MATHEMATICS OF COMPUTATION
VOLUME 56, NUMBER 193
JANUARY 1991, PAGES 359-370

CATALAN'S EQUATION $x^p - y^q = 1$ AND RELATED CONGRUENCES

M. AALTONEN AND K. INKERI

ABSTRACT. We investigate solutions of Catalan's equation $x^p - y^q = 1$ in nonzero integers x, y, p, q. By use of class numbers and congruences $p^q \equiv p \pmod{q^2}$ we show the impossibility of the equation for a large number of prime exponents p, q. Both theoretical and computer results are included. We also study lower bounds on possible, hitherto unknown, solutions $x, y > 2$; we especially wish to communicate the bound $x, y \geq 10^{500}$.

1. INTRODUCTION

Euler [4] proved in 1738 that in the sequence of squares and cubes of positive integers only $8 = 2^3$ and $9 = 3^2$ are consecutive. A century later, in 1844, Catalan conjectured more generally that there are no other consecutive nontrivial powers of positive integers, i.e., that the equation

$$x^p - y^q = 1 \tag{1}$$

has no other solutions in integers $x, y, p, q > 1$ except $x = q = 3, y = p = 2$. Even today, the conjecture is still an open problem. It is obviously sufficient to prove the conjecture when p and q are primes.

For some exponents p, q, besides Euler's case $p = 2, q = 3$, the validity of the conjecture is known. The case $q = 2, p \neq 3$ was solved by Lebesgue [13] in 1850, the cases $p = 3$ and $(q = 3, p \neq 2)$ by Nagell [14] in 1921 (or [18, pp. 198–199]), and the case $p = 2$ by Chao Ko [3] in 1964. A new step in this direction is a recent paper of Inkeri [8] (see also [7]), where it is shown that (1) has no solutions in nonzero integers for the following prime exponents p, q:

(i) $5 \leq p < 73$, $5 \leq q < 10^4$, $(p, q) \neq (19, 137), (53, 97), (53, 4889), (59, 2777), (61, 1861)$;
(ii) $5 \leq p, q < 89$;
(iii) $p \equiv q \equiv 3 \pmod 4$, $5 \leq p, q < 200$;
(iv) $p \equiv 3, q \equiv 1 \pmod 4$, $5 \leq p, q < 200$, $(p, q) \neq (19, 137), (107, 97)$.

Because of these results, we shall hereafter consider only prime exponents $p, q \geq 5$.

Received November 4, 1988; revised June 26, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D41, 11A07.

In principle, the conjecture can be verified, or a counterexample found, by exhaustive computations, for Tijdeman [22] proved in 1976 that there are no integral solutions of (1) if at least one of x, y, p, q exceeds a computable bound. In particular, as Langevin [12] has shown, $p, q < \exp 241 < 10^{105}$ and $x^p < \exp\exp\exp\exp 730$ for any solution of (1) in integers $x, y, p, q > 1$. For x and y we have the lower bounds

$$\begin{aligned} x &\geq \max\{p^{q-1}(q-1)^q + 1, q(2p+1)(2q^{p-1}+1)\}, \\ y &\geq \max\{q^{p-1}(p+1)^p - 1, p(q-1)(p^{q-1}(q-1)^q + 1)\}, \end{aligned} \tag{2}$$

due to Hyyrö [6], who also demonstrated that $x, y \geq 10^{11}$. As a corollary of (i)–(iv), Inkeri [8] improved this to $x, y > 10^{179}$. However, the region to be investigated is still far too vast for a proof of the conjecture by straightforward computations exhausting all possibilities.

In this paper we present extensions to the cases (iii) and (iv), and improvements on the lower bounds (2). We also exhibit the lower bound $x, y \geq 10^{500}$ We will, however, begin by proving in the next section some theoretical results that follow from the basic Theorem 1.

2. Some theoretical results

Let $h(-m)$ be the class number of the quadratic field $\mathbb{Q}(\sqrt{-m})$, ζ_m a primitive mth root of unity, and h_m the class number of the cyclotomic field $\mathbb{Q}(\zeta_m)$. The results (i)–(iv) are based on the following theorem (see [8]).

Theorem 1. *If p and q are odd primes for which $p^q \not\equiv p \pmod{q^2}$ and either $q \nmid h_p$ or both $p \equiv 3 \pmod 4$ and $q \nmid h(-p)$, then (1) has no solutions in nonzero integers x, y.*

Naturally, the theorem holds also with p and q interchanged, since $x^p - y^q = (-y)^q - (-x)^p$.

We now deduce from Theorem 1 some results giving simple sequences of pairs (p, q) for which (1) has only trivial solutions.

