

On $p^x - q^y = c$ and related three term exponential Diophantine equations with prime bases

short running title: Prime Base Exponential Diophantine Equations

revised 27 June 2009

Reese Scott, P. O. Box 236, Barre MA 01005, phone 978-355-3451

Robert Styer (correspondence author), Dept. of Mathematical Sciences, Villanova University, 800 Lancaster Avenue, Villanova, PA 19085, phone 610-519-4851, fax 610-519-6928, robert.styer@villanova.edu

Abstract Using a theorem on linear forms in logarithms, we show that the equation $p^x - 2^y = p^u - 2^v$ has no solutions (p, x, y, u, v) with $x \neq u$, where p is a positive prime and x, y, u , and v are positive integers, except for four specific cases, or unless p is a Wieferich prime greater than 10^{15} . More generally, we obtain a similar result for $p^x - q^y = p^u - q^v > 0$ where q is a positive prime, $q \not\equiv 1 \pmod{12}$. We solve a question of Edgar showing there is at most one solution (x, y) to $p^x - q^y = 2^h$ for positive primes p and q and positive integer h . Finally, we use elementary methods to show that, with a few explicitly listed exceptions, there are at most two solutions (x, y) to $|p^x \pm q^y| = c$ and at most two solutions (x, y, z) to $p^x \pm q^y \pm 2^z = 0$, for given positive primes p and q and integer c .

Key words: exponential Diophantine equation, Wieferich primes

§1: Introduction.

The exponential Diophantine equation

$$a^x - b^y = d \tag{i}$$

where a, b, x and y are positive integers and d is an integer, has been treated by many authors. Brief histories are given in Alex [A2], Shorey-Tijdeman [Sh-T, pp. 50-55], and [Sc]. Not included in these histories are recent results of Bennett [Be], Cao [Cao], and Terai [Te]. The main results of this paper (Theorems 2 and 6) deal with equation (i), taking a and b to be prime. Earlier results with a and b prime include the work of Stroeker and Tijdeman [St-T], De Ze Mo and Tijdeman [M-T], and deWeger [W].

The case $a = 3$ and $b = 2$ has received much special attention. Littlewood [Li] discussed the size of d . Pillai [Pi1] and Herschfeld [He] obtained results on the number of solutions for a given d . Brenner and Foster [B-F] observed that this equation does not yield to conventional congruence methods (see [G, section D-10]). Using linear forms in logarithms, Stroeker and Tijdeman [St-T] finally proved Pillai's conjecture [Pi2] that the equation $3^x - 2^y = d$ has at most one solution (x, y) except when

$$d = 1, -5, \text{ or } -13. \tag{ii}$$

This result also follows from elementary methods using the Corollary to Theorem 4 in [Sc].

The only other known instance of two solutions to the equation

$$p^x - 2^y = d \tag{iii}$$

(where p is a positive prime and d an integer) is given by

$$p = 5, d = -3. \tag{iv}$$

In [Sc] the first author used elementary methods to show that if (iii) has two solutions (x, y) and is not one of the examples in (ii) or (iv), we must have $p \equiv \pm 1 \pmod{8}$. Here we use linear forms in logarithms to improve this, showing that p must be a Wieferich prime greater than 10^{15} (see Corollary to Theorem 2). More generally, we obtain a similar result with $p^x - q^y = c$ where c is a positive integer and q is a prime, $q \not\equiv 1 \pmod{12}$ (see Theorem 2).

Taking a and $b > 1$ and $d > 0$, the question of how small d can be in comparison to b is considered by Terai [Te] and Bennett [Be]. Theorem 3 of [Te] uses a result on linear forms in logarithms (which, as pointed out by the anonymous referee of this paper, does not correspond to the cited reference [Mi1]) to show that (i) has at most one solution when $b > 1697d$, provided that $(a, b) = 1$ and $a - b = d$. The restriction $a - b = d$ can be removed using the Main Theorem of [Te]. And Bennett [Be] removes the restriction $(a, b) = 1$: although not explicitly stated by Bennett, the result that (i) has at most one solution when $b > 2410d$ is easily derived from (3.2), (3.3), and (7.1) of [Be] (see also his more general Theorem 1.4). Theorem 5 of this paper uses elementary means to show that if a and b are distinct primes with $b \not\equiv 1 \pmod{12}$, one can replace 2410 by 0.0625. (We could remove the restriction $b \not\equiv 1 \pmod{12}$ if we replace $16b > d$ by $b > d^{3/2}$, but this would require additional elementary lemmas.)

Several authors have considered the problem of Hugh Edgar posed in Section D-9 of [G]: how many solutions (x, y) are there to the equation

$$p^x - q^y = 2^h$$

for positive primes p and q and integer h ? It is shown in [C-W] and [Sc] that there are at most two solutions. Here we improve this to at most one solution, except for the special case $h = 0, p = 3, q = 2$ (see Theorem 6).

We also consider the more general equation

$$p^x \pm q^y \pm 2^z = 0.$$

In Theorem 8 of this paper, we use elementary methods to prove there are at most two solutions (x, y, z) to this set of (three nontrivial) equations, with four specified exceptions. Nagell [N2] found all solutions for the case of primes $p, q \leq 7$. Hadano [Ha] and Uchiyama [U] improved this to $p, q \leq 17$. Theorem 2 of [Sc] allows all solutions to be found for any given pair of primes p, q . We apply this result to systematically determine all solutions for pairs of primes $p, q < 1000$.

In [Sc], it was shown that the set of two equations

$$|p^x - q^y| = c$$

where p and q are distinct primes and c is any integer, has at most two solutions in positive integers x and y , except for three specific cases (there are probably only finitely many with two solutions). In Theorem 7 of this paper, we use elementary methods to improve this. We show that the set of three equations

$$|p^x \pm q^y| = c$$

has at most two solutions, except for six specific cases (there are probably an infinite number of cases with two solutions).

§2: $p^x - q^y = c$ from the standpoint of restrictions on p and q .

In this section we treat the equation

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

where p and q are distinct positive integer primes and c is a positive integer. We consider solutions in positive integers (x, y) . Theorem 2 will show that for most values of q we can severely restrict the values of p for which two solutions are possible (a base- q Wieferich prime restriction). We close this section with a brief discussion of how one can obtain a double Wieferich pair restriction on p and q .

Note that there exist at most two solutions to (1) by Theorem 3 of [Sc].

We need this preliminary result:

Theorem 1 If $q \equiv 3 \pmod{4}$ then (1) has at most one solution except when (p, q, c) equals $(2, 3, 5)$, $(2, 3, 13)$, or $(13, 3, 10)$.

Proof: Assume (p, q, c) is not one of the three listed cases. Suppose (1) has two solutions, (x_1, y_1) and (x_2, y_2) . Then by Theorem 3 of [Sc], $2 \nmid y_2 - y_1$. Consideration modulo 4 shows that $p \equiv 3 \pmod{4}$ which contradicts the Corollary to Theorem 4 of [Sc].

We now define the order of q modulo a prime p . Let $\text{ord}_p q$ be the lowest positive integer such that $p \mid q^{\text{ord}_p q} - 1$.

Theorem 2 If $q \not\equiv 1 \pmod{12}$ then (1) has at most one solution unless either

$$(A) \quad (p, q, c) = (3, 2, 1), (2, 3, 5), (2, 3, 13), (2, 5, 3), (13, 3, 10),$$

or

$$(B) \quad p^2 \mid q^{\text{ord}_p q} - 1, \text{ord}_p q \text{ is odd, and } \text{ord}_p q > 1.$$

Proof: Assume that (1) is not one of the cases enumerated in Condition (A) of this Theorem. Assume there are two solutions (x_1, y_1) and (x_2, y_2) with $x_1 < x_2$. We can assume $p > 2$ by Theorem 4 of [Sc].

Let $v = \text{ord}_p q$ and let u be the highest number such that $p^u \mid q^v - 1$. Let $w = x_1 - u$. We have

$$p^{x_1}(p^{x_2-x_1} - 1) = q^{y_1}(q^{y_2-y_1} - 1) \tag{2}$$

Now we must have $p^{x_1} \mid q^{y_2-y_1} - 1$ so that $vp^w \mid y_2 - y_1$. Since $v \log q > u \log p$ we have

$$x_2 \log p > y_2 \log q > (y_2 - y_1) \log q \geq vp^w \log q > up^w \log p$$

hence

$$x_2 > up^w \tag{3}$$

Under certain conditions, we can improve this inequality (3). Suppose $v > 1$. Let s be the least prime dividing v . Suppose $s \neq q$. Let $t = \text{ord}_s q$. Note that s is odd since $y_2 - y_1$ is odd by Theorem 3 of [Sc]. Now $s|v|p-1$ and $p-1$ divides both sides of (2). So $t|y_2 - y_1$. Also, since $(t, vp) = 1$ we conclude that $tp^w|y_2 - y_1$. Note that t is odd. Thus, if $v > 1$, $s \neq q$, and $t > 1$, we can replace (3) by

$$x_2 > 3up^w. \tag{3a}$$

In particular, if $q = 2$ then (3a) holds.

