ON HILBERT'S SOLUTION OF WARING'S PROBLEM

PAUL POLLACK

Abstract. In 1909, Hilbert proved that for each fixed k, there is a number g with the following property: Every integer $N \geq 0$ has a representation in the form $N = x_1^k + x_2^k + \cdots + x_g^k$, where the x_i are nonnegative integers. This resolved a conjecture of Edward Waring from 1770. Hilbert's proof is somewhat unsatisfying, in that no method is given for finding a value of g corresponding to a given k. In his doctoral thesis, Rieger showed that by a suitable modification of Hilbert's proof, one can give explicit bounds on the least permissible value of g. We show how to modify Rieger's argument, using ideas of F. Dress, to obtain a better explicit bound. While far stronger bounds are available from the powerful Hardy–Littlewood circle method, it seems of some methodological interest to examine how far elementary techniques of this nature can be pushed.

1. Introduction

In his *Meditationes Algebraicæ*, published in 1770, Edward Waring [17] put forward the following conjectures:

> Every integer is a cube or the sum of at most nine cubes; every integer is also the square of a square, or the sum of up to nineteen such, and so forth.

Waring had only numerical evidence for his assertions. The problem of supplying proofs for his claims has engendered a whole area of mathematics, known as *Waring's problem*. In this article, we use the term *Waring's problem* in a narrower sense, as an abbreviation for the claim implicit in Waring's words "... and so forth":

Waring's problem. *Let k be a positive integer. Show that there is some number g, depending only on k, with the property that every natural number n can be written in the form*

$$n = x_1^k + x_2^k + \cdots + x_g^k,$$

where each x_i is a natural number.

Lagrange's celebrated "four squares theorem" says precisely that $g = 4$ is admissible when $k = 2$, and Waring claimed that $g = 9$ works when $k = 3$ and that $g = 19$ works when $k = 4$. We write $g(k)$ for the smallest admisisble g corresponding to a given k, provided that at least one such g exists. The existence of $g(k)$ in certain special cases was attacked over the next hundred years or so by Liouville ($k = 4$),

2000 *Mathematics Subject Classification.* 11P05.

Key words and phrases. Waring's problem, Hilbert–Waring theorem, additive number theory, elementary methods.

Maillet ($k = 3, 5, 8$), Fleck ($k = 6$), Schur ($k = 10$), and Wieferich ($k = 7$). In 1909, Hilbert found a general solution:

Theorem A (Hilbert, 1909)**.** *$g(k)$ exists for all k.*

Hilbert's proof was a technical tour de force and a triumph of ingenuity. Hardy [4] heaped praise upon it, writing:

> It would be hardly possible for me to exaggerate the admiration which I feel for the solution of this historic problem ... it stands with the work of Hadamard and de la Vallée-Poussin, in the theory of primes, as one of the landmarks in the modern history of the theory of numbers.

But Hardy recognized that Hilbert's argument also had its defects. For example, the method is incapable (in its original form) of producing *numerical bounds* on $g(k)$. The reason for this 'ineffectivity' is as follows: Hilbert's proof makes extensive use of certain polynomial identities, coming from (we would now say) certain existence theorems in convex geometry (such as Carathéodory's theorem). Unfortunately, this argument gives no information on the size of the coefficients in the identities which arise, and such information is essential for bounding $g(k)$.

Today, Hilbert's proof of Theorem A is usually viewed as a historical curiosity, and Hardy himself must be held partly responsible. In 1920, Hardy and Littlewood [5] introduced a flexible analytic method for studying additive problems in number theory. Their first paper on this subject gave a new proof of the existence of $g(k)$. After a century of development, the *Hardy–Littlewood circle method*, as it is now called, occupies a central position in the arsenal of the analytic number theorist. One of the most notable achievements of this method, which combines the work of several mathematicians over the past century, is the determination of the exact value of $g(k)$, for every k. In particular, we now know that $g(3) = 9$ and $g(4) = 19$, as Waring predicted, and in general we have that

$$g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2 \tag{1}$$

for all but at most finitely many k. For more details, see the notes to Chapter XXI in [6].

In 1953, Rieger ([12], [13]) decided to revisit Hilbert's argument, with the goal of obtaining explicit bounds for $g(k)$. To carry out this plan, one needs an alternative means of producing Hilbert's polynomial identities, one which gives one control over the size of the coefficients. Conveniently, such a construction had been given in the interim by Hausdorff [7] and Stridsberg [15]. This permitted Rieger to show that

$$g(k) < (2k+1)^{260(k+3)^{3k+8}}. \tag{2}$$

At the end of [14], Rieger remarks that the bound (2) can be lowered "unter konsequenterer Ausnutzung von Teilbarkeitseigenschaften"[1] to

$$g(k) < (2k+1)^{260(k+1)^8}. \tag{3}$$

[1] "by a more thorough utilization of divisibility properties"

(Both of Rieger's bounds are much weaker than (1)– the interest here is in probing the limitations of the method, and not strictly in the result!) Unfortunately, no further details are provided.

