PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 41, Number 2, December 1973

THE EQUATION OF RAMANUJAN-NAGELL AND $[y^2]$

D. G. MEAD

ABSTRACT. By arithmetizing Levi's constructive test for membership in $[y^2]$ we have translated the questions of whether a given power product is in $[y^2]$ to determining whether a certain product of matrices is the zero matrix. This leads to number-theoretic problems, including the diophantine equations of the title $2^n-7=x^2$.

Introduction. In the proof of the sufficiency of the low power theorem [4] and [10], one needs information concerning the differential ideal $[y^p]$, and Ritt suggests in his "Questions for Further Investigations" [10, p. 177] a further examination of this ideal. Levi [4] obtained a constructive test for determining whether any polynomial is in $[y^p]$, and we have arithmetized his method. Restricting ourselves to $[y^2]$ for simplicity, we show that the question of determining whether a power product belongs to $[y^2]$ can be translated into determining whether a certain product of matrices is the zero matrix which in turn can be translated into a number theoretic problem. In fact we encounter a problem stated by Ramanujan in 1913 [9], first solved by Nagell in 1948 [7], and solved several times since then [1], [2], [11], [12]. It may be of some interest to note that this problem, which arose in the study of error correcting codes [11], has now appeared in an investigation in differential algebra.

Notation. Let F be a field of characteristic zero, y a differential indeterminant over F, and $R=F\{y\}$, the differential ring of polynomials in y and its derivatives, with coefficients in F. Denoting differentiation by subscripts, if $P=y_{i_1}y_{i_2}\cdots y_{i_d}$, we say that P is of degree d and weight $w=\sum_{j=1}^{d} i_j$. Levi showed [4] that if $w<d(d-1)$ then $P\in[y^2]$, the smallest differential ideal in R containing y^2, and for each $w\geqq d(d-1)$ he gave examples of P which are not in the ideal. With the above power product, assuming $i_1\leqq i_2\leqq\cdots\leqq i_d$, we associate the sequence $(a_1,\cdots,a_d)$ where $a_k=\sum_{j=1}^{k} i_j-k(k-1)$, called the weight sequence.

Levi's condition can be stated as follows: the product P is in $[y^2]$ if some entry of its weight sequence is negative. The fact that this condition is not necessary was shown in [5], which also characterized all products which are in the ideal if their weight sequences contain no number larger than 2. An indication of some of the difficulties of a similar result for

Presented to the society, November 18, 1972; received by the editors January 22, 1973.
AMS (MOS) subject classifications (1970). Primary 12H05; Secondary 10A35, 10B15.

power products, the elements of whose weight sequences are no larger than 3, is given in [**8**]. We present a new technique which can be applied to any weight sequence, but shall limit our discussion to those whose entries are $\leqq 3$.

Sequences and the reduction process. We will show how Levi's reduction process for $[y^2]$ can be stated in terms of sequences. (It is easy to generalize this to $[y^p]$.) As described above, to every ordered monomial corresponds a sequence $(a_1, \cdots, a_n)$. Conversely, to every weight sequence, $(a_1, \cdots, a_n)$ corresponds to the ordered monomial $y_{i_1}y_{i_2}\cdots y_{i_n}$ where $i_j = a_j - a_{j-1} + 2(j-1)$ if we allow the i_j to be negative and define $a_0 = 0$. If $2 + a_{i+1} + a_{i-1} - 2a_i \geqq 0$ for $i = 1, 2, \cdots, n-1$, then $i_1 \leqq i_2 \leqq \cdots \leqq i_n$. If for some k, $2 + a_{k+1} + a_{k-1} - 2a_k = t < 0$, it is easy to see that the sequence $(a_1, \cdots, a_{k-1}, a_k + t, a_{k+1}, \cdots, a_n)$ corresponds to

$$y_{i_1}y_{i_2}\cdots y_{i_{k-1}}y_{i_{k+1}}y_{i_k}y_{i_{k+2}}\cdots y_n.$$

By iterating this process, any sequence $(a_1, \cdots, a_n)$ can be put in canonical form, that is, so that in the corresponding ordered product, $i_1 \leqq i_2 \leqq \cdots \leqq i_n$.

