Internat. J. Math. & Math. Sci.
Vol. 22, No. 3 (1999) 459–462
S 0161-1712(99)22459-3

THE DIOPHANTINE EQUATION $x^2 + 2^k = y^n$, II

J. H. E. COHN

(Received 19 June 1998)

ABSTRACT. New results regarding the full solution of the diophantine equation $x^2+2^k = y^n$ in positive integers are obtained. These support a previous conjecture, without providing a complete proof.

Keywords and phrases. Diophantine equation.

1991 Mathematics Subject Classification. 11D41.

The first paper in the series [2] considered the diophantine equation $x^2 + 2^k = y^n$, where $n \geq 3$ and k was supposed odd, and demonstrated that there were exactly three families of solutions. The same problem with k even appears to be of rather greater difficulty, and was considered by Arif and Abu Muriefah [1]. They made the following conjecture:

CONJECTURE. *If $k = 2m$, the diophantine equation $x^2 + 2^k = y^n$ has precisely two families of solutions, given by $x = 2^m$ for all m and by $n = 3$, $x = 11.2^{3M}$ if $m = 3M+1$.*

This conjecture seems entirely plausible, but the authors of [1] could not prove it; indeed, there remained 30 cases with $m < 100$ for which they could not exclude other solutions. It is the object of this note to derive further results to remove all those open cases, but the goal of proving the conjecture remains infuriatingly just out of reach.

As demonstrated in [1], the conjecture would follow if it could be demonstrated that the equation

$$-1 = \sum_{r=0}^{1/2(p-1)} \binom{p}{2r+1} a^{p-2r-1}(-2^{2m})^r \tag{1}$$

had no solution in which $n = p \equiv 7 (\mathrm{mod}\, 8)$, an odd prime, a is an odd integer divisible by 3 and m is divisible by an odd power of 3. It is also shown there that if m is even but not divisible by 5, then (1) has no solution and that if $(m, 7) = 1$, then it suffices to consider $p \equiv 7 (\mathrm{mod}\, 24)$.

DEFINITION. For each prime q, define $\lambda = \lambda(q)$ and $\mu = \mu(q)$ by
(a) λ is the least positive integer such that $2^\lambda \equiv 1 (\mathrm{mod}\, q)$;
(b) $2^\lambda = 1 + \mu q$.
Then an *ordinary* prime q is one with $\mu \not\equiv 0 (\mathrm{mod}\, q)$.

REMARK 1. Of course $\lambda \mid (q-1)$. All primes $< 3.10^9$ are known to be ordinary except 1093 and 3511.

LEMMA 1. *For any solution of (1), every prime q dividing $a+2^m$ and $|a-2^m|$ satisfies $q \equiv \pm 1 \pmod 8$ and $\lambda \equiv 1 \pmod 2$. In particular, $a \equiv \pm 1 \pmod 8$. For (1) gives modulo $a^2 - 2^{2m}$,*

$$\begin{aligned} -1 &\equiv a^{p-1} \sum_{r=0}^{1/2(p-1)} \binom{p}{2r+1} (-1)^r = a^{p-1} \frac{(1+i)^p - (1-i)^p}{2i} \\ &= a^{p-1} \cdot 2^{p/2} \sin \frac{p\pi}{4} = -(2a^2)^{1/2(p-1)}, \end{aligned} \tag{2}$$

since $p \equiv 7 \pmod 8$. Hence, 2 is a quadratic residue modulo q, i.e., $q \equiv \pm 1 \pmod 8$. Also, $1 \equiv (2^{2m+1})^{1/2(p-1)} \equiv 2^{(2m+1)1/2(p-1)} \pmod q$, whence, $\lambda | (2m+1)1/2(p-1)$ and so λ must be odd.

REMARK 2. Of course all primes $\equiv 7 \pmod 8$ have odd λ, but this result eliminates many primes $\equiv 1 \pmod 8$ as possible divisors of $a \pm 2^m$, e.g., 17, 41, 97 but not, e.g., 73, 89. It is actually surprising how *few* primes $\equiv 1 \pmod 8$ survive this test; there are only 15 such below 3,000.

