ACTA ARITHMETICA
131.1 (2008)

The number $\Gamma(k)$ in Waring's problem

by

Christian Elsholtz (London)

1. Introduction. One of the fundamental problems in additive number theory is Waring's problem. Waring asserted (1770) and Hilbert [9] proved the following theorem.

Theorem. *For every positive integer k there exists a finite integer $g(k)$ such that all positive integers can be written as a sum of $g(k)$ nonnegative kth powers*:

$$n = x_1^k + \cdots + x_{g(k)}^k. \tag{1}$$

For a recent survey of this problem with many of its variants and with vast bibliography we refer to Vaughan and Wooley [13]. The question about the least integer $G(k)$ so that all *sufficiently large* integers n can be written as

$$n = x_1^k + \cdots + x_{G(k)}^k \tag{2}$$

is a major open question. It is known that $k+1 \le G(k) \ll k \log k$. This upper bound was first proved by I. M. Vinogradov [14]; for later improvements see e.g. Wooley [15]. It is readily seen that $G(k) \ge k+1$ since the number of $x_1, \dots, x_k$ with $x_1^k + \cdots + x_k^k \le N$ is at most $O(N/k!)$, as there are at most $\binom{N^{1/k}}{k} \ll N/k!$ numbers with distinct x_i and at most $O(N^{1-1/k})$ integers with two or more of the variables equal.

Another lower bound can be derived from local solubility conditions. Let $\Gamma(k)$ denote the least integer such that for all prime powers p^r and all residue classes $0 \le a \le p^r - 1$ there is a solution of

$$x_1^k + \cdots + x_{\Gamma(k)}^k \equiv a \bmod p^r.$$

This local solubility is necessary for the solubility of (2) so that

$$\max(\Gamma(k), k+1) \le G(k).$$

2000 *Mathematics Subject Classification*: Primary 11P05, 11D79; Secondary 11Y50.
Key words and phrases: Waring's problem.

Hardy and Littlewood [6] (see also [4], [5]) conjectured that $\Gamma(k)$ tends with k to infinity ([1]). They computed $\Gamma(k)$ for $k \le 36$ and verified $\Gamma(k) > 4$ for all $3 \le k \le 3000$ with the following exceptions: $\Gamma(3) = \Gamma(7) = \Gamma(19) = 4$, and for $k = 1163, 1637, 1861, 1997, 2053$ the issue remained undecided. They also studied when $\Gamma(k) > k$ holds, and showed for example that $\Gamma(k) = 4k$ if and only if $k > 2$ is a power of 2. Since $G(k) \ge \Gamma(k)$, this implies that $G(k) \ge 4k$ for infinitely many exponents k. In most cases $\Gamma(k)$ is much smaller. It seems conceivable that indeed $G(k) = \max(\Gamma(k), k+1)$, i.e. $G(k) = k+1$, unless there is a congruence obstruction.

Sekigawa and Koyama [12] calculated $\Gamma(k)$ for $k \le 200$ (thereby correcting some minor mistakes of Hardy and Littlewood) and established $\Gamma(k) > 4$ for all $19 \le k \le 3000$, i.e. they also checked the five cases $k = 1163, 1637, 1861, 1997, 2053$ that were left open by Hardy and Littlewood.

Dodson and Tietäväinen have a series of related results (see for example [1]).

The purpose of this paper is twofold. On the one hand, we relate $\Gamma(k)$ to a standard problem in prime number theory. We prove that $\Gamma(k) \to \infty$ as $k \to \infty$ follows from a widely believed conjecture. On the other hand, we extend the range for which $\Gamma(k) > 4$ is known up to $19 \le k \le 5 \cdot 10^8$ and give possible candidates k with $\Gamma(k) = 5$.

The estimates on $\Gamma(k)$ below will follow from the following elementary proposition:

PROPOSITION. *Let k denote an odd prime. Let p denote a prime of the form $p \equiv 1 \bmod k$. Let $i = (p-1)/k$.*

(i) *If $\binom{i+s}{s} < p$, then $\Gamma(k) > s$.*
(ii) *Let $s \ge 4$ and $k \ge 4^s$. If $i^s < p$, then $\Gamma(k) > s$.*

The question reduces to the question of finding a small prime in the progression 1 modulo k. Let $p(q,a)$ denote the least prime $p \equiv a \bmod q$ and let $p(q)$ denote the largest of these values over all primitive residue classes $a \bmod q$. It is known by Heath-Brown's work [8] on Linnik's constant that $p(q) < cq^{5.5}$ with some computable constant c. It is also known that the Generalized Riemann Hypothesis allows replacing the exponent 5.5 by $2 + \varepsilon$. However, a much stronger result is expected to hold: Heath-Brown put forward the following conjecture (see [7] and [11]).

