Arch. Math. 74 (2000) 350–355
0003-889X/00/050350-06 $ 2.70/0

Archiv der Mathematik

On the Diophantine equation $x^2 + 2 = y^n$

By

B. Sury

Abstract. We give an elementary proof of the fact that the only solutions of the Diophantine equation $x^2 + 2 = y^n$ for $n > 1$ are $(x, y, n) = (\pm 5, 3, 3)$.

Introduction. It is known due to T. Nagell ([2]) that the equation of the title has only the one solution $(x, y) = (5, 3)$ for $n > 1$. But, Nagell's proof is not elementary as it uses a deep result of K. Mahler on binary quadratic forms. More recently, J. H. E. Cohn ([1]) investigated the equations $x^2 + 2^k = y^n$ for odd k. However, he merely refers to Nagell's proof when $k = 1$ and his (elementary) proof for higher k does not work for $k = 1$. In the literature, there are essentially two kinds of methods used to solve such Diophantine equations. Either one uses transcendental number-theoretic techniques or a completely elementary technique manipulating congruences. The purpose of this note is to give an elementary proof of Nagell's result. We shall use a polynomial identity in the proof as the usual elementary approach turns out to be inadequate.

Some standard reductions. Suppose x, y, n satisfy the equation of the title. It easily follows that x, y, n must all be odd. Writing the equation as $y^n = (x + \sqrt{2}i)(x - \sqrt{2}i)$ and noting that $\mathbb{Q}(\sqrt{-2})$ has class number 1, it follows that one must have $x + \sqrt{2}i = \alpha^n$ where $\alpha = (m + ir\sqrt{2})$ for some integers r, m. Then, $x - \sqrt{2}i = \bar{\alpha}^n$ and subtracting, one has $\alpha^n - \bar{\alpha}^n = 2\sqrt{2}i$. One can rewrite this as

$$\sum_{l=0}^{[(n-1)/2]} \binom{n}{2l+1} (-2)^l m^{n-2l-1} r^{2l+1} = 1.$$

This gives $r = \pm 1$ and, reading modulo 2, also that both n, m are odd.

We note that, conversely, if there are integers m, n, r satisfying the above equation, then the integers x, y defined by them give a solution of the Diophantine equation of the title.

For arbitrary integers m, n, r, let us write

$$a(m, n, r) = \sum_{l=0}^{[(n-1)/2]} \binom{n}{2l+1} (-2)^l m^{n-2l-1} r^{2l+1}.$$

Note that $a(m, n, r) = \dfrac{\alpha^n - \bar{\alpha}^n}{\alpha - \bar{\alpha}}$ where $\alpha = (m + ir\sqrt{2})$. We need to solve $a(m, n, r) = 1$ for m, n, r. We start with some useful observations:

Mathematics Subject Classification (1991): 11D41.

Lemma. *(i) If $a(m,n,r) = 1$, then $r = 1$.*
(ii) *$a(m,n,1) \neq -1$ for any m,n.*
(iii) *If $a(m,n,1) = 1$, then $a(m,d,1) = 1$ for every $d|n$.*
(iv) *For any m, $a_n := a(m,n,1)$ satisfies the following recursion in n:*
$a_{n+1} = 2ma_n - (m^2+2)a_{n-1}$.
(v) *If $n = 3$ and $a(m,n,1) = 1$, then $m = \pm 1$*
i.e., the only solutions of $x^2 + 2 = y^3$ are $(x,y) = (\pm 5, 3)$.
(vi) *If $a(m,n,1) = 1$, then $n \equiv 3 \bmod 4$.*
In this case, if $n \neq 3$, and 2^s is the highest power of 2 dividing $n-3$, then $m^2 \equiv 1 + 2^s \bmod 2^{s+1}$. In particular, $m \neq 1$ if $n \neq 3$ i.e., $x^2 + 2 = 3^n$ has no solutions if $n \neq 1, 3$.

