An explicit result of the sum of seven cubes *

O. Ramaré

29th June 2007

Abstract

We prove that every integer $\geq \exp(524)$ is a sum of seven non negative cubes.

1 History and statements

In his 1770's "Meditationes Algebraicae", E.Waring asserted that every positive integer is a sum of nine non-negative cubes. A proof was missing, as was fairly common at the time, the very notion of proof being not so clear. Notice that henceforth, we shall use *cubes* to denote cubes of non-negative integers. Consequently, the integers we want to write as sums of cubes are assumed to be non-negative.

Maillet in [15] proved that twenty-one cubes were enough to represent every (non-negative) integer and later, Wieferich in [30] provided a proof to Waring's statement (though his proof contained a mistake that was mended in [12]). The Göttingen school was in full bloom and Landau [13] showed that eight cubes suffice to represent every *large enough* integer. Dickson [7] improved on this statement by establishing that the only exceptions are 23 and 239. The reader will find a full history of the subject in chapter XXV of [8].

Finally, Linnik in [14] showed that every large enough integer is a sum of seven cubes. Since then, there has been no further improvements in terms of the number of cubes required. Notice that the circle method readily proves that almost all integers are sums of at most four cubes.

From an experimental and heuristical viewpoint, computations and arguments developed in [2],[27], [16], [1], [6] tend to suggest that every integer $\geq 10^{14}$ is a sum of four cubes. The argument in [6] even leads us to believe

*MSC 2000 : primary 11P05, 11Y50 ; secondary 11B13

that 7 373 170 279 850 is the last integer that is a sum of five cubes but not of four. When it is required to exhibit a large example of an integer that is a sum of five cubes, but not of four, the simplest example I know is $10^9 + 4$.

Similarly, it is believed that 454 is the largest integer that is a sum of at least eight cubes, that 8 042 is the largest integer that is a sum of seven cubes but not of six and that 1 290 740 plays this role with respect to sums of six cubes.

By density considerations (there are less than $X^{1/3}$ cubes less than X), we see that every integer cannot be a sum of three cubes. The same would follow by studying sums of three cubes in $\mathbb{Z}/9\mathbb{Z}$. But nothing prevents sums of three cubes to have positive lower density, a hypothesis believed to be true by Hooley in [11]. There the author proves that this density is strictly less than $\Gamma(4/3)^3/6$, this value coming from size considerations only. Hooley even improves on it by taking advantage of some disparities in the distribution of cubes in some arithmetical progressions. The probabilistic models of [5] of sums of 3 cubes supports this conjecture, while giving a density that tends to zero for sums of two squares (a result known to be true by a theorem of Landau), as the model takes more and more local obstructions into account. This is in contrast with a previous probabilistic model (exposed in [10]) of Erdös for such sums that predicts a positive density for sums of three cubes but also for sums of two squares, and of course gives stronger ground to the initial conjecture. In fact, $x^3 + y^3 + z^3$ is *not* a norm and in turn, lacks the ensuing multiplicativity.

In [6], it is shown that every integer between 1 290 741 and 10^{16} is a sum of five cubes from which one readily deduces (see [23]) that every integer n verifying $455 \leq n \leq \exp(78.7)$ is a sum of seven non-negative cubes. On the other hand, note that it is proved in [1] that every integer in some special arithmetic progression, and larger than 455 is indeed a sum of seven cubes.

Our concern in this paper to show that every integer larger than a given explicit bound is indeed a sum of seven cubes. We prove that

