THE WARING PROBLEM AND ITS GENERALIZATIONS*

BY L. E. DICKSON

1. *Historical Background.* The past year has witnessed greater advances in the field which is the title of this paper than were made during the whole of its previous long history.

Additive number theory had its origin exactly 300 years ago in Fermat's assertion that he was the first to discover the general theorem that every integer is a sum of three triangular numbers, also is a sum of four squares, also is a sum of five pentagonal numbers, and so on to infinity. Here a triangular number $x(x+1)/2$ counts the number of equal spheres arranged in the form of a triangle with x spheres at the base. The proof which he claimed to possess was never published. Cauchy was the first to publish a complete proof in 1813.

In 1659, Fermat stated that his proof of the 4-square theorem was by descent; namely, any integer is a sum of 4 squares provided a certain smaller integer is such. Recently† there was published such a proof, no detail of which was beyond Fermat. The first published proof was that by Lagrange in 1770.

In the same year, Waring conjectured that every positive integer is a sum of 9 integral cubes, positive or zero, also is a sum of 19 fourth powers, and so on. His assertions were certainly empirical, based on short tables.

About 1772, J. A. Euler (son of the celebrated L. Euler) stated that, in order to express every positive integer as a sum of positive nth powers, at least I terms are necessary, where

$$(1) \qquad I = 2^n + q - 2, \qquad q = [(3/2)^n],$$

where, as usual, the notation $[x]$ denotes the largest integer $\leq x$. He doubtless knew that we must add I powers 1 or 2^n to obtain the sum $2^n q - 1$. For example, we need 4 squares, 9 cubes, 19 fourth powers, 37 fifth powers, and so on.

---

† Dickson, American Journal of Mathematics, vol. 46 (1924), p. 2.

2. *Asymptotic Theory.* The pioneer work was that by Hardy and Littlewood in 1919–1927. Let $G(n)$ denote the least integer s such that every sufficiently large integer is a sum of s integral nth powers, each ≥ 0. Their initial result was

$$G(n) \leq (n - 2)2^{n-1} + 5,$$

whence it suffices to use 9 cubes, 21 fourth powers, 53 fifth powers, and so on. In 1925, they found for $n \geq 4$ the lower result

$$(2) \qquad G(n) \leq (n - 2)2^{n-2} + n + 5 + \zeta_n,$$

where ζ_n is a relatively small function $< n^2 \log_e 2$. Their earlier 53 fifth powers are now replaced by 41.

In 1934, Vinogradow* gave $G(n) < 32(n \log_e n)^2$. He† soon obtained the astonishing result that, if $n \geq 4$,

$$(3) \qquad G(n) \leq 4n + 3k, \qquad k = [2n \log_e n + n \log_e 6].$$

This exceeds the former result given by (2) if $n = 4$, 5, or 6, but is a decided improvement if $n \geq 7$. For example, if $n = 17$, the formula (3) gives 448, in contrast with the value 491711 given by (2).

Later I supplied details‡ for Vinogradow's proof, evaluated all the constants, and proved that if

$$(4) \qquad \log_{10} \log_{10} N > 0.6621n^2, \qquad (n \geq 10),$$

every integer $\geq N$ is a sum of nth powers whose number is given by (3).

3. *Ideal Waring Theorem.* The ideal Waring theorem states that every positive integer is a sum of I integral nth powers ≥ 0, for I in (1), or technically, $g(n) = I$.

Early in 1935, I proved by use of (4) the ideal Waring theorem when $n = 11$, 12, 13, 14, 15, 17, while Zuckerman proved it independently when $n = 14$-20. When $n \geq 21$, I and hence $g(n)$ exceeds 2 million, so that there seems to be little satisfaction in knowing the exact value of the large number $g(n)$, which is already known to be finite.

＊ Comptes Rendus de l'Académie des Sciences, URSS, vol. 2 (1934), pp. 337–341.

† Annals of Mathematics, vol. 36 (1935), pp. 395–405.

‡ Annals of Mathematics, vol. 37 (1936), pp. 293–316. With extension to sums of nth powers multiplied by any given positive integers.

