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

Autor(en): **Vandiver, H.S.**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **4 (1932)**

PDF erstellt am: **11.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-5605

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

By H. S. VANDIVER, Austin (Texas, U.S.A.)

Kummer [1]) proved that the equation

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

is impossible if α, β and γ are non-zero 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 $B_1, B_2, \ldots, B_{(l-3)/2}$ have numerators which are prime to l, where $B_1 = 1/6$, $B_2 = 1/30$, etc. are the Bernoulli numbers, expressed in their lowest terms. The prime 3 is defined as regular.

Such primes l are called regular [2]). His proof of this was divided into two distinct parts: the first part proved the result for the case where α, β and γ were each prime to $\lambda = (1 - \zeta)$. The other part gives the proof for the case where one of the integers was divisible by λ. Proof of the first case was quite different from that of the second; the latter involving a method of descent as follows:

Kummer took the equation (1) with γ divisible by λ and set

$$\alpha^l + \beta^l = \eta\, \lambda^{ml}\, \omega^l \tag{2}$$

where m is a positive integer, η is a unit, and ω an integer in the field $k(\zeta)$. He showed that this relation gives

$$\alpha + \beta = \eta_0\, \lambda^{ml-l+1}\, \varrho_0^{\,l}$$
$$\alpha + \beta\zeta^r = \eta_r\, (1 - \zeta^r)\, \varrho_r^{\,l}$$

$r = 1, 2, \ldots, l-1$. From these he obtains:

$$\alpha_1^{\,l} + \beta_1^{\,l} = \eta'\, \lambda^{(m-1)l}\, \omega_1^{\,l}$$

---

[1]) Crelle's Journal, vol. 40 (1850), pp. 130—138. Proof extended to the case where α, β, γ are any integers in the field by *Hilbert*, Algebraische Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung, 1894, pp. 517—523.

[2]) In view of computations carried out in recent years by my assistants at the University of Texas, it follows that all primes less than 307 are regular excepting 37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283 and 293.

where α_1, β_1, and ω_1 are integers prime to each other in $k(\zeta)$ and η' is a unit in that field. Note that the exponent of λ has been decreased by l, otherwise the equation is of the same form as (2). The repetition of this process gives an equation of the same form with l as exponent of λ in lieu of $(m-1)l$, and this is readily shown to be impossible. As a special case of Kummer's results we infer that

$$x^l + y^l + z^l = 0 \tag{3}$$

is impossible in rational integers x, y and z none zero, if l is regular.

The object of the present paper is to give a somewhat similar method of descent to cover both cases of Fermat's Last Theorem for regular prime exponents. As usual, if in (3) xyz is prime to l this will be referred to as case I and if one of the integers is divisible by l this will be referred to as case II. As it not uncommon in mathematics a uniform method is obtained for both cases by immersing the problem in a more general one. Kummer's argument for the first part of the proof of (1) depended upon the symmetry of this equation; we consider the equation in the generalized form with θ and ω semi-primary,

$$\theta^l + \omega^l + \delta\gamma^l = 0 \tag{4}$$

where θ, ω and γ aee integers in the field $\Omega(\zeta+\zeta^{-1})$ prime to each other, δ is a unit in that field and $\theta\omega$ is prime to $(1-\zeta)(1-\zeta^{-1})$. We first assume that in (4), γ is prime to $(1-\zeta)(1-\zeta^{-1})$. Since the statement that l is regular is equivalent[3]) to the statement that the class number of $k(\zeta)$ is prime to l and θ, ω and γ are prime to each other, then we have

$$\theta + \omega\zeta^a = \eta_a' \sigma_a^l \qquad (a = 0, 1, \ldots, l-1) \tag{5}$$

where η_a' is a unit and σ_a an integer in $k(\zeta)$. It is known that,

$$\sigma_a^l \equiv d_a \pmod{\lambda^l}$$

where d_a is a rational integer. In the relation (5) put $(-a)$ in lieu of $(l-a)$. Obviously then $d_a \equiv d_{-a} \pmod{\lambda^l}$. We have then

---

[3]) *Kummer*, 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.

