MATHEMATICS OF COMPUTATION
VOLUME 53, NUMBER 188
OCTOBER 1989, PAGES 743–750

New Bound for the First Case of Fermat's Last Theorem

By Jonathan W. Tanner and Samuel S. Wagstaff, Jr.

Abstract. We present an improvement to Gunderson's function, which gives a lower bound for the exponent in a possible counterexample to the first case of Fermat's "Last Theorem," assuming that the generalized Wieferich criterion is valid for the first n prime bases. The new function increases beyond $n = 29$, unlike Gunderson's, and it increases more swiftly. Using the recent extension of the Wieferich criterion to $n = 24$ by Granville and Monagan, the first case of Fermat's "Last Theorem" is proved for all prime exponents below $156,442,236,847,241,729$.

1. Introduction. The generalized Wieferich criterion states that if the first case of Fermat's "Last Theorem" (FLT1) does not hold for the prime exponent p, i.e., the equation $x^p + y^p = z^p$ has a solution where x, y, and z are integers not divisible by p, then, for certain numbers q,

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

This criterion has been proved [1] when q is one of the first 24 primes $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$, and $p_{24} = 89$. Several authors have used the fact that the generalized Wieferich criterion has been proved for the first n primes to prove FLT1 for all prime exponents below a certain bound. The idea behind these proofs is that if FLT1 does not hold for p, then all integers q that are not divisible by any prime exceeding p_n are solutions to (1). However, (1) can have at most $(p-1)/2$ positive solutions less than $p^2/2$ [2], and, in fact, at most $(p-1)/2$ pairs of relatively prime solutions (a, b) with $1 \le a \le x$ and $1 \le b \le y$, where $xy = p^2/2$ [3]. These constraints yield a contradiction unless p is sufficiently large.

The approach just described requires a lower bound for $P_n(x)$, the number of positive integers up to x divisible by no prime exceeding p_n, or for $P_n(x,y)$, the number of pairs of relatively prime positive integers up to x and y, respectively, divisible by no prime exceeding p_n. Rosser [2] obtained a suitable lower bound for $P_n(x)$, good for small n, and his student, Gunderson [3], proved a similar one for $P_n(x, y)$. When x and y are chosen properly as functions of p, each of these lower bounds is a polynomial of degree n in $\log p$ whose leading coefficient (as a function of n) goes to zero swiftly. In each case, when n is small, there is a range of p for which the lower bound exceeds $(p-1)/2$ and gives the desired contradiction, proving FLT1 for all primes p in that range. But for all sufficiently large n, the lower bound stays less than $(p-1)/2$ for all p, which proves nothing. See [8] for a discussion of Gunderson's estimate.

Received October 7, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D41.

D. H. and Emma Lehmer [4] used a better lower bound for $P_n(x)$ when they proved FLT1 for $p < 253,747,889$. We follow the Lehmers' method and obtain a better lower bound than Gunderson's for $P_n(x, y)$. This lower bound is derived in Section 2. The implications for FLT1 are discussed in Section 3.

2. Estimate of $P_n(x, y)$. In this section we define functions $G_n(x, y)$ for $n \geq 1$ which are moderately easy to compute and which are lower bounds for $P_n(x, y)$.

Define $G_n(x, y)$ inductively as follows. Let $G_1(x, y) = \log x/\log 2 + \log y/\log 2 - 1$. For each n, $G_n(x, y)$ will be a polynomial in $\log x$ and $\log y$ of the form

$$G_n(x,y) = \sum_{i=0}^{n} \sum_{j=0}^{n-i} g_{ij}^{(n)} \log^i x \log^j y. \tag{2}$$

