ON FERMAT'S LAST THEOREM[*]

BY

H. S. VANDIVER

In two recent papers[†] the writer stated without proof four theorems concerning Fermat's last theorem. These results were employed to prove the theorem for all exponents greater than 2 and less than 211. In the present paper the proofs of Theorems I to IV of my previous papers will be given, as well as one of an additional Theorem V.

I shall first indicate the relation of the present results to the previous work done on the problem. In the year 1850 Kummer[‡] proved that the equation

$$\alpha^l + \beta^l + \gamma^l = 0 \tag{1}$$

is impossible if α, β and γ are integers in the field $k(\zeta)$ prime to each other; $\zeta = e^{2i\pi/l}$ and l is an odd prime greater than 3 such that $B_1, B_2, \cdots, B_{(l-3)/2}$ have numerators which are prime to l, where $B_1 = 1/6$, $B_2 = 1/30$, etc. are the Bernoulli numbers.

As shown by Kummer[§] the above condition concerning the Bernoulli numbers is equivalent to the statement that the class number of the field $k(\zeta)$ is prime to l. Primes l which have this property are called regular. In particular he showed that the second factor[¶] of the class number is divisible by l only if the first factor of the class number is divisible by l. This is not a sufficient condition, however, for the divisibility of the second factor by l. He computed[||] the first factor of the class number for all primes $l < 164$. He found that l is regular for all these primes excepting $l = 37$, 59, 67, 101, 103, 131, 149, and 157.

For $l = 157$, the first factor of the class number is divisible by 157^2 and not by 157^3, but in the other cases by the first power of l only. For $l = 101$,

[*] Presented to the Society, December 27, 1928; received by the editors in April, 1929.

[†] Proceedings of the National Academy of Sciences, vol. 15 (1929), pp. 48; 109–110.

[‡] Crelle's Journal, vol. 40 (1850), pp. 130–138. Proof extended by Hilbert, *Algebraische Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, 1894, pp. 517–523.

[§] Crelle's Journal, vol. 40 (1850), pp. 117–129; Journal de Mathématiques, (1), vol. 16 (1851), pp. 473–486; abstract in Berlin Monatsberichte, 1847, pp. 305–319. Also Vandiver, Bulletin of the American Mathematical Society, vol. 25 (1918–19), pp. 458–461. For a full history of the problem as far as it is connected with algebraic numbers, cf. Bulletin of the National Research Council, No. 62, February, 1928.

[¶] Crelle's Journal, vol. 40 (1850), pp. 93–116; Hilbert, Bericht, p. 377.

[||] Crelle's Journal, vol. 40 (1850), p. 117; Journal de Mathématiques, (1), vol. 16 (1851), p. 473. Berlin Monatsberichte, 1847, p. 319. Berlin Monatsberichte, 1874, pp. 239–248.

the 34th Bernoulli number is divisible by l; for $l=103$, the 12th Bernoulli number; for $l=131$, the 11th Bernoulli number; for $l=149$, the 65th Bernoulli number; for $l=157$, the 31st and 55th Bernoulli numbers.

In the year 1857 Kummer attempted to prove that

$$x^l + y^l + z^l = 0 \tag{2}$$

is impossible for rational integers x, y and z under the following three assumptions:

Assumption I. The first factor of the class number of $k(\zeta)$ is divisible by l but not by l^2.

Assumption II. If $B_n \equiv 0 \pmod{l}$, $n<(l-1)/2$, there exists an ideal in $k(\zeta)$ with respect to which as a modulus the unit

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

is not congruent to the lth power of an integer in $k(\zeta)$. Here

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

and $\epsilon(\zeta^{r^i})$ indicates the unit obtained from ϵ by the substitution (ζ/ζ^{r^i}); also r is a primitive root of l.

Assumption III. The Bernoulli number B_{nl} is not divisible by l^3.

He then applied these criteria to the exponents $l=37$, 59, and 67, the only l's less than 100 which are not regular. From the remarks made above concerning the computations of the first factors of the class numbers it follows that Assumption I is satisfied, and carrying out extensive computations Kummer concluded that Assumptions II and III were satisfied also for the three values of l mentioned above. He gave, however, only the results of the latter computations and in connection with Assumption III did not give the formula that he used on which his calculations were based.

If in (2) x, y and z be prime to l this is called the first case of Fermat's last theorem; if x, y and z are prime to each other and $xyz \equiv 0 \pmod{l}$ then this is called case II of the theorem. *Before the appearance of the papers of Kummer and between their appearance and the present time many contributions have been made to the first case of the theorem*; *in particular*[*] *the theorem has been*

[*] Dickson, Messenger of Mathematics, (2), vol. 38 (1908), pp. 14–32; Quarterly Journal of Mathematics, vol. 40 (1908), pp. 27–45; Beeger, Messenger of Mathematics, vol. 55 (1925), pp. 17–26.

proved for all exponents $2<l<14{,}000$ *in case* I. *The situation in connection with the second case is quite different, however. With the exception of the two articles by the writer cited above and another of Bernstein's*[*] *no paper has been published since the year* 1857 *which gives any new criteria for the solution of* (2) *in case* II *which are independent of x, y and z and expressible in terms of rational integers.*

In the year 1920 the writer[†] pointed out that the proofs of the results given in Kummer's 1857 Memoir on Fermat's last theorem are inaccurate and incomplete in several respects.

He later[‡] completed Kummer's proofs by modifications and extensions of the latter's arguments.

As noted above the prime $l=157$ is irregular and the first factor of the class number $k(\zeta)$ for this case is divisible by l^2. Hence the methods of Kummer's 1857 paper do not apply to this exponent since the first assumption states that the first factor of the class number $k(\zeta)$ is not divisible by l^2. *The present paper is the result, in part, of efforts to obtain criteria for the second case of Fermat's last theorem which would yield a proof of the theorem for the case* $l=157$ *at least, and hence to effect an advance over Kummer's work. Theorems* I *and* IV *as proved in the present paper each yield a proof for this exponent as well as the proofs for all other irregular primes l as exponents which are less than* 211.

Concerning the computations which prove Fermat's last theorem in the second case .for all exponents greater than 2 and less than 211, all primes less than this limit were tested as to being irregular. For a particular l, this was accomplished by testing each of the Bernoulli numbers $B_1, B_2, \cdots, B_{(l-3)/2}$ as to the divisibility of their numerators by l. By a systematic method, for primes l less than 100 the necessary computations were made by Mrs. A. C. S. Williams; for the primes l between 100 and 200 they were made by Professor Elizabeth T. Stafford. The results showed that the only irregular primes in this range were those that had been discovered by Kummer, who

[*] Bernstein, Göttinger Nachrichten, Mathematisch-Physikalische Klasse, 1910, pp. 507–516. It was pointed out by the writer, however (Proceedings of the National Academy of Sciences, vol. 6 (1920), pp. 416–421), that Bernstein's first theorem constitutes no advance over the results of Kummer's paper of the year 1850 on Fermat's last theorem, and it was shown by Pollaczek (Mathematische Zeitschrift, vol. 21, pp. 36–38) that in order for Bernstein's second theorem to yield a proof of Fermat's last theorem for a particular exponent l a number of conditions concerning the field $k(\zeta)$ must be satisfied. In particular, his theorem yields no proof for any of the three cases $l=37$, 59 and 67.

[†] Proceedings of the National Academy of Sciences, vol. 6 (1920), pp. 266–269.

[‡] Bulletin of the American Mathematical Society, vol. 28 (1922), pp. 400–407; Proceedings of the National Academy of Sciences, vol. 12 (1926), pp. 767–772.

carried his computations up to and including $l=163$. These computations concerning the Bernoulli numbers obviously do not give as much information as Kummer obtained, as he, in his work, computed the actual values of the first factor of the class number of each l. However, I regard the former computations as a sufficient check on Kummer's results.

The computations in connection with the irregular primes in testing the criteria of Theorems I to IV of this paper were carried out by Professor E. T. Stafford, Mrs. A. C. S. Williams, Mr. S. S. Wilks, and the writer.

In none of the criteria found by Kummer for the second case of Fermat's last theorem was any use made of the fact that x, y and z in (2) are rational integers. The criteria apply also if x, y and z are integers in the field defined by $(\zeta+\zeta^{-1})$, prime to each other. In Theorem V of the present article I give for the first time criteria for the second case of the theorem which are obtained by use of the fact that x, y and z are rational.

1. We first consider

Lemma 1. *If the ideal (ω) in $k(\zeta)$ is the lth power of an ideal in that field and ω is a primary number, then (ω) is the lth power of a principal ideal in the field provided that the second factor of the class number of $k(\zeta)$ is prime to l.*

This was proved in full in another paper by the writer.* It is also noted that this lemma may also be proved using a result of Takagi.† This follows since Takagi shows that if the second factor of the class number of $k(\zeta)$ is prime to l then any singular primary number in the field may be expressed in the form $\eta\theta^l$ where η is a unit and θ a number in $k(\zeta)$. This statement is equivalent to the one in the lemma since a singular primary number ω is defined to be such that (ω) is the lth power of an ideal which is not a principal ideal, ω being a number in $k(\zeta)$.

We now proceed to

Lemma 2. *If a unit η exists in $k(\zeta)$ which is of the form*

$$\eta \equiv c^l \pmod{\lambda^{2l}}$$

where c is a rational integer, then η is the lth power of a unit in $k(\zeta)$ except possibly when

$$B_{nl} \equiv 0 \pmod{l^3}$$

for n some integer in the set $1, 2, \cdots, (l-3)/2; \lambda=(1-\zeta)$.