CONJECTURE 1 (Heath-Brown). $p(q) \ll q(\log q)^2$.

([1]) To be precise, Hardy and Littlewood defined $\Gamma(k)$ differently, by means of the convergence of a singular series. However, for $k \ne 4$ both definitions are equivalent.

According to Granville [2], McCurley even suggested that

$$\overline{\lim_{q\to\infty}} \frac{p(q)}{\varphi(q)(\log q)^2} = 2$$

might hold. See Granville and Pomerance [3] for further conjectures on $p(q)$.

THEOREM 1. *If for all $\varepsilon > 0$ there is a k_ε such that $p(k,1) \le k^{1+\varepsilon}$ for $k \ge k_\varepsilon$, then $\Gamma(k) \to \infty$ as $k \to \infty$.*

The two theorems below are a more quantitative version of the last theorem.

THEOREM 2. *Suppose that Conjecture* 1 *holds, at least in the weak form $p(k,1) \ll_r k(\log k)^r$ for some real constant $r > 1$. Then*

$$\Gamma(k) \ge \left(\frac{1}{r-1} - o(1)\right)\frac{\log k}{\log\log k}.$$

So, with $r = 2$ this gives $\Gamma(k) \ge (1-o(1))\frac{\log k}{\log\log k}$. Even if the conjecture above should fail (for example in view of oscillations in the primes discovered by Maier, Friedlander, Granville and Hildebrand) other bounds on $\Gamma(k)$ can be calculated along the same lines from bounds on the primes $p(k,1)$. One can prove the following:

$$\Gamma(k) > \frac{-2 + \log p(k,1)}{\log p(k,1) - \log k - \log\Gamma(k)}.$$

Note that $\Gamma(k)$ also appears on the right hand side. Still this means: if the least prime $p \equiv 1 \bmod k$ is known, then an explicit bound on $\Gamma(k)$ can be worked out.

In another direction we prove:

THEOREM 3. *If $k \ge 4^B$ and $\Gamma(k) \le B$, then also $p(k,1) \ge \frac{1}{4}k^{1+1/(B-1)}$. In particular, if $\liminf \Gamma(k) \le B$, then $p(k,1) \ge \frac{1}{4}k^{1+1/(B-1)}$ infinitely often.*

THEOREM 4. *If $19 < k \le 5\cdot 10^8$, then $\Gamma(k) > 4$.*

2. The details

Proof of the Proposition. We start with the following well known result (see for example Theorem 1.3 of [10]):

LEMMA 1. *The cardinality of the s-fold sumset satisfies*

$$|\mathcal{A} + \cdots + \mathcal{A}| \le \binom{|\mathcal{A}| + s - 1}{s}.$$

This upper bound also holds for sumsets modulo p. Let $p \equiv 1 \bmod k$. Applying this with $\mathcal{A} = \{x^k \bmod p : 0 \le x \le p-1\}$, so that $|\mathcal{A}| = i + 1 = (p-1)/k + 1$, proves part (i) of the Proposition. For (ii) observe that for

$s \geq 4$ and $k \geq 4^s$: If $i \leq s$, then

$$\binom{i+s}{s} \leq \binom{2s}{s} \leq 4^s \leq k < p;$$

if $i > s$, then

$$\binom{i+s}{s} \leq \binom{2i}{s} \leq \frac{2^s i^s}{s!} \leq i^s.$$

So the second part directly follows from the first part.

In fact, Hardy and Littlewood used a similar result that is slightly stronger. They make use of the fact that one of the classes is the zero class which allows for a small saving. Since their condition is more involved but not much stronger, we only use this simple condition. ∎

Let us first prove Theorems 2 and 3.

Proof of Theorem 2. To apply the Proposition we can assume that $s = o(\log k)$. So we find that, with suitable positive constants c_i,

$$\binom{c_1(\log k)^r + s}{s} \leq \frac{c_2^s (\log k)^{rs}}{s!} \leq \frac{c_2^s e^s (\log k)^{rs}}{s^s}.$$

If

$$\frac{c_2^s e^s (\log k)^{rs}}{s^s} < p, \tag{3}$$

then $\Gamma(k) > s$. (3) is equivalent to

$$s(r \log\log k - \log s + 1 + \log c_2) < \log p.$$

Since $k \ll p = p(k,1) \ll_r k(\log k)^r$ it follows that $\log p(k,1) \leq \log k + r \log\log k + O(1)$ and $\log\log p(k,1) = \log\log k + o(1)$. This shows that for fixed r there is an $o(1)$ function so that

$$s = \left(\frac{1}{r-1} - o(1)\right) \frac{\log p}{\log\log p} = \left(\frac{1}{r-1} - o(1)\right) \frac{\log k}{\log\log k}$$

is admissible. ∎

The same kind of argument could be followed for other bounds on $p(k,1)$.

