THE DIOPHANTINE EQUATION $2^{n+2}-7=x^2$ AND RELATED PROBLEMS

TH. SKOLEM, S. CHOWLA AND D. J. LEWIS

1. Ramanujan [1, p. 327, Problem 464] observed that the equation $2^{n+2}-7=x^2$ has rational integral solutions for n and x when $n=1, 2, 3, 5$, and 13; and he conjectured that these were the only solutions. K. J. Sanjana and T. P. Trivedi [2] discussed but did not resolve the conjecture. By means of the Thue-Seigel-Roth Theorem it is possible to show that the above equation has only a finite number of solutions, but it is not possible to determine the exact number of solutions. Here we use the p-adic method of Skolem [3] to obtain the conjecture. The treatment of the problem in §2 is essentially that which was given by Skolem in the University of Notre Dame Number Theory Seminar in the Spring of 1958.

We also show that the sequence of integers satisfying the recursive relation

$$a_0 = a_1 = 1, \qquad a_n = a_{n-1} - 2a_{n-2} \text{ if } n > 1$$

is such that (i) $a_{n-1}^2=1$ exactly when the equation $2^{n+2}-7=x^2$ has a solution; and (ii) an integer appears in the sequence a_n at most three times.

2. Suppose n and x are rational integers such that $2^{n+2}-7=x^2$. Obviously $n\geqq 1$ and x is an odd integer prime to 7. Write

$$2^n = \frac{x^2+7}{4} = \left(\frac{x+(-7)^{1/2}}{2}\right)\left(\frac{x-(-7)^{1/2}}{2}\right).$$

The numbers $(x+(-7)^{1/2})/2$ and $(x-(-7)^{1/2})/2$ are relatively prime integers in the field $Q((-7)^{1/2})$. Here Q will be used to denote the field of rational numbers. In the field $Q((-7)^{1/2})$, $2=r\cdot r'$, where $r=(1+(-7)^{1/2})/2$ and $r'=(1-(-7)^{1/2})/2$ are conjugate, but not associate primes. Since $2^n=r^n\cdot r'^n=((x+(-7)^{1/2})/2)((x-(-7)^{1/2})/2)$, it necessarily follows that $r^n=(x\pm(-7)^{1/2})/2$.

Conversely, if n and x are rational integers such that $r^n=(x\pm(-7)^{1/2})/2$ then $2^{n+2}-7=x^2$ has a solution. Hence the number of solutions of $2^{n+2}-7=x^2$ is precisely the same as the number of rational integers n for which $r^n=(x\pm(-7)^{1/2})/2$.

We look at the first few powers of r.

Received by the editors December 12, 1958.

$$r = \frac{1}{2}(1 + (-7)^{1/2}), \qquad r^2 = \frac{1}{2}(-3 + (-7)^{1/2}),$$

$$r^3 = \frac{1}{2}(-5 - (-7)^{1/2}), \qquad r^4 = \frac{1}{2}(1 - 3(-7)^{1/2}),$$

$$r^5 = \frac{1}{2}(11 - (-7)^{1/2}), \qquad r^6 = \frac{1}{2}(9 + 5(-7)^{1/2}),$$

$$r^7 = \frac{1}{2}(-13 + 7(-7)^{1/2}), \qquad r^8 = \frac{1}{2}(-31 - 3(-7)^{1/2}), \cdots$$

$$\vdots$$

$$r^{13} = \frac{1}{2}(-181 - (-7)^{1/2}), \cdots .$$

Thus we obtain those values of n for which there is a solution and which had previousely been obtained by Ramanujan.

Observe that

$$r^{3n} = (1 - r'(-7)^{1/2})^n = 1 - C_{n,1}(r'(-7)^{1/2}) + C_{n,2}(r'(-7)^{1/2})^2 - \cdots$$
$$= A(n) + B(n)(-7)^{1/2},$$

where

$$A(n) = 1 - \frac{7}{2}C_{n,1} + \frac{3\cdot 7}{2}C_{n,2} - \frac{7^2}{2}C_{n,3} + \frac{7^2}{2}C_{n,4} + \frac{7^3}{2}C_{n,5}$$
$$- \frac{9\cdot 7^3}{2}(C_{n,6}) \cdots ,$$

and

$$B(n) = -\frac{1}{2}C_{n,1} + \frac{7}{2}C_{n,2} - \frac{5\cdot 7}{2}C_{n,3} + \frac{3\cdot 7^2}{2}C_{n,4} - \frac{11\cdot 7^2}{2}C_{n,5}$$
$$+ \frac{5\cdot 7^3}{2}C_{n,6} + \cdots .$$

