



Exponential Numbers

E. T. Bell

The American Mathematical Monthly, Vol. 41, No. 7 (Aug. - Sep., 1934), 411-419.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9890%28193408%2F09%2941%3A7%3C411%3AEN%3E2.0.CO%3B2-2>

The American Mathematical Monthly is currently published by Mathematical Association of America.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/about/terms.html>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/journals/maa.html>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is an independent not-for-profit organization dedicated to creating and preserving a digital archive of scholarly journals. For more information regarding JSTOR, please contact support@jstor.org.

EXPONENTIAL NUMBERS

By E. T. BELL, California Institute of Technology

1. In some calculations which I was asked to check, a discrepancy was easily traced to the mathematical handbook* that had been used, where the MacLaurin expansion for $e^{\sin x}$ is given incorrectly. This suggested the desirability of having some readily applicable numerical check on the tedious algebra involved in expanding functions of the type $e^{f(x)}$ in MacLaurin series, when the expansion exists, and this in turn led to the definition of *exponential integers* and the investigation of their simpler arithmetical properties, with some of which this note is concerned. The simplest of the congruence properties developed in §6 are ample for checks on the series in the handbooks.

2. Let $e^{f(x)-f(0)}$ admit a MacLaurin expansion, and let both this series and the power series expansion

$$f(x) = c_0 + c_1x + \cdots + c_nx^n + \cdots$$

be absolutely convergent and differentiable term by term for $0 < |x| < k$. The coefficients $a_n (n \geq 0)$ in

$$e^{-f(0)}e^{f(x)} = a_0 + a_1x + a_2\frac{x^2}{2!} + \cdots + a_n\frac{x^n}{n!} + \cdots$$

will be called *the exponential numbers associated with* $c_0, c_1, \cdots, c_n, \cdots$, or, using the symbolic or umbral notation, we shall say that a is associated with c . When all the $a_n (n=0, 1, \cdots)$ associated with c are integers, we shall refer to them as *exponential integers*. It will be seen presently that a sufficient condition that the a_n be exponential integers is that $r!c_r$ be an integer for all integers $r > 0$.

To avoid questions of convergence we shall give (§4) an independent definition of exponential numbers and integers, in which no infinite process is involved. However, as the coefficients first presented themselves as above, we have given the preliminary definition. Some examples in §7 illustrate the general theorems of §§3-6.

3. For some $0 < |x| < k$ let both of the expansions

$$(3.1) \quad f(x) = \sum_{n=0} c_n x^n, \quad e^{-f(0)}e^{f(x)} = \sum_{n=0} \alpha_n \frac{x^n}{n!}$$

be absolutely convergent and termwise differentiable. Write

$$(3.2) \quad c_n \equiv a_n/n!,$$

and pass to the umbral notation. Then we have

$$(3.3) \quad f(x) = e^{ax}, \quad e^{-a_0}e^{e^{ax}} = e^{ax}.$$

* W. Láska, *Sammlung von Formeln*, Braunschweig, 1888-1894. This handbook is still quite popular with some physicists. The error mentioned is only one of several that reappear, without acknowledgement to Láska, in later handbooks.

By the usual rules of the umbral calculus¹ we may proceed to differentiate the second of these with respect to x , under the hypotheses on (3.1); the umbrae a , α are treated as ordinaries until symbolic formulas are translated back into ordinary notation, when a^n , α^n ($n=0, 1, \dots$) are replaced by a_n , α_n . It is to be noted that if ϕ , ψ are umbrae, and p , q ordinaries $\neq 0$,

$$(p\phi + q\psi)^0 = p^0\phi^0q^0\psi^0 = \phi^0\psi^0 = \phi_0\psi_0.$$

Thus we find

$$ae^{ax}e^{\alpha x} = \alpha e^{\alpha x}, \quad ae^{(a+\alpha)x} = \alpha e^{\alpha x},$$

and hence, by equating coefficients of x^n ,

$$(3.4) \quad a(a + \alpha)^n = \alpha^{n+1} (n \geq 0), \quad \alpha_0 = 1.$$

In ordinary notation, (3.4) is

$$(3.5) \quad \sum_{j=0}^n \binom{n}{j} a_{j+1} \alpha_{n-j} = \alpha_{n+1} (n \geq 0), \quad \alpha_0 = 1.$$

The special cases when $f(x)$ is an even, an odd function of x give recurrences which may be derived from (3.5). It is more interesting however to obtain them independently.