To prove this we set

* Proceedings of the National Academy of Sciences, 1929. Note that the relation just above (7) gives $\omega\omega_{-1}^{l-1}=\theta^l$ which with $\omega\omega_{-1}=\gamma_1\sigma_1{}^l$ yields $\omega=\gamma\sigma^l$, where γ and γ_1 are units.

† Crelle's Journal, vol. 157 (1927), p. 236. Cf. also Bernstein, Göttinger Nachrichten, loc. cit., p. 514.

$$\eta^t = E_1^{a_1} E_2^{a_2} \cdots E_{(l-3)/2}^{a_{(l-3)/2}} \tag{3}$$

the a's and t being rational integers Since the E's form an independent system in $k(\zeta)$ this is always possible. Further we may assume that l is not a common factor of all the integers $t, a_1, a_2, \cdots, a_{l_1}, l_1=(l-3)/2$. For if it is, and $t=l^h t_1$, $a_1=l^h a_1^1, \cdots, a_{l_1}=l^h a_{l_1}^1$ with l prime to at least one of the integers $t_1, a_1^1, a_2^1, \cdots, a_{l_1}^1$, then (3) holds with t_1 in lieu of t, a_1^1 in lieu of a_1, etc., since all the E's are real.

We may, by the hypothesis in the theorem, set

$$\eta = c^l + \lambda^{2l}\alpha_1 = c^l + l^2\alpha, \tag{3a}$$

where α_1 and α are integers in $k(\zeta)$. We may write

$$\alpha = m_0 + m_1\zeta + \cdots + m_{l-2}\zeta^{l-2},$$

with the m's rational integers. If w is an arbitrary variable, set

$$\alpha(w) = m_0 + m_1 w + \cdots + m_{l-2}w^{l-2}.$$

Now ϵ may be put in the form

$$\zeta^{(1-r)/2}\frac{\zeta^r - 1}{\zeta - 1}.$$

Set $r' \equiv (1-r)/2 \pmod{l}$, with r' a positive rational integer. Put

$$\epsilon(w) = w^{r'}\frac{w^r - 1}{w - 1}$$

and

$$E_i(w) = \prod_{j=1}^{l_1} \epsilon(w^{r^j})^{r^{-2ij}};$$

$\epsilon(w)$ is obviously a polynomial in w with rational integral coefficients. Set

$$\rho = r^{l^2};$$

then $(E_i(w))^\rho$ is also a polynomial in w with rational integral coefficients, since it may be written as

$$\prod_{j=0}^{l_1} \epsilon(w^{r^j})^{\rho r^{-2ij}}$$

and ρr^{-2ij} is a positive integer because $l^2 > 2ij$. Now consider the expression

$$A = \prod_{i=1}^{l_1} E_i^{a_i\rho(l-1)}(w) - (c^l + l^2\alpha(w))^{\rho(l-1)t}.$$

It is a polynomial in w with rational integral coefficients, and vanishes for $w=\zeta$ by (3) and (3a).

Since

$$\frac{w^l - 1}{w - 1}$$

is irreducible in the rational field it therefore follows that

$$A = X\frac{w^l - 1}{w - 1},$$

where X is a polynomial in w with rational integral coefficients. Further if A is divided by w^l-1 we obtain a remainder which is of degree $<l$ and divisible by

$$\frac{w^l - 1}{w - 1}.$$

Hence this remainder is of the form

$$\frac{b(w^l - 1)}{w - 1}$$

where b is a rational integer. We therefore write

$$\text{(3b)} \qquad \sum_{i=1}^{l_1} E_i^{a_i\rho(l-1)}(w) = (c^l + l^2\alpha(w))^{\rho t(l-1)} + V(w^l - 1) + b\frac{w^l - 1}{w - 1},$$

where V is a polynomial in w with rational integral coefficients. Put $w=1$ in the above; we have

$$\text{(3c)} \qquad \sum_{i=1}^{l} r^{(l-1)a_i\rho(1+r^{-2i}+\cdots+r^{-(l-3)i})} = c^{l\rho(l-1)t} + bl.$$

Since

$$1 + r^{-2i} + \cdots + r^{-(l-3)i} = \frac{r^{-i(l-1)} - 1}{r^{-2i} - 1},$$

then

$$\rho\frac{r^{-i(l-1)} - 1}{r^{-2i} - 1}$$

is an integer divisible by l, and since

$$c^{l(l-1)} \equiv r^{l(l-1)} \equiv 1 \pmod{l^2},$$

the relation (3c) gives

$$bl \equiv 0 \pmod{l^2}; \qquad b \equiv 0 \pmod{l}.$$

Set $b=b_1l$ and $w=e^v$; then (3b) gives

$$\text{(3d)}\qquad \prod_{i=1}^{l_1} E_i^{a_i\rho(l-1)}(e^v) = (c^l + l^2\alpha(e^v))^{\rho(l-1)t} + V(e^{vl} - 1) + b_1 l\,\frac{e^{vl}-1}{e^v-1}\,.$$

To proceed further with this relation we first derive some properties of the E's. We have

$$\frac{d}{dv}\log\frac{e^{rv}-1}{e^v-1} = \frac{r-1}{2} + (r^2-1)\frac{B_1}{2!}v - (r^4-1)\frac{B_2}{4!}v^3 + \cdots,$$

$$B_1 = 1/6,\ B_2 = 1/30,\ \cdots;\ |v| < \frac{2\pi}{r},$$

whence

$$\left[\frac{d^{2i}\log\dfrac{e^{rv}-1}{e^v-1}}{dv^{2i}}\right]_{v=0} = (-1)^{i+1}\frac{B_i}{2i}(r^{2i}-1).$$

We shall now show that

$$\text{(3e)}\qquad \left[\frac{d^k\log F(e^{rv})}{dv^k}\right]_{v=0} = r^k\left[\frac{d^k\log F(e^v)}{dv^k}\right]_{v=0}$$

where $F(e^v)$ is a polynomial in e^v. Set

$$\frac{d^{k-1}\log F(e^v)}{dv^{k-1}} = \frac{A(e^v)}{B(e^v)}$$

where $A(e^v)$ and $B(e^v)$ are polynomials in e^v. Assume that

$$\frac{d^{k-1}\log F(e^{rv})}{dv^{k-1}} = r^{k-1}\frac{A(e^{rv})}{B(e^{rv})}\,.$$

This is true for $k=2$. We shall then show that this then holds for k in lieu of $k-1$. Differentiate each member of this equation and we obtain

$$\frac{d^k\log F(e^{rv})}{dv^k} = \frac{r^k}{B(e^{rv})}\,\frac{dA(e^{rv})}{dv} - \frac{r^kA(e^{rv})}{B^2(e^{rv})}\,\frac{dB(e^{rv})}{dv} = r^kG(e^{rv})$$

and in the same way

$$\frac{d^k\log F(e^v)}{dv^k} = G(e^v).$$

Putting $v=0$ in these relations we obtain (3e) which gives the relation desired. Applying this to the E's,

$$\text{(4)}\qquad \left[\frac{d^{2i}\log E_n(e^v)}{dv^{2i}}\right]_{v=0}$$

$$= (1 + r^{2i-2n} + r^{4i-4n} + \cdots r^{2i(l-3)/2-2n(l-3)/2})\frac{(-1)^{i+1}B_i}{2i}(r^{2i} - 1).$$

Hence if $i \neq n$,

$$\left[\frac{d^{2i}\log E_n(e^v)}{dv^{2i}}\right]_{v=0} = \frac{r^{(l-1)(i-n)}-1}{r^{2i-2n}-1}(-1)^{i+n}\frac{B_i}{2i}(r^{2i}-1), \tag{4a}$$

and if $i=n$,

$$\left[\frac{d^{2n}\log E_n(e^v)}{dv^{2n}}\right]_{v=0} = \frac{(-1)^{n+1}B_n(l-1)(r^{2n}-1)}{4n}. \tag{5}$$

So far in this paper we have put no limitation on r except that it be a primitive root of l; we may then further assume that $r^{l-1}\equiv 1 \pmod{l^2}$. In (3d) take logarithms of both members, differentiate $2kl$ times, $k=1, 2, \cdots, l_1$, with respect to v, set $v=0$ and reduce the result modulo l^2. In the left hand member we employ (4) and (4a) modulo l^2 and using $r^{l-1}\equiv 1 \pmod{l^2}$ we obtain, modulo l^2,

$$a_k r^{l^2}\frac{(l-1)^2}{2}\quad\frac{(-1)^{kl+1}B_{kl}}{2kl}(r^{2kl}-1).$$

As to the right hand member, denote it by Z; then

$$\frac{d^{kl}\log Z}{dv} = \frac{d^{kl-1}}{dv}\left(\frac{1}{Z}\frac{dZ}{dv}\right) = D_{kl-1}(Z^{-1}D(Z)),$$

say. With the latter notation we have

$$D_{kl-1}(Z^{-1}D(Z)) = Z^{-1}D_{kl}(Z) + (kl-1)D_{kl-1}(Z)D(Z^{-1}) \\ + \cdots + D(Z)D_{kl-1}(Z^{-1}).$$

When we substitute $v=0$ in this relation we obtain on the right hand side the sum of a number of fractions each of whose denominators is of the form 1 (mod l^2) and whose numerators are each divisible by l^2 except possibly the term $[Z^{-1}D_{kl}(z)]_{v=0}$. It may be shown that this term is divisible by l^2, however, since

$$D_{kl}\left[(e^{vl}-1)V + b_1 l\frac{e^{vl}-1}{e^v-1}\right]_{v=0} \\ \equiv [(e^{vl}-1)D_{kl}(V) + klD_{kl-1}(V)D(e^{vl}-1)]_{v=0} \equiv 0 \pmod{l^2},$$

observing that

$$D_i\left(\frac{e^{vl}-1}{e^v-1}\right) \equiv 0 \pmod{l}\ ;\quad i \not\equiv 0 \pmod{(l-1)},$$

and

$$[D_s(e^{vl}-1)]_{v=0} \equiv 0 \pmod{l^2}\ ;\quad s > 1.$$

Hence $[D_{kl}(Z)]_{v=0}$ is divisible by l^2 and therefore

$$a_k B_{kl} \equiv 0 \pmod{l^3},$$

and using the hypothesis of the lemma we have

$$a_k \equiv 0 \pmod{l},$$

hence by our assumption at the beginning of the proof, $t \not\equiv 0 \pmod{l}$, giving from (3)

$$\eta^t = \delta^l$$

where δ is a unit in $k(\zeta)$. Raise each side to the power t_1, with t_1 a rational integer such that $tt_1 \equiv 1 \pmod{l}$; we have $\eta = \delta_1{}^l$, which proves Lemma 2.

