A remark on the number field analogue of Waring's constant $g(k)$

Paul Pollack[*]

Department of Mathematics, University of Georgia, Athens, Georgia 30602, United States of America

Received XXXX, revised XXXX, accepted XXXX
Published online XXXX

Key words Waring's problem, Waring's constant, Pythagoras number
MSC (2010) 11P05 (primary), 11R04, 11R47 (secondary)

Let K be a number field, and let k be an integer with $k \geq 2$. Let $\mathcal{O}^{\geq 0}$ be the collection of totally nonnegative integers in K (i.e., the totally positive integers together with zero). We let $g(k, K)$ denote the smallest positive integer with the following property: Every element of $\mathcal{O}^{\geq 0}$ that is a sum of kth powers of elements of $\mathcal{O}^{\geq 0}$ is the sum of g such kth powers. Work of Siegel in the 1940s shows that $g(k, K)$ is well-defined for all k and K. In this note, we prove that $g(k, K)$ cannot be bounded by a function of k alone: For each $k \geq 2$,

$$\sup_K g(k, K) = \infty.$$

1 Introduction

Let R be a semiring. For each pair of positive integers k and s, we let $R_k[s]$ denote the collection of elements of R that can be written in the form $\sum_{i=1}^{s} \alpha_i^k$ with all $\alpha_i \in R$, and we let $R_k[\infty] = \bigcup_{s=1}^{\infty} R_k[s]$. The kth *Waring constant of* R is the number

$$g_R(k) := \inf\{s : R_k[s] = R_k[\infty]\}.$$

That is, $g_R(k)$ is the least positive integer s with the property that every sum of kth powers in R is a sum of s kth powers, if any such s exists; otherwise, $g_R(k) = \infty$. An alternative notation, introduced by Joly [1], is $w(k; R)$. This same quantity is also sometimes called the *kth Pythagoras number of R*.

Waring's original conjecture, proposed in 1770 [2, p. 336] and settled by Hilbert in 1909 [3], is that $g_{\mathbb{Z}^{\geq 0}}(k) < \infty$ for every positive integer k. We now know several families of R for which $g_R(k) < \infty$ for all k. For instance, this holds if $R = F[x]$ for F a finite field (Paley [4]), for the matrix rings $R = \mathrm{M}_n(\mathbb{Z})$ (Richman [5]), and for all $\mathfrak{p}$-adic rings R (Ramanujam [6]).[1] In fact, in each of these families, the quantity $g_R(k)$ can be bounded by a constant depending only on k and not on the particular R in question.

The subject of this note is Waring's problem for rings of integers of number fields. The most important early results in this direction are due to Siegel, with the following theorem proved in [7, 8]. For a number field K, we let $\mathcal{O}$ denote its ring of integers. We use a superscript "≥ 0" to indicate a restriction to *totally nonnegative* elements, meaning totally positive or zero.

Theorem A *Let $k \geq 2$. Let K be a number field, and let R denote the subring of $\mathcal{O}$ generated by the kth powers of elements of $\mathcal{O}$. There is a positive integer $G = G(k, K)$ for which the following holds: Every totally positive element of R of sufficiently large norm is the sum of G kth powers of elements of $\mathcal{O}^{\geq 0}$. In fact, if K is not totally real, then the phrase "of sufficiently large norm" may be omitted.*

On its face, Theorem A does not appear to fit into our notational framework for discussing Waring-type problems. But in fact, it easily implies a result of this kind, namely that

$$g_{\mathcal{O}^{\geq 0}}(k) < \infty \qquad \text{for all pairs of } K, k.$$

[*] Corresponding author E-mail: pollack@uga.edu, Phone: +01 706 621 3275, Fax: +01 706 542 5907

[1] By a $\mathfrak{p}$-adic ring, we mean the ring of integers belonging to the completion of a number field at a finite place.

