MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 361-363

NEW SOLUTIONS OF $a^{p-1} \equiv 1 \pmod{p^2}$

PETER L. MONTGOMERY

Dedicated to the memory of my undergraduate advisor, D. H. Lehmer

ABSTRACT. We tabulate solutions of $a^{p-1} \equiv 1 \pmod{p^2}$ where $2 \le a \le 99$ and where p is an odd prime, $p < 2^{32}$.

1. INTRODUCTION AND SUMMARY

Some number-theoretic questions such as Fermat's conjecture [4] require primes p satisfying

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

for given a not a power. Brillhart, Tonascia, and Weinberger [2] list all solutions of (1) for $2 \le a \le 99$ and $3 \le p < 10^6$, plus some solutions for higher p. Lehmer [3] subsequently extended the $a = 2$ search to $p < 6 \cdot 10^9$, finding only the known solutions $p = 1093$ and $p = 3511$. Aaltonen and Inkeri [1] list solutions for prime $a < 1000$ and $p < 10^4$. Table 1 (next page) extends the table in [2] to $p < 2^{32}$, giving 23 new solutions. Included are the first solutions for $a = 66$ and $a = 88$.

The table in [2] identifies where (1) holds modulo p^3, with the only solutions for $a \le 99$ and $p > 7$ being $(a, p) = (42, 23)$ and $(68, 113)$. This search found no more such solutions.

The pair $(a, p) = (5, 1645333507)$ satisfies $p^{a-1} \equiv 1 \pmod{a^2}$ as well as (1). This supplements the pairs $(2, 1093)$, $(3, 1006003)$, and $(83, 4871)$ listed in [1, p. 365].

The largest known p for which multiple a satisfy (1) with $2 \le a \le 99$, a not a power, is $p = 331$, for which $a = 18$ and $a = 71$ satisfy (1).

The Fibonacci sequence is defined by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \ge 2$. If $p \ne 5$, then $F_{p-\epsilon} \equiv 0 \pmod{p}$, where $\epsilon = +1$ if $p \equiv \pm 1 \pmod{5}$ and $\epsilon = -1$ if $p \equiv \pm 2 \pmod{5}$. Williams [5, pp. 85–86] reports no solution of $F_{p-\epsilon} \equiv 0 \pmod{p^2}$ with $p < 10^9$. This search found no such solution with $p < 2^{32}$.

Received by the editor June 21, 1991.
1991 *Mathematics Subject Classification.* Primary 11-04; Secondary 11D61.
Key words and phrases. Diophantine equation, Fermat quotient, Fibonacci congruence.
This work was supported by U.S. Army fellowship DAAL03-89-G-0063. Thanks to the Department of Mathematics at UCLA and to my graduate advisor David G. Cantor for supplying the computers on which this work was done.

TABLE 1. Solutions of $a^{p-1} \equiv 1 \pmod{p^2}$ with $2 \leq a \leq 99$ and $3 \leq p < 2^{32}$. New solutions are in **bold** font

a	Values of p	a	Values of p
2	1093 3511	55	3 30109 **7278001**
3	11 1006003	56	647 **7079771**
5	20771 40487 53471161 **1645333507**	57	5 47699 86197
6	66161 534851 3152573	58	131 **42250279**
7	5 491531	59	2777
10	3 487 56598313	60	29
11	71	61	
12	2693 123653	62	3 19 127 1291
13	863 1747591	63	23 29 36713 401771
14	29 353	65	17 163
15	29131	66	**89351671**
17	3 46021 48947	67	7 47 268573
18	5 7 37 331 33923 1284043	68	5 7 19 113 2741
19	3 7 13 43 137 63061489	69	19 223 631 **2503037**
20	281 46457 9377747 122959073	70	13 142963
21		71	3 47 331
22	13 673 1595813 **492366587**	72	
23	13 2481757 13703077[1]	73	3
24	5 25633	74	5
26	3 5 71 **486999673**	75	17 43 347 31247
28	3 19 23	76	5 37 1109 9241 661049
29		77	32687
30	7 160541	78	43 151 181 1163 56149 **4229335793**
31	7 79 6451 **2806861**	79	7 263 3037 **1012573** **60312841**
33	233 47441	80	3 7 13 6343
34		82	3 5
35	3 1613 3571	83	4871 13691 **315746063**
37	3 77867	84	163 653 20101
38	17 127	85	11779
39	8039	86	68239
40	11 17 307 66431	87	1999 48121
41	29 1025273 **138200401**	88	**2535619637**
42	23	89	3 13
43	5 103	90	
44	3 229 5851	91	3 293
45	1283 131759 **157635607**	92	727 383951 **12026117** **18768727** **1485161969**
46	3 829	93	5 509 9221 81551
47		94	11 241 32143 463033
48	7 257	95	2137 15061
50	7	96	109 5437 8329 **12925267**
51	5 41	97	7 **2914393**
52	461 **1228488439**	98	3 28627 **61001527**
53	3 47 59 97	99	5 7 13 19 83
54	19 1949		

