MATHEMATICS OF COMPUTATION
Volume 74, Number 250, Pages 927–936
S 0025-5718(04)01666-7
Article electronically published on June 8, 2004

# SOLUTIONS OF THE CONGRUENCE $a^{p-1} \equiv 1 \pmod{p^r}$

WILFRID KELLER AND JÖRG RICHSTEIN

Abstract. To supplement existing data, solutions of $a^{p-1} \equiv 1 \pmod{p^2}$ are tabulated for primes $a, p$ with $100 < a < 1000$ and $10^4 < p < 10^{11}$. For $a < 100$, five new solutions $p > 2^{32}$ are presented. One of these, $p = 188748146801$ for $a = 5$, also satisfies the "reverse" congruence $p^{a-1} \equiv 1 \pmod{a^2}$. An effective procedure for searching for such "double solutions" is described and applied to the range $a < 10^6$, $p < \max(10^{11}, a^2)$. Previous to this, congruences $a^{p-1} \equiv 1 \pmod{p^r}$ are generally considered for any $r \geq 2$ and fixed prime $p$ to see where the smallest prime solution $a$ occurs.

## 1. Introduction

In this paper we will be concerned with solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$, where the base $a$ is not a power of another integer, $p$ is an odd prime, and $r \geq 2$. The congruence is of interest in relation to several number-theoretical questions, as is summarized in [4]; see also the bibliography therein.

Historically, much computational effort has been devoted to finding solutions $p$ in the particular case of $r = 2$ and small fixed bases $a$. Especially for $a = 2$, where only the two celebrated solutions $p = 1093$ and $p = 3511$ are known, the search has been pushed to considerably high limits, more recently in [6] up to $4 \cdot 10^{12}$, and then extended to $8 \cdot 10^{12}$ by R. McIntosh [14] and to $4.8 \cdot 10^{13}$ by R. Brown [5]. Finally, an Internet based search conducted by J. Knauer and the second author [13] attained the limit of $1.25 \cdot 10^{15}$. For bases in the range $2 < a < 100$, the first substantial tabulation is found in [4], which covers, at least, all solutions $p < 10^6$, and was subsequently extended to $2 \cdot 10^8$ in [11] and to $2^{32}$ in [18].

For the range $100 < a < 1000$, solutions $p < 10^4$ are given in Table 1 of [1] for prime bases $a$ only. In this table, the omission of three consecutive lines should be noted, corresponding (in our notation) to $a = 709$, with solutions $p = 17$, 199, 1663, to $a = 719$ with $p = 3$, 41, and to $a = 727$ with $p = 11$. M. Aaltonen has kindly informed us that these additions conform with the original data produced for the paper [1], so the missing lines were obviously lost during the typesetting process.

Extending those data, in our Table 1 we present all 133 solutions $p$ existing for $10^4 < p < 10^{11}$. For the bases $a = 103$, 167, 211, 281, 283, 383, 409, 563, 661, 769, 853, 877, and 929 no solution was previously known, so in each case the smallest one is shown in the table.

---

Received by the editor July 30, 2001 and, in revised form, September 1, 2003.
2000 *Mathematics Subject Classification.* Primary 11A07; Secondary 11D61, 11–04.
*Key words and phrases.* Fermat quotient, Diophantine equation, primitive roots, large primes.
The second author was supported by the Killam Trusts.

TABLE 1. Solutions of $a^{p-1} \equiv 1 \pmod{p^2}$ for primes $a$, $p$ with $100 < a < 1000$ and $10^4 < p < 10^{11}$

