ON THE DIOPHANTINE EQUATION  
\[ x^2 + 2^k = y^n \]

S. AKHTAR ARIF and FADWA S. ABU MURIEFAH  
Department of Mathematics  
Girls College of Education  
Al-Riyadh, SAUDI ARABIA  

(Received June 21, 1995 and in revised form September 29, 1995)

ABSTRACT. By factorizing the equation \( x^2 + 2^k = y^n \), \( n \geq 3 \), \( k \)-even, in the field \( \mathbb{Q}(i) \), various theorems regarding the solutions of this equation in rational integers are proved. A conjecture regarding the solutions of this equation has been put forward and proved to be true for a large class of values of \( k \) and \( n \).

KEY WORDS AND PHRASES: Diophantine equation, primitive root and the order of an integer  

1. INTRODUCTION

In his recent paper Cohn [1] has given a complete solution of the equation \( x^2 + 2^k = y^n \) when \( k \) is an odd integer and \( n \geq 3 \). He proved that when \( k \) is an odd integer there are just three families of solutions. This equation is a special case of the equation \( ax^2 + bx + c = dy^n \), where \( a, b, c \) and \( d \) are integers, \( a \neq 0, b^2 - 4ac \neq 0, d \neq 0 \), which has only a finite number of solutions in integers \( x \) and \( y \) when \( n \geq 3 \), see [2].

The first result regarding the title equation for general \( n \) is due to Lebesgue [3] who proved that when \( k = 0 \) the equation has no solution in positive integers \( x, y \) and \( n \geq 3 \), and when \( k = 2 \), Nagell [4] proved that the equation has the only solutions \( x = 2, y = 2, n = 3 \) and \( x = 11, y = 5, n = 3 \).

In this paper we prove some results regarding the equation \( x^2 + 2^k = y^n \), where \( k \) is even, say \( k = 2m \) and since the results are known for \( m = 0, 1 \), we shall assume that \( m > 1 \) The various results proved in this paper seem to suggest the

CONJECTURE. The diophantine equation  
\[ x^2 + 2^{2m} = y^n, \quad n \geq 3, \quad m > 1 \]  
has two families of solutions given by \( x = 2^m, y^n = 2^{2m+1} \), and by \( m = 3M + 1, n = 3, x = 11 \cdot 2^{3M}, y = 5 \cdot 2^{2M} \).

In this paper we are able to prove the above conjecture for all values of \( m \) when \( n = 3, 7 \) and when \( n \) has a prime divisor \( p \neq 7 \pmod{8} \), but we are unable to prove that if \( m = 3^{2k+1} \cdot m', (m', 3) = 1 \), and all prime divisors of \( n \) are congruent to 7 modulo 8, then equation (1.1) has no solution in \( x \) odd integer  

In the end we have verified that the conjecture is correct for all \( m < 100 \) except possibly for 30 values of \( m \) The values \( m = 2, 3 \) are solved in [5].
2. CASE WHEN \( n \) IS AN EVEN INTEGER

We first consider the case when \( n \) is an even integer. We prove the following

**THEOREM 1.** If \( n \) is even, then the diophantine equation (1.1) has no solution in integers \( x \) and \( y \)

**PROOF.** Let \( n = 2r \), \( r \geq 2 \), then \( x^2 + 2^m y^2 = y^2 \). If \( x \) is odd, then also \( y \) is odd. By factorization \((y' + x)(y' - x) = 2^r\), we get \( y' + x = 2^a \), \( y' - x = 2^b \), where \( a \) and \( b \) have the same parity and \( a > b \geq 1 \). Thus \( y' = 2^{a-1}(2^{b-r} + 1) \) and then \( y' = x^2 + 1 \) where \( x_1 = 2^{a-b} \), yielding no solution for \( r \geq 3 \) [3] and if \( r = 2 \) it is easy to check that there is no solution. If \( x \) is even then writing \( x = 2^a X \), \( y = 2^b Y \), where \( a > 0 \), \( b > 0 \) and both \( X \) and \( Y \) are odd. Then \( 2^{a+1} x^2 + 2^m = 2^{2b+1} Y^2 \). If \( a = m \), we get \( 2^{a+1}(X^2 + 1) = 2^{2b+1} Y^2 \). Since \( X \) is odd let \( X^2 = 8T + 1 \) then

\[
2^{a+1}(4T + 1) = 2^{2b+1} Y^2 \]

which obviously is not valid.