Corollary 1. *Suppose $q \nmid h_p$ or both $p \equiv 3 \pmod 4$ and $q \nmid h(-p)$. If $p = 2kq + e$ with $q \nmid k$ and $e^q \equiv e \pmod{q^2}$ (e.g., $e = \pm 1$), then equation (1) has only trivial solutions.*

Proof. By the assumptions,

$$p^q = (2kq + e)^q = (2kq)^q + \cdots + 2kq^2e^{q-1} + e^q \equiv e \pmod{q^2}.$$

We now easily see that

$$p^q \equiv p \pmod{q^2}$$

is absurd, since otherwise it would follow, by combining this and the former congruence, that $p = 2kq + e \equiv e \pmod{q^2}$ and so $q|k$, contrary to the assumption $q \nmid k$. Thus the assumptions of Theorem 1 are valid and our result follows. □

Let d be the discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$. It is well known (see [15, p. 389]) that for the class number $h(d)$ of this field the following estimates hold:

$$h(d) \le \frac{2}{\pi}|d|^{1/2}\left(1+\log\left(\frac{2}{\pi}|d|^{1/2}\right)\right) \tag{3}$$

and, if $|d| > \exp 24$,

$$h(d) \le \tfrac{1}{3}|d|^{1/2}\log|d|. \tag{4}$$

If $p \equiv 3 \pmod 4$, then in the field $\mathbb{Q}(\sqrt{-p})$, $d = -p$, and we shall later replace (4) also by the estimate

$$h(-p) \le \tfrac{1}{2}p^{1/2}\log p, \tag{5}$$

which is weaker than (4), but is valid for all primes in question (namely for $p \ge 7$), as one may infer from (3) by a simple calculation.

Lemma 1. *The class number $h(-p)$ of $\mathbb{Q}(\sqrt{-p})$ satisfies the condition $h(-p) < q$ in the following four cases*:

$$\text{(i) } p = 2q+1, \qquad \text{(ii) } p = 4q-1,$$
$$\text{(iii) } p = 6q+1, \qquad \text{(iv) } p < q^{1.462}, \qquad p \equiv 3 \pmod 4.$$

Proof. Clearly, $p \equiv 3 \pmod 4$ in every case. Since $h(-p) < p/4$ (see, e.g., [5]), $(2q+1)/4 < q$, and $(4q-1)/4 < q$, (i) and (ii) are obvious.

(iv) Let $2t = 1.462$. Now by (5) we have

$$\begin{aligned} h(-p)/q &\le \tfrac{1}{2}p^{1/2}\log p/q \\ &< (t/(1-t))\log q^{1-t}/q^{1-t} \le 731/(269e) < 1, \end{aligned}$$

and the result follows.

(iii) By a simple calculation it may easily be verified that

$$p/q = 6 + 1/q \le 6.2 < q^{0.462}, \tag{6}$$

when $q \ge 53$. If $5 \le q < 53$, then $p = 6q+1$ is a prime only for $q = 5, 7, 11, 13, 17, 23, 37, 47$. Correspondingly, $p = 31, 43, 67, 79, 103, 139, 223, 283$ and $h(-p) = 3, 1, 1, 5, 5, 3, 7, 3$ (see [1, Table 4]). Thus, it is immediately seen that $h(-p) < q$ for $q < 53$, and for $q \ge 53$ the same follows by (6) from case (iv). This finishes the proof. □

The following theorem brings to mind the well-known criterion of Sophie Germain (and its many analogies) concerning the first case of Fermat's Last Theorem.

Theorem 2. *Equation* (1) *has no solutions in nonzero integers x, y in the cases* (i), (ii), (iii) *mentioned in Lemma* 1, *and also in the last case* (iv) *provided that p can be presented in the form $2kq+e$, so that k and e satisfy the assumptions of Corollary* 1.

Proof. Above we have established that in every case, $p \equiv 3 \pmod 4$. From Lemma 1 it always follows that also $q \nmid h(-p)$. Finally, we see that p has the representation $p = 2kq + e$ required in Corollary 1. This corollary then gives the result for all four cases. □

Corollary 2. *Let* $q = kp + r$, *where* k *and* r *are some integers with* $k > 0$, $2 \nmid r$, $|r| < p$, $r^q \equiv r \pmod{q^2}$. *If* $p \equiv 3 \pmod 4$ *and* (1) *has a solution in nonzero integers, then*

$$pQ_q(k) \equiv -1 \pmod q, \tag{7}$$

where $Q_q(k) = (k^q - k)/q$. ($Q_q(k)$, or more commonly $Q_q(k)/k$, is called Fermat's quotient.)