| $a$ | $p$ | $a$ | $p$ | $a$ | $p$ |
|---|---|---|---|---|---|
| 101 | 1050139 | 283 | 46301 | 641 | 24481 |
| 103 | 24490789 | 313 | 1259389 | 643 | 460609 |
| 107 | 613181 | 317 | 2227301 | | 7354807 |
| 109 | 20252173 | 331 | 6134718817 | 647 | 15266862761 |
| 127 | 13778951 | 337 | 30137417 | 653 | 22171 |
| 131 | 754480919 | 353 | 465989 | | 637699 |
| 137 | 18951271 | | 17283818861 | 659 | 65983 |
| | 4483681903 | 359 | 24350087 | 661 | 441583073 |
| 149 | 29573 | 383 | 28067251 | 691 | 84131 |
| | 121456243 | 389 | 29569 | | 10843045487 |
| | 2283131621 | | 211850543 | 719 | 4414200313 |
| 151 | 14107 | 397 | 279421 | 739 | 5681059 |
| | 5288341 | | 13315373041 | 757 | 242789 |
| | 15697215641 | 401 | 115849 | 769 | 1305827821 |
| 157 | 122327 | 409 | 34583 | 773 | 787711 |
| | 4242923 | | 1894600969 | | 26259199 |
| | 5857727461 | 419 | 22891217 | | 142719149 |
| 163 | 3898031 | 421 | 350677 | 787 | 427541 |
| 167 | 64661497 | 431 | 12755833 | 797 | 14607661 |
| 173 | 56087 | 433 | 129497 | 809 | 448110371 |
| 179 | 35059 | | 244403 | 821 | 37871 |
| | 126443 | 439 | 170899693 | | 209140301 |
| 191 | 379133 | 443 | 3406223 | 839 | 11840951 |
| 197 | 6237773 | 457 | 1589513 | 853 | 1125407 |
| 199 | 77263 | 479 | 500239 | 857 | 32478247 |
| | 1843757 | 491 | 661763933 | 863 | 12049 |
| 211 | 279311 | 499 | 81307 | 877 | 78926821 |
| 227 | 40277 | | 24117560837 | 881 | 22385723 |
| 233 | 86735239 | 509 | 7215975149 | | 94626144313 |
| 239 | 74047 | 521 | 8938997 | 887 | 60623 |
| | 212855197 | 523 | 19289 | 907 | 3497891 |
| | 361552687 | 547 | 1691778551 | 911 | 318917 |
| | 12502228667 | 557 | 39829 | 929 | 62199604679 |
| 241 | 35407 | 563 | 18920521 | 937 | 22343 |
| 251 | 395696461 | 569 | 25359067 | | 500861 |
| 257 | 49559 | 571 | 308383 | | 1031299 |
| | 648258371 | 577 | 1381277 | | 258469889 |
| 263 | 267541 | 587 | 22091 | 953 | 513405611 |
| | 159838801 | | 6343317671 | 967 | 44830663 |
| 269 | 65684482177 | 599 | 35771 | 971 | 401839 |
| 271 | 168629 | 607 | 40303229 | | 7672759 |
| | 16774141 | 613 | 81371669 | 977 | 37589 |
| | 235558417 | | 18419352383 | 991 | 26437 |
| | 12145092821 | 619 | 11682481 | | |
| 281 | 3443059 | | 52649183399 | | |

For prime bases $a < 100$ we also searched the interval $2^{32} < p < 10^{11}$, obtaining four new solutions characterized by the following pairs $(a, p)$:

$$(5, 6692367337),\ (23, 15546404183),\ (37, 76407520781),\ (97, 76704103313).$$

While in [18] the only prime bases $a < 100$ that remained without a solution $p < 2^{32}$ were $a = 29$, 47, 61, we can now assert that for $a = 29$, 47, 61, 113, 139, 311, 347, 983 the smallest solution, if one exists, must be greater than $10^{11}$.

The particular cases of $a = 3$ and $a = 5$ were further examined up to $p < 10^{13}$, which revealed one more solution for $a = 5$. Thus, the congruence $5^{p-1} \equiv 1 \pmod{p^2}$ is now known to hold for

$$p = 20771,\ 40487,\ 53471161,\ 1645333507,\ 6692367337,\ 188748146801,$$

and for no other $p < 10^{13}$. The first two of these solutions were found by Riesel in 1961 (as reported in [20]), the third was first published in [4], and the fourth was found by Montgomery [18].

In [8] it was noted that $p = 1645333507$ produced 14 solutions $(a, p)$ with $a < p$, the highest number of solutions known for a prime $p$. This is a consequence of the fact that for a small basis $a$ satisfying the congruence, the power $a^n$, which also gives a solution, remains below $p$ for several successive exponents $n$, and additional solutions with $a < p$ might also occur. Accordingly, we observed that $p = 6692367337$ has $5^n < p$ for $n = 1, 2, \ldots, 14$, and $a^{p-1} \equiv 1 \pmod{p^2}$ is also satisfied for $a = 4961139411$ and for $a = 6462265338$, giving a total of 16 solutions $a < p$. For $p = 188748146801$, instead, we have $5^n < p$ for $n = 1, 2, \ldots, 16$, but no further solution $a < p$ exists.

The solution $(a, p) = (5, 188748146801)$ turned out to be one of those exceptional instances where the "reverse" congruence $p^{a-1} \equiv 1 \pmod{a^2}$ is also satisfied. Aside from $(a, p) = (3, 1006003)$ and $(a, p) = (5, 1645333507)$, presented in [1] and [18], respectively, only three such pairs of odd primes with $a, p > 5$ were previously known; see [8] and §4. All of them had $a, p < 10^6$. Through a systematic search restricted to such occurrences, we were able to show that no other pair of this kind exists in the range $a < 10^6$, $p < \max(10^{11}, a^2)$. The details will also be given in §4.

As is usual, for all the solutions found, we checked if they satisfied $a^{p-1} \equiv 1 \pmod{p^3}$, but this was never the case. One might suspect that, except for the smallest odd primes $p = 3$ and $p = 5$, this would generally be a rare event. In fact, in the range of Table 1 in [18] only the pairs $(a, p) = (18, 7)$, $(19, 7)$, $(42, 23)$ and $(68, 113)$ lead to such a solution, apparently supporting that impression. None of these pairs satisfies the congruence for the modulus $p^4$.

