ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 3, Summer 1985

ON THE DIOPHANTINE EQUATION $1 + p^a = 2^b + 2^c p^d$

LEO J. ALEX AND LORRAINE L. FOSTER

ABSTRACT. In this paper the exponential Diophantine equation $1 + p^a = 2^b + 2^c p^d$, where a, b, c, d are non-negative integers and p is an odd prime, is studied. All solutions to the equation are found for which $p \leqq 499$. This work extends earlier work of the authors and J. L. Brenner.

1. Introduction. In this paper we consider the equation

$$1 + p^a = 2^b + 2^c p^d \tag{1}$$

where p is an odd prime and a, b, c and d are non-negative integers. This equation is of the form

$$1 + x = y + z, \tag{2}$$

or, more generally,

$$\sum X_i = 0, \tag{3}$$

where the primes dividing xyz in (2) and $\prod X_i$ in (3) are specified.

There has been very little work done in general to solve such Diophantine equations. For example the equation

$$1 + 2^a 3^b = 5^c + 2^d 3^e 5^f \tag{4}$$

is unsolved. Some of these equations have an infinite number of trivial solutions. (For example the equation (4) above has infinitely many solutions of the form $c = f = 0$, $a = d$, and $b = e$.) It is unknown whether such equations always have only a finite number of non-trivial solutions.

It follows from work of Dubois and Rhin [6] and Schlickewei [7] that the related equation $p^a \pm q^b \pm r^c \pm s^d = 0$ has only finitely many solutions when p, q, r and s are distinct primes. However, their methods do not seem to apply when the terms in the equation are not powers of distinct primes.

The authors and J. L. Brenner [1], [2], [4], [5] have recently developed techniques which solve such equations in some cases. These techniques

Received by the editors February 2, 1984. Revised April 30, 1984

involve careful consideration of the equation modulo a series of primes and prime powers.

Such equations arise quite naturally in the character theory of finite groups. If G is a finite simple group and p is a prime dividing the order of G to the first power only, then the degrees $x_1, x_2, \ldots, x_m$ of the ordinary irreducible characters in the principal p-block of G satisfy an equation of the form $\sum \delta_i x_i = 0$, $\delta_i = \pm 1$, where the primes dividing $\prod x_i$ are those in $|G|/p$. Much information concerning the group G can be obtained from the solutions to this degree equation. For example, one of the authors in [3] has used solutions to the equation

$$1 + 2^a = 3^b 5^c + 2^d 3^e 5^f$$

to characterize the simple groups $L(2, 7)$, $U(3, 3)$, $L(3, 4)$ and A_8.

In §2 several general results regarding equation (1) arede rived.

In §3 the results obtained in §2 are used to find all solutions to equation (1) with $p \leqq 499$.

2. Equations of the form $1 + p^a = 2^b + 2^c p^d$. In this section we derive several general results regarding equation (1). We first note that if (a, b, c, d) is a solution to equation (1) with $b > 0$, then clearly $c > 0$.

LEMMA 2.1. *Suppose $p \equiv 3 \pmod 8$ and let (a, b, c, d) be a solution to equation (1) such that $b > 0$. Then*

(i) *either b or c is equal to 1 or 2;*

(ii) *if $p \geqq 11$, then b or c is 2 and a is odd; and*

(iii) *if $p \geqq 11$ and $d > 0$, then $c = 2$.*

PROOF. Since $1 + 3^a \equiv 2^b + 2^c 3^d \pmod 8$, either b or c is equal to 1 or 2. Write $p - 1 = 2m$, $m = 4k + 1 \geqq 5$. Then if b or c is 1, $0 \equiv 2^x \pmod m$ for $x = c$ or b, a contradiction. Hence $b, c \geqq 2$ and consideration mod 4 implies that a is odd. Finally, if $d > 0$, then $1 \equiv 2^b \pmod p$, $b < 3$ and $c = 2$.

LEMMA 2.2. *Let $p \equiv 5 \pmod 8$, $p > 5$. Then there is no solution to equation (1) with $b > 0$.*

PROOF. Suppose that (a, b, c, d) is a solution with $b > 0$. Since $1 + 5^a \equiv 2^b + 2^c 5^d \pmod 8$, clearly b or c is 1. Let $p - 1 = 4m$, $m > 1$, m odd. Then $0 \equiv 2^x \pmod m$, where $x = c$ or b, a contradiction.

LEMMA 2.3. *Let $p \equiv 1 \pmod 8$ and suppose that p is not a Fermat prime. Then equation (1) has no solution with $b > 0$.*

PROOF. Suppose that (a, b, c, d) is a solution with $b > 0$. Then consideration mod 8 implies that b or c is 1. Further, since p is not a Fermat prime, $p - 1$ has an odd factor $m > 1$. Thus we obtain a contradiction mod m.

The following obvious result is useful.

LEMMA 2.4. *If* $p \equiv -1 \pmod 3$ *and* (a, b, c, d) *is a solution to equation* (1) *then* $(a, b, c, d) \equiv (0, 0, 0, 0), (0, 0, 1, 1), (1, 0, 0, 1), (1, 0, 1, 0), (1, 1, 0, 0)$ *or* $(1, 1, 1, 1) \pmod 2$.

THEOREM 2.5. *Let* $p = 2^q - 1$, $q > 2$ *(so that* p *is a Mersenne prime). Then the solutions to equation* (1) *are* $(a, b, c, d) = (t, 0, 0, t)$ *and* $(1, q - 1, q - 1, 0)$, $t \geqq 0$.

PROOF. Let (a, b, c, d) be another solution. Since q must be an odd prime, $p \equiv 1 \pmod 3$, $2 \equiv 2^b + 2^c \pmod 3$, $b \equiv c \equiv 0 \pmod 2$, and $bc \neq 0$. Hence $1 + (2^q - 1)^a \equiv 0 \pmod 4$, so that a is odd.

Case I. $d = 0$. We may write equation (1) as $1 + p^a = 2^b + 2^c$. If $b, c \leqq q - 1$, then clearly since $0 \equiv 2^b + 2^c \pmod{2^q}$, it follows that $b = c = q - 1$, $a = 1$, a contradiction. If b or c is q then $p^a = 2^x + p$, where $x = c$ or b, also a contradiction. If $b, c \geqq q + 1$, then $2^q \equiv 2^q a \equiv 1 + p^a \equiv 0 \pmod{2^{q+1}}$, another contradiction.

Case II. $d > 0$. Here $1 \equiv 2^b \pmod p$, q divides b, $b \geqq 2q > q + 1$. Hence $2^q \equiv 2^c p^d \pmod{2^{q+1}}$, $c \geqq q + 1$, again a contradiction.

LEMMA 2.6. *Let* $p = 48k + 7$, $k \geqq 0$. *Then the solutions to equation* (1) *are* $(a, b, c, d) =$

(i) $(t, 0, 0, t)$ *and* $(1, 2, 2, 0)$ *if* $p = 7$, *and*

(ii) $(t, 0, 0, t)$ *if* $p > 7$.

Here $t \geqq 0$.

PROOF. Let (a, b, c, d) be another solution. Since $2 \equiv 2^b + 2^c \pmod 3$, b and c are even. Consideration mod 8 implies that either $b = c = 2$ or $b, c \geqq 4$. In the former case, $1 \equiv 2^2 \pmod p$, a contradiction; in the latter case $1 + p^a \equiv 0 \pmod{16}$. Since $p \equiv 7 \pmod{16}$, $p^2 \equiv 1 \pmod{16}$, and we again have a contradiction.

LEMMA 2.7. *Let* $p = 56k + 43$, $k \geqq 0$. *Then the only solutions to equation* (1) *are* $(a, b, c, d) = (t, 0, 0, t)$, $t \geqq 0$.