Assuming $G_n(x, y)$ has been defined, define

$$\begin{aligned} G_{n+1}(x,y) = G_n(x,y) &+ \sum_{i=0}^{n} \sum_{j=0}^{n-i} g_{ij}^{(n)} \frac{\log^i p_{n+1}}{i+1} \left(B_{i+1}\left(\frac{\log x}{\log p_{n+1}}\right) - D_{i+1}^{(i,j,n)} \right) \log^j y \\ &+ \sum_{i=0}^{n} \sum_{j=0}^{n-i} g_{ij}^{(n)} \frac{\log^j p_{n+1}}{j+1} \left(B_{j+1}\left(\frac{\log y}{\log p_{n+1}}\right) - D_{j+1}^{(i,j,n)} \right) \log^i x, \end{aligned}$$

where $B_n(X) = \sum_{k=0}^{n} B_k \binom{n}{k} X^{n-k}$ is the nth Bernoulli polynomial, B_k is the kth Bernoulli number ($B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$, $B_5 = 0$, etc.), and $D_k^{(i,j,n)}$ is either the maximum value M_k or minimum value m_k of $B_k(x)$ on the unit interval $0 \leq x \leq 1$, according as $g_{ij}^{(n)} \geq 0$ or $g_{ij}^{(n)} < 0$. Note that $G_{n+1}(x, y)$ has the form (2), with n replaced by $n + 1$. Indeed, substitution of the definition of the Bernoulli polynomials in the definition of $G_{n+1}(x, y)$ gives the following recursion formulas:

$$\begin{aligned} g_{ij}^{(n+1)} &= g_{ij}^{(n)} + \sum_{m=i-1}^{n-j} g_{mj}^{(n)} \frac{B_{m+1-i}}{m+1} \binom{m+1}{i} \log^{m-i} p_{n+1} \\ &\quad + \sum_{m=j-1}^{n-i} g_{im}^{(n)} \frac{B_{m+1-j}}{m+1} \binom{m+1}{j} \log^{m-j} p_{n+1} \quad \text{when } i > 0, j > 0, \\ g_{00}^{(n+1)} &= g_{00}^{(n)} + \sum_{m=0}^{n} g_{m0}^{(n)} \frac{\log^m p_{n+1}}{m+1} (B_{m+1} - D_{m+1}^{(m,0,n)}) \\ &\quad + \sum_{m=0}^{n} g_{0m}^{(n)} \frac{\log^m p_{n+1}}{m+1} (B_{m+1} - D_{m+1}^{(0,m,n)}), \\ g_{0j}^{(n+1)} &= g_{0j}^{(n)} + \sum_{m=0}^{n-j} g_{mj}^{(n)} \frac{\log^m p_{n+1}}{m+1} (B_{m+1} - D_{m+1}^{(m,j,n)}) \\ &\quad + \sum_{m=j-1}^{n} g_{0m}^{(n)} \frac{\log^{m-j} p_{n+1}}{m+1} B_{m+1-j} \binom{m+1}{j} \quad \text{when } 1 \leq j \leq n, \\ g_{0,n+1}^{(n+1)} &= g_{0n}^{(n)} / ((n+1) \log p_{n+1}), \end{aligned}$$

$$g_{i0}^{(n+1)} = g_{i0}^{(n)} + \sum_{m=0}^{n-i} g_{im}^{(n)} \frac{\log^m p_{n+1}}{m+1} (B_{m+1} - D_{m+1}^{(i,m,n)})$$
$$+ \sum_{m=i-1}^{n} g_{m0}^{(n)} \frac{\log^{m-i} p_{n+1}}{m+1} B_{m+1-i} \binom{m+1}{i} \quad \text{when } 1 \le i \le n, \text{ and}$$
$$g_{n+1,0}^{(n+1)} = g_{n0}^{(n)} / ((n+1) \log p_{n+1}).$$

The case $n = 1$ has $g_{00}^{(1)} = -1$ and $g_{10}^{(1)} = g_{01}^{(1)} = 1/\log 2$.