Nevertheless, it has been known for more than a century [7] that for any power $p^r$ of an arbitrarily chosen prime $p$, infinitely many bases $a$ exist for which $a^{p-1} \equiv 1 \pmod{p^r}$ is satisfied and that a complete incongruent set of them may be determined quite easily. Moreover, the totality of those bases $a$ happens to include an infinitude of primes. On the other hand, for increasing exponents $r$ the first appropriate $a$, prime or not, may be quite a large number. We will be exhibiting the smallest prime solution for $p = 3$ and $r = 165896$, which is a number of 79153 decimal digits.

Finally, we note that for bases $a \leq 1000$ including composite values of $a$, a complete table of solutions has been produced for $p < 10^{10}$ and is available from the authors. For easier reference, an excerpt covering prime bases only can be seen at [12]. The complete table contains 2735 solutions $(a, p)$. The number of solutions observed for each $a$ gives the frequencies 60, 145, 273, 229, 171, 70, 37, 11, and 3 for the occurrence of 0, 1, 2, 3, 4, 5, 6, 7, or 8 solutions, respectively. The highest number of eight known solutions corresponds to the composite bases $a = 260$, 476, and to the prime base $a = 937$. For this prime base the solutions are $p = 3$, 41, 113, 853, 22343, 500861, 1031299, 258469889.

## 2. Solutions $a$ for fixed modulus $p^r$

Probably the first concise statement about the solutions of $a^{p-1} \equiv 1 \pmod{p^r}$ for a fixed modulus $p^r$ is the following theorem proved by Meyer [16] in 1902.

**Theorem 1.** *Let $p$ be a prime, $r \geq 2$, and consider the set of $p^{r-1}(p-1)$ integers $a < p^r$ such that $(a,p) = 1$. Then $a^{p-1} - 1$ is divisible by $p^s$, $s = 1, 2, \ldots, r-1$, but not by $p^{s+1}$, for exactly $p^{r-1-s}(p-1)^2$ of these integers $a$, and is divisible by $p^r$ for the remaining $p-1$ such integers.*

As a corollary, we see that $a^{p-1} \equiv 1 \pmod{p^r}$ has exactly $p-1$ solutions that are incongruent modulo $p^r$, independent of the exponent $r$. These solutions occur in pairs $a$, $p^r - a$ and include the trivial solutions 1, $p^r - 1$. Therefore a listing of the $(p-3)/2$ solutions in the interval $1 < a < (p^r - 1)/2$ would suffice to describe the complete set.

Remarkably, the algorithmic determination of these solutions was also mastered more than a century ago. Thus, Cunningham [7] tabulated the solutions $a$ for $r = 2$ and all $p \leq 101$ in 1900. But he also gave (with perfect accuracy) the solutions for higher powers $p^r$, which include $5^r$ up to $r = 8$ and $7^r$ up to $r = 9$. From his tables we learn, in particular, that the four nontrivial solutions of $a^6 \equiv 1 \pmod{7^9}$ are

$$a = 14906455,\ 14906456,\ 25447151,\ 25447152.$$

The tabulation for $r = 2$ was extended to $p < 200$ by Beeger [2] and to $p < 500$ by Meissner [15], both in 1914. Meissner's table, however, was not included in his paper.

Apparently the first comprehensive table of solutions produced in the computer age is the recent one of Ernvall and Metsänkylä [8], who listed all pairs $a, p < 10^6$ satisfying $a^{p-1} \equiv 1 \pmod{p^2}$, with inclusion of bases $a$ that are congruent modulo $p^2$. Also in [8] it was shown that the closest possible proximity of two solutions as observed in the Cunningham example above is a quite general phenomenon. In fact, for every prime $p \equiv 1 \pmod 6$ and each $r \geq 2$ there exists a solution $a$ such that $a + 1$ also satisfies the congruence. For $r = 2$ this had already been proven by Beeger [2].

As to the computational aspect, we note that the clue for an effective determination of the solutions for $r = 2$ was given, and exemplified for $p = 11$, by Worms de Romilly [21] in a charming little note of 1901. The procedure was restated and extensively used by Beeger in [2]. It can be expressed more generally as follows.

