EXTENSIONS OF WARING'S THEOREM ON FOURTH POWERS*

BY L. E. DICKSON

1. *Introduction.* In 1770 Waring conjectured that every positive integer p is a sum of nineteen integral biquadrates. It is shown in § 8 that eight of them may be taken equal if $p \leqq 4100$. Again, sixteen of them may be taken equal in pairs if $p \leqq 2400$. All possible similar results are included in Theorem 1 of § 3.

2. *Notations and Definitions.* The form

$$(1) \qquad (a_1, \cdots, a_n) = a_1x_1^4 + \cdots + a_nx_n^4, \qquad (0 < a_1 \leqq a_2 \leqq a_3 \cdots),$$

is said to be of *order* n and *weight* $a_1+a_2+ \cdots +a_n$. Since $ax^4 = x^4+ \cdots +x^4$, to a terms, a form of weight w is equal to a sum of w biquadrates. But 79 is not a sum of fewer than nineteen biquadrates. Hence 19 is the minimum weight of a form (1) which represents all positive integers.

Let f be a form (1) which represents p, and let $a_1 = r+s$. The form $g = (r, s, a_2, \cdots, a_n)$ shall be said to be derived from f by the *partition* of a_1 into $r+s$. If we give to the first two variables in g the same value x_1 as was employed in $f = p$, we see that also g represents p. Hence *any form derived from f by partition represents every integer which can be represented by f* (and usually represents further integers).

Write $a = 2^4$, $b = 3^4$, $c = 4^4$, $\cdots$. If a positive integer m can be expressed as a linear combination of $1, a, b, \cdots$, with integral coefficients $\geqq 0$ whose sum is $\leqq 19$, in one and only one way, m shall be called a *simple* number. In case there are exactly two such expressions, m shall be called a *double* number. Similarly for a *triple* or *k-fold* number.

* Presented to the Society, December 31, 1926.

For example, $19=3+a$ is a double number, while $4+a$ is a simple number.

We write 1_2 for 1, 1; and 1_s for s ones.

3. *Summary of Results.*

THEOREM 1. *If a form of weight* 19 *represents all positive integers, it is* $A=(1122337)$, $B=(1122346)$, $C=(11112238)$, $D=(11112247)$, *or* $E=(11122228)$, *or a form derived from one of the five by partition.*

It is proved* in §§ 6, 7 that both A and B (of the minimum order 7) represent every positive integer $p\leqq 7^4=2401$. A like method was used to verify that D represents every $p\leqq 1300$, and that $F=(1122238)$ represents every $p\leqq 2000$ except the four-fold number

$$443 = 9 + a + 2b + c = 10 + 6a + b + c$$
$$= 6 + 2a + 5b = 7 + 7a + 4b.$$

The partitions $2=1+1$ and $3=1+2$ of F give C and E, respectively, and they represent $1+8+a+2b+d$. Hence C and E both represent every $p\leqq 2000$.

A form is evidently more likely to represent the integers just exceeding a given biquadrate than those just preceding it. As an excellent further check, it was verified that A, B, and F each represent 4000 up to $4096=8^4$. The same is therefore true of C and E.

4. *Conditions that a Form of Weight* 19 *shall Represent all Integers.* Let such a form f have the notation (1). Then

$$a_1 + a_2 + \cdots + a_n = 19. \tag{2}$$

To prove that

$$a_k \leqq 1 + a_1 + a_2 + \cdots + a_{k-1} \qquad (k = 2, \cdots, n), \tag{3}$$

write s for $a_1+\cdots+a_{k-1}$ and suppose that $a_k>1+s$. For $i=1,\cdots,k-1$, partition a_i into as many ones. Thus a

[*] Mr. K. C. Yang kindly extended my computations from 2000 to 2400 for A and B, and from 1000 to 1300 for D and E.

partition of f is $(1_s, a_k, \cdots, a_n)$, which does not represent $1+s$. The latter is a simple number since $19 \geqq s+a_k > 1+2s$, whence $1+s<10$.

Since f represents 1, $a_1=1$. By (3) with $k=2$, $a_2 \leqq 2$. If $a_2=2$, f would not represent the simple number $110=13+a+b$. Apply (3) with $k=3$. Hence

$$a_1 = 1, \quad a_2 = 1, \quad a_3 \leqq 3. \tag{4}$$

If $a_n \geqq 9$, a partition of f is $(1_{10}, 9)$ which does not represent the simple number $8+3a$. Hence

$$a_n \leqq 8. \tag{5}$$

By (2), (4), (5), we see that $n>4$.