Applying our assumption that $q \not\equiv 1 \pmod{12}$ along with Theorem 1, either $q = 2$ or $q \equiv 5 \pmod{12}$. In either case, $q \equiv 2 \pmod{3}$. Recalling Theorem 3 of [Sc] and considering equation (1) modulo 3, we get $p > 3$ and

$$2 \nmid y_2 - y_1, 2 \nmid x_2 - x_1, 2|x_1 - y_1, 2|x_2 - y_2. \tag{4}$$

Suppose that $2|x_2$. Then we have

$$p^{w+u} = p^{x_1} > c = p^{x_2} - q^{y_2} \geq p^{x_2/2} + q^{y_2/2} > p^{x_2/2} > p^{up^w/2}.$$

We thus obtain

$$2u + 2w > up^w. \tag{5}$$

If $w > 0$ then (5) is impossible since $p > 3$. Thus, when $q \not\equiv 1 \pmod{12}$, we have

$$2|x_1, 2|y_1 \text{ for all } w > 0. \tag{6}$$

If (3a) holds, in particular when $q = 2$, we can improve both (5) and (6). Again assuming $2|x_2$, we can replace (5) by

$$2u + 2w > 3up^w \tag{5a}$$

which is impossible for all values of w and so, when $q = 2$,

$$2|x_1, 2|y_1 \text{ for all } w \geq 0. \tag{6a}$$

We have p odd, so that if q is odd, (4) gives

$$p \equiv q \pmod{24}. \tag{7}$$

Now $q \geq 2$ and by Corollary 1.7 of [Be], $p \geq 7$. This allows us to apply formula (7.1) of [Be] (letting $a = p$ and $b = q$) which is an inequality that holds whenever $x_2/\log q \geq 2409.08$. (This inequality is derived in Section 6 of [Be] using a result on linear forms in logarithms of Mignotte [Mi1]. Although this bound could be improved by sharpening the bounds on p and q , or by substituting different values for the variables in Mignotte's original formula, the improvements are not needed here.) Noting that $p^{x_1} > c$, we see that the first term on the right side of (7.1) is less than $\log(7/6)/(\log 2 \log 7) + x_1/\log q < 0.12 + x_1/\log q$. Combining this with (7.1), we see that at least one of the following inequalities must hold:

$$x_2/\log q < 2409.08 \tag{8}$$

or

$$x_2/\log q < x_1/\log q + 0.12 + 22.997(\log(x_2/\log q) + 2.405)^2. \tag{9}$$

We now consider the case $q = 2$. By (3a), we can take $x_2 = 3kup^w$ where k is a real number greater than 1. And $x_1 = w + u$. Now we consider inequality (9) as an inequality in the variables k , u , and w for given p and q . Taking $q = 2$, if we assume that $w > 0$, we see that if the inequality holds for any k , u , and w , it holds for $k = u = w = 1$. Substituting $k = u = w = 1$ into (9), we have

$$3p/\log 2 < 2/\log 2 + 0.12 + 22.997(\log(3p/\log 2) + 2.405)^2.$$

We see that when $w > 0$, both (8) and (9) imply that $3p/\log 2 < 2409.08$, so $p < 557$. Now recalling (2) and the fact that $2 \nmid y_2 - y_1$, we see that p cannot be a Fermat prime and neither p nor any of the divisors of $p - 1$ can be congruent to 3 or 5 modulo 8. Also, since $2 \nmid x_2 - x_1$, we see that 2^{y_1} is the highest power of 2 dividing $p - 1$; and since y_1 is even, we must have $p \equiv 1 \pmod{16}$. Combining all of these restrictions eliminates from consideration all possible values of $p < 557$ except $p = 113$ and $p = 449$. For these two values of p , the greatest odd number dividing $p - 1$ is 7, so that neither of these primes has the property that $\text{ord}_p 2$ is odd, since neither prime divides $2^7 - 1$.

So far we have shown that if $q = 2$ then $w = 0$. If $u = 1$, we have a contradiction since (6a) shows $x_1 = u$ must be even. Therefore, $u > 1$ when $q = 2$.

Now we turn to the case q odd. Here we consider only the case $u = 1$ and use Proposition 4.4 of [Be] to get $w \leq 5$. (We could improve this bound on w as Bennett himself suggests, but it is not necessary for our purposes.) We replace the term $x_1/\log q$ on the right side of (9) by the constant term $6/\log 5$ since $q \geq 5$ and u and w are bounded. Then (9) implies (8). Assuming $w > 0$ and $u = 1$, (6) implies $q < p^{(w+1)/2}$. Combining this with (3) and (8), we have

$$\frac{p^w}{\frac{w+1}{2} \log p} < 2409.08.$$

From this, one can show that $q, p < 24331$ when $w > 0$. We now can use a simple computer program to show that it is not possible to find two solutions to (1) for primes p and q in this range [St2]. We use the fact that $x_2 - x_1$ and $y_2 - y_1$ are both odd when $q \not\equiv 1 \pmod{12}$ along with the restriction (7), and apply the straightforward "bootstrapping" methods of [GLS] and [St1] to (2) to reach a contradiction for each pair of primes. In this way we show $w = 0$ when $u = 1$, which is a contradiction since (4) shows that $x_1 = 1$ implies $p - q^{y_1} = c = p^{x_2} - q^{y_2} \geq p^{x_2/2} + q^{y_2/2} > p$.

Thus, we have shown that $u > 1$ for both the case $q = 2$ and q odd. This fulfills the first condition stated in (B) of Theorem 2. The second condition, that the $\text{ord}_p q$ be odd, is given by Theorem 4 of [Sc], while the third condition, that $\text{ord}_p q > 1$, is given by Theorem 1.6 of [Be]. (The specific case $(a, b, c) = (2, 5, 3)$ is missing in Theorem 1.6 of [Be], but it is clear from the context what is intended.) This concludes the proof of Theorem 2.

Corollary to Theorem 2 Let p be any positive prime, and d be any integer positive or negative. Then the equation

$$p^x - 2^y = d \tag{10}$$

has at most one solution in positive integers (x, y) unless one of the following two conditions holds: either

$$(A) \quad (p, d) = (3, 1), (3, -5), (3, -13), (5, -3)$$

or

$$(B) \quad p^4 | 2^{\text{ord}_p 2} - 1 \text{ whenever } p \not\equiv 65 \pmod{192}, \text{ and, in all cases, } p^2 | 2^{\text{ord}_p 2} - 1$$

with $\text{ord}_p 2$ odd, $p > 10^{15}$, and $2|x_1 = u$, where x_1 is the value of x in the lower of the two solutions of (10), and u is the greatest number such that $p^u | 2^{\text{ord}_p 2} - 1$.

Proof: We assume the listed cases of (A) are excluded. Assume (10) has two solutions (so that $p > 2$). Then Theorem 4 of [Sc] shows that $d > 0$, so that Theorem 2 of this paper applies to show that $p^2 | 2^{\text{ord}_p 2} - 1$ and $\text{ord}_p 2$ is odd. [Mc] states that the only two Wieferich primes less than 10^{15} are 1093 and 3511 (see [C-P] for a published bound). Both of these are congruent to 1 modulo 3 which is impossible when two solutions exist by Theorem 3 of [Sc]. The requirement that $2 | x_1 = u$ follows from (6a) and the fact that in handling the case of $q = 2$ in Theorem 2 we showed that $w = 0$ for all values of u , not just $u = 1$.

It remains to show that $x_1 = 2$ implies $p \equiv 65 \pmod{192}$. Since the existence of two solutions requires $p \equiv 2 \pmod{3}$, it suffices to show that $p \equiv 1 \pmod{64}$. We use the notation of Theorem 2 and recall (6a). Suppose $4 | y_1$ and $4 \nmid x_1$. Then there are two possibilities modulo 5: either $d \equiv 0 \pmod{5}$ and $p \equiv \pm 1 \pmod{5}$, or $d \equiv 3 \pmod{5}$ and $p \equiv \pm 2 \pmod{5}$. Both these possibilities require $2 | x_2 y_2$ which contradicts (4). Thus, $x_1 = 2$ implies $4 \nmid y_1$. Recalling (2) and (4), we see that $2^{y_1} | p - 1$ and $y_1 > 2$, so that $2^6 | p - 1$ when $x_1 = 2$. This concludes the proof of the corollary.