In 1971, Dress [2, 3] showed how an identity familiar from the study of the easier Waring problem (Lemma 3 below) could be combined with (a simplified version of) the convex geometry approach to yield a short and conceptually simple proof of Theorem A. It seems of some historical and methodological interest to explain how his ideas can be used to prove the following bound, somewhat stronger than that claimed by Rieger:

Theorem 1. *$g(k) \le k^{(480+o(1))k^5}$ as $k \to \infty$.*

Here and throughout the article, $o(1)$ denotes a quantity which tends to zero as $k \to \infty$.

For the sake of readability, we have been somewhat coy with our expression for the exponent in Theorem 1. But it is easy to be completely explicit: Making trivial estimates in our proof, we find that for every $k \ge 2$,

$$\begin{aligned} g(k) &\le 2^{420k^3+420k^2+139k-6}(2k+1)^{480k^5+1440k^4+1644k^3+828k^2+162k} \\ &< (2k+1)^{480k^5+1440k^4+1854k^3+1038k^2+\frac{463}{2}k-3} < (2k+1)^{1808k^5}, \end{aligned}$$

which is smaller than the bound (3) for every k.

Finally, we remark that a very different elementary proof of Theorem A was proposed by Linnik [9]. Linnik's proof uses Schnirelmann's notion of density, first introduced to study Goldbach's problem, and is strongly influenced by the analytic approach. Variants of Linnik's argument are discussed by Newman [11], Hua [8, §19.7], and Nesterenko [10, §3]. For the *asymptotic* Waring problem, concerning the least number $G(k)$ of nonnegative kth powers needed to represent all *sufficiently large* integers, Bredikhin and Grishina [1] have shown by elementary methods that $G(k) = O(k \log (2k))$. Up to the value of the implied constant, this matches the best result so far achieved by analytic means.

2. Preparation

We need the following explicit version of Hilbert's identities:

Lemma 1. *Let k be an integer with $k \ge 2$. For some positive integer M with*

$$M \le k^{(160+o(1))k^5},$$

there is an identity in indeterminates $X_1, \dots, X_5$ of the form

$$M(X_1^2 + X_2^2 + \cdots + X_5^2)^k = \sum_{i=0}^{Q} (a_{i1}X_1 + a_{i2}X_2 + a_{i3}X_3 + a_{i4}X_4 + a_{i5}X_5)^{2k}, \tag{4}$$

where the a_{ij} are integers. Moreover, we can arrange that $a_{0i} = 0$ for $1 \le i \le 4$ while $a_{05} = 1$, so that the first summand on the right-hand side is X_5^{2k}.

Remark. We may suppose that in the identity (4), none of the $Q+1$ right-hand summands vanishes identically. Then in the expansion of each summand, each of $X_1^{2k}, \dots, X_5^{2k}$ appears with a nonnegative coefficient, and at least one appears with a positive coefficient. Consequently, in (4), at least one of $X_1^{2k}, \dots, X_5^{2k}$ appears with a coefficient not less than $(Q+1)/5$. Since each appears with coefficient M on the left-hand side, we must have $Q < 5M$.

Proof. We describe how to derive this from Rieger's work in [12] (see also [14, §1]). Let n be a natural number and let $\beta_1, \dots, \beta_n$ be n distinct real numbers. Choose real numbers $\rho_1, \dots, \rho_n$ so that for all $0 \le l < n$,

$$\sum_{i=1}^{n} \beta_i^l \rho_i = \begin{cases} l!/\frac{l}{2}! & \text{if } l \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

The existence and uniqueness of the ρ_i is immediate since the coefficient matrix of this system is of Vandermonde type.