PROOF. Suppose that (a, b, c, d) is another solution. By Lemma 2.1, b or c is 2. Hence $2 \equiv 1 + p^a \equiv 2^b + 2^c \equiv 2^x + 4 \pmod 7$, where $x = c$ or b, a contradiction.

LEMMA 2.8. *Let* $p = 184k + 139$, $k \geqq 0$. *Then the only solutions to equation* (1) *are* $(a, b, c, d) = (t, 0, 0, t)$, $t \geqq 0$.

PROOF. Let (a, b, c, d) be another solution. By Lemma 2.1, without loss of generality, $c = 2$. Then consideration mod 23 yields a contradiction.

THEOREM 2.9. *Let p be a prime of the form* $2 \cdot 9^k + 1, k \geqq 1$. *Then the solutions to equation* (*1*) *are* $(a, b, c, d) =$

(i) $(t, 0, 0, t)$, $t \geqq 0$, *for* $k \geqq 1$, *and*

(ii) $(1, 2, 4, 0)$ *and* $(1, 4, 2, 0)$, *for* $k = 1$.

PROOF. Let (a, b, c, d) be another solution. By Lemma 2.1 a is odd and without loss of generality we may assume $c = 2$. Thus we have $2 \equiv 2^b + 4 \pmod 9$ so that $b \equiv 4 \pmod 6$. Similarly, if $k > 1$, $-2 \equiv 2^b \pmod{81}$ so that $b \equiv 28 \pmod{54}$. Suppose $d > 0$. Then $1 \equiv 2^b \pmod p$ so that $3 \mid b$, a contradiction. Hence we may assume $d = 0$, so that $p^a = 2^b + 3$. If $k = 1$, then $19^a \equiv 3 \pmod{64}$ so that $a \equiv 5 \pmod{16}$. Thus $12 \equiv 2^b \pmod{17}$, a contradiction.

Hence $k > 1$. If k is even we have $3^a \equiv p^a \equiv 2^b + 3 \pmod 5$ so that $b \equiv 2 \pmod 4$, and hence $b \equiv 10 \pmod{12}$. Thus $p^a \equiv 0 \pmod{13}$, again a contradiction. Thus k is odd and $-1 \equiv p^a \equiv 2^b + 3 \pmod 5$ so that $b \equiv 0 \pmod 4$, and, in fact, $b \equiv 4 \pmod{12}$. Therefore $p^a \equiv 6 \pmod{13}$. We have three cases.

Case I. $k \equiv 0 \pmod 3$. Then $3^a \equiv p^a \equiv 6 \pmod{13}$, a contradiction.

Case II. $k \equiv 1 \pmod 3$. Here $6^a \equiv 6 \pmod{13}$ so that $a \equiv 1 \pmod{12}$. Also $p^a \equiv 0$, 13^a or $9^a \pmod{19}$. Clearly $p^a \not\equiv 0 \pmod{19}$. Since $b \equiv 28 \pmod{54}$ we have $2^b + 3 \equiv 1 \pmod{19}$. But $13^a \equiv 1 \pmod{19}$, $9^a \equiv 1 \pmod{19}$ imply that 18 divides a, 9 divides a, respectively. These are both contradictions.

Case III. $k \equiv 2 \pmod 3$. Now $7^a \equiv 6 \pmod{13}$ so that $a \equiv 7 \pmod{12}$, $p \equiv 2 \pmod 7$, $2 \equiv 2^a \equiv 2^b + 3 \equiv 5 \pmod 7$, another contradiction.

THEOREM 2.10. *Let* $p = 2^{2^n} + 1$ *be a Fermat prime*, $n \geqq 2$. *Then* $(a, b, c, d) = (t, 0, 0, t), (1, 1, 2^n, 0), (1, 2^n, 1, 0)$ *and* $(2, 2^{n+1}, 1, 1)$, $t \geqq 0$, *are solutions to equation* (*1*). *Suppose that* (a, b, c, d) *is another solution. Then:*

(i) $c = 1, d > 2$ *and* $b = 2^{n+1}kp$ *for some positive integer* k,

(ii) $(a, d) \equiv (2, 1)$ *or* $(2^{n+2} + 2, 3 \cdot 2^{n+1} + 1) \pmod{2^{n+3}}$ *and* k *is odd*,

(iii) $(a, k, d) \equiv (2, 5, 1) \pmod 6$, *and*

(iv) (a, b, c, d) *does not exist for* $n = 2, 3, 4$.

PROOF. (i). Let $x = p - 1$. Clearly $b > 0$, $c > 0$. Also $\mathrm{ord}_p 2 = 2^{n+1}$. Consideration of equation (1) modulo 4 implies that b or $c = 1$. Suppose that $b = 1$. Then consideration mod p gives $d = 0$ and $p^a = 1 + 2^c$. Hence $2^{n+1} \mid 2c$, $2^n \mid c$. By hypothesis $c > 2^n$ so that $2^c \equiv 0 \pmod{2x}$ and hence $p^a \equiv 1 \pmod{2x}$. Since $p^a \equiv (x + 1)^a \equiv ax + 1 \pmod{2x}$, we conclude that a is even. However, since $x \equiv 1 \pmod 3$ we then have $0 \equiv 2^c \pmod 3$, a contradiction. Hence $c = 1$ and $1 + p^a = 2^b + 2p^d$. If $d = 0$ we have $p^a = 1 + 2^b$ which leads to a contradiction as in the preceding case. Hence $d \geqq 1$, $1 \equiv 2^b \pmod p$, $2^{n+1} | b$, $2^b = x^{2b'}$ for some positive integer b', $1 + (x+1)^a = x^{2b'} + 2(x+1)^d$. Thus $2^a \equiv 2^{d+1} \pmod 3$, $a \not\equiv d \pmod 2$. Since $1 + (ax + 1) \equiv 2(dx + 1) \pmod{2x}$, we have $a \equiv 0 \pmod 2$ and hence $d \equiv 1 \pmod 2$. Thus we may write $a = 2a'$ $d = 2d' + 1$ for some integers a', d', where $a' > 0$, $d' \geqq 0$. Suppose $d' = 0$ so that $(x+1)^{2a'} = x^{2b'} + 2x + 1$. By hypothesis $b' > 1$, $a' > 1$ and hence $((x+1)^{a'} + x^{b'}) \cdot ((x+1)^{a'} - x^{b'}) = 2x + 1$. Since $(x+1)^{a'} + x^{b'} > a'x + 1 + x \geqq 3x + 1$, we again have a contradiction. Hence $d' > 0, d \geqq 3$. Since $x^p \equiv (p-1)^p \equiv -1 \pmod{p^2}$, we conclude that $\text{ord}_{p^2} x = 2p$. Thus, since $1 \equiv x^{2b'} \pmod{p^2}$, we have $p \mid b'$, $b' = pk$ for some positive integer k. Thus we have established (i).