If \( a \neq m \), then \( 2rb = \text{min}(2a, 2m) \). If \( a < m \), then \( 2rb = 2a \), and we get \( X^2 + 2^{(m-a)} = Y^2 \) which is not soluble for \( X \) and \( Y \) odd as we proved in the first part of this theorem, and if \( a > m \) then \( 2rb = 2m \) and we obtain \((2^{a-m} X^2 + 1) = Y^2 \) which has no solutions [3].

3. CASE WHEN \( n \) IS AN ODD INTEGER

Now we proceed to consider the case where \( n \) is an odd integer.

We first prove that it is sufficient to consider \( x \) odd. Because if \( x \) is even, then also \( y \) must be even and if \( x = 2^a X \), \( y = 2^b Y \) where both \( X \) and \( Y \) are odd, we obtain from (1.1) \( 2^{2u} x^2 + 2^m = 2^{2m} y^2 \), and therefore of the three powers of 2, \( 2u, 2m \) and \( 2n \), which occur here, two must be equal and the third is greater. There are thus three cases:

**Case a:** \( 2u > 2m = 2n \); then \((2^{u-m} X^2 + 1) = Y^2 \) and this has no solution by [3].

**Case b:** \( 2m > 2u = 2n \), then \( X^2 + 1 = 2^{m-2u} Y^2 \). Here modulo 8 we see that \( X^2 + 1 = 2^2 Y^2 \) and this equation has been proved by C. Størmer to have no solution except \( X = Y = 1 \), so \( x = 2^m \).

**Case c:** \( 2m > 2u = 2n \), then \( X^2 + (2^{m-u} Y^2 = Y^2 \), and the problem is reduced to the one with \( X \) odd.

**THEOREM 2.** If \( n \) is an odd integer, the diophantine equation (1.1) has no solution in odd integer \( x \) if \( m = 3^{2k} m' \), where \( k \geq 0 \), \((m', 3) = 1 \).

**PROOF.** It is sufficient to consider \( n = p \), an odd prime. The field \( Q(\sqrt{-1}) \) has unique prime factorization and so we may write equation (1.1) as

\[
(x + 2^{m} \sqrt{-1})(x - 2^{m} \sqrt{-1}) = y^2
\]

where the factors on the left hand side have no common factor. Thus for some rational integers \( a \) and \( b \)

\[
x + 2^{m} \sqrt{-1} = (a + b \sqrt{-1})^p
\]

(3.1)

so that \( y = a^2 + b^2 \) and exactly one of \( a \) and \( b \) is even and the other is odd. From (3.1), we have

\[
2^m = b \left\{ 1/2^{(p-1)} \sum_{r=0}^{p-1} \binom{p}{2r+1} a^{p-2r-1} (-b^2)^r \right\}
\]

the case when \( a \) is even and \( b \) is odd can be easily eliminated. Hence \( a \) is odd and \( b \) is even. Since the term in brackets is odd, we get \( b = \pm 2^m \) and

\[
\pm 1 = \frac{p}{3} a^{p-1} - \binom{p}{3} b^2 a^{p-3} + ... + (-1)^{p-1} b^p-1.
\]

(3.2)

By Lemma 5 in [5] the plus sign is impossible. Since \( m > 1 \), by Lemma 4 in [5] the minus sign implies that \( p \equiv 7 \pmod{8} \) and \( 2^{3m} \equiv 1 \pmod{9} \) which implies that \( 3 | m \). So
ON THE DIOPHANTINE EQUATION \( z^2 + 2^m y^3 = \phi(n) \)

\[-1 = \sum_{r=0}^{\frac{\phi(n)}{2}} \left( \frac{p}{2r+1} \right) a^{2r-2} (-2^m)^{-r}. \quad (3.3)\]