We present a brief description of Levi's reduction process for $[y^2]$, and the simplification introduced in [**5**]. The product $Y = y_{i_1}y_{i_2}\cdots y_{i_n}$ is called an α-term if $i_1 + 2 \leqq i_2 + 2 \leqq \cdots \leqq i_{n-1} + 2 \leqq i_n$, and the α-terms are linearly independent over F, modulo $[y^2]$. If $W = Y \cdot y_i y_{i+1}$, then by solving for $y_i y_{i+1}$ in $(y^2)_{2i+1}$ we obtain

$$W \equiv Y \sum_{j=0}^{i-1} \frac{2C_j^{2i+1}}{2C_i^{2i+1}}(-1)y_j y_{2i+1-j} \quad \text{modulo } [y^2].$$

Similarly,

$$Yy_i^2 \equiv Y \sum_{j=0}^{i-1} \frac{C_j^{2i}}{C_i^{2i}}(-2)y_j y_{2i-j}.$$

In [**5**] it is shown we can suppress the numbers $2C_j^{2i+1}/2C_i^{2i+1}$, and C_j^{2i}/C_i^{2i} (which are there called first multipliers) and we write the above,

$$W \equiv^M Y \sum_{j=0}^{i-1} (-1)y_j y_{2i+1-j}, \quad \text{and} \quad Yy_i^2 \equiv^M Y \sum_{j=0}^{i-1} (-2)y_j y_{2i-j},$$

respectively. In [**4**] it is shown that after a finite number of steps any monomial is congruent, modulo $[y^2]$, to a linear combination of α-terms, and an element of R is in $[y^2]$ if and only if, in its expression as a linear combination of α-terms, all coefficients are zero. Since all of the congruences in this paper will be "multiplier" congruences, we drop the M and write $\equiv$, rather than $\equiv^M$

Turning to sequences, we note that $(a_1, \cdots, a_n)$, in canonical form, is an α-term if and only if $f(j)=a_{j+1}+a_{j-1}-2a_j\geqq 0$ for $j=1, 2, \cdots, n-1$. Assume $f(k)=-1$. Then, corresponding to the above, we have

$$(a_1, \cdots, a_n) \equiv -\sum_{j=1}^{a_k} (a_1, \cdots, a_{k-1}, a_k - j, a_{k+1}, \cdots, a_n),$$

where, in general, the sequences on the right side of the congruence will not be in canonical form. It is easy to see that if the canonical form of $(a_1, \cdots, a_{k-1}, a_k-r, a_{k+1}, \cdots, a_n)$ has a negative entry, and hence is in the ideal, the same is true for all $j>r$, and the sum can be terminated with any such r. If $f(k)=-2$ (which corresponds to $i_k=i_{k+1}$), then we have

$$(a_1, \cdots, a_n) \equiv -2\sum_{j=1}^{a_k} (a_1, \cdots, a_{k-1}, a_k - j, a_{k+1}, \cdots, a_n).$$

This completes the description of the reduction process, for if $(a_1, \cdots, a_n)$ is in canonical form, then $f(k)\geqq -2$ for $k=1, 2, \cdots, n-1$.