We will prove by induction on n that $P_n(x, y) \ge G_n(x, y)$ for $n \ge 1$, $x \ge 1$ and $y \ge 1$. For the base step, note that $P_1(x, y)$ is the number of pairs of integers of the form $(2^a, 1)$ or $(1, 2^b)$ with $0 \le a \le [(\log x)/(\log 2)]$ and $0 \le b \le [(\log y)/(\log 2)]$. Therefore,

$$\begin{aligned} P_1(x, y) &= \left(\left[\frac{\log x}{\log 2} \right] + 1 \right) + \left(\left[\frac{\log y}{\log 2} \right] + 1 \right) - 1 \\ &\ge \frac{\log x}{\log 2} + \frac{\log y}{\log 2} - 1 = G_1(x, y). \end{aligned}$$

Now assume that $P_n(x, y) \ge G_n(x, y)$ for some $n \ge 1$. Write p for p_{n+1}. By definition, $P_{n+1}(x, y)$ is the number of pairs of relatively prime integers (a, b) having no prime factor greater than p, with $1 \le a \le x$ and $1 \le b \le y$. We may count these pairs as follows. There are $P_n(x, y)$ pairs in which neither a nor b is divisible by p. There are $P_n(x/p^s, y)$ pairs (a, b) in which a is exactly divisible by p^s. There are $P_n(x, y/p^s)$ pairs (a, b) in which b is exactly divisible by p^s. Therefore,

$$P_{n+1}(x, y) = P_n(x, y) + \sum_{s=1}^{[\log x/\log p]} P_n(x/p^s, y) + \sum_{s=1}^{[\log y/\log p]} P_n(x, y/p^s).$$

By the induction hypothesis, this quantity is greater than or equal to

$$\begin{aligned} &G_n(x, y) + \sum_{s=1}^{[\log x/\log p]} G_n(x/p^s, y) + \sum_{s=1}^{[\log y/\log p]} G_n(x, y/p^s) \\ &= G_n(x, y) + \sum_{i=0}^{n} \sum_{j=0}^{n-i} g_{ij}^{(n)} \sum_{s=1}^{[\log x/\log p]} \log^i \frac{x}{p^s} \log^j y \\ &\quad + \sum_{i=0}^{n} \sum_{j=0}^{n-i} g_{ij}^{(n)} \sum_{s=1}^{[\log y/\log p]} \log^j \frac{y}{p^s} \log^i x. \end{aligned}$$

By [5, Lemma on p. 345],

$$\begin{aligned} \frac{\log^k p}{k+1} \left(B_{k+1} \left(\frac{\log z}{\log p} \right) - m_{k+1} \right) &\ge \sum_{s=1}^{[\log z/\log p]} \log^k \frac{z}{p^s} \\ &\ge \frac{\log^k p}{k+1} \left(B_{k+1} \left(\frac{\log z}{\log p} \right) - M_{k+1} \right). \end{aligned} \tag{3}$$

Therefore,

$$P_{n+1}(x,y) \geq G_n(x,y) + \sum_{i=0}^{n}\sum_{j=0}^{n-i} g_{ij}^{(n)} \frac{\log^i p_{n+1}}{i+1}\left(B_{i+1}\left(\frac{\log x}{\log p_{n+1}}\right) - D_{i+1}^{(i,j,n)}\right)\log^j y$$

$$+ \sum_{i=0}^{n}\sum_{j=0}^{n-i} g_{ij}^{(n)} \frac{\log^j p_{n+1}}{j+1}\left(B_{j+1}\left(\frac{\log y}{\log p_{n+1}}\right) - D_{j+1}^{(i,j,n)}\right)\log^i x,$$

which is the definition of $G_{n+1}(x,y)$.

3. Implications for Fermat's Last Theorem. We computed the coefficients of the polynomials $G_n(x,y)$ defined in Section 2 for $n \leq 50$. We then computed the solution to $G_n(p/\sqrt{2}, p/\sqrt{2}) = (p-1)/2$, by iterating the mapping $p \to 2G_n(p/\sqrt{2}, p/\sqrt{2}) + 1$. We performed these computations first on a personal computer, and then with double precision on a CYBER 205 for more accuracy. In Table 1 below, we list the values of M_n and m_n, defined in Section 2, used in our calculations. These values were computed using the formulas on page 538 of [6]. However, we corrected a tiny error in formulas (17) and (18) of that paper: the exponents of 3 and 5 should be $-2k-1$ rather than $-2k$ in these formulas and in the first inequality following (18).