**Theorem 2.** *Let $a_1$ be a primitive root of the prime $p$ and define $a_r = a_1^{p^{r-1}} \bmod p^r$ for any $r \geq 2$. Then $\{a_r^m \bmod p^r : m = 0, 1, \ldots, p-2\}$ represents a complete set of incongruent solutions of $a^{p-1} \equiv 1 \pmod{p^r}$, each of which generates an infinite sequence of solutions in arithmetic progression with difference $p^r$.*

The listed solutions $a_r^m \bmod p^r$ may be given in a computationally more convenient form, which is derived from the fact that for a primitive root $a_1$ of $p$ we always have $a_r^{(p-1)/2} \equiv -1 \pmod{p^r}$. As a consequence, $a_r^{(p-1)/2+m} \equiv -a_r^m \pmod{p^r}$ for $m = 0, 1, \dots (p-3)/2$. Hence the set of incongruent solutions is equivalently described by $\{\pm a_r^m \bmod p^r : m = 0, 1, \dots, (p-3)/2\}$.

As an example, consider $p = 7$, $r = 2$, $a_1 = 3$, $a_2 = 31$. The expression $a_r^m \bmod p^r$ gives $a_2^m \equiv 1, 31, 30 \pmod{49}$ for $m = 0, 1, 2$, the companion solutions being $-1 \equiv 48$, $-31 \equiv 18$, $-30 \equiv 19$. In increasing order we then have the solutions $a = 1, 18, 19, 30, 31, 48$, and all those obtained by successively adding $7^2 = 49$, starting with $a = 50, 67, 68, 79, 80, 97, 99$. Thus, in the range of Table 1 in [4], which is $1 < a < 100$, the prime $p = 7$ must occur as a solution for 12 different bases $a$, which is in accordance with the table.

By using the same procedure, we can now determine for which of those bases the congruence $a^{p-1} \equiv 1 \pmod{p^3}$ is also satisfied. With $a_3 = 325$ we get the solutions $a = 1, 18, 19, 324, 325, 342, \dots$, two of which are within the range of the considered table.

For the larger table covering $1 < a \le 1000$, mentioned in §1, we could have predicted that it contains $999 \cdot 2/3^2 = 222$ pairs $(a, 3)$, as well as $\lfloor 999 \cdot 4/5^2 \rfloor = 159$ pairs $(a, 5)$ and $\lfloor 999 \cdot 6/7^2 \rfloor = 122$ pairs $(a, 7)$. Moreover, the expression $999 \cdot \sum (p-1)/p^2$, extended to all odd primes $p < 10^5$, should give a good estimate for the number of solutions $(a, p)$ with $p$ in that range. In fact, while about 2001 solutions are predicted, 2020 are actually counted in the table.

## 3. The smallest prime solution $a$

Turning our attention now to prime solutions $a$, we know by Dirichlet's theorem that infinitely many do exist for any modulus $p^r$. In our examples for $p = 7$, $r = 2$, 3, we readily found a prime base, $a = 19$, which, incidentally, was the same for both exponents. But this cannot always be expected. For instance, in the case $p = 11$, $r = 3$, by the above procedure we would have had to list 19 composite solutions $a$ before encountering the first prime solution $q = 2663$. It is therefore desirable to have an easily computable upper bound for the first occurrence of a prime solution $q$, which may be obtained by exhibiting a well-defined example.

**Theorem 3.** *Let $q_{+1}$ be the smallest prime of the form $2hp^r + 1$, let $q_{-1}$ be the smallest prime of the form $2hp^r - 1$, and define $q_0 = \min(q_{+1}, q_{-1})$. Then $a = q_0$ is a prime solution of $a^{p-1} \equiv 1 \pmod{p^r}$. For $p = 3$, this is always the smallest prime solution.*

For the proof we assume $p - 1 = d \cdot 2^s$ with $d$ odd. Then we have the factorization

$$a^{d \cdot 2^s} - 1 = (a^d - 1)(a^d + 1) \prod_{i=1}^{s-1} (a^{d \cdot 2^i} + 1),$$

where $a^d - 1$ is always divisible by $a - 1$ and $a^d + 1$ is divisible by $a + 1$ whenever $d$ is odd, which we are assuming. Therefore, if either $a - 1$ or $a + 1$ is an even multiple of $p^r$, say $2hp^r$, then $a = 2hp^r + 1$ or $a = 2hp^r - 1$, respectively, is an odd solution of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. Since these solutions are in arithmetic progression, we have only to search, in each case, for the first $h$ making $a$ a prime to settle the main statement of the theorem.

For $p = 3$ the above factorization simplifies to $a^2 - 1 = (a-1)(a+1)$, implying that every prime solution $a > 2$ must be of one of the forms $2h \cdot 3^r + 1$ or $2h \cdot 3^r - 1$.

