A NEW LOWER BOUND FOR THE EXPONENT IN THE FIRST CASE OF FERMAT'S LAST THEOREM[1]

BARKLEY ROSSER

1. **Introduction.** In this paper is proved the theorem: If p is an odd prime and

$$a^p + b^p + c^p = 0 \tag{1}$$

has a solution in integers prime to p, then $p > 41{,}000{,}000$.

It seems certain that still higher lower bounds for p can be deduced by the methods of this paper. However an argument is given which makes it seem unlikely that an indefinitely high lower bound can be so deduced.

2. **Preliminary results.** Unless otherwise specified, we shall assume that p is an odd prime for which (1) can be satisfied by integers prime to p. Hence[2] $p > 8{,}000{,}000$. Also $x \equiv y$ shall denote $x \equiv y \pmod{p}$. Also any statement regarding factorization of a polynomial is to be understood modulo p.

Morishima has proved[3] that for each odd prime $m \leqq 43$, there is a t ($t \not\equiv 0$, $\not\equiv 1$) such that each of the values

$$t, \quad \frac{1}{t}, \quad 1 - t, \quad \frac{1}{1 - t}, \quad \frac{t - 1}{t}, \quad \frac{t}{t - 1} \tag{2}$$

satisfies each of the following relations when substituted for x:

$$\{(m^{p-1} - 1)/p\}(x^{m-1} - 1) \equiv 0, \tag{3}$$

$$x^4 \not\equiv 1, \tag{4}$$

$$x^6 \not\equiv 1. \tag{5}$$

Morishima further proved that for each odd prime $m \leqq 31$, there is no t such that the values in (2) satisfy (4), (5), and

$$x^{m-1} \equiv 1. \tag{6}$$

Hence for such m's, $(m^{p-1} - 1)/p \equiv 0$. That is

$$m^{p-1} \equiv 1 \pmod{p^2}. \tag{7}$$

[1] Presented to the Society, September 8, 1939.

[2] Barkley Rosser, *On the first case of Fermat's last theorem*, this Bulletin, vol. 45 (1939), pp. 636–640. This paper will be referred to as I.

[3] Taro Morishima, *Über den Fermatschen Quotienten*, Japanese Journal of Mathematics, vol. 8 (1931), pp. 159–173.

In this paper we shall use the fact that $p > 8{,}000{,}000$ to prove that, for $m = 37$ or 41, there is no t such that the values in (2) satisfy (4), (5), and (6). Hence we can conclude that (7) holds for each prime $m \leqq 41$ (since it is well known that (7) holds for $m = 2$). This fact is then used to prove that $p > 41{,}000{,}000$.

Until §6, we assume that m is an odd prime, $n = (m-1)/2$, and that a t exists such that the values of (2) satisfy (4), (5), and (6).

We reduce the consideration of (4), (5), and (6) to a familiar theory[4] by replacing t by $-a$. Then since the polynomials in (4), (5), and (6) are all even functions, we see that each of

$$(8)\qquad \begin{array}{l} a, \ \dfrac{1}{a}, \ -1-a, \ \dfrac{1}{-1-a}, \ \dfrac{1+a}{-a}, \ \dfrac{-a}{1+a}, \\ -a, \ \dfrac{1}{-a}, \ 1+a, \ \dfrac{1}{1+a}, \ \dfrac{1+a}{a}, \ \dfrac{a}{1+a}, \end{array}$$

must satisfy (4), (5), and (6). Put

$$b = \frac{-a^6 - 3a^5 + 5a^3 - 3a - 1}{a^2(a+1)^2},$$

and define

$$f(x) = (x-a)(x-1/a)(x+1+a)(x+1/(1+a))(x+(1+a)/a)(x+a/(1+a)).$$

Then $f(x) = x^6 + 3x^5 + bx^4 + (2b-5)x^3 + bx^2 + 3x + 1$.

We shall prove in §3 that $f(x)f(-x)$ has no multiple factors if $m \leqq 67$. So for $m \leqq 67$, $f(x)f(-x)$ must divide $x^{m-1} - 1$. Also note that $f(x)f(-x)$ has no factors in common with either $x^4 - 1$ or $x^6 - 1$, by (4) and (5).

Lemma 1. *If $\phi(x)$ is a polynomial in x and $f(x)f(-x)$ has no multiple factors, then a n.a.s.c. that $f(x)f(-x)$ divide $\phi(x)$ is that $f(x)$ divide both $\phi(x)$ and $\phi(x+1)$.*

Proof. By comparing the values in (8), one quickly sees that $f(-x) = f(x-1)$. So $f(-x)$ divides $\phi(x)$ if and only if $f(x-1)$ divides $\phi(x)$, if and only if $f(x)$ divides $\phi(x+1)$.