Remark: The corollary shows that $p = 3$ is the only value of p for which there exists more than one d giving two solutions to (10): when $p = 5$, the only such d is $d = -3$; if $p > 5$, then (2) and (4) show that y_1 is unique, and the corollary shows that x_1 is unique.

The proofs of Theorems 1 and 2 can be easily generalized to allow q to be composite. In Theorem 2, however, this would require more restrictions on q modulo 12, and a further computer search.

Reversing the roles of the primes p and q , one can also obtain $q^2 | p^{\text{ord}_q p} - 1$, so that p and q form a double Wieferich pair, when various restrictions are placed on p and q . There are several ways to do this; we sketch one example here.

Suppose that $2 < q \not\equiv 1 \pmod{12}$ and $p < 2q$, suppose that $p - 1$ and $q - 1$ have no odd factors in common, and finally suppose that (p, q, c) is not one of the specific cases listed in Theorem 2 (A). Then $p^x - q^y = c$ has at most one solution unless both $p^2 | q^{\text{ord}_p q} - 1$ and $q^2 | p^{\text{ord}_q p} - 1$. (We could improve the $p < 2q$ to $p < (3 - \epsilon)q$ for any $\epsilon > 0$ where the computational bounds would depend on ϵ .)

The proof of a claim like this parallels that of Theorem 2. Assume (1) has two solutions under the restrictions

above. Define $v_1, s_1, t_1, u_1,$ and w_1 in analogy to $v, s, t, u,$ and w except with p and q reversed. Note that we must have $2 < p \equiv q \equiv 5 \pmod{12}$. Now $q \not\equiv 1 \pmod{p}$ by Theorem 1.6 of [Be], and clearly $p \not\equiv 1 \pmod{q}$. Thus we have $v > 1, v_1 > 1, s \neq q,$ and $s_1 \neq p$. Our restriction on $p - 1$ and $q - 1$ gives $t > 1$ and $t_1 > 1$. Thus, we have (3a) and the analogous result $x_2 \log p > 3u_1 q^{w_1} \log q$. From (3a), we see that (6a) applies, so we can take $y_1 > 1$. And the analogous form of (3a) allows us to substitute $3k_1 u_1 q^{w_1} / \log p$ for the value $x_2 / \log q$ in (9). And the term $x_1 / \log q$ in (9) which corresponds to $\log c / \log a \log b$ in Equation (7.1) of [Be] can be replaced by $2q / \log p$, by noting that Theorem 1.3 of [Be] gives $c < q^p$.

Now we let $w_1 > 0$ and we see, using $p < 2q$, that our substituted form of (9) gives bounds $q < 34100$ and $p < 68200$. A computer search [St2] reveals no double solutions to (1) in this range. To handle the case of $w_1 = 0$, we see that since $y_1 > 1$ we have shown that $q^2 | p^{\text{ord}_q p} - 1$. Thus, we have both $q^2 | p^{\text{ord}_q p} - 1$ and $p^2 | q^{\text{ord}_p q} - 1$. Double Wieferich pairs appear in [Ste] and [Mi2]. Steiner [Ste] lists the four double Wieferich pairs with p, q less than 10^6 : (2, 1093), (83, 4871), (911, 318917) and (2903, 18787). Though there could be infinitely many, according to Steiner only two other pairs are known, (3, 1006003) and (5, 1645333507).

§3: $p^x - q^y = c$ from the standpoint of restrictions on c .

We now consider $p^x - q^y = c$ from the viewpoint of restrictions on c , specifically $c < q$ and then c a power of 2. We will need the following preliminary result.

Theorem 3 Let r be any odd positive integer, let A and B be coprime integers greater than 1, let PQ be the largest squarefree divisor of AB , with P and Q chosen so that $(AB/P)^{1/2}$ is an integer. Then if there exists a positive integer x such that

$$A + B = r^x \tag{11}$$

we must have

$$x < \frac{1}{2} Q P^{1/2} \log P \tag{12}$$

for $P \geq 3$ and

$$\begin{cases} x \leq Q/2 & \text{when } P = 1 \\ x \leq (Q + 1)/2 & \text{when } P = 2. \end{cases} \tag{13}$$

Proof: Assume (11) holds. Then by Theorem 2 of [Sc] we obtain

$$x \leq \frac{3^{u+v}}{2} h(-P) \frac{Q}{2^{n-1}} \prod_{i=g}^n \frac{q_i + 1}{q_i}. \quad (14)$$

Here $q_1 q_2 \dots q_n$ is the prime factorization of Q , $q_1 < q_2 < \dots < q_n$, $g = 1$ when Q is odd and $g = 2$ when Q is even, $h(-P)$ is the lowest h such that \mathfrak{a}^h is principal for every ideal \mathfrak{a} in $\mathbf{Q}(\sqrt{-P})$, $u = 1$ or 0 as $3 < P \equiv 3 \pmod{8}$ or not, we omit the factor 2^{n-1} when $Q = 1$, and finally $v = 1$ or 0 as (11) is or is not the special case

$$3^{2N+1} \left(\frac{3^{N-1} - 1}{8} \right) + \left(\frac{3^{N+1} - 1}{8} \right) = \left(\frac{3^N - 1}{2} \right)^3 \quad (15)$$

for N odd.

We observe that (14) gives

$$x \leq \frac{3^{u+v}}{2} h(-P) \frac{4}{3} Q. \quad (16)$$

When Q is not an odd prime we can improve this to

$$x \leq \frac{3^{u+v}}{2} h(-P) Q. \quad (17)$$

When $P = 1$ or 2 , we have $u = v = 0$. Thus, (14) implies (13) and so we can henceforth assume $P > 2$.

We first prove the theorem for $v = 0$, handling the case $v = 1$ at the end of the proof. So assume $v = 0$. Let H be the class number of $\mathbf{Q}(\sqrt{-P})$; of course, $H \geq h(-P)$. Let $\left(\frac{a}{b}\right)$ be the Kronecker symbol. Note that if D is the discriminant of $\mathbf{Q}(\sqrt{-P})$,

$$\sum_{i=1}^{|D|} \left(\frac{D}{i}\right) = 0.$$

We will also use the fact that when $k \geq 5$,

$$\left(\sum_{i=1}^k \frac{1}{i} \right) - \log k < \log 2.$$

Now consider the case $P \equiv 3 \pmod{4}$, taking $P \geq 11$. Applying the standard class number formula (for example, [Co, pp. 163, 171]), we get

$$H = \frac{\sqrt{P}}{\pi} \sum_{i=1}^{\infty} \left(\frac{-P}{i}\right) / i < \frac{\sqrt{P}}{\pi} \left(\log \left(\frac{P-1}{2} \right) + \log 2 \right)$$

from which we get

$$H < \frac{\sqrt{P}}{\pi} \log P. \quad (18)$$

Combining (18) with (17) proves Theorem 3 when $v = 0$, $P \equiv 3 \pmod{4}$, and $P \geq 11$.

$P = 3$ and $P = 7$ both give $H < \sqrt{P} \log P$. Combining this with (17) proves Theorem 3 in these two cases, provided $v = 0$. So Theorem 3 holds when $v = 0$ and $P \equiv 3 \pmod{4}$.

Now consider the case $P \not\equiv 3 \pmod{4}$. Recall that $P > 2$. The class number formula gives

$$H < \frac{2\sqrt{P}}{\pi} \left(\log(2P) + \log 2 - \frac{\log P}{2} - 0.577/2 \right) < \frac{2\sqrt{P}}{\pi} \left(\frac{\log P}{2} + 1.1 \right).$$

For $P \geq 10$, this gives

$$H < \frac{2}{\pi} \sqrt{P} \log P. \quad (19)$$

For $2 < P < 10$ the only possible values are $P = 5$ and $P = 6$, and (19) holds for these values also.

Combining (19) with (16), we see that Theorem 3 holds for all P provided $v = 0$.