4. *Solution of Waring's Problem.* An essential step was a material lowering of the constant given by (4). The largeness of the constant given by (4) was due mainly to the approximation to the number of the divisors of an integer. This divisor function is entirely avoided in a new treatment[*] of the final part of the asymptotic theory, which shows that, if

$$(5) \qquad\qquad \log_{10} N = 2n^7, \qquad\qquad (n \geqq 9),$$

every integer $\geqq N$ is a sum of $M = 4n - 2 + 6k$ integral nth powers. Here $M < I$. It remains to prove that every positive integer $< N$ is a sum of I nth powers. To indicate the general nature of this proof, note that if every integer J between E and $E + 2^n$ is known to be a sum of m nth powers, then every integer between $E + 2^n$ and $E + 2 \cdot 2^n$ can be expressed in the form $J + 2^n$ and hence is a sum of $(m+1)$ nth powers. We readily compute m when $E = 2^n q$, so that our initial interval contains 3^n. Hence the preceding fact shows that all integers between $2^n q$ and $2^n q + 3^n$ are sums of $m + q$ nth powers. Then all integers on to $2^n q + 2 \cdot 3^n$ are sums of $m + q + 1$ powers, and so on. After making a certain number of such single ascents, we reach a point for which we may make a general number of ascents at one step by use of a general formula[†] involving logarithms. In this way I obtained the following result.

THEOREM 1. *Let* $3^n = 2^n q + r$, $0 < r < 2^n$. *If* $n > 6$ *and*

$$(6) \qquad\qquad 2^n \geqq q + r + 3,$$

then $g(n) = I$ *(that is, the ideal Waring theorem holds).*

This inequality holds if $4 \leqq n \leqq 400$. If it should fail for any $n > 400$, then the decimal for $r/2^n$ would begin with at least 50 figures 9. Below 400, it begins with two 9's only when $n = 157$ and $n = 163$, and for both the third figure is less than 9.

Although (6) will rarely, if ever, fail, I have proved also the following fact.

THEOREM 2. *If* (6) *fails, write* $f = [(4/3)^n]$. *Then* $g(n) = I + f$ *or* $I + f - 1$, *according as* $2^n =$ *or* $< fq + f + q$.

Theorem 1 for $n \geq 8$, but not Theorem 2, was obtained independently by S. S. Pillai.* Now that Waring's problem has been solved when $n \geq 6$, it is natural to undertake the following two direct generalizations.

5. *First Generalization.* Define $g(n, m)$ so that every integer $\geq m$ is a sum of g nth powers, while not every integer $\geq m$ is a sum of $g - 1$ powers. Thus $g(n, 0) = g(n, 1) = g(n)$.

While $g(12) = 4223$, I proved† that $g(12, 2 \cdot 3^{12}) = 2405$, $g(12, 3 \cdot 3^{12}) = 1560$, $g(12, 8^{12} + 7^{12} + 2 \cdot 5^{12}) \leq 440$. Also,‡ $g(14, 4^{14}) = 5184 < I/3$, and so on. I obtain§ many such results for $n = 9$ and $n = 11$.

6. *Second Generalization.* I shall now announce‖ remarkable new results.

THEOREM 3. *Let $d = 1$ or 2, according as q is odd or even. If $9 \leq n \leq 400$, every positive integer is a sum of $4n + 2 - d$ integral nth powers ≥ 0 and the doubles of $P = \frac{1}{2}(2^n + q - 4n + d) - 2$ such powers. Here $4n + 2 - d + 2P = I$. Expressed otherwise, in the ideal Waring theorem we may take $2P$ of the powers equal in pairs.*

We have therefore reduced the number of variables or summands from I to $I - P$. Except for small n's, $I - P$ just exceeds $I/2$.

Similar theorems reduce the number of summands from I to approximately I/a, for any integer a that is not too large.

THEOREM 4. *If $a \leq 4n$, $16 \leq n \leq 400$, every positive integer is a sum of $m = 4n + 2an$ integral nth powers ≥ 0 and the a-tuples of $\{ (I - m)/a \} - 2$ powers, where $\{ x \}$ denotes the least integer $\geq x$.*

THEOREM 5. *If $a = 3$ or 4, $11 \leq n \leq 400$, Theorem 4 holds with $m = 4n$.*

Evident corollaries are obtained from Theorems 4 and 5 by partitioning each a into arbitrary positive integral parts, which may differ for the various a's. For example, $5x^n = 3x^n + 2x^n$.

---

* Journal of the Indian Mathematical Society, vol. 2 (1936), pp. 16–44.