Lemma 2. *If $f(x)f(-x)$ has no multiple factors and divides $x^{4N} - 1$, then either*

A. *$f(x)$, $x^{2N} - 1$, and $(x+1)^{2N} + 1$ have a common factor, or*

B. *$f(x)f(-x)$ divides $x^{2N} - 1$.*

[4] In particular we shall use the results of L. E. Dickson, *On the last theorem of Fermat*, Messenger of Mathematics, vol. 38 (1908), pp. 14–32.

PROOF. Use Lemma 1 and the results of Dickson[4] (loc. cit., §11, pp. 20-21).

3. $f(x)f(-x)$ **has no multiple factors if** $m\leqq 67$. By (4) and (5) one can readily see that the only cases in which $f(x)f(-x)$ can have a multiple root are:

I. $a^2+a-1\equiv 0$,
II. $a^2-a-1\equiv 0$,
III. $a^2+3a+1\equiv 0$.

In case I, $x^{2n}-1$ and x^2-x-1 have the factor $x+a$ in common by (6). In case II, $x^{2n}-1$ and x^2-x-1 have the factor $x-a$ in common by (6). In case III, $x^{2n}-1$ and x^2-x-1 have the factor $x+a+1$ in common by (6). So it suffices to prove that $x^{2n}-1$ and x^2-x-1 have no factors in common.

LEMMA 3. *If* $n\leqq 33$, *then* $x^{2n}-1$ *and* x^2-x-1 *have no common factor modulo* p.

PROOF. Divide $x^n\pm 1$ by x^2-x-1. If $a_1, a_2, \cdots$ are the Fibonacci numbers, that is $a_1=a_2=1$, $a_{j+2}=a_{j+1}+a_j$, and $Q_j(x)=a_1x^j+a_2x^{j-1}+\cdots+a_jx+a_{j+1}$, then $x^n\pm 1=(x^2-x-1)Q_{n-2}(x)+a_nx+(a_{n-1}\pm 1)$. The eliminant of x^2-x-1 and $a_nx+(a_{n-1}\pm 1)$ is $(a_{n-1})^2+a_{n-1}a_n-(a_n)^2\pm(2a_{n-1}+a_n)+1$. However $(a_{j-1})^2+a_ja_{j-1}-(a_j)^2=(-1)^j$. So the eliminant of $x^n\pm 1$ and x^2-x-1 is $1+(-1)^n\pm(2a_{n-1}+a_n)$. However $a_j=(k^j-l^j)/5^{1/2}$, where $k=(1+5^{1/2})/2$, $l=(1-5^{1/2})/2$. So a_j equals the integer nearest to $k^j/5^{1/2}$. Hence $x^n\pm 1$ and x^2-x-1 have no common factor if $n\leqq 33$, since $p>8{,}000{,}000$ and factorization is modulo p. Therefore $x^{2n}-1$ and x^2-x-1 have no common factor if $n\leqq 33$.

4. **Proof that** $m\neq 37$. Assume $m=37$, and then use Lemma 2 with $N=9$.

Case 1. $x-\alpha$ is a common factor of $f(x)$, $x^{18}-1$, and $(x+1)^{18}+1$. By (5), $x-\alpha$ is not a factor of x^6-1. So $x-\alpha$ is a common factor of $(x^6+x^3+1)(x^6-x^3+1)$ and $(x+1)^{18}+1$.

Subcase I. $x-\alpha$ is a common factor of x^6+x^3+1 and $(x+1)^{18}+1$. So $\alpha^9\equiv 1$ and $(\alpha^2+2\alpha+1)^9/\alpha^9+1\equiv 0$. Put $\beta=\alpha+1/\alpha$. Then $A=\beta^3-3\beta+1\equiv 0$, and, since $\beta+2=(\alpha+1)^2/\alpha$,

$$(\beta+2)^9+1=((\beta+2)^3+1)((\beta+2)^6-(\beta+2)^3+1)\equiv 0.$$

If $(\beta+2)^3+1\equiv 0$, then $6\beta^2+15\beta+8\equiv 0$, $23\beta+52\equiv 0$, and[5] $2516=2^2\cdot 17\cdot 37\equiv 0$. So

[5] Here, and at corresponding places later, a contradiction results from the fact that $p>8{,}000{,}000$.

$$(\beta+2)^6-(\beta+2)^3+1\equiv 0,\qquad B=417\beta^2+699\beta-137\equiv 0,$$
$$B\beta-417A=C=699\beta^2+1096\beta-411\equiv 0,$$
$$3B-C=534\beta^2+1001\beta\equiv 0.$$

However $\beta\equiv 0$ would contradict $A\equiv 0$. So $534\beta+1001\equiv 0$. So $883{,}227=3\cdot 37\cdot 73\cdot 109\equiv 0$.