Proof. Clearly, $2|k$ and $r > -p$, so that $q > (k-1)p \geq p$. Hence, $q \nmid rkh(-p)$. From Theorem 1 we have $p^q \equiv p \pmod{q^2}$ and thus

$$k^q p \equiv (kp)^q = (q - r)^q \equiv q^q - \cdots - r^q \equiv -r \pmod{q^2}.$$

Therefore,

$$0 \equiv k^q p + r = (k^q - k)p + q \pmod{q^2},$$

from which the result follows, dividing by q. □

Notice that (7), since $q = kp + r$, may also be written in the form

$$r(k^{q-1} - 1)/q \equiv 1 \pmod q.$$

Corollary 2 gives rise to the problem of determining the solutions of the congruence

$$(x^p - x)/p \equiv m \pmod p \qquad (m \text{ an integer, } p \text{ an odd prime }).$$

Obviously, it is sufficient to treat only the cases $m = 0, \dots, p-1$. As is well known, the congruence $x^p - x \equiv 0 \pmod{p^2}$ has exactly $p-1$ roots incongruent $\bmod\, p^2$ and prime to p. From this result we can easily see that the same is valid also for every congruence $x^p - x \equiv mp \pmod{p^2}$ $(m = 1, 2, \dots, p-1)$. Indeed, since for an integer x

$$(x - mp)^p = x^p - p^2 m x^{p-1} + \cdots - (mp)^p \equiv x^p \pmod{p^2},$$

the congruence $(x - mp)^p - (x - mp) \equiv mp \pmod{p^2}$ holds for every root x of $x^p \equiv x \pmod{p^2}$. These roots prime to p for the congruences with $m = 0, 1, \dots, p-1$ total $p(p-1)$ $(= \varphi(p^2)$, φ Euler's function). But this is exactly the number of the integers prime to p and pairwise incongruent $\bmod\, p^2$. Naturally, the set of these integers contain all the roots in question.

We still treat the corresponding question about the congruences $x^{p-1} - 1 \equiv mp \pmod{p^2}$ $(m = 0, 1, \dots, p-1)$ in a different way. In the interval $0 < x < p^2$, only the integers prime to p ($\varphi(p^2)$ in number) can now also be roots. If g is a primitive root $\bmod\, p^2$, then $(g^{r(p-1)} - 1)/p$ runs through a full residue system $\bmod\, p$ when r runs through the sequence $0, 1, \dots, p-1$. It is immediately seen that for $m \equiv (g^{r(p-1)} - 1)/p \pmod p$ at least the integers g^{tp+r} $(t = 0, 1, \dots, p-2)$ $(p-1$ in number) are roots of the above congruence.

All the p congruences thus have at least $p(p-1)$ roots. According to what was said above about the roots, we infer that every congruence has exactly $p-1$ roots (also in the case $m=0$).

We now treat briefly the connection of the difference $d=p-q$ with Theorem 1 and begin with the twin pairs p, q. Obviously, one of the members of a twin pair is congruent to $3 \pmod 4$.

Corollary 3. *Let* $p=q+2$. *If* (1) *has a solution in nonzero integers, then*

$$(8) \qquad p^q \equiv p \pmod{q^2} \quad \text{or} \quad q^p \equiv q \pmod{p^2}$$

according as $p \equiv 3 \pmod 4$ *or* $q \equiv 3 \pmod 4$.

Proof. For $p \equiv 3 \pmod 4$ we have $q \nmid h(-p)$, since $h(-p) < (q+2)/4 < q$. Likewise, for $q \equiv 3 \pmod 4$, $p \nmid h(-q)$, since $h(-q) < q < p$. The result follows immediately from Theorem 1. □

According to the table computed by the first author, (5,7) is the only twin pair (p, q) in the interval $0 < p, q < 10^4$ (cf. also Riesel's table and the table in this paper), for which (8) is valid (namely, $7^5 \equiv 7 \pmod{5^2}$). Recall that for the pair (5,7), equation (1) has only trivial solutions (see [8]).

Lemma 2. *If* $p-q=d$, *then*

$$(9) \qquad Q_q(p) \equiv Q_q(d) - 1 \pmod q, \qquad Q_p(q) \equiv -Q_p(d) - 1 \pmod p.$$

Proof. The first congruence in (9) follows directly from

$$p^q - p = (d+q)^q - (d+q) \equiv d^q - d - q \pmod{q^2},$$

dividing by q. In addition, we obtain also the second congruence, observing that $q-p=-d$ and $Q_p(-d) = -Q_p(d)$. □

The following includes Corollary 3.

Theorem 3. *Let* $p=q+d$ *with* $-3p < d < 3q$. *Suppose* (1) *has a solution in nonzero integers.*

(i) *If* $p \equiv 3$ *or* $q \equiv 3 \pmod 4$, *then, respectively,*

$$(10) \qquad Q_q(p) \equiv 0 \pmod q \quad \text{or} \quad Q_p(q) \equiv 0 \pmod p.$$

(ii) *If* $4|d$ *and* p (*and so also* q) *is congruent to* $3 \bmod 4$, *then* $Q_q(d) \equiv 1 \pmod q$ *and* $Q_p(d) \equiv -1 \pmod p$.