For some $0 < |x| < k_0$ let both of the expansions

$$(3.6) \quad h(x) = \sum_{n=0} b_{2n} x^{2n}, \quad e^{-h(0)} e^{h(x)} = \sum_{n=0} \eta_{2n} \frac{x^{2n}}{(2n)!}$$

be absolutely convergent and termwise differentiable, and similarly for $0 < |x| < k_1$ and

$$(3.7) \quad g(x) = \sum_{n=0} d_{2n+1} x^{2n+1}, \quad e^{g(x)} = \sum_{n=0} \omega_n \frac{x^n}{n!}.$$

Write

$$(3.8) \quad b_{2n} \equiv r_{2n}/(2n)!, \quad d_{2n+1} \equiv s_{2n+1}/(2n+1)!.$$

Then, from (3.6), (3.7), we have

$$(3.9) \quad h(x) = \cosh rx, \quad e^{-r_0} e^{\cosh rx} = \cosh \eta x,$$

$$(3.10) \quad g(x) = \sinh sx, \quad e^{\sinh sx} = e^{\omega x}.$$

Differentiation of these with respect to x gives

$$r \sinh rx \cosh \eta x = \eta \sinh \eta x, \quad s \cosh sx \cdot e^{\omega x} = \omega e^{\omega x};$$

whence

¹ Due to Blissard. There is a sufficient account of this calculus in E. Lucas' *Théorie des Nombres*, Chap. 13. In my *Algebraic Arithmetic*, 1927, I have developed this calculus further.

$$\begin{aligned} r[\sinh(r + \eta)x + \sinh(r - \eta)x] &= 2\eta \sinh \eta x, \\ s[e^{(\omega+s)x} + e^{(\omega-s)x}] &= 2\omega e^{\omega x}; \end{aligned}$$

which give the recurrences

$$(3.11) \quad r[(r + \eta)^{2n+1} + (r - \eta)^{2n+1}] = 2\eta^{2n+2} (n \geq 0), \quad \eta_0 = 1,$$

$$(3.12) \quad s[(\omega + s)^n + (\omega - s)^n] = 2\omega^{n+1} (n \geq 0), \quad \omega_0 = 1;$$

or, in ordinary notation,

$$(3.13) \quad \sum_{j=0}^n \binom{2n+1}{2j} r_{2n+2-2j} \eta_{2j} = \eta_{2n+2} (n \geq 0), \quad \eta_0 = 1,$$

$$(3.14) \quad \sum_{j=0}^{[n/2]} \binom{n}{2j} s_{2j+1} \omega_{n-2j} = \omega_{n+1} (n \geq 0), \quad \omega_0 = 1.$$

Instead of using the umbral calculus we might have obtained the recurrences (3.5), (3.13), (3.14) by Leibniz' theorem applied to the first derivatives of the generating functions for α , η , ω .

4. The arithmetical properties of the coefficients α , η , ω are implied by the recurrences and are independent of the origin of the α_n , η_n , ω_n as coefficients in power series. Accordingly we lay down the following *definitions of the exponential numbers α_n , η_n , ω_n ($n \geq 0$) of the first, second and third kinds respectively, associated respectively with c_n , b_{2n} , d_{2n+1} :*

$$(4.1) \quad a(a + \alpha)^n = \alpha^{n+1} (n \geq 0), \quad \alpha_0 = 1,$$

$$a_n \equiv n!c_n;$$

$$(4.2) \quad r[(r + \eta)^{2n+1} + (r - \eta)^{2n+1}] = 2\eta^{2n+2} (n \geq 0), \quad \eta_0 = 1,$$

$$r_{2n} \equiv (2n)!b_{2n};$$

$$(4.3) \quad s[(\omega + s)^n + (\omega - s)^n] = 2\omega^{n+1} (n \geq 0), \quad \omega_0 = 1,$$

$$s_{2n+1} \equiv (2n + 1)!d_{2n+1}.$$

The equivalents of (4.1), (4.2), (4.3) in ordinary notations are (3.5), (3.13), (3.14). As already indicated, (4.2), (4.3) are special cases of (4.1).

When the exponential numbers are integers, we shall call them *exponential integers*.

A sufficient condition that the α_n ($n \geq 0$) be integers is that all $j!c_j$ ($j > 0$) be integers, by (4.1). The corresponding condition for η_{2n} ($n \geq 0$) is that all $(2j)!b_{2j}$ ($j > 0$) be integers; and for ω_n ($n \geq 0$), that all $(2j+1)!b_{2j+1}$ ($j \geq 0$) be integers.

