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, $i \geqq 1$ is of the form $4j+1$. Let $r=3$, 4, 5, or 6. Then every integer $N \equiv r \pmod 4$, $N \geqq r$ 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 $2Kp_1^{2a_1} \cdots p_t^{2a_t}$, where $p_\nu \equiv 3 \pmod 4)$, $\nu = 1, 2, \cdots, t$, 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, $i\geqq 1$ is of the form $8j+1$ or $8j+3$. Then every odd integer $M\geqq 3$ is a sum of exactly three integers m_i and every even integer $M\geqq 4$ is a sum of exactly four integers m_i. The results for M odd and $M\equiv 0$ (mod 8) are the best possible.*

THEOREM 4. *Every sufficiently large integer $N\equiv 2$ (mod 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 $M\equiv 2, 4, 6$ (mod 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

$$k = \sum_{\nu=1}^{3} x_\nu^2 .$$

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

$$(1) \qquad 8j + 3 = \sum_{\nu=1}^{3} x_\nu^2 .$$

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

* E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, vol. I, pp. 550–555.

† 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 $8j+3$.

$$8j + 3 = \sum_{\nu=1}^{3} (2s_\nu + 1)^2,$$

$$N = 4j + 3 = \sum_{\nu=1}^{3} \left\{ s_\nu^2 + (s_\nu + 1)^2 \right\}.$$

Obviously s_ν and $s_\nu+1$ have no common factor and are not both odd. Hence by Lemma 2 every prime factor of the integer $S_\nu^2+(S_\nu+1)^2$ is of the form $4j+1$. 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

$$N \equiv \sum_{j=1}^{s} n_{i_j} \pmod 4 \tag{2}$$

has no solution when $s<r$. Therefore the equation

$$N = \sum_{j=1}^{s} n_{i_j} \tag{3}$$

certainly has no solution when $s<r$.

When $r=5$ we consider the set of all integers $N=p_1^{2a_1}\cdots p_t^{2a_t}$, where every p_ν is of the form $4j+3$. 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 $2Kp_1^{2a_1}\cdots p_t^{2a_t}$, where $p_\nu\equiv 3 \pmod 4$ and every prime factor of K is of the form $4j+1$, there exist integers u and v such that*

$$8j + 2 = u^2 + v^2. \tag{4}$$

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

$$8j + 2 = 2\left\{ y^2 + (y + 1)^2 + z^2 + (z + 1)^2 \right\} - 2,$$

$$N = 4j + 2 = y^2 + (y + 1)^2 + z^2 + (z + 1)^2.$$

Every prime factor of $y^2+(y+1)^2$ and $z^2+(z+1)^2$ is of the form $4j+1$ and this completes the proof.

---

* E. Landau, loc. cit., pp. 549–550.

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 (mod 16) then $2k-21\equiv 3$ or 11 (mod 16). Then*

$$(5) \qquad \begin{aligned} 2k - 21 &= \sum_{i=1}^{3} x_i^2, \\ 2k + 3 &= \sum_{i=1}^{3} (x_i^2 + 8). \end{aligned}$$

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

If $k\equiv 7$ or 15 (mod 16) then $2k-3\equiv 11$ (mod 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

$$(6) \qquad 0 < z \leqq x,\ z \equiv \Delta \pmod{D}, \qquad (z - a_i)(z - b_i) \not\equiv 0 \pmod{p_i}, \qquad (i = 1, 2, \cdots, r).$$

Then by R, (8) we have

$$P(D, x; p_1, p_2, \cdots, p_r) > \frac{E}{D}x - R,$$

where

$$E = 1 - 2\sum_{\alpha\leqq r}\frac{1}{p_\alpha} + 4\sum_{\alpha\leqq r}\sum_{\substack{\beta\leqq r_1\\ \beta<\alpha}}\frac{1}{p_\alpha p_\beta} - \cdots - 2^{2n+1}\sum_{\alpha\leqq r}\cdots\sum_{\substack{\mu<r_n\\ \mu<\cdots<\beta<\alpha}}\frac{1}{p_\alpha p_\beta\cdots p_\mu},$$

$$R = (2r + 1)(2r_1 + 1)^2 \cdots (2r_n + 1)^2, \qquad r > r_1 > \cdots > r_n \geqq 1.$$