(6) $$\frac{\theta + \omega\,\zeta^a}{\theta + \omega\,\zeta^{-a}} \equiv \frac{\eta'_a}{\eta'_{-a}} \pmod{\lambda^l}.$$

Now $\eta'_a = \zeta^{ak}\,\beta$ where β is a real unit in $k(\zeta)$ and k a rational integer, and since $(\theta + \omega\,\zeta^{-a})$ is obtained from $(\theta + \omega\,\zeta^a)$ by the substitution (ζ/ζ^{-1}) we have $\eta'_a/\eta'_{-a} = \zeta^{2ak}$ so that (6) gives[4])

$$\theta + \omega\,\zeta^a \equiv \zeta^{2ak}\;\theta + \omega\,\zeta^{2ak-a} \pmod{\lambda^l}$$

whence

$$\theta\,(1 - \zeta^{2ak}) \equiv \omega\,(\zeta^{(2k-1)a} - \zeta^a) \pmod{\lambda^l}$$

which holds for $a = 0, 1, \ldots, l-1$. Giving a these values in turn and adding the resulting congruences we obtain, using

$$\frac{\zeta^{sl} - 1}{\zeta^s - 1} = 0,\quad s \not\equiv 0 \pmod{l};$$

$l\theta \equiv 0 \pmod{\lambda^l}$, or $\theta \equiv 0 \pmod{\lambda}$ unless $2k - 1 \equiv 0 \pmod{l}$ or $k \equiv 0 \pmod{l}$. The first and third relations are impossible and the second used in (5) enables us to write this relation in the form

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

where η_a is a real unit in $k(\zeta)$, and σ_a is semi-primary.

Now assume in (4) that γ is a multiple of λ. One of the integers $\theta + \omega\,\zeta^i$; $i = 0, 1, \ldots, l-1$, is necessarily divisible by λ, say $\theta + \omega\,\zeta^a$, and since $\theta + \omega\,\zeta^a = \theta + \omega\,\zeta^b + \omega\,(\zeta^a - \zeta^b)$, then each $\theta + \omega\,\zeta^i$ is divisible by λ. For $i = 0$ we have $\theta + \omega$ divisible by λ^2, since θ and ω are semi-primary. But from $\theta + \omega\,\zeta^a = \theta + \omega + \omega\,(1 - \zeta)$ we infer that $\theta + \omega\,\zeta^a$ is divisible by λ but not by λ^2 for $a \not\equiv 0$. Hence for $a \not\equiv 0$ we have

(8) $$\frac{\omega + \zeta^a\,\theta}{1 - \zeta} = \eta''_a\,\varrho_a^l$$

---

[4]) The relation $\eta'_a = \zeta^{ak}\,\beta$ is obtained by reducing (6) modulo λ^2 by known methods. Cf. *Vandiver*, Algebraic Numbers, II, Bulletin, National Research Council, Washington, D. C., Febr., 1928, 62, p. 41.

which may be combined with (7) to form the relation

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

where η_a is a real unit and σ_a is an integer in $k(\zeta)$ and the ambiguous sign is $\pm$ according as γ is not or is divisible by λ. For a particular a in (8a) set $(-a)$ in place of a. These relations give, since η_a is real,

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

where σ_{-a} is obtained from σ_a by the substitution (ζ/ζ^{-1}). Now we consider this relation mod. $\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal divisor of $\theta + \omega\zeta$. We then obtain exactly as in a former paper of the writer's, if $a \neq \pm 1$ and $l > 3$,[5])

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

and this gives as on page 635 of the same reference

$$\left\{\frac{E_n}{\mathfrak{p}}\right\} = 1; \qquad n = 1, 2, \ldots, \frac{l-3}{2},$$

for $\mathfrak{p}$ a prime ideal divisor of $\theta + \omega\zeta$. Hence

$$\left\{\frac{E_n}{\sigma_1}\right\} = 1. \tag{9}$$

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

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

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

---

[5]) Transactions of the American Mathematical Society, vol. 31, (1929), p. 633.