We finally note some results from [5, pp. 428–430], which will prove useful. If (A) and (A_i) are sequences, and $(A)\equiv\sum \alpha_i(A_i)$ for some rational numbers α_i, then $(0, A)\equiv\sum \alpha_i(0, A_i)$. Also, $(1, 1, A)\equiv-(0, 1, A)$; for $\varepsilon=0, 1$, if $(A, \varepsilon)\equiv\alpha(0, \cdots, 0, \varepsilon)$ then $(A, \varepsilon, B)\equiv\alpha(0, \cdots, 0, \varepsilon, B)$; and if $(a_1, \cdots, a_n, \varepsilon)\equiv\alpha(0, \cdots, 0, \varepsilon)$ and $(\varepsilon, a_n, \cdots, a_1, 0)=\beta(0, \cdots, 0)$ then $\beta=0$ if and only if $\alpha=0$. It is clear that no confusion will arise if we delete a sequence of 0's at the beginning of a sequence; thus we write $(1, 2, 2, 2)\equiv-2(1, 2)+(1, 2, 2)$ rather than the more precise

$$-2(0, 0, 1, 2) + (0, 1, 2, 2).$$

The following relation will be useful:

$$\begin{aligned}(0, 2, 2, 2) &\equiv -2(1, 2, 2) - 2(0, 2, 2)\\ &\equiv 2(1, 1, 2) + 2(1, 0, 2) + 4(1, 2) + 4(0, 2)\\ &\equiv -2(1, 2) - 4(0, 2) + 4(1, 2) + 4(0, 2)\end{aligned}$$

or

$$(*) \qquad (0, 2, 2, 2) \equiv 2(1, 2).$$

Matrices. As will be seen shortly, the sequence defined by $g(0)=0$, $g(1)=1$, $g(n+2)=g(n+1)-2g(n)$ will be important for our work. It is easy to prove that $g(n)=0$ if and only if $n=0$, and we note that $|g(n)|=1$

if $n=1, 2, 3, 5, 13$. We first describe the procedure for sequences $(a_1, \cdots, a_n)$ with $a_i \leqq 2$.

The following relations, $(1,2,2) \equiv 0(1,2)+(1,2,2)$, and $(1,2,2,2) \equiv -2(1,2)+(1,2,2)$ can be summarized by the matrix congruence

$$\begin{pmatrix} (1,2,2) \\ (1,2,2,2) \end{pmatrix} \equiv M_2 \begin{pmatrix} (1,2) \\ (1,2,2) \end{pmatrix} \quad \text{where } M_2 = \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix}.$$

Therefore, with $2_i = 2$,

$$\begin{pmatrix} (1, 2_1, \cdots, 2_{n+1}) \\ (1, 2_1, \cdots, 2_{n+2}) \end{pmatrix} \equiv M_2^n \begin{pmatrix} (1,2) \\ (1,2,2) \end{pmatrix}$$

where

$$M_2^n = \begin{pmatrix} (-1)^{n-1} 2g(n-1) & (-1)^{n-1} g(n) \\ (-1)^n 2g(n) & (-1)^n g(n+1) \end{pmatrix}.$$

Similarly,

$$\begin{pmatrix} (1,2,1) \\ (1,2,2,1) \end{pmatrix} \equiv T_{21}((0,1))$$

where $T_{21} = \binom{2}{0}$. Thus,

$$A = (1, 2_1, \cdots, 2_{n+1}, 1) \equiv (1,0) M_2^n T_{21}(0,1) = 4(-1)^{n-1} g(n-1)(0,1)$$

and since $(0, 1)$ is an α-term, A is in $[y^2]$ if and only if $g(n-1)=0$, i.e., $n=1$. Thus $(1,2,2,1)$ is in $[y^2]$, and using $(*)$, we find $(0,2,2,2,2,1)$ is also in $[y^2]$. Using a remark at the end of the previous section and $(*)$, we conclude $(1,2,2,2,2,0)$ and $(2,2,2,2,2,2,0)$ are also in the ideal. In this way we easily obtain the main results of §4 in [5].