2. We now enunciate

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_{nl}, $n=1, 2, \cdots, (l-3)/2$, *is divisible by* l^3;

the equation (2) *is impossible in case* II.

The proof is, in the main, an extension of Kummer's argument employed in his 1857 memoir already cited here.

We consider the equation

$$\omega^l + \theta^l = \eta\kappa^{ml}\xi^l, \tag{6}$$

where ω, θ and ξ are integers in the field defined by $\zeta+\zeta^{-1}$ and are also prime to each other in that field; η is a unit in this field and

$$\kappa = (1-\zeta)(1-\zeta^{-1}).$$

Also the rational integer m is greater than 1. We shall show this equation to be impossible under the assumptions mentioned; it follows easily that (2) is impossible in case II under the same assumptions.

Evidently

$$\prod_{a=0}^{l-1}(\omega + \zeta^a\theta) = \eta\kappa^{ml}\xi^l. \tag{7}$$

We note that from

$$\omega + \zeta^a\theta + (\zeta^r - \zeta^a)\theta = \omega + \zeta^r\theta$$

it is possible to infer that each one of the factors of (7) is divisible by $(1-\zeta)$ but the right hand member of (7) is divisible by a higher power of $\lambda=(1-\zeta)$ than l. Hence one of the factors on the left hand side is divisible by λ^2.

Since $\omega+\theta$ is real it is divisible by κ and since, if $a \not\equiv 0 \pmod{l}$,

$$\omega + \zeta^a\theta = \omega + \theta + (\zeta^a - 1)\theta,$$

we have that the expression on the left is divisible by λ but not by λ^2. Also $\omega+\zeta^a\theta$ and $\omega+\zeta^b\theta$ have no factor in common aside from λ since their difference is $(\zeta^a-\zeta^b)\theta$ and θ is prime to ω, hence

$$\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right) = \mathfrak{j}_a{}^l \qquad (a = 1,2,\cdots,l-1),$$

$$(\omega+\theta) = (\kappa)^{ml-(l-1)/2}\mathfrak{j}_0{}^l.$$

By Lemma I,

$$\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right)\left(\frac{\omega+\zeta^{-a}\theta}{1-\zeta^{-a}}\right)^{l-1} = (\rho_a')^l, \tag{7a}$$

where $\rho_a{}'$ is an integer in $k(\zeta)$.* But we also have

$$\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right)\left(\frac{\omega+\zeta^{-a}\theta}{1-\zeta^{-a}}\right) = (\mathfrak{j}_a\mathfrak{j}_{-a})^l, \tag{7b}$$

and since $\mathfrak{j}_a\mathfrak{j}_{-a}$ belongs to the field $k(\zeta+\zeta^{-1})$ we have, if h is the class number of $k(\zeta+\zeta^{-1})$,

$$(\mathfrak{j}_a\mathfrak{j}_{-a})^h \sim 1, \tag{7c}$$

with h prime to l; hence if $hh_1 = 1+sl$, s and h_1 rational integers, then

$$(\mathfrak{j}_a\mathfrak{j}_{-a})^{hh_1} \sim (\mathfrak{j}_a\mathfrak{j}_{-a})(\mathfrak{j}_a\mathfrak{j}_{-a})^{sl},$$

which with (7b) and (7c) gives

$$\mathfrak{j}_a\mathfrak{j}_{-a} \sim 1\ ;$$

hence by (7b),

$$\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right)\left(\frac{\omega+\zeta^{-a}\theta}{1-\zeta^{-a}}\right) = (\rho_a'')^l\beta, \tag{7d}$$

where β is a unit and ρ'' an integer in $k(\zeta+\zeta^{-1})$. Multiplying this by (7a) we have

$$\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right)^2\left(\frac{\omega+\theta^{-a}\theta}{1-\zeta^{-a}}\right)^l = \beta(\rho_a''\rho_a')^l$$

and

$$\frac{\omega+\zeta^a\theta}{1-\zeta^a} = \eta_a\rho_a{}^l \qquad (a = 1,2,\cdots,l-1), \tag{8}$$

where η_a is a real unit in $k(\zeta)$, ρ_a an integer in that field. Also since the second factor of the class number of $k(\zeta)$ is prime to l we have

$$\omega+\theta = \eta_0\kappa^{ml-(l-1)/2}\rho_0{}^l, \tag{8a}$$

* Here ρ is not used in the same sense as on p. 617.

where ρ_0 is an integer in $k(\zeta+\zeta^{-1})$. If we write ρ_{-a} for the integer in the field $k(\zeta)$ which is obtained from ζ_a by means of the substitution (ζ/ζ^{-1}), we have from the relation (8) for a and $-a$, and (8a), three relations from which we may eliminate ω and θ and obtain, if η' is a unit in k (ζ),

$$\rho_a{}^l - \rho_{-a}{}^l = \eta_a'(1-\zeta)^{(2m-1)l}\rho_0{}^l.$$

Decomposing the left hand member into linear factors we note from the above that we have, if $\mathfrak{a}$ is an ideal in k (ζ)

$$\text{(9)} \qquad \frac{\rho - \zeta^i\rho_{-a}}{1-\zeta^i} = \mathfrak{a}_i{}^l \qquad (i = 1,2, \cdots, l-1)\,;$$

$$\text{(9a)} \qquad \rho_a - \rho_{-a} \equiv 0 \qquad (\text{mod } (1-\zeta)^{(2m-2)l+1}).$$

The left hand member of (9) is unaltered by the substitution (ζ/ζ^{-1}) and since the second factor of the class number of $k(\zeta)$ is prime to l we have in the same way that (7d) was obtained

$$\frac{\rho_a - \zeta^i\rho_{-a}}{1-\zeta^i} = \eta_i''\mu_i{}^l \qquad (i = 1,2, \cdots, l-1),$$

where η_i'' is a unit and μ_i is an integer in $k(\zeta+\zeta^{-1})$. This relation with (9a) gives

$$\rho_a \equiv \eta_i''\mu_i{}^l \qquad (\text{mod } \lambda^{(2m-2)l}).$$

Since $m>1$, then $(2m-2)l \geqq 2l$. Using the relation (8) with the last relation given, we obtain

$$\frac{\omega+\zeta^a\theta}{1-\zeta^a} \equiv \eta_a(\eta_i'')^l\mu^{l^2} \qquad (\text{mod } \lambda^{(2m-2)l}).$$

We have a similar relation with b in place of a and division of these two relations gives

$$\text{(10)} \qquad \frac{\eta_a(\eta_i'')^l}{\eta_b(\eta_i{}^{(3)})^l} \equiv c^{l^2} \qquad (\text{mod } \lambda^{2l}),$$

where c is a rational integer with η_b and $\eta_i{}^{(3)}$ units in $k(\zeta)$. By Lemma 2 it follows that the unit on the left hand side is the lth power of a unit in $k(\zeta)$. We may now write, if $\rho_a^* = (\eta_i'')^{-l}\rho_a$,

$$\frac{\omega+\zeta^a\theta}{1-\zeta^a} = \eta_a(\eta_i'')^l\rho_a{}^{*l}\,;$$

from the product of this expression and that obtained after making the substitution (ζ/ζ^{-1}) we have

$$\omega^2 + (\zeta^a + \zeta^{-a})\omega\theta + \theta^2 = \eta_a{}^*(2 - \zeta^a - \zeta^{-a})\omega^{*l},$$

$$\eta_a{}^* = (\eta_a(\eta_i'')^l)^2$$

and ω^* is an integer in $k(\zeta+\zeta^{-1})$. We have a similar equation for b in place of a and also from (8a)

$$\omega^2 + 2\omega\theta + \theta^2 = \eta_0^2\kappa^{2ml-l+1}\rho_0{}^{2l}.$$

Elimination of the quantities $\omega^2+\theta^2$ and $\omega\theta$ from these three equations gives, if $a \not\equiv \pm b \pmod{l}$,

$$\text{(10a)} \qquad \eta_a{}^*\omega^{*l} - \eta_b{}^*\theta^{*l} = \frac{\eta_0^2\kappa^{2ml-l+1}(\zeta^a + \zeta^{-a} - \zeta^b - \zeta^{-b})\rho_0^{2l}}{(2 - \zeta^a - \zeta^{-a})(2 - \zeta^b - \zeta^{-b})}\,.$$

Dividing through by η_a^* we obtain as a coefficient of θ^* the quantity which by (10) we saw was the lth power of a unit in $k(\zeta)$, and noting also that the right hand member may be simplified by using the relation

$$\zeta^a + \zeta^{-a} - \zeta^b - \zeta^{-b} = (\zeta^{-b} - \zeta^{-a})(\zeta^{a+b} - 1),$$

we obtain

$$\text{(10b)} \qquad \omega_1{}^l + \theta_1{}^l = \delta\kappa^{(2m-1)l}\xi_1{}^l,$$

with δ a unit in $k(\zeta)$. This equation is exactly the same form as (6) with ω_1, θ_1, ξ_1 integers in $k(\zeta)$ prime to each other and $2m-1>1$, since $m>1$. Comparing the value of ξ_1 with the value of ξ we see, however, that since $\xi_1=\rho_0^2$, then ξ_1 necessarily contains a lesser number of distinct prime ideal factors than does ξ, aside from the exceptional case when ξ/ρ_0 is a unit in $k(\zeta)$, in which event

$$\frac{\omega + \zeta^i\theta}{1 - \zeta^i}$$

is a unit in the field $k(\zeta)$ where $i=1, 2, \cdots, l-1$, whence

$$\frac{\omega + \zeta^i\theta}{1 - \zeta^i} = \frac{\zeta^k(\omega + \zeta^{-i}\theta)}{1 - \zeta^{-i}},$$

which gives, using $\omega+\theta\equiv 0 \pmod{l}$,

$$(1 - \zeta^k)(1 - \zeta^i) \equiv 0 \qquad \pmod{l},$$

and this is impossible for $l>3$.