Proof of Theorem 3. Suppose that $\Gamma(k) \leq B$ for some absolute integer $B > 1$. Suppose, for contradiction, that $\binom{(p-1)/k+B}{B} < p$ for some small prime $p(k,1) = p$. Then $\Gamma(k) > B$ by the Proposition. Since this is not the case, we must have

$$\binom{(p-1)/k + B}{B} \geq p.$$

If $B \leq (p-1)/k$, then

$$p \leq \binom{2(p-1)/k}{B} \leq \frac{2^B p^B}{k^B},$$

which implies that $p > (k/2)^{1+1/(B-1)} \geq \frac{1}{4}k^{1+1/(B-1)}$. If $B > (p-1)/k$, then

$$p \leq \binom{2B}{B} \leq 4^B,$$

which is a contradiction for $p > k \geq 4^B$. ∎

Proof of Theorem 1. The proof is a calculation similar to the one in Theorem 2.

Assume that $s \geq 4$ and $p \geq 4^s$. By the Proposition, if $i^s < p$, then $\Gamma(k) > s$. Choose $s = 1/\varepsilon$. So, for $k \geq 4^{1/\varepsilon}$,

$$i^s < \left(\frac{p}{k}\right)^{1/\varepsilon} \leq \left(\frac{k^{1+\varepsilon}}{k}\right)^{1/\varepsilon} = k < p.$$

Now, since ε is arbitrarily small, $\Gamma(k) > s = 1/\varepsilon$ is arbitrarily large. ∎

Proof of Theorem 4. We now describe our computations. In view of $\Gamma(k_1k_2) \geq \Gamma(k_1)$ we can mainly concentrate on prime values of k. We only need to study a few composite integers k.

For prime $k > 2$ we searched for the least prime $p(k,1) = p \equiv 1 \bmod k$ and checked the condition $\binom{i+4}{4} < p$. For most primes k this condition is satisfied and readily shows that $\Gamma(k) > 4$. The set of odd primes which did not satisfy this condition was very small:

$$k = 3, 5, 7, 13, 17, 19, 31, 59, 167, 197, 227, 317, 389, 457, 521,$$
$$1163, 1637, 1861, 1997, 2053, 3833, 5227, 5641, 6637, 7213, 19891.$$

For these few values we explicitly determined the number $\gamma_4(k,p)$ of residue classes modulo $p = p(k,1)$ that are representable as a sum of four kth powers. If $\gamma_4(k,p) < p$, then there is a residue class modulo p which is not the sum of four kth powers, so that $\Gamma(k) > 4$.

In all but one of the cases the least prime $p(k,1)$ was sufficient to prove $\Gamma(k) > 4$. For $k = 31$ we used the second smallest prime, 373, of the form $1 \bmod k$. For an exact determination of $\Gamma(k)$ one would not only have to consider the least prime, but this was not our object here. There are no serious time constraints to extend this calculation. The most time consuming part, namely the determination of large sumsets will probably never occur again so that for large k it suffices to check whether $p(k,1)$ is sufficiently small. The following table shows the exponent k, the least prime $p(k,1)$ (the 2nd least prime for $k = 31$), $i = (p(k,1)-1)/k$ and $\gamma_4(k,p)$, the number of residue classes that can be represented as a sum of four kth powers. For $k \notin \{3,7,19\}$ the table shows that $p(k,1) > \gamma_4(k,p)$, which implies $\Gamma(k) > 4$.

k	$p(k,1)$	i	$\gamma_4(k,p)$	k	$p(k,1)$	i	$\gamma_4(k,p)$	k	$p(k,1)$	i	$\gamma_4(k,p)$
3	7	2	7	5	11	2	9	7	29	4	29
13	53	4	41	17	103	6	61	19	191	10	191
31	373	12	361	59	709	12	541	167	2339	14	1779
197	3547	18	2629	227	5449	24	5353	317	8243	26	8009
389	9337	24	1464	457	13711	30	12361	521	16673	32	16139
1163	37217	32	16865	1637	62207	38	30971	1861	74441	40	63801
1997	87869	44	77617	2053	94439	46	85607	3833	229981	60	203281
5227	397253	76	384409	5641	327179	58	270803	6637	424769	64	358017
7213	432781	60	288241	19891	1551499	78	941071				

Observe that for the "bad example" $k = 19891$,

$$\Gamma(19891) > 4 \quad \text{and} \quad \frac{\log 19891}{\log\log 19891} \approx 4.31$$

support the conditional lower bound in Theorem 2.

