NOTES ON THE DIOPHANTINE EQUATION $x^2+7y^2=2^{n+2}$

S. B. TOWNES[1]

1. **Introduction.** In [1] the authors define $r=\frac{1}{2}[1+(-7)^{1/2}]$ and $r^n=\frac{1}{2}[b_{n-1}+a_{n-1}(-7)^{1/2}]$ with $b_{n-1}^2+7a_{n-1}^2=2^{n+2}$, $n\geqq 1$. They prove that, except for $a_0=a_1=1$, and $a_2=a_4=a_{12}=-1$, $|a_n|>1$. They also prove that no integer appears in the sequence $\{a_i\}$ more than three times. In [2] Miss P. Chowla, using a different notation, proves that in the sequence $\{b_i\}$, except for $b_0=b_3=1$, an integer appears only once if $i+1$ is a power of 2. She also states, without explicit proof, that no integer appears more than twice in the sequence $\{b_i\}$. In [1] the authors ask for an explicit formula $N(c)$ with the property that for an arbitrary positive integer c, if $n>N(c)$, then $|a_n|\neq c$.

It is convenient to change the notation so that $r^n=\frac{1}{2}[b_n+a_n(-7)^{1/2}]$, $b_n^2+7a_n^2=2^{n+2}$, $n\geqq 1$, and $a_1=b_1=1$.

In these notes it will be shown that for $|a_i|>1$, no two terms of the sequence $\{a_i\}$ are equal, with the exception of $a_4=a_8=-3$. The desired formula $N(c)$ will be developed.

2. **Proof of the uniqueness of the** a_i. One may deduce from the definition of r^n that

$$2a_{(n+1)s} = b_{ns}a_s + b_s a_{ns} \tag{1}$$

and

$$2b_{(n+1)s} = b_{ns}b_s - 7a_{ns}a_s. \tag{2}$$

LEMMA 1. *For all values of n, a_n and b_n are odd integers with $a_n\equiv b_n \pmod 4$.*

The lemma is true for $a_1=b_1=1$. Assume it is true for arbitrary n. From (1) and (2), with $s=1$, $2a_{n+1}=b_n+a_n\equiv 2 \pmod 4$, and $2b_{n+1}=b_n-7a_n\equiv 2 \pmod 4$. Furthermore, $b_n+a_n\equiv b_n-7a_n \pmod 8$, hence $a_{n+1}\equiv b_{n+1} \pmod 4$, which proves the lemma.

To get useful expressions for b_{ns} and a_{ns}, expand

$$\left[\frac{b_s+a_s(-7)^{1/2}}{2}\right]^n = \frac{b_{ns}+a_{ns}(-7)^{1/2}}{2}$$

and get

Received by the editors August 31, 1961 and, in revised form, November 22, 1961.

[1] The author thanks the referee for his suggestions, all of which have been incorporated in this paper.

$$2^{n-1}b_{ns} = b_s^n - \frac{7n(n-1)}{2} b_s^{n-2} a_s^2 + \cdots + A, \tag{3}$$

in which A is $n(-7)^{(n-1)/2}a_s^{n-1}b_s$ if n is odd, and $(-7)^{n/2}a_s^n$, if n is even. Also

$$2^{n-1}a_{ns} = a_s\left[nb_s^{n-1} - \frac{7n(n-1)(n-2)}{3!} b_s^{n-3} a_s^2 + \cdots + B\right], \tag{4}$$

in which B is $(-7)^{(n-1)/2}a_s^{n-1}$ if n is odd, and $(-7)^{(n-2)/2}na_s^{n-2}b_s$ if n is even. Since $b_s^2+7a_s^2=2^{s+2}$, one may substitute $2^{s+2}-b_s^2$ for $7a_s^2$ in (3) and (4) and get, for all values of $n \geqq 2$,

$$\begin{aligned} b_{ns} = {} & b_s^n - n2^s b_s^{n-2} + \frac{n}{2}\binom{n-3}{1} 2^{2s} b_s^{n-4} - \cdots \\ & + (-1)^{i-1} \frac{n}{i-1}\binom{n-i}{i-2} 2^{(i-1)s} b_s^{n-2i+2} + \cdots, \\ & \qquad 3 \leqq i \leqq \frac{1}{2}(n+2), \end{aligned} \tag{5}$$

and

$$\begin{aligned} a_{ns} = a_s\Big[& b_s^{n-1} - (n-2)2^s b_s^{n-3} + \cdots \\ & - (-1)^{i-1}\binom{n-i}{i-1} 2^{(i-1)s} b_s^{n-2i+1} + \cdots \Big], \\ & \qquad 2 \leqq i \leqq \frac{1}{2}(n+1). \end{aligned} \tag{6}$$