Hence we obtain by repetition of the process used in connection with (6a) an unlimited series of integers in the field $k(\zeta)$, ξ_1, ξ_2, ξ_3, $\cdots$, in each of which the number of distinct ideal factors is less than in the preceding, which is impossible. This completes the proof of Theorem I.

3. We now consider

THEOREM II. *Under the assumptions*

(1) *only one of the Bernoulli numbers* (*say* B_n) *in the set*

$$B_1, B_2, \cdots, B_{l_1} \tag{11}$$

is divisible by l;

(2) *the Bernoulli number* B_{nl} *is not divisible by* l^3;

the equation (2) *is impossible in rational integers none zero.*

For proof suppose first that the second factor of the class number of $k(\zeta)$ is prime to l; it then follows from Theorem I that (2) is impossible in case II in view of Assumption 2 of the present theorem. The theorem follows immediately for case I since it is known[*] that if (2) is satisfied in this case then at least two of the Bernoulli numbers in the set (11) are divisible by l.

Consider now the only other possibility, that is, when the second factor of the class number is divisible by l in case II. Furtwängler[†] showed that if f is an arbitrary algebraic field and f' the superfield of f obtained by adjoining ζ, then any class in the irregular class group[‡] of f may be represented in the form

$$(c)_f = c_1^{x_1} \cdots c_e^{x_e}$$

$$(x_i = 0, 1, \cdots, l^{h_i} - 1\,;\ h_1 + \cdots + h_l = h'),$$

where $ql^{h'}$ is the class number of f with q prime to l, and also any class in the irregular class group of f' may be written in the form (if $(c)_f$ is now interpreted in f')

$$(c)_f C,$$

where C is a class in f' such that, if $s_1, \cdots, s_j$ are the substitutions of the relative group of f' with respect to f, then if $C = C_{s_1}$,

$$C_{s_1} C_{s_2} \cdots C_{s_j} = 1,$$

where C_s represents the class of ideals obtained from C by the substitution s on the ideals of C. Let the field f be $k(\zeta+\zeta^{-1})$ and then f' is $k(\zeta)$, so every class in the irregular class group of $k(\zeta)$ may be written in the form

$$c_k C$$

[*] Kummer, Berlin Abhandlungen, Mathematisch-Physikalische Klasse, 1857, pp. 61–65.

[†] Mathematische Annalen, vol. 63 (1906), pp. 21–22; Pollaczek, Mathematische Zeitschrift, vol. 21 (1924), p. 22.

[‡] The irregular class group is obtained by considering the group of classes formed by the qth powers of all the ideals in f. Hence the principal class in the irregular class group consists of ideals which are $l^{h'}$th powers of ideals in f.

where

$$CC_s = 1$$

with $s = (\zeta/\zeta^{-1})$. Now consider from (6)

$$\left(\frac{\omega + \zeta^a\theta}{1 - \zeta^a}\right).$$

This has no prime ideal factor which belongs to the field $k(\zeta+\zeta^{-1})$ since if $\mathfrak{q}$ is such an ideal, then

$$\frac{\theta + \zeta^a\omega}{1 - \zeta^a} \equiv \frac{\theta + \zeta^{-a}\omega}{1 - \zeta^{-a}} \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{q})$$

which gives

$$(\zeta^a - \zeta^{-a})\omega \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{q}),$$

which contradicts the assumption that ω and ξ are prime to each other. Hence all prime ideal factors of $(\omega+\zeta^a\theta)/(1-\zeta^a)$ belong to the C classes and the relative norm of each belongs to the principal class of the irregular class group in $k(\zeta)$. We may then write

$$\left[\left(\frac{\theta + \zeta^a\omega}{1 - \zeta^a}\right)\left(\frac{\theta + \zeta^{-a}\omega}{1 - \zeta^{-a}}\right)\right]^q_. = \eta_1(\tau')^l$$

and using $qq_1 \equiv 1$ (mod l) since q is prime to l we have, using notation of (8),

$$\frac{\theta + \zeta^a\omega}{1 - \zeta^a}\cdot\frac{\theta + \zeta^{-a}\omega}{1 - \zeta^{-a}} = \eta_a^2\tau_a^l,$$

$$\frac{\theta + \zeta^b\omega}{1 - \zeta^b}\cdot\frac{\theta + \zeta^{-b}\omega}{1 - \zeta^{-b}} = \eta_b^2\tau_b^l,$$

$$\theta^2 + \omega^2 + 2\theta\omega = \eta_0^2\kappa^{2ml-l+1}\tau_0^{2l},$$

with $a \not\equiv \pm b$ (mod l), and elimination of the two quantities $\theta^2+\omega^2$ and $\omega\theta$ from these three equations gives

$$(12) \qquad \eta_a^2\tau_a^l - \eta_b^2\tau_a^l = \delta'\kappa^{(2m-1)l}(\xi')^l,$$

where δ' is a unit and ξ' an integer in $k(\zeta+\zeta^{-1})$. This relation shows that η_a^2/η_b^2 is a primary unit in $k(\zeta+\zeta^{-1})$. But we shall now show that if the second factor of the class number is divisible by l this is contrary to the second assumption of our theorem.

Using the assumption as to the second factor it follows that E_n is the lth power of a unit in $k(\zeta)$, but that $E_{n'}, n' \neq n$, is not an lth power. Suppose that there exists a primary unit η which is not the lth power of a unit in $k(\zeta)$, we may then set

$$\eta^t = E_1^{s_1} E_2^{s_2} \cdots E_{l_1}^{s_{l_1}} .$$

As in the proof of Lemma II, we may replace this by an identity in e^v of the type (3b). Differentiating $2k$ times and setting $v=0$ we have, using (4a) and (5),

$$s_i B_i \equiv 0 \qquad (\mathrm{mod}\ l),$$

and $s_i \equiv 0$ (mod l) except for $i=n$. Now $E_n=(E')^l$. Hence η^t is the lth power of a unit with η not the lth power of a unit, hence $t\equiv 0$ (mod l), and as in the proof of Lemma II, we have $s_n \not\equiv 0$ (mod l). It then follows that $\eta^t \equiv c^l$ (mod l^2) and we find as from (3b), $B_{nl}\equiv 0$ (mod l^3) which contradicts Assumption 2 of our theorem. Hence in (12), η_a^2/η_b^2 is the lth power of a unit in $k(\zeta)$ and (12) reduces to the same form as (6). Repetition of this process leads to a contradiction as in the proof of Theorem I. This completes the proof of Theorem II.

4. We now proceed to

THEOREM III. *If* $l\equiv 1$ (mod 4) *and all the numbers in* (11) *which are divisible by l have even subscripts, then* (2) *is impossible in rational integers none zero.*

This proof depends, in part, on a remarkable device employed by Mirimanoff.* Consider first the relation (2) in case I. Then Kummer, as pointed out in the proof of Theorem II, proved that, if (2) holds in this case, $B_{l_1}\equiv B_{l_1-1} \equiv 0$ (mod l) and one of these subscripts is odd. This proves the theorem for case I.

In case II, consider the generalized form (6) again. Using the result employed in the proof of Theorem II, that all ideal divisors of $(\omega+\zeta^a\theta)/(1-\zeta^a)$ are such that their relative norms with respect to the field $k(\zeta+\zeta^{-1})$ belong to the principal class of the irregular class group, we obtain as before

$$\left(\frac{\theta+\zeta^a\omega}{1-\zeta^a}\right)\left(\frac{\theta+\zeta^{-a}\omega}{1-\zeta^{-a}}\right) = \eta_a\tau_a{}^l,$$

and this may be written, if $\kappa_a=(1-\zeta^a)(1-\zeta^{-a})$,

$$(\theta+\omega)^2-(\kappa_a)\theta\omega = \eta_a\kappa_a\tau_a{}^l, \tag{13}$$

$$(\theta+\omega)^2 = \eta_0\kappa^{2ml-l+1}\tau_0{}^l. \tag{13a}$$

Now, following Mirimanoff, we may assume, since $l\equiv 1$ (mod 4), that $(\theta+\omega)^2$

* Crelle, vol. 111 (1893), pp. 26–30.

and $\theta\omega$ belong to the sub-field of $k(\zeta)$ defined by $(\theta+\theta^{-1}+\theta^{r^w}+\theta^{-r^w})$ which we shall call k'; $w=(l-1)/4$. Suppose that the distinct Bernoulli numbers in the set (11) which are divisible by l are

$$B_{a_1}, B_{a_2}, \cdots, B_{a_e}.$$

By the hypothesis of the theorem the a's are all even. Now according to Pollaczek* there exists a fundamental system of l_1 real units in $k(\zeta)$ such that

$$\beta_i^{s-r^{2i}} = (\beta_i')^l \qquad (i = 1,2, \cdots, l_1), \tag{13b}$$

s standing for the substitution (ζ/ζ^r), and r is a primitive root of l. It was also shown by the writer† that there exists a certain system of independent real units in $k(\zeta)$,

$$\alpha_1, \alpha_2, \cdots, \alpha_{l_1},$$

which have the property

$$\alpha_i^{s-r^{2i}} = (\alpha_i')^l,$$

and also

$$\alpha_i = \beta_i^{c_i}(\beta_i'')^l,$$

c_i a rational integer and β_i'' a unit in $k(\zeta)$. As the E's as defined in the present paper also have this property, it follows as in the Annals paper that

$$E_i = \beta_i^{d_i}(\beta_i^{(3)})^l, \tag{14}$$

where $\beta_i^{(8)}$ is a unit in $k(\zeta)$ and d_i is a rational integer.