(When $K = \mathbb{Q}$, this is the Waring–Hilbert theorem.) To see this, given k and K, first choose G and C so that all totally positive $\alpha \in R$ with $N\alpha \geq C$ are sums of G kth powers of elements of $\mathcal{O}^{\geq 0}$. Since $(\mathcal{O}^{\geq 0})_k[\infty] \subset R$, certainly all $\alpha \in (\mathcal{O}^{\geq 0})_k[\infty]$ with norm exceeding C are sums of G kth powers of elements of $\mathcal{O}^{\geq 0}$. Now consider those $\alpha \in (\mathcal{O}^{\geq 0})_k[\infty]$ with $N\alpha \leq C$. Let U denote the group of totally positive units in $\mathcal{O}$. Then the set of α being considered here is finite, up to multiplication by an element of U. Since U is finitely generated, U/U^k is finite. This allows us choose a finite set of β's such that any α under consideration is a multiple of some β by the kth power of a totally positive unit. Now letting G_0 be the maximum number of kth powers of elements of $\mathcal{O}^{\geq 0}$ needed to represent any β, we have $g_{\mathcal{O}^{\geq 0}}(k) \leq \max\{G_0, G\}$.

Siegel conjectured in [7] that the G in Theorem A could be taken to depend only on k, and this was confirmed by later results of Birch [9] and Ramanujam (op. cit.; see also [10]); according to their work, we may take $G = \max\{8k^5, 2^k + 1\}$. Here we prove the contrasting result that the Waring constants $g_{\mathcal{O}^{\geq 0}}(k)$ cannot be bounded solely in terms of k.

Theorem 1.1 *For every $k \geq 2$, we have $\sup_K g_{\mathcal{O}^{\geq 0}}(k) = \infty$, where the supremum is taken over all number fields K.*

Remarks.

(i) We have already mentioned that $g_R(k)$ is bounded in terms of k uniformly across all $\mathfrak{p}$-adic rings R. It follows that the phenomenon described in Theorem 1.1 is a genuinely global one.

(ii) Let K be an arbitrary number field. Siegel showed already in 1921 [11, Satz 2] that for any integer $k \geq 2$, every totally positive element of K is a sum of kth powers of totally positive elements of K, with the number of summands bounded solely in terms of k.[2] Consequently, $\sup_K g_{K^{\geq 0}}(k) < \infty$.

The proof of Theorem 1.1 is inspired by an argument of Scharlau [12], who showed (in our notation) that $\sup_K g_{\mathcal{O}}(2) = \infty$. (This disproved a conjecture of Peters [13].) Scharlau's theorem does not immediately imply the case $k = 2$ of Theorem 1.1, nor does it appear to be trivially implied by it.

2 Proof of Theorem 1.1

Throughout this section, $k \geq 2$ is fixed.

Let $q_1, q_2, q_3, \ldots$ be a sequence of distinct primes congruent to 1 modulo 4. Put

$$K_t = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_2}, \ldots, \sqrt{q_t});$$

here, by $\sqrt{q_i}$, we mean the positive square root of q_i living inside $\mathbb{R}$. Thus, each K_t is a subfield of $\mathbb{R}$.

Since the discriminants of the fields $\mathbb{Q}(\sqrt{q_i})$ are pairwise relatively prime, $[K_t : \mathbb{Q}] = 2^t$, and K_t has ring of integers $\mathbb{Z}[\{\frac{1+\sqrt{q_i}}{2} : i = 1, 2, \ldots, t\}]$. With Q_i the smallest odd integer exceeding $\sqrt{q_i}$, we let

$$\eta_t = \sum_{i=1}^{t} \left(\frac{Q_i + \sqrt{q_i}}{2} \right)^k.$$

Clearly, η_t is a sum of t kth powers of totally positive integers from K_t.

We will prove the following proposition.