Finally, we consider $v = 1$, that is, the special case (15). The case $N = 1$ is trivial. The case $N = 3$ gives $P = 30$ and $x = 3$, while the case $N = 5$ gives $P = 2730$ and $x = 6$. In both of these cases, it is easy to verify that the theorem holds. To prove the cases of Theorem 3 with $v = 1$ and $N \geq 7$, it suffices to show that $H \geq 3h(-P)$. To do this, we note that if (11) is the special case (15), $64AB$ must have three divisors of the form $3^k + 1$ where $k = (N - 1)/2$, $k = (N + 1)/2$ or $k = (N \pm 1)/4$. Now $3^k + 1$ cannot be a perfect square when $k > 1$ nor can it be twice a perfect square. So each of these three factors must have an odd prime divisor raised to an odd power. Since all three of these factors have no odd number greater than one that divides any two of them, we find that the three factors in question each contribute a distinct odd prime to P . Recalling that $3|P$ as well, we have P divisible by at least four odd primes. Thus, the discriminant of the field $\mathbf{Q}(\sqrt{-P})$ is divisible by at least four primes, and therefore $H \geq 2^{4-2}h(-P) = 4h(-P)$. This proves Theorem 3.

Theorem 4 Let p be a positive prime, and b and c positive integers relatively prime to p . Then if $b > c$,

$$p^x - b^y = c \quad (20)$$

has at most one solution in positive integers (x, y) with $y > 1$.

Proof: Assume (20) has two solutions (x_1, y_1) and (x_2, y_2) with $x_1 < x_2$ and $2 \leq y_1 < y_2$. Then we have

$$b^{y_2} + c = p^{x_2} = (b^{y_1} + c)^{x_2/x_1},$$

i.e.,

$$b^{y_2} \left(1 + \frac{c}{b^{y_2}}\right) = b^{y_1 x_2/x_1} \left(1 + \frac{c}{b^{y_1}}\right)^{x_2/x_1}.$$

From this we see that $y_2 > y_1 x_2/x_1$. Since all the variables involved are integers, we have $x_1 y_2 \geq y_1 x_2 + 1$.

So now we have

$$b^{(y_1 x_2 + 1)/x_1} \leq b^{y_2} < p^{x_2} = b^{y_1 x_2/x_1} \left(1 + \frac{c}{b^{y_1}}\right)^{x_2/x_1}.$$

From this we see that $b < \left(1 + \frac{c}{b^{y_1}}\right)^{x_2}$ so that

$$x_2 > \frac{\log b}{\log \left(1 + \frac{c}{b^{y_1}}\right)} > \frac{\log b}{c/b^{y_1}} = \frac{b^{y_1} \log b}{c} > b^{y_1 - 1} \log b. \quad (21)$$

The equation $p^x - b^y = 1$ yields no cases with two solutions satisfying $y > 1$; see [Lev] or [Cas]. Thus, we will assume $c > 1$. By Theorem 4 of [Sc] we can take p odd.

First we consider the case when y_2 is odd. Applying Theorem 3 of this paper (taking $P > 2$) to the equation $b^{y_2} + c = p^{x_2}$ and using our assumption $c < b$, we see that

$$x_2 < \frac{1}{2}(bc)^{1/2} \log(bc) < b \log(b),$$

contradicting (21).

Next we consider the case when y_2 is even. By Theorem 3 of [Sc], y_1 must be odd, hence $y_1 \geq 3$. Again we apply Theorem 3 of this paper (with $P > 2$) to the equation $b^{y_2} + c = p^{x_2}$ to get

$$x_2 < \frac{1}{2}bc^{1/2} \log c < \frac{1}{2}b^{3/2} \log b < b^2 \log b$$

which contradicts (21). Applying Theorem 3 of this paper with $P \leq 2$ is easily seen to lead to the same contradictions. This concludes the proof of the theorem.

If we restrict b to be a prime not congruent to 1 mod 12, we can significantly improve Theorem 4 using only elementary methods.

Theorem 5 Let p and q be distinct positive primes, $q \not\equiv 1 \pmod{12}$, and c a positive integer. If $c < 31p$ or $c < 16q$, then the equation

$$p^x - q^y = c \tag{22}$$

has at most one solution in positive integers (x, y) except when (p, q, c) is $(3, 2, 1)$, $(2, 3, 5)$, $(2, 3, 13)$, $(2, 5, 3)$, or $(13, 3, 10)$.

Proof: Assume (p, q, c) is not one of the listed exceptions, and assume (22) has two solutions (x_1, y_1) and (x_2, y_2) . From the Corollary of Theorem 2, along with (2) and (4), it follows that $q = 2$ implies $c = p^{x_1} - q^{y_1} > p^2 - (p - 1) > 10^{15}p$. Since also $p > 2$ by the Corollary of Theorem 4 of [Sc], we can assume $2 \nmid pq$. By Theorem 1, we can assume $q \equiv 1 \pmod{4}$, and, since $q \not\equiv 1 \pmod{12}$ we can assume $q \equiv 5 \pmod{12}$. So now, by the same method used in the proof of Theorem 2, we have (4). (Here we are not assuming $x_1 < x_2$.) From (4) we derive $p \equiv q \pmod{24}$ and $c = (p^{x_2/2} + q^{y_2/2})(p^{x_2/2} - q^{y_2/2})$ where without loss of generality we can assume $2 \mid y_2$ and $2 \nmid y_1$. Let $r = p^{x_2/2} - q^{y_2/2}$. Then we derive

$$r \equiv 4 \pmod{12} \text{ if } 2 \nmid x_2/2 \text{ and } 2 \mid y_2/2$$

$$r \equiv 8 \pmod{12} \text{ if } 2 \mid x_2/2 \text{ and } 2 \nmid y_2/2$$

$$r \equiv 0 \pmod{24} \text{ if } 2 \mid x_2/2 - y_2/2$$

If $r = 4$ then $q^{y_2/2} \equiv \pm 1$ or 0 modulo 5. If $q^{y_2/2} \equiv -1 \pmod{5}$ then $q \equiv \pm 2 \pmod{5}$ and $p^{x_2/2} \equiv c \equiv 3 \pmod{5}$, making the solution (x_1, y_1) impossible since $2 \nmid x_1 y_1$. If $q \equiv 0 \pmod{5}$, then $p \equiv -1 \pmod{5}$ and $c \equiv 1 \pmod{5}$, so that the solution (x_1, y_1) is again impossible. If $q \equiv 1 \pmod{5}$ then $p = 5$ and, since $q^{y_2/2} < p^{x_2/2}$, we must have $x_2 > 2$; therefore $c = 2rp^{x_2/2} - r^2 \geq 40p - 16 > 31p$. Also, when $r = 4$, $c = 2rq^{y_2/2} + r^2 \geq 40q + 16 > 16q$, so we can assume $r > 4$.

If $r = 8$, $x_2 > 2$, so that $c = 2rp^{x_2/2} - r^2 \geq 80p - 64 > 31p$. Also when $r = 8$, $c \geq 16q + 64 > 16q$. So we can assume $r > 8$.

If $r \geq 16$, $c = 2rq^{y_2/2} + r^2 > 16q$. And $c = p^{x_2} - (p^{x_2/2} - r)^2 \geq p^{x_2} - (p^{x_2/2} - 16)^2 \geq 32p - 256 > 31p$ if $p > 256$.

So either the theorem holds or $p < 256$ and $c \geq 32p^{x_2/2} - 256$. If $x_2 > 2$ then $c \geq 160p - 256 > 31p$; so we can assume $x_2 = 2$. If $24 \mid c$, then $c \geq 48p - 576 > 31p$ unless $p = 5, 17$, or 29 . Since $x_2 = 2$ we have

$q^{y_2/2} < p$ so that (p, q) must be $(29, 5)$ which is impossible by (2) and (4) since $2 \mid \text{ord}_5 29$. So $24 \nmid c$ and, since $x_2 = 2$, $4 \mid y_2$ so that $q^2 < p < 256$, giving $q = 5$. Then we must have $p \equiv 1 \pmod{5}$ since $2 \nmid \text{ord}_5 p$; this requires $p \equiv 101 \pmod{120}$ so that $p = 101$. But then (2) becomes impossible modulo 11. This completes the proof of Theorem 5.

It is easy to see that the proof of Theorem 5 also works to establish $c > 2q$ and $c > p$ when q is a composite positive integer with $q \equiv 2 \pmod{3}$.

The next theorem answers Hugh Edgar's question posed in [G, section D-9].

Theorem 6 Let p and q be distinct positive primes, and let h be an integer. Then $p^x - q^y = 2^h$ has at most one solution in positive integers (x, y) , except when $p = 3$, $q = 2$ and $h = 0$.