If $a_{n-1}>4$, a partition of f is $(1_9, 5, 5)$, which does not represent the simple number $235=9+4a+2b$, since 9 is not a sum of certain of (1, 1, 1, 5, 5). Hence

$$a_{n-1} \leqq 4. \tag{6}$$

If $a_{n-2}>3$, a partition of f is $G=(1_7, 4, 4, 4)$. But G does not represent the simple number $221=11+3a+2b$, since 11 is not a sum of certain of (1, 1, 4, 4, 4). Hence

$$a_{n-2} \leqq 3. \tag{7}$$

Let $(111a_4 \cdots)$ with $a_4>2$ represent the simple number $15+2a$. Then 15 is a sum of certain of $1, a_4, \cdots, a_n$, contrary to $a_4+\cdots+a_n=19-3=16$, $a_i \geqq 3$.

Let $(113 \cdots)$ represent $15+2a$. Then 15 is a sum of certain of $(3, a_4, \cdots, a_n)$, contrary to $a_4+\cdots+a_n=14$, $a_i \geqq 3$.

These two results and (4) give

$$a_3=1 \text{ or } 2. \text{ If } a_3=1, \text{ then } a_4=1 \text{ or } 2. \tag{8}$$

The following forms are excluded:

$$(1_5,3,3,3,5), \quad (1_5,3,3,4,4), \quad (1_4,3_5), \quad (1_2,2_6,5). \tag{9}$$

No one of the first three represents the simple number $207=13+2a+2b$. The fourth does not represent the simple number $141=12+3a+b$.

A partition of $(1_7, 4, 8)$ is G above (7). Partitions of $(1_5, 3, 3, 8)$ and $(1_5, 3, 4, 7)$ give the first and second forms (9) respectively. This proves

(10) f does not end with 4, 8, or 3, 3, 8, or 3, 4, 7.

Let $a_{n-3}>2$. By (7), $a_{n-3}=a_{n-2}=3$. By (6), $a_{n-1}=3$ or 4. In the second case, a partition gives (9_2). If, in the first case, $a_n \geqq 5$, a partition gives (9_1). This proves

(11) If $a_{n-3}>2$, then $a_{n-3}=a_{n-2}=a_{n-1}=3$, $a_n=3$ or 4.

5. *Proof of Theorem* 1. If $n=5$, (4)–(6) give

$$a_1 + \cdots + a_5 \leqq 1 + 1 + 3 + 4 + 8 = 17,$$

contrary to (2). Next, let $n=6$. If $a_3=1$, (4)-(7) give

$$a_1 + \cdots + a_6 \leqq 1 + 1 + 1 + 3 + 4 + 8 = 18,$$

contrary to (2). Hence $a_3=2$. By (2), (5)-(7),

$$19 - 4 = a_4 + a_5 + a_6, \quad a_4 \leqq 3, \quad a_5 \leqq 4, \quad a_6 \leqq 8,$$

whence the three signs are all =. By (10), the ending 4, 8 is excluded. Hence $n \geqq 7$.

Let $n=7$. By (5)-(7), $a_5 \leqq 3$, $a_6 \leqq 4$, $a_7 \leqq 8$. If $a_3=a_4=1$, (2) gives $f=(1111348)$, which is excluded by (10). Next, let $a_3=1$, $a_4=2$. Then $a_5+a_6+a_7=19-5=14$, whence the sets of values of a_5, a_6, a_7 are 2, 4, 8; 3, 3, 8; 3, 4, 7, all excluded by (10). By (8), there remains only the case $a_3=2$. If $a_4>2$, (11) contradicts (2). Hence $a_4=2$, $a_5+a_6+a_7=13$. If $a_5=3$, f is A or B. If $a_5=2$, f is either (1122247), a partition of which gives the fourth excluded form (9), or else (1122238), the least number not represented by which is the quadruple number

$$443 = 9 + a + 2b + c = 10 + 6a + b + c$$
$$= 6 + 2a + 5b = 7 + 7a + 4b.$$

Let $n=8$. By (5)-(7), $a_6 \leqq 3$, $a_7 \leqq 4$, $a_8 \leqq 8$.