The computation above is a proof for prime values of k. For composite k it suffices to check that $\Gamma(k) > 4$ for $k \in \{2\cdot 3,\ 2\cdot 7,\ 2\cdot 19,\ 3\cdot 3,\ 3\cdot 7,\ 3\cdot 19,\ 7\cdot 7,\ 7\cdot 19,\ 19\cdot 19\}$. This was easily checked by the same programme. ∎

We also give a list of primes k that are candidates for $\Gamma(k) = 5$. We checked all primes $k \le 28\,600$. (The bound was due to memory constraints.) For most primes k we found $\Gamma(k) > 5$. For the following k none of the first three primes $p \equiv 1 \bmod k$ suffices to prove $\Gamma(k) \ge 6$:

$$\{5, 31, 59, 167, 197, 227, 317, 389, 457, 521, 1861, 1997, 2053, 3833, 5227,$$
$$5641, 6637, 7213, 18637, 19891\}.$$

Of course it is conceivable that there are some further k beyond our search bound. For $k \le 200$ the values satisfy indeed $\Gamma(k) = 5$, by the results of [6] and [12], for the other values the question remains open.

The author would like to thank Jörg Brüdern, Samir Siksek, Trevor Wooley and the referee for discussions and comments.

The paper was completed while enjoying the hospitality of the Mathematical Institute of the Hungarian Academy of Sciences. The author was supported by the Finite Structures project, in the framework of the European Community's "Structuring the European Research Area" programme.

References

[1] M. M. Dodson and A. Tietäväinen, *A note on Waring's problem in* GF(p), Acta Arith. 30 (1976), 159–167.

[2] A. Granville, *Least primes in arithmetic progressions*, in: Théorie des nombres (Québec, 1987), de Gruyter, Berlin, 1989, 306–321.

[3] A. Granville and C. Pomerance, *On the least prime in certain arithmetic progressions*, J. London Math. Soc. (2) 41 (1990), 193–200.

[4] G. H. Hardy and J. E. Littlewood, *Some problems of Partitio Numerorum (IV): The singular series in Waring's problem and the value of the number $G(k)$*, Math. Z. 12 (1922), 161–188.

[5] —, —, *Some problems of Partitio Numerorum (VI): Further researches in Waring's problem*, ibid. 23 (1925), 1–37.

[6] —, —, *Some problems of Partitio Numerorum (VIII): The number $\Gamma(k)$ in Waring's problem*, Proc. London Math. Soc. (2) 28 (1928), 518–542.

[7] D. R. Heath-Brown, *Almost-primes in arithmetic progressions and short intervals*, Math. Proc. Cambridge Philos. Soc. 83 (1978), 357–375.

[8] —, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) 64 (1992), 265–338.

[9] D. Hilbert, *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen* (*Waringsches Problem*), Math. Ann. 67 (1909), 281–300.

[10] M. Nathanson, *Additive Number Theorem, Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math. 165, Springer, New York, 1996.

[11] P. Ribenboim, *The New Book of Prime Number Records*, Springer, New York, 1996.

[12] H. Sekigawa and K. Koyama, *Nonexistence conditions of a solution for the congruence $x_1^k + \cdots + x_s^k \equiv N \pmod{p^n}$*, Math. Comp. 68 (1999), 1283–1297.

[13] R. C. Vaughan and T. D. Wooley, *Waring's problem: A survey*, in: Number Theory for the Millennium (Urbana, IL, 2000), M. A. Bennett *et al.* (eds.), A K Peters, Boston, 2002, 301–340.

[14] I. M. Vinogradov, *On Waring's problem*, Ann. of Math. (2) 36 (1935), 395–405.

[15] T. D. Wooley, *Large improvements in Waring's problem*, ibid. 135 (1992), 131–164.

Department of Mathematics
Royal Holloway, University of London
Egham
Surrey TW20 0EX, UK
E-mail: christian.elsholtz@rhul.ac.uk

Received on 24.1.2007
and in revised form on 30.7.2007 (5377)