(ii). Define $z = 2^{2^{n-1}} + 1$, $n \geqq 2$. Clearly $\text{ord}_z 2 = 2^n$ and $x \equiv 1 \pmod z$. Hence $p \equiv 2 \pmod z$ and $2^{2a'} \equiv 2 \cdot 2^{2d'+1} \pmod z$, so that $2a' \equiv 2d' + 2 \pmod{2^n}$ and $a' \equiv d' + 1 \pmod{2^{n-1}}$. Now since $1 + (x+1)^{2a'} \equiv 2(x+1)^{2d'+1} \pmod{2x^2}$, we have

$$a'(2a' - 1)x + 2a' \equiv 2(2d' + 1) \pmod{2x}. \tag{5}$$

Hence a' is odd, say $a' = 2a'' + 1$, $2a'' + 1 \equiv d' + 1 \pmod{2^{n-1}}$ and

$$2a'' \equiv d' \pmod{2^{n-1}}. \tag{6}$$

From congruence (5) we obtain $x + 2(2a'' + 1) \equiv 2(2d' + 1) \pmod{2x}$, so that $2^2(a'' - d') \equiv x \pmod{2x}$, $a'' \equiv d' \pmod{2^{2^n-2}}$, $a'' \equiv d' \pmod{2^{n-1}}$, $n \geqq 2$. Hence from congruence (6), $a'' \equiv 0$ and thus $d' \equiv 0 \pmod{2^{n-1}}$. Write $a'' = 2^{n-1}v$, $d' = 2^{n-1}u$, for positive integers u, v. We now consider equation (1) modulo $w = x^2 + 1$. Clearly $\text{ord}_w x = 4$. Also, it is easily seen that $\text{ord}_w p = 2^{n+3}$. For by induction, $(x+1)^{2^j} \equiv 2^{2^{j-1}} \pmod w$ for $j \geqq 3$. Hence $(x+1)^{2^{n+2}} \equiv x^2 \equiv -1 \pmod w$, so that $\text{ord}_w p = 2^{n+3}$ as asserted. Observe also that $\text{ord}_w 2 = 2^{n+2}$. It now follows from equation (1) that $1 + (x+1)^{2a'} \equiv x^{2b'} + 2(x+1)^{2d'}(x+1) \pmod w$, so that $1 + (2^{2^n+1})^{a'} \equiv x^{2b'} + 2(2^{2^n+1})^{d'}\, p \pmod w$. Suppose that b' is even. Then $p \in \langle 2 \rangle$, contradicting the fact that $\text{ord}_w 2 < \text{ord}_w p$. Hence b' is odd. Further, $p^a \equiv 2^{2(2^{n-1}v)+1}\, x$, $p^d \equiv 2^{2^{n-1}u}(-1)^{2^{n-2}u}(x+1)$, $x^{2b'} \equiv (-1)^{b'} \equiv -1 \pmod w$. Hence $2 + 2^{2^n v}(2x) \equiv 2(2^{2^{n-1}u})(-1)^{2^{n-2}u}(x+1) \pmod w$ so that $1 + 2^{2^n v}x \equiv 2^{2^{n-1}u}(-1)^{2^{n-2}u}(x+1) \pmod w$. Since $\text{ord}_w 2 = 2^{n+2}$, we consider the cases $v \equiv 0, 1, 2, 3 \pmod 4$.

Case I. $v \equiv 0 \pmod 4$. Here $1 \equiv 2^{2^{n-1}u}(-1)^{2^{n-2}u} \pmod w$ yields $u \equiv 0 \pmod 8$.

Case II. $v \equiv 1 \pmod 4$. Here $1 + (2^{2^n v})x \equiv 1 + x^2 \equiv 0 \pmod w$ so that we have an immediate contradiction.

Case III. $v \equiv 2 \pmod 4$. In this case $1 - x \equiv 1 + 2^{2^n v}x \equiv 2^{2^{n-1}u}(-1)^{2^{n-2}u}(x+1) \pmod w$. Multiplication by $1 + x$ yields $2 \equiv 2^{2^{n-1}u}(-1)^{2^{n-2}u}(2x) \pmod w$ so that $1 \equiv 2^{2^{n-1}u+2^n}(-1)^{2^{n-2}u} \pmod w$. Thus $u \equiv 6 \pmod 8$ yields a solution.

Case IV. $v \equiv 3 \pmod 4$. Here $2 \equiv 1 - x^2 \equiv 2^{2^{n-1}u}(-1)^{2^{n-2}u} \cdot (x + 1)$, $1 \equiv 2^{2^{n-1}u-1}(-1)^{2^{n-2}u}p \pmod w$, $p \in \langle 2 \rangle$, a contradiction.

Thus we have established that b' is odd so that k is odd and $(a, d) \equiv (2, 1)$ or $(2^{n+2} + 2, 3 \cdot 2^{n+1} + 1) \pmod{2^{n+3}}$.

(iii). We consider $1 + p^a = x^{2kp} + 2p^d$ where $(a, k, d) \equiv (0, 1, 1) \pmod 2$ using the moduli 7, 9 and 13 successively. Observe that $p \equiv 2 \pmod 3$. Also, easy induction arguments establish that $x \equiv 2$ or $4 \pmod 7$ according as n is even or odd. Note that $\mathrm{ord}_7 x = 3$ and $x^{2p} \equiv x \pmod 7$ in either case. Further, $x \equiv -2$ or $4 \pmod 9$ according as n is even or odd for $n \geqq 2$, and $x \equiv 3$ or $9 \pmod{13}$ according as n is even or odd. Thus, it is routine to verify that $(a, k, d) \equiv (2, 5, 1) \pmod 6$.

(iv). *Case* I. $n = 2$, $p = 17$. By (ii), $(a, d) \equiv (2, 1)$ or $(18, 25) \pmod{32}$. Consider the prime $Q_1 = 137$. Clearly $x^{2p} \equiv 2^{Q_1 - 1} \equiv 1 \pmod{Q_1}$ so that $17^a \equiv 2 \cdot 17^d \pmod{Q_1}$. Now $\mathrm{ord}_{Q_1} 17 = 4 \cdot 17$ so that, since $(a, d) \equiv (2, 1) \pmod 4$, $17^{4r+1} \equiv 2 \pmod{Q_1}$ for some r, a contradiction.

Case II. $n = 3$, $p = 257$. Consider the modulus $Q_2 = 98689 = 384p + 1$. One finds that $\mathrm{ord}_{Q_2} p = 64p$ and $\mathrm{ord}_{Q_2} x = 8p$. By (ii), $(a, d) \equiv (2, 1)$ or $(34, 49) \pmod{64}$. Since $x^{2kp} \equiv \pm x^{2p} \equiv \pm 37468 \pmod{Q_2}$, we have the four possibilities given by

$$1 + p^{64A+2} \equiv \pm 37468 + 2p^{64D+1} \pmod{Q_2},$$

and

$$1 + p^{64A+34} \equiv \pm\, 37468 + 2p^{64D+49} \pmod{Q_2},$$

where $0 \leqq A \leqq p - 1$, $0 \leqq D \leqq p - 1$. Thus $1 + (66049)\,(55741)^A \equiv \pm 37468 + (514)\,(55741)^D \pmod{Q_2}$, or $1 + (26836)\,(55741)^A \equiv \pm 37468 + (28403)\,(55741)^D \pmod{Q_2}$. Only two solutions occur and these are $(A, D) \equiv (133, 202), (215, 179) \pmod p$. (These appear in the first congruence with the plus sign taken.) Hence $(a, d) \equiv (8514, 12929)$ or $(13762, 11457) \pmod{64p}$. We now consider equation (1) modulo the prime $Q_3 = 1543 = 6p + 1$. We note that $\mathrm{ord}_{Q_3} x = \mathrm{ord}_{Q_3} p = 3p$. From (iii) and the above results we conclude that $(a, d) \equiv (290, 79)$ or $(398, 406) \pmod{771}$. In each case, since $x^{2kp} \equiv x^p \pmod{Q_3}$, we have a contradiction.