Proof. (i) As we noticed above, if $a(m,n,r) = 1$, then m,n are odd and $r = \pm 1$. Now, $m^2 \equiv 1 \bmod 4$; so $m^{n-1} = (m^2)^{(n-1)/2} \equiv 1$ and $m^{n-3} \equiv 1 \bmod 4$. Further, we have

$$\begin{aligned} 1 = a(m,n,r) &= \sum_{l=0}^{(n-1)/2} \binom{n}{2l+1} (-2)^l m^{n-2l-1} r^{2l+1} \\ &\equiv \binom{n}{1} m^{n-1} r - 2\binom{n}{3} m^{n-3} r^3 \equiv nr - 2r^3 \binom{n}{3} \bmod 4. \end{aligned}$$

As $3^{-1} \equiv -1 \bmod 4$, one has $2\binom{n}{3} = \dfrac{n(n-1)(n-2)}{3} \equiv -n(n-1)(n-2) \bmod 4$. Thus,

$$1 = a(m,n,r) \equiv nr + r^3 n(n-1)(n-2) \bmod 4.$$

If $n \equiv 1 \bmod 4$, one has then $1 \equiv r \bmod 4$.
If $n \equiv -1 \bmod 4$, one has $1 \equiv -r - 6r^3 \bmod 4$.
In either case, $r \neq -1$. As $r = \pm 1$, we get $r = 1$.
(ii) If $a(m,n,1) = -1$, then evidently $a(m,n,-1) = 1$ from the very definition of $a(m,n,r)$. This contradicts (i).
(iii) Now $\dfrac{a(m,n,1)}{a(m,d,1)} = \dfrac{\alpha^n - \bar{\alpha}^n}{\alpha^d - \bar{\alpha}^d}$ is in $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$. So, $a(m,d,1) | a(m,n,1)$ if $d|n$. This proves our assertion in view of (ii).
(iv) Now $a_l = \dfrac{\alpha^l - \bar{\alpha}^l}{\alpha - \bar{\alpha}}$ for any l where $\alpha = m + \sqrt{2}i$. So, one has

$$\begin{aligned} (\alpha - \bar{\alpha}) a_{n+1} &= \alpha^{n+1} - \bar{\alpha}^{n+1} = \alpha(\alpha^n - \bar{\alpha}^n) + \alpha\bar{\alpha}^n - \bar{\alpha}^{n+1} \\ &= \alpha(\alpha^n - \bar{\alpha}^n) + \alpha\bar{\alpha}^n - \bar{\alpha}\alpha^n + \bar{\alpha}\alpha^n - \bar{\alpha}^{n+1} \\ &= \alpha(\alpha^n - \bar{\alpha}^n) + \alpha\bar{\alpha}(\bar{\alpha}^{n-1} - \alpha^{n-1}) + \bar{\alpha}(\alpha^n - \bar{\alpha}^n) \\ &= (\alpha + \bar{\alpha})(\alpha^n - \bar{\alpha}^n) - \alpha\bar{\alpha}(\alpha^{n-1} - \bar{\alpha}^{n-1}) \\ &= 2m(\alpha^n - \bar{\alpha}^n) - (m^2+2)(\alpha^{n-1} - \bar{\alpha}^{n-1}). \end{aligned}$$

Therefore, $a_{n+1} = 2ma_n - (m^2+2)a_{n-1}$.
(v) Is obvious as

$$(*) \qquad 1 = a(m,n,1) = \sum_{l=0}^{(n-1)/2} \binom{n}{2l+1} (-2)^l m^{n-2l-1}$$

reduces to $1 = 3m^2 - 2$ i.e., $m^2 = 1$ then.

(vi) Recall that m, n must be odd as $a(m,n,1) = 1$. Now, if $n \equiv 1 \bmod 2^t$, then

$$2^k \binom{n}{2k+1} = \frac{2^k n(n-1)}{(2k+1)2k} \binom{n-2}{2k-1} \equiv 0 \bmod 2^{t+1}$$

for $k \geqq 3$ as $\dfrac{2^k}{2k}$ is *even* i.e., the power of 2 dividing $2k$ is less than k.