TABLE 2. Smallest solutions $a = q_{\min} \le q_0$ of $a^{p-1} \equiv 1 \pmod{p^r}$

| | $p$ | $q_{\min}$ | $q_0$ | $p$ | $q_{\min}$ | $q_0$ |
|---|---|---|---|---|---|---|
| $r = 2$ | 3 | 17 | 17 | 43 | 19 | 3697 |
| | 5 | 7 | 101 | 47 | 53 | 8837 |
| | 7 | 19 | 97 | 53 | 521 | 56179 |
| | 11 | 3 | 241 | 59 | 53 | 6961 |
| | 13 | 19 | 337 | 61 | 601 | 44651 |
| | 17 | 131 | 577 | 67 | 1301 | 17957 |
| | 19 | 127 | 2887 | 71 | 11 | 50411 |
| | 23 | 263 | 4231 | 73 | 619 | 10657 |
| | 29 | 41 | 10091 | 79 | 31 | 37447 |
| | 31 | 229 | 7687 | 83 | 269 | 41333 |
| | 37 | 691 | 5477 | 89 | 3187 | 47527 |
| | 41 | 313 | 3361 | 97 | 53 | 56453 |
| $r = 3$ | 3 | 53 | 53 | 43 | 3623 | 159013 |
| | 5 | 193 | 251 | 47 | 6397 | 1245877 |
| | 7 | 19 | 1373 | 53 | 9283 | 893261 |
| | 11 | 2663 | 2663 | 59 | 63463 | 410759 |
| | 13 | 239 | 13183 | 61 | 38447 | 453961 |
| | 17 | 653 | 78607 | 67 | 36809 | 1804577 |
| | 19 | 2819 | 27437 | 71 | 21499 | 715823 |
| | 23 | 8401 | 194671 | 73 | 75227 | 1556069 |
| | 29 | 10133 | 48779 | 79 | 1523 | 2958233 |
| | 31 | 6287 | 59581 | 83 | 55933 | 9148591 |
| | 37 | 691 | 202613 | 89 | 42937 | 8459629 |
| | 41 | 10399 | 413527 | 97 | 341293 | 5476039 |

When $p > 3$, the prime $q_0$ defined by the theorem can sometimes also be the smallest prime solution of all, as in the above example of $p = 11$, $r = 3$, where $q_0 = q_{+1} = 2 \cdot 11^3 + 1 = 2663$ while $2 \cdot 11^3 - 1$ is divisible by 3.

In Table 2 and Table 3 some specific results illustrating the above can be seen for primes $p < 100$ and $2 \le r \le 5$, as well as for a few small primes and moduli up to $r = 10$. Note the case of $p = 7$, $r = 9$ in relation to Cunningham's example.

Table 4 reflects the fact that with current computational means the smallest solution with $p = 3$ can easily be determined for quite arbitrary large exponents $r$. Considerably larger examples are found for some isolated values of $r$. In fact, if $a = 2 \cdot 3^r - 1$ is a prime, then the congruence $a^2 \equiv 1 \pmod{3^r}$ is satisfied for this but for no smaller prime base $a$. Similarly, if $a = 2 \cdot 3^r + 1$ is a prime and the companion number $2 \cdot 3^r - 1$ is not, then again we have at once the smallest prime solution $a$ for the corresponding power $p^r$.

We have shown that $2 \cdot 3^r - 1$ is prime for $r = 1$, 2, 3, 7, 8, 12, 20, 23, 27, 35, 56, 62, 68, 131, 222, 384, 387, 579, 644, 1772, 3751, 5270, 6335, 8544, 9204, 12312, 18806, 21114, 49340, 75551, 90012, and for no other $r \le 100000$.

Also, it is known that $2 \cdot 3^r + 1$ is prime for $r = 1$, 2, 4, 5, 6, 9, 16, 17, 30, 54, 57, 60, 65, 132, 180, 320, 696, 782, 822, 897, 1252, 1454, 4217, 5480, 6225, 7842, 12096, 13782, 17720, 43956, 64822, 82780, 105106, 152529, 165896, and for no other $r \le 170000$.

These findings yield, in particular, the explicit expression for the smallest prime solution modulo the power $3^r$ for each of the exponents $r = 1252$, 1454, 1772, 3751,