Theorem 1 *Every integer* $n \geq \exp(524)$ *is a sum of seven cubes.*

Watson [29] had already greatly simplified Linnik's original proof, though it remained ineffective, and independently, McCurley [16] and Cook [4] corrected this defect. McCurley [16] even proved a theorem similar to the one above with 1 077 334 instead of 524. The method we use has been partially set in [23] where we had a similar statement but with 205 000 instead of 524. In both these approaches, the crux of the method was to show that some arithmetic progression did indeed contain a fairly small prime and the battle was on the link between the size of the modulus q involved and the size of the wanted prime. If the later was of size X, McCurley's proof needed a modulus of size about $(\operatorname{Log} X)^{12}$ (barring exceptional moduli) while we required only a modulus of size about $(\operatorname{Log} X)^6$. Here, we replace the prime by a product of two well localized primes. We produce moduli q for which we are sure that more than half of the reduced residue classes contain primes, from which we deduce that every reduced residue class contains a product of two primes. The gain stems from the method used: our main tool is a large sieve extension of the Brun-Titchmarsh inequality and the avoiding of the prime number Theorem in arithmetic progressions leads to most of our improvement. This alone would give a lower bound of size about exp(780). An additional gain comes from using the special structure of the moduli we are interested in, namely products of three terms, but we need a digression before pursuing this explanation.

First a remark about the order of magnitude. When working on the lower range, near exp(780) say, the product of the two primes we are to build should be of size about $\exp(780/3)/780^4 \simeq \exp(233)$, and since both primes are going to be of the same size, this latter should be about $X = \exp(116)$. On the other side the modulus will be of size $780^6 \simeq \exp(40)$ which behaves more like $X^{1/3}$ than like $\operatorname{Log}^6 X$. This in turn implies that the prime number theorem in arithmetic progressions is completely unsuitable for this purpose.

Next, the distribution of primes in arithmetic progressions modulo q often stumbles on the possible existence of so called Siegel zeros, that would have the effect that only about half the residue classes would contain primes. When abording the problem of this distribution through zeros of L-functions, this effect is well controlled and is avoided by a simple fact: two coprime moduli q_1 and q_2 not too far apart in size cannot have a Siegel zero simultaneously. The remedy (used in [16] and [4]) is thus to create two moduli, and one of them will be good. The condition of coprimality is not minor in any sense: if q has a Siegel zero, then the distribution of primes modulo $3q$ for instance is still going to be unbalanced.

From a sieve point of view, zeros do not appear as such, but a similar role is played by the fact that we can only prove that the number of primes in a given arithmetic progression is about twice what it should be. Indeed, this implies that in this case primes cannot accumulate on a subset of $(\mathbb{Z}/q\mathbb{Z})^*$ that would contain less than $\phi(q)/2$ elements. This can be made accurate is q is a very small power of a X (see [9] and [18]). This is only the rough philosophy when q becomes a power of X. A link between the factor 2 and a possible Siegel zero is also detailed in [19] and in [21].

The fact is that we have a similar effect, even if we are not actually able to produce a corresponding zero. And, indeed, by using a large sieve extension of the Brun-Titchmarsh inequality, we see that primes cannot accumulate in some small sets modulo two coprime moduli of similar size. And that the density of the set attained can even be shown to be fairly close to one if we are ready to chose one moduli among say T candidates. Exactly how close this would be depends on the size of the moduli, say q and of T, but we can roughly show that more than $(1 + 2 \operatorname{Log} X/(T \operatorname{Log}(X/q^2)))^{-1} \phi(q)$ classes are reached and this indeed will be larger than a half if T is large enough in terms of $\operatorname{Log}(X/q^2)$.

At this level, we reach the mentioned exp(780) and there is still some ground to cover. The next idea is to say that the moduli we are interested in are of shape $u^2v^2w^2$, which u, v and w of the same size B. So we can hope for a large sieve inequality for an average on such moduli *once* u and v are being fixed. This would replace the $\operatorname{Log}(X/q^2) = \operatorname{Log}(X/B^{12})$ by $\operatorname{Log}(X/B^8)$. Such an inequality is readily proved via a suitable generalization provided section 5, but its use in giving a lower bound for the number of classes reached finds a hurdle: the possible existence of a Siegel zero modulo u^2v^2, or its analogue, a possible Siegel zero effect. To discard this case, we can however apply the same process when fixing u in u^2v^2, meeting a possible Siegel zero effect modulo u^2 and finally avoiding it by applying yet again this process to the moduli u^2. And this amounts to our final result, when one adds some numerical consideration.