One may verify (5) for $n=2$ and $n=3$ by actual computation. Now assume it is true for arbitrary $n \geqq 3$, and use (1) and (2) to get $2b_{(n+1)s}$. Replace $-7a_s^2$, which occurs in $-7a_{ns}a_s$ in (6), by $b_s^2-2^{s+2}$. The first two terms of $2b_{(n+1)s}$ are easily computed and agree with (5). The ith term, which may be seen to use the $(i-1)$st term of (6), as well as the ith terms of (5) and (6), is equal to

$$(-1)^{i-1}\left[4\binom{n+1-i}{i-2} + \binom{n-i}{i-1} + \frac{n}{i-1}\binom{n-i}{i-2}\right] 2^{(i-1)s} b_s^{n-2i+3},$$

which, on simplifying, becomes

$$(-1)^{i-1} \frac{2(n+1)}{i-1}\binom{n+i-1}{i-2} 2^{(i-1)s} b_s^{n-2i+3},$$

and on division by 2, becomes the ith term of $b_{(n+1)s}$.

In a similar way (6) may be verified by mathematical induction.

LEMMA 2. *For n odd and greater than* 1, $b_n \equiv 3 \pmod 8$.

In the ith term of (5), the coefficient of $2^{(i-1)s}b_s^{n-2i+2}$ is easily seen to be an integer, since it is

$$(-1)^{i-1}\left\{\binom{n-i+1}{i-1}+\binom{n-i}{i-2}\right\}.$$

Thus all terms after the third are multiples of 8. Let $s=1$, and use (5) to see that $b_n \equiv 1-2n+2n(n-3) \equiv 1+2n^2 \equiv 3 \pmod 8$, since n is odd.

From here on, to avoid repetition, let the equation $x \equiv 1 \pmod{2^t}$ imply that $x \not\equiv 1 \pmod{2^{t+1}}$.

LEMMA 3. *For $n=2^r$, $r \geqq 3$,* $b_n \equiv 1 \pmod{2^{r+2}}$.

Since $b_8 = -31 \equiv 1 \pmod{2^5}$, the lemma is true for $n=3$. Assume the lemma true for arbitrary r with $n=2^r$, $r \geqq 3$. Then by (5)

$$b_{2n} = b_n^2 - 2^{n+1} \tag{7}$$

and

$$b_{2n} \equiv b_n^2 \equiv 1 \pmod{2^{r+3}}.$$

LEMMA 4. *With n odd and greater than* 1, *and $s=2^r$, $r \geqq 1$, $b_{ns} \equiv 1 \pmod{2^{r+2}}$.*

For $s=2$, use (7) to see that $b_{2n} \equiv 1 \pmod{2^3}$. For $s=4$, use (7) again, with n replaced by $2n$ to get $b_{4n} \equiv 1 \pmod{2^4}$. With $r \geqq 3$, so that $2^r > r+2$, use (5) to get $b_{ns} = b_s^n - n2^s b_s^{n-2} + \cdots$. Since $b_s \equiv 1 \pmod{2^{r+2}}$, and n is odd, then $b_{ns} \equiv b_s^n \equiv 1 \pmod{2^{r+2}}$.

LEMMA 5. *Except for* $b_1 = b_4 = 1$, $|b_n| > 1$.

The values of b_1 and b_4 are easily computed. The remainder of the lemma follows from Lemmas 2, 3, and 4.

LEMMA 6. *For m any odd integer, and $a_r \equiv 0 \pmod m$, then $a_{r+s} \equiv 0$ or $\not\equiv 0 \pmod m$ according as $a_s \equiv$ or $\not\equiv 0 \pmod m$.*

Since $(a_r, b_r) = (a_s, b_s) = 1$, and $2a_{r+s} = a_r b_s + a_s b_r \equiv a_s b_r \pmod m$, the lemma is true.

LEMMA 7. *If t is the least value of n for which $a_n \equiv 0 \pmod m$, m any odd integer greater than* 1, *then $a_u \equiv 0 \pmod m$ if and only if u is a multiple of t.*

If u is a multiple of t, then $a_u \equiv 0 \pmod m$ by (6). To prove the converse let $u=qt+v$, $0\leqq v<t$. Then $2a_u=a_{qt}b_v+a_vb_{qt}\equiv a_vb_{qt}$ (mod m). Now $(a_n, b_n)=1$, and if $0<v<t$ then $a_n\not\equiv 0$ (mod m). Hence $v=0$ and the lemma follows.