We seek rational integers n such that $B(n) = \pm 1/2$. This can occur, only if $B(n) = \pm 1/2$ in each of the p-adic fields. For each prime p, the polynomials $C_{n,s}$ assume p-adic integral values as n ranges over the integers. Furthermore, if $s > 1$, for every rational integer n, the terms $(7^{[n/s]}/(n-1))C_{n,s}$ lie in the prime ideal of the 7-adic numbers. Hence

$$B(n) + \frac{1}{2} = (n-1)\left(-\frac{1}{2} + \frac{7}{2}\left(\frac{n}{2}\right) - \frac{5\cdot 7}{2}\left(\frac{n(n-2)}{3}\right) + \cdots\right)$$
$$= (n-1)U(n)$$

where for every rational integer n, $U(n)$ is a unit in the 7-adic numbers. Thus $B(n) = -1/2$ in the 7-adic numbers, and hence in Q, only if $n = 1$. We shall later show that $B(n)$ never assumes the value $1/2$. Now

$$r^{3n+1} = r(A(n) + B(n)(-7)^{1/2})$$
$$= \left(\frac{1}{2}A(n) - (7/2)B(n)\right) + (-7)^{1/2}\left(\frac{1}{2}A(n) + \frac{1}{2}B(n)\right)$$
$$= A_1(n) + B_1(n)(-7)^{1/2},$$

and

$$B_1(n) = \frac{1}{2} - 2C_{n,1} + 7C_{n,2} - 3\cdot 7C_{n,3} + 7^2C_{n,4} - 7^2C_{n,5} - 7^3C_{n,6} + .$$

Then

$$B_1(n) = \frac{1}{2} = n\left(-2 + \frac{7}{2}(n-1) - \frac{3\cdot 7}{3!}(n-1)(n-2) + \cdots\right)$$
$$= nV(n),$$

where, for every rational integer n, $V(n)$ is a 7-adic unit. Hence $B_1(n) = 1/2$ only if $n = 0$. Also

$$B_1(n) + \frac{1}{2} = (n-4)\left(1 + \frac{7(12n + 2n^2 + 7n^3)}{4} + \frac{7^3}{n-4}C_{n,5} + \cdots\right)$$
$$= (n-4)W(n),$$

where $W(n)$ is always a 7-adic unit; hence $B_1(n) = -1/2$ only if $n = 4$.

Finally

$$r^{3n+2} = A_2(n) + B_2(n)(-7)^{1/2},$$

where

$$B_2(n) = \frac{1}{2} - C_{n,1} + 2\cdot 7C_{n,3} - 2\cdot 7^2C_{n,4} - 2\cdot 7^2C_{n,5} - 6\cdot 7^3C_{n,6} + \cdots.$$

Now

$$B_2(n) - \frac{1}{2} = n\left(-1 + \frac{7}{3}(n-1)(n-2) - \frac{7^2}{12}(n-1)(n-2)(n-3) + \cdots\right)$$

and hence $B_2(n) = 1/2$ only if $n = 0$. Also

$$B_2(n) + \frac{1}{2} = (n-1)\left(-1 + \frac{7}{3}n(n-2) - \frac{7^2}{12}n(n-2)(n-3) + \cdots\right)$$

and hence $B_2(n) = -1/2$ only if $n = 1$.