Now consider the primary units in $k(\zeta)$. Any such may be written in the form

$$s + \sigma l = \gamma = \prod_{i=1}^{l_1} \beta_i^{g_i}, \tag{15}$$

where s is a rational integer and σ an integer in $k(\zeta)$. As in the proof of Lemma II, we may replace this by an identity in e^v and obtain

$$(s + l\sigma(e^v))^{l-1} = \prod_{i=1}^{l_1} \gamma_i^{g_i}(e^v) + \frac{e^{vl} - 1}{e^v - 1}X \tag{15a}$$

where

$$\gamma_i \equiv 1 \pmod{\lambda},$$

and X is a polynomial in e^v with rational integral coefficients. Now using (14), replacing it by an identity in e^v, differentiating $2i$ times and setting $v=0$, we have from (4a)

* Loc. cit., p. 7.

† Annals of Mathematics, 1929.

$$(-1)^{i-1}\frac{B_i(r^{2i}-1)}{4i}(l-1) \equiv d_i\left[\frac{d^{2i}\log\beta_i(e^v)}{dv^{2i}}\right]_{v=0}, \tag{16}$$

modulo l. We have similarly, $t<l-1$,

$$(l-1)\left[\frac{d^t\log\beta_i(e^v)}{dv^t}\right]_{v=0} \equiv \frac{d^t\log\gamma_i(c^v)}{dv^t} \qquad (\text{mod } l). \tag{17}$$

We also have from (13b) after replacing it by an identity in e^v

$$\left[\frac{d^t\log\beta_i(e^v)}{dv^t}\right]_{v=0} \equiv 0 \qquad (\text{mod } l) \tag{18}$$

for $t\neq 2i$. Differentiating (15a) $2i$ times and setting $v=0$, we have, using (17) and (18),

$$g_i\left[\frac{d^{2i}\beta_i(e^v)}{dv^{2i}}\right]_{v=0} \equiv 0 \qquad (\text{mod } l),$$

and employing (16) we see that $d_i\not\equiv 0$ (mod l); $g_i\equiv 0$ (mod l) except for $i=a_1, a_2, \cdots, a_e$. Hence, from (15), any primary unit in $k(\zeta)$ may be written in the form

$$\gamma = \prod_\alpha \beta_\alpha^{g_\alpha}\delta^l$$

where δ is a unit in $k(\zeta)$ and α ranges over the set $a_1, \cdots, a_e$.

Now consider the unit η_a which occurs in (13). We may write it in the form

$$\eta_a = \prod_{i=1}^{l_1}\beta_i^{h_i'}.$$

Let $h_i' \equiv 2h_i$ (mod l), where h_i is a rational integer, and we have

$$\eta_a = \prod_{i=1}^{l_1}\beta_i^{2h_i}\delta_1^{\,l}, \quad 0 \leqq h_i < l,$$

where δ_1 is a unit in $k(\zeta)$. The relation (13) then becomes

$$(\theta+\omega)^2 - (\kappa_a)\theta\omega = \kappa_a\prod_i\beta_i^{2h_i}(\phi_a')^l. \tag{19}$$

Set

$$\theta = \prod_{i=1}^{l_1}\beta_i^{h_i}\beta_i^{h_i}(\zeta^{r^w})\theta', \; \omega = (\theta/\theta')\omega',$$

where $\beta_i(\zeta^{r^w})$ represents the unit obtained from β_i by the substitution (ζ/ζ^{r^w}) with $w=(l-1)/4$. Now $\beta_i\beta(\zeta^{r^w})$ belongs to the field k'. Hence

$(\theta'+\omega')^2$ and $\theta'\omega'$ belong to this field, since $(\theta+\omega)^2$ and $\theta\omega$ do. From (19) we then have

$$(\theta' + \omega')^2 - (\kappa_a)\theta'\omega' = \kappa_a \frac{\prod_i \beta_i^{h_i}}{\prod_i \beta_i^{h_i}(\zeta^{r^w})}(\phi_a')^l. \tag{20}$$

We have

$$\beta_i(\zeta^r) = \beta_i^{r^{2i}}\delta_2^l,$$

where δ_2 is a unit in $k(\zeta)$. Hence

$$\beta_i(\zeta^{r^w}) = \beta_i^{r^{2iw}}\delta_3^l = \beta_i\delta_4^l$$

if i is even and the δ's are units in $k(\zeta)$. If i is odd we have

$$\beta_i(\zeta^{r^w}) = \beta_i^{r^{i(l-1)/2}}(\delta_3')^l.$$

Hence (20) becomes

$$(\theta' + \omega')^2 - (\kappa_a)\theta'\omega' = \kappa_a \prod_s \beta_s^{h_s(1-r^{s(l-1)/2})}\phi_a^l, \tag{21}$$

where s ranges over all the odd integers in the set $1, 2, \cdots, l_1$. Dividing through by κ_a, we have, using $\theta'+\omega'\equiv 0 \pmod{l^2}$,

$$\theta'\omega' \equiv \prod_s \beta_s^{h_s(1-r^{s(l-1)/2})}\phi_a^l \pmod{l}.$$

Setting ζ^{r^w} for ζ in this relation we have, since $\theta'\omega'$ is unaltered by this substitution,

$$\prod_s \beta^{2h_s(r^{s(l-1)/2}-1)} \equiv c \pmod{l},$$

where c is a rational integer. Since all the Bernoulli numbers divisible by l have even subscripts and none can be an s and all the g's in (15) are divisible by l except for $i=a_1, a_2, \cdots, a_e$, then

$$2h_s(r^{s(l-1)/2} - 1) \equiv 0 \pmod{l}$$

and $h_s=0$, so (21) becomes

$$(\theta' + \omega')^2 - (\kappa_a)\theta'\omega' = \kappa_a\phi_a^l.$$

Setting ζ^{r^w} for ζ in this relation gives

$$(\theta' + \omega')^2 - (2 - \zeta^{ar^w} - \zeta^{-ar^w})\theta'\omega' = \kappa_a(\zeta^{r^w})(\phi_a(\zeta^{r^w}))^l.$$

Taking these two equations with (13a) and eliminating $(\theta'+\omega')^2$ and $\theta'\omega'$ we obtain

$$\phi_a^l - (\phi_a(\zeta^{r^w}))^l = \gamma\kappa^{(2m-1)l}\tau_0^l,$$

where γ is a unit in $k(\zeta)$. This equation belongs to the same class as (6) and we obtain an equation therefrom of the same form as (13) and having the property that $(\phi_a - \phi_a(\zeta^{r^w}))^2$ and $\phi_a\phi_a(\zeta^{r^w})$ each belong to the field k'. We may then proceed as in the last part of the proof of Theorem I and ultimately reach a contradiction.

5. We may now proceed to

Theorem IV. *Under the following assumption*:

None of the units E_a, $k = a_1, a_2, \cdots, a_s$, *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* $a_1, a_2, \cdots, a_s$ *are the subscripts in the Bernoulli numbers in the set* (11) *which are divisible by* l;
the relation (2) *is impossible in case* II.

To prove this we note first that it follows from this assumption that the second factor* of the class number of $k(\zeta)$ is prime to l. Instead of the generalized equation (6a) we shall here consider the same form with $\eta = 1$ and ω, θ and ξ integers in the field $k(\zeta + \zeta^{-1})$ prime to each other, that is, we consider the equation

$$\omega^l + (\kappa^m\xi)^l = -\theta^l.$$

Set

$$-\kappa^m\xi = \phi,$$

so that

$$\omega^l + \phi^l = -\theta^l. \tag{22}$$

As in the proof of Theorem I we note that $(\omega + \zeta^a\phi)(\omega + \zeta^a\phi)^{l-1}$ is a primary number in $k(\zeta)$, so that we have as in the said proof

$$\omega + \zeta^a\phi = \eta_a\sigma_a{}^l \qquad (a = 1, 2, \cdots, l-1), \tag{23}$$

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

$$\sigma_{-a}{}^l(\omega + \zeta^a\phi) = \sigma_a{}^l(\omega + \zeta^{-a}\phi). \tag{23a}$$

Now θ is prime to $\mathfrak{p}$, for if divisible by $\mathfrak{p}$, we may assume $\mathfrak{p}$ prime to ω and we obtain from (22), in the same manner in which (23) was derived,

$$\theta + \zeta^a\phi = \gamma_a\tau^l, \tag{24}$$

where γ_a is a real unit and τ an integer in $k(\zeta)$. Since θ is divisible by $\mathfrak{p}$ it is also divisible by $\mathfrak{p}_{-1}$ since θ belongs to the field $k(\zeta + \zeta^{-1})$. Hence using power characters† we have

* Stafford and Vandiver, Proceedings of the National Academy of Sciences, 1930; Vandiver, Bulletin of the American Mathematical Society, vol. 35 (1929), pp. 333–35.