Case III. $n = 4$, $p = 65537$. Consider the prime $Q_4 = 50332417 = 256 \cdot 3p + 1$. We find that $\mathrm{ord}_{Q_4} x^{2p} = 12$, $\mathrm{ord}_{Q_4} p = 128p$. Since $k \equiv 5 \pmod 6$ and $(a, d) \equiv (2, 1)$ or $(66, 97) \pmod{128}$, we have four possibilities as in the previous case. These are given by

$$1 + p^{128A+2} \equiv \pm x^{10p} + 2p^{128D+1} (\text{mod } Q_4),$$

and

$$1 + p^{128A+66} \equiv \pm x^{10p} + 2p^{128D+97} (\text{mod } Q_4),$$

where $0 \leqq A \leqq p - 1, 0 \leqq D \leqq p - 1$. Thus we have:

$$1 + (17928511)^A (16842924) \equiv 287000 23\delta + (17928511)^D \cdot (131074) (\text{mod } Q_4), \tag{7}$$

or

$$1 + (17928511)^A (32053706) \equiv 28700023\delta + (17928511)^D \cdot (26892932) (\text{mod } Q_4) \tag{8}$$

where $\delta = \pm 1$. There are 345 solutions (A, D) (mod p) to congruences (7) and (8). These are listed in Tables 2.1 through 2.4. Finally, we consider the prime $Q_5 = 2359333 = 36p + 1$. Now $\text{ord}_{Q_5} p = 3p$ and $\text{ord}_{Q_5} x = 9p$. Since $(a, d) \equiv (2, 1)$ (mod 3) each (A, D) in Tables 2.1 through 2.4 generates a unique pair (a, d) (mod $3p$). (These are also listed in the tables.) Note that $x^{2kp} \equiv x^{(1+3r)p} \equiv 1380078, 1513046$ or 1825542 (mod Q_5), for $r = 0, 1, 2$. In none of the 345 cases is $1 + p^a - 2p^d \equiv x^{2pk}$ (mod Q_5), so we are finished.

A	D	a	d
1182	7947	151298	34162
1464	49103	187394	59170
2076	46130	69119	71848
2389	352	43646	176131
3539	47696	125309	75685
5545	36083	54392	162109
7088	60811	186359	50443
7639	44098	125813	73900
8870	46404	21233	41383
8986	52435	101618	157981
9296	16938	75761	5344
9682	24758	190706	88786
10787	18187	69998	99679
11091	31661	43373	185926
11938	1552	86252	133120
12706	61162	184556	95371

TABLE 2.1. Solutions (A, D) (mod p) to equation (7) and corresponding pairs (a, d) (mod $3p$), $\delta = 1$.

A	D	a	d
13569	6639	163946	63349
14140	6848	171497	155638
14308	34802	193001	194752
14537	24028	156776	60883
14543	46844	157544	163240
14893	57203	71270	112915
15183	22620	173927	142807
17066	39984	87266	6067
18217	33434	103520	19648
18397	50041	126560	48160
19273	27382	42077	96973
19286	5996	174815	46582
20169	46920	25691	107431
20445	10568	61019	41965
20939	39567	189788	149302
21078	335	142043	108418
22340	40956	172505	130483
22818	14803	168152	59749
23228	49994	89558	173218
24109	12369	71252	10345
25764	6085	152018	123511
26467	62380	176465	54664
27348	48765	158159	146980
28437	12621	100940	42601
29062	22221	115403	91735
29109	7443	186956	166261
29195	37192	66890	172987
29216	43831	69578	39724
29481	56531	37961	26899
30523	43910	105800	180910
31538	23809	170183	32851
32399	57732	83780	115090
32414	32794	85700	3265
32689	24952	186437	179155
34009	11772	158786	130540
34853	24734	4670	85714
34992	12194	153536	53482
35730	4869	51389	33400
40365	39131	54836	159031
40858	5057	52403	123001

TABLE 2.1. Continued.

A	*D*	*a*	*d*
41820	19714	44465	98524
42971	62553	60719	142345
44256	56284	159662	60820
44651	12634	79148	175339
44652	48565	13739	55843
44932	31795	180653	72004
45288	45849	95147	166954
45956	10805	49577	72301
46333	56974	163370	149140
46450	57971	178346	14608
46645	10784	6695	69613
48530	20467	182438	194908
49220	12664	74147	179179
49620	27365	59810	29260
50093	31249	185891	2116
51507	63565	104735	9733
52003	25986	102686	180433
54347	2571	140570	132478
55033	46454	97304	113320
55409	4415	79895	40825
56202	6626	115862	127222
56920	25313	142229	159826
56992	14467	151445	16741
57228	64917	50579	51715
57448	31659	13202	120133
57707	61696	177428	163723
57758	13125	183956	107113
58907	18407	134417	62302
58959	20209	75536	161884
59131	33437	32015	20032
59250	54572	112784	169369
59689	17868	103439	124384
60050	40937	84110	193588
60625	568	26636	7168
60777	27145	111629	66637
61691	18656	97547	94174
62129	30871	153611	150343
62723	2704	33032	83965
63436	36991	189833	147259

TABLE 2.1 Continued.

A	D	a	d
1865	18079	107648	85855
3243	44253	21884	159277
3399	31202	41852	127174
3797	3190	158333	146173
4506	20736	183548	98266
4591	46718	128891	147112
5921	27870	36983	28363
7056	22573	116726	71254
7994	36434	105716	10426
8300	49705	144884	5152
8584	30358	50162	84679
9771	3301	71024	160381
11353	44490	11372	189613
11885	25408	13931	40912
13013	30512	158315	38854
13587	3138	166250	8443
14053	26777	160361	150607
16444	27676	73187	134605
17342	40166	122594	94900
17862	28481	123617	172108
17886	6569	126689	119926
18090	1865	152801	107647
18433	54632	131168	177049
20123	7819	85340	148852
20492	1252	132572	94720
20573	55923	142940	80149
20985	24078	130139	132820
21335	62003	43865	137482
22804	54928	100823	83863
23751	34286	90965	128704
26206	25838	143057	30415
27634	10312	129230	74734
28203	57264	70988	55186
28212	10165	72140	55918
28288	51529	16331	42013
28325	1846	152141	170752
28924	64656	97739	18307
29880	38021	89033	16951
31322	34420	142535	14782

TABLE 2.2. Solutions (A, D) (mod p) to equation (7) and corresponding pairs (a, d) (mod $3p$), $\delta = -1$.

A	*D*	*a*	*d*
31477	12418	31301	147691
31934	5686	24260	72439
31937	9271	24644	138097
31992	44719	162758	153388
32379	25741	15683	83536
32619	33335	46403	6976
32830	41324	7874	46513
33092	29456	172484	100297
33940	8338	149954	18673
34037	49763	96833	143650
35280	62110	190400	20104
35291	58194	60734	174226
35462	17042	82622	84193
36760	25487	117692	182098
37607	15539	160571	88420
37609	62389	29753	55816
38389	60857	129593	187405
38809	39035	183353	146743
38831	9679	120632	190321
39264	1684	110519	150016
40465	35982	2099	83644
40749	13249	103988	57448
41143	42006	88883	68272
41802	18687	42161	32605
41847	18894	47921	59101
43373	39820	112175	116149
43483	54545	191792	165913
43535	58244	132911	49552
45494	2258	187052	157951
47518	43518	118439	65197
47863	40445	162599	130612
48633	32082	130085	174277
50207	10420	3872	88558
50569	21342	115745	175834
51169	2664	192545	144382
52428	8899	26012	90481
53495	7648	31514	126964
53717	18764	59930	107998
54215	13106	123674	170218
54580	38773	39320	178744

TABLE 2.2. Continued.

A	D	a	d
54872	13770	11159	189673
55217	46674	55319	75943
55464	11653	21398	49771
57188	1930	110996	181504
59159	45239	166673	154411
59563	36282	87311	122044
60711	14508	103181	87526
60959	35763	3851	55612
61290	51076	177293	180640
62778	4630	171146	133882
62909	35014	56840	90814
63079	55407	144137	14101
64303	64428	104198	185734
64795	9192	167174	193522
65095	59861	8963	59917

TABLE 2.2. Continued.