Now we consider the two cases \(3|a\) and \((3, a) = 1\) separately. If \((a, 3) = 1\), then from (3.3) we get

\[-1 \equiv \left( \frac{p}{1} \right) - \left( \frac{p}{3} \right) + \left( \frac{p}{5} \right) - \ldots - \left( \frac{p}{p} \right) \pmod{3},\]

which can be written as

\[-1 \equiv \frac{(1 + i)^p - (1 - i)^p}{2i} \pmod{3},\]

but since \(p \equiv 7 \pmod{8}\), we find that \(\frac{(1+i)^p - (1-i)^p}{2i} \equiv 1 \pmod{3}\) which is a contradiction. So \(3|a\), say \(a = 3^S a'\), where \((a', 3) = 1\) and \(S \geq 1\). Now let \(p = 1 + 2.3^S N\), where \((N, 2) = (N, 3) = 1\) and \(\delta \geq 0\). We can rewrite (3.3) as

\[2^{m(p-1)} - 1 = \sum_{r=1}^{\frac{\phi(n)}{2}} (-1)^{\frac{p-1}{2}} \left( \frac{p}{p-2r} \right) a^{2r} (-2^m)^{-2r-1}.\]

The general term in the right hand side is

\[\left( \frac{p}{p-2r} \right) a^{2r} (-2^m)^{-2r-1} = \left( \frac{p}{2r} \right) a^{2r} (-2^m)^{-2r-1} \equiv \frac{\phi(3^S + e)}{\phi(3^S - 2k - 1)} \pmod{3},\]

Since \(3^{2r-2} \geq r(2r - 1)\), for \(r \geq 1\), this right hand side is divisible by at least \(3^{2S+\delta}\), that is

\[2^{m(p-1)} - 1 \equiv 1 \pmod{3^{2S+\delta}}.\]

Since \(2\) is a primitive root of \(3^{2S+\delta}\), \(\phi(3^{2S+\delta}) | m(p-1)\), that is \(3^{2S-2k-1}|m'N\). But \((m', 3) = (N, 3) = 1\), so \(2S - 2k - 1 = 0\), which is impossible.

**Corollary 1.** If \((3, m) = 1\), then the diophantine equation (1.1) has no solution in \(z\) odd.

**Corollary 2.** The diophantine equation (1.1) has no solution in \(z\) odd integer if \(n\) has a prime divisor \(p \equiv 7 \pmod{8}\).

From Corollary 2 and Case b in Section 3, we can deduce the following theorem:

**Theorem 3.** The equation \(x^2 + 2^m y^3 = \phi(m)\) has a solution only if \(m \equiv 1 \pmod{3}\) and if this condition is satisfied it has exactly two solutions given by

\[x = 2^m, \quad y = 2^{3m} \quad \text{and} \quad x = 11.2^{m-1}, \quad y = 5.2^{3m-1}.\]

**Proof.** From Corollary 2 it is sufficient to consider \(x\) even. From Case b we get \(x = 2^m\) as a solution, and Case c gives \(X^2 + 2^{(m-u)} = \phi^3\). If \(m - u = 0\), then there is no solution [3], and if \(m - u = 1\), then we get \(X = 11, Y = 5\) [4], so \(x = 11.2^u = 11.2^{m-1}\) and \(y = 5.2^u = 5.2^{3m-1}\) is a solution.

**Theorem 5.** The diophantine equation \(x^2 + 2^m y^3 = \phi^7\) has a solution only if \(m \equiv 3 \pmod{7}\) and the unique solution is given by \(x = 2^m\) and \(y = 2^{3m+1}\).

**Proof.** If \(x\) is odd, then by using the same method as in [6] we can prove that the equation has no solution. If \(x\) is even we get \(x = 2^m\), \(y = 2^{3m+1}\) as the unique solution.

From the above three theorems we deduce that
THEOREM 6. The diophantine equation (1.1), where \( n \) has no prime divisor \( p \equiv 7 \pmod{8} \) greater than 7 and \( n \mid 2m + 1 \) has a unique solution given by \( x = 2^m \) and \( y = 2^{k \equiv 1} \) if \((3, n) = 1\) And if \( 3 \mid n \) it has exactly one additional solution \( x = 11.2^m \) and \( y = 5.2^{k \equiv 1} \)

NOTE We consider two solutions of the equation (1.1) different if they have different values of \( x \).

THEOREM 7. The diophantine equation \( x^2 + 2^{2m} = y^p \) for given \( m > 0 \) and prime \( p \) has at most one solution with \( x \) odd.