LEMMA 8. *For $n=1$ and for $n=4$, $a_{2n}=a_n$, but for all other values of n, $|a_{2n}|>|a_n|$.*

In general, $a_{2n}=a_nb_n$. But $b_1=b_4=1$, and for all other values of n, by Lemma 5, $|b_n|>1$.

LEMMA 9. *For $s>1$, and $n=3$, 5, or 13, then $|a_{ns}|>|a_s|$.*

For $s=2$, 3, or 4, the lemma may be verified by actually computing a_{ns} and a_s in each case. Now assume $s\geqq 5$, and by (6)

$$a_{3s} = a_s(b_s^2 - 2^s),$$

$$a_{5s} = a_s(b_s^4 - 3\cdot 2^s b_s^2 + 2^{2s}),$$

$$a_{13s} = a_s(b_s^{12} - 11\cdot 2^s b_s^{10} + \cdots).$$

Since the proofs are closely analogous, only the first will be given in detail. In each case, the proof is accomplished by showing the coefficient of a_s is greater than 1 in absolute value by showing it is $\not\equiv 1$ (mod 2^s) but $\equiv 1$ (mod 8). To prove that $|a_{3s}|>|a_s|$, note that if s is odd then $b_s\equiv 3$ (mod 8), and therefore $b_s^2\equiv 1$ (mod 8), but $\not\equiv 1$ (mod 2^s). If s is even, let $s=k\cdot 2^r$, with k odd. By Lemma 4, $b_s = q\cdot 2^{r+2}+1$, q odd, and therefore $b_s^2\equiv 1$ (mod 2^{r+3}). Thus $b_s^2\not\equiv 1$ (mod 2^s).

LEMMA 10. *If r and s are positive powers of the same odd prime p, then $|a_{rs}|>|a_s|$.*

It is sufficient to prove that $|a_{p^{t+1}}|>|a_{p^t}|$. For $p=3$ or 5, the lemma is true by Lemma 9. Now assume $p>5$. Use (6) to get

$$a_{p^{t+1}} = a_{p^t}[b_{p^t}^{p-1} - (p-2)2^{p^t}b_{p^t}^{p-2} + \cdots],$$

all subsequent terms containing 2^{2p^t} as a factor. Let $p=k\cdot 2^u+1$, k odd. Then $b^{p-1}\equiv 1$ (mod 2^{u+2}). Now $p^t\geqq k\cdot 2^u+1$. If $k=1$, then $u>2$ since $p>5$, and $2^{p^t}>2^{u+2}$ since $2^u+1>u+2$. If $k>1$, then $k\cdot 2^u+1>u+2$ for $u\geqq 1$. Thus $|a_{p^{t+1}}|>|a_{p^t}|$.

LEMMA 11. *For r and s each greater than 2, then $|a_{rs}|>|a_s|$.*

Let p^u divide rs, but not s. If p is 2, 3, 5, or 13, then $|a_{rs}|>|a_s|$ by Lemmas 8 and 9. If p is some other prime, then $|a_{rs}|\geqq|a_s|$, and

$|a_{rs}| \geqq |a_{p^u}| > 1$, by Lemma 7 and [1]. Since s is not a multiple of p^u, a_s is not a multiple of a_{p^u}, by Lemmas 7 and 10. Were $|a_{rs}| = |a_s|$ then a_s would be a multiple of a_{p^u}, hence $|a_{rs}| > |a_s|$.

THEOREM 1. *Except for* $a_1 = a_2 = 1$, $a_3 = a_5 = a_{13} = -1$, *and for* $a_4 = a_8 = -3$, *if* $|a_r| = |a_s|$, *then* $r = s$.

This is a consequence of Lemmas 7, 8, and 11.

3. **The formula** $N(c)$. A formula for $N(c)$ will now be developed through a series of lemmas.

LEMMA 12. *For p any odd prime* $a_p \equiv (-7)^{(p-1)/2} \pmod{p}$, *and* $b_p \equiv 1 \pmod{p}$.

Since $a_7 = 7$, and $b_7 = -13$, the lemma is true for $p = 7$. For p any other odd prime, by (3) and (4),

$$2^{p-1}a_p = p - \frac{7p(p-1)(p-2)}{3!} + \cdots + (-7)^{(p-1)/2},$$

and

$$2^{p-1}b_p = 1 - \frac{p(p-1)}{2!} + \cdots + p(-7)^{(p-1)/2},$$

from which the lemma follows by inspection.