Now suppose that there is an n such that $B(n) = 1/2$. Let $\xi = r^n$, then $\xi^3 - \xi'^3 = (-7)^{1/2} = (\xi - \xi')(\xi^2 + \xi\xi' + \xi'^2)$. Since ξ and ξ' are integers in $Q((-7)^{1/2})$, each of these factors is an integer $Q((-7)^{1/2})$ and hence the absolute value (as complex numbers) of each factor cannot be smaller than 1. Thus

$$|\xi - \xi'| \leqq 7^{1/2}, \qquad |\xi^2 + \xi\cdot\xi' + \xi'^2| \leqq 7^{1/2}.$$

Let $\xi = a + bi$, then

$$|b| \leqq \frac{1}{2}7^{1/2} \quad \text{and} \quad |\xi^2 + \xi\cdot\xi' + \xi'^2| = |3a^2 - b^2| \leqq 7^{1/2}.$$

Consequently

$$a^2 \leqq \frac{7^{1/2} + b^2}{3} \leqq \frac{7}{12} + \frac{7^{1/2}}{3}$$

$$a^2 + b^2 \leqq \frac{7}{4} + \frac{7}{12} + \frac{7^{1/2}}{3} < 4.$$

However $N(\xi) = a^2 + b^2 = N(r^n) = 2^n$, and hence $n = 1$, which is impossible. We have thus shown Ramanujan's conjecture to be correct.

The equation $2^{n+2} - 7 = x^2$ *has rational integral solutions exactly when* $n = 1, 2, 3, 5,$ *and* 13.

3. We have seen that $2^{n+2} - 7 = x^2$ has a solution exactly for those n for which $a_{n-1} = \pm 1$, where

$$r^n = \frac{1}{2}(b_{n-1} + a_{n-1}(-7)^{1/2}) = (c_{n-1} + a_{n-1}r).$$

We observe that

$$r^{n+1} = c_{n-1}r + a_{n-1}r^2 = -2a_{n-1} + (a_{n-1} + c_{n-1})r = c_n + a_n r.$$

Thus $a_{n+1} = a_n - 2a_{n-1}$ if $n > 1$, while $a_0 = a_1 = 1$. Hence the sequence $\{a_n\}$ is exactly that of the introduction.

Since $2^n = r^n r'^n$, it follows that $2^{n+2} - 7a_{n-1}^2 = b_{n-1}^2$. Conversely, if $2^{n+2} - 7y^2 = x^2$ then $2^{-1}(x + y(-7)^{1/2}) = 2^{-1}(b_{n-1} \pm a_{n-1}(-7)^{1/2})$ and hence $y = \pm a_{n-1}$. Thus

For a given rational integer n, the expression $2^{n+2} - 7y^2$ is the square of a rational integer if and only if $y^2 = a_{n-1}^2$.

We have seen that 1 occurs in the sequence $\{a_n\}$ exactly twice and -1 occurs exactly three times. From the recursive relation one observes that each a_n is odd. We next study how often an odd integer c can occur in the sequence $\{a_n\}$. Clearly c occurs in the sequence as many times as there are integers n such that either $2B(n) = c$, or $2B_1(n) = c$, or $2B_2(n) = c$.

Let $F(n) = a_0 + a_1 n + a_2 n^2 + \cdots$ be a p-adic power series where each a_i is a p-adic integer and at least one is a unit. Suppose $F(n)$ converges for all p-adic integers, then for each rational integer j, all but a finite number of the a_i are divisible by p^j. Hence

$$F(n) = \sum_{j=0}^{\infty} p^j f_j(n),$$

where $f_j(n)$ are polynomials with unit coefficients and $f_0(n) \not\equiv 0$.

Since f_0 has unit coefficients, on applying the division algorithm, with f_0 as divisor, one obtains polynomials with integer coefficients. Determine $g_1, h_1, g_2, h_2, \cdots$ in sequence, so that

$$f_1 = f_0 h_1 + g_1, \qquad 0 \leqq \deg g_1 < \deg f_0,$$

$$f_2 - g_1 h_1 = f_0 h_2 + g_2, \qquad 0 \leqq \deg g_2 < \deg f_0,$$

$$\vdots$$

$$f_m - g_1 h_{m-1} - g_2 h_{m-2} - \cdots - g_{m-1} h_1 = f_0 h_m + g_m, \quad 0 \leqq \deg g_m < \deg f_0.$$

Since the f_j have unit coefficients, the resulting polynomials g_j and h_j have integer coefficients.

Let $g(n) = f_0(n) + \sum_{i=1}^{\infty} p^i g_i(n)$, $H(n) = 1 + \sum_{i=1}^{\infty} p^i h_i(n)$. Then

$$F(n) = g(n)H(n),$$

where

(i) $g(n)$ is a polynomial with unit coefficients and such that $\deg g = \deg f_0$ and $g \equiv f_0 \pmod{p}$.

