evaluated for $w=0$; *in* (30) *we make special conventions of the same type as those made in connection with* (13).

In connection with Theorem 4, it is of interest to note the unexpanded forms corresponding to (20), namely,

$$Y_{\infty j} = \sum_{v=1}^{j} z^{-a_v} \frac{(j-1)!}{(j-v)!} \left[\frac{\partial^{j-v}}{\partial w^{j-v}} z^{-w} F_v(w, z) \right]_{w=0}, \qquad j = 1, 2, \cdots, s. \tag{31}$$

THE COLLEGE OF ST. FRANCIS

ON THE FIRST CASE OF FERMAT'S LAST THEOREM*

BARKLEY ROSSER

We prove the following theorem:

THEOREM. *If* p *is an odd prime,* α, β, *and* γ *are integers in the field of the* p*th roots of unity,* $\alpha\beta\gamma$ *is prime to* p, *and*

$$\alpha^p + \beta^p + \gamma^p = 0,$$

then $p \geqq 8{,}332{,}403$.

As ordinary integers are integers in the field of the pth roots of unity, we infer the following:

COROLLARY. *The equation*

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

has no solution in integers prime to p *if* p *is an odd prime less than* 8,332,403.

To abbreviate statements, we shall say that an odd prime p is improper if there are integers α, β, and γ in the field of the pth roots of unity such that $\alpha\beta\gamma$ is prime to p and

$$\alpha^p + \beta^p + \gamma^p = 0.$$

Then the theorem to be proved can be stated in the form:

THEOREM. *There are no improper odd primes less than* 8,332,403.

The proof is based on a theorem of Morishima† which, in our

* Presented to the Society, February 25, 1939.

† Taro Morishima, *Über die Fermatsche Vermutung*, Japanese Journal of Mathematics, vol. 11 (1935), pp. 241–252. Earlier results of a similar nature are due to Pollaczek, Frobenius, Vandiver, Mirimanoff, and Wieferich. Compare Dickson's *History of the Theory of Numbers.*

terminology, can be stated as follows:

THEOREM. *If p is an improper odd prime, then for each prime $m \leqq 31$,*

$$m^{p-1} \equiv 1 \pmod{p^2}.$$

Let us say that x is an F number relative to p if

$$x^{p-1} \equiv 1 \pmod{p^2}.$$

Let g be a primitive root modulo p^2. Then the only powers of g which are F numbers relative to p are powers whose exponents are multiples of p. Therefore, there are exactly $p-1$ residues of p^2 which are F numbers relative to p. Hence, there are exactly $p-1$ integers between $-p^2/2$ and $p^2/2$ which are F numbers relative to p. However, $-x$ is an F number relative to p if x is. This proves the following lemma:

LEMMA 1. *There are exactly $(p-1)/2$ positive integers less than $p^2/2$ which are F numbers relative to p.*

Now suppose that p is an improper odd prime. Then, by Morishima's theorem, every prime not greater than 31 is an F number relative to p. However, the product of two F numbers is an F number. Hence, every integer having no prime factors greater than 31 is an F number relative to p. Therefore, by Lemma 1, there can be at most $(p-1)/2$ positive integers less than $p^2/2$ which have no prime factor greater than 31. So if we define $\phi_n(N)$ as the number of positive integers not greater than N having no prime factor greater than the nth prime, we may state the next lemma:

LEMMA 2. *If p is an improper odd prime, then*

$$2\phi_{11}(p^2/2) \leqq p - 1.$$

We seek a lower bound for $\phi_{11}(x)$. To this end we prove the following statement:

LEMMA 3. *If $n \geqq 1$, $a > 1$, $N \geqq 1$, then*

$$\sum_{s=0}^{[\log N/\log a]} [\log (N/a^s)]^n > \frac{1}{2} (\log N)^n + \frac{(\log N)^{n+1}}{(n+1) \log a}.$$

The theorem is obviously independent of the base of the logarithms. However, to simplify later computations, we shall take all logarithms to the base 10.