Proof: Suppose c is even, and that (1) has two solutions (x_1, y_1) and (x_2, y_2) with $x_1 < x_2$. Assume (p, q, c) is not one of the specific cases of Theorem 3 of [Sc], so y_1 and y_2 have opposite parities. We introduce an alternate notation for the two solutions that emphasizes parity rather than size: denote the solutions (x_a, y_a) and (x_b, y_b) with $2 \nmid y_a$ and $2 \mid y_b$. Write (1) in the form

$$p^x - 1 = q^y - 1 + c. \tag{23}$$

Let u_a be the highest number such that $2^{u_a} \mid p^{x_a} - 1$. Let v_a be the highest number such that $2^{v_a} \mid q^{y_a} - 1$. Let u_b be the highest number such that $2^{u_b} \mid p^{x_b} - 1$. Let v_b be the highest number such that $2^{v_b} \mid q^{y_b} - 1$. Let h be the highest number such that $2^h \mid c$. Note that $v_b > v_a$.

Now two of the numbers u_a, v_a , and h must be equal and the remaining number must be greater than the other two, similarly for u_b, v_b and h . Suppose $u_a \geq u_b$. If $v_b = h$ then $u_a \geq u_b > h = v_b > v_a$ which is impossible. And if $u_b = v_b$, then $h > u_b = v_b > v_a$ and $u_a \geq u_b = v_b > v_a$, which is impossible. Thus, we must have $u_b = h$ in which case either $u_a = h < v_a$ or $u_a > h = v_a$. In either case,

$$u_a \geq u_b \text{ implies } q > 2^h. \tag{24}$$

Now let $c = 2^h$. The case $h = 0$ has been handled by elementary means, see for example [Lev] or [Cas]. So assume $h > 0$. Note that none of the exceptional cases of Theorem 3 of [Sc] have $c = 2^h$. Cao and Wang

[C-W], using an earlier result of Cao [Cao] (see also Lemma 4 of Section 5 of this paper) have shown that if (1) has two solutions with $c = 2^h$, the lower solution has $x_1 = 1$ and $2|y_1$, so that $y_1 = y_b$. Now (24) shows that $q > 2^h = c$. Since y_1 is even, we have $y_1 > 1$ so Theorem 4 applies to complete the proof.

We can take q composite in Theorem 6 if, instead of using the result from [Cao] (or from Lemma 4 of this paper), we use a more general (but non-elementary) result in which q is not restricted to be prime. Such a result has been obtained independently by three different methods: the most direct approach is that of Luca [Lu], who uses results of Bilu, Hanrot, and Voutier [BHV]; a second proof was given by Le [Le], using linear forms in logarithms and several auxiliary lemmas; the result can also be obtained by considering the equation $x^n + 2^\alpha y^n = Cz^2$, handled by Bennett and Skinner [B-S, Theorem 1.2] using (in the words of those authors) "combinations of every technique we have currently available." See also earlier work of Ljunggren [Lj], Nagell [N1], Cohn [CoJ1], [CoJ2], and Arif and Muriefah [A-M].

Corollary to Theorem 6 Let a and b be positive integers greater than one, and let c be any positive integer. Then if there exists more than one solution in positive integers (x, y) to the equation

$$a^x - b^y = c,$$

we must have at least one of a, b, c divisible by at least two primes, except for the four specific cases listed in (A) of the Corollary of Theorem 2.

Proof: Assume there exists a choice of a, b, c all primes or prime powers (including the possibility $c = 1$) for which the equation has two solutions (x, y) . It is easy to see that we must have $(a, b) = 1$. Exclude from consideration the cases listed in (A). It follows from Theorem 6 above and from Theorem 4 of [Sc] that we can take $b = 2$. Using Theorem 3 of [Sc] and considering the equation modulo 3, we see that we can take $c = 3^k$ for some $k > 0$. Then, for one of the solutions (x, y) , $a^x - b^y$ is a difference of squares which we can factor to obtain $2^{y/2+1} = 3^k - 1$, from which we obtain $y = 4$, $k = 2$, and $a = 5$, which is impossible by Theorem 4 of [Sc].

§4. Solutions to $|p^x \pm q^y| = c$

Theorem 7 Let x and y be positive integers, and take $u, v \in \{0, 1\}$. Then for distinct positive primes

p and q and positive integer c , the equation

$$(-1)^u p^x + (-1)^v q^y = c \quad (25)$$

has at most two solutions (x, y, u, v) except when (p, q, c) or (q, p, c) is:

$(3, 2, 5)$ which has four solutions, or

$(3, 2, 1)$, $(3, 2, 7)$, $(3, 2, 11)$, $(3, 2, 13)$, or $(5, 2, 3)$ which each have three solutions.

Further, if M is a Mersenne prime greater than 3, F a Fermat prime greater than 3, and if $c > 3$, then (25)

has exactly two solutions when $q = 2$ and (p, c) is one of the following:

$(M, M + 2)$, $(F, F - 2)$, $(M, 2M + 1)$, $(F, 2F - 1)$, $(M, M^2 + M + 1)$, $(F, F^2 - F + 1)$.

(Note that for a solution, x and y uniquely determine u and v .)

Proof:

Using Theorem 5 of [Sc] when $p + q \geq c$ and in all other cases using Theorem 2 of [Sc], we can easily verify the indicated number of solutions for the six (p, q, c) listed.

From here on, assume (p, q, c) is not one of the six exceptions given. If (25) has three solutions, for a proper choice of p and q we have one of the following six possibilities:

$$p^{x_1} - q^{y_1} = p^{x_2} - q^{y_2} = p^{x_3} - q^{y_3} \quad (26)$$

$$p^{x_1} - q^{y_1} = p^{x_2} - q^{y_2} = -p^{x_3} + q^{y_3} \quad (27)$$

$$p^{x_1} - q^{y_1} = p^{x_2} - q^{y_2} = p^{x_3} + q^{y_3} \quad (28)$$

$$p^{x_1} - q^{y_1} = -p^{x_2} + q^{y_2} = p^{x_3} + q^{y_3} \quad (29)$$

$$p^{x_1} + q^{y_1} = p^{x_2} + q^{y_2} = -p^{x_3} + q^{y_3} \quad (30)$$

$$p^{x_1} + q^{y_1} = p^{x_2} + q^{y_2} = p^{x_3} + q^{y_3} \quad (31)$$

Solutions to (26) and (27) are handled by Theorem 5 of [Sc]. We proceed to (28) which we break into the equations

$$p^{x_1} - q^{y_1} = p^{x_2} - q^{y_2} \quad (28a)$$

$$p^{x_n} - p^{x_3} = q^{y_n} + q^{y_3} \text{ where } n = 1 \text{ or } 2. \quad (28b)$$

From (28b), we see that p divides the sum of two powers of q , therefore the congruence $q^t \equiv -1 \pmod{p}$ has a solution t . Thus, if $p > 2$, then $2 \mid \text{ord}_p q$. Applying Theorem 4 of [Sc] to (28a), we must have one of the specific cases we have already excluded.

We proceed to (29), which we break into three equations:

$$p^{x_1} + p^{x_2} = q^{y_1} + q^{y_2} \quad (29a)$$

$$p^{x_1} - p^{x_3} = q^{y_1} + q^{y_3} \quad (29b)$$

$$p^{x_2} + p^{x_3} = q^{y_2} - q^{y_3} \quad (29c)$$

Assume first that p and q are odd primes. Then from (29a), we see that $2 \mid \text{ord}_q p$ and $2 \mid \text{ord}_p q$. So we cannot have both p and q congruent to 3 modulo 4. From (29b), since $2 \mid \text{ord}_q p$, we must have $2 \mid x_1 - x_3$, so 8 divides the left hand side of (29b), so $q \equiv 7 \pmod{8}$. In the same manner using (29c), we show that $p \equiv 7 \pmod{8}$, impossible since this contradicts p and q not both congruent to 3 modulo 4.

So one of p or q is 2; without loss of generality, $q = 2$. Now from (29a) we find that $2 \mid \text{ord}_p 2$, therefore $p \not\equiv 7 \pmod{8}$, so 8 does not divide the left side of (29a), so $y_1 = 1$ or 2. (Note that $y_2 = 1$ or 2 would make (29c) impossible.) Turning to (29c), again $p \not\equiv 7 \pmod{8}$ shows that 8 does not divide the left side, and we must have $y_3 = 1$ or 2. In (29b), we must have $p^{x_1} = 9$ and $p^{x_3} = 3$, so $c = 5$ or $c = 7$, which cases have both been excluded from consideration.