Suppose 2^a is the highest power of 2 dividing $n-1$ i.e., $n \equiv 1 + 2^a \bmod 2^{a+1}$. Using the above fact and writing $(*)$ modulo 2^{a+1}, one gets

$$1 = \sum_{l=0}^{(n-1)/2} \binom{n}{2l+1} (-2)^l m^{n-2l-1} \equiv \binom{n}{1} m^{n-1} - 2\binom{n}{3} m^{n-3} + 4\binom{n}{5} m^{n-5} \bmod 2^{a+1}.$$

Let us look at the three terms one at a time. As m is odd, we have $m^{2^a} = m^{\phi(2^{a+1})} \equiv 1 \bmod 2^{a+1}$ and as $n \equiv 1 \bmod 2^a$, we also have $m^{n-1} \equiv 1 \bmod 2^{a+1}$. Using $n \equiv 1 + 2^a \bmod 2^{a+1}$, the first term is then

$$nm^{n-1} \equiv 1 + 2^a \bmod 2^{a+1}.$$

Now, the second term is $2\binom{n}{3} m^{n-3} = \dfrac{n(n-1)(n-2)}{3} m^{n-3}$. Let us substitute $n \equiv 1 + 2^a \bmod 2^{a+1}$ and write 3^{-1} for the inverse of 3 modulo 2^{a+1}. Then, the second term is

$$3^{-1}(1+2^a)2^a(2^a-1)m^{n-3} \bmod 2^{a+1}.$$

Using further the fact that $2^a t \equiv 2^a \bmod 2^{a+1}$ if t is odd, the second term is seen to be $\equiv 2^a$ modulo 2^{a+1}.

Finally, the third term is

$$\begin{aligned}
&\frac{n(n-1)(n-2)(n-3)(n-4)}{30} m^{n-5} \\
&\equiv \frac{(1+2^a)2^a(2^a-1)(2^a-2)(2^a-3)}{30} m^{n-5} \bmod 2^{a+1} \\
&\equiv (1+2^a)2^a(2^a-1)\left(\frac{2^a-2}{2}\right)(2^a-3)m^{n-5} \bmod 2^{a+1} \\
&\equiv (1+2^a)2^a(2^a-1)(2^{a-1}-1)(2^a-3)m^{n-5} \bmod 2^{a+1}.
\end{aligned}$$

If $a > 1$, $2^{a-1} - 1$ is odd, and the third term is $\equiv 2^a \bmod 2^{a+1}$.

Therefore, if $a > 1$, the sum of the three terms is

$$1 \equiv (1 + 2^a) - 2^a + 2^a = 1 + 2^a \bmod 2^{a+1}$$

which is absurd. Hence, we conclude that if $a(m,n,1) = 1$, then a must be 1 i.e., the statement $n \equiv 1 + 2^a \bmod 2^{a+1}$ simply becomes $n \equiv 3 \bmod 4$. This was the first assertion in (vi).

Finally, if $n \equiv 3 \bmod 2^s$, then

$$2^k \binom{n}{2k+1} = \frac{2^k n(n-1)(n-2)(n-3)}{(2k+1)2k(2k-1)(2k-2)} \binom{n-4}{2k-3} \equiv 0 \bmod 2^{s+1}$$

for $k \geqq 3$ as the power of 2 dividing the denominator is at the most k.

Taking for s the maximum possible value, we have $n \equiv 3 + 2^s \bmod 2^{s+1}$. As before, we rewrite $(*)$ modulo 2^{s+1} using the above congruence to get:

$$1 = a(m,n,1) = \sum_{l=0}^{(n-1)/2} \binom{n}{2l+1} (-2)^l m^{n-2l-1} \equiv nm^{n-1} - 3^{-1}n(n-1)(n-2)m^{n-3} + 15^{-1}\frac{n(n-1)(n-2)(n-3)(n-4)}{2} m^{n-5} \bmod 2^{s+1}.$$

Substituting $n \equiv 3 + 2^s \bmod 2^{s+1}$, this becomes

$$1 \equiv (3+2^s)m^{n-1} - 3^{-1}(2^s+3)(2^s+2)(2^s+1) + 15^{-1}(3+2^s)\left(\frac{2^s+2}{2}\right)(2^s+1)2^s(2^s-1)m^{n-5} \bmod 2^{a+1}.$$

Again, we look at the three terms one by one.