Now by a theorem of Kummer[6])

$$\left\{\frac{E_n}{\sigma_1}\right\} = \zeta^T,$$

$$\text{where } T \equiv \frac{r^{2n}-1}{2n} B_n (-1)^{n-1} \left[\frac{d^{l-2n} \log \sigma_1 (e^v)}{dv^{l-2n}}\right] v = 0$$

mod. l, where if $\sigma_1(\zeta) = c_0 + c_1 \zeta + \ldots + c_{l-2} \zeta^{l-2}$ then $\sigma_1(e^v) = c_0 + c_1 + e^v + \ldots + c_{l-2} e^{v(l-2)}$, and since all of $B's$ are prime to l then (9) gives

$$\left[\frac{d^{l-2n} \log \sigma_1 (e^v)}{dv^{l-2n}}\right] \equiv (\text{mod } l) \quad v = 0 \tag{10}$$

$n = 1, 2, \ldots, \frac{l-1}{2}$; true for last n since σ_1 is semi-primary.

Consider the expression

$$\sigma_1 (e^v)\, \sigma_{-1}^{l-1} (e^v) = F(e^v).$$

We have $$\sigma_{-1} (e^v) = \sigma_1 (e^{-v}).$$

Whence using a result proved by the writer[7])

$$\left[\frac{d^{2k} \log F(e^v)}{dv^{2k}}\right] \equiv 0 \,(\text{mod } l) \quad v = 0$$

and therefore by combining with (10) we have

$$\left[\frac{d^h \log F(e^v)}{dv^h}\right] \equiv 0 \,(\text{mod } l) \quad v = 0$$

$h = 1, 2, \ldots l-2$. Consequently if $\sigma_1 \sigma_{-1}^{l-1} = a' + \lambda^s \rho$ where ρ is an integer in $k(\zeta)$, then $s \geqq l-1$, and if $\sigma_1 \sigma_{-1}^{l-1} = a' + \lambda^{l-1} \rho$ then this can be written in the form $a + \lambda^l \rho_2$ following a known result[8]).

---

[6]) Crelle, vol. 44, (1852), pp. 121—30. Cf. also *Hilbert*, Algebraische Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung, 1894, p. 471.

[7]) Transactions of the American Mathematical Society, vol. 31, (1929), p. 619, relation (3*e*).

[8]) *Landau*, Vorlesungen über Zahlentheorie, III, pp. 269 - 270.

Hence $\sigma_1 \sigma_{-1}^l \equiv \sigma_{-1} a \pmod{\lambda^l}$, and since $\sigma_{-1}^l \equiv a_1 \pmod{\lambda^l}$, we have $\sigma_1 a_1 \equiv \sigma_{-1} a \pmod{\lambda^l}$. Using $\sigma_1 \equiv \sigma_{-1} \pmod{\lambda}$ and reducing, modulo λ gives $a \equiv a_1 \pmod{l}$, whence

$$\sigma_1 \equiv \sigma_{-1} \pmod{\lambda^{l-1}}. \tag{10a}$$

As already noted in (7) and (8a), σ_a may be multiplied by an arbitrary power of ζ, hence we may define it as semi-primary, that is, of the form $c \pmod{\lambda^2}$, where c is a rational integer.

This shows that the relation (10a), which was proved only for $l > 3$, is also true for $l = 3$.

We then consider, using (8a)

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

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

$$\sigma_1^l \pm \sigma_{-1}^l = \eta_0'\,\sigma_0^l \tag{10b}$$

where η_0' is a unit in $k(\zeta)$. *This relation is not of the same form as* (4) *since* σ_1 *and* σ_{-1} *do not belong to the field* $\Omega(\zeta + \zeta^{-1})$, hence it requires a bit different treatment. Consider the case where we have the plus sign in the left hand member, that is when σ_0 is prime to λ. Since σ_1 and σ_{-1} are prime to each other, we obtain, in the manner that (5) was derived,

$$\sigma_1 + \zeta^a\,\sigma_{-1} = \zeta^s\,\xi_a'\,\tau_a^l$$

where ξ_a' is *a* real unit in $k(\zeta)$. Using (10a) we have

$$\sigma_1(1 + \zeta^a) \equiv \zeta^s\,\xi_a'\,h \pmod{\lambda^2}$$

where h and s are rational integers. Setting ζ^{-1} for ζ in this relation and dividing yields easily $s \equiv a/2 \pmod{l}$.