A	D	a	d
2998	45089	187199	135307
3100	49881	3644	93313
3569	16084	194750	27202
5717	51105	76472	53374
6021	23495	49847	234829
6265	37588	15542	27160
6333	54619	89783	44407
6369	47781	94391	21124
6715	51323	73142	146815
8908	31302	157235	74533
11740	2770	126509	92509
12074	19442	103724	194878
12352	33357	8234	140962
12355	44536	8618	130060
13148	59767	44585	113518
13435	18997	146858	6844
15755	8051	181670	113107
16107	34341	161189	70303
16188	28812	171557	149035
17070	55067	87842	36214
17374	28918	61217	97066

TABLE 2.3. Solutions (A, D) (mod p) to equation (8) and corresponding pairs (a, d) (mod $3p$), $\delta = 1$.

A	*D*	*a*	*d*
18024	53859	13343	12664
18148	15757	160289	181957
19336	25951	115742	110512
20137	11063	21659	105421
20514	33346	135452	74017
20753	54357	34970	76408
21696	27702	90137	6955
22653	26455	16022	175024
26048	59116	122897	30190
26652	14855	134672	964
26847	25363	159632	35248
27632	34113	129038	41119
28647	34317	193421	67231
28786	9146	145676	56656
29231	63122	137099	84199
29306	57884	146699	3568
29649	33536	125066	32800
30410	27579	91400	187822
31339	44028	79238	130573
31819	61083	140678	150892
32711	55262	189317	61174
34963	50362	149888	89344
36952	16923	11258	3520
37089	60270	94331	46828
37317	9998	123515	165712
39240	47024	173048	186376
41411	36734	123251	48922
41419	50531	189812	45439
41530	63708	7409	93670
43619	33676	12653	116257
44211	16457	22892	9409
45408	21828	176108	41527
46719	62000	147305	137194
47244	47814	17894	25348
48118	6	64229	865
48442	60026	105701	81133
48478	16551	110309	152515
48895	10520	163685	35917
50306	27708	82145	7723
51332	9497	16862	101584

TABLE 2.3. Continued.

A	D	a	d
52006	27599	168671	59308
52880	35212	18395	116254
52965	21831	160349	41911
53013	35519	166493	90013
54960	15702	22487	43843
55014	8939	29399	30160
55076	7138	102872	61780
55163	33320	114008	5152
57679	55177	108371	115831
58110	2475	32465	120286
59404	33683	132560	51616
59544	60481	19406	8299
60008	37965	144335	140953
60229	37198	41549	173851
60323	15997	184655	16066
61041	44694	14411	19210
63200	60423	159689	66412
64338	11872	43205	77899
64482	34084	61637	168481

TABLE 2.3. Continued.

A	D	a	d
74	14828	140612	194119
1140	60227	14912	106861
2176	25149	81983	73393
2985	28352	54461	155692
3620	56680	4667	111604
3727	30601	83900	115879
5153	37848	4280	125977
5320	25334	91193	162610
7037	22019	48821	131512
8517	12068	172724	37450
10660	34747	184880	56734
10763	10800	132527	6220
13281	4270	192683	87898
13589	59245	101033	46702
13803	21094	62888	78649
13929	37664	79016	167962
14797	12654	124583	46921

TABLE 2.4. Solutions (A, D) (mod p) to equation (8) and corresponding pairs (a, d) (mod $3p$), $\delta = -1$.

A	D	a	d
14887	28618	136103	58666
16103	22987	29603	124342
16321	24538	123044	126259
18346	35169	185633	176287
20892	50368	183836	90112
21676	60679	22040	33643
21895	61415	50072	62314
22651	60980	146840	6634
22977	56069	57494	164470
24302	56939	96020	79219
27913	20034	33932	8506
28127	6264	192398	15445
28616	2407	58379	46045
29520	37763	108554	180634
30248	52318	70664	143101
30814	37114	12038	163099
31022	12290	169736	65866
31865	51029	81029	109183
32415	52532	85892	104956
33757	58056	192131	156658
34987	29568	152960	49192
35914	7478	75005	39763
36908	19892	136700	55867
37841	55752	59513	58357
38443	40712	5495	164884
38565	50857	86648	152704
39010	2486	78071	187231
39175	20724	99191	96826
39352	5412	121847	103000
40277	56278	174710	60148
40394	43840	189686	40972
41029	7754	139892	75091
41408	63983	122867	194407
41953	25504	61553	53296
42060	43792	140786	34828
42702	36823	26351	125851
43519	40808	65390	177172
44294	54692	99053	184825
45914	36668	109802	40474
46016	19905	122858	188605

TABLE 2.4. Continued.

A	D	a	d
47388	9395	36326	88528
48200	27638	9188	64300
49946	35803	36065	191902
50542	23196	177890	20020
50678	10238	129761	196432
50681	33448	130145	87073
50961	65454	100448	120547
51689	33018	62558	97570
53663	20576	118619	143419
53914	9491	19673	100816
53972	1634	158171	78175
55426	39564	16598	149014
56291	36648	61781	168988
56397	34970	9812	19741
56424	20439	13268	60346
60158	49623	163535	60289
60288	40801	114638	45202
61291	12543	177485	32713
62864	61804	116681	177643

TABLE. 2.4. Continued.

3. Solution of Equation (1). Here we find all solutions to equation (1) with $p \leqq 499$. We begin by handling the cases that follow immediately from the results of §2. The remaining cases are then handled individually.

LEMMA 3.1. *Equation (1) has solutions* $(a, b, c, d) =$

(i) $(t, 0, 0, t)$, $t \geqq 0$, *when* $p = 13, 29, 37, 41, 43, 53, 61, 73, 89, 97, 101, 103, 109, 113, 137, 139, 149, 151, 157, 163, 173, 181, 193, 197, 199, 211, 229, 233, 241, 269, 277, 281, 293, 313, 317, 337, 349, 353, 373, 379, 389, 397, 401, 409, 421, 433, 439, 449, 457, 461, 487, 491$;

(ii) $(t, 0, 0, t)$, $t \geqq 0$, *and* $(1, 2, 2, 0)$ *when* $p = 7$;

(iii) $(t, 0, 0, t)$, $t \geqq 0$, $(1, 1, 4, 0)$, $(1, 4, 1, 0)$ *and* $(2, 8, 1, 1)$ *when* $p = 17$;

(iv) $(t, 0, 0, t)$, $t \geqq 0$, $(1, 2, 4, 0)$ *and* $(1, 4, 2, 0)$ *when* $p = 19$;

(v) $(t, 0, 0, t)$, $t \geqq 0$, *and* $(1, 4, 4, 0)$ *when* $p = 31$;

(vi) $(t, 0, 0, t)$, $t \geqq 0$, *and* $(1, 6, 6, 0)$ *when* $p = 127$; *and*

(vii) $(t, 0, 0, t)$, $t \geqq 0$, $(1, 1, 8, 0)$, $(1, 8, 1, 0)$ *and* $(2, 16, 1, 1)$ *when* $p = 257$.

PROOF. Part (i) follows immediately from Lemmas 2.2, 2.3, 2.6, 2.7, 2.8 and Theorem 2.9. Parts (ii), (v) and (vi) follow from Theorem 2.5. Parts (iii) and (vii) follow from Theorem 2.10, and part (iv) follows from Theorem 2.9.

LEMMA 3.2. *The solutions to equation (1) when $p = 3$ are $(a, b, c, d) = (t, 0, 0, t)$, $(4, 6, 1, 2)$, $(3, 4, 2, 1)$, $(3, 2, 3, 1)$, $(2, 3, 1, 0)$, $(2, 1, 3, 0)$, $(2, 2, 1, 1)$ and $(1, 1, 1, 0)$.*

PROOF. Let (a, b, c, d) be another solution. Then $a \geqq 5$.

Case I. $b = 1$. Clearly $d = 0$ and $c \geqq 4$. Thus $3^a \equiv 1 \pmod{16}$ so that $a \equiv 0 \pmod 4$. But then $2^c \equiv 0 \pmod 5$, a contradiction.

Case II. $b = 2$. Then consideration modulo 9 yields $d = 1$, $3^{a-1} = 1 + 2^c$, and we have a contradiction as in case I.