† Duke Mathematical Journal, vol. 2 (1936), pp. 192–204.

‡ Monatshefte für Mathematik und Physik, vol. 43 (1936), pp. 391–400.

§ This Bulletin, vol. 42 (1936), pp. 525–529.

‖ To appear in volume 2 of Acta Arithmetica.

In the proof of these theorems for the small values of n, it was necessary to resort to facts obtained by tables. It is an interesting and economical fact that we need not construct tables of sums of values of these new functions involving a, but that we may derive the necessary information from published tables of sums of values of x^n. In fact, I prove the following theorem.

THEOREM 6. *For $g^n \leq E < 2g^n$, let all integers in the interval $K = (E, E+P)$ be sums of h integral nth powers ≥ 0. Then all integers in the same interval K are sums of $(g-1)(a-1)+1$ integral nth powers and the a-tuples of $[h/a]$ powers.*

7. *Polynomial Summands (Asymptotic Results).* Without precision or any details, Waring implied that there is a Waring problem with polynomial summands $f(x)$. Kamke[*] employed a polynomial $f(x)$ of degree $n \geq 2$ having rational coefficients, that of x^n being positive, such that $f(x)$ is an integer ≥ 0 for every integer $x \geq 0$, and proved that every positive integer is a sum of a limited number of 1's and a limited number of values of $f(x)$ for integers $x \geq 0$. The proof rests on the simultaneous solvability of the equation

$$(7) \qquad\qquad l_j = x_1{}^j + \cdots + x_N{}^j, \qquad (j = 1, \cdots, n),$$

in integers $x \geq 0$, when the l_j are given integers lying in certain intervals, while N is an existing function of n. It would be interesting to know the minimum value of N.

Equations (7) for $n = 2$, also when coefficients are inserted, have been recently[†] discussed at length.

For

$$s \geq (n - 2)2^{n-1} + 5,$$

Landau[‡] found an asymptotic expression for the number of ways to express a given integer as a sum of s values of $f(x)$.

Further progress was blocked by the lack of a solution of the following problem: To find a reasonably small value of $m = m(f, p)$ such that every integer is congruent modulo p (a

[*] Mathematische Annalen, vol. 83 (1921), pp. 85–112. Journal für Mathematik, vol. 152 (1923), pp. 30–32.

[†] Dickson, American Journal of Mathematics, vol. 56 (1934), pp. 513–528; Quarterly Journal of Mathematics, vol. 5 (1934), pp. 283–290.

[‡] Mathematische Zeitschrift, vol. 31 (1930), pp. 319–338.

prime) to a sum of m values of the polynomial $f(x)$. For any f of degree $n < 28$, I proved* that we may take m smaller than the value given by the equation (2) of Hardy and Littlewood.

Under specified mild restrictions on the coefficients of $f(x)$, R. D. James† proved that $G(f) \leq 9$ if $n = 3$, while Miss M. G. Humphreys‡ proved that

$$G(f) \leq (n - 2)2^{n-1} + 5$$

if $n = 4$, 5, 6, or 7, and under strong conditions on $f(x)$ also for $8 \leq n \leq 28$.

K. S. Ghent§ extended Landau's asymptotic result to the expression

$$(8) \qquad F = a_1 f(x_1) + \cdots + a_s f(x_s),$$

where the a_j are given positive integers. Under mild conditions on the a_i and f, he proved that $G(F) \leq 9$ for $n = 3$ and that $G(F) \leq 21$ for $n = 4$.

L. Hua writes me that he has proved that $G(f)$ is less than or equal to the value given by (2) if f is an odd polynomial such that, for no integers l and d $(d > 1)$, $f(x) \equiv l \pmod{d}$ for every x.

The preceding papers found for $G(f)$ a limit which is the same as the initial or final limit for $G(x^n)$ obtained by Hardy and Littlewood. It is hoped that future investigations will reduce $G(f)$ to a limit at least close to that obtained by Vinogradow for $G(x^n)$. We should then be able to evaluate $g(f)$.

8. *Value of $g(f)$ for Polynomials f.* For the polynomial

$$(9) \qquad f(x) = \frac{1}{6}\,\epsilon(x^3 - x) + \sigma x, \qquad \sigma \not\equiv 2a \pmod{3} \text{ if } \epsilon = 3a,$$

we can actually determine‖ positive integers C and v such that every integer $\geq N = C \cdot 3^{3v}$ is a sum of nine values of (9). Here N is relatively small compared to the constant arising from the

---

* American Journal of Mathematics, vol. 57 (1935), pp. 463–474. Proof by cyclotomy.