[1] Incorrectly printed as "1370377" in [2].

2. PROGRAMMING CONSIDERATIONS

As in [2] and [3], it suffices to compute the last two digits of the base p representation of each intermediate result. Since (1) is equivalent to $a^{(p-1)/2} \equiv \pm 1 \pmod{p^2}$, we can save a squaring mod p^2.

The programs in [2] fixed the base a and looped through values of p. One can instead check all values of a together for a given p. Then the value of $a^{(p-1)/2} \pmod{p^2}$ need be calculated the long way (binary method of exponentiation) only for prime a: if $a = a_1 a_2$ where

$$a_1^{(p-1)/2} \equiv \pm(1 + pb_1) \pmod{p^2} \quad \text{and} \quad a_2^{(p-1)/2} \equiv \pm(1 + pb_2) \pmod{p^2},$$

then $a^{(p-1)/2} \equiv \pm(1 + p(b_1 + b_2)) \pmod{p^2}$. The latter computation reduces to an addition modulo p. Since $\pi(100) = 25$ whereas there are 87 nonpowers below 100, this represents a potential 70% savings.

The search for $p < 2^{31}$ was done on a DECstation 3100 (MIPS architecture). To compute a product $ab \bmod p$ where $0 \le a,\ b < p$ but where ab may exceed the largest single-precision integer, the program computed $q = a \cdot b \cdot \frac{1+\epsilon}{p}$, using floating-point arithmetic, where $2^{-50} \ll \epsilon \ll 1/p$. The relative error in any floating-point computation is at most 2^{-52} (53-bit mantissas), ensuring that

$$\frac{ab}{p} \le q \le \frac{ab}{p}(1 + 1/p) < \frac{ab}{p} + 1$$

and hence that $\lfloor \frac{ab}{p} \rfloor \in \{\lfloor q \rfloor, \lfloor q \rfloor - 1\}$; the choice is made using the sign of $r = ab - p\lfloor q \rfloor$. Since $-2^{31} < -p \le r < p < 2^{31}$, this r can be computed by integer arithmetic modulo 2^{32}.

This technique fails for $p > 2^{31}$ unless the program uses 64-bit arithmetic to compute the tentative remainder (it would also require converting unsigned 32-bit integers to/from floating point). Instead, the computations for $p > 2^{31}$ were done on a NeXT with a Motorola 68040 chip. The 68040 can divide a 64-bit unsigned integer by a 32-bit unsigned integer, obtaining quotient and remainder in one instruction (if the quotient does not overflow), but the MIPS architecture lacks such. The 3100 tried all primes in an interval of length 10 million per hour. The 68040 computations took slightly longer, searching an interval of length 7 million per hour.

Bibliography

1. M. Aaltonen and K. Inkeri, *Catalan's equation* $x^p - y^q = 1$ *and related congruences*, Math. Comp. **56** (1991), 359–370.
2. J. Brillhart, J. Tonascia, and P. Weinberger, *On the Fermat quotient*, Computers in Number Theory (A. O. L. Atkin and B. J. Birch, eds.), Academic Press, London and New York, 1971, pp. 213–222.
3. D. H. Lehmer, *On Fermat's quotient, base two*, Math. Comp. **36** (1981), 289–290.
4. Daniel Shanks and H. C. Williams, *Gunderson's function in Fermat's last theorem*, Math. Comp. **36** (1981), 291–295.
5. H. C. Williams, *The influence of computers in the development of number theory*, Comput. Math. Appl. **8** (1982), 75–93.

Department of Mathematics, Oregon State University, Corvallis, Oregon 97331-4605

E-mail address: pmontgom@math.orst.edu