Case III. $b \geqq 3$, $c = 1$. If $d = 0$ consideration modulo 16 and 5 gives a contradiction as in case I. Hence $d > 0$. Considerations modulo 8, 9 and 13 give $(a, b, d) \equiv (4, 6, 2) \pmod{(6, 12, 6)}$. If $d = 2$, then $2^b \equiv -17 \pmod{243}$, whence $b \equiv 114 \pmod{162}$. Hence $3^a \equiv 143 \pmod{163}$, so that $a \equiv 94 \pmod{162}$. Since $b \equiv 6 \pmod{36}$ and $a \equiv 13 \pmod{27}$ we now obtain a contradiction modulo 109. Hence we may suppose $d > 2$. But then $2^b \equiv 1 \pmod{27}$, whence $b \equiv 0 \pmod{18}$. Thus $b \equiv 18 \pmod{36}$. Then consideration mod 37 gives another contradiction.

Case IV. $b \geqq 3$, $c = 2$. Here considerations mod 8 and mod 3 imply that a is odd and $d > 0$. If $d = 1$ then $2^b \equiv -11 \pmod{243}$, whence $b \equiv 40 \pmod{162}$. But then consideration mod 163 gives $a \equiv 13 \pmod{162}$, and then consideration mod 13 produces a contradiction. Lastly, suppose $d \geqq 2$ so that $2^b \equiv 1 \pmod 9$, $b \equiv 0 \pmod 6$. Then mod 13 gives a final contradiction.

LEMMA 3.3. *The solutions to equation (1) when $p = 5$ are $(a, b, c, d) = (t, 0, 0, t)$, $t \geqq 0$, $(2, 4, 1, 1)$, $(1, 2, 1, 0)$ and $(1, 1, 2, 0)$.*

PROOF. Let (a, b, c, d) be another solution. Consideration mod 4 gives b or c is 1.

Case I. $d = 0$. Without loss of generality let $c = 1$, $5^a = 2^b + 1$, $a \geqq 2$. Then $2^b \equiv -1 \pmod{25}$, so that $b \equiv 10 \pmod{20}$. Then we have an immediate contradiction mod 11.

Case II. $d = 1$. Here $a \geqq 3$. Since $2^b \equiv 1 \pmod 5$, $b \equiv 0 \pmod 4$, $c = 1$ and $5^a = 2^b + 9$. Thus $2^b \equiv -9 \pmod{125}$, so that $b \equiv 64 \pmod{100}$. Hence $5^a \equiv 88 \pmod{101}$, so that $a \equiv 9 \pmod{25}$. Now we have a contradiction mod 11.

Case III. $d > 1$. Since $2^b \equiv 1 \pmod{25}$, $b \equiv 0 \pmod{20}$ and $c = 1$. Hence $5^a \equiv 2 \cdot 5^d \pmod{11}$, which is impossible.

LEMMA 3.4. *The solutions to equation (1) when $p = 11$ are $(a, b, c, d) = (t, 0, 0, t)$, $t \geqq 0$, $(1, 3, 2, 0)$ and $(1, 2, 3, 0)$.*

PROOF. Let (a, b, c, d) be another solution so that $a > 1$. By Lemma 2.1, b or $c = 2$.

Case I. $d = 0$. Without loss of generality, $c = 2$, $11^a \equiv 2^b + 3$. By inspection $b \geqq 6$ and thus $11^a \equiv 3 \pmod{64}$ and $a \equiv 7 \pmod{16}$. Since $3 \equiv 11^7 \pmod{17}$, we have $2^b \equiv 0 \pmod{17}$, a contradiction.

Case II. $d \geqq 1$. Here $2^b \equiv 1 \pmod{11}$ so that $b \equiv 0 \pmod{10}$. Thus $c = 2$. Then consideration modulo 5 gives $b \equiv 3 \pmod 4$, a contradiction.

LEMMA 3.5. *The solutions to equation (1) when $p = 23$ are $(a, b, c, d) = (t, 0, 0, t)$, $t \geqq 0$, $(1, 3, 4, 0)$ and $(1, 4, 3, 0)$.*

PROOF. Let (a, b, c, d) be another solution.

Case I. $d = 0$. Without loss of generality suppose $b \geqq c$. By Lemma 2.4 $(a, b, c) \equiv (0, 0, 0), (1, 0, 1)$ or $(1, 1, 0) \pmod 2$. Thus consideration mod 16 gives $c = 3$, $b \geqq 4$ and a odd. Hence $b \geqq 5$ so that $23^a \equiv 7 \pmod{32}$, and hence $a \equiv 3 \pmod 4$. Then $2^b \equiv 0 \pmod 5$, a contradiction.

Case II. $d \geqq 1$. Here $2^b \equiv 1 \pmod{23}$, so that $b \equiv 0 \pmod{11}$. Thus $23^a \equiv 2^c 23^d \pmod{89}$, so that $a \equiv 8c + d \pmod{88}$. Hence by Lemma 2.4, $(a, b, c, d) \equiv (0, 0, 0, 0), (1, 0, 0, 1)$ or $(1, 1, 1, 1) \pmod 2$. Now consideration mod 16 gives $c = 3$. Also $2^b \equiv 5 \pmod{11}$, whence $b \equiv 4 \pmod{10}$. This contradicts $b \equiv c \pmod 2$.

LEMMA 3.6. *The solutions to equation (1) when $p = 47$ are $(a, b, c, d) = (t, 0, 0, t)$, $t \geqq 0$, $(1, 5, 4, 0)$ and $(1, 4, 5, 0)$.*

PROOF. Let (a, b, c, d) be another solution.

Case I. $d = 0$. Without loss of generality let $b \geqq c$. By Lemma 2.4 $(a, b, c) \equiv (0, 0, 0), (1, 0, 1)$ or $(1, 1, 0) \pmod 2$. Consideration mod 32 implies that a is odd, $c = 4$ and $b \geqq 5$. Then consideration mod 64 gives $a \equiv 3 \pmod 4$. But then $2^b \equiv 6 \pmod{17}$, a contradiction.

Case II. $d \geqq 1$. Here $2^b \equiv 1 \pmod{47}$ so that $b \equiv 0 \pmod{23}$. Thus $47^a = 2^c 47^d \pmod{178481}$, whence $a \equiv 11(7760)c + d \pmod{178480}$. In particular $a \equiv d \pmod 4$. From Lemma 2.4 we have $(a, b, c, d) \equiv (0, 0, 0, 0), (1, 0, 0, 1)$ or $(1, 1, 1, 1) \pmod 2$. Now considerations mod 64 and mod 17 give a contradiction.

LEMMA 3.7. *Equation (1) has only the trivial solutions $(t, 0, 0, t)$, $t \geqq 0$ when $p = 59, 83, 107, 167, 179, 223, 227, 239, 251, 283, 307, 311, 331, 347, 359, 367, 419, 431, 443, 463, 467, 479$ and 499.*

PROOF. In each case we assume that (a, b, c, d) is another solution and then obtain a contradiction.

($p = 59$). By Lemma 2.1, b or c is 2. When $d = 0$ let $c = 2$. Then $2^b \equiv 56 \pmod{59}$ so that $b \equiv 21 \pmod{58}$. In particular b is odd. Then considerations mod 32 and mod 17 give a contradiction. When $d \geqq 1$, $2^b \equiv 1 \pmod{59}$, so that $b \equiv 0 \pmod{58}$. Thus b is even and $c = 2$. But then $2^b \equiv -2 \pmod{29}$, so that $b \equiv 15 \pmod{28}$, another contradiction.