In Table 2, we give the coefficients of $G_{24}(x,x)$. Following earlier authors, we have used base 10 for logarithms. In Table 3, we list Gunderson's lower bound on a possible counterexample to FLT1 and our new bound $R(n)$, which is the largest number x for which $G_n(x/\sqrt{2}, x/\sqrt{2}) \geq (x-1)/2$. Let $Q(n)$ be the least prime number greater than $R(n)$. FLT1 is then true for all prime exponents below $Q(n)$, assuming the generalized Wieferich criterion holds for the first n primes. In particular, since the generalized Wieferich criterion has been proved up to $p_{24} = 89$, FLT1 is now proved for all prime exponents below $Q(24) = 156,442,236,847,241,729$.

Each value of $R(n)$ shown in Table 3 is larger than the corresponding value of Gunderson's function. In Gunderson's day, when the Wieferich criterion had been proved only up to the eleventh prime (or, some thought, up to the fourteenth), the advantage of a better approximation to $P_n(x,y)$ was not as significant as it is today. Our function $R(n)$ increases beyond $n = 29$, unlike Gunderson's function [8]. We hope this encourages further extension of the Wieferich criterion. We suspect, however, that our function may suffer the same fate as Gunderson's and peter out eventually because of the following weakness inherent in our iteration procedure. The lemma of [5], which we used to derive (3), must cover the worst case, which presumably occurs only rarely. We have not tried to compute the exact point of failure, because D. Coppersmith recently showed us a new method of computing lower bounds for $P_n(x,y)$ that always increase with n. Using the Wieferich criterion up to p_{24}, his method proves FLT1 for all primes up to about 7.568×10^{17}.

It should be noted that an old result of Lenstra provides a lower bound for $R(n)$ which increases monotonically. He proved [7] that if p is an odd prime, then there exists a prime $q < 4\ln^2 p$ for which (1) fails. It follows immediately that $R(n) \geq \exp(\sqrt{p_n}/2)$.

TABLE 1
Minima and maxima of Bernoulli polynomials on $[0, 1]$.