† American Journal of Mathematics, vol. 56 (1934), pp. 303–315.

‡ Duke Mathematical Journal, vol. 1 (1935), pp. 361–375.

§ Chicago Dissertation, 1935, 49 pp. Condensed in Duke Mathematical Journal.

‖ Dickson, Transactions of this Society, vol. 36 (1934), pp. 1–12, 739–741.

analytic theory, whence the algebraic theory is the better for finding $g(f)$. If $\sigma = 1$, $1 \leqq \epsilon \leqq 6$, then* $g(f) \leqq 9$. A. Sugar readily computed $g(f)$ for any ϵ when $\sigma = 1$.

Elsewhere I obtained† systematically 116 cubic polynomials F for which $g(F) \leqq 9$. For many of them, $g(F) = 4$ or 5 empirically.

The analytic theory of prime numbers has been applied‡ to show that all large numbers are sums of 8 values of (9) for certain sets ϵ, σ.

Given a Waring theorem for a polynomial $q(x)$ of degree n, we may deduce§ instantaneously a Waring theorem for $f(x) - hx$, where f is an even function of degree $2n$ and h is any integer. Hence we deduce an upper limit to $g(F)$, for many polynomials F of degrees 4, 6, 8, 10.

9. *A Paradox.* Granted that an integer m is a sum of s integral values of the function x^n, for example, we see that $m + sc$ is evidently a sum of s values of $x^n + c$, where c is a constant positive integer, and conversely. It would therefore seem that a Waring problem for x^n is the same as for $x^n + c$, except for small integers. While this is true in the above unimportant sense, it is false in the really important case.

For summands x^n, it is immaterial whether we say in modern parlance that m is a sum of exactly s values (one of which is zero), or whether we return to the periods of Fermat, Waring, and others, and say that m is a sum of s or fewer (positive) values. But the function $x^n + c$ does not take the value zero for an integral value $\geqq 0$ of x and the corresponding two problems are essentially different.

I have proved‖ quite recently that, if $n \geqq 9$,

$$g(x^n + 1) = 2^{n-1} + q - 1,$$

---

* By $g(f) = m$ we mean that all positive integers are sums of m values of f, but not all are sums of $m-1$ values of f.

† Acta Arithmetica, vol. 1 (1936), pp. 184–196.

‡ James, Mathematische Annalen, vol. 109 (1933), pp. 196–199. L. Hua, ibid., vol. 111 (1935), pp. 622–628.

§ Dickson, Transactions of this Society, vol. 36 (1934), pp. 371–378; vol. 39 (1936), pp. 205–208.

‖ Here $g(f) = m$ means that all positive integers are sums of m or fewer values of f, but not all are sums of $m-1$ or fewer values.

which is materially smaller than I, where

$$q = [(3^n + 1)/(2^n + 1)].$$

Also that $g(x^3+1) \leq 8$. But proofs are not yet possible for the best results for small n's. I find that all positive integers $< N$ are sums of k or fewer values of x^n+1, where the following table holds:*

n	3	4	5	6	7
$\log_{10} N$	9	4.6115	27.616	38.8893	4405.26
k	7	14	22	41	85
I	9	19	37	73	143

For $f(x) = x^n+2$, let $Q = [f(3)/f(2)]$ and let $\{x\}$ denote the least integer $\geq x$. For $n \geq 9$, every integer > 1 is a sum of $Q - 1 + \{(2^n+3)/3\}$ or fewer values of x^n+2.

For $n \geq 11$, every integer > 2 (except 5) is a sum of $Q + 2^{n-2} + 1$ or fewer values of x^n+3.

n	9	11	12	14
$g(x^n)$	548	2132	4223	16673
$g(x^n+1)$	293	1109	2176	8482
$g(x^n+2, 1)$	209	769	1495	5753
$g(x^n+3, 5)$	167(?)	599	1154	4338

All integers between 1 and one billion are sums of 7 or fewer values of x^3+2. Further reductions of g arise when $c \geq 4$. But now various small integers are not sums of values of x^n+c.