COROLLARY 1. *There is no solution unless $p \equiv 15 \pmod{16}$.*

PROOF. For $a \equiv \pm 1 \pmod 8$, $a^2 \equiv 1 \pmod{16}$ and then (1) gives $-1 \equiv pa^{p-1} \equiv p \pmod{16}$. □

LEMMA 2. *If $q|a$ then if $2^\rho \| \lambda$, $2^{\rho-1} | m$.*

PROOF. For $2^{m(p-1)} \equiv 1 \pmod q$ and so $\lambda | m(p-1)$, whence the result since $2 \| (p-1)$. □

THEOREM 1. *For any solution of (1), if $q \neq p$ is an ordinary prime dividing a, then also $q|m$. In fact, if $q^\alpha \| a$, then $m \equiv 2\lambda\mu\nu p q^{2\alpha-1} \pmod{q^{2\alpha}}$, where $(\nu|q) = 1$.*

PROOF. We have from (1)

$$2^{m(p-1)} - 1 = a^2 \left\{ \binom{p}{2} 2^{m(p-3)} - a^2 \binom{p}{4} 2^{m(p-5)} + \cdots \right\}, \tag{3}$$

and so $q^{2\alpha} | 2^{m(p-1)} - 1$. Since q is an ordinary prime, $q^{2\alpha-1} | m(p-1)$.

First, suppose that $q \nmid (p-1)$. Then we find that the second factor on the right-hand side of (3) is not divisible by q since $q \neq p$, and so $q^{2\alpha} \| 2^{m(p-1)} - 1$. Thus, since q is an ordinary prime, $q^{2\alpha-1} \| m(p-1)$, and so $q^{2\alpha-1} \| m$. Now, since $2^\lambda = 1 + \mu q$, we find that $2^{\lambda q^{2\alpha-1}} \equiv 1 + \mu q^{2\alpha} \pmod{q^{2\alpha+1}}$, and then if $t = m(p-1)/\lambda q^{2\alpha-1}$, $2^{m(p-1)} - 1 \equiv (1+\mu q^{2\alpha})^t - 1 \equiv \mu t q^{2\alpha} \pmod{q^{2\alpha+1}}$, whereas modulo $q^{2\alpha+1}$, the right-hand side of (3), is congruent to $\nu q^{2\alpha} \binom{p}{2}$, where ν is a quadratic residue modulo q. Thus, $m(p-1)\mu/\lambda q^{2\alpha-1} \equiv \nu p(p-1)/2 \pmod q$ and the result follows as $q \nmid (p-1)$.

Secondly, if $q|(p-1)$, suppose that $q^\kappa \| (p-1)$ with $p = 1 + rq^\kappa$. Then the second factor on the right-hand side of (3) is congruent to $rq^\kappa \cdot 2^{m(p-3)-1}$ modulo $q^{\kappa+1}$, whereas the left-hand side $\equiv \mu q^{2\alpha+\kappa} \cdot (m(p-1))/(\lambda q^{2\alpha+\kappa-1}) \equiv \mu q^{2\alpha+\kappa} \cdot (mr)/(\lambda q^{2\alpha-1}) \pmod{q^{2\alpha+\kappa+1}}$, and the result follows as before. □

COROLLARY 2. *There can be no solution unless $m \equiv 3^{2\alpha-1} p \pmod{3^{2\alpha}}$, $\alpha \geq 1$.*

PROOF. For $3|a$, and so with $q = 3$, $\lambda = 2$, $\mu = 1$, $\nu = 1$. □

THEOREM 2. *Solutions of (1) are possible only if either*

$$m = 3^{2\alpha-1}(24K+13) \qquad \textit{and} \qquad p \equiv 127 (\mathrm{mod}\, 144) \tag{4}$$

or

$$m \equiv 0 (\mathrm{mod}\, 1020) \qquad \textit{and} \qquad 5|a \quad \textit{and} \quad 17|a. \tag{5}$$