PROOF. We know that the solution is \( y = a^2 + 2^{2m} \) where \( a \) is odd and

\[-1 = \sum_{r=0}^{2^m-1} \left( \frac{p}{2^r + 1} \right) a^{p-2r-1} \left( -2^{2m} \right)^r,
\]

if two different solutions were to arise from odd \( a_1 > a > 0 \), we should obtain

\[0 = \sum_{r=0}^{2^m-1} \left( \frac{p}{2^r + 1} \right) \frac{a_1^{p-2r-1} - a^{p-2r-1}}{a_1^2 - a^2} \left( -2^{2m} \right)^r \equiv p \frac{a_1^{p-1} - a^{p-1}}{a_1^2 - a^2} \pmod{2}. \tag{3.4}\]

Since \( p \equiv 3 \pmod{4} \) the number

\[\frac{a_1^{p-1} - a^{p-1}}{a_1^2 - a^2} = a_1^{p-3} + a_1^{p-5} a^2 + \ldots + a^{p-3}\]

is odd, so (3.4) is impossible.

We need the following lemma to prove the next theorem.

LEMMA (Cohn [5]) If \( q \) is any odd prime that divides \( a \), satisfying (3.3), then

\[2^{m(q - 1)} \equiv 1 \pmod{q^2}.
\]

THEOREM 8. If \( m \) is even and \( (5, m) = 1 \), then the diophantine equation (1.1) has no solution in \( x \) odd.

PROOF. First suppose that \( 5 \mid a \) in (3.3), then by the last lemma \( 2^{8m} \equiv 1 \pmod{25} \) But \( \text{ord}(2) \pmod{25} \) is equal to 20, so \( 20 \mid 8m \), hence \( 5 \mid m \), and so if \((5, m) = 1 \), then \((a, 5) = 1\). Since \( m \) is even so \( 2^{2m} \equiv 1 \pmod{5} \) If \( a^2 \equiv 1 \pmod{5} \) then from (3.3)

\[-1 \equiv \left( \frac{p}{1} \right) - \left( \frac{p}{3} \right) + \left( \frac{p}{5} \right) - \ldots - \left( \frac{p}{p} \right) \pmod{5} \]
\[-\equiv \left( 1+i \right)^p - \left( 1-i \right)^p \equiv -3 \pmod{5} \]

which is impossible.

If \( a^2 \equiv -1 \pmod{5} \), then from (3.3)

\[-1 \equiv - \left( \frac{p}{1} \right) - \left( \frac{p}{3} \right) - \left( \frac{p}{5} \right) - \ldots - \left( \frac{p}{p} \right) \pmod{5}.
\]

So, \( 1 \equiv 2^{p-1} \pmod{5} \) which is impossible since \( p \equiv 7 \pmod{8} \), and the theorem is proved.

NOTE. We can easily prove that: If \( m \) is odd, then equation (1.1) may have a solution in \( x \) odd only if \( a^2 \equiv 1 \pmod{5} \). Because if we suppose \( 5 \mid a \), then from equation (3.3) we get

\[2^{m(p-1)} \equiv 1 \pmod{25}.
\]

Hence \( 20 \mid m (p - 1) \), showing thereby that \( m \) is even, and if we suppose that \( a^2 \equiv -1 (\pmod{5}) \) then for \( m \) odd \( 2^{2m} \equiv -1 (\pmod{5}) \), so (3.3) gives
ON THE DIOPHANTINE EQUATION \( x^2 + 2^m = y^n \)

\[-1 \equiv -\left( \frac{p}{1} \right) + \left( \frac{p}{3} \right) - \ldots - \left( \frac{p}{p} \right) \quad \text{(mod 5)}\]

like before \( 1 \equiv -3 \text{(mod 5)} \) which is not true.

**Theorem 9.** The diophantine equation \( x^2 + 2^{2m} = y^n \), \( m > 1 \), \( (m, 7) = 1 \) may have a solution in \( x \) odd only if \( p \equiv 7 \text{(mod 24)} \).

**Proof.** Since \( 3|m, 2^{2m} \equiv 1 \text{(mod 7)} \) Now \( (a \pm i)^6 \equiv a^2 + 1 \text{(mod 7)} \), so if \( p \equiv 7 + 8k \) and by using (3.3) we have

\[-1 \equiv \frac{(a+i)^p - (a-i)^p}{2i} \quad \text{(mod 7)}
\]

\[\equiv \frac{(a^2 + 1)^k \cdot (a+i)^7 - (a-i)^7}{2i} \quad \text{(mod 7)}.\]

So \( (a^2 + 1)^k \equiv 1 \text{(mod 7)} \) We consider the different values of \( a \) If