TABLE 3. Smallest solutions $a = q_{\min}$ of $a^{p-1} \equiv 1 \pmod{p^r}$

| | $p$ | $q_{\min}$ | $p$ | $q_{\min}$ | $p$ | $q_{\min}$ |
|---|---|---|---|---|---|---|
| $r = 4$ | 3 | 163 | 29 | 78017 | 61 | 8065789 |
| | 5 | 443 | 31 | 690143 | 67 | 3246107 |
| | 7 | 3449 | 37 | 398023 | 71 | 1353383 |
| | 11 | 45989 | 41 | 1977343 | 73 | 5934307 |
| | 13 | 239 | 43 | 574081 | 79 | 15631613 |
| | 17 | 15541 | 47 | 1513367 | 83 | 2864371 |
| | 19 | 2819 | 53 | 4388179 | 89 | 14754769 |
| | 23 | 60793 | 59 | 3198427 | 97 | 15012733 |
| $r = 5$ | 3 | 487 | 29 | 24639193 | 61 | 130702609 |
| | 5 | 14557 | 31 | 40373093 | 67 | 304154189 |
| | 7 | 32261 | 37 | 70697317 | 71 | 143584109 |
| | 11 | 275393 | 41 | 31851901 | 73 | 183298237 |
| | 13 | 220861 | 43 | 47289133 | 79 | 79451167 |
| | 17 | 15541 | 47 | 456330179 | 83 | 1058782027 |
| | 19 | 2342959 | 53 | 10000453 | 89 | 352845203 |
| | 23 | 1051847 | 59 | 154075723 | 97 | 567620413 |
| $r = 6$ | 3 | 1459 | 11 | 2120879 | 19 | 2342959 |
| | 5 | 14557 | 13 | 7654109 | 23 | 90603883 |
| | 7 | 152617 | 17 | 24527681 | | |
| $r = 7$ | 3 | 4373 | 7 | 3294173 | 11 | 28723679 |
| | 5 | 735443 | | | | |
| $r = 8$ | 3 | 13121 | 7 | 3376853 | 11 | 174625993 |
| | 5 | 3124999 | | | | |
| $r = 9$ | 3 | 39367 | 5 | 7812499 | 7 | 135967277 |
| $r = 10$ | 3 | 472391 | 5 | 78124999 | 7 | 135967277 |

TABLE 4. Smallest solutions $a = q_0 = 2h \cdot 3^r + \varepsilon$ of $a^2 \equiv 1 \pmod{3^r}$

| $r$ | $h$ | $\varepsilon$ | $r$ | $h$ | $\varepsilon$ | $r$ | $h$ | $\varepsilon$ |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | $-1$ | 20 | 1 | $-1$ | 200 | 6 | $+1$ |
| 3 | 1 | $-1$ | 30 | 1 | $+1$ | 300 | 79 | $+1$ |
| 4 | 1 | $+1$ | 40 | 20 | $-1$ | 400 | 56 | $+1$ |
| 5 | 1 | $+1$ | 50 | 4 | $-1$ | 500 | 39 | $+1$ |
| 6 | 1 | $+1$ | 60 | 1 | $+1$ | 600 | 602 | $-1$ |
| 7 | 1 | $-1$ | 70 | 5 | $-1$ | 700 | 11 | $+1$ |
| 8 | 1 | $-1$ | 80 | 7 | $-1$ | 800 | 35 | $+1$ |
| 9 | 1 | $+1$ | 90 | 22 | $+1$ | 900 | 61 | $+1$ |
| 10 | 4 | $-1$ | 100 | 45 | $-1$ | 1000 | 51 | $+1$ |

4217, 5270, 5480, 6225, 6335, 7842, 8544, 9204, 12096, 12312, 13782, 17720, 18806, 21114, 43956, 49340, 64822, 75551, 82780, 90012, 105106, 152529, 165896. The prime $a = 2 \cdot 3^{165896} + 1$ has 79153 digits.

It should be remarked that most of the primality proofs were accomplished with Gallot's excellent program `Proth.exe` [9]. The seven primes having $r > 50000$ were discovered by I. Buechel and the first author in the period 1999–2003, using that program.

TABLE 5. Values of $r$ where the smallest prime solution of $a^4 \equiv 1 \pmod{5^r}$ is $a = q_0 = 2h \cdot 5^r + \varepsilon$

| $r$ | $h$ | $\varepsilon$ | $r$ | $h$ | $\varepsilon$ | $r$ | $h$ | $\varepsilon$ |
|---|---|---|---|---|---|---|---|---|
| 8 | 4 | −1 | 40 | 11 | +1 | 63 | 3 | +1 |
| 9 | 2 | −1 | 41 | 28 | +1 | 65 | 3 | −1 |
| 10 | 4 | −1 | 42 | 8 | +1 | 66 | 9 | −1 |
| 11 | 3 | −1 | 44 | 5 | +1 | 69 | 2 | −1 |
| 13 | 1 | +1 | 45 | 1 | +1 | 71 | 15 | −1 |
| 15 | 2 | −1 | 46 | 6 | +1 | 72 | 3 | −1 |
| 23 | 3 | +1 | 47 | 12 | +1 | 81 | 6 | −1 |
| 24 | 1 | −1 | 48 | 6 | −1 | 83 | 18 | +1 |
| 26 | 8 | +1 | 49 | 9 | −1 | 84 | 28 | −1 |
| 27 | 3 | +1 | 50 | 2 | +1 | 85 | 27 | −1 |
| 28 | 3 | −1 | 51 | 6 | −1 | 88 | 55 | −1 |
| 30 | 1 | −1 | 52 | 25 | −1 | 89 | 11 | −1 |
| 33 | 3 | +1 | 53 | 5 | −1 | 95 | 5 | −1 |
| 36 | 13 | −1 | 54 | 1 | −1 | 96 | 1 | −1 |
| 38 | 10 | −1 | 60 | 12 | −1 | 98 | 24 | +1 |
| 39 | 2 | −1 | 62 | 15 | +1 | 99 | 13 | +1 |