Since $m^{2^s} \equiv 1 \bmod 2^{s+1}$, we have $m^{n-3} \equiv 1 \bmod 2^{s+1}$ i.e., $m^{n-1} \equiv m^2 \bmod 2^{s+1}$. Using this as before with the evident observation that $2^s t \equiv 2^s \bmod 2^{s+1}$ if t is odd, the first term is

$$(3+2^s)m^{n-1} \equiv (3+2^s)m^2 \equiv 3m^2 + 2^s \bmod 2^{s+1}.$$

Similarly, the second term is $\equiv 2^s - 2 \bmod 2^{s+1}$.

The third term is

$$15^{-1}(3+2^s)\left(\frac{2^s+2}{2}\right)(2^s+1)2^s(2^s-1)m^{n-5} = 15^{-1}(3+2^s)(2^{s-1}+1)(2^s+1)2^s(2^s-1)m^{n-5} = t2^s \equiv 2^s \bmod 2^{s+1}$$

because t is odd. We have used the fact that $s > 1$ (i.e., that $n \equiv 3 \bmod 4$) which we proved already. So, the sum of the three terms is

$$1 = a(m,n,1) \equiv 3m^2 - 2 + 2^s \bmod 2^{s+1}.$$

Thus, one obtains $3(m^2-1) \equiv 2^s \bmod 2^{s+1}$. In other words,

$$m^2 - 1 \equiv 3^{-1}2^s \equiv 2^s \bmod 2^{s+1}.$$

The proof of the lemma is complete.

We shall use another identity to augment some of the information given by the lemma and complete the solution of the Diophantine equation. It is not clear to us as to how to use parts (iii) and (iv) of the lemma.

A polynomial identity to complete the proof. As an off-shoot of an algebro-geometric question about embeddings of the affine line in 3-space, the curious polynomial identity

$$\sum_{l=0}^{[k/2]} (-1)^l \binom{k-l}{l} (XY)^l (X+Y)^{k-2l} = \sum_{d=0}^{k} X^d Y^{k-d}$$

was noticed in ([3]). This turns out to suit our present purpose well. Take for X, Y the complex numbers α and $\bar{\alpha}$, and $k = n-1$ with n odd. As $\alpha = m + \sqrt{2}i$, we note that $\alpha\bar{\alpha} = m^2 + 2$ and $\alpha + \bar{\alpha} = 2m$. Now, we have

$$a(m,n,1) = \frac{\alpha^n - \bar{\alpha}^n}{\alpha - \bar{\alpha}} = \sum_{d=0}^{n-1} \alpha^d \bar{\alpha}^{n-1-d}.$$

Using the identity, we get therefore

$$\text{(A)} \qquad a(m,n,1) = \sum_{l=0}^{(n-1)/2} (-1)^l \binom{n-1-l}{l} (m^2+2)^l (2m)^{n-1-2l}.$$

Let us observe in passing that we have obtained for any odd n an identity in $\mathbb{Z}[T]$:

$$\sum_{l=0}^{(n-1)/2} (-1)^l \binom{n-1-l}{l} (T^2+2)^l (2T)^{n-1-2l} = \sum_{r=0}^{(n-1)/2} \binom{n}{2r+1} (-2)^r T^{n-2r-1}.$$

To complete the solution of the Diophantine equation, we start with the assumption that $a(m,n,1)=1$. We may also take $n>3$ because we have already dealt with $n=3$ in the lemma and we know that n is odd. *We shall write a_n instead of $a(m,n,1)$ for simplicity.* By the lemma (vi), one has an integer $a \geqq 2$ such that $n \equiv 3+2^a \bmod 2^{a+1}$ and $m^2 \equiv 1+2^a \bmod 2^{a+1}$. Let us compute $a_n \bmod 2^{a+1}$ using (A).