We turn now to weight sequences $(a_1, \cdots, a_n)$ where $a_i \leqq 3$. As before, it is easy to show that

$$\begin{pmatrix} (1,2,3,3) \\ (1,2,2,3,3) \\ (1,3,3) \end{pmatrix} \equiv M_3 \begin{pmatrix} (1,2,3) \\ (1,2,2,3) \\ (1,3) \end{pmatrix} \quad \text{where } M_3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 3 & 4 \\ 0 & -2 & -2 \end{pmatrix},$$

and that

$$M_3^n = \begin{pmatrix} (-1)^n & & 0 \\ 0 & -g(n+3) & 4g(n) \\ 0 & -2g(n) & 8g(n-3) \end{pmatrix}.$$

Similarly, we obtain the "transition" matrices,

$$\begin{pmatrix}(1,2,3,2)\\(1,2,2,3,2)\\(1,3,2)\end{pmatrix} \equiv T_{32}\begin{pmatrix}(1,2)\\(1,2,2)\end{pmatrix} \qquad \text{where } T_{32}=\begin{pmatrix}2 & 0\\0 & -2\\0 & 1\end{pmatrix},$$

$$\begin{pmatrix}(1,2,3,1)\\(1,2,2,3,1)\\(1,3,1)\end{pmatrix} \equiv T_{31}((0,1)) \qquad \text{where } T_{31}=\begin{pmatrix}0\\-4\\1\end{pmatrix},$$

$$\begin{pmatrix}(1,2,0)\\(1,2,2,0)\end{pmatrix} \equiv T_{20}((0,0)) \qquad \text{where } T_{20}=2\begin{pmatrix}1\\2\end{pmatrix},$$

and

$$\begin{pmatrix}(1,2,3)\\(1,2,2,3)\end{pmatrix} \equiv T_{23}\begin{pmatrix}(1,2,3)\\(1,2,2,3)\\(1,3)\end{pmatrix} \qquad \text{where } T_{23}=\begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\end{pmatrix}.$$

The following illustrates how the problem of membership in the ideal for sequences $(a_1, \cdots, a_n)$ with $a_i \leqq 3$ can be stated in terms of the above matrices. Note $P=(1, 3_1, \cdots, 3_{r+1}, 2)$ with $3_i=3$ is in $[y^2]$ if and only if $(0,0,1)M_3^r T_{32}=(0, 4(g(r)+2g(r-3)))$ is the zero matrix. Since $g(r)+2g(r-3)=-g(r-2)$, it follows that $(1, 3_1, 3_2, \cdots, 3_{r+1}, 2)$ is in the ideal if and only if $r=2$. Also, using $T_{20}=2\binom{1}{2}$, we see that $(1, 3_1, \cdots, 3_{r+1}, 2, 0) \in [y^2]$ only if $(1, 3_1, \cdots, 3_{r+1}, 2) \in [y^2]$. Similarly, $(1,0,0)M_3^n T_{31}$ is the zero matrix for every n, and $(1,0,0)M_3^n$ is never the zero matrix (since M_3 is nonsingular). That is, $(1, 2, 3_1, \cdots, 3_{n+1}, 1)$ is in the ideal for every $n \geqq 0$, and $(1, 2, 3_1, \cdots, 3_k)$ is never in the ideal. The conclusions in this paragraph contain the main results in [**8**].

We can now characterize all sequences $(a_1, \cdots, a_n)$ in the ideal where $1<a_i\leqq 3$ for $1<i<n$, which do not start with $(2, 3, \cdots)$ or $(2, 2, 3, \cdots)$ or end with $(\cdots, 3, 2, 0)$ or $(\cdots, 3, 2, 2, 0)$.

THEOREM 1. *With* $2_i=2$, $3_i=3$, n_i *and* $m_j \geqq 0$, *and* $I=[y^2]$,

(1) $(1, 3_1, \cdots, 3_{n+1}, 2) \in I$ *if and only if* $n=2$.

$(1, 2_1, \cdots, 2_{n_1+1}, 3_1, \cdots, 3_{m_1+1}, \cdots, 3_1, \cdots, 3_{m_k+1}, 1) \in I$ *if and only if either* $m_k=2$ *or* $n_i=0$ *for every* i.