To extend the recurrences (4.1)–(4.3), let

$$P(x) \equiv h_0 + h_1x + \cdots + h_mx^m, \quad h_m \neq 0,$$

be any polynomial of degree m in x . Then, by (4.1), we have

$$a \sum_{n=0}^m h_n(a + \alpha)^n = \alpha \sum_{n=0}^m h_n \alpha^n,$$

and therefore

$$(4.4) \quad aP(a + \alpha) = \alpha P(\alpha).$$

In the same way, from (4.2), we find

$$(4.5) \quad r[(r + \eta)P((r + \eta)^2) + (r - \eta)P((r - \eta)^2)] = 2\eta^2 P(\eta^2),$$

and from (4.3),

$$(4.6) \quad s[P(\omega + s) + P(\omega - s)] = 2\omega P(\omega).$$

Finally, $P(x)$ may be replaced by a power series, provided the series in (4.4)–(4.6) are then convergent.¹

The generating function of ω being odd, the numbers ω satisfy a bilinear recurrence,²

$$(4.7) \quad (\omega' - \omega'')^{2m} = 0 (m > 0), \quad \omega' \equiv \omega \equiv \omega'',$$

or, in ordinary notation,

$$(4.8) \quad 2 \sum_{j=0}^{m-1} (-1)^j \binom{2m}{j} \omega_j \omega_{2m-j} + (-1)^m \omega_m^2 = 0 (m > 0).$$

This can be proved from (4.1), or as suggested in the footnote.

5. The simplest arithmetical properties of exponential integers follow from theorems concerning the residues of binomial coefficients to a prime modulus.³ We shall require the following.

Let p be prime. Then

$$(5.1) \quad \binom{p}{r} \equiv 0 \pmod{p}, \quad 0 < r < p; \quad \binom{p}{p} \equiv \binom{p}{0} \equiv 1 \pmod{p}.$$

¹ It is sometimes said that a result such as (4.4) is a generalization of the result such as (4.1) from which it is derived. This is incorrect: (4.1) and (4.4) express the same fact; they are logically equivalent, for it is obvious that each implies the other. Nevertheless (4.4) is sometimes more suggestive than (4.1).

² Such recurrences are most readily obtained by the symbolic method. Here

$$1 = e^{g(x)} e^{-g(x)}, = e^{g(x)+g(-x)}$$
since $g(x)$ is odd; hence

$$1 = e^{(\omega' - \omega'')x},$$

where $\omega'^m \equiv \omega_m$, $\omega''^m \equiv \omega_m$. Hence $(\omega' - \omega'')^0 = 1$, $(\omega' - \omega'')^n = 0$ ($n > 0$). If n is odd, the last is a trivial identity. But if $n = 2m$, we have (4.8). The infinite formal processes used in this derivation are independent of questions of convergence, and have been validated in my book cited.

³ See Lucas, loc. cit., §228; several are due to Lucas. See also Dickson, *History of the Theory of Numbers*, vol. 1, Chap. 9. The convenient symbolic expression (5.4) for the residue of $(\lambda + \mu)^N$ modulo p was given in my paper on Anharmonic Polynomials, *Transactions of the American Mathematical Society*, vol. 34 (1922), p. 109.

It will be convenient to use the customary extension of the notation $\binom{m}{n}$ to negative values of m ,

$$\binom{-m}{0} = 1, \quad \binom{-m}{n} = (-m)(-m-1)\cdots(-m-n+1)/n!$$

for $m > 0, n > 0$. The next residue theorem may then be written

$$(5.2) \quad \binom{p-j}{h} \equiv \binom{-j}{h} \pmod{p}, \quad 0 \leq h < p-j < p.$$

The third residue theorem is

$$(5.3) \quad \binom{m}{n} \equiv \binom{m_1}{n_1} \binom{m_1'}{n_1'} \pmod{p},$$

$$m > 0, n \geq 0, m = m_1 p + m_1', n = n_1 p + n_1',$$

$$0 \leq m_1', n_1' < p; \binom{r}{s} = 0 \text{ if } s > r.$$

A similar reduction may be applied to $\binom{m_i}{n_i}$, provided at least one of m_i, n_i , exceeds p , and so on.