($p = 83$). By Lemma 2.1, b or c is 2. When $d = 0$, let $c = 2$. Then $2^b \equiv$

80 (mod 83) so that $b \equiv 31$ (mod 82) and b is odd. Now considerations mod 32 and 17 yield a contradiction. When $d \geqq 1$, $2^b \equiv 1$ (mod 83), so that $b \equiv 0$ (mod 82), $c = 2$. Also $2^b \equiv -2$ (mod 41) so that $b \equiv 11$ (mod 20), a contradiction.

($p = 107$). By Lemma 2.1, b or c is 2. When $d = 0$ let $c = 2$. Here considerations mod 16 and 5 give a contradiction. When $d \geqq 1$, $2^b \equiv 1$ (mod 107), so that $b \equiv 0$ (mod 106). Now we get an immediate contradiction mod 53.

($p = 167$). When $d = 0$, considerations mod 16 and mod 7 give a contradiction. When $d \geqq 1$, consideration mod 16 gives $c = 1$ with a, d even, or $c = 3$ with a odd. When $c = 1$ we have a contradiction mod 7, and when $c = 3$ we get a contradiction using the moduli 7, 3 and 83.

($p = 179$). Here consideration mod 89 gives $b \equiv c \equiv 0$ (mod 11) contradicting Lemma 2.1.

($p = 223$). There are no non-trivial solutions in this case by [**4**].

($p = 227$). By Lemma 2.1, b or c is 2. When $d = 0$ considerations modulo 8, 5 and 113 give a contradiction. When $d \geqq 1$ considerations mod 227 and 113 give a contradiction.

($p = 239$). Consideration mod 7 gives $b \equiv c \equiv 0$ (mod 3). Then considerations mod 32 and mod 239 yield a contradiction.

($p = 251$). By Lemma 2.1, b or c is 2. When $d = 0$ let $c = 2$. Then considerations modulo 8, 9 and 7 give a contradiction. When $d > 0$ considerations modulo 251 and 5 give a contradiction.

($p = 283$). Here Lemma 2.1 implies without loss of generality, that $c = 2$. Thus $2^b \equiv 45$ (mod 47), an impossibility.

($p = 307$). Here Lemma 2.1 implies that a is odd and (without loss of generality) $c = 2$. Then considerations mod 17 and mod 307 give a contradiction.

($p = 311$). Here we use the moduli 31 and 16 to obtain a contradiction.

($p = 331$). Here Lemma 2.1 gives $c = 2$, without loss of generality. When $d = 0$ mod 331 gives a contradiction; when $d > 0$ considerations mod 331 and 11 give a contradiction.

($p = 347$). Again Lemma 2.1 implies $c = 2$. When $d = 0$ we obtain a contradiction using mod 16 and mod 5; when $d > 0$ we have a contradiction from the moduli 347 and 173.

($p = 359$). Let $d = 0$. If a is even, we get a contradiction mod 16 and mod 359. When a is odd, considerations mod 16, 3 and 5 give a contradiction. Thus $d > 0$. Then $2^b \equiv 1$ (mod 359) so that $b \equiv 0$ (mod 179). If a is even, mod 16 gives $c = 1$, d even, a contradiction to Lemma 2.4. Similarly, if a is odd we conclude $c = 3$, $2^b \equiv -6$ (mod 179), and $b \equiv 20$ (mod 178). Thus by Lemma 2.4, b and d are even and we have an immediate contradiction modulo 5.

($p = 367$). Here consideration mod 32 implies min $(b, c) = 1$ or 4 when

a is even or odd, respectively. Without loss of generality let $c = \min(b, c)$. When $c = 1$ we have an immediate contradictoin modulo 3. Thus a is odd and $c = 4$. When $d = 0$ we have a contradiction modulo 23. When $d > 0$ considerations mod 367 and mod 61 imply a contradiction.

($p = 419$). Here Lemma 2.1 implies that a is odd and (without loss of generality) $c = 2$. When $d = 0$ we obtain a contradiction modulo 16, 5 and 3. When $d > 0$, considerations mod 419, 3, 7 and 19 give a contradiction.

($p = 431$). When a is even, using mod 32 we find that $\min(b, c) = 1$. Without loss of generality let $c = 1$. Then $2^b \equiv 0 \pmod{5}$, an absurdity. Similarly, when a is odd, mod 32 gives $\min(b, c) = 4$. Let $c = 4$. Then $2^b \equiv -14 \pmod{43}$, another absurdity.

($p = 443$). Here, from Lemma 2.1, c = 2. Considerations mod 13 and mod 17 yield a contradiction.

($p = 463$). Here mod 7 gives $b \equiv c \equiv 0 \pmod{3}$. But then, from mod 32 we have $\min(b, c) = 1$ or 4, a contradiction.

($p = 467$). Here from Lemma 2.1 we may suppose that a is odd and $c = 2$. When $d = 0$, considerations mod 9 and mod 13 imply a contradiction. When $d > 0$, considerations mod 467, 9, 13 and 5 produce an absurdity.

($p = 479$). Here considerations mod 64, 239 and 479 give a contradiction.

($p = 499$). Here Lemma 2.1 implies that a is odd and (without loss of generality) $c = 2$. When $d = 0$ we have a contradiction modulo 5 and 17. When $d > 0$ clearly $b \geqq 5$. Thus we obtain a contradiction from considerations mod 3, 5, 32, 17 and 13.

LEMMA 3.8. *The solutions to equation* (*1*) *other than* $(t, 0, 0, t)$, $t \geqq 0$, *are* $(a, b, c, d) =$

(i) $(1, 6, 2, 0)$ and $(1, 2, 6, 0)$ when $p = 67$,
(ii) $(1, 6, 3, 0)$ and $(1, 3, 6, 0)$ when $p = 71$,
(iii) $(1, 6, 4, 0)$ and $(1, 4, 6, 0)$ when $p = 79$,
(iv) $(1, 7, 2, 0)$ and $(1, 2, 7, 0)$ when $p = 131$,
(v) $(1, 7, 6, 0)$ and $(1, 6, 7, 0)$ when $p = 191$,
(vi) $(1, 8, 3, 0)$ and $(1, 3, 8, 0)$ when $p = 263$,
(vii) $(1, 8, 4, 0)$ and $(1, 4, 8, 0)$ when $p = 271$, and
(ix) $(1, 8, 7, 0)$ and $(1, 7, 8, 0)$ when $p = 383$.

PROOF. In each case suppose that (a, b, c, d) is another solution.

(i). ($p = 67$). Here, by Lemma 2.1, we may suppose that a is odd and $c = 2$. Then mod 3 implies that b is even. When $d = 0$, considerations mod 256 and 257 yield an absurdity. When $d > 0$ considerations mod 67 and 89 yield $b \equiv 0 \pmod{66}$ and $a \equiv 10 + d \pmod{11}$. But then we have a contradiction mod 23.

(ii). ($p = 71$). When $d = 0$, without loss of generality, let $b \geqq c$. By Lemma 2.4, $(a, b, c) \equiv (0, 0, 0), (1, 0, 1)$ or $(1, 1, 0) \pmod 2$. Then consideration mod 16 implies that a is odd, $c = 3$ and $b \geqq 4$. Thus $b \geqq 7$ so that, using the moduli 128 and 17 we have a contradiction. When $d > 0$ we have $2^b \equiv 1 \pmod{71}$, whence $b \equiv 0 \pmod{35}$. Consider the prime $q = 122921$, a divisor of $2^{35} - 1$. Since $71^a \equiv 71^d 2^c \pmod q$ and since $71^{(1756)(27)} \equiv 2 \pmod q$, we have $a \equiv (1756)(27c) + d \pmod{61460}$. In particular, $a \equiv d \pmod 4$. Thus from Lemma 2.4 and the modulus 16 we conclude that a is odd, $b \equiv c \pmod 2$, and, in fact, $c = 3$, so that b is odd. But then we have a contradiction mod 5.