(2) $(1, 3_1, \cdots, 3_{n_1+1}, 2_1, \cdots, 2_{m_1+1}, 3_1, \cdots, 3_{n_2+1}, \cdots, 3_1, \cdots, 3_{n_k+1}, 1) \in I$ *if and only if one of* n_1 *and* n_k *is* 2.

(3) $(1, 2_1, \cdots, 2_{n_1+1}, 3_1, \cdots, 3_{m_1+1}, 2_1, \cdots, 2_{n_2+1}, \cdots, 3_1, \cdots, 3_{m_k+1}, 2_1, \cdots, 2_{n_{k+1}+1}, 1) \in I$ *if and only if* $\sum_{i=1}^{k+1} n_i=1$.

(4) $(1, 3_1, \cdots, 3_{n+1}, 1) \in I$ *if and only if* $n=5$.

(5) $(2_1, \cdots, 2_{n_1+3}, 3_1, \cdots, 3_{m_1+1}, \cdots, 3_1, \cdots, 3_{m_k+1}, 2_1, \cdots, 2_{n_k+1}, 1) \in I$ *if and only if* $\sum_{i=1}^{k+1} n_i = 1$.

(6) $(2_1, \cdots, 2_{n_1+3}, 3_1, \cdots, 3_{m_1+1}, \cdots, 3_1, \cdots, 3_{m_k+1}, 2_1, \cdots, 2_{n_k+3}, 0) \in I$ *if and only if* $\sum_{i=1}^{k+1} n_i = 1$.

(7) *In any of the above, replace* $(a_1, \cdots, a_n)$ *by* $(a_n, a_{n-1}, \cdots, a_1)$.

PROOF. Having just seen a proof of the first part of (1), we establish (3) before completing the proof of (1). With $n_1, n_2, \cdots, m_1, m_2, \cdots$ two sequences of nonnegative integers, let

$$(\alpha_k, \beta_k) = (1, 0)\left(\prod_{i=1}^{k-1} M_2^{n_i} T_{23} M_3^{m_i} T_{32}\right) M_2^{n_k}.$$

Then we find the following recursion relations for $k \geqq 2$:

$$\begin{aligned} 2^{-1}\alpha_k &= (-1)^{m_{k-1}+n_k-1} 2\alpha_{k-1} g(n_k - 1) \\ &\quad + (-1)^{n_k} 2\beta_{k-1} g(n_k)(g(m_{k-1} + 3) + 2g(m_{k-1})), \\ 2^{-1}\beta_k &= (-1)^{m_{k-1}+n_k-1} \alpha_{k-1} g(n_k) \\ &\quad + (-1)^{n_k} \beta_{k-1} g(n_k + 1)(g(m_{k-1} + 3) + 2g(m_{k-1})). \end{aligned}$$

The determinant of this system of equations, with α_{k-1} and β_{k-1} the unknown, is

$$(-1)^{m_{k-1}-1}(g(m_{k-1} + 3) + 2g(m_{k-1}))\det\begin{pmatrix} 2g(n_k - 1) & 2g(n_k) \\ g(n_k) & g(n_k + 1) \end{pmatrix}$$

and this is not zero since $g(m_{k-1}+3)+2g(m_k) = -g(m_{k-1}+1)$ and

$$\begin{pmatrix} 2g(n_k - 1) & 2g(n_k) \\ g(n_k) & g(n_k + 1) \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ 1 & 1 \end{pmatrix}^{n_k}.$$

