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

S. B. TOWNES

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 $b_n^2 + 7a_n^2 = 2n+2$, $n \geq 1$. 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 $\{a_n\}$ more than three times. In [2] Miss P. Chowla, using a different notation, proves that in the sequence $\{b_n\}$, except for $b_3 = b_7 = 1$, 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 $\{b_n\}$. 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 $r^n = \frac{1}{2}[b_n + a_n(-7)^{1/2}]$, $b_{n+1}^2 + 7a_{n+1}^2 = 2n+2$, $n \geq 1$, and $a_1 = b_1 = 1$.

In these notes it will be shown that for $|a_i| > 1$, no two terms of the sequence $\{a_n\}$ 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

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

and

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

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

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

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.
NOTES ON THE DIOPHANTINE EQUATION \( x^3 + 7y^3 = z^2 \)

The Diophantine equation \( x^3 + 7y^3 = z^2 \) is studied with particular emphasis on finding integer solutions.\\

In this context, we define \( A = n(7^{-1/3}a^{n-1}_s) \) if \( n \) is odd, and \( (-7)^{n/2}a^n_s \) if \( n \) is even. Also,\\

\[
2^{n-1}a_{ns} = a_s \left[ nb^{n-1}_s - \frac{7n(n-1)(n-2)}{3!} b^{n-2}_s a_s + \cdots + B \right],
\]

where \( B = (-7)^{(n-1)/2}a^{n-1}_s \) if \( n \) is odd, and \( (-7)^{(n-2)/2}na^{n-2}_s b_s \) if \( n \) is even. Since \( b^2_s + 7a^2_s = 2s^2 + 2 \), one may substitute \( 2s^2 - b^2_s \) for \( 7a^2_s \) in (3) and (4) and get, for all values of \( n \geq 2 \),\\

\[
b_{ns} = b^2_s - n2s^{n-2} + \frac{n}{2} \binom{n-3}{1} 2s^{n-4} + \cdots + (-1)^{i-1} \frac{n}{i-1} \binom{n-i}{i-2} 2^{(i-1)s} b^{n-2i+2}_s + \cdots,
\]

where \( 3 \leq i \leq \frac{1}{2} (n + 2) \), and\\

\[
a_{ns} = a_s \left[ b^{n-1}_s - (n - 2)2s^{n-3} + \cdots - (-1)^{i-1} \frac{n}{i-1} \binom{n-i}{i-2} 2^{(i-1)s} b^{n-2i+1}_s + \cdots \right],
\]

where \( 2 \leq i \leq \frac{1}{2} (n + 1) \).

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

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

which, on simplifying, becomes\\

\[
(-1)^{i-1} \frac{2(n+1)}{i-1} \binom{n+i-1}{i-2} 2^{(i-1)s} b^{n-2i+3}_s
\]
and on division by 2, becomes the \(i\)th term of \(b_{(n+1)\ast}\).

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 \(i\)th term of (5), the coefficient of \(2^{-(i-1)}b_i^{n-2i+2}\) 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 \(x \equiv 1 \pmod{2^r}\) imply that \(x = 1 \pmod{2^{r+1}}\).

**Lemma 3.** For \(n = 2^r, r \geq 3, b_n \equiv 1 \pmod{2^{r+2}}\).

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

\[
(7) \quad b_{2n} = b_n^2 - 2^{n+1}
\]

and

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

**Lemma 4.** With \(n\) odd and greater than 1, and \(s = 2^r, r \geq 1, b_n\equiv 1 \pmod{2^{r+2}}\).

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 \(b_{4n} \equiv 1 \pmod{2^5}\). With \(r \geq 3\), so that \(2^r > r+2\), use (5) to get \(b_{4n} = b_n^4 - 2n^2 + 2n^2 + \cdots \). Since \(b_n \equiv 1 \pmod{2^{r+2}}\), and \(n\) is odd, then \(b_{4n} \equiv b_n^4 \equiv 1 \pmod{2^{r+2}}\).

**Lemma 5.** Except for \(b_1 = b_3 = 1, |b_n| > 1\).

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 \(a_{r+s} \equiv 0 \pmod{m}\) or \(\not\equiv 0 \pmod{m}\) according as \(a_s \equiv 0 \pmod{m}\).

Since \((a_r, b_s) = (a_s, b_r) = 1\), and \(2a_{r+s} = a_rb_s + a_sb_r \equiv a_rb_r \pmod{m}\), 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 con-
verse let $u = qt + v$, $0 \leq v < t$. Then $2a_u = a_qb_s + a_sqbt \equiv a_qb_t \pmod{m}$. Now $(a_n, b_n) = 1$, and if $0 < v < t$ then $a_n \not\equiv 0 \pmod{m}$. 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 $n = 3, 5, 13$, then $|a_{ns}| > |a_s|$.