To pass to the general case, we apply (5.3) to $(\lambda + \mu)^N$, where λ, μ are either ordinaries or umbrae (the latter includes the former as a special case), and N is an integer > 0 . Let

$$N = g_n p^n + g_{n-1} p^{n-1} + \cdots + g_1 p + g_0,$$

$$0 \leq g_j < p (j = 0, \cdots, n-1), g_n \neq 0, g_n < p,$$

be the expression of N in the scale of p . Then we find easily the following congruences,

$$(5.4) \quad (\lambda \pm \mu)^N \equiv \sum_{i=0}^n (\lambda^{p^i} \pm \mu^{p^i})^{g_i} \pmod{p},$$

(the upper or the lower signs being taken throughout), in which, if λ, μ are umbrae, all the indicated binomial expansions and subsequent multiplications are to be performed as in common algebra before exponents are lowered.

6. Let α, η, ω in §4 be exponential integers, and let p be prime. Then, applying (5.1) to §4, we get

$$(6.1) \quad a_1 \alpha_p + a_{p+1} \equiv \alpha_{p+1} \pmod{p},$$

$$r_{p+1} \equiv \eta_{p+1} \pmod{p}, \quad p > 2,$$

$$(6.3) \quad s_1 \omega_p \equiv \omega_{p+1} \pmod{p}, \quad p > 2.$$

It is easily seen that the second and third of these are included in the first, and similarly for all following triads of congruences in this section.

From the recurrences in §4 written in ordinary notation, we get the following by (5.2),

$$(6.4) \quad a_{p-k+1} + \sum_{j=0}^{p-k-1} \binom{-k}{j} a_{j+1} \alpha_{p-k-j} \equiv \alpha_{p-k+1} \pmod{p},$$

$$0 < p - k < p;$$

$$(6.5) \quad \sum_{j=0}^{(p-1)/2-k} \binom{-2k}{2j} r_{p+1-2k-2j} \eta_{2j} \equiv \eta_{p+1-2k} \pmod{p},$$

$$p > 2, 0 < p - 2k < p;$$

$$(6.6) \quad \sum_{j=0}^{[(p-2k)/2]} \binom{-2k}{2j} s_{2j+1} \omega_{p-2k-2j} \equiv \omega_{p-2k+1} \pmod{p},$$

$$p > 2, 0 < p - 2k < p;$$

$$s_{p-2h} + \sum_{j=0}^{(p-3)/2-h} \binom{-2h-1}{2j} s_{2j+1} \omega_{p-2h-1-2j} \equiv \omega_{p-2h} \pmod{p},$$

$$p > 2, 0 \leq h \leq (p-3)/2.$$

The corresponding congruence from (4.8) gives a theorem on quadratic residues.

The following very special cases of (5.4) applied to §4 will suffice.

$$(6.7) \quad a(a^p + \alpha^p)(a + \alpha)^h \equiv \alpha^{p+h+1} \pmod{p},$$

$$(6.8) \quad r[(r^p + \eta^p)(r + \eta)^{2h} + (r^p - \eta^p)(r - \eta)^{2h}] \equiv 2\eta^{p+2h+1} \pmod{p}, \quad p > 2,$$

$$(6.9) \quad s[(\omega^p + s^p)(\omega + s)^h + (\omega^p - s^p)(\omega - s)^h] \equiv 2\omega^{p+h+1} \pmod{p};$$

(6.7), (6.9) are valid for $0 \leq h < p$, (6.8) for $0 \leq 2h < p$. For $h=0$, these become (6.1)–(6.3).

7. The coefficients in the MacLaurin expansions in §3 can be calculated successively by the recurrences in §4. If desired, the recurrences can be solved to give the coefficients explicitly as determinants; the results, however, are useless for computation and appear to have no value for the deduction of arithmetical theorems. Herschel's theorem in the calculus of finite differences is sometimes useful in furnishing manageable explicit forms from which something can be inferred. If $\phi(e^t)$ has a MacLaurin expansion, Herschel's theorem¹ gives the expansion in the form

$$\phi(e^t) = \phi(1) + \phi(E)0 \cdot t + \phi(E)0^2 \cdot \frac{t^2}{2!} + \dots \equiv \phi(E)e^{0 \cdot t},$$

where $E \equiv 1 + \Delta$ is the usual operator in finite differences.