Beyond $p = 3$, the case of $p = 5$ might also be of special interest. Since for this prime we have

$$a^{p-1} - 1 = a^4 - 1 = (a-1)(a+1)(a^2+1),$$

the smallest prime solution of $a^4 \equiv 1 \pmod{5^r}$ must be of the form $a = 2h \cdot 5^r + 1$ or of the form $a = 2h \cdot 5^r - 1$, or it must be a solution of the congruence $a^2 \equiv -1 \pmod{5^r}$. The latter has two different roots for each $r$ that can be determined recursively (cf. [3], p. 198). However, to see whether the smallest prime base $a$ satisfying $a^4 \equiv 1 \pmod{5^r}$ is one of these roots, it is not necessary to know them in advance. Instead, we can use our general procedure for finding the smallest appropriate prime $a$ of all and then compare with the smallest primes of the forms $a = 2h \cdot 5^r \pm 1$. This was actually carried out for all $r \leq 300$. The result for $r \leq 100$ is shown in Table 5. Exponents that are not listed have their least prime solution satisfying $a^2 \equiv -1 \pmod{5^r}$. This is observed for a total of 191 exponents $r \leq 300$.

Returning to the more modest dimensions of Table 2, we note in its first segment devoted to $r = 2$ that the smallest prime solution $q_{\min}$ may sometimes be smaller than $p$, as is the case for $p = 11$, 43, 59, 71, 79, and 97. It has generally been asked [19, p. 345] how many prime solutions $a < p$ or even $a < \sqrt{p}$ of $a^{p-1} \equiv 1 \pmod{p^2}$ may exist for a fixed prime $p$.

We have examined all 664577 primes $p$ with $5 \leq p < 10^7$ in this regard. It turned out that 618178 = 93.02% of these primes do not have one single prime solution $a < p$, or, in other terms, for all these primes we have $q_{\min} > p$. For the remaining 46399 primes with $q_{\min} < p$, the exact number of prime solutions $a < p$ is 1, 2, 3, or 4 for 44784, 1575, 37 and 3 primes $p$, respectively. Four such solutions were found for $p = 24329$, with $a = 1777$, 3301, 4919, 13691, for $p = 2105669$, with $a = 248891$, 654923, 1296877, 1865299, and for $p = 9656869$, with $a = 788393$, 1639607, 1786913, 7860337. Only 76 primes $p$ show just one prime solution $a < \sqrt{p}$, the smallest being $p = 11$, as seen in Table 2.

## 4. Search for prime bases $a$ satisfying the "reverse" congruence

As was mentioned in §1, only three pairs $(a, p)$ of primes with $a, p > 5$ are currently known which simultaneously satisfy both congruences

$$a^{p-1} \equiv 1 \pmod{p^2} \qquad \text{and} \qquad p^{a-1} \equiv 1 \pmod{a^2}.$$

These pairs are $(a, p) = (4871, 83)$, $(18787, 2903)$, and $(318917, 911)$. The first one was discovered by M. Aaltonen (see [10]) and the other two by Mignotte and Roy [17]. Note that the last pair also appeared in our Table 1 (in reverse order). The paper [10] and the report [17] point to the most important application of those pairs, which is the study of Catalan's equation.

Consistently using the procedure outlined in Theorem 2, the search for pairs $(a, p)$ satisfying both of the above congruences can be carried out with great efficiency, and some insights about the chances of finding a new one might possibly be obtained.

We know how to generate a complete sequence of bases $a$ satisfying the first congruence, up to some arbitrary limit. Since we are interested in prime bases only, the composite ones can be eliminated by some convenient sieving process. Then only the remaining bases $a$ have to be checked out as possible solutions of the second congruence. As an example, let us consider the case of $p = 83$. The first prime solutions $a$ are

$$a = 269, 293, 401, 821, 1451, 1453, 2161, 2633, 3181, 3851, \mathbf{4871}, 5839, \ldots\ ,$$

the eleventh of which yields the known solution. Up to this point, the other 641 existing odd primes could implicitly be ignored. More generally, to the limit of $a < 10^7$, of the existing 664578 odd primes only 8001 had to be tested. Similarly, for $p = 2903$ the prime bases $a$ to be taken into account are

$$a = 5347, 11593, \mathbf{18787}, 35437, 38651, 45821, 205991, 213611, 252667, \ldots\ ,$$

altogether 231 of the 664578 odd primes existing below $10^7$.

The quantitative version of Dirichlet's theorem about primes in an arithmetic progression (see [19, pp. 274–275]) leads to the general statement that for a fixed prime $p$ and a high limit $N$ for $a$, about $\pi(N)/(p-1)$ primes would have to be tested to reach that limit. Thus, for $p = 83$ and $p = 2903$ we obtain an estimate of 8104 and 229 primes, respectively, in good agreement with the actual frequencies.