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

$$(7) \qquad \sum_{3\leqq p\leqq w}{}' \frac{1}{p} = \frac{1}{\alpha}\log\log w + c_1(\alpha) + o(1).$$

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

$$(8) \qquad \prod_{3\leqq p\leqq w}{}' \left(1 - \frac{2}{p}\right) = \frac{c_2(\alpha)}{(\log w)^{2/\alpha}} + o\left(\frac{1}{(\log w)^{2/\alpha}}\right).$$

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

Now let h and h_0 be any two numbers such that

$$1 < h < h_0^\alpha, \qquad 0 < 2\log h_0 < 1.$$

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

$$0 < \sum_{w<p\leqq w^h}{}' \frac{1}{p} < \log h_0,$$

$$\prod_{w<p\leqq w^h}{}' \left(1 - \frac{2}{p}\right) > \frac{1}{h_0^2}\cdot$$

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

* K. Knopp, *Theorie und Anwendung der Unendlichen Reihen*, page 218.

$$E > \prod_{\nu=1}^{r}\left(1 - \frac{2}{p_\nu}\right)\left\{E_1 - h_0^2\,\Phi_2 - \frac{2h_0^4 \log^6 h_0\, e^2(e^2-5)}{1 - e^2h_0^2 \log^2 h_0}\right\},$$

$$R < c_8 p_r^{(h+1)/(h-1)},$$

where c_8 depends only on α, 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

$$P(D, x; p_1, \cdots, p_r) > \frac{C}{D}\,\frac{x}{(\log p_r)^{2/\alpha}} - C'p_r^{(h+1)/(h-1)}, \tag{9}$$

where C and C' depend only on α, 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*

$$\sum_{\substack{3 \leqq p \leqq w \\ p \equiv 3 \pmod 4}} \frac{1}{p} = \frac{1}{\phi(4)} \log\log w + c_1 + o(1).$$

Then $\alpha = 2$ and we may take $h = 1.68 < (1.3)^2$. From (9) we have

$$P(D, x; p_1, \cdots, p_r) > \frac{C}{D}\,\frac{x}{\log p_r} - C'p_r^{268/68}. \tag{10}$$

Let $p_1, p_2, \cdots, p_r$ be the primes $7, 11, \cdots$ 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.

$$a_i = 0, \qquad b_i = x, \qquad \text{if} \qquad p_i \nmid x;$$
$$a_i = 0, \qquad b_i = 1, \qquad \text{if} \qquad p_i \mid x.$$

We choose Δ so that $z \equiv 1 \pmod 4$ and so that neither Δ nor $x - \Delta$ is divisible by 3. Then Δ is determined (mod 12). Using the fact that $p_r \leqq x^{1/4}$ the inequality (10) becomes

$$P(12, x; p_1, \cdots, p_r) > \frac{2C}{3}\,\frac{x}{\log x} - C'x^{268/272}.$$

Hence for x sufficiently large we have $P(12, x; p_1, \cdots, p_r) \geqq 1$. Going back to the definition of $P(12, x; p_1, \cdots, p_r)$ we see that this means that there is at least one integer z such that

$$0 < z \leqq x, \qquad z \equiv \Delta \pmod{12}, \qquad \begin{array}{ll} z(z-x) \not\equiv 0 \pmod{p_i}, & p_i \nmid x; \\ z(z-1-x) \not\equiv 0 \pmod{p_i}, & p_i \mid x. \end{array}$$

---

* E. Landau, loc. cit., pp. 449–450.

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 $4j+3$. 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*

$$\sum_{\substack{3\leqq p\leqq w \\ p\,\equiv\,5 \text{ or } 7 \pmod 8}} \frac{1}{p} = \frac{2}{\phi(8)} \log\log w + 2c_1 + o(1),$$

and again $\alpha=2$, $h=1.68$. This time we choose Δ so that z has the following values (mod 8) and so that neither Δ nor $x-\Delta$ is divisible by 3.

$$\begin{array}{llll} z \equiv 1, & x - z \equiv 1 & \text{if} & x \equiv 2 \pmod 8, \\ z \equiv 1, & x - z \equiv 3 & \text{if} & x \equiv 4 \pmod 8, \\ z \equiv 3, & x - z \equiv 3 & \text{if} & x \equiv 6 \pmod 8. \end{array}$$

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.