We see α_1 and β_1 cannot both be zero, hence, by induction the same is true for α_k and β_k. If $(\alpha_k, \beta_k)T_{21} = (0)$ then $\alpha_k = 0$. But, if $\alpha_k = 0$ then either $n_k = 1$ and $\beta_{k-1} = 0$ or $n_k = 0$ and $\alpha_{k-1} = 0$. Also, if $\beta_k = 0$ then $\beta_{k-1} = 0$ and $n_k = 0$. The conclusion (3) now follows readily. Since $(\alpha_k, \beta_k)T_{23}M_3^r T_{31} = 4\beta_k(g(r+3)+g(r)) = 4\beta_k(g(r-2))$, we see $(1, 2_1, \cdots, 2_{n_1+1}, 3_1, \cdots, 3_{m_1+1}, \cdots, 3_1, \cdots, 3_{m_k+1}, 1) \in I$ if and only if either $\beta_k = 0$ or $r = 2$. From this, one can easily complete the proof of (1).

To obtain the result in (2), with $m_1, m_2, \cdots$ and $n_1, n_2, \cdots$ sequences of nonnegative integers, we let $(\alpha_k, \beta_k, 0) = (0, 0, 1)\prod_{i=1}^{k}(M_3^{m_i} T_{32} M_2^{n_i} T_{23})$. Then

$$\alpha_1 = (-1)^{n_1} 8g(m_1 - 2)g(n_1), \qquad \beta_1 = (-1)^{n_1} 4g(m_1 - 2)g(n_1 + 1),$$

and for $k \geqq 1$,

$$\alpha_{k+1} = 4(-1)^{n_k}((-1)^{m_k-1}g(n_k - 1)\alpha_k + g(n_k)g(m_k + 1)\beta_k),$$
$$\beta_{k+1} = 2(-1)^{n_k}((-1)^{m_k-1}g(n_k)\alpha_k + g(n_k + 1)g(m_k + 1)\beta_k).$$

By induction one can prove that if $\beta_1 \neq 0$, then for all $k > 1$, $\alpha_k/\beta_k = 2a_k/b_k$ where a_k and b_k are odd; i.e., if $\beta_1 \neq 0$, then $\beta_i \neq 0$ for all i. (It is clear that if $\beta_1 = 0$ then $\alpha_i = \beta_i = 0$ for all i.) Now,

$$(\alpha_k, \beta_k, 0)M_3^t T_{31} = ((-1)^t\alpha_k, \beta_k(-g(t + 3)), \beta 4g(t))\begin{pmatrix} 0 \\ -4 \\ 1 \end{pmatrix}$$
$$= 4\beta_k(g(t + 3) + g(t)) = 4\beta_k(4g(t - 2))$$

and this is the zero matrix only if $\beta_k = 0$ or $t = 2$. This completes the proof of (2). (From (1), (2) states that a sequence of this type is in the ideal only if it has a factor in the ideal.)

To obtain (4), we note $(0, 0, 1)M_3^n T_{31} = (8(g(n) + g(n-3))) = (8g(n-5))$ which is zero only if $n = 5$. From equation (*) and the remarks at the end of the previous section, the results (5), (6), and (7) follow.

The equation of Ramanujan-Nagell. Ramanujan [**9**] conjectured that the diophantine equation $x^2 + 7 = 2^{n+2}$ had only 5 solutions corresponding to $n = 1, 2, 3, 5, 13$. This conjecture was first proved correct by Nagell [**7**]. An equivalent problem, which Mersenne numbers are triangular numbers, i.e., solve $2^m - 1 = k(k+1)/2$, was solved by Browkin and Schinzel [**1**]. Another equivalent problem, for what value of n is $g(n) = \pm 1$ if $g(1) = g(2) = 1$ and $g(n+2) = g(n+1) - 2g(n)$, was solved by Chowla, Dunton and Lewis [**2**], and by Skolem, Chowla and Lewis [**12**]. In the proof of the following theorem, we encounter the same problem.