PROOF. (a) If $m \equiv 1 (\mathrm{mod}\, 4)$, then $2^{2m} \equiv 4 \equiv -8^2 (\mathrm{mod}\, 17)$ and then (1) gives $-1 \equiv ((a+8)^p - (a-8)^p/(16)) (\mathrm{mod}\, 17)$, or $(a+8)^{15} - (a-8)^{15} \equiv 1 (\mathrm{mod}\, 17)$ in view of Corollary 1. Now, neither $a \equiv \pm 8 (\mathrm{mod}\, 17)$ satisfy this, whereas, for other values of a, we should obtain $(a^2-8^2) \equiv (a-8)(a+8)^{16} - (a+8)(a-8)^{16} \equiv 1 (\mathrm{mod}\, 17)$ or $a^2 \equiv -3 (\mathrm{mod}\, 17)$ which is impossible.

(b) If $m \equiv 0 (\mathrm{mod}\, 4)$, then $2^{2m} \equiv 1 \equiv -4^2 (\mathrm{mod}\, 17)$ and then (1) gives $-1 \equiv ((a+4)^p - (a-4)^p)/(8) \equiv ((a+4)^{15} - (a-4)^{15})/(8) (\mathrm{mod}\, 17)$. Here, neither $a \equiv \pm 4 (\mathrm{mod}\, 17)$ satisfy this, whereas, for other values of a, we require $-8(a^2-4^2) \equiv (a-4)(a+4)^{16} - (a+4)(a-4)^{16} \equiv -8 (\mathrm{mod}\, 17)$ or $17|a$.

Similarly, $2^{2m} \equiv 1 \equiv -2^2 (\mathrm{mod}\, 5)$ and then (1) gives $-1 \equiv ((a+2)^3 - (a-2)^3)/(4) (\mathrm{mod}\, 5)$, whence, $5|a$. Thus, in this case, m must be divisible by 3, 5, and 17 as well as 4.

(c) If $m = 6 (\mathrm{mod}\, 8)$, then $m \equiv 6 (\mathrm{mod}\, 24)$ and since $\lambda(97) = 48$, we find that $2^{2m} \equiv 22 \equiv -47^2 (\mathrm{mod}\, 97)$ and so, similarly, we find that we must have $-1 \equiv ((a+47)^p - (a-47)^p)/(94) (\mathrm{mod}\, 97)$ and a simple calculation shows that this cannot occur for any $p \equiv 15 (\mathrm{mod}\, 16)$, and so this case cannot arise.

(d) If $m \equiv 2 (\mathrm{mod}\, 8)$, then $m \equiv 18 (\mathrm{mod}\, 24)$ and now $2^{2m} \equiv -33^2 (\mathrm{mod}\, 97)$. We find that this can occur for $p \equiv 15 (\mathrm{mod}\, 16)$ only if $p \equiv 31 (\mathrm{mod}\, 96)$ and, in particular, only if $p \equiv 1 (\mathrm{mod}\, 3)$.

Similarly, we find that $2^{2m} \equiv \pm 9 (\mathrm{mod}\, 193)$, and then this can occur for $p \equiv 15 (\mathrm{mod}\, 16)$ only if $p \equiv 2 (\mathrm{mod}\, 3)$. Thus, this case is impossible.

(e) If $m \equiv 3 (\mathrm{mod}\, 4)$, i.e., $m \equiv 3 (\mathrm{mod}\, 12)$, then $2^{2m} \equiv -1 (\mathrm{mod}\, 13)$ and, as above, this yields, from (1), $(a+1)^p - (a-1)^p \equiv -2 (\mathrm{mod}\, 13)$ which is impossible if $p \equiv 2 (\mathrm{mod}\, 3)$, i.e., $p \equiv 11 (\mathrm{mod}\, 12)$ since again neither $a \equiv \pm 1 (\mathrm{mod}\, 13)$ satisfy this, whereas, for other values of a, we should obtain $-2(a^2-1) \equiv (a-1)(a+1)^{12} - (a+1)(a-1)^{12} \equiv -2 (\mathrm{mod}\, 13)$ which is impossible.