2 A modified form of G.L.Watson's lemma

We state and prove a lemma similar to the one used by Watson in [29]. The central identity is however different and is due to E.Bombieri. We still add summands of the type $(a+x)^3 + (a-x)^3$ with a fixed a to shift the problem from representations by sums of cubes to representations by sums of squares. G.L.Watson's lemma as well as ours relies on the fact that every integer congruent to 3 modulo 8 is a sum of 3 squares, while Yu Linnik introduced coefficients in the resulting ternary quadratic form to encompass all possible residue classes. The introduction of the factor γ is the only novelty when compared to a similar lemma proved in [23].

Lemma 1 *Let n, s, u, v and w be positive integers, t a non-negative integer and γ a positive real number. Let us assume that*

(1) $1 \le u < v < w$,

(2) $\gcd(uvw, 6n) = 1$ *and s is odd,*

(3) u, v, w and s are pairwise coprime.

(4) $n - t^3 \equiv 1[2]$,

(5) $n - t^3 \equiv 0[3s]$,

$$(6)\ \begin{cases} 4(n-t^3)\equiv v^6w^6s^3[u^2], \\ 4(n-t^3)\equiv u^6w^6s^3[v^2], \\ 4(n-t^3)\equiv u^6v^6s^3[w^2], \end{cases} \qquad (7)\ \gamma \le \min(3, 2(w/v)^6, (w/u)^6).$$

Set $\delta = (1+(w/u)^6+(w/v)^6)/4$. *If*

$$0 \le \frac{uv}{6w}\left(\frac{n}{u^6v^6s^3} - \delta - \frac{3\gamma}{4}\right)^{1/3} \le \frac{t}{6uvws} \le \frac{uv}{6w}\left(\frac{n}{u^6v^6s^3} - \delta\right)^{1/3}$$

then n *is a sum of seven non-negative cubes.*

Proof : Set $N = 8(n-t^3)$. Our hypotheses give us the expression

$$N = 2(u^6v^6 + v^6w^6 + w^6u^6)s^3 + 6su^2v^2w^2c$$

where $c \equiv 3[8]$. We can then write c as a sum of 3 non-negative squares: $c = x^2+y^2+z^2$. We choose x, y and z so as to have $0 \le x \le y \le z$. This implies that $x^2 \le c/3$, and that $y^2 \le c/2$. Our size condition on t is also equivalent to

$$0 \le c \le \gamma(u^2v^2s/w)^2$$

so that, using $\gamma \le 3$ and $x^2 \le c/3$, we get

$$0 \le x \le u^2v^2s/w.$$

Similarly with $\gamma \le 2(w/v)^6$ and $y^2 \le c/2$, one obtains

$$0 \le y \le u^2w^2s/v$$

and finally $\gamma \le (w/u)^6$ and $z^2 \le c$ lead to

$$0 \le z \le v^2w^2s/u.$$

Next notice that

$$(1)\qquad \begin{aligned} & (u^2v^2s+wx)^3 + (u^2v^2s-wx)^3 \\ + \ & (u^2w^2s+vy)^3 + (u^2w^2s-vy)^3 \\ + \ & (v^2w^2s+uz)^3 + (v^2w^2s-uz)^3 \\ = \ & 2(u^6v^6+u^6w^6+v^6w^6)s^3 + 6su^2v^2w^2(x^2+y^2+z^2) \end{aligned}$$

where the involved cubes are non-negatives due to the upper bound on c. This gives a writing of N as 6 non-negatives cubes, all of them even. The lemma follows readily.

◇ ◇ ◇

3 Using lemma 1

Let u, v and w be prime numbers $\equiv 5[6]$ and prime to n. Let ℓ be a residue class modulo $u^2v^2w^2$ such that ℓ^3 is congruent to $4n/(v^6w^6)$ modulo u^2, to $4n/(u^6w^6)$ modulo v^2, and to $4n/(u^6v^6)$ modulo w^2. This is possible because every invertible residue class modulo $u^2v^2w^2$ is indeed a cube, u, v and w being primes $\equiv 5[6]$. Select s an integer having all its prime factors $\equiv 5[6]$ and $\equiv \ell[u^2v^2w^2]$. Finally select $t \equiv 0[uvw]$ and so that $t^3 \equiv n-1[2]$ and $t^3 \equiv n[6s]$ which can again be achieved because of the condition imposed on the prime factors of s. It is possible to choose t in the desired interval if it contains more than $6suvw$ integers, which is certainly true if its length is larger than $6suvw+1$. This means