For the remainder of the proof we put $n := 2k+1$. Then if the β_i and ρ_i are as above, it is straightforward to check that

$$\frac{(2k)!}{k!}(X_1^2 + \cdots + X_5^2)^k = \sum_{\substack{\lambda_1,\dots,\lambda_5 \\ 1 \le \lambda_i \le n}} \prod_{i=1}^{5} \rho_{\lambda_i} \left(\sum_{j=1}^{5} \beta_{\lambda_j} X_j \right)^{2k}. \tag{5}$$

One can show that the β_i may be selected so that the corresponding ρ_i are all positive: Indeed, suppose that $\beta_1^*, \beta_2^*, \dots, \beta_n^*$ are the roots of the polynomial

$$\sum_{j=0}^{k} (-1)^{k-j} \frac{n!}{(k-j)!(1+2j)!} x^{1+2j},$$

numbered so that $\beta_1^* = 0$. (Cognoscenti will recognize this as a Hermite polynomial in disguise.) Then the β_i^* are distinct [12, top of p. 5]; moreover, if we select $\beta_i = \beta_i^*$ for each i, then the corresponding ρ_i are all positive [12, top of p. 6]. It now follows from Cramer's rule that the ρ_i are positive whenever $(\beta_1, \dots, \beta_n)$ is sufficiently close (in $\mathbf{R}^n$) to $(\beta_1^*, \dots, \beta_n^*)$. In fact, let

$$\begin{aligned} N_0 &:= 8 \cdot (2k+1)! \cdot (2k+1)^{4k^2+6k+3} \\ &= k^{(4+o(1))k^2}. \end{aligned}$$

Let $\beta_1 = \beta_1^*$, and for $1 < i \le n$, let β_i be the smallest rational number not less than β_i^* which can be written as a fraction with denominator N_0. Rieger's calculations [12, pp. 17–23] show that the β_i are all distinct and that the corresponding ρ_i are all positive. Since the β_i are rational, Cramer's rule implies that the ρ_i are rational. In fact ([12, pp. 23–24]), each of $\rho_1, \dots, \rho_n$ can be written as a fraction with denominator not exceeding

$$(4k+2)^{\binom{2k+1}{2}} N_0^{2\binom{2k+1}{2}} \le k^{(16+o(1))k^4}.$$

Let D be the least common denominator of $\rho_1, \dots, \rho_n$; thus

$$D \le (k^{(16+o(1))k^4})^{2k+1} \le k^{(32+o(1))k^5}.$$

We clear the denominators in (5) by multiplying through by $D^5 N_0^{2k}$; this has the effect of replacing each ρ_{λ_i} with $D\rho_{\lambda_i}$ and each β_{λ_j} with $N_0\beta_{\lambda_j}$. Then with

$$\begin{aligned} M :&= D^5 N_0^{2k} \frac{(2k)!}{k!} \\ &\le k^{(160+o(1))k^5}, \end{aligned}$$

we obtain a representation of $M(X_1^2 + \cdots + X_5^2)^k$ as a linear combination, with positive integer coefficients, of terms of the form $(\sum_{i=1}^5 a_i X_i)^{2k}$, where the a_i are integers. Thus $M(X_1^2 + \cdots + X_5^2)^k$ has a representation in the form (4).

To complete the proof of Lemma 1, it remains only to argue that we can arrange for the first right-hand summand in (4) to equal X_5^{2k}. To verify this, it is enough to show that on the right-hand side of (5), there is some choice of the λ_i for which the corresponding summand involves only the indeterminate X_5. But this follows from our selection of $\beta_1 = \beta_1^* = 0$; we may take $\lambda_i = 1$ for $i < 5$ and $\lambda_5 = 2$. □

If k is understood and h is a natural number, we write $\Sigma(h)$ for the set of integers that are expressible as a sum of h nonnegative integral kth powers. Lemma 1 has the following important consequence:

Lemma 2. *Suppose $k \ge 2$. Fix an identity of the type described in Lemma 1. If l is a nonnegative integer and x is any integer with $|x| \le \sqrt{l}$, then $Ml^k - x^{2k} \in \Sigma(Q)$.*

Proof. Since $l - x^2 \ge 0$, Lagrange's four squares theorem shows that we can write $l - x^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ with integers x_i. The result follows upon evaluating both sides of (4) with $X_i := x_i$ for $1 \le i \le 4$ and $X_5 := x$. □

The following identity is familiar from the study of the so-called 'easier Waring problem'; it can be proved by applying the forward difference operator $(2k-1)$ times to the polynomial T^{2k}. See, e.g., [18], [16, Exercise 1, p. 25].

Lemma 3. *For every positive integer k, there is an identity in T of the form*

$$\sum_{i=1}^{R} (T + a_i)^{2k} - \sum_{j=1}^{R} (T + a_j')^{2k} = AT + B.$$

Here $R = 2^{2k-2}$, $A = (2k)!$, $B = \frac{2k-1}{2}(2k)!$, and $a_1, \dots, a_R, a_1', \dots, a_R'$ are nonnegative integers smaller than $2k$.

