Read 13 January 1960

The Diophantine Equation $x^2 + 7 = 2^n$

By T. Nagell

In Vol. 30 of the Norsk Matematisk Tidsskrift, pp. 62–64, Oslo 1948, I published a proof of the following theorem:[1]

When x is a positive integer, the number x^2+7 is a power of 2 only in the following five cases: $x = 1, 3, 5, 11, 181$.

Since prof. L. J. Mordell drew my attention to a paper by Chowla, Lewis and Skolem in the Proceedings of the American Mathematical Society, Vol. 10 (1959), p. 663–669, on the same subject, I consider it necessary to publish in English my proof of 1948 which is quite elementary.

The problem consists in determining all the positive integers x and y which satisfy the relation

$$\frac{1}{4}(x^2+7) = 2^y. \tag{1}$$

It is evident that the difference of two integral squares u^2 and v^2 is equal to 7 only for $u^2 = 16$ and $v^2 = 9$. Hence we conclude that the exponent y in (1) can be even only for $y = 2$ and $x = 3$. Thus we may suppose that y is odd and $\geqq 3$.

Passing to the quadratic field $K(\sqrt{-7})$, in which factorization is unique, we get from (1)

$$\frac{x \pm \sqrt{-7}}{2} = \left(\frac{1+\sqrt{-7}}{2}\right)^y, \tag{2}$$

whence

$$\left(\frac{1+\sqrt{-7}}{2}\right)^y - \left(\frac{1-\sqrt{-7}}{2}\right)^y = \pm\sqrt{-7}. \tag{3}$$

Considering this equation modulo

$$\left(\frac{1-\sqrt{-7}}{2}\right)^2 = \frac{-3-\sqrt{-7}}{2},$$

we get, since y is odd and $\geqq 3$, and since

$$\left(\frac{1+\sqrt{-7}}{2}\right)^2 = \frac{-3+\sqrt{-7}}{2} \equiv 1 \left(\operatorname{mod} \frac{-3-\sqrt{-7}}{2}\right),$$

[1] The theorem is set as a problem in my *Introduction to Number Theory*, Stockholm and New York 1951 (Problem 165, p. 272).

the congruence

$$\frac{1+\sqrt{-7}}{2} \equiv \pm\sqrt{-7} \left(\bmod \frac{-3-\sqrt{-7}}{2}\right).$$

But this congruence is possible only when the right-hand side is $-\sqrt{-7}$. Hence, we must take the lower sign in (3). Thus equation (3) may be written

$$-2^{y-1} = \binom{y}{1} - \binom{y}{3}\cdot 7 + \binom{y}{5}\cdot 7^2 - + \cdots \pm \binom{y}{y}\cdot 7^{\frac{1}{2}(y-1)}. \tag{4}$$

This equation implies the congruence

$$-2^{y-1} \equiv y \pmod 7,$$

which has the solutions

$$y \equiv 3,\ 5,\ 13 \pmod{42}.$$

Suppose first $y \equiv 3 \pmod{42}$ and put

$$y-3 = 7^z \cdot 6 \cdot h,$$

where h is an integer not divisible by 7. The number

$$\binom{y}{2k+1}\cdot 7^k = \frac{y(y-1)(y-2)(y-3)}{(2k-2)(2k-1)2k(2k+1)}\cdot\binom{y-4}{2k-3}\cdot 7^k$$

is divisible by 7^{z+1} for $k \geqq 2$, since $7^{k-1} > 2k+1$.
Hence we get from (4)

$$-2^{y-1} \equiv y - \frac{7}{6} y(y-1)(y-2) \pmod{7^{z+1}},$$

and thus

$$-2^{y-1} \equiv -4 \equiv y-7 \pmod{7^{z+1}}.$$

But this implies

$$y-3 \equiv 0 \pmod{7^{z+1}},$$

which is contrary to our hypothesis on y. Thus the only possibility is $y=3$ corresponding to $x=5$.

Suppose next that $y \equiv 5 \pmod{42}$ and put

$$y-5 = 7^z \cdot 6 \cdot h,$$

where h is an integer not divisible by 7. The number

$$\binom{y}{2k+1}\cdot 7^k = \frac{y(y-1)\ldots(y-5)}{(2k-4)(2k-3)\ldots(2k+1)}\cdot\binom{y-6}{2k-5}\cdot 7^k$$

is divisible by 7^{z+1} for $k \geqq 3$, since $7^{k-1} > 2k+1$.

Hence we get from (4)

$$-2^{y-1} \equiv -16 \equiv y - 70 + 49 \pmod{7^{z+1}}.$$

But this implies

$$y - 5 \equiv 0 \pmod{7^{z+1}}$$

which is contrary to our hypothesis on y. Thus the only possibility is $y=5$ corresponding to $x=11$.

Finally consider the case $y \equiv 13 \pmod{42}$ and put

$$y - 13 = 7^z \cdot 6 \cdot h,$$

where h is an integer not divisible by 7. The number

$$\binom{y}{2k+1} \cdot 7^k = \frac{y(y-1)\dots(y-13)}{(2k-12)\dots(2k+1)} \cdot \binom{y-14}{2k-13} \cdot 7^k$$

is divisible by 7^{z+1} for $k \geqq 7$, since $7^{k-2} > 2k+1$. Hence we get from (4)

$$-2^{12} \equiv -4096 \equiv y - \binom{y}{3} \cdot 7 + \binom{y}{5} \cdot 7^2 - \binom{y}{7} \cdot 7^3 + \binom{y}{9} \cdot 7^4 - \binom{y}{11} \cdot 7^5 + \\ + \binom{y}{13} \cdot 7^6 \pmod{7^{z+1}}.$$

We may replace y by 13 in all the terms on the right-hand side which are divisible by 7. Then we get the congruence

$$-4096 \equiv y - 4109 \pmod{7^{z+1}}.$$

Hence

$$y - 13 \equiv 0 \pmod{7^{z+1}},$$

which is contrary to our hypothesis on y. Thus the only possibility is $y=13$, corresponding to $x=181$.

Tryckt den 5 augusti 1960

Uppsala 1960. Almqvist & Wiksells Boktryckeri AB