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

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

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

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

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 $\not\equiv 1 \pmod{2^s}$ but $\equiv 1 \pmod{8}$. To prove that $|a_{3s}| > |a_s|$, note that if $s$ is odd then $b_s \equiv 3 \pmod{8}$, and therefore $b_s^2 \equiv 1 \pmod{8}$, but $\not\equiv 1 \pmod{2^s}$. 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 $b_s^2 \equiv 1 \pmod{2^{r+3}}$. Thus $b_s^2 \not\equiv 1 \pmod{2^s}$.

**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 $|a_{pr^s}| > |a_{pr^e}|$. For $p = 3$ or 5, the lemma is true by Lemma 9. Now assume $p > 5$. Use (6) to get

$$a_{pr^s} = a_{pr}[b_{pr^e} - (p - 2)^{pr^e} b_{pr^e}] + \cdots,$$

all subsequent terms containing $2^{pr^e}$ as a factor. Let $p = k \cdot 2^u + 1$, $k$ odd. Then $b_{pr^e} \equiv 1 \pmod{2^{u+2}}$. Now $p \geq k \cdot 2^u + 1$. If $k = 1$, then $u > 2$ since $p > 5$, and $2^s > 2^{u+2}$ since $2^u + 1 > u + 2$. If $k > 1$, then $k \cdot 2^u + 1 > u + 2$ for $u \geq 1$. Thus $|a_{pr^s}| > |a_{pr^e}|$.

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

**Theorem 1.** Except for \( a_1 = a_2 = 1, a_4 = a_6 = a_{13} = -1 \), and for \( a_4 = a_8 = -3 \), if \( |a_s| = |a_s| \), 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 \( a_p \equiv (-7)^{(p-1)/2} \) (mod \( p \)), and \( b_p \equiv 1 \) (mod \( p \)).

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),
\[
2^{r-1}a_p = p - \frac{7p(p-1)(p-2)}{3!} + \cdots + (-7)^{(p-1)/2},
\]
and
\[
2^{r-1}b_p = 1 - \frac{p(p-1)}{2!} + \cdots + p(-7)^{(p-1)/2},
\]
from which the lemma follows by inspection.

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

If \((-7/p) = -1\), by Lemma 12, \( 2a_{p+1} = a_p + b_p \equiv 0 \) (mod \( p \)). 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 \((-7/p) = 1\), \( a_{p-1} \equiv 0 \) (mod \( p \)).

**Lemma 14.** If \( p \) is any odd prime, \( r > 1 \), and \( a_s \equiv 0 \) (mod \( p^{r-1} \)), then \( a_{sp} \equiv 0 \) (mod \( p^r \)).

By (4),
\[
2^{r-1}a_{sp} = a_s \left( pb_s^{r-1} - \frac{7p(p-1)(p-2)}{3!} b_{p-1} a_s - \cdots \right),
\]
and \( a_{sp} \equiv 0 \) (mod \( p^r \)), 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 \( a_s \equiv 0 \) (mod \( p \)).

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 \( a_s \equiv 0 \) (mod \( p^r \)).

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

\[
c = 7^{p} \prod_{i,j} q_i^{e_i} n_j^{f_j}, \quad g \geq 0, \ i \geq 0, \ f_j \geq 0, \ e_i \geq 1, \ f_j \geq 1.
\]

**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, \( a_{N(c)} = 0 \) (mod \( c \)). Suppose \( |a_n| = c, \ n > 3 \). By Theorem 1, this is true for only one \( n \). By Lemma 7, this \( n \) must be a factor of \( N(c) \), therefore \( n \leq N(c) \). Thus for all values of \( c \), if \( n > N(c) \), then \( |a_n| \neq c \).

**REFERENCES**


**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 \( n = \sum_{i=1}^{s} a_i + \sum_{j=1}^{t} b_j \) where the \( a_i \) and \( b_j \) are positive integers subject to the conditions \( r \leq s, \ a_i \geq a_{i+1}, \ b_j \geq b_{j+1}, \ a_i \geq b_i \). 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 \( b_j \) immediately beneath \( a_i \). Thus for \( n = 3 \) the partitions in question are (omitting + signs)

\[
3, \ 21, \ 2, \ 111, \ 11.
\]

\[
1 \ 1
\]

In this note the following two theorems will be proved.

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

Received by the editors January 6, 1962.