Subcase II. $x-\alpha$ is a common factor of x^6-x^3+1 and $(x+1)^{18}+1$. So $\alpha^9\equiv -1$ and $(\alpha^2+2\alpha+1)^9/\alpha^9\equiv 1$. Put $\beta=\alpha+1/\alpha$. Then

$$\beta^3-3\beta-1\equiv 0,$$
$$(\beta+2)^9-1\equiv((\beta+2)^3-1)((\beta+2)^6+(\beta+2)^3+1)\equiv 0.$$

If $(\beta+2)^3-1\equiv 0$, then $6\beta^2+15\beta+8=0$, $23\beta+28\equiv 0$, and $724=2^2\cdot 181\equiv 0$. So

$$(\beta+2)^6+(\beta+2)^3+1\equiv 0,\qquad 447\beta^2+861\beta+271\equiv 0,$$
$$37(187\beta+302)\equiv 0.$$

Using $187\beta+302\equiv 0$, we get $1{,}620{,}673=73\cdot 149^2\equiv 0$.

Case 2. $f(x)f(-x)$ divides $x^{18}-1$. Because of (5), $f(x)f(-x)$ divides $x^{12}+x^6+1$. So $f(x)f(-x)\equiv x^{12}+x^6+1$. Comparing the coefficients of x^{10} and x^8, we get $2b-9\equiv 0$ and $b^2-10b+30\equiv 0$. So $21\equiv 0$.

5. **Proof that $m\neq 41$.** Assume $m=41$. Use Lemma 2 with $N=10$.

Case 1. $f(x)$, $x^{20}-1$, and $(x+1)^{20}+1$ have a common factor. The discussion in Dickson (loc. cit., pp. 23–24) will eliminate this case.

Case 2. $f(x)f(-x)$ is a factor of $x^{20}-1$. By Lemma 2 with $N=5$, either $f(x)$, $x^{10}-1$ and $(x+1)^{10}+1$ have a common factor, or else $f(x)f(-x)$ divides $x^{10}-1$. The latter is impossible, so let $x-\alpha$ be a common factor of $f(x)$, $x^{10}-1$, and $(x+1)^{10}+1$. Because of (4), $x-\alpha$ is not a factor of x^2-1.

Subcase I. $x-\alpha$ is a common factor of $x^4+x^3+x^2+x+1$ and $(x+1)^{10}+1$. Then $\alpha^5\equiv 1$. So $(\alpha^2+2\alpha+1)^5/\alpha^5+1\equiv 0$. Put $\beta=\alpha+1/\alpha$. Then $\beta^2\equiv -\beta+1$, $(\beta+2)^5+1\equiv 0$. So $5(11\beta+16)\equiv 0$. So $41\equiv 0$.

Subcase II. $x-\alpha$ is a common factor of $x^4-x^3+x^2-x+1$ and $(x+1)^{10}+1$. Then $\alpha^5\equiv -1$. So put $\beta=\alpha+1/\alpha$. Then $\beta^2\equiv\beta+1$, $(\beta+2)^5-1\equiv 0$. So $275\beta+174\equiv 0$. So $2501=41\cdot 61\equiv 0$.

6. **Proof that $p>41{,}000{,}000$.** We have now proved

$$37^{p-1}\equiv 1 \pmod{p^2},\qquad 41^{p-1}\equiv 1 \pmod{p^2}.$$

So we can argue as in I and conclude that $p>41{,}000{,}000$.

7. **The non-generality of this method.** It seems certain that the

lower bound just obtained is not the best that this method will produce. For instance, now that we know that $p>41{,}000{,}000$, it is almost certain that we can prove that (7) holds for $m=43$ (in fact, this probably follows from $p>8{,}000{,}000$). Also, the fact that $p>41,\ 000{,}000$ will probably make it easier to prove that, for appropriate $m>43$, the values of (2) must satisfy (3), (4), and (5), and so, for these m's also, (7) undoubtedly holds. Nevertheless the methods of this paper will apparently fail for very large values of p.

To see the difficulty that would arise, let us ignore any difficulties inherent in the proof that the values of (2) must satisfy (3), (4), and (5), and assume that for any m, this result would be easily forthcoming. Then, for any m, (7) would hold except for these p's which are factors of the eliminant of $x^{m-1}-1$ and $(x+1)^{m-1}-1$. As $p>41{,}000{,}000$, we could then prove that (7) holds for all $m\leqq N_1$ (undoubtedly $N_1>43$). From this, by the method of I, we could prove that $p>M_1$. From this we could then prove that (7) holds for all $m\leqq N_2$, and so on. Unfortunately the M's and N's would probably not increase indefinitely.