Proposition 2.1 *We can select the sequence $q_1, q_2, q_3, \ldots$ in such a way that each η_t is not a sum of fewer than t kth powers of totally nonnegative integers in K_t.*

So with $K = K_t$ and $\mathcal{O}$ the ring of integers of K, considering the element η_t reveals that $g_{\mathcal{O}^{\geq 0}}(k) \geq t$. Since t can be taken arbitrarily large, Theorem 1.1 follows immediately.

[2] Siegel used Hilbert's method to prove this. The Birch–Ramanujam result implies the analogous (and stronger) theorem with $\mathcal{O}[1/k!]$ replacing K: Indeed, let α be a totally positive element of $\mathcal{O}[1/k!]$. If j is a large positive integer, then $k!^{kj}\alpha$ is a totally positive element of $k!\mathcal{O}$. Since $k!\mathcal{O} \subset R$ (see top of p. 134 in [7]), the Birch–Ramanujam theorem implies that if j is large enough, then $k!^{kj}\alpha$ is a sum of $\max\{2^k + 1, 8k^5\}$ kth powers in $\mathcal{O}^{\geq 0}$. Now divide this representation of $k!^{kj}\alpha$ through by $k!^{kj}$, absorbing this factor into the kth powers.

Proof of Proposition 2.1. We let $q_1 = 5$ and select $q_2, q_3, q_4, \ldots$ inductively. Suppose that $t \geq 2$ and that we have already selected $q_1, \ldots, q_{t-1}$ in such a way that η_{t-1} is not a sum of fewer than $t-1$ kth powers of totally nonnegative integers in K_{t-1}. (Obviously, this is satisfied when $t = 2$.) We will show how to select q_t so that η_t is not a sum of fewer than t kth powers of totally nonnegative integers in K_t. In fact, we will prove that it suffices to choose q_t sufficiently large in terms of $q_1, \ldots, q_{t-1}$.

To see what constraints on q_t are necessary, let us suppose we have a representation

$$\eta_t = \sum_i \alpha_i^k, \tag{1}$$

where each α_i is a totally nonnegative integer in K_t and the right-hand sum has fewer than t terms. We can (and will) assume that no $\alpha_i = 0$; thus, each α_i is totally positive.

To begin with, observe that for each $i = 1, 2, \ldots, t$,

$$\left(\frac{Q_i + \sqrt{q_i}}{2}\right)^k = \frac{1}{2^k}\left(\sum_{\ell \text{ even}} \binom{k}{\ell} Q_i^{k-\ell} q_i^{\ell/2} + \sum_{\ell \text{ odd}} \binom{k}{\ell} Q_i^{k-\ell} q_i^{(\ell-1)/2}\sqrt{q_i}\right).$$

Therefore, using $\mathrm{Tr}(\cdot)$ for the trace from K_t down to $\mathbb{Q}$,

$$\begin{aligned}\mathrm{Tr}(\eta_t) &= \frac{2^t}{2^k}\sum_{i=1}^{t}\sum_{\ell \text{ even}} \binom{k}{\ell} Q_i^{k-\ell} q_i^{\ell/2} \\ &= C_{t-1} + \frac{2^t}{2^k}\sum_{\ell \text{ even}} \binom{k}{\ell} Q_t^{k-\ell} q_t^{\ell/2},\end{aligned}$$

say. Here C_{t-1} depends only on $q_1, \ldots, q_{t-1}$. Noting that $\sqrt{q_t} < Q_t < 2 + \sqrt{q_t}$, we see that

$$\mathrm{Tr}(\eta_t) \leq C_{t-1} + \frac{2^t}{2^k}\sum_{\ell \text{ even}} \binom{k}{\ell} Q_t^k = C_{t-1} + 2^{t-1}Q_t^k \leq C_{t-1} + 2^{t-1}q_t^{k/2}(1 + 2/\sqrt{q_t})^k. \tag{2}$$