(iii) *If* $4 \nmid d$ (*i.e.,* $2\|d$), *then* $Q_q(d) \equiv 1 \pmod q$ *or* $Q_p(d) \equiv -1 \pmod p$ *according as* $p \equiv 3$ *or* $q \equiv 3 \pmod 4$.

Proof. We have $h(-p) < p/4 < q$ and $h(-q) < q/4 < p$.

If now $p \equiv 3$ or $q \equiv 3 \pmod 4$, then by Theorem 1 (observing that (1) also has the form $(-y)^q - (-x)^p = 1$) (10) is valid.

From Lemma 2 we see that the congruences in (10) have as consequences respectively the conditions

$$(11) \qquad Q_q(d) \equiv 1 \pmod q, \qquad Q_p(d) \equiv -1 \pmod p.$$

Observing that in (ii), $p \equiv q \equiv 3 \pmod 4$, and in (iii) either $p \equiv 3$ or $q \equiv 3 \pmod 4$, the assertions follow. □

Johnson in his two papers [9, 10] presented some results concerning Fermat's quotient and hence also the congruences of the form $q^p \equiv q \pmod{p^2}$. Combining these results and Theorem 1, new results may be obtained, in addition to the ones deduced above. As an illustration we offer only the following Theorem 4, which is closely related to Meissner's following well-known result, proved also by Johnson in both of his papers mentioned above: If $0 < a < p$ and the order of $a \pmod p$ is $2, 3, 4$, or 6, then $Q_p(a) \not\equiv 0 \pmod p$.

Johnson defined the semiorder of an integer $a \pmod p$ (p an odd prime) to be the smallest positive integer d (denoted $\operatorname{sord}_p a$) such that $a^d \equiv \pm 1 \pmod p$. The following simple lemma holds.

Lemma 3. *If for an integer* a

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

then also $a^d \equiv \pm 1 \pmod{p^2}$, *where* $d = \operatorname{sord}_p a$.

Proof. We have $a^d = \pm 1 + mp$ ($m \in \mathbb{Z}$) and $d \mid p-1$, i.e., $p-1 = kd$ ($k \in \mathbb{Z}$). From this it follows that

$$1 \equiv a^{p-1} \equiv (\pm 1)^k + k(\pm 1)^{k-1} mp \pmod{p^2},$$

and so $p|m$, since p is odd. □

If $d = \operatorname{sord}_p a$ and thus $a^d \equiv \pm 1 \pmod p$, then a belongs to the exponent $d \pmod p$ in the case of + sign and to $2d$ otherwise.

Theorem 4. *If* p *and* q *are primes* ≥ 5 *and either* $p \equiv 3 \pmod 4$ *or* $q \nmid h_p$, *then* (1) *has only trivial solutions in both of the cases* (i) $q|p^2+1$, $p < 1.4q$, *and* (ii) $q|p^6-1$, $p \leq 1.65q$.

Proof. Since $q > p/4 > h(-p)$ in both of the cases (i) and (ii), we have $q \nmid h(-p)$ for $p \equiv 3 \pmod 4$. Suppose now that the congruence $p^q \equiv p \pmod{q^2}$ holds.

In (i) the semiorder of $p \pmod q$ is 2. Since now $p^{q-1} \equiv 1 \pmod{q^2}$, it follows from Lemma 3 that $q^2 \mid p^2+1$. This is, however, impossible, because it is easy to see that $p^2+1 \neq q^2$ and $p^2+1 < 1.96q^2 + 0.04q^2 \leq 2q^2$, by the assumptions $p < 1.4q$ and $q \geq 5$.

If in (ii) $q \mid p^2-1$, then $q \mid p \pm 1$. But this is impossible, since $q \neq p \pm 1 < 1.65q + 0.2q < 2q$. Thus $q \mid p^2+p+1$ or $q \mid p^2-p+1$ and $\operatorname{sord}_q p = 3$ in both cases. Now by Lemma 3, $q^2 \mid p^3 \mp 1$ (respectively) and further $q^2 \mid p^2 \pm p + 1$, since $q \nmid p \mp 1$. Every prime factor $\neq 3$ of $p^2 \pm p + 1$ is of the form $6n+1$. But these expressions are $< 3q^2$, by $p \leq 1.65q$ and $q \geq 7$. Therefore $p^2 \pm p + 1 = q^2$, because the left-hand side is odd for both signs. Now $(2q)^2 - (2p \pm 1)^2 = 3$, from which it easily follows that $q = 1$, a contradiction.