Based on this approach, it would be desirable to derive some heuristic result about the expectation of encountering some new "double solution" $(a, p)$.

If a uniform upper limit $N$ is envisaged for the practical search, as $p$ becomes larger and larger, the complete set of incongruent basic solutions $a < p^2$ extends over an interval that eventually exceeds that limit. Since we cannot discern in advance which of the basic solutions to be generated would surpass the prescribed limit $N$, their totality has to be calculated anyway. Under these circumstances we found it reasonable always to sieve through the complete set of available "candidates" and to test the remainder for the desired property.

By actual computation we have determined that no further pair of those in question exists for $p < 10^6$ and $a < \max(10^{11}, p^2)$ or vice versa. The crossing point is $p \approx 316228$, and the highest of the varying limits attained was about $10^{12}$. In practice, multiples of 3, 5, 7, 11, or 13 among the generated odd values of $a$ were first eliminated, the remaining ones being subjected to a simple Fermat test. Although this procedure fails to detect a few composite values of $a$, testing them unnecessarily does not really affect the efficiency of the program.

We have also tested (or re-tested) the $44784 \cdot 1 + 1575 \cdot 2 + 37 \cdot 3 + 3 \cdot 4 = 48057$ pairs $(a, p)$ with $a < p < 10^7$ referred to at the end of §3, which slightly extends the covered range.

## References


1. M. Aaltonen and K. Inkeri, *Catalan's equation $x^p - y^q = 1$ and related congruences*, Math. Comp. **56** (1991), 359–370. MR 91g:11025
2. N. G. W. H. Beeger, *Quelques remarques sur les congruences $r^{p-1} \equiv 1 \pmod{p^2}$ et $(p-1)! \equiv -1 \pmod{p^2}$*, Messenger of Math. **43** (1914), 72–84.
3. D. Bressoud and S. Wagon, *A course in computational number theory*, Key College Publishing, Emeryville, CA, 2000. MR 2001f:11200
4. 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, 213–222. MR 47:3288
5. R. Brown, electronic mail dated 13 June 2001.
6. R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433–449. MR 97c:11004
7. A. Cunningham, *Period-lengths of circulates*, Messenger of Math. **29** (1900), 145–179.
8. R. Ernvall and T. Metsänkylä, *On the p-divisibility of Fermat quotients*, Math. Comp. **66** (1997), 1353–1365. `http://users.utu.fi/taumets/fermat/fermat.htm`. MR 97i:11003
9. Y. Gallot, `Proth.exe`: A Windows program for finding very large primes, `http://www.utm.edu/research/primes/programs/gallot/`.
10. K. Inkeri, *On Catalan's conjecture*, J. Number Theory **34** (1990), 142–152. MR 91e:11030
11. W. Keller, *New prime solutions p of $a^{p-1} \equiv 1 \pmod{p^2}$*, Abstracts Amer. Math. Soc. **9** (1988), 503.
12. W. Keller and J. Richstein, *Fermat quotients $q_p(a)$ that are divisible by p*, `http://www.informatik.uni-giessen.de/cnth/FermatQuotient.html`.
13. J. Knauer and J. Richstein, *The continuing search for Wieferich primes*, Math. Comp., to appear.
14. R. McIntosh, electronic mail dated 23 February 2001.
15. W. Meissner, *Über die Lösungen der Kongruenz $x^{p-1} \equiv 1 \bmod p^m$ und ihre Verwertung zur Periodenbestimmung* mod $p^\kappa$, Sitzungsber. Berliner Math. Ges. **13** (1914), 96–107.
16. W. F. Meyer, *Ergänzungen zum Fermatschen und Wilsonschen Satze*, Arch. Math. Physik (3) **2** (1902), 141–146.
17. M. Mignotte and Y. Roy, *L'équation de Catalan*, Prépubl. de l'IRMA 513/P-299, Université Louis Pasteur et CNRS, Strasbourg, 1992.
18. P. L. Montgomery, *New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$*, Math. Comp. **61** (1993), 361–363. MR 94d:11003
19. P. Ribenboim, *The new book of prime number records*, 3rd ed., Springer-Verlag, New York, 1996. MR 96k:11112
20. H. Riesel, *Note on the congruence $a^{p-1} \equiv 1 \pmod{p^2}$*, Math. Comp. **18** (1964), 149–150. MR 28:1156
21. Worms de Romilly, *Équation $a^{p-1} = 1 + \text{mult. } p^2$*, L'Intermédiaire des Math. **8** (1901), 214–215.



Universität Hamburg, 20146 Hamburg, Germany
*E-mail address*: `keller@rrz.uni-hamburg.de`

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia B3H 3J5, Canada
*E-mail address*: `joerg@mathstat.dal.ca`