For comparison, we estimate the trace of the right-hand side of (1). Write each

$$\alpha_i = \frac{1}{2}(\mu_i + \nu_i\sqrt{q_t}),$$

where $\mu_i, \nu_i \in K_{t-1}$. From our description of the integers of K_t, it follows that both μ_i and ν_i are integers of K_{t-1}. Moreover,

$$\alpha_i^k = \frac{1}{2^k}\left(\sum_{\ell \text{ even}} \binom{k}{\ell} \mu_i^{k-\ell}\nu_i^\ell q_t^{\ell/2} + \sum_{\ell \text{ odd}} \binom{k}{\ell} \mu_i^{k-\ell}\nu_i^\ell q_t^{(\ell-1)/2}\sqrt{q_t}\right),$$

and so

$$\mathrm{Tr}(\alpha_i^k) = \frac{1}{2^k}\sum_{\ell \text{ even}} \binom{k}{\ell} q_t^{\ell/2}\mathrm{Tr}(\mu_i^{k-\ell}\nu_i^\ell).$$

To handle the trace terms on the right-hand side, we use that α_i is totally positive. For any $\sigma \in \mathrm{Gal}(K_{t-1}/\mathbb{Q})$, we can extend σ in two ways to an element of $\mathrm{Gal}(K_t/\mathbb{Q})$; one of these fixes $\sqrt{q_t}$ while the other sends it to $-\sqrt{q_t}$. Since the image of $\alpha_i = \frac{1}{2}(\mu_i + \nu_i\sqrt{q_t})$ under both extensions is positive, it follows that

$$\sigma(\mu_i) \geq |\sigma(\nu_i)|\sqrt{q_t}. \tag{3}$$

We proved this inequality for $\sigma \in \mathrm{Gal}(K_{t-1}/\mathbb{Q})$, but of course it remains valid for all $\sigma \in \mathrm{Gal}(K_t/\mathbb{Q})$, since both sides depend only on the restriction of σ to K_{t-1}. For even $\ell \leq k$, we raise both sides of (3) to the power $k - \ell$ and multiply by the (nonnegative) number $\sigma(\nu_i)^\ell = |\sigma(\nu_i)|^\ell$ to find that

$$\sigma({\mu_i}^{k-\ell}\nu_i^\ell) \geq |\sigma(\nu_i^k)| q_t^{(k-\ell)/2}.$$

Summing on σ,

$$\mathrm{Tr}(\mu_i^{k-\ell}\nu_i^{\ell}) \geq q_t^{(k-\ell)/2} \cdot S(\nu_i^k),$$

where $S\colon K_t \to \mathbb{R}$ is defined by

$$S(\theta) = \sum_{\sigma} |\sigma(\theta)|.$$

(Unless otherwise specified, sums on σ run over all elements of $\mathrm{Gal}(K_t/\mathbb{Q})$.) Inserting this estimate above,

$$\begin{aligned}\mathrm{Tr}(\alpha_i^k) &\geq \frac{1}{2^k}\sum_{\ell \text{ even}} \binom{k}{\ell} q_t^{k/2} \cdot S(\nu_i^k)\\ &= \frac{1}{2} q_t^{k/2} \cdot S(\nu_i^k).\end{aligned}$$

Hence,

$$\mathrm{Tr}\left(\sum_i \alpha_i^k\right) \geq \frac{1}{2} q_t^{k/2} \sum_i S(\nu_i^k).$$

Recall that ν_i is an algebraic integer. So using $\mathrm{N}(\cdot)$ for the norm from K_t to $\mathbb{Q}$, we see that if $\nu_i \neq 0$, then

$$S(\nu_i^k) = \sum_{\sigma} |\sigma(\nu_i^k)| \geq 2^t \cdot \left(\prod_{\sigma} |\sigma(\nu_i^k)|\right)^{1/2^t} \geq 2^t \cdot |\mathrm{N}(\nu_i^k)|^{1/2^t} \geq 2^t.$$

In the first inequality, we used the so-called "AM-GM inequality" connecting the arithmetic and geometric means.

