A PROBLEM IN ADDITIVE NUMBER THEORY*

BY

R. D. JAMES

1. Introduction. Some time ago the author was asked by Professor D. N. Lehmer if there was anything known about the representation of an integer \( h \) in the form

\[
h = \sum_{i=1}^{s} h_i,
\]

where all the prime factors of each \( h_i \) are of a given form. A search of the literature seemed to indicate that various theorems had been conjectured but none actually proved.† For example, L. Euler stated without proof that every integer of the form \( 4j+2 \) is a sum of two primes each of the form \( 4j+1 \). Even the weaker statement that every integer of the form \( 4j+2 \) is a sum of two integers which have all their prime factors of the form \( 4j+1 \) has not yet been proved.

In view of the absence of any definite results in the literature it seems worthwhile to point out that some very interesting theorems can be obtained in an elementary way. This is done in Part I of this paper and the results are summarized in Theorems 1, 2, and 3 below. In Part II we use the method of Viggo Brun‡ to prove a general theorem and from this we deduce Theorems 4 and 5 below.

**Theorem 1.** Consider the set of all integers \( n_i \) with the property that \( n_0 = 1 \) and that every prime factor of each \( n_i, i \geq 1 \) is of the form \( 4j+1 \). Let \( r = 3, 4, 5, \) or \( 6 \). Then every integer \( N \equiv r \pmod{4}, N \geq r \) is a sum of exactly \( r \) integers \( n_i \), all but three of which may be taken equal to 1. Except for \( r = 6 \) this result is the best possible in the sense that there is an infinite number of integers \( N \equiv r \pmod{4} \) which are not the sum of fewer than \( r \) integers \( n_i \).

**Theorem 2.** Let \( N \) be any integer of the form \( 4j+2 \). If the integer \( 8j+2 \) is of the form \( 2K p_1^{2v_1} \cdots p_t^{2v_t} \), where \( p_v \equiv 3 \pmod{4}, v = 1, 2, \cdots, t \), and every prime factor of \( K \) is of the form \( 4j+1 \), then \( N \) is a sum of exactly two integers \( n_i \).

* Presented to the Society, April 3, 1937; received by the editors March 23, 1937.
† L. E. Dickson, *History of the Theory of Numbers*, vol. I, Chap. XVIII, and vol. II, Chap. VIII.
‡ See the paper by H. Rademacher, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, vol. 3 (1924), pp. 12–30.
Theorem 3. Consider the set of all integers \( m_i \) with the property that \( m_0 = 1 \) and that every prime factor of \( m_i \), \( i \geq 1 \) is of the form \( 8j + 1 \) or \( 8j + 3 \). Then every odd integer \( M \geq 3 \) is a sum of exactly three integers \( m_i \) and every even integer \( M \geq 4 \) is a sum of exactly four integers \( m_i \). The results for \( M \) odd and \( M \equiv 0 \pmod{8} \) are the best possible.

Theorem 4. Every sufficiently large integer \( N \equiv 2 \pmod{4} \) is a sum of two integers which have all except possibly two of their prime factors of the form \( 4j + 1 \).

Theorem 5. Every sufficiently large integer \( M \equiv 2, 4, 6 \pmod{8} \) is a sum of two integers which have all except possibly two of their prime factors of the form \( 8j + 1 \) or \( 8j + 3 \).

Part I

2. Preliminary lemmas. The lemmas which follow are well known and we shall state them without proof.

Lemma 1.* If \( k \) is any integer such that

\[ k \not\equiv 0, 7, 12 \text{ or } 15 \pmod{16} \]

then there exist integers \( x_1, x_2, \) and \( x_3 \) such that

\[ k = \sum_{r=1}^{3} x_r^2. \]

Lemma 2.† If \( x \) and \( y \) have no common factor and are not both odd, every prime factor of \( x^2 + y^2 \) is of the form \( 4j + 1 \).

Lemma 3. If \( x \) and \( y \) have no common factor and \( x \) is odd, every prime factor of \( x^2 + 2y^2 \) is of the form \( 8j + 1 \) or \( 8j + 3 \).