Lemma 4. *Let k be a positive integer and let $\kappa := 1 - 1/k$. Suppose $x \ge 0$. For each positive integer t, there are natural numbers $z_1, \dots, z_t$ with*

$$0 \le x - (z_1^k + z_2^k + \cdots + z_t^k) \le k^k x^{\kappa^t}.$$

Proof. We choose the z_i successively by the greedy algorithm, i.e., each z_i is chosen as large as possible so that $(x - (z_1^k + \cdots + z_{i-1}^k)) - z_i^k \geq 0$. Starting from the estimate $0 \leq x - \lfloor x^{1/k} \rfloor^k \leq k x^\kappa$ furnished by the mean value theorem, a straightforward induction shows that

$$0 \leq x - (z_1^k + \cdots + z_t^k) \leq k^{1+\kappa+\cdots+\kappa^{t-1}} x^{\kappa^t} \leq k^k x^{\kappa^t},$$

since $\sum_{j=0}^\infty \kappa^j = (1-\kappa)^{-1} = k$. □

3. Proof of Theorem 1

Proof. We may assume that $k \geq 2$. Given such a k, fix identities of the type described in Lemma 1 and Lemma 3. We first investigate the number of kth powers needed to represent an integer n satisfying

$$n \geq \max\{2^{10k}(RM)^3, k^{4k}\}. \tag{6}$$

Put $l = \lfloor (n/RM)^{1/k} \rfloor$. Since $n \geq RM$, we have

$$l \geq \frac{1}{2}(n/RM)^{1/k}. \tag{7}$$

Moreover, writing $\kappa := 1 - 1/k$, we have by the mean value theorem that

$$0 \leq (n/RM) - l^k \leq k(n/RM)^\kappa,$$

so that

$$n = RMl^k + r \quad \text{for some integer } r \text{ with } \quad 0 \leq r \leq k(RM)^{1/k} n^\kappa.$$

Let t be the smallest positive integer with $\kappa^t \leq (4k)^{-1}$; for future use, notice that since

$$\kappa^t = (1 - 1/k)^t \leq \exp(-t/k),$$

we have $t \leq \lceil k \log 4k \rceil$. By Lemma 4, we may choose nonnegative integers $z_1, \ldots, z_{t-1}$ so that if we put

$$r' := r - (z_1^k + z_2^k + \cdots + z_{t-1}^k),$$

then

$$r' \leq k^k r^{\kappa^{t-1}} \leq k^k (k^{\frac{1}{2k}} (RM)^{\frac{1}{4k}} n^{\frac{1}{4k}}) \leq 2k^k (nRM)^{\frac{1}{4k}}.$$

Here we have used that $\kappa^{t-1} \leq 2\kappa^t \leq (2k)^{-1}$, and that $k^{\frac{1}{2k}} \leq e^{\frac{1}{2e}} < 2$.

Suppose now that $x_1, \ldots, x_R$ are integers each of absolute value not exceeding $\sqrt{l}$. Then for each $1 \leq i \leq R$, Lemma 2 shows that

$$Ml^k - x_i^{2k} \in \Sigma(Q). \tag{8}$$

In the notation of Lemma 3, we now choose each $x_i := m + a_i'$, for some integer m to be selected. Then with $y_i := m + a_i$, Lemma 3 implies that

$$\begin{aligned} n &= RMl^k + r \\ &= \sum_{i=1}^{R}(Ml^k - x_i^{2k}) + \sum_{i=1}^{R} x_i^{2k} + \sum_{j=1}^{t-1} z_j^k + r' \\ &= \sum_{i=1}^{R}(Ml^k - x_i^{2k}) + \sum_{i=1}^{R} y_i^{2k} + \sum_{j=1}^{t-1} z_j^k + r' - (Am + B). \end{aligned} \tag{9}$$

We choose m so that

$$0 \le r' - (Am + B) < A, \quad \text{i.e., so that} \quad m := \lfloor (r' - B)/A \rfloor; \tag{10}$$

to see that this is permissible, we need to check that with this choice of m, each $x_i = m + a_i'$ has absolute value not exceeding $\sqrt{l}$. We have

$$\begin{aligned} |x_i| \le |m| + |a_i'| &\le r'/A + B/A + 2k = r'/A + (2k-1)/2 + 2k \\ &< \frac{2k^k}{(2k)!}(nRM)^{\frac{1}{4k}} + 3k \le (nRM)^{\frac{1}{4k}} + 3k \le 4(nRM)^{\frac{1}{4k}}. \end{aligned}$$

Here we have used that

$$\frac{(2k)!}{k^k} \ge \frac{(2k)(2k-1)\cdots(k+1)}{k^k} = 2(2-1/k)(2-2/k)\cdots(2-(k-1)/k) \ge 2,$$

and that (from (6))

$$n \ge k^{4k}, \quad \text{so that} \quad k \le n^{\frac{1}{4k}} \le (nRM)^{\frac{1}{4k}}.$$

So from (7), we have $|x_i| \le \sqrt{l}$ as long as

$$(4(nRM)^{\frac{1}{4k}})^2 \le \frac{1}{2}(RM)^{-1/k} n^{1/k},$$

which is a consequence of our assumption in (6) that $n \ge 2^{10k}(RM)^3$.