We infer that $p^q \equiv p \pmod{q^2}$ is impossible in every case, and so our theorem follows from Theorem 1. □

It seems probable that there exist infinitely many pairs (p, q) for which the assumptions of Theorems 2 and 4 are valid, but this is not yet known. However, using Theorem 1, also the following theorem can be proved.

Theorem 5. *There exists an infinite sequence of prime pairs* (p, q) *with* $\min\{p, q\} \to \infty$ *such that Catalan's equation* (1) *has only the trivial solutions.*

Naturally, this is included as a special case in Tijdeman's result mentioned above, but we do not know any other ways for verifying a result of this kind. It is not difficult to construct a proof for Theorem 5 from Theorem 1, on the basis of the following auxiliary facts:

(i) the estimate (4) of the class number $h(-p)$;

(ii) the number of the incongruent roots of the congruence $x^{q-1} \equiv 1 \pmod{q^2}$ is $q-1$;

(iii) the number of primes $p \leq x$ in the arithmetic progression $4m+3$ is asymptotically equal to $\frac{1}{2}x/\log x$ for $x \to \infty$.

3. Numerical results

Solutions of the congruence $p^q \equiv p \pmod{q^2}$ have been computed by many scientists. Riesel [20] has tabulated all solutions for natural p and odd primes q within the ranges $2 \leq p \leq 10$, $q < 500000$ and $11 \leq p \leq 150$, $q < 10^4$. For $p < 100$ the upper bounds on q have been enlarged by Brillhart, Tonascia, and Weinberger [2], and Keller (see [19, p. 276]). We wrote a computer program to find all odd prime solutions $p, q < 10^4$. Our Table 1 contains the solutions found for $p < 1000$. The full table up to 10^4 can be requested from the first author.

Remark. Within the range $3 \leq p, q < 10^4$ the pair $p = 83, q = 4871$ is the only one satisfying both congruences

$$p^q \equiv p \pmod{q^2}, \qquad q^p \equiv q \pmod{p^2}. \tag{12}$$

A better-known example is $p = 2$, $q = 1093$, related to Fermat's Last Theorem. A third one, namely $p = 3$, $q = 1006003$, can be found in the table of Brillhart, Tonascia, and Weinberger [2] (see also [19, p. 276]). We know of no more examples.

Consider the primes p, q with $73 \leq p, q < 10^4$ and $p \equiv q \equiv 3 \pmod 4$. Among these, there are only eight pairs (p, q) with the property $p \mid h(-q)$ (see [16]): $p = 79$, $q = 4391, 5399, 7127$; $p = 83$, $q = 3911, 5039, 8423$; $p = 107$, $q = 8231$; $p = 139$, $q = 9239$. Fortunately, for each one, $q \nmid h(-p)$, since $h(-p) < p < q$, and $p^q \not\equiv p \pmod{q^2}$. Hence, Theorem 1 ensures that (1) has no nontrivial solutions x, y for these eight pairs (p, q). Accordingly, again by Theorem 1, nontrivial solutions of (1) can exist only if p and q satisfy

TABLE 1

Solutions of $p^q \equiv p \pmod{q^2}$, p, q *primes,* $p < 1000$, $q < 10^4$

p	q	p	q	p	q
2	1093 3511	271	3	617	101 1087 6007
3	11	277	1993	619	7 73
7	5	293	5 7 19 83	631	3 1787 5741
11	71	307	3 5 19 487	641	43
13	863	313	7 41 149 181	643	5 17 307 859
17	3	317	107 349	647	3 23
19	3 7 13 43 137	331	211 359	653	13 17 19 1381
23	13	337	13	659	23 131 2221 9161
31	7 79 6451	349	5 197 433 7499	673	61
37	3	353	8123	677	13 211
41	29	359	3 23 307	683	3 1279
43	5 103	367	43 2213	691	37 509 1091 9157
53	3 47 59 97	373	7 113	701	3 5
59	2777	379	3	733	17
67	7 47	389	19 373	739	3 9719
71	3 47 331	397	3	743	5
73	3	401	5 83 347	751	5 151 409
79	7 263 3037	419	173 349 983 3257	757	3 5 17 71
83	4871	421	101 1483	761	41 907
89	3 13	431	3 2393	773	3
97	7	433	3	787	37 41
101	5	439	31 79	797	8273
107	3 5 97	443	5	809	3 59
109	3	449	3 5 1789	811	3 211
127	3 19 907	457	5 11 919	821	19 83 233 293 1229
131	17	461	1697 5081	823	13 2309
137	29 59 6733	463	1667	827	3 17 29 9323
149	5	467	3 29 743 7393	829	3 17
151	5 2251	479	47 2833	839	5227
157	5	487	3 11 23 41 1069	857	5 41 157 1697
163	3	491	7 79	859	71
173	3079	499	5 109	863	3 7 23 467
179	3 17	503	3 17 229 659 6761	881	3 7 23
181	3 101	509	7 41	883	3 7
191	13	521	3 7 31 53	887	11 607
193	5 4877	523	3 9907	907	5 17
197	3 7 653	541	3	911	127
199	3 5	547	31	919	3
223	71 349	557	3 5 7 23	937	3 41 113 853
227	7	569	7 263	941	11 1499
229	31	571	23 29	947	5021
233	3 11 157	577	3 13 17 71	953	3
239	11 13	587	7 13 31	967	11 19 4813
241	11 523 1163	593	3 5	971	3 11 401 9257
251	3 5 11 17 421	599	5	977	11 17 109 239 401
257	5 359	601	5 61	991	3 13 431
263	7 23 251	607	5 7	997	197 1223
269	3 11 83 8779	613	3 4073		