† Hilbert, loc. cit., p. 365.

$$\left\{\frac{\zeta^a\phi}{\mathfrak{p}\mathfrak{p}_{-1}}\right\} = \left\{\frac{\gamma_a}{\mathfrak{p}\mathfrak{p}_{-1}}\right\},$$

and since ϕ and γ_a are in the field $k(\zeta+\zeta^{-1})$ we obtain

$$\left\{\frac{\zeta^a}{\mathfrak{p}\mathfrak{p}_{-1}}\right\} = \left\{\frac{\zeta}{\mathfrak{p}}\right\}^{2a} = 1,$$

and $p-1\equiv 0 \pmod{l^2}$, which contradicts our hypothesis concerning p. Hence the σ's are prime to $\mathfrak{p}$. Hence we obtain from (23) by raising both members to the power c, $p=1+cl$,

$$(24a) \qquad (\omega+\zeta^a\phi)^c \equiv (\omega+\zeta^{-a}\phi)^c \pmod{\mathfrak{p}},$$

or

$$\omega^c + c\omega^{c-1}\zeta^a\phi + \cdots + \zeta^{ac}\phi^c \equiv \omega^c + c\omega^{c-1}\zeta^{-a}\phi + \cdots + \zeta^{-ca}\phi^c \pmod{\mathfrak{p}}.$$

Multiply both sides by ζ^a. We have, after setting $a=0$ (for which the above relation obviously holds), $1, 2, \cdots, l-1$, and adding the resulting congruences,

$$(25) \qquad \phi\omega^{c-1} \equiv 0 \pmod{\mathfrak{p}}$$

under the assumption that $c<l-1$. Now ω is not divisible by $\mathfrak{p}$, as we can obtain a contradiction by assuming it divisible by $\mathfrak{p}$ and employing (23) in the same way that (24) was used. Hence we obtain from (25)

$$(25a) \qquad \phi \equiv 0 \pmod{\mathfrak{p}}.$$

Since $p=1+cl$, it is of the first degree and we may therefore write

$$p = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{l-1},$$

the $\mathfrak{p}$'s being distinct ideals. Now $\mathfrak{p}$ was an arbitrary prime ideal divisor of p and since p is not divisible by the square of an ideal it follows that we may write in lieu of (25a)

$$\phi \equiv 0 \pmod{p}.$$

We shall now show that $(\omega+\theta)$ is divisible by (p). In order to effect this we again consider (22) and obtain, exactly as in the proof of Theorem I,

$$(26) \qquad \frac{\omega+\zeta^a\theta}{1-\zeta^a} = \eta_a\rho_a{}^l,$$

$$(26a) \qquad \omega+\theta = \eta_0\kappa^{ml-(l-1)/2}\rho_0{}^l,$$

where the η's are units and the ρ's integers in $k(\zeta)$. Since ϕ is divisible by p let us assume that

$$\omega + \zeta^k\theta \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{p}_n),$$

where $\mathfrak{p}_n$ is a prime ideal divisor of p for

$$k \not\equiv 0 \qquad (\mathrm{mod}\ l).$$

Make the substitution in this congruence $(\zeta/\zeta^{k'})$ where

$$kk' \equiv 1 \qquad (\mathrm{mod}\ l).$$

By this substitution $\mathfrak{p}_n$ is changed into another prime ideal divisor of p which we shall call $\mathfrak{p}$, hence, if ω' and θ' are the corresponding conjugates of ω and θ,

$$(27) \qquad \omega' + \zeta\theta' \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{p}).$$

It then follows that $\omega' + \zeta^a\theta'$ is prime to $\mathfrak{p}$ for $a \neq 1$, and, from (26),

$$\frac{\omega' + \zeta^k\theta'}{\zeta^k - 1}\rho'^{\,l}_{-k} = \frac{\omega' + \zeta^{-k}\theta'}{\zeta^{-k} - 1}\rho'^{\,l}_{k}.$$

If we assume now that k is any integer in the set $1, 2, \cdots, l-1$ excepting unity, we may raise both sides of this relation to the power c and obtain, since the ρ's are prime to p,

$$(27\mathrm{a}) \qquad (\omega' + \zeta^k\theta')^c \equiv (\zeta^k\omega' + \theta')^c \qquad (\mathrm{mod}\ \mathfrak{p}),$$
$$k = 2, 3, \cdots, l-1.$$

We also have

$$\omega' + \zeta^k\theta' - \omega' - \zeta\theta' \equiv \theta'(\zeta^k - \zeta) \qquad (\mathrm{mod}\ \mathfrak{p}),$$

and from (27) and (27a),

$$\left\{\frac{\theta'(\zeta^k - \zeta)}{\mathfrak{p}}\right\} = \left\{\frac{\theta'(1 - \zeta^{k+1})}{\mathfrak{p}}\right\},$$

the symbol denoting the lth power character, or

$$\left\{\frac{\zeta}{\mathfrak{p}}\right\}\left\{\frac{\zeta^{k-1} - 1}{\mathfrak{p}}\right\} = \left\{\frac{\zeta^{k+1} - 1}{\mathfrak{p}}\right\},$$

whence

$$(28) \qquad \left\{\frac{\zeta}{\mathfrak{p}}\right\}\left\{\frac{\dfrac{\zeta^{k-1} - 1}{\zeta - 1}}{\mathfrak{p}}\right\} = \left\{\frac{\dfrac{\zeta^{k+1} - 1}{\zeta - 1}}{\mathfrak{p}}\right\}.$$

Now consider the expression

$$\left\{\frac{\dfrac{\zeta^t - 1}{\zeta - 1}}{\mathfrak{p}}\right\} = \zeta^T,$$

where

$$T = \operatorname{ind}\left(\frac{\zeta^t - 1}{\zeta - 1}\right).$$

Using a known formula[*] we have

$$\text{(29)} \qquad \operatorname{ind}\left(\frac{\zeta^t - 1}{\zeta - 1}\right) \equiv \frac{1}{2}(t - 1) \operatorname{ind} \zeta - 2 \sum_{n=1}^{l_1} \frac{\operatorname{ind} E_n(\zeta^t) - \operatorname{ind} E_n(\zeta)}{r^{2n} - 1} \pmod{l}.$$

Now if

$$t \equiv r^i \pmod{l},$$

then because of the relation[†]

$$E_n^{s^i - r^{2in}} = \eta^l\,;\ \eta \text{ a unit in } k(\zeta),$$

we may write

$$\text{(29a)} \qquad \operatorname{ind} E_n(\zeta^t) \equiv t^{2n} \operatorname{ind} E_n(\zeta) \pmod{l}.$$

Substituting in (29) we obtain

$$\text{(29b)} \qquad \operatorname{ind}\left(\frac{\zeta^t - 1}{\zeta - 1}\right) \equiv \frac{1}{2}(t - 1) \operatorname{ind} \zeta - 2 \sum_{n=1}^{l_1} \frac{(t^{2n} - 1) \operatorname{ind} E_n(\zeta)}{r^{2n} - 1} \pmod{l}.$$

Now apply this relation to (28). We obtain

$$\sum_{n=1}^{l_1} \frac{((k - 1)^{2n} - 1) \operatorname{ind} E_n(\zeta)}{r^{2n} - 1} \equiv \sum_{n=1}^{l_1} \frac{((k + 1)^{2n} - 1) \operatorname{ind} E_n(\zeta)}{r^{2n} - 1} \pmod{l}.$$

Now expand the powers of $k-1$ and $k+1$ by the binomial theorem and arrange the results in descending powers of k. We have, after noting that the coefficients of the even powers of k are the same on both sides of the congruence,

$$\text{(30)} \qquad A_{l-4}k^{l-4} + A_{l-6}k^{l-6} + \cdots + A_1 k \equiv 0 \pmod{l},$$

where the A's are expressions involving t, r, and $\operatorname{ind} E_n(\zeta)$. We have

$$A_{l-4} = \frac{2(l - 3)}{r^{l-3} - 1} \operatorname{ind} E_{l_1}(\zeta).$$

Formula (30) is true for all values of k excepting $k=1$. If we put $k=2$, 4,

[*] Kummer, Crelle's Journal, vol. 56, p. 277.

[†] Here we are using the Kronecker-Hilbert notation of symbolic powers, $E_n^{s^i}$ corresponding to the substitution $E_n(\zeta)/E_n(\zeta^{r^i})$.