(ii) $H(n)$ is a power series with p-adic integer coefficients and converges to a unit for every integer value of n.

It follows that $F(n)=0$ exactly for those n for which $g(n)=0$. Hence

The number of p-adic integer solutions of $\sum_{i=0}^{\infty} a_i n^{i=0}$ *is at most* J, *where* J *is the largest integer for which* a_J *is a unit.*

This result was first stated by Strassman [4].

Now $2B(n)=un+7n^2C(n)$, where u is a 7-adic unit and $C(n)$ is a power series with 7-adic integer coefficients. Then $2B(n)=c$ for exactly one 7-adic integer and hence for at most one rational integer. One can also show that if $7^j \mid c$ then $7^j \mid n$.

Also

$$2B_1(n) = 1 - u_1 n + 7n^2 C_1(n)$$

and

$$2B_2(n) = 1 - u_2 n + 7n^2 C_2(n)$$

where u_1 and u_2 are 7-adic units and the $C_i(n)$ are power series with 7-adic integers as coefficients. Consequently neither $B_1(n)$ nor $B_2(n)$ may assume the value c more than once. Hence

No integer appears in the sequence $\{a_n\}$ *more than three times.*

The preceding discussion does not determine the exact number of times an integer c occurs in the sequence $\{a_n\}$. In order to do so, one would need to use special arguments as we did for $+1$.

We have shown that for each integer c there exists an N_c such that if $n>N_c$ then $a_n \neq c$. It would be interesting to have an explicit formula for N_c.

4. As a small generalization of Ramanujan's problem, we prove the following.

If A *is an odd rational integer incongruent to* 1 *modulo* 8, *the equation* $2^n+A=x^2$ *has at most one rational integer solution for* (n, x). *If there is a solution then* $0 \leqq n \leqq 2$.

Let $\mathfrak{O}$ denote the ring of integers in $Q(A^{1/2})$. If x is a rational integer, $x+A^{1/2}$ and $x-A^{1/2}$ have the same $\mathfrak{p}$-adic value for any prime $\mathfrak{p}$ of $\mathfrak{O}$.

(i) If $A \equiv 3 \pmod 4$, then $\pi=1+A^{1/2}$ is a prime in $\mathfrak{O}$ and $2=\pi^2 u$, where u is a unit in $\mathfrak{O}$. If $2^n=x^2-A$, then $x+A^{1/2}=x-1+\pi=\pi^n v$, where v is a unit in $\mathfrak{O}$. But $\pi^2 \nmid (x-1+\pi)$, hence $n \leqq 2$. On the other hand $(1+A)$ and $(2+A)$ cannot both be squares of rational integers.

(ii) If $A \equiv 5 \pmod 8$, 2 is a prime in $\mathfrak{O}$. If $2^n=x^2-A$, then $n=2k$ and $2 \nmid x$; but then $4^k+5 \equiv 1 \pmod 8$, and consequently $k=1$ and $n=2$.

It is easily seen that if $A \equiv 2 \pmod 8$, the equation $2^n+A=x^2$ has

at most one solution. The case $A \equiv 0 \pmod 4$ can be reduced to an equation with smaller A.

In a future paper we shall discuss the case $A \equiv 1 \pmod 8$. The simple arguments used in the section are not applicable to this last case, since the ideal (2) splits into two distinct prime ideals in $\mathfrak{O}$. We also hope to discuss such questions as the existence of a bound $N(p, A, k)$ such that for given rational integers p, A and k the equation $p^n + A = x^k$ has at most $N(p, A, k)$ rational integer solutions for (n, x).

Bibliography

1. S. Ramanujan, *Collected papers of Ramanujan*, Cambridge, Cambridge University Press, 1927.

2. K. J. Sanjana and T. P. Trivedi, J. Indian Math. Soc. vol. 5 (1913) pp. 227–228.

3. Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8de Skand. Mat. Kongr. Forh., Stockholm, 1934, pp. 163–188.

4. R. Strassman, *Über den Wertevorrat von Potenzreihen im Gebiet det p-adischen Zahlen*, J. Reine Angew. Math. vol. 159 (1928) pp. 13–28.

University of Notre Dame and
University of Colorado