n	m_n	M_n
1	−0.15000000000000000000 E+01	−0.50000000000000000000 E+00
2	0.16666666666666666667 E+00	0.41666666666666666667 E+00
3	−0.48112522430000000000 E−01	0.48112522430000000000 E−01
4	−0.95833333333333333333 E−01	−0.33333333333333333333 E−01
5	−0.24458190870000000000 E−01	0.24458190870000000000 E−01
6	0.23809523809523809524 E−01	0.70684523809523809524 E−01
7	−0.26065114260000000000 E−01	0.26065114260000000000 E−01
8	−0.99739583333333333333 E−01	−0.33333333333333333333 E−01
9	−0.47550561640000000000 E−01	0.47550561640000000000 E−01
10	0.75757575757575757576 E−01	0.22712476325757575758 E+00
11	−0.13249665844000000000 E+00	0.13249665844000000000 E+00
12	−0.75921706873855311355 E+00	−0.25311355311355311355 E+00
13	−0.52356641061000000000 E+00	0.52356641061000000000 E+00
14	0.11666666666666666667 E+01	0.34998575846354166667 E+01
15	−0.27850407419174720773 E+01	0.27850407419174720773 E+01
16	−0.21276254152784160539 E+02	−0.70921568627450980392 E+01
17	−0.19188487584572014681 E+02	0.19188487584572014681 E+02
18	0.54971177944862155388 E+02	0.16491311443778207726 E+03
19	−0.16622912456675811145 E+03	0.16622912456675811145 E+03
20	−0.15873717180483268969 E+04	−0.52912424242424242424 E+03
21	−0.17684658253063159639 E+04	0.17684658253063159639 E+04
22	0.61921231884057971014 E+04	0.18576366612582966901 E+05
23	−0.22666655909265818844 E+05	0.22666655909265818844 E+05
24	−0.25974074901948887787 E+06	−0.86580253113553113553 E+05
25	−0.34449186089429466637 E+06	0.34449186089429466637 E+06
26	0.14255171666666666667 E+07	0.42765514575162778298 E+07
27	−0.61257087042251506579 E+07	0.61257087042251506579 E+07
28	−0.81894693000060605138 E+08	−0.27298231067816091954 E+08
29	−0.12599480348174813897 E+09	0.12599480348174813897 E+09
30	0.60158087390064236838 E+09	0.18047426205813954085 E+10
31	−0.29680816595114507324 E+10	0.29680816595114507324 E+10
32	−0.45348947294237387529 E+11	−0.15116315767092156863 E+11
33	−0.79392600378647102296 E+11	0.79392600378647102296 E+11
34	0.42961464306116666667 E+12	0.12888439291334862731 E+13
35	−0.23931352922352727888 E+13	0.23931352922352727888 E+13
36	−0.41134965614865936628 E+14	−0.13711655205088332772 E+14
37	−0.80744275041701406077 E+14	0.80744275041701406077 E+14
38	0.48833231897359316667 E+15	0.14649969569172264147 E+16
39	−0.30310995949998174742 E+16	0.30310995949998174742 E+16
40	−0.57889738025785104173 E+17	−0.19296579341940068149 E+17
41	−0.12591698546830878159 E+18	0.12591698546830878159 E+18
42	0.84169304757368261500 E+18	0.25250791427206650873 E+19
43	−0.57602631907583269025 E+19	0.57602631907583269025 E+19
44	−0.12101421556217378033 E+21	−0.40338071854059455413 E+20
45	−0.28890015886661637002 E+21	0.28890015886661637002 E+21
46	0.21150748638081991606 E+22	0.63452245914245373676 E+22
47	−0.15821357120470909276 E+23	0.15821357120470909276 E+23
48	−0.36259879566889491923 E+24	−0.12086626522296525935 E+24
49	−0.94258671460125389549 E+24	0.94258671460125389549 E+24
50	0.75008667460769643669 E+25	0.22502600238230879776 E+26

TABLE 2

Coefficients of the polynomial $G_{24}(x, x)$.

n	Coefficient of x^n in $G_{24}(x, x)$
0	−0.11124693077293400420 E+05
1	−0.19363548438737002094 E+05
2	−0.17375140357104685401 E+05
3	−0.10771895369339379062 E+05
4	−0.51882790358553534694 E+04
5	−0.20907991529685734580 E+04
6	−0.70902615515628871565 E+03
7	−0.22286316542789616349 E+03
8	−0.55123529031930888302 E+02
9	−0.15365746661965683662 E+02
10	−0.24374081976518702390 E+01
11	−0.72982679905736685353 E+00
12	−0.47984527735836055517 E−01
13	−0.23921139849329798596 E−01
14	0.44997965855754343485 E−03
15	−0.51977514439278889268 E−03
16	0.43284207081650198488 E−04
17	−0.70685578836264089938 E−05
18	0.89402321136888100622 E−06
19	−0.56052466000600451515 E−07
20	0.85939038723613860659 E−08
21	−0.23138055120705401572 E−09
22	0.39150182529613663587 E−10
23	−0.37681535318820797427 E−12
24	0.67109909952638698046 E−13

TABLE 3

Old and new lower bounds for a possible counterexample to FLT1.