PROOF. Let w denote $[\log N/\log a]$. Let $f(x)$ be the function whose graph consists of the series of straight lines joining

$$(0, [\log (N/a^0)]^n) \quad \text{and} \quad (1, [\log (N/a^1)]^n),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$
$$(w-1, [\log (N/a^{w-1})]^n) \quad \text{and} \quad (w, [\log (N/a^w)]^n),$$
$$(w, [\log (N/a^w)]^n) \quad \text{and} \quad (w+1, 0).$$

Let $g(x)$ be the step function $(\log N - [x] \log a)^n$. Then

$$\sum_{s=0}^{w} [\log (N/a^s)]^n = \int_0^{w+1} g(x)dx = \int_0^{w+1} (g(x) - f(x))dx + \int_0^{w+1} f(x)dx.$$

For x an integer, $f(x) = (\log N - x \log a)^n$. As the second derivative of $(\log N - x \log a)^n$ is nonnegative, we have that

$$f(x) \geqq (\log N - x \log a)^n, \qquad 0 \leqq x \leqq \log N/\log a.$$

Therefore,

$$\sum_{s=0}^{w} [\log (N/a^s)]^n \geqq \int_0^{w+1} (g(x) - f(x))dx + \int_0^{\log N/\log a} (\log N - x \log a)^n dx$$
$$= \int_0^{w+1} (g(x) - f(x))dx + \frac{(\log N)^{n+1}}{(n+1) \log a}.$$

As the area between $f(x)$ and $g(x)$ is a series of triangles whose bases are all unity and whose combined altitude equals $(\log N)^n$,

$$\int_0^{w+1} (g(x) - f(x))dx = (\log N)^n/2.$$

DEFINITION. *Let $f_n(x)$ be a polynomial in x defined by the following recursion on n:*

$$f_1(x) = \frac{x}{\log 2}, \qquad f_{n+1}(x) = \frac{1}{\log p_{n+1}} \int_0^x f_n(y)dy + \frac{1}{2} f_n(x).$$

LEMMA 4. *If $x \geqq 1$, then $\phi_n(x) > f_n(\log x)$.*

PROOF BY INDUCTION ON n. If $n=1$, put $w = [\log x/\log 2]$. Then $2^0, 2^1, 2^2, \cdots, 2^w$ are all not greater than x, so that

$$\phi_1(x) = w + 1 > \log x/\log 2 = f_1(\log x).$$

Assume that the theorem is true for n. Then $\phi_{n+1}(x)$ is the number of integers not greater than x, having no prime factor greater than p_{n+1}. These may be counted as follows. First count the ones not di-

visible by p_{n+1}. There are $\phi_n(x)$ of these. Then count the ones divisible by p_{n+1}, but not by $(p_{n+1})^2$. There are $\phi_n(x/p_{n+1})$ of these, and so on. Hence, if $w = [\log x/\log p_{n+1}]$, then

$$\phi_{n+1}(x) = \sum_{s=0}^{w} \phi_n(x/(p_{n+1})^s) > \sum_{s=0}^{w} f_n(\log x/(p_{n+1})^s).$$

By Lemma 3 and the definition of $f_{n+1}(x)$, we get

$$\phi_{n+1}(x) > f_{n+1}(\log x).$$

By successively computing $f_1(x)$, $f_2(x)$, $\cdots$, we computed $f_{11}(x)$. The result was

$$\begin{aligned} f_{11}(x) = {} & 0.00000005447197741x^{11} + 0.000003295918757x^{10} \\ & + 0.00008081950130x^9 + 0.001046349948x^8 \\ & + 0.007817038320x^7 + 0.03463081936x^6 \\ & + 0.09016427288x^5 + 0.1322851609x^4 \\ & + 0.1003412456x^3 + 0.03325580732x^2 \\ & + 0.003244070402x. \end{aligned}$$

Let $\Sigma_1, \Sigma_2, \cdots, \Sigma_{n-1}$ denote the elementary symmetric functions of $\log 3, \log 5, \log 7, \cdots, \log p_n$.