We proceed to (30), which we express as two equations,

$$p^{x_1} - q^{y_2} = p^{x_2} - q^{y_1} \quad (30a)$$

$$p^{x_3} + p^{x_n} = q^{y_3} - q^{y_n} \text{ with } n = 1, 2. \quad (30b)$$

First assume both p and q are odd. If $p^{x_1} < q^{y_2}$ we must have, by Theorem 4 of [Sc], that $2 \nmid \text{ord}_q p$. But (30b) shows that $2 \mid \text{ord}_q p$. So $p^{x_1} > q^{y_2}$, and now Theorem 3 of [Sc] applies to show if $2 \mid y_1 - y_2$, then $p = 13$ and $q = 3$. But then (30b) becomes impossible modulo 3, so 2 does not divide $y_1 - y_2$. If we let 2^{t_n} be the highest power of 2 dividing the right hand side of (30b), as n changes value from 1 to 2, t_n must also change value, i.e., $t_1 \neq t_2$. On the other hand, $2 \mid \text{ord}_q p$, so 2 divides $x_1 - x_2$. If 2^{s_n} is the highest power of 2 dividing the left hand side of (30b) for $n = 1, 2$, then $s_1 = s_2$. This leads to a contradiction. Thus, either p or q equals 2.

Now if (30a) corresponds to one of the specific cases listed in part (a) of Theorem 4 in [Sc], then we must have $c = 11, 35, 259$, or 133 . All of these require p or q equal to 3, except 133 which requires p or q equal to 5. The case $c = 11$ has already been excluded from consideration. In the remaining cases, $7 \mid c$, which we can use to show that the equation $q^{y_3} - p^{x_3} = c$ is impossible, since each case leads to a contradiction between the equation viewed modulo 7 and viewed modulo 8.

So we can assume that (30a) is not one of the specific cases listed in Theorem 4 of [Sc], which shows that if $p = 2$ then $\text{ord}_q 2$ must be odd, contradicted by (30b), so we must have $q = 2$ with both sides of (30a) positive. Theorem 3 of [Sc] shows that $2 \nmid y_1 - y_2$ since (30a) cannot be one of the exceptional cases of Theorem 3 of [Sc]. Viewing (30a) modulo 3 we see that $p \equiv 2 \pmod{3}$, $2 \nmid x_1 - x_2$, and $2 \nmid x_n - y_n$ with $n = 1, 2$. In (30b) we can choose n such that $2 \mid x_3 - x_n$, $y_n = 1$, $q^{y_3} - q^{y_n} \equiv 6 \pmod{8}$, $2 \nmid x_n$. But this contradicts $2 \nmid x_n - y_n$.

Finally, we proceed to (31). Without loss of generality, $x_1 > x_2 > x_3$ and $y_1 < y_2 < y_3$. Now $p^{x_2} \leq p^{x_1}/p < c/p$ and $q^{y_2} \leq q^{y_3}/q < c/q$, so $c = p^{x_2} + q^{y_2} < c/p + c/q < c$, an impossibility. This completes the proof of the first part of Theorem 7.

For the proof of the second part, note the following equations:

$$\begin{aligned} M + 2 &= 2(M + 1) - M \\ F - 2 &= 2(F - 1) - F \\ (M + 1) + M &= (M + 1)^2 - M^2 \\ F + (F - 1) &= F^2 - (F - 1)^2 \end{aligned}$$

These show that the cases listed in the second part of Theorem 7 have at least two solutions. The restriction M , F , and c all greater than 3 simply eliminates those cases listed earlier. This completes the proof of Theorem 7.

§5. Solutions to $p^x \pm q^y \pm 2^z = 0$

Theorem 8 Let x , y , and z be positive integers, and take $i, j \in \{0, 1\}$. Then for given distinct positive primes p , q , and r , the equation

$$p^x + (-1)^i q^y + (-1)^j r^z = 0 \quad ((32))$$

has at most two solutions (x, y, z, i, j) except when (p, q, r) is a permutation of one of the following:

(5, 3, 2) which has 7 solutions,

(7, 3, 2) which has 4 solutions,

(11, 3, 2) which has 3 solutions,

(13, 3, 2) which has 3 solutions.

(Clearly, for any solution, (x, y, z) uniquely determines (i, j) in (1).)

Proof: We can assume $r = 2$. We assume also that (p, q, r) is not one of the specific cases listed in the theorem. We will need the following lemmata.

Lemma 1: Let a and b be distinct positive integers, and let p be a positive odd prime. Let $2^u \parallel \text{ord}_p a$ and $2^v \parallel \text{ord}_p b$, taking $0 \leq u \leq v$ (recall $\text{ord}_p a$ is the least positive t such that $a^t \equiv 1 \pmod{p}$.) Take j in the set $\{0, 1\}$ and let x and y be positive integers such that

$$a^x \equiv (-1)^j b^y \pmod{p}.$$

Let $s = 0$ when $j = 0$ and let $s = (\text{ord}_p b)/2$ when $j = 1$. Then, for either choice of j , s is an integer, and $2|y + s$ when $u < v$, while $2|x - (y + s)$ when $u = v$.

Proof: The following properties of $\text{ord}_p a$ are easily verified:

$$2|\text{ord}_p a \text{ iff } \exists m \text{ such that } a^m \equiv -1 \pmod{p}; a^m \equiv -1 \pmod{p} \text{ iff } m \text{ is an odd multiple of } (\text{ord}_p a)/2. \quad (33)$$

If $\text{ord}_p a$ is odd, then $\text{ord}_p(-a)$ is even. (34)

$$\text{ord}_p a^n = \frac{\text{ord}_p a}{(\text{ord}_p a, n)}. \quad (35)$$

Assume $a^x \equiv (-1)^j b^y \pmod p$. If $j = 1$, we cannot have $u = v = 0$, by (34) above, so $v \geq 1$ and s is an integer. So, for either choice of j , $a^x \equiv b^{y+s} \pmod p$ by (33), $\text{ord}_p a / (\text{ord}_p a, x) = \text{ord}_p b / (\text{ord}_p b, y+s)$ by (35), and the lemma follows.

Lemma 2. The equation

$$3^x + 2^y = n^z. \quad (36)$$

has no solutions in positive integers (x, y, z, n) with $z > 1$ except for $3^2 + 2^4 = 5^2$.

Proof: After Theorem 2 of [Sc], we have $z = 1$, unless $2 \mid x$, $2 \mid y$, and $z = 2$. In this case we subtract 3^x from both sides of (36) and factor the right side as a difference of squares to derive the equation $3^{x/2} = 2^{y-2} - 1$, which has as its only solution $x = 2$ and $y = 4$, proving the lemma.

Lemma 3. [Stroecker and Tijdeman] The equation

$$3^x - 2^y = 3^w - 2^z = d$$

has no solutions in positive integers (w, x, y, z) with $w \neq x$ except when d equals 1, -5 , or -13 ; in each of these cases it has exactly one solution.

This was first proven in [St-T] using Baker's method. It also follows as an immediate corollary of Theorem 4 in [Sc].

Lemma 4. [Cao] The equation

$$q^n + 2^h = p^w \quad (37)$$

where p and q are distinct positive primes, n is positive and even, h is a positive integer, and $w > 1$ has as its only solutions

$$3^2 + 2^4 = 5^2, \quad 7^2 + 2^5 = 3^4, \quad 5^2 + 2 = 3^3, \quad \text{and} \quad 11^2 + 2^2 = 5^3.$$

As far as we know, there is no published proof of this lemma, although existence of a proof is mentioned in [Cao] which is an abstract of a paper in Chinese. For this reason, we give a proof here which may differ from Cao's proof.

Assume first that $2 \mid w$ as well as $2 \mid n$. Subtract q^n from both sides and factor the right side as a difference of squares to get the result

$$p^{w/2} = 2^{h-2} + 1 = q^{n/2} + 2$$

which implies $p^{w/2}$ must be either 5 or 9. This gives the first two specific cases listed in the theorem as the only possible solutions to (37) in the case where $2 \mid w$.

Consider now the case $2 \nmid w$. As always $w > 1$ and $2 \mid n$. Set e equal to 0 or 1 according as 2 divides h or not. Set $p = a_1^2 + 2^e b_1^2$, with b_1 even if $e = 0$, so the choice of positive integers a_1 and b_1 is unique. Then (37) becomes

$$\pm(q^{n/2} \pm 2^{(h-e)/2} \sqrt{-2^e}) = (a_1 + b_1 \sqrt{-2^e})^w. \quad (37a)$$

Using Lemmata 1–3 of [Sc] we obtain $b_1 = 2^{(h-e)/2}$ and similarly $a_1 = q^k$ where $0 \leq k \leq n/2$. Suppose $k > 0$. Then $w = 1$ satisfies (37) for this choice of p , q , and h , if we relax the condition $w > 1$ to $w > 0$. By Lemma 6 of [Sc], it is the only solution.