THEOREM 2. *With* $2_i = 2$, *and* $3_i = 3$, $(2, 3_1, \cdots, 3_{n+1}, 2_1, \cdots, 2_{r+1}, 1) \in I$ *if and only if*:
$r = 2$, $n = 0$, *or*
$r = 3$, $n = 1, 2, 4, 12$, *or*
$r = 5$, $n = 3, 7$, *or*
$r = 13$, $n = 11$.

PROOF. If $(2, 3_1, \cdots, 3_{n+1}, 2_1, \cdots, 2_{r+1}, 1) \in I$ then since $2(0, 2) = (1, 2, 2) - (1, 2)$ we should have $(-1, 1)T_{23}M_3^n T_{32}M_2^r T_{21} = (0)$. But this product equals $(-1)^{r+1}8((-1)^{n-1}g(r-1) + g(r)g(n+1)) = 0$, and since $(g(r), g(r-1)) = 1$, we must have $g(r) = \pm 1$. In each of the references [**2**], [**3**], [**6**], [**7**], [**11**], [**12**], it is shown that this only occurs if $r = 1, 2, 3, 5, 13$. $(g(3) = g(5) = g(13) = -1.)$

If $r=1$, then $g(n+1)=0$ for which there is no nonnegative solution. If $r=2$, then $g(n+1)=(-1)^n$ and $n=1$. If $r=3$, we see that $-g(n+1)=(-1)^n$ which implies $n=1, 2, 4, 12$. If $r=5$, then $(-1)^{n-1}(-3)=g(n+1)$. To show that $n+1=4, 8$ are the only solutions we will show that $|g(k)|=3$ only for $k=4, 8$. Similarly, for $r=13$, we need $(-1)^{n-1}45=g(n+1)$ and we show that $|g(k)|=45$ only for $k=12$.

The proof of the theorem will be complete once we have proved the following lemma.

LEMMA. *If* $g(1)=g(2)=1$ *and* $g(n+2)=g(n+1)-2g(n)$ *then*
(a) $|g(n)|=3$ *if and only if* $n=4, 8$.
(b) $|g(n)|=45$ *if and only if* $n=12$.

PROOF. From the conditions on $g(n)$, it is well known that if m and n are positive integers and $m|n$ then $g(m)|g(n)$. Also, it is easy to show that $g(n+8)=g(n+4)-16g(n)$ for all n.

The remainders of $g(n)$ modulo 64 are 1, 1, -1, -3, -1, followed by a periodic pattern of 16 terms: 5, 7, -3, -17, -11, -23, -19, -1, -27, -25, 29, 15, 21, -9, 13, 31. Therefore if $g(n)=-3$, then $n=4$, or $n\equiv 8$ (16); i.e., $n=4(4t+2)$. (We also note $g(n)$ can never be $+3$.) For $t>0$, $g(4t+2)\neq\pm 1$ and since $4t+2|n$, $g(4t+2)|g(n)$ or $g(4t+2)=-3$. But $4t+2\not\equiv 8$ (16) and this contradiction completes the proof of (a).

Before turning to (b) we show that $|g(n)|=5$ only if $n=6$. From the remainders modulo 64, we see that if $|g(n)|=5$ then $g(n)=5$ and $n\equiv 6$ (mod 16); i.e., $n=2(8t+3)$. If $t>0$, then $g(8t+3)\neq\pm 1$, and hence $g(8t+3)=5$. But $8t+3\not\equiv 6$ (16) and $|g(n)|=5$ only if $n=6$.

The proof of (b) can be done in a similar manner. We first show that $|g(n)|$ never takes on the value 9 or 15. If $|g(n)|=9$ then $g(n)=-9$ and $n\equiv 3$ (mod 16). The remainders of $g(4t+3)$ modulo 10 repeat in blocks of 6 and we find $n\equiv 24t+3=3(8t+1)$. For $t>0$, $g(8t+1)\neq\pm 1$, ± 3; hence $g(8t+1)=-9$ which implies $8t+1\equiv 3$ (mod 16). This is a contradiction and we conclude $|g(n)|$ is never 9. If $|g(n)|=15$ then $g(n)=15$ and $n\equiv 17$ (mod 16). The remainders of $g(4k+1)$ modulo 17 repeat in blocks of 36 (most easily seen as 4 groups of 9 each) and if $g(n)=15$ then $n\equiv 21$ or 141 (mod 144). This contradicts the above and we see $|g(n)|$ never takes on the value 15.

