MATHEMATICS OF COMPUTATION
VOLUME 36, NUMBER 153
JANUARY 1981

# Gunderson's Function in Fermat's Last Theorem

By Daniel Shanks and H. C. Williams

**Abstract.** We study Gunderson's function which gives a bound on the first case of Fermat's last theorem, assuming that the generalized Wieferich criterion is valid for the first $n$ prime bases. We note two unexpected phenomena.

**1. Introduction.** Wieferich's criterion states that if

$$p^2 \nmid 2^{p-1} - 1, \tag{1}$$

for the odd prime $p$, then any solution of

$$x^p + y^p = z^p \tag{2}$$

in integers must have $p \mid xyz$; i.e., the *first case* of Fermat's last theorem is true for the exponent $p$. As is known [1], the only $p < 3 \cdot 10^9$ for which

$$p^2 \mid 2^{p-1} - 1 \tag{3}$$

are $p = 1093$ and $p = 3511$. Mirimanoff's criterion is the same as Wieferich's except that the base 2 in (1) is replaced by 3. For this base [1], one has

$$p^2 \mid 3^{p-1} - 1 \tag{4}$$

only for $p = 11$ and $p = 1{,}006{,}003$ if $p < 2^{30}$. Consequently, the first case is true for all $p < 3 \cdot 10^9$.

Apropos, we note the following in passing. The heuristic probability of (3) is $p^{-1}$. Likewise for (4). Assuming that these are independent events, it follows that the heuristic probability $\theta$ of a counterexample for the first case satisfies

$$\theta < \sum_{3 \cdot 10^9}^{\infty} p^{-2} < 4 \cdot 10^{-10}.$$

We shall see that $\theta$ is even smaller.

Recently [2], the Lehmers extended the calculation of (3) to all $p < 5 \cdot 10^9$, and they found no other solution. Thus, the bound on the first case is $5 \cdot 10^9$. They are continuing. Suppose one wanted to increase the bound to, say, $10^{11}$ or $10^{13}$ or $10^{15}$. Obviously, that would require enormous calculations if it were done this way.

Now (1) generalizes to

$$p^2 \nmid q_i^{p-1} - 1, \tag{5}$$

and this is a valid criterion not only for $q_1 = 2$ and $q_2 = 3$, but also for $q_3 = 5$, $q_4 = 7$, and all prime $q_i$ up to $q_{11} = 31$. It was said to be valid also for $q_{12} = 37$, $q_{13} = 41$, $q_{14} = 43$, but in Gunderson's thesis [3] he questions the validity of the proofs that had been given for these last three cases. We return to that presently.

Received May 5, 1980.
1980 *Mathematics Subject Classification.* Primary 10A20, 10B15, 10–04.


0025-5718/81/0000-0028/$02.25

Since (5) is, in any case, a valid criterion up to $q_{11} = 31$, the heuristic probability above now becomes

$$\theta < \sum_{5 \cdot 10^9}^{\infty} p^{-11} < 10^{-98}.$$

We replace this heuristic estimate by the following exact (but weaker) result of Gunderson [3]:

THEOREM N. *If*

$$p^2 \mid q_i^{p-1} - 1,$$

*for all prime $q_i$ from $q_1 = 2$ to $q_n$, then $p$ must satisfy the inequality*

$$f_n(p) = \frac{(2n-2)!}{(n-1)!\,(n-1)!} \frac{4}{n!} \frac{\left[\log(p/\sqrt{2})\right]^n}{\log q_1 \cdot \log q_2 \cdot \cdots \log q_n} \leqslant p - 1. \tag{6}$$

The proof is combinatorial and it uses known results in the analytic theory of primes. It does *not* use algebraic number theory.

But if (5) is a valid criterion up to $q_n$ (that would require algebraic number theory), and if $f_n(p) > p - 1$, then the first case is true for all such $p$.

For $n = 11$, $q_{11} = 31$, we solve for $f_n(p) = p - 1$ by computing [4] the limit of the iterative sequence:

$$p = f_n(p) + 1. \tag{7}$$

We call this limit $G(11)$ and find that

$$G(11) = 1{,}110{,}601{,}026.794. \tag{8}$$

The first prime greater than $G(11)$ is

$$P(11) = 1{,}110{,}601{,}027. \tag{9}$$

With some further argument, Gunderson now concludes that the first case is true for all $p < P(11)$, except that he rounds this down to $1.1 \cdot 10^9$.