First, let $a_3=1$. Then $a_4 \leqq 2$ by (8). If $a_5>2$, (11) gives $a_5+a_6+a_7+a_8=12$ or 13, while $a_1+a_2+a_3+a_4 \leqq 5$, contrary to the relation (2). Hence we find $a_5 \leqq 2$. If $a_4=2$, then

$a_5=2$, $a_6+a_7+a_8=19-7=12$. The sets of values of a_6, a_7, a_8 are 2, 2, 8; 2, 3, 7; 2, 4, 6; 3, 3, 6; 3, 4, 5. The first gives E. For the second, f is derived from A by the partition $3=1+2$. For the last three sets, f is a partition of B. Finally, let $a_4=1$. If $a_5=2$, the sets of values of a_6, a_7, a_8 are 2, 3, 8; 2, 4, 7; 3, 3, 7; 3, 4, 6. The first two give C and D. The last two yield partitions $2=1+1$ of A and B. If $a_5=1$, the sets are 2, 4, 8; 3, 3, 8; 3, 4, 7, which are excluded by (10).

Second, let $a_3=2$. If $a_4\geqq 3$, f is evidently $(1, 1, 2, 3_5)$, a partition of which is the third excluded form (9). Hence $a_4=2$. If $a_5>2$, f is evidently the partition (11223334) of A. There remains the case $f=(11222a_6a_7a_8)$. The sets of values of a_6, a_7, a_8 are 2, 2, 7; 2, 3, 6; 2, 4, 5; 3, 3, 5; 3, 4, 4. For the first and third sets, the partitions $7=2+5$ and $4=2+2$ respectively yield the fourth excluded form (9). For the second and last sets, f is a partition of B. For the fourth set, f is a partition of A.

Let $n=9$. By (5)-(7), $a_7\leqq 3$, $a_8\leqq 4$, $a_9=8$.

First, let $a_6>2$. By (11), $a_6=a_7=a_8=3$, $a_9=3$ or 4. We get the third excluded form (9) and the partitions $(1_4, 2, 3_3, 4)$ and $(1_3, 2_2, 3_4)$ of A.

Second, let $a_6=1$. Since the ending 4, 8 is excluded, f is evidently one of the partitions $(1_6, 2, 3, 8)$, $(1_6, 2, 4, 7)$, $(1_6, 3, 3, 7)$, $(1_6, 3, 4, 6)$ of C, D, A, B, respectively.

Finally, let $a_6=2$. If $a_5=1$, the symbol for f contains 1_5 and 2, followed by 2, 2, 8; 2, 3, 7; 2, 4, 6; 3, 3, 6; or 3, 4, 5. Thus f is a partition of C, A, B, A, or B, respectively. For $a_5=2$, $a_4=1$, f contains 1_4 and 2_2, followed by 2, 2, 7; 2, 3, 6; 2, 4, 5; 3, 3, 5; or 3, 4, 4, and is a partition of A or B. For $a_5=a_4=2$, $a_3=1$, f contains 1_3 and 2_3, followed by 2, 2, 6; 2, 3, 5; 2, 4, 4; or 3, 3, 4, and is a partition of B. There remains only the case in which f contains 1_2 and 2_4, followed by 2, 2, 5; 2, 3, 4; or 3, 3, 3. The first yields the fourth excluded form (9). The last two yield partitions of B.

Let $n\geqq 10$. The forms which satisfy (2), (5)-(7), and $a_1=a_2=1$ are all partitions of A, B, C or D. We subdivide cases according to the number of 1's in the symbol. For example if $n=10$, the first case yields only $(1_8, 3, 8)$ and $(1_8, 4, 7)$.

6. *Forms related to B.* The tables employed extend to $7^4=2401$. To the sums of two biquadrates we add the double of each such sum, and obtain a table α of all integers <2401 which are represented by (1122). To each number in α we add the triples of biquadrates and obtain a table β of all integers <2401 which are represented by (11223). To each number in β we add the quadruples of biquadrates and obtain the following table γ of all integers <2401 which are represented by (112234):