So $w > 1$ implies $k = 0$ and $p = 2^h + 1$. By Theorem 13 of [B-H], $w \equiv 3 \pmod{4}$ and w is unique for given (p, h) . Now assume $h \geq 3$. $2^h \equiv 1 \pmod{5}$ and $p \equiv 2 \pmod{5}$ so that $p^w \equiv 3 \pmod{5}$ and $p^w - 2^h = q^n \equiv 2 \pmod{5}$, impossible when n is even. This contradiction shows that $h = 1$ or 2 . Each of these cases has a solution at $w = 3$, which is the only solution by Theorem 13 of [B-H]. Thus, we arrive at the last two exceptional equations listed in Lemma 4, concluding the proof of the lemma.

Returning to the proof of Theorem 8 itself, we observe the three forms that (32) can take are Equations

$$p^x + q^y = 2^z \quad (38)$$

$$q^y + 2^z = p^x \quad (39)$$

$$p^x + 2^z = q^y \quad (40)$$

By Theorem 6 of [Sc], (38) has at most one solution, while (39) and (40) have at most two solutions each. We divide the remainder of the proof into two cases.

Case 1

$$3 \nmid pq$$

Assume (39) has two solutions, (x_1, y_1, z_1) and (x_2, y_2, z_2) . Assume further that we have $2 \mid y_1 - y_2$. Then consideration modulo 3 shows that $2 \mid z_1 - z_2$, contradicting Lemma 6 of [Sc].

Thus, $2 \nmid y_1 - y_2$. We take y_1 even, so z_1 is even, and we have

$$q^{y_1} + 2^{z_1} = p^{x_1} \text{ where } 2 \mid y_1 \text{ and } 2 \mid z_1 \tag{39a}$$

$$q^{y_2} + 2^{z_2} = p^{x_2} \text{ where } 2 \nmid y_2. \tag{39b}$$

Let $2^u \parallel \text{ord}_p q$ and let $2^v \parallel \text{ord}_p 2$. Applying Lemma 1 to (39a), we get $\max(u, v) \geq 2$. Then applying Lemma 1 to (39b), we get $v \geq u$. If $v > u$, then $2 \mid z_2$, so that $q \equiv 1 \pmod{3}$, and, if a third solution exists, we must have (38) or (40) with $2 \nmid z$ (by consideration modulo 3), contradicting $2 \mid z$ (required by Lemma 1). If $v = u$, then $2 \nmid z_2$ so that $q \equiv 2 \pmod{3}$, and, if a third solution exists, we must have (38) or (40) with $2 \nmid x - y$ (by consideration modulo 3), contradicting $2 \mid x - y$ (required by Lemma 1).

Thus we see that if there are two solutions to (39) there cannot be three solutions to (32). Similarly, (40) cannot have two solutions if (32) has three solutions.

Therefore, if there are more than two solutions to (32), there must be exactly one solution to each of (38), (39), and (40). Now (38) has three possible types of solutions (assigning roles to p and q without loss of generality):

Type 1

$$p \equiv -q \equiv 5 \pmod{8} \text{ with } 2 \nmid xy$$

Type 2

$$p \equiv -q \equiv 1 \pmod{8} \text{ with } 2 \nmid xy$$

Type 3

$$2 \mid x \text{ and } 2 \nmid y \text{ and } q \equiv 7 \pmod{8}$$

Since $3 \nmid pq$, we have $q \equiv 1 \pmod{3}$ and $2 \nmid z$ for the Type 3 solution.

Assume (32) has three solutions.

Suppose $q \equiv 7 \pmod{8}$ and y is odd in (38). Then if $p \equiv 1$ or $3 \pmod{8}$, then p is a quadratic residue modulo q and (40) is impossible since a prime congruent to 3 modulo 4 cannot divide a sum of two of its residues. If $p \equiv 5$ or $7 \pmod{8}$, then p is a quadratic non-residue modulo q , and (39) becomes impossible modulo 3.

So if (32) has more than two solutions then the solution to (38) must be of Type 1. In this case, we have $p \equiv q \equiv 2 \pmod{3}$, otherwise (39) and (40) are impossible. If $p \equiv q \equiv 2 \pmod{3}$ then $2 \mid z$ in (38), so p and q are quadratic residues of each other. Viewing (40) modulo q , we have $2 \nmid z$ whereas viewing (40) modulo p we have $2 \mid z$, a contradiction.

We conclude that if $3 \nmid pq$ then (32) has at most two solutions.

Case 2

$$q = 3$$

(38) has at most one solution by Theorem 6 of [Sc]. Lemma 4 implies that, since $y = 1$ is impossible in (40), $2 \nmid x$, so p^x is determined modulo 3, so the parity of z is determined. Now Lemma 6 of [Sc] shows that (40) has at most one solution.

We will show that (39) also has at most one solution. Applying Lemma 2 to (39), $x = 1$. The existence of two solutions with $x = 1$ is impossible since Lemma 3, along with (16), (17) and (18) of [Sc], shows $3^x + 2^z = 3^w + 2^y = c$ implies $c = 11, 35$, or 259 . Only 11 is prime and $(p, q, r) = (11, 3, 2)$ is already excluded.

So if there are more than two solutions to (32) when $q = 3$, then (38), (39), and (40) each have precisely one solution. If $p \equiv 1$ or $3 \pmod{8}$ then (38) is impossible.

Assume $p \equiv 5 \pmod{8}$. Apply Lemma 4 to (40) to see that x is odd. Therefore, viewing (40) modulo 8, we see that y is even and $z = 2$. In this case, subtracting 4 from both sides of (40) and factoring the differences of squares shows that $p = 5$ (one of the excluded cases.)

Assume $p \equiv 7 \pmod{8}$. Consider (39) modulo p to see that $\left(\frac{3}{p}\right) = -1$, so that $p \equiv 1 \pmod{3}$.

Returning to (38), note that $p \equiv 1 \pmod{3}$ implies $2 \mid z$. Subtract 3^y from both sides of (38) and factor the differences of squares to yield $p = 7$, an excluded case.

We conclude that (32) has at most two solutions except for the cases listed in Theorem 8. It is easy to verify (for instance, using Theorem 2 of [Sc] or more elementary arguments) the specific number of solutions in these special cases. This finishes the proof of Theorem 8.

Observations: We do not use the full generality of Lemma 4: for the purposes of the proof of Theorem 8, when $2 \nmid w$ in Lemma 4, we need to consider only $h = 1$, $p = 3$ (writing $(1 + \sqrt{-2})^j = a_j + b_j\sqrt{-2}$ and considering the sequence $b_j \pmod{9}$, we see that any solution to $q^{2m} + 2 = 3^w$ with $w > 1$ must have $3 \mid w$ so that $5 \mid a_w b_w$, so $q = 5$ and Theorem 1 of [Sc] shows that the only solution with w odd is $5^2 + 2 = 3^3$).

When $3 \nmid pq$, Lemma 1 is only needed to handle the case $p \equiv q \equiv 1 \pmod{8}$, although the lemma is useful to handle the other cases as well.

Also observe that we used Lemmas 2 and 3 to show that (39) has at most one solution when $q = 3$ unless $p = 5$ or 11 . In fact, these lemmas were only necessary when $p \equiv 11 \pmod{24}$. The other cases could have been shown via Lemma 6 of [Sc] along with elementary considerations of quadratic residues and considerations modulo 3, 8, and p .

We conclude by noting that Theorem 2 of [Sc] gives us efficient bounds for solutions (x, y, z) to

$$p^x \pm q^y \pm 2^z = 0 \tag{41}$$

for any given pair of primes p and q . Nagell [N2] found all solutions (x, y, z) for the case of primes $p, q \leq 7$. Hadano [Ha] and Uchiyama [U] improved this to $p, q \leq 17$. We have applied the bounds from Theorem 2 of [Sc] to systematically determine all solutions for pairs of primes $p, q < 1000$ [St2]. There are 481 solutions in this range. Of the 481 solutions, 35 of these have all three powers equal to one (twin primes), 328 have exactly one power exceeding one (in 315 of these, the exponent of 2 exceeds one), 113 have exactly two of

the powers exceeding one, and 5 solutions have all three powers greater than one:

$$\begin{aligned}
 3^2 + 2^4 &= 5^2 \\
 7^2 + 2^5 &= 3^4 \\
 11^2 + 2^2 &= 5^3 \\
 7^3 + 13^2 &= 2^9 \\
 17^3 + 2^7 &= 71^2
 \end{aligned}
 \tag{42}$$

The question naturally arises whether there are any further examples of (41) with all of x , y and z greater than one. Using only the arithmetic of cubic fields, Rabinowitz [Ra] obtained results from which it easily follows that if there are any further examples with all three exponents greater than one, then either x or y must be relatively prime to 6. Using deeper methods, Bennett and Skinner [B-S] obtained results from which it easily follows that if there are any further examples with all three exponents greater than one, then $2 \nmid xy$. The methods of [B-S] handle many specific cases of (41), provided at least two of x , y and z are greater than one. (In this section, however, we have always treated the possibility that any or all of the exponents could equal one.)