At this time (1948), this was the largest bound known, but in 1969 the bound became $3 \cdot 10^9$, as we indicated above. Suppose it can be shown that (5) is also valid for $q_{12} = 37$. Then we have

$$G(12) = 4{,}343{,}289{,}919.341 \quad \text{and} \quad P(12) = 4{,}343{,}289{,}943,$$

which is still not up to the Lehmers' bound $5 \cdot 10^9$. If (5) is also valid for $q_{13} = 41$, we have

$$G(13) = 16{,}018{,}986{,}861.269 \quad \text{and} \quad P(13) = 16{,}018{,}986{,}869.$$

This is now beyond the Lehmers' bound, and

$$G(14) = 57{,}441{,}749{,}341.414$$
$$P(14) = 57{,}441{,}749{,}347$$

is well beyond that bound.

It is clear that one should validate the previous claims made for $q_{12} = 37$, $q_{13} = 41$ and $q_{14} = 43$, if one can. In part, this involves manipulation with large determinants, and so it should be put on a computer. But if that is done, why stop at $q_{14} = 43$? If one continues, one either

(a) validates $q_{15} = 47$, etc., and thereby obtains still larger bounds, or

(b) finds, that for some reason not now known, some $q_i$ fails.

Since the latter, if true, must have some interesting number-theoretic significance, one can characterize this program as a no-lose situation [4].

**2. The Behavior of $G(n)$.** Suppose the program above succeeds, and we validate all $q_i$ up to $q_{19} = 67$. Then we have

$$G(19) = 13{,}207{,}844{,}119{,}604.000.$$

Similarly, for $q_{24} = 89$ and $q_{29} = 109$, we have

$$G(24) = 714{,}591{,}416{,}091{,}369.752 \quad \text{and} \quad G(29) = 4{,}408{,}660{,}978{,}137{,}437.699.$$

The obvious question is this: How does $G(n)$ go to infinity? The somewhat surprising answer is: It does not. In fact, $G(29)$ is its maximum, and then we have

$$G(30) = 4{,}107{,}554{,}462{,}428{,}530.576,$$

$$G(31) = 2{,}321{,}192{,}058{,}339{,}786.958,$$

$$G(32) = \quad 268{,}690{,}071{,}898{,}783.248.$$

What happens next is even more surprising. There is no $G(33)$. It disappears!

To clarify this paradoxical behavior, let us first note something that Gunderson does not. Besides the root $p = G(n)$ of

$$f_n(p) = p - 1 \tag{10}$$

there is a *second, smaller root* that we shall call $L(n)$; i.e., $G(n)$ is the greater root and $L(n)$ is the lesser root.

For example, for $n = 11$, we have the root

$$L(11) = 214.311 \tag{11}$$

besides the much larger root $G(11)$ previously given in (8).

In Table 1 below we list $L(n)$ and $G(n)$ to one rounded decimal place, together with the prime bounds $P(n)$ for $n = 4$ to 32. Just as $P(n)$ is the smallest prime greater than $G(n)$, we define $p(n)$ to be the largest prime less than $L(n)$. We list it also.

TABLE 1

| n | p(n) | L(n) | G(n) | P(n) |
|---|---|---|---|---|
| 4 | 5 | 5.3 | 7616.1 | 7621 |
| 5 | 7 | 8.5 | 52735.2 | 52747 |
| 6 | 13 | 13.4 | 350357.5 | 350377 |
| 7 | 19 | 22.2 | 2032170.2 | 2032171 |
| 8 | 37 | 37.1 | 11360889.4 | 11360891 |
| 9 | 61 | 64.1 | 57557706.7 | 57557771 |
| 10 | 113 | 116.3 | 256482782.3 | 256482803 |
| 11 | 211 | 214.3 | 1110061026.8 | 1110061027 |
| 12 | 409 | 413.1 | 4343289919.3 | 4343289943 |
| 13 | 821 | 821.0 | 16018986861.3 | 16018986869 |
| 14 | 1657 | 1663.0 | 57441749341.4 | 57441749347 |
| 15 | 3469 | 3476.1 | 194810995856.2 | 194810995901 |
| 16 | 7583 | 7587.6 | 611028198337.9 | 611028198353 |
| 17 | 17299 | 17303.4 | 1779859830918.2 | 1779859830937 |
| 18 | 40433 | 40446.2 | 5026694771491.7 | 5026694771491 |
| 19 | 99023 | 99023.8 | 13207844119604.0 | 13207844119609 |
| 20 | 251983 | 251986.4 | 32905961806749.9 | 32905961806759 |
| 21 | 661273 | 661379.9 | 79066452863726.0 | 79066452863731 |
| 22 | 1831831 | 1831849.7 | 176236114699864.1 | 176236114699937 |
| 23 | 5324273 | 5324279.0 | 369783910563050.3 | 369783910563121 |
| 24 | 16496587 | 16496599.7 | 714591416091369.8 | 714591416091389 |
| 25 | 55525819 | 55525851.5 | 1242237613389766.7 | 1242237613389779 |
| 26 | 201337207 | 201337223.2 | 1985337583473801.8 | 1985337583473817 |
| 27 | 788516591 | 788516606.7 | 2926704423622306.3 | 2926704423622393 |
| 28 | 3441834751 | 3441834803.3 | 3835841028759220.9 | 3835841028759227 |
| 29 | 17069688871 | 17069688882.5 | 4408660978137437.7 | 4408660978137503 |
| 30 | 103529269037 | 103529269062.9 | 4107554462428530.6 | 4107554462428531 |
| 31 | 1003547805149 | 1003547805186.3 | 2321192058339787.0 | 2321192058339793 |
| 32 | 47149278315319 | 47149278315328.5 | 268690071898783.2 | 268690071898799 |