$\cdots, l-3$, in turn, we obtain l_1 congruences from which we infer that (cf. (31a))

$$0 \equiv A_1 \equiv A_3 \equiv A_5 \cdots \equiv A_{l-4} \qquad (\mathrm{mod}\, l),$$

since the determinant formed by the coefficients of the A's is prime to l. From the coefficient of A_{l-4} already found we obtain

$$\mathrm{ind}\, E^{l_1}(\zeta) \equiv 0 \qquad (\mathrm{mod}\, l).$$

Also

$$A_{l-6} = 2\binom{l-3}{3}\frac{\mathrm{ind}\, E_{l_1}(\zeta)}{r^{l-3}-1} + \frac{2(l-5)\mathrm{ind}\, E_{l_1-1}(\zeta)}{r^{l-5}-1}\,.$$

From this we obtain

$$\mathrm{ind}\, E_{l_1-1}(\zeta) \equiv 0 \qquad (\mathrm{mod}\, l).$$

Proceeding in this way we find that all the E's are such that

$$\mathrm{ind}\, E_n \equiv 0 \qquad (\mathrm{mod}\, l),$$

which contradicts the first assumption in our theorem. From this it easily follows that

$$\left\{\frac{E_n}{\mathfrak{p}_i}\right\} = 1 \qquad (i = 1, 2, \cdots, l-1)\,;$$

using (29a), hence, $\omega + \zeta^k\theta \not\equiv 0$ (mod $\mathfrak{p}_i$); $k \not\equiv 0$ (mod l). We have then completely established the fact that

$$\omega + \theta \equiv 0 \qquad (\mathrm{mod}\, p)$$

in (26a). Because of this relation we obtain from (26a)

$$\rho_0 \equiv 0 \qquad (\mathrm{mod}\, p).$$

Taking (26) and multiplying it by the equation which was obtained from it by a substitution (ζ/ζ^{-1}), then substituting b in lieu of a in the result and also squaring equation (26a), we obtain three equations from which we may eliminate $\omega^2+\theta^2$ and $\omega\theta$ as was done in the proof of Theorem I. We obtain an equation of the type (10a), the only possible difference being in the unit which appears in the right hand member. If we transpose the term $\eta_b^*\theta^{*l}$ to the right hand member and take lth power characters of each member we obtain, since

$$\rho_0 \equiv 0 \qquad (\mathrm{mod}\, p),$$

$$\left\{\frac{\eta_a^*}{\mathfrak{p}}\right\} = \left\{\frac{\eta_b^*}{\mathfrak{p}}\right\},$$

where $\mathfrak{p}$ is a prime ideal divisor of p. From this we have

$$\left\{\frac{\eta_a^*\eta_b^{*l-1}}{\mathfrak{p}}\right\} = 1.$$

In transforming this expression we shall employ a method which has proved of great use in handling a number of questions in cyclotomic field theory. Since the E's form a system of independent units in $k(\zeta)$ we may set

$$(31) \qquad (\eta_a^*\eta_b^{*l-1})^d = E_1^{d_1}E_2^{d_2} \cdots E_{(l-3)/2}^{d_{(l-3)/2}}.$$

Suppose now that d is divisible by l; then we may assume, as at the beginning of the proof of Lemma II, that not all the d's are divisible by l. Hence by a previous paper of the writer's† we infer that $E_s^{d_s}$ is the lth power of a unit in $k(\zeta)$, $s=1, 2, \cdots, l_1$, where $l_1=(l-3)/2$, and therefore $E_s=\gamma^l$, where γ is a unit in $k(\zeta)$, for some s. Then, as we have already seen during the course of the proof of Theorem III, s is included in the set $a_1, a_2, \cdots, a_e$. But this gives

$$\left\{\frac{E_s}{\mathfrak{p}}\right\} = 1,$$

contrary to the assumption stated in Theorem IV. Hence

$$d \not\equiv 0 \qquad (\mathrm{mod}\ l).$$

Then in the revised equation (10a) we can also set ζ^k in lieu of ζ; $k=1, 2, \cdots, l-1$. In view of the relation (29a) we have, from (31),

$$d \text{ ind } (\eta_a^*(\zeta^k)\eta_b^*(\zeta^k)^{l-1}) \equiv \sum_{n=1}^{l_1} d_n k^{2n} \text{ ind } E_n \equiv 0 \qquad (\mathrm{mod}\ l), \quad k = 1,2, \cdots, l-1.$$

We obtain l_1 congruences, and since the determinant

$$(31\mathrm{a}) \qquad \begin{vmatrix} 1 & 1 & 1 & & 1 \\ 2^2 & 2^4 & 2^6 & \cdots & 2^{l-3} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ l_1^2 & l_1^4 & & \cdots & l_1^{l-3} \end{vmatrix} = \prod_{i,j}^{1 \text{ to } l_1} (i+j)(i-j)(l_1!)^2, \quad i>j,$$

is prime to l we obtain

$$d_n \text{ ind } E_n \equiv 0 \qquad (\mathrm{mod}\ l); \quad n = 1,2, \cdots, l_1.$$

† Bulletin of the American Mathematical Society, vol. 35 (1929), pp. 333–335.

Now also the unit $\eta_a^*\eta_b^{l-1}$ is a primary unit in $k(\zeta)$. This follows immediately from the revised equation (10a). Hence the only E's which can appear in (31) are those referred to in the Assumption of our Theorem IV which shows that all the d's appearing as exponents are divisible by l. Hence $(\eta_a^*\eta_b^{*l-1})^d$ and therefore $\eta_a^*\eta_b^{*l-1}$ is the lth power of a unit in $k(\zeta)$. Now using our revised equation (10a) and dividing through by η_a^*, we obtain

$$\omega_1^l + \theta_1^l = \delta_1\kappa^{(2m-1)l}\xi_1^l, \tag{32}$$

where ω_1, θ_1, ξ_1 are integers in $k(\zeta)$ and δ_1 is a unit in that field. Also the first three integers mentioned are prime to each other in $k(\zeta)$ with ξ_1 divisible by p. This equation is a more generalized form than (22). However we may proceed as in the treatment of (22), obtaining

$$\frac{\omega_1 + \zeta^a\theta_1}{1 - \zeta^a} = \alpha_a\nu_a^l \ ,$$

$$\omega_1 + \theta_1 = \alpha_0\kappa^{(2m-1)l-(l-1)/2}\nu_0^l,$$

where $a=1, 2, \cdots, l-1$; the α's are units and the ν's integers in $k(\zeta)$. Since ξ_1 is divisible by p it follows that either ν_0 or ν_a is divisible by a prime ideal divisor of p and we may show exactly as in our treatment of (26) and (26a) that $\omega_1+\theta_1$ is divisible by p. Also eliminating ω_1 and θ_1 as ω and θ were eliminated from the equations based on (26) and (26a) and showing that the units involving α are lth powers of units in $k(\zeta)$ as it was proved that the units involving the η's were lth powers, we find

$$\omega_2^l + \theta_2^l = \delta_2\kappa^{(4m-3)l}\xi_2^l, \tag{32a}$$

with ξ_2 divisible by p and prime to the integers ω_2 and θ_2, and δ_2 being a unit in the field. This equation is of precisely the same form as (32), hence by repetition of this process we obtain as in the proof of Theorem I an unlimited series of ideals in each of which the number of distinct prime ideal factors is less than in the preceding, which is impossible. This completes the proof of Theorem IV.

6. We shall now consider the equation (2) with x, y and z rational integers, and derive criteria for the solution of it in such a way that the fact that x, y and z are rational integers is employed during the argument. As noted in the introduction to this paper this is apparently the first time criteria of this type have been obtained for the second case of Fermat's last theorem. The theorem is as follows:

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*

$$\left\{\frac{E_a}{\mathfrak{p}}\right\} \neq 1$$

holds, where a *ranges over the values* $a_1, a_2, \cdots, a_s$, *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 (2) *is impossible in rational integers none zero.*

For proof consider the equation (2). If this holds then by the first assumption in our theorem it follows that one of the integers x, y, and z is divisible by p. If none of these integers is divisible by l then the theorem follows because of Theorem IV in a previous paper.* If we suppose that one of these integers, say z, is divisible by l, then it follows that z is divisible by p since if x or y is divisible by p we have by Furtwängler's Theorem

$$p^{l-1} \equiv 1 \pmod{l^2},$$

which contradicts the assumption that

$$p \not\equiv 1 \pmod{l^2},$$

for it is known that in order that Assumption 1 of the Theorem hold we must have

$$p \equiv 1 \pmod{l}.$$

We now proceed with equation (2) in the same manner as in the treatment of (32), and we find that $x+y$ is divisible by p. We then find as before an equation of the type (32a) with ξ_2 divisible by p and we ultimately reach a contradiction as described previously.

7. We now consider the application of these theorems to Fermat's last theorem for special exponents. The work of Kummer concerning the examination of special exponents has been described in the introduction to this paper. It was also stated in the introduction that the primes l less than 211 were tested as to being regular. The main formula employed for this is

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

* Annals of Mathematics, (2), vol. 27 (1926), p. 55.

The proof of this formula and the details of the computations will be given in a paper by Professor E. T. Stafford and myself.* As noted before, the only irregular exponents found within the range mentioned were those which had previously been discovered by Kummer. Hence we may state

THEOREM VI. *The equation*

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

is impossible for all odd prime exponents** l **less than** 211 **excepting possibly** $l=37$, 59, 67, 101, 103, 131, 149 **and** 157 **if** α, β **and** γ **are integers in the field** $k(\zeta)$ **none zero.

As already noted only one of the Bernoulli numbers in the set (11) is divisible by l in each of the cases $l=37$, 59, 67, 101, 103, 131, 149. We then apply Theorem II to these cases by employing the formula given by

LEMMA 3. *If* $1<a<(l-1)/2$ *and* l *is a prime integer* >5 *then*

$$(33)\qquad \frac{(-1)^{a-1}B_{al}(2^{2al}-1)}{2al} \equiv 1^{2al-1}+3^{2al-1}+5^{2al-1}+\cdots+(l-2)^{2al-1}$$
$$\equiv B'_{al} \pmod{l^2}$$

and

$$(33a)\qquad \frac{(-1)^{a}B_{al}(2^{2al}-1)}{2^{2al}al} = A_a$$
$$\equiv 1^{2al-1}+2^{2al-1}+\cdots+\left(\frac{l-1}{2}\right)^{2al-1} \pmod{l^2}.$$

To prove these relations we employ the Bernoulli summation formula

$$s_n(l) = lb_n + l\frac{n}{2}(lb_{n-1}) + l^2\frac{n(n-1)}{2\cdot 3}(lb_{n-2})$$
$$+\cdots+ l\frac{l^{r-1}}{r+1}\binom{n}{r}(lb_{n-r})+\cdots,$$

where

$$s_n(l) = 1^n+2^n+\cdots+(l-1)^n,$$

and

$$b_{2a} = (-1)^{a-1}B_a,\quad b_{2a+1}=0,\quad a>0,$$

and n is an arbitrary positive integer.