3. The proof of Theorem 1. We suppose first that \( r = 3 \) so that \( N \) is of the form \( 4j + 3 \). We have

\[ 8j + 3 \not\equiv 0, 7, 12, \text{ or } 15 \pmod{16}, \]

so that by Lemma 1

\[ 8j + 3 = \sum_{r=1}^{3} x_r^2. \]

Since \( x_r^2 \) is of the form \( 4j \) or \( 4j + 1 \) according as \( x_r \) is even or odd, it follows that each \( x_r \) in (1) must be odd. Let \( x_r = 2s_r + 1 \). Then (1) becomes

† Lemmas 2 and 3 follow from the fact that \( -1 \) is a quadratic residue of an odd prime \( p \) if and only if \( p \) is of the form \( 4j + 1 \), and that \( -2 \) is a quadratic residue of an odd prime \( p \) if and only if \( p \) is of the form \( 8j + 1 \) or \( 8j + 3 \).
\[8j + 3 = \sum_{r=1}^{3} (2s_r + 1)^2,\]

\[N = 4j + 3 = \sum_{r=1}^{3} \{s_r^2 + (s_r + 1)^2\}.

Obviously \(s_r\) and \(s_r + 1\) have no common factor and are not both odd. Hence by Lemma 2 every prime factor of the integer \(S_r^2 + (S_r + 1)^2\) is of the form 47 + 1. This proves the first part of Theorem 1 when \(r = 3\).

Now let \(r = 4, 5,\) or 6. Then \(N - r + 3 \equiv 3 \pmod{4}\) and thus \(N - r + 3\) is a sum of exactly three integers \(n_i\). It follows that \(N\) itself is a sum of exactly \(r\) integers \(n_i\), all but three of which are equal to 1.

To prove the last statement of the theorem when \(r = 3\) or 4 we observe that since we have each \(n_i \equiv 1 \pmod{4}\) the congruence

\[(2) \quad N \equiv \sum_{i=1}^{s} n_i \pmod{4}\]

has no solution when \(s < r\). Therefore the equation

\[(3) \quad N = \sum_{i=1}^{s} n_i\]

certainly has no solution when \(s < r\).

When \(r = 5\) we consider the set of all integers \(N = p_1^{a_1} \cdots p_t^{a_t}\), where every \(p_i\) is of the form 47 + 3. It is evident that \(N \equiv 1 \pmod{4}\). For these integers the congruence (2) has no solution when \(1 < s < 5\) and hence the equation (3) has no solution when \(s < 5\).

4. The proof of Theorem 2. Since the integer \(8j + 2\) is of the form \(2Kp_1^{a_1} \cdots p_t^{a_t}\), where \(p_i \equiv 3 \pmod{4}\) and every prime factor of \(K\) is of the form 47 + 1, there exist integers \(u\) and \(v\) such that\

\[(4) \quad 8j + 2 = u^2 + v^2.\]

By the argument used in the proof of Theorem 1, both \(u\) and \(v\) must be odd. Let \(u = 2y + 1\), \(v = 2z + 1\). Then (4) becomes

\[8j + 2 = 2\{y^2 + (y + 1)^2 + z^2 + (z + 1)^2\} - 2,
\]

\[N = 4j + 2 = y^2 + (y + 1)^2 + z^2 + (z + 1)^2.\]

Every prime factor of \(y^2 + (y + 1)^2\) and \(z^2 + (z + 1)^2\) is of the form 47 + 1 and this completes the proof.

5. The proof of Theorem 3. We suppose first that $M = 2k + 3$. If

$$k \not\equiv 0, 7, 12, \text{ or } 15 \pmod{16}$$

we have

$$k = \sum_{i=1}^{3} x_i^2,$$

$$2k + 3 = \sum_{i=1}^{3} (2x_i^2 + 1).$$

By Lemma 3 every prime factor of $2x_i^2 + 1$ is of the form $8j + 1$ or $8j + 3$.

If $k \equiv 0$ or $12 \pmod{16}$ then $2k - 21 \equiv 3$ or $11 \pmod{16}$. Then*

$$2k - 21 = \sum_{i=1}^{3} x_i^2,$$

(5)

$$2k + 3 = \sum_{i=1}^{3} (x_i^2 + 8).$$

In (5) every $x_i$ is odd and the result follows from Lemma 3.

If $k \equiv 7$ or $15 \pmod{16}$ then $2k - 3 \equiv 11 \pmod{16}$ and we have

$$2k - 3 = \sum_{i=1}^{3} x_i^2,$$

$$2k + 3 = \sum_{i=1}^{3} (x_i^2 + 2).$$

Again $x_i$ is odd and the theorem follows as before.