For any $n$, the derivative

$$D = \frac{d}{dp}[f_n(p) - (p-1)]$$

is simply given by

$$D = \frac{p-1}{p}\frac{n}{\log(p/\sqrt{2})} - 1 \tag{12}$$

if $p$ is a root of (10). Therefore, (12) gives $D$ both for $p = L(n)$ and $p = G(n)$. The reader may verify that $D > 0$ at $p = L(n)$ and $D < 0$ at $p = G(n)$ for every $n$ in the table. Further, $D$ has only one zero in between. Therefore, we have the wanted condition

$$f_n(p) > p - 1$$

for all primes $p$ in the interval

$$p(n) < p < P(n). \tag{13}$$

First, we return briefly to Gunderson's bound $P(11)$ given in (9). The lower bound in (13) for $n = 11$ is actually $p(11) = 211$. However, that is no real problem since we saw that (1) above was already valid up to $p = 1091$. Further, the interval in (13) for $n = 11$ is overlapped at its lower end by the interval (13) for smaller $n$. So Gunderson's bound $P(11)$ is certainly valid.

Next, we tabulate the derivatives $D$, computed from (12), for $n = 11$, 29, 30, 31, and 32. We find

| $n$ | $D$ at $p = L(n)$ | $D$ at $p = G(n)$ |
|---|---|---|
| 11 | 1.1806 | −0.4629 |
| 29 | 0.2492 | −0.1871 |
| 30 | 0.1992 | −0.1574 |
| 31 | 0.1360 | −0.1152 |
| 32 | 0.0277 | −0.0267 |

We see that the graph $y = f_{32}(p)$ is nearly tangent to $y = p - 1$, and the relative slopes are rapidly decreasing with $n$. From (12) we see that, for an $n$ slightly larger than 32, and a $p$ slightly larger than $\sqrt{2}\, e^{32}$, the two roots $G(n)$ and $L(n)$ would coalesce. So it is no longer surprising that $G(33)$, and $L(33)$ also, disappear, since $f_{33}(p)$ and $p - 1$ no longer intersect.

**3. Conclusion.** We conclude by repeating the statement at the end of Section 1 that it would be desirable to prove the validity of the generalized criteria (5) for $q_{12} = 37$, $q_{13} = 41$, $q_{14} = 43$, etc., as far as this is feasible to do. If this really could be done up to $q_{29} = 109$, we would attain the large bound

$$P(29) = 4{,}408{,}660{,}978{,}137{,}503$$

for the first case.

But Gunderson's Theorem N stops there. To go further, one would have to modify Gunderson's Theorem N. We believe that that can be done but do not attempt it here. Alternatively, one could revert to checking (1) above for $p \geqslant P(29)$.

Obviously, that would not be a very clever procedure. However, "just for fun", we did verify that (1) is valid for $p = P(29)$.

Department of Mathematics
University of Maryland
College Park, Maryland 20742

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

1. J. BRILLHART, J. TONASCIA & P. WEINBERGER, "On the Fermat quotient," *Computers in Number Theory*, Academic Press, London, 1971, pp. 213–222.

2. D. H. LEHMER & EMMA LEHMER, "Cyclotomy with $\mu(n) = 0$." (To appear.)

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. DANIEL SHANKS, *Solved and Unsolved Problems in Number Theory*, 2nd ed., Chelsea, New York, 1978, pp. 232, 233.

NOTE ADDED. In [5], D. H. Lehmer extends the data on (3) to $6 \cdot 10^9$. There are no further solutions to that limit. Since the calculation was done *ab initio*, it also confirms the earlier calculation [1].

5. D. H. LEHMER, "On Fermat's quotient, base two," *Math. Comp.*, v. 36, 1981, pp. 289–290.