So, we are left with $p \equiv 31 (\mathrm{mod}\, 48)$, $m \equiv 3 (\mathrm{mod}\, 12)$, i.e., $m \equiv 3, 15, 27, 39, 51$, or $63 (\mathrm{mod}\, 72)$. Of these values, 15 and 51 can be dismissed in view of the corollary to Theorem 1, 3 and 27 are impossible modulo 577 by a calculation similar to those employed above since $2^{144} \equiv 1 (\mathrm{mod}\, 577)$. This leaves just $m \equiv 39$ or $63 (\mathrm{mod}\, 72)$, both of which are $\equiv 7 (\mathrm{mod}\, 8)$, and modulo 73 we find that either of them requires $p \equiv 1 (\mathrm{mod}\, 9)$. Thus, in view of the corollary to Theorem 1, we must have $m = 3^{2\alpha-1}(24K+13)$ with $p \equiv 127 (\mathrm{mod}\, 144)$. □

LEMMA 3. *A solution of (1) can occur only if either*

$$p \equiv 1 (\mathrm{mod}\, 9) \tag{6}$$

or

$$p \equiv 4 \text{ or } 7 (\mathrm{mod}\, 9),\ 73 \mid a,\ 73 \mid m; \tag{7}$$

or

$$p \equiv 2 (\mathrm{mod}\, 3),\ 73 \mid a,\ 73 \mid m,\ 9 \mid a,\ 27 \mid m. \tag{8}$$

PROOF. Since $2^9 \equiv 1 (\mathrm{mod}\, 73)$ and $3|m$, it follows that $2^m \equiv 1$ or 8 or $64 (\mathrm{mod}\, 73)$ and then we find as above that *either* $73|a$ *or* $p \equiv 55 (\mathrm{mod}\, 72)$. The latter gives the first case. Since 73 is an ordinary prime, by Theorem 1, the former gives $73|m$, and since $\lambda(73) = 9$, we see, as in Lemma 2, that $9|m(p-1)$, and so unless $p \equiv 1 (\mathrm{mod}\, 3)$, $9|m$ and then the result follows by Theorem 1 and its corollary. □

Using this, we see that the only values of m under 1000 that are still open for odd x are 39, 111, 183, 255, 327, 351, 399, 471, 543, 615, 687, ,759, 831, 903, and 975, for all of which the only possible p satisfy $p \equiv 127 (\mathrm{mod}\, 144)$. The third case of Lemma 3 is most unlikely to occur for it would require m to be even, and then it can be shown that m would have to be divisible by $2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 37 \cdot 73 \cdot 241 \cdot 433$.

Finally to prove that there are no solutions other than those of the conjecture with $m < 100$, it merely remains to check that (1) has no solutions with $m = 39$. This is accomplished by a calculation using the methods of [3]. We omit the details.

REFERENCES

[1] S. A. Arif and F. S. Abu Muriefah, *On the diophantine equation* $x^2 + 2^k = y^n$, Internat. J. Math. Math. Sci. **20** (1997), no. 2, 299–304. CMP 97 11. Zbl 881.11038.

[2] J. H. E. Cohn, *The diophantine equation* $x^2 + 2^k = y^n$, Arch. Math. (Basel) **59** (1992), no. 4, 341–344. MR 93f:11030. Zbl 770.11019.

[3] ———, *The diophantine equation* $x^2 + C = y^n$, Acta Arith. **65** (1993), no. 4, 367–381. MR 94k:11037. Zbl 795.11016.

COHN: DEPARTMENT OF MATHEMATICS, ROYAL HOLLOWAY UNIVERSITY OF LONDON, EGHAM, SURREY TW20 0EX, ENGLAND

E-mail address: J.Cohn@rhbnc.ac.uk