w^l \equiv 0 \pmod{p}$$

has no solution u, v and w all rational integers prime to p, and $p \not\equiv 1 \pmod{l^2}$;

(2) *the relation*

$$\left\{\frac{E_a}{\mathfrak{P}}\right\} \not\equiv 1$$

holds, where a ranges over the values $a_1, a_2, \ldots, a_s$, these integers being the subscripts of Bernoulli numbers in the set (11) *which are divisible by l, and $\mathfrak{P}$ is a prime ideal divisor of p;*

the equation (7a) *is impossible in rational integers none zero.*

In Theorem V the symbol

$$\left\{\frac{E_n}{\mathfrak{P}}\right\}$$

denotes the lth power-character of E_n with respect to the ideal $\mathfrak{P}$.

The proofs of the above-mentioned theorems were more or less different. In particular, if we substitute the argument given at the beginning of the present paper in lieu of the argument given on pages 632–635 for the proof that $\omega + \theta \equiv 0 \pmod{p}$, the proof of Theorem IV is largely different from that of Theorem V if we retain the original argument as to $\omega + \theta \equiv 0 \pmod{p}$ as part of the proof of Theorem V, as is necessary, since in the latter case we cannot assume $p = 1 + cl$ with $c < (l - 1)$.

In T, the first three theorems quoted above were applied to the particular values of $l < 211$, which were irregular. Here I shall consider the application of these three theorems to (7a) for $210 < l < 307$, and irregular; and the application of Theorem V to all irregular values of $l < 307$.

Concerning Theorem I the first assumption holds for all irregular primes l, $210 < l < 307$, since we have shown that all the cyclotomic fields defined by these l's are properly irregular. As to the second assumption in Theorem I, this was shown to hold for the cases $l = 233, 257$ and 263, as stated in N, page 303. This assumption was examined by Mr. M. M. Abernathy for the case $l = 271$, who found

$$A_{42} \equiv 271 \cdot 181 \pmod{271^2},$$

where

$$A_n = \frac{(-1)^n B_{nl}(2^{2nl} - 1)}{2^{2nl}\, nl}.$$

The case $l = 283$ was disposed of by Mr. J. A. Clack, who found,

$$A_{10} \equiv 283 \cdot 71 (\text{mod } 283^2) .$$

Hence Theorem I proves the last theorem for all irregular l's, $210 < l < 307$, excepting 293, for which latter prime it was not tested.

The first two assumptions mentioned in Theorem III are satisfied only for $l = 233$, 257 and 293, within the range mentioned. The third assumption mentioned holds as already shown. Hence Theorem III proves the last theorem for $l = 233$, 257 and 293.

As to the application of Theorem IV, the results of the computations in establishing the fact that the irregular cyclotomic fields defined by the irregular primes l, $210 < l < 307$ are properly irregular, incidentally show that the assumptions in Theorem IV holds for all these primes, since the value of p selected was $< (l^2 - l)$ for each l. Hence Theorem IV proves the last theorem for all irregular l's such that $210 < l < 307$.

The application of Theorem V to special exponents has not been mentioned in any of my preceding papers. The first assumption in it states that there exists a rational prime integer p such that the congruence

$$u^l + v^l + w^l \equiv 0 (\text{mod } p) \qquad (14)$$

has no solution u, v and w all rational integers prime to p, and $p \not\equiv 1 (\text{mod } l^2)$. The congruence mentioned has obvious solutions when $p \equiv 1 (\text{mod } 3)$. Using the results of Dickson,[9] we note that the congruence (14) is impossible for $l = 37$, $p = 149$, hence the first assumption of Theorem V holds for $l = 37$, the second assumption holds, since 149 is the value of p used in verifying that

$$\left\{\frac{E_{16}}{\mathfrak{P}}\right\} \not\equiv 1$$

where $l = 37$. In a similar way our computations concerning the properly irregular cyclotomic fields mentioned in T, page 641–642, and in the present paper, together with Dickson's results concerning the trinomial congruence, proved the last theorem, for

$$l = 37, 67, 101, 131, 149, 157, 233 \text{ and } 293.$$

For the irregular primes < 307 not included in the list just mentioned, the values of p which were used in our irregular field computations are in each case of the form $6l + 1$; consequently the congruence (14) has solutions. Hence, in order to test Theorem V for the exceptional values of l such as 59, 103, etc., it would be necessary to select a value of p such that $p \not\equiv 1 (\text{mod } 3)$ and not included in Dickson's exceptions. We have not carried out such computations and the questions as to whether Theorem

V yields proofs of the last theorem for all irregular primes < 307 remains open.

In T, page 614 and elsewhere,[10] the writer has referred to Kummer's results on Fermat's last theorem for irregular prime exponents. The first assumption of the theorem states that the first factor of the class number of $k(\zeta)$ is divisible by l but not by l^2. Hence, under this restriction Kummer's results may be applied to special exponents in the Fermat relation, since his assumptions II and III are equivalent to those of Theorem I of T. However, owing to assumption I, Kummer's argument, as corrected by the writer,[11] is far simpler than the proof given of Theorem I in T; the proof of the latter requiring lemma I of T which involves in its proof Furtwängler's law of reciprocity. Also the proof of the lemma depending upon the results of Takagi involves the existence of a class-field. Kummer's proof depends on considerations much simpler than those involved in the proof of the existence of a class-field or of the law of reciprocity. Also, in other respects Kummer's argument is different from that I have given on pages 621–624 of T. Hence we may regard his work as furnishing more or less different proofs of the last theorem for all irregular l's < 307, excepting 157, in which case the first factor of the class number of $k(\zeta)$ is divisible by 157^2.

To summarize, we shall now list the irregular primes < 307, together with the number of different proofs, which have been mentioned in this paper, in each case:

37,5; 59,3; 67,3; 101,5; 103,3; 131,4; 149,4; 157,3; 233,5; 257,4; 263,3; 271,3; 283,3; 293,4.

Using also the fact that Fermat's last theorem is true for regular prime exponents, we may then state that the last theorem has been proved for all exponents < 307.

[1] *Trans. Am. Math. Soc.*, **31**, 613–642 (1929). This paper will be referred to as T.

[2] These PROCEEDINGS, **16**, 298–305 (1930). This paper will be referred to as N.

[3] Landau, *Vorlesungen über Zahlentheorie*, **3**, 240.

[4] Kummer, *Crelle*, **40**, 130–138 (1850); Landau, loc. cit., 271–274.

[4a] *Trans. Am. Math. Soc.*, **31**, 633 (1929).

[5] These PROCEEDINGS, **16**, 743–749 (1930).

[6] *Ibid.*, **16**, 139–150 (1930).

[7] *Ibid.*, **16**, 303 (1930).

[7a] Miss Stafford's previous computations concerning the regularity of the primes l such that $157 < l < 211$, were checked by Mr. Abernathy by the methods just described concerning the sums of the rows and columns, and Miss Stafford's conclusion that all such primes are regular, was confirmed.

[8] Cf. errata to Vol. **33** of the *Trans. Am. Math. Soc.*

[9] *Messenger of Math.*, [2], **38**, 14–32 (1908).

[10] *Bull. Nat. Res. Coun.*, **62**, Feb., 1928, 34, 44.

[11] *Bull. Am. Math. Soc.*, **28**, 400–407 (1922); these PROCEEDINGS, **12**, 767–772 (1926).