The simplest example is (ϵ umbral)

$$e^{-1}e^{\epsilon x} = e^{\epsilon x}, \quad \epsilon_0 = 1, \quad \epsilon_n \equiv \left(1 + \frac{\Delta}{1!} + \frac{\Delta^2}{2!} + \dots + \frac{\Delta^n}{n!}\right) 0^n.$$

¹ See Boole, *Finite Differences*, (reprinted by Stechert), p. 24. The so-called "differences of nothing" required in numerical work are tabulated for a short range by Steffensen, *Interpolation* (Williams and Wilkins, 1927), p. 55.

But (a well known formula),

$$\frac{\Delta^n 0^m}{n!} = \frac{1}{n!} \sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r)^m;$$

whence,

$$\epsilon_n = \sum_{s=1}^n \frac{1}{(s-1)!} \left[\sum_{r=0}^{s-1} (-1)^r \binom{s-1}{r} (s-r)^{n-1} \right], \quad n > 0.$$

The ϵ 's have interesting connections with the numbers of Bernoulli and Stirling but these need not be discussed now. Using Steffensen's table (loc. cit.) for $\Delta^n 0^m/n!$ we get

$$\epsilon_1 = 1, \epsilon_2 = 2, \epsilon_3 = 5, \epsilon_4 = 15, \epsilon_5 = 52, \epsilon_6 = 203, \epsilon_7 = 877,$$

$$\epsilon_8 = 4140, \epsilon_9 = 21147, \epsilon_{10} = 115975.$$

Referring to (4.1), we see that here $a_n = 1 (n \geq 0)$, and hence the congruence (6.1) becomes, for $\alpha \equiv \epsilon$,

$$\epsilon_p + 1 \equiv \epsilon_{p+1} \pmod{p}.$$

The cases $k=1, 2$ of (6.4) give

$$1 + \sum_{j=0}^{p-2} (-1)^j \epsilon_{p-1-j} \equiv \epsilon_p \pmod{p},$$

$$1 + \sum_{j=0}^{p-3} (-1)^j (j+1) \epsilon_{p-2-j} \equiv \epsilon_{p-1} \pmod{p}, \quad p > 2;$$

while (6.7) with $h=1$ gives

$$2 + \epsilon_p + \epsilon_{p+1} \equiv \epsilon_{p+2} \pmod{p},$$

and with $h=2$,

$$5 + \epsilon_p + 2\epsilon_{p+1} + \epsilon_{p+2} \equiv \epsilon_{p+3} \pmod{p}, \quad p > 2,$$

and so on. These are verified by the above numerical values. Incidentally, the check renders probable the accuracy of Steffensen's table.

Further simple illustrations of expansions of the type (3.1) giving sequences of exponential integers defined by recurrences of the type (3.4) or (4.1) are given by $e^{f(x)}$ where $f(x) = \tan x$ or $\arctan x$.

In (4.2) take $r_{2n} = (-1)^n$, and therefore $b_{2n} = (-1)^n/(2n)!$. Hence, in (3.6), $h(x) = \cos x$. The coefficients can be calculated by (4.2) or (3.13). Write $\eta \equiv \kappa$ in this case. Then

$$\sum_{j=0}^n (-1)^j \binom{2n+1}{2j} \kappa_{2j} = (-1)^{n+1} \kappa_{2n+2},$$

and we find

$$\kappa_0 = 1, \kappa_2 = -1, \kappa_4 = 4, \kappa_6 = -31, \kappa_8 = 379, \kappa_{10} = -6556,$$

which are sufficient for verifying the congruences. Thus (6.2) becomes

$$\kappa_{p+1} \equiv (-1)^{(p+1)/2} \pmod{p}, \quad p > 2,$$

which is checked, and similarly for (6.5) with $k=1$,

$$\sum_{j=0}^{(p-3)/2} (-1)^j (2j+1) \kappa_{2j} \equiv (-1)^{(p-1)/2} \kappa_{p-1} \pmod{p}, \quad p > 2,$$

and for (6.8) with $h=1$,

$$\kappa_{p+3} \equiv 2[(-1)^{(p+3)/2} - \kappa_{p+1}] \pmod{p}, \quad p > 2.$$

Combining the first and third of these we get the simpler result

$$\kappa_{p+3} \equiv 4(-1)^{(p+3)/2} \pmod{p}, \quad p > 2.$$

As an example of the remaining type, take $s_{2n+1} = (-1)^n$ in (4.3), and hence $g(x) = \sin x$ in (3.7). Write $\omega \equiv \sigma$ for this choice, and calculate the σ by (3.14). Then

$$\begin{aligned} \sigma_0 = 1, \sigma_1 = 1, \sigma_2 = 1, \sigma_3 = 0, \sigma_4 = -3, \sigma_5 = -8, \sigma_6 = -3, \sigma_7 = 56, \\ \sigma_8 = 217, \sigma_9 = 64, \sigma_{10} = -2951, \sigma_{11} = -12672, \sigma_{12} = 5973. \end{aligned}$$