$$(2) \qquad \Big(\frac{n}{u^6v^6s^3}-\delta\Big)^{1/3} - \Big(\frac{n}{u^6v^6s^3}-\delta-\frac{3\gamma}{4}\Big)^{1/3} \geq \frac{6w}{uv}(1+\rho)$$

with $\rho = 1/(6suvw)$. Before continuing, let us mention that we shall seek u, v and w to be as small as possible, and since they are to be coprime with n, the best we can do is to take them of size $\operatorname{Log} n$. This means that δ will be about constant in size and ρ will be very small. Since

$$(3) \qquad x^{1/3} - (x-\theta)^{1/3} \geq \theta/(3x^{2/3}) \quad \text{for } x \geq \theta \geq 0$$

it is enough to have $u^6v^6s^3 \leq n/(\delta + \frac{3\gamma}{4})$ and

$$(4) \qquad \gamma \geq 24(1+\rho)\frac{w}{uv}\Big(\frac{n}{u^6v^6s^3}-\delta\Big)^{2/3},$$

which means thst

$$(5) \qquad n^{1/3}/\big(\tfrac{3\gamma}{4}+\delta\big)^{1/3} \geq su^2v^2 \geq n^{1/3}/\left(\left(\frac{uv\gamma}{24(1+\rho)w}\right)^{3/2}+\delta\right)^{1/3}.$$

The lower bound being much smaller than the upper bound, the problem is really to find a prime s in the proper arithmetical progression and of size about $n^{1/3}/\big(\frac{3\gamma}{4}+\delta\big)^{1/3}$. Note that in (5), we can replace ρ by any upper bound (see (4)).

4 Creating enough primes $\equiv 5[6]$

Lemma 2 *Let $B \geq A \geq 1$ be two real numbers. There are more than $M \geq 1$ prime numbers prime to the integer n and congruent to b modulo q if*

$$\vartheta(B;q,b) - \vartheta(A;q,b) \geq \operatorname{Log} n + M \operatorname{Log} B.$$

Proof : The product P of primes $p \equiv b[q]$ in $]A, B]$ which divide n verifies

$$\operatorname{Log} P \leq \operatorname{Log} n.$$

The condition thus ensures the existence of at least M other primes in the concerned interval. ◇◇◇

We shall only need case of $q = 6$, $b = 5$ and $y = x$ of the following lemma due to the current author and R.Rumely in [25], but it requires no extra effort to state it in general.

Lemma 3 *For $1 \leq x \leq 10^{10}$, any integer $q \leq 72$ and any b prime to q, we have*

$$\max_{1 \leq y \leq x} \left| \vartheta(y; q, b) - \frac{y}{\phi(q)} \right| \leq 2.072\sqrt{x}.$$

Lemma 4 *There are more than M prime numbers prime to n and congruent to 5 modulo 6 lying in the interval $[\beta \operatorname{Log} n, (\beta + \xi(M, \beta, n_0)) \operatorname{Log} n]$ if $\operatorname{Log} n$ is larger that $\operatorname{Log} n_0$, where $\xi(M, \beta, n_0)$ is the smallest positive solution of*

$$\frac{\xi - 2}{2} = \frac{2.072(\sqrt{\beta} + \sqrt{\beta + \xi})}{\sqrt{\operatorname{Log} n_0}} + M \frac{\operatorname{Log}\operatorname{Log} n_0 + \operatorname{Log}(\beta + \xi)}{\operatorname{Log} n_0}$$

provided $\operatorname{Log} n \leq 10^{10}$.

We have $\xi \geq 2$.