From the remainders modulo 64 we find $|g(n)|=45$ only if $g(n)=45$ and $n=16t+12=4(4t+3)$. For $t>1$, $|g(4t+3)|\neq 1$, 3, 5, 9, 15. Hence $g(4t+3)=45$ which is impossible since $4t+3$ is odd; therefore we have shown $|g(n)|=45$ only if $n=12$.

Although other results similar to those in Theorem 2 can easily be obtained, we have not been successful in characterizing all sequences

$(a_1, \cdots, a_n) \in I$ with $a_i \leqq 3$, no less all sequences in I. Indeed, the appearance of the equation of Ramanujan-Nagell suggests that the search for a necessary and sufficient test for membership in $[y^2]$, stated in terms of the sequences $(a_1, \cdots, a_n)$, may involve difficult, and possibly deep, number theoretic problems.

However, it may be of some interest to note that the same problem (the equation of Ramanujan-Nagell), which has attracted a fair amount of theoretical attention over the years, also arose in the study of error correcting codes, and has now reappeared in a problem in differential algebra. One wonders whether there is perhaps something fundamental about Ramanujan's problem, as well as when and where it may arise again.

REFERENCES

1. J. Browkin and A. Schinzel, *Sur les nombres de Mersenne qui sont triangulaires*, C. R. Acad. Sci. Paris **242** (1956), 1780–1781. MR **17,** 1055.

2. S. Chowla, M. Dunton and D. J. Lewis, *All integral solutions of* $2^n - 7 = x^2$ *are given by* $n=3$, 4, 5, 7, 15, Norske Vid. Selsk. Forh. (Trondheim) B **33** (1960), no. 9; 37–38. MR **26** #6118.

3. Helmut Hasse, *Über eine diophantische Gleichung von Ramanujan-Nagell und ihre verallgemeinerung*, Nagoya Math. J. **27** (1966), 77–102. MR **34** #136.

4. H. Levi, *On the structure of differential polynomials and on their theory of ideals*, Trans. Amer. Math. Soc. **51** (1942), 532–568. MR **3,** 264.

5. D. G. Mead, *Differential ideals*, Proc. Amer. Math. Soc. **6** (1955), 420–432. MR **17,** 123.

6. L. J. Mordell, *Diophantine equations*, Pure and Appl. Math., vol. 30, Academic Press, New York, 1969, pp. 205-206. MR **40** #2600.

7. T. Nagell, *The diophantine equation* $x^2 + 7 = 2^n$, Ark. Math. **4** (1960), 185–187; Nordisk Mat. Tidskr. **30** (1948), 62–64. MR **24** #A83.

8. K. B. O'Keefe, *Unusual power products and the ideal* $[y^2]$, Proc. Amer. Math. Soc. **17** (1966), 757–758. MR **33** #4053.

9. S. Ramanujan, *Problem* 465, J. Indian Math. Soc. **5** (1913), 120.

10. J. F. Ritt, *Differential algebra*, Amer. Math. Soc. Colloq. Publ., vol. 33, Amer. Math. Soc., Providence, R.I., 1950. MR **12,** 7.

11. H. S. Shapiro and D. L. Slotnick, *On the mathematical theory of error correcting codes*, IBM J. Res. Develop. **3** (1959), 25–34. MR **20** #5092.

12. T. Skolem, S. 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. MR **22** #25.

13. *Elementary problem* E-2367, Amer. Math. Monthly **79** (1972), 772.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, DAVIS, CALIFORNIA 95616