Note that three of the equations in (42) satisfy

$$1/x + 1/y + 1/z < 1 \tag{43}$$

Even if one allows the bases to be any coprime integers, we only know seven other examples satisfying (43): $1 + 2^3 = 3^2$, $3^5 + 11^4 = 122^2$, and five extraordinarily large solutions found by Beukers and Zagier [Ma].

Twelve triples of primes $\{p, q, 2\}$ have more than one solution (x, y, z) to (41): $\{3, q, 2\}$ for $q = 5, 7, 11, 13, 17, 19, 23, 29$ and 73 , plus $\{5, 7, 2\}$, $\{5, 11, 2\}$, and $\{7, 11, 2\}$. Four of these are the listed exceptions in Theorem 8, and the other eight have precisely two solutions. It seems likely that these eight are the only examples with two solutions.

References:

[A1] L. J. Alex, Diophantine equations related to finite groups, *Comm. Algebra*, **4**, no. 1 (1976), 77–100.

- [A2] L. J. Alex, review 83k:10053, *Mathematical Reviews*, American Mathematical Society, Providence, (1983) (also appears as D60–266 in *Reviews in Number Theory 1973–83*, edited by Richard Guy, American Mathematical Society, Providence, 1984).
- [A-M] S. A. Arif, F. S. A. Muriefah, On the Diophantine equation $x^2 + 2^k = y^n$, *Internat. J. Math. Math. Sci.*, **20**, no. 2 (1997), 299–304.
- [B-H] E. Bender and N. Herzberg, Some Diophantine equations related to the quadratic form $ax^2 + by^2$, in *Studies in Algebra and Number Theory*, G.-C. Rota, Ed., pp. 219–272, Advances in Mathematics Supplementary Studies, Vol. 6, Academic Press, San Diego, 1979.
- [Be] M. Bennett, On some exponential equations of S. S. Pillai, *Canadian Journal of Mathematics*, **53**, no. 5 (2001), 897–922.
- [B-S] M. Bennett and C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canadian Journal of Mathematics*, to appear.
- [Bk] F. Beukers, The Diophantine equation $Ax^p + By^q = Cz^r$, *Duke Math. J.*, **91**, no. 1 (1998), 61–88.
- [B-H-V] Y. Bilu, G. Hanrot, P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, With an appendix by M. Mignotte, *J. Reine Angew. Math.*, **539**, (2001), 75–122.
- [B-F] J. L. Brenner and L. L. Foster, Exponential Diophantine Equations, *Pacific J. of Math.*, **101**, no. 2 (1982), 263–301.
- [Cao] Z. F. Cao, On the Equation $x^2 + 2^m = y^n$ and Hugh Edgar’s Problem. *Kexue Tongbau* [in Chinese], **31**, (7) (1986), pp. 555–556.
- [C-W] Z. F. Cao and D. Z. Wang, On a problem of Hugh Edgar, it *Kexue Tongbau*, **32**, (14), (1987), 1043–1046.
- [Cas] J. W. S. Cassels, On the equation $a^x - b^y = 1$, *American Journal of Mathematics*, **75**, (1953), 159–162.

- [Co] H. Cohn, *Advanced Number Theory*, Dover Pub., New York, 1980 (reprint of *A Second Course in Number Theory*, John Wiley and Sons, New York, 1962)
- [CoJ1] J. H. E. Cohn, The Diophantine equation $x^2 + 2^k = y^n$, *Arch. Math. (Basel)*, **59**, no. 4 (1992), 341–344.
- [CoJ2] J. H. E. Cohn, The Diophantine equation $x^2 + 2^k = y^n$, II, *Int. J. Math. Math. Sci.*, **22**, no. 3 (1999), 459–462.
- [C-D-P] R. Crandall, K. Dilcher, and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* **66**, no. 217 (1997), 433–449.
- [C-P] R. Crandall and C. Pomerance, *A Computational Perspective*, Springer Verlag, New York, 2001
- [G] R. K. Guy, *Unsolved Problems in Number Theory, second edition*, Springer-Verlag, New York, 1994.
- [Ha] T. Hadano, On the Diophantine equation $a^x + b^y = c^z$, *Math. J. Okayama Univ.*, **19**, no. 1 (1976/77), 25–29.
- [He] A. Herschfeld, The equation $2^x - 3^y = d$, *Bull. Amer. Math. Soc. (N. S.)*, **42**, no. 4 (1936), 231–234.
- [Le] M. Le, On Cohn’s conjecture concerning the Diophantine equation $x^2 + 2^m = y^n$, *Archiv der Mathematik*, **78**, (2002), 26–35.
- [Lev] W. J. Leveque, On the equation $a^x - b^y = 1$, *American Journal of Mathematics*, **74**, (1952), 325–331.
- [Li] J. E. Littlewood, *Some Problems in Real and Complex Analysis*, Heath, Lexington MA., 1968, Problem 1.
- [Lj] W. Ljunggren, Über die Gleichung $x^2 + 2 = y^k$, *Ark. Mat.*, **29 A**, 13, (1943), 1–11.
- [Lu] F. Luca, On the equation $x^2 + 2^a 3^b = y^n$, *Int. J. Math. Math. Sci.*, **29**, no. 4 (2002), 239–244.
- [Ma] B. Mazur, Questions about Powers of Numbers, *Notices of the American Mathematical Society*, **47**, no.

2 (2000), 195–202.

[Mc] Richard McIntosh, letter dated 3/3/03 posted on the web at
<http://www.loria.fr/~zimmerma/records/Wieferich.status>

[Mi1] M. Mignotte, A corollary to a theorem of Laurent-Mignotte-Nesterenko, *Acta Arithmetica*, **86**, (1998), 101-111.

[Mi2] M. Mignotte, Catalan's equation just before 2000, *Number Theory, Turku 1999*, deGruyter, Berlin, (2001), 247–254.

[M-T] D. Z. Mo, R. Tijdeman, Exponential Diophantine equations with four terms, *Indag. Math. (N.S.)*, **3**, no. 1 (1992), 47–57.

[N1] T. Nagell, Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns, *Nova Acta Soc. Sci. Upsal.*, **4** 16, no. 2 (1955), 38 pp.

[N2] T. Nagell, Sur une classe d'équations exponentielles, *Ark. Mat.*, **3**, (1958), 569–582.

[Pi1] S. S. Pillai, On the inequality $0 < a^x - b^y \leq n$, *J. Indian Math. Society*, **19**, (1931), 1–11.

[Pi2] S. S. Pillai, On the equation $2^x - 3^y = 2^X + 3^Y$, *Bull. Calcutta Soc.*, **37**, (1945), 15-20.

[Ra] S. Rabinowitz, The solution of $y^2 \pm 2^n = x^3$, *Proc. Amer. Math. Soc.*, **62**, no. 1 (1977), 1–6.

[Sc] R. Scott, "On the Equations $p^x - b^y = c$ and $a^x + b^y = c^z$ ", *Journal of Number Theory*, **44**, no. 2 (1993), 153-165.

[Sh-T] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, 1986.

[Ste] R. Steiner, Class number bounds and Catalan's equation, *Math. Comp.*, **67**, no. 223 (1998), 1317–1322.

[St-T] R. J. Stroeker and R. Tijdeman, Diophantine Equations, pp. 321-369, *Computational Methods in Number Theory*, MC Track 155, Central Math Comp Sci, Amsterdam, 1982.

[St1] R. Styer, Small two variable exponential Diophantine equations, *Math. Comp.*, **60**, no. 202 (1993), 811-816.

[St2] R. Styer, <http://www.homepage.villanova.edu/robert.styer/ReeseScott/index.htm>, contains links to programs and data files.

[Te] N. Terai, Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations, *Acta Arithmetica*, **90**, no. 1 (1999), 17-35.

[U] S. Uchiyama, On the Diophantine equation $2^x = 3^y + 13^z$, *Math. J. Okayama Univ.*, **19**, no. 1 (1976/77), 31-38.

[W] B. M. M. de Weger, Solving exponential Diophantine equations using lattice basis reduction algorithms, *J. Number Theory*, **26**, no. 3 (1987), 325-367.