(iii). ($p = 79$). Here using mod 3 we find that b and c are even. When $d = 0$ we conclude that a is odd and $c = 4$ from mod 32. Thus $b \geqq 8$. Now, we obtain our contradiction from considerations mod 256 and 17. When $d > 0$ we have $2^b \equiv 1 \pmod{79}$ so that $b \equiv 0 \pmod{39}$. Thus $b \equiv 0 \pmod{78}$. Consideration mod 32 implies that a is odd and $c = 4$. We then obtain a contradiction using the moduli 79 and 3121. Note that $\mathrm{ord}_{3121} 2 = 156$ and $\mathrm{ord}_{3121} 79 = 4$.

(iv). ($p = 131$). Here by Lemma 2.1 we may suppose that a is odd and $c = 2$. If $d = 0$ we have a contradiction using the moduli 256, 17 and 257. When $d > 0$, $2^b \equiv 1 \pmod{131}$, whence $b \equiv 0 \pmod{130}$. We then have a contradiction mod 5.

(v). ($p = 191$). When a is even considerations modulo 8 and 5 yield a contradiction. When a is odd, using mod 128 we conclude that $\min(b, c) = 6$. When $d = 0$ the moduli 256, 17 and 5 produce an absurdity. When $d > 0$, $2^b \equiv 1 \pmod{191}$, so that $b \equiv 0 \pmod{95}$. Then considerations mod 5 and mod 31 give a contradiction.

(vi). ($p = 263$). When $d = 0$, without loss of generality, let $b \geqq c$. If a is even, mod 16 gives $c = 1$. Thus $2^b \equiv 0 \pmod{11}$, an impossibility. If a is odd, from mod 16, $c = 3$. Clearly $b > 12$. Then considerations mod 2048 and mod 257 give a contradiction. If $d > 0$ then $2^b \equiv 1 \pmod{263}$ so that $b = 0 \pmod{131}$. If a is even, mod 16 gives $c = 1$ and d is even, and we again have a contradiction mod 11. Thus a is odd. Now from mod 16 we conclude that $c = 3$. Consideration mod 131 implies that $b \equiv 8 \pmod{130}$. Hence $b \equiv 0 \pmod{262}$. Thus $263^a \equiv 8 \cdot 263^d \pmod{1049}$, and hence $a \equiv 244 + d \pmod{1048}$. Thus $a \equiv d \pmod 2$, an impossibility by Lemma 2.4.

(vii). ($p = 271$). When $d = 0$, without loss of generality, let $b \geqq c$. Consideration mod 32 gives $c = 1$ or 4. When $c = 1$ we have a contradiction mod 271. When $c = 4$, $271^a \equiv 15 \pmod{512}$ so that $a \equiv 17 \pmod{32}$. We then obtain $2^b \equiv 5 \pmod{97}$ which is impossible. When $d > 0$,

$2^b \equiv 1 \pmod{271}$, whence $b \equiv 0 \pmod{135}$. Also $b \geqq 135$. Hence $52^a \equiv 2^c 52^d \pmod{73}$. Thus $5^{3a} \equiv 5^{8c+3d} \pmod{73}$ so that $3a \equiv 8c + 3d \pmod{72}$. Thus $c \equiv 0 \pmod 3$. But, since $2 \equiv 2^b + 2^c \pmod 3$, we have $c \equiv 0 \pmod 2$. Hence $c \equiv 0 \pmod 6$, $c \geqq 6$. We now have a contradiction mod 32.

(viii). ($p = 383$). When $d = 0$ considerations mod 256, 3, 512 and 5 give a contradiction. When $d > 0$ we have $2^b \equiv 65 \pmod{191}$ so that $b \equiv 8 \pmod{95}$. Also, since $2^b \equiv 1 \pmod{383}$, we have $b \equiv 0 \pmod{191}$, $b \geqq 191$. When a is even mod 256 implies that $c = 1$ and d is even, a contradiction to Lemma 2.4. When a is odd, mod 256 and Lemma 2.4 yield $c = 7$, $b \equiv d \pmod 2$. Then consideration mod 512 gives $(a, b, d) \equiv (1, 1, 1)$ or $(3, 0, 0) \pmod{(4, 2, 2)}$. Then mod 5 gives $(a, b, d) = (1, 3, 3)$ or $(3, 0, 2) \pmod 4$. Then using mod 17, we have $(a, b, d) = (1, 7, 7)$, $(5, 3, 7)$, $(3, 0, 2)$ or $(7, 0, 6) \pmod 8$. Now we obtain contradictions in each case from consideration mod 41.

We now summarize our results in Table 3.1. The table gives the solutions to equation (1) with $p \leqq 499$ other than the trivial solutions $(t, 0, 0, t)$, t an arbitrary integer.

Prime p	*Non-Trivial Solutions to equation (1)*
3	(4, 6, 1, 2), (3, 4, 2, 1), (3, 2, 3, 1), (2, 3, 1, 0), (2, 1, 3, 0), (2, 2, 1, 1), (1, 1, 1, 0)
5	(2, 4, 1, 1), (1, 2, 1, 0), (1, 1, 2, 0)
7	(1, 2, 2, 0)
11	(1, 3, 2, 0), (1, 2, 3, 0)
17	(1, 1, 4, 0), (1, 4, 1, 0), (2, 8, 1, 1)
19	(1, 2, 4, 0), (1, 4, 2, 0)
23	(1, 3, 4, 0), (1, 4, 3, 0)
31	(1, 4, 4, 0)
47	(1, 5, 4, 0), (1, 4, 5, 0)
67	(1, 6, 2, 0), (1, 2, 6, 0)
71	(1, 6, 3, 0), (1, 3, 6, 0)
79	(1, 6, 4, 0), (1, 4, 6, 0)
127	(1, 6, 6, 0)
131	(1, 7, 2, 0), (1, 2, 7, 0)
191	(1, 7, 6, 0), (1, 6, 7, 0)
257	(1, 1, 8, 0), (1, 8, 1, 0), (2, 16, 1, 1)
263	(1, 8, 3, 0), (1, 3, 8, 0)
271	(1, 8, 4, 0), (1, 4, 8, 0)
383	(1, 8, 7, 0), (1, 7, 8, 0)

TABLE 3.1. Non-trivial solutions to equation (1).

ACKNOWLEDGEMENT. The authors would like to thank Gabriel Robbins, Roy E. Rhodes and James N. Foster for their assistance with some of the more horrendous calculations. Mr. Rhodes used a Compupro 8–16 *C* to compute Tables 2.1–2.4.

REFERENCES

1. L. J. Alex, *Diophantine equations related to finite groups*, Comm. in Algebra **4** (1976), 77–100.

2. ———, *The Diophantine equation* $3^a + 5^b = 7^c + 11^d$, The Mathematics Student. **48** (1980), 134–138.

3. ———, *Simple groups and a Diophantine equation*, Pacific J. Math. **104** (1983), 257–262.

4. L. J. Alex and L. L. Foster, *On Diophantine equations of the form* $1 + 2^a = p^b q^c + 2^d p^e q^f$, Rocky Mountain J. of Math **13** (1983), 321–331.

5. J. L. Brenner and L. L. Foster, *Exponential Diophantine equations*, Pacific J. Math. **101** (1982), 263–301.

6. E. Dubois and G. Rhin, *Sur la majoration de formes linéaires a coefficients algebriques réels et p-adiques: Demonstration d'une conjecture de K. Mahler*, C. R. Acad. Sci. Paris, A **282** (1876), 1211–1214.

7. H. P. Schlickewei, *Uber die diophantische Gleichung* $x_1 + x_2 + \ldots + x_n = 0$, Acta Arith. **33** (1977), 183–185.

STATE UNIVERSITY COLLEGE, ONEONTA, NEW YORK 13820

CALIFORNIA STATE UNIVERSITY, NORTHRIDGE, CALIFORNIA 91330