Since $\eta_t \notin K_{t-1}$, there is at least one value of i with $\nu_i \neq 0$. If there are at least two such values of i, then

$$\mathrm{Tr}(\eta_t) = \mathrm{Tr}\left(\sum_i \alpha_i^k\right) \geq 2 \cdot \frac{1}{2} q_t^{k/2} \cdot 2^t = 2^t q_t^{k/2}.$$

If q_t is sufficiently large in terms of $q_1, \ldots, q_{t-1}$, then the final expression here exceeds the final term in (2). Thus, assuming that q_t is chosen sufficiently large, there must be exactly one index i with $\nu_i \neq 0$, say $i = j$.

We consider further the value of ν_j. The conditions for equality in AM-GM imply that if $S(\nu_j^k) = 2^t$, then $|\sigma({\nu_j}^k)| = 1$ for all σ, and so $\nu_j = \pm 1$. Turning it around, if $\nu_j \neq \pm 1$, then $S(\nu_j^k) > 2^t$.

Claim 2.2 *If $\nu_j \neq \pm 1$, then $S(\nu_j^k) \geq (1+\delta)\cdot 2^t$, where δ is a positive constant depending only on $q_1, \ldots, q_{t-1}$.*

To see the claim, start by noting that for $\alpha \in K_{t-1}$, we have

$$S(\alpha) = 2 \sum_{\sigma \in \mathrm{Gal}(K_{t-1}/\mathbb{Q})} |\sigma(\alpha)|.$$

In particular, the value of $S(\alpha)$, for $\alpha \in K_{t-1}$, does not depend on the choice of q_t. If α is an integer of K_{t-1} and $S(\alpha)$ lies below a given bound, then $\prod_{\sigma \in \mathrm{Gal}(K_{t-1}/\mathbb{Q})}(X - \sigma(\alpha))$ is a polynomial with bounded integer coefficients having α as a root; hence, there are only finitely many possibilities for α. We quickly deduce that, as α ranges over integers of K_{t-1}, there is a smallest value of $S(\alpha)$ exceeding 2^t, and the claim follows. So if $\nu_j \neq \pm 1$, then

$$\mathrm{Tr}(\eta_t) \geq \frac{1}{2} q_t^{k/2} \cdot S(\nu_j^k) \geq \frac{1}{2} q_t^{k/2} \cdot (1+\delta)2^t = (1+\delta)2^{t-1} \cdot q_t^{k/2}.$$

But if q_t is sufficiently large in terms of $q_1, \ldots, q_{t-1}$, this contradicts (2).

Hence, for large enough q_t, the equality (1) forces $\nu_i = 0$ for all $i \neq j$ and $\nu_j = \pm 1$. Therefore $\alpha_i \in K_{t-1}$ for $i \neq j$, and (1) assumes the form

$$\left(\frac{Q_1+\sqrt{q_1}}{2}\right)^k + \dots + \left(\frac{Q_t+\sqrt{q_t}}{2}\right)^k = \sum_{i\neq j} \alpha_i^k + \left(\frac{1}{2}(\mu_j \pm \sqrt{q_t})\right)^k, \tag{4}$$

where the $\pm$ is the sign of ν_j. Comparing the K_{t-1}-coefficients of $\sqrt{q_t}$ on both sides,

$$\sum_{\ell \text{ odd}} \binom{k}{\ell} Q_t^{k-\ell} q_t^{(\ell-1)/2} = \sum_{\ell \text{ odd}} \binom{k}{\ell} \mu_j^{k-\ell} \nu_j^{\ell} q_t^{(\ell-1)/2}.$$

Recall that μ_j is nonnegative (in fact, from (3), totally nonnegative). If $\nu_j = -1$, then the immediately preceding right-hand side is nonpositive, whereas the left-hand side is clearly positive. So $\nu_j = +1$, and

$$\sum_{\ell \text{ odd}} \binom{k}{\ell} Q_t^{k-\ell} q_t^{(\ell-1)/2} = \sum_{\ell \text{ odd}} \binom{k}{\ell} \mu_j^{k-\ell} q_t^{(\ell-1)/2}.$$