We may then write

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

where ξ_a is a real unit and τ_a is an integer in $\Omega(\zeta+\zeta^{-1})$, being unaltered by the substitution (ζ/ζ^{-1}). We also have for the case γ divisible by λ, by proceeding with (10b) as in the derivation of (8), the relation,

$$\sigma_1 - \zeta^a \sigma_{-1} = (1-\zeta^a)\,\xi_a\,\tau_a^l\,;\quad a \not\equiv 0.$$

Then we may write

$$\sigma_1 \pm \zeta^a \sigma_{-1} = (1 \pm \zeta^a)\,\xi_a\,\tau_a^l \tag{11}$$

the ambiguous signs being positive or negative according as γ is not or is divisible by λ. Using $\sigma_1 \equiv \sigma_{-1} \pmod{\lambda^{l-1}}$ we have, since this relation is true in both cases,

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

and also

$$\xi_{-a} \equiv \sigma_1 \pmod{\lambda^{l-1}}$$

Hence ξ_a/ξ_{-a} is primary. (Note that ξ_{-a} is not necessarily obtained from ξ_a by the substitution (ζ/ζ^{-1})). Since it is a unit and the field is regular,[9]) it is the l-th power of a unit in $k(\zeta)$. Taking $a = 1, -1$, in (11) together with

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

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 l-th power we obtain

$$\theta_1^l + \omega_1^l + \delta_1\,\gamma_1^l = 0 \tag{12}$$

which is the same form as (4), 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 (12) as were used in connection with (4) and we shall obtain the relation

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

[9]) *Landau*, l. c., p. 240.

of the same type as (4) and (12) but σ_0 is a divisor ot γ, and τ_0 is a divisor of σ_0 and hence γ_1 is a divisor of γ; and similarly γ_2 is a divisor of γ_1 and so on. Proceeding in this way we have an infinite series of ideals each containing less ideal prime factors than the preceding, which is impossible, unless at some stage, possibly in (4), we find that γ_s is a unit in $k(\zeta)$; but if this latter condition holds then we have for some s, since in (8) η_a is real,

$$\frac{\theta_s + \zeta\,\omega_s}{1 \pm \zeta} = \frac{\theta_s + \zeta^{-1}\,\omega_s}{1 \pm \zeta^{-1}}$$

which gives tor the plus sign in the denominators $\theta_s = \omega_s$ which is impossible, since, if applied to

$$\theta_s^l + \omega_s^l + \delta_s\,\gamma_s^l = 0 \tag{13}$$

we find $2\,\theta_s^l = -\delta_s\,\gamma_s^l$. The relation with the minus signs in the denominators gives $\theta_s = -\omega_s$ which substituted in (13) leads to $\gamma = 0$ and this is contrary to hypothesis.

The above argument assumed that in (4) $\theta\,\omega$ was prime to λ in $k(\zeta)$. If θ is divisible by λ then (4) gives $\omega^l \equiv -\delta\,\gamma^l \pmod{\lambda^l}$ whence δ is primary and is therefore the $l-th$ power of a unit and this case reduces to one of those already discussed. We may therefore state the Theorem. *The relation*

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

is impossible for integers α, β and γ in the field $\Omega(\zeta + \zeta^{-1})$ prime to each other and none zero; η being a given unit in this field and l a given regular prime.

The method above described leads to an extension of this theorem with η replaced by certain given non-units in $k(\zeta)$, to which general equation the method of proof properly belongs.

(Eingegangen den 8. September 1931)