0–13, 16–28, 32–43, 48–58, 64–73, 80–93, 96–106, 108, 112–23, 128–38, 144–53, 160–73, 176–88, 192–203, 208–18, 225–33, 241–53, 256–68, 272–83, 288–98, 304–13, 320–33, 336–48, 352–63, 368–78, 384–93, 400–13, 416–28, 432–43, 448–58, 465–73, 481–93, 498–508, 512–23, 528–38, 544–53, 560–73, 576–88, 592–603, 608–18, 624–37, 639–53, 656–68, 672–83, 688–98, 705–15, 717, 721–33, 737–48, 753–63, 768–78, 784–97, 800–13, 816–28, 832–43, 848–58, 864–77, 880–93, 896–908, 912–23, 928–38, 945–57, 961–70, 972–3, 977–88, 993–1003, 1009–18, 1024–37, 1040–50, 1052–3, 1056–68, 1072–83, 1088–98, 1104–17, 1120–30, 1132, 1136–48, 1152–63, 1168–78, 1185–97, 1201–10, 1212, 1217–28, 1233–43, 1249–61, 1265–77, 1280–92, 1296–1308, 1312–23, 1328–41, 1344–57, 1360–72, 1376–88, 1392–1403, 1408–21, 1424–33, 1435–7, 1440–8, 1450–52, 1456–68, 1472–83, 1488–1501, 1505–17, 1521–32, 1536–48, 1552–63, 1568–81, 1584–97, 1600–12, 1616–28, 1632–43, 1648–61, 1664–76, 1680–88, 1690–1, 1696–1708, 1713–23, 1728–41, 1745–56, 1761–72, 1777–88, 1792–1803, 1808–21, 1824–36, 1840–51, 1856–68, 1872–85, 1888–1901, 1904–16, 1920–32, 1934, 1936–48, 1952–65, 1968–81, 1985–96, 1998, 2000–11, 2017–28, 2033–45, 2048–61, 2064–76, 2080–92, 2096–2106, 2108, 2112–25, 2128–41, 2144–56, 2160–72, 2176–88, 2192–2205, 2208–20, 2225–36, 2241–52, 2257–66, 2268, 2273–85, 2290–2300, 2304–16, 2320–32, 2336–46, 2352–65, 2368–80, 2384–95, 2400.

THEOREM 2. *$B_m = (112234m)$ represents all positive integers $\leqq 2400$ if and only if $m = 6, 7, 8, 9$.*

The numbers in table γ together with the numbers obtained by adding 6 to them give all numbers $\leqq 2400$ except $p = 240$, 480, and $q = 1455$. Each $p - 6 \cdot 2^4$ and $q - 6 \cdot 3^4$ is in γ. This proves Theorem 2 when $m = 6$.

For $m = 7$, 8, or 9, the numbers in γ together with the numbers obtained by adding m to them give all numbers $\leqq 2400$.

The least positive integer not represented by B_m is 234, 74, 59, 44, 29, 14 when $m = 10$, 11, 12, 13, 14, $m > 14$, respectively.

7. *Forms related to A.* To each number in table β(§ 6) we add the triples of biquadrates and obtain the following table δ of all integers < 2401 which are represented by (112233):

0–12, 16–27, 32–42, 48–57, 64–72, 80–92, 96–105, 112–22, 128–37, 144–52, 160–72, 176–87, 192–202, 209–17, 225–32, 241–52, 256–67, 272, 274–82, 288–97, 304–12, 320–32, 336–47, 352–62, 368–77, 384–92, 400–2, 404–12, 416–27, 432–42, 449–57, 465–72, 482, 484–92, 497–507, 512–22, 528–37, 544–52, 560–72, 576–87, 592–602, 608–12, 614–7, 624–36, 640–52, 656–67, 672–82, 689–97, 705–14, 716, 721–7, 729–32, 737–47, 753–62, 768–77, 784–96, 800–12, 816–27, 832–42, 848–57, 864–76, 880–9, 891–2, 896–907, 912–22, 929–37, 945–56, 961–8, 971–2, 977–87, 993–1002, 1009–17, 1024–36, 1040–9, 1051, 1056–63, 1065–7, 1072–82, 1088–97, 1104–16, 1120–9, 1131, 1136–47, 1152–62, 1169–77, 1185–96, 1201–8, 1211, 1217–24, 1226, 1233–7, 1240–2, 1249–60, 1265–76, 1280–91, 1296–1307, 1312–22, 1328–40, 1344–56, 1360–7, 1369–71, 1376–87, 1392–1401, 1408–20, 1424–32, 1434–6, 1440–8, 1450–1, 1456–67, 1472–82, 1489–1500, 1505–16, 1521–31, 1536–47, 1552–62, 1568–80, 1584–93, 1595, 1600–7, 1609–10, 1616–27, 1632–42, 1648–60, 1664–5, 1667–72, 1674–5, 1680–7, 1690–1, 1697–1707, 1712–22, 1729–40, 1745–7, 1749–55, 1761–70, 1778–87, 1792–1802, 1808–20, 1824–7, 1829–33, 1835, 1840–7, 1849–50, 1856–67, 1872–84, 1888–1900, 1904–15, 1920–31, 1934, 1936–47, 1952–64, 1969–77, 1979–80, 1982, 1985–95, 2001–10, 2017–25, 2027, 2033–44, 2048–60, 2064–75, 2080–91, 2096–2107, 2112–24, 2128–39, 2144–55, 2160–71, 2176–7, 2179–85, 2187, 2192–2204, 2209–19, 2225–35, 2241–51, 2257–65, 2274–84, 2290–9, 2304–14, 2320–31, 2336–45, 2352, 2354–64, 2368–79, 2384–5, 2387–94, 2400.