Proof : We are to verify the hypothesis of lemma 2 with $q = 6$ and $b = 5$. We are to check that

$$\frac{\xi - 2}{2} \geq \frac{2.072(\sqrt{\beta} + \sqrt{\beta + \xi})}{\sqrt{\operatorname{Log} n_0}} + M \frac{\operatorname{Log}\operatorname{Log} n_0 + \operatorname{Log}(\beta + \xi)}{\operatorname{Log} n_0}$$

which is readily done. ◇◇◇

When we seek an interval containing primes coprime with n, we are forced to consider the worst case when all prime factors of n are indeed in this interval. But in such a case, we could consider a shifted interval: it would then contain no divisor of n and would be smaller. Introducing such a dichotomy is however numerically too heavy: we should typically consider whether n is divisible by the first 200 primes congruent to 5 modulo 6, amounting to 2^{200} cases ... The following lemma is a simple minded way of putting such an idea to practice. We will use it with $M = 2T$.

Lemma 5 *Let $T|M$ be integers and $\beta > 0$ be a real number. Let $\alpha = ((2+\beta+\xi(M,\beta,n_0))/\beta)^{T/M}$. There exists an interval $[A, \alpha A]$ with A in $[\beta \operatorname{Log} n, (\beta+\xi(M,\beta,n_0)) \operatorname{Log} n]$ which contains more than T primes coprime to n and congruent to 5 modulo 6 if $\operatorname{Log} n$ is larger that $\operatorname{Log} n_0$.*

PROOF : Set $A_0 = \beta \operatorname{Log} n$. Among the M/T intervals $[\alpha^j A_0, \alpha^{j+1} A_0]$ with $j \in \{0, 1, \cdots, M/T - 1\}$, by lemma 4, one of them contains more than T primes in the proper congruent class. The lemma follows readily. ⋄ ⋄ ⋄

5 General characters in a sieve context

Here, we work in a general context, which does not cost much more, but enables us to uncover the general lines and to prepare future applications.

Let K be a fixed positive integer. Let $\mathcal{Q}$ be a set of moduli K-*closed under division*, by which we mean the following conditions:

1. Every $q \in \mathcal{Q}$ is divisible by K.
2. For every $q \in \mathcal{Q}$ and every positive integer ℓ divisible by K, if $\ell | q$ then ℓ belongs to $\mathcal{Q}$.

Let also $\mathcal{K} = (\mathcal{K}_q)_{q \in \mathcal{Q}}$ be a compact set, which as in [26], means that

1. For every $q \in \mathcal{Q}$, $\mathcal{K}_q$ is a subset of $\mathbb{Z}/q\mathbb{Z}$,
2. For every $\ell, q \in \mathcal{Q}$, if $\ell | q$ then $\mathcal{K}_\ell = \mathcal{K}_q / \ell\mathbb{Z}$.

We further assume that the Johnsen-Gallagher condition is satisfied, that is to say

$$\text{(JG)} \qquad \forall \ell, q \in \mathcal{Q}/\ell|q, \quad \text{the number} \sum_{\substack{b \in \mathcal{K}_q \\ b \equiv a[\ell]}} 1 \ \text{does not depend on } a \in \mathcal{K}_\ell.$$

Let us note here that similar material is also developed in [24]. In the application we have in mind, we shall take $\mathcal{K}_q = (\mathbb{Z}/q\mathbb{Z})^*$ the subgroup of invertible elements of $\mathbb{Z}/q\mathbb{Z}$. There, all moduli q will be divisible by a fixed K; since we shall restrict our attention to q's such that q/K and K are coprime, we could make do by properly twisting the usual objects.

We consider next $\mathscr{F}_q$ the vector space of functions from $\mathbb{Z}/q\mathbb{Z}$ to $\mathbb{Z}$ that vanish out of $\mathcal{K}_q$, which we endow with the hermitian product

$$(6) \qquad [f|g]_{\mathcal{K}_q} = \frac{1}{|\mathcal{K}_q|} \sum_{a \in \mathcal{K}_q} f(a)\overline{g(a)}.$$

A definition is required here to clarify our subsequent steps.