both congruences of (12), which is the case only when $p = 83$, $q = 4871$ (or $q = 83$, $p = 4871$).

The case $p \equiv 3$, $q \equiv 1 \pmod 4$, $73 \le p, q < 10^4$, can be handled in a similar way, but the number of exceptional pairs is much larger: 17 pairs with $q \mid h(-p)$ and some 160 solutions of $p^q \equiv p \pmod{q^2}$. We shall be content with the smaller range $p, q < 500$ and present the following theorem.

Theorem 6. *Equation* (1) *has no solutions in nonzero integers* x, y *for the following prime exponents* p, q:

(a) $p \equiv q \equiv 3 \pmod 4$, $5 \le p, q < 10^4$, $(p, q) \ne (83, 4871), (4871, 83)$;
(b) $p \equiv 3, q \equiv 1 \pmod 4$, $5 \le p, q < 500$, $(p, q) \ne (19, 137), (107, 97), (223, 349), (251, 421), (419, 173), (419, 349), (499, 109)$.

4. Improved lower bounds

According to Hyyrö [6], a solution $x, y > 1$ of (1) satisfies the relations

$$\begin{aligned}
&(13) && x - 1 = p^{q-1}a^q, && y + 1 = q^{p-1}b^p,\\
&(14) && (x^p - 1)/(x - 1) = pu^q, && (y^q + 1)/(y + 1) = qv^p,\\
&(15) && y = pau, && x = qbv,\\
&(16) && a = qa_0 - 1, \quad a_0 \ge 1, && b = pb_0 + 1, \quad b_0 \ge 1,\\
&(17) && a \equiv (q^{p-1} - 1)/p \pmod p, && b \equiv -(p^{q-1} - 1)/q \pmod q,\\
&(18) && u = p^{q-1}a_1^q u_1 + 1, \; a_1 \ge q - 1, && u_1 \ge 1, 2 \mid a_1 u_1, \quad q \mid a_1 + 1,\\
&(19) && v = q^{p-1}b_1^p v_1 + 1, b_1 \ge 1, && v_1 \ge 1, \quad 2 \mid b_1 v_1, \quad p \mid b_1 - 1,
\end{aligned}$$

where a, b, u, v are nonzero integers and a_1 (b_1) is the greatest factor of a (b) which has no prime factor of the form $kq + 1$ $(kp + 1)$. In addition, either $2 \mid a_0, 2 \mid b_1$ or $2 \mid b_0, 2 \mid a_1$.

From (14)–(16), (18), and (19) it follows that

$$\begin{aligned}
pu \equiv pu^q \equiv 1 \pmod q, &\qquad qv \equiv qv^p \equiv 1 \pmod p,\\
u_1 \equiv 1 - u \pmod q, &\qquad v_1 \equiv v - 1 \pmod p,
\end{aligned}$$

and hence we also have the congruences

$$(20)\qquad \begin{aligned}
u \equiv p^{q-2}, \quad u_1 \equiv 1 - p^{q-2} \pmod q,\\
v \equiv q^{p-2}, \quad v_1 \equiv q^{p-2} - 1 \pmod p.
\end{aligned}$$

For given p, q, these can be used to improve the lower bounds (2). For instance, (20) implies in general that $u_1 \ge 2$, whereas $u_1 \ge 1$ was used to obtain (2).