Viewed as a function of the real variable μ_j, the right-hand side is strictly increasing for $\mu_j \geq 0$. So the displayed equality forces $\mu_j = Q_t$. Putting these deductions together, we see that the final summand on the left-hand side of (4) is the same as the final summand on its right-hand side. Subtracting this common value reveals that

$$\eta_{t-1} = \sum_{i \neq j} \alpha_i^k.$$

So we have expressed η_{t-1} as a sum of fewer than $t-1$ kth powers of totally positive integers from K_{t-1}. This contradicts our induction hypothesis. □

3 Concluding remarks

It seems reasonable to also consider the Waring numbers (or higher Pythagoras numbers) of $\mathcal{O}$ and not only $\mathcal{O}^{\geq 0}$. As remarked in the introduction, Scharlau showed [12] that $\sup_K g_{\mathcal{O}}(2) = \infty$, and his construction was the inspiration for our proof of Theorem 1.1. It is possible to modify his construction to prove that $\sup_K g_{\mathcal{O}}(k) = \infty$ for every positive even integer k. In fact, if $q_1, q_2, q_3, \dots$ is a suitably-chosen sequence of primes congruent to 1 mod 4, then

$$\sum_{i=1}^{t} \left(\frac{1+\sqrt{q_i}}{2}\right)^k$$

cannot be expressed as a sum of fewer than t kth powers of integers of K_t. The proof is similar to, but simpler than, our proof of Theorem 1.1. By contrast, for odd values of k, it is known that

$$\sup_K g_{\mathcal{O}}(k) \leq 2^{k-1} + 8k^5.$$

This follows from elementary arguments of Stemmler [14], with the local analysis there replaced by the results of Ramanujam alluded to previously (see also [15]).

Acknowledgements The author is supported by a grant from the National Science Foundation, award DMS-1402268. He thanks Enrique Treviño and the anonymous referee for several useful comments.

References

[1] J. R. Joly, Sommes de puissances d-ièmes dans un anneau commutatif, Acta Arith. **17**, 37–114 (1970).
[2] E. Waring, Meditationes algebraicæ (American Mathematical Society, Providence, RI, 1991).

[3] D. Hilbert, Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem), Math. Ann. **67**, 281–300 (1909).
[4] R. Paley, Theorems on polynomials in a Galois field, Quart. J. Math. **4**, 52–63 (1933).
[5] D. Richman, The Waring problem for matrices, Linear and Multilinear Algebra **22**, 171–192 (1987).
[6] C. Ramanujam, Sums of m-th powers in p-adic rings, Mathematika **10**, 137–146 (1963).
[7] C. Siegel, Generalization of Waring's problem to algebraic number fields, Amer. J. Math. **66**, 122–136 (1944).
[8] C. Siegel, Sums of mth powers of algebraic integers, Ann. of Math. (2) **46**, 313–339 (1945).
[9] B. Birch, Waring's problem in algebraic number fields, Proc. Cambridge Philos. Soc. **57**, 449–459 (1961).
[10] B. Birch, Waring's problem for $\mathfrak{p}$-adic number fields, Acta Arith. **9**, 169–176 (1964).
[11] C. Siegel, Darstellung total positiver Zahlen durch Quadrate, Math. Z. **11**, 246–275 (1921).
[12] R. Scharlau, On the Pythagoras number of orders in totally real number fields, J. Reine Angew. Math. **316**, 208–210 (1980).
[13] M. Peters, Summen von Quadraten in Zahlringen. J. Reine Angew. Math. **268/269**, 318–323 (1974).
[14] R. Stemmler, The easier Waring problem in algebraic number fields, Acta Arith. **6**, 447–468 (1960/1961).
[15] M. Bhaskaran, Sums of mth powers in algebraic and Abelian number fields, Arch. Math. (Basel) **17**, 497–504 (1966), errata in **22**, 370–371 (1971).