As in §6, we may take all but s, $(s \geq 4n)$, of the summands equal in sets of a. For example, let $c = 1$, $a = 3$. Write $m = 2n/3$ if n is divisible by 3, but $m = 1 + 2[n/3]$ if n is prime to 3. Then every positive integer is a sum of $3 + 6m$ or fewer values of x^n+1 and the triples of

$$(2^{n-1} \pm 1)/3 + [(q - 1)/3] - m$$

or fewer values, where the sign is $+$ or $-$ according as n is even or odd.

---

* For $n=4$, only 487–488 require 14. For $n=5$, only 229–230 and 961–962 require 22. For $n=6$, only 713–714 require 41. We made only a short new table to reach a point beyond which known tables for x^n are applicable.

10. *Homogeneous Summands.* A highly important feature of Vinogradow's method is the use of a parameter y^n. If we replace his summand x^n by $F(x, z)$ we must have $y^n F(x, z) = F(X, Z)$, whence F must be homogeneous and of degree n. In this case, H. Chatland has overcome the difficulties arising by the replacement of x^n by F except the following ones. We seek forms F with many distinct values. To be precise, let F take M distinct values when $0 \leqq x \leqq Q$, $0 \leqq z \leqq Q$; we desire that $M/(Q+1)^2$ shall be 0.99 or some number just less than unity. I would welcome any information.

I have treated this problem for forms divisible by the square or higher power of a linear form. Let $f(x, z)$ be a form of degree t whose coefficients are integers $\geqq 0$, that of z^t being greater than zero. We obtain only distinct values of $F = x^m f$ if we employ integers $x > 0$, $y \geqq 0$ such that f is not divisible by any mth power > 1. It suffices to treat $f \equiv 0$ (mod p^m), p a prime, and hence to discuss $z \equiv cx$ (mod N), where N is a power of p. The latter problem would be the trivial classic one if x, z took the values $0, 1, \cdots, N-1$. On the contrary, they shall here take values $\leqq Q$. The problem is solved by use of the following theorem.

Let c and N be given integers, $0 < c < N$. Let X denote the least residue $\geqq 0$ of cx modulo N. Let r be the greatest integer $< N/c$. Then, for $1 \leqq x \leqq Q$, there are at most $[Q/r]$ values $X < c$.

Evidently we shall obtain a lower[*] value for $g(F)$ than for the case of a function of one variable.

For
$$F(x, z) = x^m(z^n + cx^n),$$
we have
$$F(1, z) = z^n + c.$$

Hence $g(F)$ is smaller than $g(z^n+c)$, which was found in §9. In particular, all positive integers $\leqq 12466$ are sums of 13 or fewer values of $x^4(x^4+z^4)$.

James[†] found $g(x^3+cxy^2)$ for every c. The case $y=0$ shows that $g \leqq 9$.

---

[*] Dickson, American Journal of Mathematics, vol. 48 (1936), pp. 241–248.

[†] Journal of the London Mathematical Society, vol. 10 (1935), pp. 84–88.

11. *Latest Asymptotic Papers*. H. Heilbronn* gave a much shorter proof of the result by Vinogradow; but it leads to a far greater constant.

Vinogradow† modified his method by using Weil's approximation and obtained $G(n) \leqq 2 [n(n-2) \log_e 2 + 2n]$, which is 40, 56, 214 when $n = 5, 6, 12$.

Proofs that $G(4) \leqq 17$ were given independently by T. Estermann‡ and by H. Davenport and Heilbronn.§ The method used by the latter has been extended to any exponent n by Alaoglu, who found $G(5) \leqq 30$, $G(6) \leqq 51$.

For the writer's report on Waring's problem see an article in this Bulletin (vol. 39 (1933), pp. 701–727). On the converse problem, see another article in this Bulletin (vol. 40 (1934), pp. 711–714).

THE UNIVERSITY OF CHICAGO

---

* Acta Arithmetica, vol. 1 (1936), pp. 212–221.

† Mathematical Institute, Stekloff, vol. 9 (1935), pp. 5–15. (Russian.) Announced in Comptes Rendus, Paris, vol. 199 (1934), pp. 174–175.

‡ Proceedings of the London Mathematical Society, vol. 41 (1936), pp. 126–142.

§ Proceedings of the London Mathematical Society, vol. 41 (1936), pp. 143–150, 449–453.