LEMMA 5.

$$f_n(x) = \frac{1}{n!(\log 2)\Sigma_{n-1}} \left\{ x^n + \frac{n\Sigma_1}{2} x^{n-1} + \frac{n(n-1)\Sigma_2}{2^2} x^{n-2} + \cdots + \frac{n(n-1)\cdots(2)\Sigma_{n-1}}{2^{n-1}} x \right\}.$$

PROOF BY INDUCTION ON n. If $n = 1$, the proof is simple. Suppose the lemma true for n. Let $\Sigma_1^*, \Sigma_2^*, \cdots, \Sigma_n^*$ denote the elementary symmetric functions of $\log 3, \log 5, \log 7, \cdots, \log p_{n+1}$. Then

$$\Sigma_1^* = \Sigma_1 + \log p_{n+1}, \qquad \Sigma_2^* = \Sigma_2 + \Sigma_1 \log p_{n+1}, \cdots,$$
$$\Sigma_{n-1}^* = \Sigma_{n-1} + \Sigma_{n-2} \log p_{n+1}, \quad \Sigma_n^* = \Sigma_{n-1} \log p_{n+1}.$$

From these relations, it readily follows that $f_{n+1}(x)$ has the desired form.

The value computed for $f_{11}(x)$ was checked by use of the above explicit formula. The computations were performed on a ten place machine, the tenth place being rounded off. This produced unavoidable errors in the tenth significant figure. However, the largest discrepancy

which occurred between the two computed values of $f_{11}(x)$ was five units in the tenth significant figure. This seemed a satisfactory check.

We now prove the main theorem. Let p be an improper odd prime. As $2^2 \equiv 4 \pmod 9$, $2^4 \equiv 16 \pmod{25}$, and $2^6 \equiv 15 \pmod{49}$, p is not 3, 5, or 7. So* $p \geqq 11$ and $p^2/2 > 60$. However, $2\phi_{11}(60) = 108$. So by Lemma 2, $p \geqq 109$ and $p^2/2 > 5940$. Therefore by Lemma 4, $2\phi_{11}(p^2/2) > 689.18$. So $p \geqq 691$ and $p^2/2 > 238{,}740$. Similarly, we get $2\phi_{11}(p^2/2) > 6993.24$, $p \geqq 6995$; $2\phi_{11}(p^2/2) > 67{,}682.70$, $p \geqq 67{,}684$; $2\phi_{11}(p^2/2) > 411{,}815.08$, $p \geqq 411{,}817$. Now

$$\frac{d}{dx}(f_{11}(\log(x^2/2))) < \frac{22(0.4343)}{x \log(x^2/2)} f_{11}(\log(x^2/2)).$$

If $x \geqq 411{,}817$, then $22(0.4343)/\log(x^2/2) < 1$, and so

$$\frac{d}{dx}(2f_{11}(\log(x^2/2))) < \frac{1}{x} 2f_{11}(\log(x^2/2)).$$

Hence, if $x > 2f_{11}(\log(x^2/2))$ and $411{,}817 \leqq x < y$, then $y > 2f_{11}(\log(y^2/2))$. However, for $x = 8{,}332{,}366$, we have $2f_{11}(\log(x^2/2)) = 8{,}332{,}366.22$. So for $411{,}817 \leqq x \leqq 8{,}332{,}366$,

$$2f_{11}(\log(x^2/2)) > x.$$

Therefore $p - 1 > 8{,}332{,}366$ and $p \geqq 8{,}332{,}403$.

CORNELL UNIVERSITY

* It was shown by Meissner (Sitzungsberichte der Akademie der Wissenschaften, Berlin, vol. 35 (1913), pp. 663–667) and Beeger (Messenger of Mathematics, vol. 55 (1925), pp. 17–26 and Nieuw Archief voor Wiskunde, vol. 20 (1939), pp. 51–54) that 1093 and 3511 are the only primes p less than 16,000 such that $2^{p-1} \equiv 1 \pmod{p^2}$. From this, one could quickly conclude that an improper odd prime must be greater than 16,000, because the only possibilities below 16,000 are 1093 and 3511, and we eliminate these as follows: $3^7 = 1 + 2 \cdot 1093$, so that $3^{1092} = (1 + 2 \cdot 1093)^{156} \equiv 1 + 312 \cdot 1093 \pmod{1093^2}$. Hence, 1093 is not improper. If 3511 were improper, we would have $3510^{3510} = (2 \cdot 3^2 \cdot 5 \cdot 13)^{3510} \equiv 1 \pmod{3511^2}$ by Morishima's theorem. However, $3510^{3510} = (3511 - 1)^{3510} \equiv 1 - 3510 \cdot 3511 \pmod{3511^2} \equiv 1 + 3511 \pmod{3511^2}$. As a matter of interest, it might be noted that one can prove that $3^{3510} \equiv 1 + 7 \cdot 3511 \pmod{3511^2}$.