Note that $(m^2+2)^k \equiv 3^k$ or $3^k+2^a \bmod 2^{a+1}$ according as k is even or odd. Therefore, mod 2^{a+1}, one has

$$\begin{aligned} 1 = a_n &\equiv \sum_{l\,even} \binom{n-1-l}{l} 3^l (2m)^{n-1-2l} - \sum_{l\,odd} \binom{n-1-l}{l} (3^l+2^a)(2m)^{n-1-2l} \\ &\equiv \sum_{l=0}^{(n-1)/2} (-1)^l \binom{n-1-l}{l} 3^l (2m)^{n-1-2l} - \sum_{l\,odd} \binom{n-1-l}{l} 2^a (2m)^{n-1-2l} \bmod 2^{a+1}. \end{aligned}$$

Since $n \geqq 3 \bmod 4$ by lemma (vi), we know that $(n-1)/2$ is odd. Also, unless $l=(n-1)/2$, we get $2^a(2m)^{n-1-2l} \equiv 0 \bmod 2^{a+1}$. Therefore, we have

$$1 = a_n \equiv \sum_{l=0}^{(n-1)/2} (-1)^l \binom{n-1-l}{l} (2m)^{n-1-2l} 3^l - 2^a \bmod 2^{a+1}$$

where 2^a is the term corresponding to $l=(n-1)/2$ in the second sum.

Finally, lemma (vi) gives $m^2 \equiv 1+2^a \bmod 2^{a+1}$ which implies that $(2m)^{2r} \equiv 2^{2r} \bmod 2^{a+1}$ for each $r>0$. Thus,

$$1 = a_n \equiv \sum_{l=0}^{(n-1)/2} (-1)^l \binom{n-1-l}{l} 2^{n-1-2l} 3^l + 2^a \bmod 2^{a+1}.$$

Writing $b_n = \sum_{l=0}^{(n-1)/2} (-1)^l \binom{n-1-l}{l} 2^{n-1-2l} 3^l$, we get

$$\text{(B)} \qquad b_n \equiv 1+2^a \bmod 2^{a+1}.$$

Now $b_n = \dfrac{\beta^n - \overline{\beta}^n}{\beta - \overline{\beta}}$ where $\beta = 1+\sqrt{2}i$. Let us write $n-3=2^a b$ with b odd. The binomial expansion gives $\beta^{2^a b} = 1+2^a b\beta + 2^{a+1}\lambda$ for some $\lambda \in \mathbb{Z}[\sqrt{-2}]$. Since $\beta^3 = \beta - 6$, we get $b_n = \dfrac{\beta^n - \overline{\beta}^n}{\beta - \overline{\beta}} = 1 + 2^{a+1}\mu$ for some $\mu \in \mathbb{Z}[\sqrt{-2}]$. As $\mu \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$, we finally obtain $b_n \equiv 1 \bmod 2^{a+1}$. This contradicts (B). We have therefore proved Nagell's result:

Theorem. *The Diophantine equation* $x^2 + 2 = y^n$, $n > 1$ *has only the solutions* $(x, y, n) = (\pm 5, 3, 3)$.

Acknowledgements. We would like to thank the referee for suggestions to improve the exposition and to clarify some points.

References

[1] J. H. E. Cohn, The Diophantine equation $x^2 + 2^k = y^n$. Arch. Math. **59,** 341–344 (1992).
[2] T. Nagell, Verallgemeinerung eines Fermatschen Satzes. Arch. Math. **5,** 153–159 (1954).
[3] B. Sury, A curious polynomial identity. Nieuw Arch. Wisk. **11,** 93–96 (1993).

Eingegangen am 4. 1. 1999

Anschrift des Autors:

B. Sury
Stat-Math Division
Indian Statistical Institute
8th Mile, Mysore Road
R.V. College
P.O., Bangalore
560 059, India