From (9), together with (8) and (10), we see that n is a sum of

$$RQ + R + (t-1) + (A-1) \tag{11}$$

nonnegative kth powers. We have

$$R = 2^{2k-2}, \quad A = (2k)!, \quad t \le \lceil k \log 4k \rceil,$$

and by the remark following Lemma 1, we may assume that

$$Q < 5M \le k^{(160+o(1))k^5}.$$

Inserting these expressions into (11), we find that every n satisfying (6) is a sum of at most $k^{(160+o(1))k^5}$ nonnegative kth powers.

But if n does not satisfy (6), then trivially n is a sum of $\max\{2^{10k}(RM)^3, k^{4k}\} \le k^{(480+o(1))k^5}$ kth powers, each of which is either 0 or 1. $\square$

Acknowledgements

The author thanks the referees for suggestions which enhanced the readability of the paper. He also gratefully acknowledges the support of the National Science Foundation, under award DMS-0802970.

References

[1] Bredikhin B. M. and Grishina T. I., An elementary estimate of $G(n)$ in Waring's problem, Mat. Zametki, 1978, 24, 7–18, 141.
[2] Dress F., Méthodes élémentaires dans le problème de Waring pour les entiers, Université de Provence, Marseille, 1971, Journées Arithmétiques Françaises, Mai 1971.
[3] ———, Théorie additive des nombres, problème de Waring et théorème de Hilbert, Enseignement Math. (2), 1972, 18, 175–190; errata, ibid., 1972, 18, 301–302.
[4] Hardy G. H., Some famous problems of the theory of numbers and in particular Waring's problem (an inaugural lecture delivered before the University of Oxford), Clarendon Press, Oxford, 1920.
[5] Hardy G. H. and Littlewood J. E., Some problems of "Partitio Numerorum" I: A new solution of Waring's problem, Göttingen Nachr., 1920, 33–54.
[6] Hardy G. H. and Wright E. M., An introduction to the theory of numbers, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman.
[7] Hausdorff F., Zur Hilbertschen Lösung des Waringschen Problems, Math. Ann., 1909, 67, 301–305.
[8] Hua L. K., Introduction to number theory, Springer-Verlag, Berlin, 1982, Translated from the Chinese by P. Shiu.
[9] Linnik Yu. V., An elementary solution of the problem of Waring by Schnirelman's method, Mat. Sb., 1943, 12, 225–230.
[10] Nesterenko Yu. V., On Waring's problem (elementary methods), Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI), 2005, 322, 149–175, 254.
[11] Newman D. J., A simplified proof of Waring's conjecture, Michigan Math. J., 1960, 7, 291–295.
[12] Rieger G. J., Zur Hilbertschen Lösung des Waringschen Problems: Abschätzung von $g(n)$, Mitt. Math. Sem. Giessen., 1953, 44, 35 pp.
[13] ———, Zur Hilbertschen Lösung des Waringschen Problems: Abschätzung von $g(n)$, Arch. Math., 1953, 4, 275–281.
[14] ———, Zum Waringschen Problem für algebraische Zahlen and Polynome, J. Reine Angew. Math., 1955, 195, 108–120.
[15] Stridsberg E., Sur la démonstration de M. Hilbert du théorème de Waring, Math. Ann., 1912, 72, 145–152.
[16] Vaughan R. C., The Hardy-Littlewood method, second ed., Cambridge Tracts in Mathematics, vol. 125, Cambridge University Press, Cambridge, 1997.
[17] Waring E., *Meditationes algebraicæ*, American Mathematical Society, Providence, RI, 1991, Translated from the Latin, edited and with a foreword by D. Weeks, with an appendix by F. X. Mayer, translated from the German by D. Weeks.
[18] Wright E. M., *An easier Waring's problem*, J. London Math. Soc., 1934, 9, 267–272.

Department of Mathematics, University of Illinois, 1409 West Green St., Urbana, IL 61801, USA
E-mail address: pppollac@illinois.edu