We may now readily verify that $A=(1122337)$ represents all positive integers <2401. The numbers in δ together with the numbers obtained by adding 7 to them give all integers <2401 except

p = 240, 403, 480–1, 483, 613, 976, 1216, 1232,
1238–9, 1673, 1696, 1748, 1828, 2273, 2353;
q = 620, 735, 1071, 1245–6, 1375, 1615, 1695, 1855.

Each $p-7\cdot 2^4$ and $q-7\cdot 3^4$ is in δ.

Finally, $(112233m)$ fails to represent 621, 622, 73, 58, 43, 13 when $m=8$, 9, 10, 11, 12, $m\geqq 13$, respectively.

THEOREM 3. *The form* $(112233m)$ *represents all positive integers* <2401 *if and only if* $m=7$.

8. THEOREM 4. *Every positive integer* $\leqq 4100$ *can be expressed in the form* $S+8x^4$, *where S is a sum of eleven integral biquadrates, and* $x=0$, 1, *or* 2.

At the suggestion of Jacobi, Bretschneider* gave a Table 1 of all those decompositions of 1, · · · , 4100 into biquadrates >0 for which the number of the latter is a minimum. From it† we conclude that all numbers $\leqq 4100$ are sums of eleven biquadrates $\geqq 0$, except

(12) 12–15, 27–31, 42–47, 57–63, · · · , 4091–5.

* Journal für Mathematik, vol. 46 (1853), pp. 1–23.

† Or by taking the aggregate of the numbers in Parts XI–XVIII of his Table 2, which lists the integers which are sums of a prescribed number of biquadrates >0.

If p occurs in the set (12), $p-8$ is not in it except for $p=232$, 240, 472, 480. For these four, $p-8\cdot 2^4$ is not in the set (12). This proves Theorem 4.

9. Corresponding results for cubes are obtained in the writer's paper in the American Mathematical Monthly for April, 1927. Assistance has been provided by the Carnegie Institution for the more elaborate investigation of fifth and higher powers.

THE UNIVERSITY OF CHICAGO

TESTS FOR PRIMALITY BY THE CONVERSE OF FERMAT'S THEOREM*

BY D. H. LEHMER

There are, generally speaking, two distinct methods for determining the primality of a large integer without trying possible divisors. Up to this time the method which goes by the name of Lucas' test† has yielded the most results. It is particularly well adapted to the investigation of Mersenne numbers and has consequently led to the identification of the three largest primes heretofore known, namely, $2^{89}-1$, $2^{107}-1$ and $2^{127}-1$. The other method is based on the converse of Fermat's theorem. It is the purpose of this paper to discuss certain improvements in this method, and to apply it to some numbers of the form $10^n \pm 1$.

It has long been known that the simple converse of Fermat's theorem, namely: *If* $a^x \equiv 1 \pmod{N}$ *for* $x=N-1$, *then* N *is a prime*, is *not* true, as is shown by the simple example: $4^{14} \equiv 1 \pmod{15}$. A true converse of this theorem was first given by Lucas‡ in 1876: *If* $a^x \equiv 1 \pmod{N}$ *for* $x=N-1$, *but not for* $x<N-1$, *then* N *is a prime.* In 1891 he proved the following theorem.§

* Presented to the Society, San Francisco Section, April 2, 1927.

† American Journal, vol. 1 (1878), pp. 184–220.

‡ Lucas, loc. cit., p. 302.

§ *Théorie des Nombres*, 1891, pp. 423, 441.