The rest of the theorem is a consequence of the first part since $M - 1$ is odd if $M$ is even. The results can be shown to be the best possible by using congruential conditions similar to those used in the proof of Theorem 1.

**Part II**

6. The Viggo Brun method. In this part we use the results of the paper by Rademacher to which reference was made above. This will be cited as R.†

Let $p_1, p_2, \cdots$, be any infinite set of primes which are all distinct. Let $a_1, a_2, \cdots, b_1, b_2, \cdots$, be any integers such that $a_i \neq b_i$. For $(\Delta, D) = 1$ let

$$P(\Delta, D, x; a_1, b_1, p_1; \cdots; a_r, b_r, p_r) = P(D, x; p_1, \cdots, p_r)$$

* The case $k = 0, M = 3$ is not included here but obviously $M = 3 = 1 + 1 + 1$.

† T. Estermann, Journal für die Reine und Angewandte Mathematik, vol. 168 (1932), pp. 106-116, has improved Rademacher’s results. For the problem which we are considering, however, Estermann’s method does not yield anything more.
denote the number of integers \( z \) which satisfy the conditions

\[
0 < z \leq x, \quad z \equiv \Delta \pmod{D}, \quad (z - a_i)(z - b_i) \not\equiv 0 \pmod{p_i}, \quad (i = 1, 2, \ldots, r).
\]

Then by R, (8) we have

\[
P(D, x; p_1, p_2, \ldots, p_r) > \frac{E}{D} x - R,
\]

where

\[
E = 1 - 2 \sum_{\alpha \leq r} \frac{1}{p_\alpha} + 4 \sum_{\alpha \leq r} \sum_{\beta < \alpha} \frac{1}{p_\alpha p_\beta} - \cdots - 2^{n+1} \sum_{\alpha \leq r} \sum_{\mu < r_n} \frac{1}{p_\alpha p_\beta \cdots p_\mu},
\]

\[
R = (2r + 1)(2r_1 + 1)^2 \cdots (2r_n + 1)^2, \quad r > r_1 > \cdots > r_n \geq 1.
\]

We now assume that the primes \( p_1, \ldots, p_r \) are the first \( r \) primes in order of any infinite set of primes which have the property that

\[
\sum_{\alpha \leq r} \frac{1}{p_\alpha} = \frac{1}{\alpha} \log \log w + c_1(\alpha) + o(1).
\]

Here \( \sum' \) or \( \prod' \) denotes the sum or product over all primes of the set which are \( \leq w \). From (7) and a general theorem on infinite series* it follows that

\[
\prod_{\alpha \leq r} \left(1 - \frac{2}{p_\alpha}\right) = \frac{c_2(\alpha)}{(\log w)^{2/\alpha}} + o\left(\frac{1}{(\log w)^{2/\alpha}}\right).
\]

If \( \alpha = 1 \), this reduces to the case treated by Rademacher.

Now let \( h \) and \( h_0 \) be any two numbers such that

\[
1 < h < h_0^\varepsilon, \quad 0 < 2 \log h_0 < 1.
\]

Then from (7) and (8) it follows that there is a number \( w_0 \) such that for all \( w \geq w_0 \) we have

\[
0 < \sum_{\alpha \leq r} \frac{1}{p_\alpha} < \log h_0,
\]

\[
\prod_{\alpha \leq r} \left(1 - \frac{2}{p_\alpha}\right) > \frac{1}{h_0^\varepsilon}.
\]

These are precisely the equations (15a) which are used in R. All the results obtained there go over to the case which we are considering. Thus from R, (18) and (26) we obtain

\[
E > \prod_{r=1}^{L} \left( 1 - \frac{2}{p_r} \right) \left\{ E_1 - h_0^2 \phi_2 - \frac{2h_0^4 \log^4 h_0 e^2(e^2-5)}{1 - e^2h_0^2 \log^2 h_0} \right\},
\]
\[
R < c_3 p_r^{(h+1)/(h-1)},
\]
where \(c_3\) depends only on \(\alpha, h, h_0, \) and \(E_1 > 1 - 2 \log h_0, \phi_2 < (10 \log^4 h_0)/3.\) If we take \(h_0 = 1.3\) we find that
\[
(9) \quad P(D; x; p_1, \ldots, p_r) > \frac{C}{D} \frac{x}{(\log p_r)^{2/\alpha}} - C' p_r^{(h+1)/(h-1)},
\]
where \(C\) and \(C'\) depend only on \(\alpha, h.\) It is this inequality which we use to prove Theorems 4 and 5.