To see this, let us first consider the eliminant of $x^{m-1}-1$ and $(x+1)^{m-1}-1$. Let $x-\alpha$ be a common factor. Then $\alpha^{m-1}\equiv 1$ and $(\alpha+1)^{m-1}\equiv 1$. We break this into cases (essentially corresponding to a factorization of the eliminant (see Dickson,[6] p. 28), by considering the eliminants of $(x+1)^u-x^v$ and $x^{m-1}-1$ for small values of u and v. The case $u=1$, $v=2$ was treated in Lemma 3, and two eliminants of the order $k^{m/2}$ were obtained. If m is the rth prime, m is of the order of $r\log r$ (see Landau,[7] pp. 213–215). So the eliminants are of the order of r^{br}.

Now we consider the lower bounds for p which can be obtained by the method of I. Let the Σ's be as in Lemma 5 of I and let r be large. Then $\Sigma_1=\theta(p_r)-\log 2<2r\log r$ (Landau, loc. cit., p. 195). So $\Sigma_j<(\Sigma_1)^j/j!<(2r\log r)^j/j!$. Also, since r is large, $r!(\log 2)\Sigma_{r-1}>(e^{-r}r^r)e^r=r^r$. Substituting these in the formula for $f^r(x)$ in Lemma 5 of I, we get

$$f_r(x) < (x + r\log r)^r/r^r.$$

If $x>(2\log r)^r$, then $f_r(\log x^2/2)<x/2$. So the method of I will not give a lower bound as great as $(2\log r)^r$, whereas the eliminant of x^{p_r-1} and x^2-x-1 is of the order of r^{br}.

To the above argument, one might object that firstly it is not the

[6] L. E. Dickson, *On the last theorem of Fermat*, Quarterly Journal of Mathematics, vol. 40 (1908), pp. 27–45.

[7] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen.*

size of the eliminants but the size of their largest prime factor which is important, and secondly it is not essential to take the m's in order of magnitude. In answer, it should be pointed out that after one passes the limits of factor tables, it becomes impracticable to deal with the factors of the eliminant rather than the eliminant. Therefore, since the eliminant (in one case at least) appears to be an increasing function of m, one is compelled to work with monotone increasing m.

Cornell University

SOME UNIFORMLY CONVEX SPACES

R. P. BOAS, JR.[1]

1. **Introduction.** A Banach space is said to be uniformly convex if to every ϵ, $0<\epsilon<1$, there is a $\delta(\epsilon)$, $0<\delta(\epsilon)<2$, such that $\|x\|=\|y\|=1$ and $\|x-y\|\geqq\epsilon$ imply $\|x+y\|<2-\delta(\epsilon)$. J. A. Clarkson, who introduced the concept of uniform convexity [5], proved that the spaces L^p and l^p are uniformly convex if $p>1$, basing his proof on the following inequalities[2] among norms of elements of L^p or l^p:

$$\|x+y\|^p+\|x-y\|^p\leqq 2^{p-1}(\|x\|^p+\|y\|^p), \qquad p\geqq 2; \tag{1.1}$$

$$\|x+y\|^p+\|x-y\|^p\leqq 2(\|x\|^{p'}+\|y\|^{p'})^{p-1}, \qquad p\geqq 2; \tag{1.2}$$

$$\|x+y\|^{p'}+\|x-y\|^{p'}\leqq 2(\|x\|^p+\|y\|^p)^{p'-1}, \quad 1<p\leqq 2. \tag{1.3}$$

The uniform convexity of L^p and l^p follows by inspection from either (1.1) or (1.2) if $p\geqq 2$, and from (1.3) if $1<p\leqq 2$. As Clarkson observed, (1.1) is a consequence of (1.2), since $\{(1/2)(a^r+b^r)\}^{1/r}$ is an increasing function of r for positive a and b [6, p. 26], so that the right side of (1.1) is not less than that of (1.2). However, (1.1) is interesting because it is considerably simpler to prove than (1.2) (see §3), so that the uniform convexity of L^p and l^p can be established more easily for $p\geqq 2$ than for $1<p<2$.

In this note I give a short proof of Clarkson's inequalities (and of a general set of inequalities, which includes them), using M. Riesz's convexity theorem for linear forms. This proof has the advantage that it can be generalized to show that the spaces $L^p\{L^q\}$, $L^p\{l^q\}$, $l^p\{L^q\}$, $l^p\{l^q\}$ are all uniformly convex[3] if $p>1, q>1$. Here $L^p\{E\}$ is

[1] National Research Fellow.

[2] Here, as throughout this note, $p'=p/(p-1)$; similarly for other letters.

[3] These results suggest the possibility that $L^p\{E\}$ and $l^p\{E\}$ are uniformly convex whenever E is; but I can offer no evidence for or against this conjecture.