The congruences are, from (6.3),

$$\sigma_p \equiv \sigma_{p+1} \pmod{p}, \quad p > 2;$$

from the first of (6.6), with $k=1$,

$$\sum_{j=0}^{[(p-2)/2]} (-1)^j (2j+1) \sigma_{p-2-2j} \equiv \sigma_{p-1} \pmod{p}, \quad p > 2,$$

and from the second, with $h=1$,

$$(-1)^{(p-3)/2} + \sum_{j=0}^{(p-5)/2} (-1)^j (j+1)(2j+1) \sigma_{p-3-2j} \equiv \sigma_{p-2} \pmod{p}, \quad p > 4;$$

while from (6.9) with $h=1$ we get

$$\sigma_{p+1} + (-1)^{(p+1)/2} \equiv \sigma_{p+2} \pmod{p}, \quad p > 2.$$

All of the congruences are checked by the above numerical values.

From the well known expansions for $e^{x \cos \phi}$, $e^{x \sin \phi}$ in series of Bessel coefficients, we find immediately the following independent expressions for the integers κ , σ :

$$\kappa_{2t} = e^{-1} (-1)^t \sum_{s=1}^{\infty} i^s J_s(-i) s^{2t} (t > 0),$$

$$\sigma_{2t} = 2(-1)^t \sum_{s=0}^{\infty} (-1)^s J_{2s}(-i)(2s)^{2t} (t > 0),$$

$$\sigma_{2t+1} = 2i(-1)^t \sum_{s=1}^{\infty} (-1)^s J_{2s-1}(-i)(2s-1)^{2t+1} (t \geq 0),$$

where $i \equiv (-1)^{1/2}$.

ON FERMAT'S LAST THEOREM¹

By GLENN JAMES, University of California at Los Angeles

1. Introduction. We consider the equation

$$(1) \quad x^n + y^n = z^n,$$

where n is an odd prime integer, x, y, z are positive integers relatively prime in pairs and $y > x$. There is no loss of generality in this last restriction, since if $x = y, z$ cannot be an integer. In this paper we confine ourselves to the so-called "first case," namely that in which $x, y, z \not\equiv 0 \pmod n$. Certain intervals, in which $z - y$ must lie if x, y, z satisfy (1), are easily established by analytic methods. For instance²

$$(2) \quad 2[1 - (1/2)^{1/n}]x^n/z^{n-1} > z - y > x^n/(nz^{n-1}).$$

This paper is a first step in an attempt to prove Fermat's Last Theorem by excluding $z - y$ from some such interval by means of number theory properties of x, y, z and n . Our central theorem states that (1) fails unless

$$z - y \geq (cn + 1)^n, \quad c \geq 2.$$

This theorem, incidentally, completes the various attempts to prove that x, y , and z are composite.³

Another by-product is a proof of the cubic case, which seems to be new and suggests another possible point of attack on the general problem.

2. Preliminary Considerations. It was proved by P. Barlow⁴ that if (1) holds when $x, y, z \not\equiv 0 \pmod n$, then

$$(3) \quad x + y = r^n, \quad z - x = s^n, \quad z - y = t^n$$

¹ Presented to the American Mathematical Society, August 31, 1932.

² To establish these limits one writes (1) in the form

$$x^n + [z - (z - y)]^n = z^n \text{ or } (x^n/z^n) + [1 - (z - y)/z]^n = 1.$$

Putting v for x^n/z^n and αv for $(z - y)/z$ we get $v + (1 - \alpha v)^n = 1$. Whence $\alpha = (1/v)[1 - (1 - v)^{1/n}] = j(v)$. Now, $1/2 > v > 0$, $j(0) = 1/n$ and $j'(v) > 0$, whence $2[1 - (1/2)^{1/n}] > \alpha > 1/n$. From this (2) readily follows.

³ H. F. Talbot, Trans. Royal Society, Edinburgh, vol. 21 (1857), pp. 403-6, and others proved that x, y, z are composite unless $z - y$ is unity. We have removed this troublesome case.

⁴ Jour. Nat. Phil. Chem. and Arts., vol. 27 (1810), p. 193.