To make further improvements on (2), we first combine (15), (13), and (1) to obtain the equalities

$$\begin{aligned} x &= qbv = q^{1/p}y^{1/p}(1+1/y)^{1/p}v \\ &= q^{1/p}x^{1/q}(1-1/x^p)^{1/pq}(1+1/y)^{1/p}v, \\ y &= pau = p^{1/q}x^{1/q}(1-1/x)^{1/q}u \\ &= p^{1/q}y^{1/p}(1+1/y^q)^{1/pq}(1-1/x)^{1/q}u. \end{aligned}$$

Application of the estimates

$$(1+1/z)^{1/k} > 1 + 1/2kz, \qquad (1-1/z)^{1/k} > 1 - 1/k(z-1)$$

$(k, z > 1)$ then gives the inequalities

$$\begin{aligned} x &> q^{1/p}x^{1/q}[1 - 1/pq(x^p-1)][1+1/2py]v > q^{1/p}x^{1/q}v, \\ y &> p^{1/q}y^{1/p}[1+1/2pqy^q][1-1/q(x-1)]u. \end{aligned}$$

Therefore, we obtain the following

Theorem 7. *Let p and q be odd primes. If $x, y > 1$ is a solution of* (1), *then*

$$\begin{aligned} x &> \{q^{1/p}v\}^{q/(q-1)}, \\ y &> \{p^{1/q}[1-1/q(x-1)]u\}^{p/(p-1)}. \end{aligned}$$

The dominant terms within the braces are v and u, which can be bounded from below by the use of (18)–(20). The improvement, compared to (2), is therefore in the exponents, which are slightly larger than 1. For example, for the exceptional pair $p = 137$, $q = 19$, (2) gives $\log x > 177.9$ (base 10 logarithm); by using the properties (16), (17), and (19) for b, b_1, v, this can be improved to $\log x > 179$ (see [8]). On the other hand, by (20), $v_1 \equiv 100 \pmod{137}$, whence $v > 100 \cdot 19^{136}$ by (19), and Theorem 7 yields

$$\log x > 19[(\log 19)/137 + \log 100 + 136 \log 19]/18 > 185.6.$$

A different approach is provided by continued fractions. Let

$$\alpha = q^{1-1/p}p^{-1+1/q} \quad \text{and} \quad r = \min\{p, q\}.$$

Let further $[C_0, C_1, C_2, \ldots]$ be the regular continued fraction of α and A_i/B_i $(i = 0, 1, 2, \ldots)$ its convergents. Hyyrö [6] proved that a/b is actually one of these convergents and thereby obtained the following theorem from (13), (16), and (17).

Theorem 8. *Let p and q be odd primes. Then the solutions of*

$$|x^p - y^q| = 1, \qquad x, y > 0,$$

are exactly those x, y *which satisfy, for a positive integer* i, *the conditions*

$$x = p^{q-1}A_i^q + (-1)^i, \qquad y = q^{p-1}B_i^p - (-1)^i, \tag{21}$$

$$A_i > 1, \qquad B_i > 1, \tag{22}$$

$$A_i \equiv (-1)^{i+1} \pmod{q}, \qquad A_i \equiv (-1)^i(q^{p-1} - 1)/p \pmod{p}, \tag{23}$$

$$B_i \equiv (-1)^i \pmod{p}, \qquad B_i \equiv (-1)^{i+1}(p^{q-1} - 1)/q \pmod{q}, \tag{24}$$

$$C_{i+1} \geq (-1)^{i+1}A_i^{r-2}, \qquad C_{i+1} \geq (-1)^i B_i^{r-2}, \tag{25}$$

$$x^p - y^q = (-1)^i. \tag{26}$$

We used the preceding results to compute the lower bound

$$x, y \geq 10^{500} \tag{27}$$

on any possible solution $x, y > 1$ of (1) for prime exponents $p, q \geq 5$. The bounds (2) are increasing both in p and q and yield the bound (27) when $\max\{p, q\} > 710$ or $p, q \geq 73, \max\{p, q\} > 266$. If $\max\{p, q\} < 710$ and $p < 73$ (or $q < 73$), the only possibilities, according to (i) in §1, are $(p, q) = (19, 137), (53, 97)$. Also, by Theorem 6, when $p, q < 266$, there are no nonzero solutions if $p \equiv q \equiv 3 \pmod{4}$ or $p \equiv 3, q \equiv 1 \pmod{4}$, $(p, q) \neq (19, 137), (107, 97)$. Thus, there are 159 pairs (p, q) left for further investigation. For each one of these we checked whether (2) implies (27) and, if not, we computed the continued fraction of $\alpha = q^{1-1/p}p^{-1+1/q}$ accurately enough so that (21) implied (27); at each step we checked (22)–(25) for a possible solution x, y. The computations revealed no potential solution, and we conclude that (27) holds.

5. Program developments

The verification of the congruence $p^q \equiv p \pmod{q^2}$ is easily done by repeated squarings and multiplications (see [11, p. 441]). All prime solutions p, q, $3 \leq p, q < 10^4$, were found in approximately four minutes.