n	n^{th} Prime	Gunderson's Bound	New Bound $R(n)$
2	3	93.1	131.1
3	5	861.4	1392.4
4	7	7616.1	13072.2
5	11	52735.2	94815.6
6	13	350357.5	661393.5
7	17	2032170.2	4081068.2
8	19	11360889.4	24522706.9
9	23	57557706.7	135923041.4
10	29	256482782.3	679635322.1
11	31	1110061026.8	3349178854.4
12	37	4343289919.3	15336498683.8
13	41	16018986861.3	67731590890.3
14	43	57441749341.4	295931100415.4
15	47	194810995856.2	1252907293603.9
16	53	611028198337.9	5065786519632.0
17	59	1779859830918.2	19682144283255.1
18	61	5026694771491.7	75886223273546.4
19	67	13207844119604.0	282770978928089.1

TABLE 3 (*continued*)

20	71	32905961806749.9	1033891266050714.6
21	73	79066452863726.0	3755162741164996.1
22	79	176236114699864.1	13262862527392256.9
23	83	369783910563050.3	46102892590386280.7
24	89	714591416091369.8	156442236847241649.8
25	97	1242237613389766.7	515062466154238954.0
26	101	1985337583473801.8	1674645737493287555.5
27	103	2926704423622306.3	5419082591859180578.1
28	107	3835841028759220.9	17329485401608772032.6
29	109	4408660978137437.7	55163979858622168394.3
30	113	4107554462428530.6	173642818878629237045.3
31	127	2321192058339787.0	524859226635802191198.6
32	131	268690071898783.2	1571770419526751987469.2
33	137		4640623723046428548069.9
34	139		13652745852383582733431.9
35	149		39266115083304516886158.9
36	151		112563302180710531159197.0
37	157		318818792908136203807583.0
38	163		892674241903000482296716.3
39	167		2481895280814579774851979.7
40	173		6826818305097123485543963.2
41	179		18586018953742069863067495.0
42	181		50461623282714716212095944.4
43	191		134745590008715569795727433.3
44	193		358879895908370471644356537.7
45	197		950274143425938949741842917.6
46	199		2509904603458487705005232870.0
47	211		6511699273735784412415745299.5
48	223		16615035813391291134156987180.0
49	227		42185393245604823986455364248.0
50	229		106875542151091718623981352256.0

Acknowledgments. We would like to thank Bennett Levitan for a helpful discussion, and the University of Pennsylvania and Purdue University for the use of computing facilities. We thank the referee for helpful comments.

School of Medicine
University of Pennsylvania
Philadelphia, Pennsylvania 19104
E-mail: jwt@penndrls.bitnet

Department of Computer Sciences
Purdue University
West Lafayette, Indiana 47907
E-mail: *ssw@arthur.cs.purdue.edu*

1. ANDREW GRANVILLE & MICHAEL B. MONAGAN, "The first case of Fermat's last theorem is true for all prime exponents up to 714,591,416,091,389," *Trans. Amer. Math. Soc*, v. 306, 1987, pp. 329–359.

2. BARKLEY ROSSER, "On the first case of Fermat's last theorem," *Bull. Amer. Math. Soc.*, v. 45, 1939, pp. 636–640.

3. NORMAN G. GUNDERSON, *Derivation of Criteria for the First Case of Fermat's Last Theorem and the Combination of These Criteria to Produce a New Lower Bound for the Exponent*, Thesis, Cornell University, Sept., 1948.

4. D. H. & EMMA LEHMER, "On the first case of Fermat's last theorem," *Bull. Amer. Math. Soc.*, v. 47, 1941, pp. 139–142.

5. D. H. LEHMER, "The lattice points of an n-dimensional tetrahedron," *Duke Math. J.*, v. 7, 1940, pp. 341–353.

D. H. LEHMER, "On the maxima and minima of Bernoulli polynomials," *Amer. Math. Monthly*, v. 47, 1940, pp. 533–538.

7. H. W. LENSTRA, JR., "Miller's primality test," *Inform. Process. Lett.*, v. 8, 1979, pp. 86–88.

8. DANIEL SHANKS & H. C. WILLIAMS, "Gunderson's function in Fermat's Last Theorem," *Math. Comp.*, v. 36, 1981, pp. 291–295.