LEMMA 13. *For p any odd prime, if* $(-7/p) = 1$, *then* $a_{p-1} \equiv 0 \pmod{p}$, *and if* $(-7/p) = -1$, *then* $a_{p+1} \equiv 0 \pmod{p}$.

If $(-7/p) = -1$, by Lemma 12, $2a_{p+1} = a_p + b_p \equiv 0 \pmod{p}$. From the two equations $2a_p = a_{p-1} + b_{p-1}$ and $2b_p = -7a_{p-1} - b_{p-1}$, get $4a_{p-1} = a_p - b_p$. Hence for $(-7/p) = 1$, $a_{p-1} \equiv 0 \pmod{p}$.

LEMMA 14. *If p is any odd prime,* $r > 1$, *and* $a_s \equiv 0 \pmod{p^{r-1}}$, *then* $a_{sp} \equiv 0 \pmod{p^r}$.

By (4),

$$2^{p-1}a_{ps} = a_s\left(pb_s^{p-1} - \frac{7p(p-1)(p-2)}{3!} b_s^{p-3}a_s^2 - \cdots\right),$$

and $a_{sp} \equiv 0 \pmod{p^r}$, since the expression in the parentheses has p as a factor of the first term and a_s as a factor of every other term.

LEMMA 15. *For every odd prime p there exists an s such that* $a_s \equiv 0 \pmod{p}$.

For $p = 7$, $s = 7$. For p any other odd prime, s is $p - (-7/p)$, by Lemma 13.

COROLLARY. *For every odd prime p, and for every* $r > 0$, *there exists an s such that* $a_s \equiv 0 \pmod{p^r}$.

This follows from Lemma 14 by mathematical induction.

We are now ready to derive a formula $N(c)$. Let q_i be any odd prime for which -7 is a quadratic residue, and n_j any for which -7 is a quadratic non-residue. Let c, any positive odd integer, be written in the form

$$c = 7^g \prod_{i,j} q_i^{e_i} n_j^{f_j}, \qquad g \geqq 0,\ i \geqq 0,\ j \geqq 0,\ e_i \geqq 1,\ f_j \geqq 1.$$

THEOREM 2. *Let $N(1)=13$, $N(3)=8$, and for c any odd integer greater than 3, let $N(c)$ be the least common multiple of all the factors 7^g, q_i-1, n_j+1, $q_i^{e_i-1}$, $n_j^{f_j-1}$, then if $n>N(c)$, $|a_n| \neq c$.*

By [1], $|a_n|>1$ if $n>13$. By Theorem 1, if $n>8$ $|a_n| \neq 3$. By Lemmas 12, 13, 14, and 15, $a_{N(c)} \equiv 0 \pmod{c}$. Suppose $|a_n| = c$, $c>3$. By Theorem 1, this is true for only one n. By Lemma 7, this n must be a factor of $N(c)$, therefore $n \leqq N(c)$. Thus for all values of c, if $n>N(c)$, then $|a_n| \neq c$.

REFERENCES

1. Th. Skolem, P. Chowla, and D. J. Lewis, *The Diophantine equation $2^{n-2}-7=x^2$ and related problems*, Proc. Amer. Math. Soc. **10** (1959), 663–669.

2. P. Chowla, *A class of Diophantine equations*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 569–570.

UNIVERSITY OF HAWAII

TWO NEW REPRESENTATIONS OF THE PARTITION FUNCTION

BASIL GORDON

MacMahon [1] defined a two-rowed partition of the positive integer n as a representation of the form $n=\sum_{i=1}^r a_i + \sum_{j=1}^s b_j$ where the a_i and b_j are positive integers subject to the conditions $r \geqq s$, $a_i \geqq a_{i+1}$, $b_j \geqq b_{j+1}$, $a_i \geqq b_i$. Such partitions may be conveniently visualized by placing the summands on two rows, the a_i on the top row and the b_j on the bottom row, with each b_i immediately beneath a_i. Thus for $n=3$ the partitions in question are (omitting + signs)

$$\begin{array}{ccccc} 3, & 21, & 2, & 111, & 11. \\ & & 1 & & 1 \end{array}$$

In this note the following two theorems will be proved.

THEOREM 1. *The number of two-rowed partitions of n satisfying $a_i > a_{i+1}$, $b_j > b_{j+1}$ is $p(n)$, the ordinary partition function of n.*

Received by the editors January 6, 1962.