7. The proof of Theorem 4. Let \(x\) in (6) be of the form \(4j+2.\) Consider the infinite set of primes \(p\) which are of the form \(4j+3.\) In this case we have*
\[
\sum_{\substack{3 \leq p \leq w \leq x \atop p \equiv 3 \pmod{4}}} \frac{1}{\phi} = \frac{1}{\phi(4)} \log \log w + c_1 + o(1).
\]
Then \(\alpha = 2\) and we may take \(h = 1.68 < (1.3)^2.\) From (9) we have
\[
(10) \quad P(D; x; p_1, \ldots, p_r) > \frac{2C}{3} \frac{x}{\log x} - C' x^{268/272}.
\]
Let \(p_1, p_2, \ldots, p_r\) be the primes 7, 11, \ldots up to the largest prime of the form \(4j+3\) which does not exceed \(x^{1/4}.\) We choose \(a_i\) and \(b_i\) in the following manner.
\[
a_i = 0, \quad b_i = x, \quad \text{if} \quad p_i \mid x;
\]
\[
a_i = 0, \quad b_i = 1, \quad \text{if} \quad p_i \nmid x.
\]
We choose \(\Delta\) so that \(\Delta = 1 \pmod{4}\) and so that neither \(\Delta\) nor \(x - \Delta\) is divisible by 3. Then \(\Delta\) is determined \(\pmod{12}.\) Using the fact that \(p_r \leq x^{1/4}\) the inequality (10) becomes
\[
P(12; x; p_1, \ldots, p_r) > \frac{2C}{3} \frac{x}{\log x} - C' x^{268/272}.
\]
Hence for \(x\) sufficiently large we have \(P(12; x; p_1, \ldots, p_r) \geq 1.\) Going back to the definition of \(P(12; x; p_1, \ldots, p_r)\) we see that this means that there is at least one integer \(z\) such that
\[
0 < z \leq x, \quad z \equiv \Delta \pmod{12}, \quad z(z - x) \neq 0 \pmod{p_i}, \quad p_i \mid x;
\]
\[
z(z - 1 - x) \neq 0 \pmod{p_i}, \quad p_i \nmid x.
\]

This shows that there is at least one integer \( z \) for which 
\[
x = z + (x - z),
\]
where neither \( z \) nor \( x-z \) is divisible by 2 or by any prime of the form \( 4j+3 \) which does not exceed \( x^{1/4} \). If a prime of the form \( 4j+3 \) does divide \( z \) or \( x-z \), then it must be greater than \( x^{1/4} \). This proves that not more than three primes of the form \( 4j+3 \) can divide \( z \) or \( x-z \). The number three can be reduced to two by the following argument. Both \( z \) and \( x-z \) are of the form \( 4j+1 \), but a product of three primes of the form \( 4j+3 \) is again of the form \( 4j+1 \). Therefore not more than two primes of the form \( 4j+3 \) can divide \( z \) or \( x-z \). This proves Theorem 4.

8. The proof of Theorem 5. The proof of this theorem is only slightly different from the proof of Theorem 4. We have

\[
\sum_{3 \leq p \leq w} \frac{1}{p} = \frac{2}{\phi(8)} \log \log w + 2c_1 + o(1),
\]
and again \( \alpha = 2 \), \( h = 1.68 \). This time we choose \( \Delta \) so that \( z \) has the following values (mod 8) and so that neither \( \Delta \) nor \( x-\Delta \) is divisible by 3.

\[
\begin{align*}
z & = 1, \quad x - z = 1 \quad \text{if} \quad x \equiv 2 \pmod{8}, \\
z & = 1, \quad x - z = 3 \quad \text{if} \quad x \equiv 4 \pmod{8}, \\
z & = 3, \quad x - z = 3 \quad \text{if} \quad x \equiv 6 \pmod{8}.
\end{align*}
\]

The inequality (10) then shows that not more than three primes of the form \( 8j+5 \) or \( 8j+7 \) can divide \( z \) or \( x-z \). An argument similar to that used in the proof of Theorem 4 shows finally that not more than two primes of the form \( 8j+5 \) or \( 8j+7 \) can divide \( z \) or \( x-z \). This completes the proof of Theorem 5.

* E. Landau, loc. cit.

The University of California, Berkeley, Calif.