1. \( a^2 \equiv 0 \text{(mod 7)} \), then from the last lemma \( 2^{12m} \equiv 1 \text{(mod 49)} \) but \( \text{ord}(2) \text{mod 49} \) is 21, so \( 7|m \), hence if \( (7, m) = 1 \), there is no solution in this case.
2. \( a^2 \equiv 1 \text{(mod 7)} \), then \( 2^k \equiv 1 \text{(mod 7)} \), so \( k \equiv 0 \text{(mod 3)} \) and \( p \equiv 1 \text{(mod 3)} \)
3. \( a^2 \equiv 2 \text{(mod 7)} \), then \( 3^k \equiv 1 \text{(mod 7)} \), so \( k \equiv 0 \text{(mod 6)} \) and \( p \equiv 1 \text{(mod 3)} \)
4. \( a^2 \equiv 4 \text{(mod 7)} \), then \( 5^k \equiv 1 \text{(mod 7)} \), so \( k \equiv 0 \text{(mod 6)} \) and \( p \equiv 1 \text{(mod 3)} \).

So if \( p \equiv 2 \text{(mod 3)} \), there is no solution. Combining \( p \equiv 7 \text{(mod 8)} \) and \( p \equiv 1 \text{(mod 3)} \) we get \( p \equiv 7 \text{(mod 24)} \).

**Examples.** The equations \( x^2 + 2^{30} = y^{23} \), \( x^2 + 2^{34} = y^{47} \), have no solutions in \( x \) odd.

### 4. PARTICULAR EQUATIONS

In this section we consider some particular equations and solve them completely.

**Example 1.** Consider the equation \( x^2 + 2^8 = y^n \). By Theorem 1 and Corollary 1 it suffices to consider \( n \) odd and \( x \) even. Then Case b gives \( u = 4, X = Y = 1 \), i.e. \( x = 2^4 \). Case c gives \( 8 > 2u = n\nu \), then \( X^2 + (2^{4-u})^2 = Y^n \). For \( 3|n \) the sole solution is \( X = 11, u = 3 \) whence \( x = 11.2^3, y = 5.2^2, n = 3 \).

By using methods similar to the above and considering the equation \( X^2 + 2^{2(m-u)} = Y^n \), in \( X \) odd and \( \nu \leq m - 1 \) we can solve the equation \( x^2 + 2^{2m} = y^n \) completely for \( 4 \leq m \leq 14 \). For the other values of \( m > 15 \) we need also Theorems 4, 5, 6, and 9 to solve the case when \( x \) is even and \( n \) is odd.

**Example 2.** Consider the equation \( x^2 + 2^{46} = y^n \). As in Example 1 we get from Case b \( u = 43, X = Y = 1 \), i.e. \( x = 2^{43} \). Case c gives \( 8 > 2u = n\nu \), then \( X^2 + (2^{43-u})^2 = Y^n \), with \( X \) odd. For \( 3|n \) the sole solution is \( X = 11, u = 42 \) whence \( x = 11.2^{42} \). Otherwise, all the prime factors of \( n \) must be congruent to 7 modulo 8 but be unequal to 7. Thus since \( n < 86, \) \( n \) must be prime \( p \). Next, the new \( m = 43 - u \) must be divisible by an odd power of 3, and \( u \) a multiple of \( p \). The only possibility would be \( u = p = 31, m = 12 \), so \( X^2 + 2^{24} = Y^{31} \), which has no solution by Theorem 8.

**Example 3.** Consider the equation \( x^2 + 2^{198} = y^n \). As we solved before we find \( x = 2^{99}, y = 2, n = 199 \). Case c gives \( 198 > 2u = n\nu \), then \( X^2 + (2^{99-u})^2 = Y^n \) with \( X \) odd. For \( 3|n \) there is no solution (Theorem 4). Otherwise as in Example 2, we get the only possibility \( u = 69, p = 23, m = 30 \), so \( X^2 + 2^{90} = Y^{31} \) which has no solution (Theorem 9).

By using the above methods we are able to verify the conjecture for \( m < 100 \) except possibly for the values \( m = 3, 15, 21, 27, 30, 33, 39, 44, 46, 51, 52, 57, 58, 60, 61, 64, 67, 68, 69, 70, 75, 77, 82, 83, 87, 88, 90, 91, 93, 94 \).
REFERENCES

[1] COHN, J.H.E., The diophantine equation $x^2 + 2^k = y^n$, Archiv der Mat., 59 (1992), 341-344


Submit your manuscripts at http://www.hindawi.com