Set $n=2al$. The second term in the right hand member of the summation formula is zero. The third term is divisible by l^4, since by the von Staudt-Clausen Theorem lb_{n-2} is either a fraction divisible by l or, if $n-2$ is divisible by $l-1$, then l appears to the first power in the denominator of b_{n-2}, but the

* Proceedings of the National Academy of Sciences, 1930.

latter condition can not hold for $n=2al$. Also it is easily seen by induction that $l^{r-1}>l^2\ (r+1)$ for $l>5$, and $r>3$. Hence $l^{r-1}/(r+1)$ is divisible by l^3 and the corresponding term in the above expansion is divisible by l^4, hence $s_n(l)\equiv lb_n \pmod{l^4}$ for $n=2al$.

We now introduce the formula[*]

$$\frac{(n^i - 1)\sum_{a=1}^{p-1} a^i}{p} = \sum_{a=1}^{p-1}\sum_{s=1}^{i}\binom{i}{s} a^{i}\left(\frac{y_a}{a}\right)^s p^{s-1},$$

where i is an arbitrary integer, n is an integer prime to p and not unity, and

$$y_a \equiv -\frac{a}{p} \pmod{n}, \quad 0 \leqq y_a < n.$$

Setting $n=2$ in this formula, $i=2al$ and $p=l$, and employing the congruence just obtained, we have

$$(-1)^{a-1}(2^{2al}-1)B_{al} \equiv (1^{2al-1}+3^{2al-1}+\cdots+(l-2)^{2al-1})2al$$
$$+\,(1^{2al-2}+3^{2al-2}+\cdots+(l-2)^{2al-2})\frac{2al(2al-1)}{2}l \pmod{l^3}.$$

It is known that

$$1^k+3^k+\cdots+(l-2)^k \equiv 0 \pmod{l}$$

if k is even. Consequently the last relation reduces to (33). Also it is known that

$$1^n+2^n+\cdots+(l-1)^n \equiv 0 \pmod{l^2}$$

if n is odd and $n\not\equiv 1 \pmod{(l-1)}$. Hence subtracting this congruence from the preceding we obtain (33a), since $2al-1\not\equiv 1 \pmod{(l-1)}$. The congruence (33a) was previously obtained for the case n arbitrary by Mirimanoff[†] who gave a different proof.

For $l=37$ the right-hand member of (33), with $a=16$, was computed directly by Mrs. A. C. S. Williams, who found

$$B'_{16\cdot 37} \equiv 42\cdot 37 \pmod{37^2}.$$

This agrees with Kummer's[‡] calculations, as he found

$$\frac{B_{16\cdot 37}}{37} \equiv 35\cdot 37 \pmod{37^2}.$$

[*] Vandiver, Annals of Mathematics, (2), vol. 18 (1925), p. 112, relation (7a).

[†] Crelle's Journal, vol. 115 (1895), p. 300.

[‡] 1857 Article, p. 73.

Similarly Mrs. Williams found that

$$B'_{22\cdot 59} \equiv 59\cdot 17 \qquad \pmod{59^2},$$

which also checks with Kummer's computations for that prime. For the case $l=67$ she found $B'_{9\cdot 67}\equiv 67\cdot 13 \pmod{67^2}$. This gives $B_{29\cdot 67}\equiv 67^2\cdot 41 \pmod{67^2}$, in lieu of Kummer's result that $B_{29\cdot 67}\equiv 67^2\cdot 49 \pmod{67^3}$. In my opinion this indicates a misprint in Kummer's article. Also, the computations of Mrs. Williams concerning these three primes were all checked by the writer.

An excellent check on the computations of the A's and B''s is the fact that we must find them in each case divisible by l.

For the known irregular primes >100 and <211 the A's in (33a) were computed by Mr. S. S. Wilks using Monroe and Marchant electrical computing machines. He found $A_{34}\equiv 96\cdot 101 \pmod{101^2}$; $A_{12}\equiv 10\cdot 103 \pmod{103^2}$; $A_{11}\equiv 103\cdot 131 \pmod{131^2}$; $A_{65}\equiv 133\cdot 149 \pmod{149^2}$. In the case 157 where $B_{31}\equiv B_{55}\equiv 0 \pmod{l}$ Mr. Wilks found $A_{31}\equiv 39\cdot 157 \pmod{157^2}$ and $A_{55}\equiv 156\cdot 157 \pmod{157^2}$.

All the computations concerning the B''s and A's were abbreviated by a method which I shall describe for the case 67. We note that the right hand member of (33) may be put in the form

$$1+\frac{3^{32\cdot 37}}{3}+\frac{5^{32\cdot 37}}{5}+\cdots+\frac{35^{32\cdot 37}}{35}$$

and $2^{58\cdot 67}$ was reduced modulo 67^2 so that $2^{58\cdot 67}\equiv 3188 \pmod{67^2}$. Similarly $3^{58\cdot 67}\equiv 3859$, and it was noted that $5^{58\cdot 67}\equiv(3^2\cdot 2^3)^{58\cdot 67} \pmod{67^2}$, so that $5^{58\cdot 67}$ is obtained easily from our reductions for the cases 2 and 3. Similarly $7^{58\cdot 67}\equiv(5\cdot 2^3\cdot 3)^{58\cdot 67} \pmod{67^2}$ and so on. These powers of all the odd integers less than $l-1$ were found modulo 67^2, then the expressions $1/3, 1/5, \cdots, 1/65$ were computed modulo 67^2, and the resulting integers were multiplied in the corresponding powers in the formula.

Applying the above mentioned computations to Theorem II, we establish Fermat's last theorem for all the regular primes less than 211 excepting 157.

Theorem III includes two assumptions which are satisfied simultaneously only in the cases $l=37$ and $l=101$.

In order to test Theorem IV for the known irregular primes less than 211 the symbol

$$\left\{\frac{E_a}{\mathfrak{p}}\right\}$$

was computed for the particular values of l and a. For $l=37$ we have $a=16$, $p=149$, $r=2$, and $\zeta\equiv 17 \pmod{\mathfrak{p}}$. Hence to test whether or not the above mentioned symbol is 1 we reduce E_{16} (17) modulo 149, obtain its index modulo 148 using Cahen's tables of indices in the second volume of his *Théorie des Nombres* (which companion tables were checked independently by comparing one with the other). These computations were carried out by Professor Stafford (except for $l=157$, which case was computed by the writer) and are fully described in the joint article already referred to. She found ind E_{16} $(17)\equiv 24$ (mod 37) which agrees with Kummer's results in his 1857 Memoir. Similarly for $l=59$, $p=709$, $\zeta\equiv 385$ (mod $\mathfrak{p}$), $r=2$, $a=22$, and ind E_{22} $(385)\equiv 50$ (mod 59). For $l=67$, $p=269$, $\zeta\equiv 47$ (mod $\mathfrak{p}$), $r=2$, $a=29$, and ind E_{29} $(47)\equiv 4$ (mod 67). The cases 59 and 67 agree with Kummer's computations in his Memoir just cited. For $l=101$, $p=809$, $\zeta\equiv 100$ (mod $\mathfrak{p}$), $r=2$, $a=34$, and ind E_{34} $(100)\equiv 45$ (mod 101). For $l=103$, $p=619$, $\zeta\equiv 315$ (mod $\mathfrak{p}$), $r=5$, $a=12$, and ind E_{12} $(315)\equiv 65$ (mod 103). For $l=131$, $p=263$, $r=2$, $\zeta\equiv 100$ (mod 131), $a=11$ and ind E_{11} $(100)\equiv 52$ (mod 131). For $l=149$, $p=1093$, $r=10$, $\zeta\equiv 354$ (mod $\mathfrak{p}$) and $a=65$, we have E_{65} $(354)\equiv 127$ (mod 149). For $l=157$, $p=1571$, $r=139$, $\zeta\equiv 1024$ (mod $\mathfrak{p}$), and $a=31$, we have ind E_{31} $(1024)\equiv 150$ (mod 157). For $l=157$, $a=55$, we have $p=1571$, $r=139$, $\zeta\equiv 1024$ (mod $\mathfrak{p}$) and ind $E_{55}\equiv 39$ (mod 157). These computations show that the assumptions in Theorem IV are satisfied for all the known irregular primes we are considering, and also show that the second factor of the class number of each of the fields defined by these known irregular primes is prime to l. The latter statement follows because if the second factor of the cyclotomic field defined by l is divisible by l, then $E_{a_1}^{n_1} E_{a_2}^{n_2} \cdots E_{a_e}^{n_e}$ is the lth power of a unit in the field with not all the n's divisible by l. It follows therefrom that each E_a^n is the lth power of a unit in the field.* Through these results and those obtained concerning the A's and B's, we have also a test of Theorem I for all the irregular primes.

We have then tested the first four theorems for all of our known irregular primes and we may enunciate

THEOREM VII. *The equation*

$$x^n + y^n = z^n$$

is impossible in rational integers none zero if

$$2 < n < 211.$$

Note. Since the above was written, Theorem VII has been extended to $n<269$.

* Vandiver, Bulletin of the American Mathematical Society, vol. 35 (1929) pp. 323–335.

UNIVERSITY OF TEXAS,
AUSTIN, TEXAS