To compute the continued fraction of $\alpha = q^{1-1/p}p^{-1+1/q}$, we choose integers c_i, d_i $(i = 1, 2)$ so that

$$\begin{aligned} p^{1/q} &= (c_1/d_1)(1 + z_1)^{1/q}, \qquad & z_1 &= (pd_1^q - c_1^q)/c_1^q, \quad |z_1| < 1, \\ q^{1/p} &= (c_2/d_2)(1 + z_2)^{1/p}, \qquad & z_2 &= (qd_2^p - c_2^p)/c_2^p, \quad |z_2| < 1. \end{aligned} \tag{28}$$

Using the binomial series

$$(1 + z)^{1/k} = \sum_{n=0}^{\infty} \binom{1/k}{n} z^n, \tag{29}$$

we then compute a rational lower bound β and a rational upper bound γ on $\alpha : \beta < \alpha < \gamma$. The continued fractions of β and γ are computed accurately by the Euclidean algorithm. As far as the partial denominators of β coincide with those of γ, they coincide with the partial denominators of any number between β and γ (cf. [23]). When the partial denominators of β and γ fail to coincide, we use (29) to compute sharper approximants β' and $\gamma' : \beta < \beta' < \alpha < \gamma' < \gamma$, and continue computations with β', γ'.

Unfortunately, the use of (28) and (29) leads to computations with very large integers. About 40 minutes was needed to compute the lower bound $x, y \geq 10^{500}$.

Bibliography

1. Z. I. Borevich and J. P. Shafarevich, *Number theory*, Academic Press, London and New York, 1966.
2. J. Brillhart, J. Tonascia, and P. Weinberger, *On the Fermat quotient*, Computers in Number Theory (A. B. L. Aitkin and B. J. Birch, eds.), Academic Press, London and New York, 1971, pp. 213–322.
3. Chao Ko, *On the Diophantine equation* $x^2 = y^n + 1$, Sci. Sinica (Notes) **14** (1964), 457–460.
4. L. Euler, *Theorematum quorundam arithmeticorum demonstrationes*, Opera Omnia, Ser. I, Vol. II, Comm. Arithm., I, Teubner, Leipzig, 1915, pp. 38–58.
5. M. Gut, *Abschätzungen für die Klassenzahlen der quadratischen Körper*, Acta Arith. **8** (1963), 113–122.
6. S. Hyyrö, *Über das Catalansche Problem*, Ann. Univ. Turku Ser. A I **79** (1964).
7. K. Inkeri, *On Catalan's problem*, Acta Arith. **9** (1964), 285–290.
8. ____, *On Catalan's conjecture*, J. Number Theory **34** (1990), 142–152.
9. W. Johnson, *On the nonvanishing of Fermat's quotient* $(\operatorname{mod} p)$, J. Reine Angew. Math. **292** (1977), 196–200.
10. ____, *On the p-divisibility of the Fermat quotients*, Math. Comp. **32** (1978), 297–301.
11. D. E. Knuth, *The art of computer programming*, Vol. 1, Addison-Wesley, 1981.
12. M. Langevin, *Quelques applications de nouveaux résultats de van der Porten*, Sém. Delange-Pisot-Poitou, 17^e année, No. G 12, 1975/76.
13. V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'equation* $x^m = y^2 + 1$, Nouvelle Ann. de Math. **9** (1850), 178–181.
14. T. Nagell, *Des équations indéterminées* $x^2 + x + 1 = y^n$ *et* $x^2 + x + 1 = 3y^n$, Norsk Mat. Forenings Skrifter Ser. I **2** (1921).
15. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, PWN, Warszawa, 1974.
16. B. Oriat, *Groupe des classes d'idéaux des corps quadratiques imaginaires* $\mathbb{Q}(d^{1/2})$, $-24572 < d < 0$, Théorie des Nombres, Années 1986/87–1987/88, Fasc. 2, Publ. Math. Fac. Sci. Besançon, Univ. France-Comté, Besançon, 1988.
17. O. Perron, *Kettenbrüche*, Chelsea, New York, 1950.
18. P. Ribenboim, *Consecutive powers*, Exposition. Math. **2** (1984), 193–221.
19. ____, *The book of prime number records*, Springer-Verlag, New York, 1988.
20. H. Riesel, *Note on the congruence* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **18** (1964), 149–150.
21. T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Univ. Press, Cambridge, 1986.
22. R. Tijdeman, *On the equation of Catalan*, Acta Arith. **29** (1976), 197–209.
23. B. M. M. de Weger, *Solving exponential Diophantine equations using lattice basis reduction algorithms*, J: Number Theory **26** (1987), 325–367.

Department of Mathematics, University of Turku, SF-20500 Turku, Finland
E-mail address: mataalt@bontu.utu.fi