Definition 1 *A sequence* $(\mathscr{K}_q)_{q\leq Q}$ *is said to be an orthonormal system on* $\mathcal{K}$ *if*

a. For all $q \in \mathcal{Q}$, $\mathscr{K}_q \subset \mathscr{F}_q$.

b. Let ℓ *and* q *be both in* $\mathcal{Q}$ *with* $\ell | q$ *and let* χ *be an element of* $\mathscr{K}_\ell$. *Then* $\tilde{\chi}$ *defined by* $\tilde{\chi}(x) = \chi(x + \ell\mathbb{Z})$ *if* $x \in \mathcal{K}_q$ *and* $\tilde{\chi}(x) = 0$ *otherwise, is in* $\mathscr{K}_q$.

c. $\forall(\chi_1, \chi_2) \in \mathscr{K}_q^2$, *we have*

$$[\chi_1|\chi_2]_{\mathcal{K}_q} = \begin{cases} 0 & \text{if } \chi_1 \neq \chi_2, \\ 1 & \text{if } \chi_1 = \chi_2 \end{cases} \tag{7}$$

d. $|\mathscr{K}_q| = |\mathcal{K}_q|$.

e. If χ *comes (according to* (c)*) from* $\mathscr{K}_{\ell_1}$ *and from* $\mathscr{K}_{\ell_2}$, *then* χ *comes from* $\mathscr{K}_{(\ell_1,\ell_2)}$, *where* (ℓ_1, ℓ_2) *is the gcd of* ℓ_1 *and* ℓ_2.

We shall call *characters* the elements of $\mathscr{K}_q$, even though they are usually not linked with any group structure. The notion of *induced* character is natural from (3), while the one of K*-conductor* is simply established from (e). Let $\mathscr{K}_q^*(K)$ be the set of characters of conductor q. We shall explain later why it is safe to make the dependence in K explicit in our notation.

Condition (e) is more restrictive than it seems so let us give an example where it is not satisfied, while all other conditions are. Take $\mathcal{K}_2(1) = \{1, 2\}$, $\mathcal{K}_3(1) = \{1, 2\}$, and $\mathcal{K}_6(1) = \{1, 2\}$; in $\mathscr{K}_2$, $\mathscr{K}_3$ et $\mathscr{K}_6$, we put the constant function equal to 1, and of conductor 1, and the function that is 1 on 1 and -1 on 2. This last function is induced by a function modulo 2 and by a function modulo 6 but by no function modulo 1.

The existence of such a system is a problem to which we give a partial answer in a lemma below. When $\mathcal{K}_q = \mathbb{Z}/q\mathbb{Z}$, then the additive characters modulo q ($n \mapsto e(na/q)$) build such a system while if $\mathcal{K}_q$ is the set of invertible elements, we can take the set of multiplicative characters modulo q as $\mathscr{K}$. In this last example when $K = 1$, the 1-conductor above is the usual conductor. But note that if K is larger, the K-conductor $\mathfrak{f}_K$ is linked with the usual $\mathfrak{f}$ by

$$\mathfrak{f}_K = K\mathfrak{f}/(\mathfrak{f}, K). \tag{8}$$

A similar remark also holds for the multiplicative characters. We shall write $a \operatorname{mod}_K^* q$ to say that a ranges the points of $\mathbb{Z}/q\mathbb{Z}$ such that, when writing $a/q = b/t$, with $(b, t) = 1$, the $\operatorname{lcm}(K, t) = [K, t] = q$. It is clear from these examples at least that the K-conductor depends strongly on K, but the reader should be even more wary of this dependence because of the *induced system*: usually, we start with a compact set $\mathcal{K}$ defined by $\mathcal{K} = (\mathcal{K}_q)_q$ where q ranges *all* positive integers. We then restrict this system by limiting q to be in a special set $\mathcal{Q}$ and in particular to be divisible by some K; it would then be natural to confuse $\mathscr{K}_q^*(1)$ and $\mathscr{K}_q^*(K)$, a situation that our notation prevents.

By (c) and (d), $\mathscr{K}_q$ is an orthonormal basis of $\mathscr{F}_q$. In particular, when $q \in \mathcal{Q}$ and a is an integer, the function $e_{\mathcal{K}_q}(.a/q)$ defined by $x \mapsto e(xa/q)$ if $x \in \mathcal{K}_q$ and by $x \mapsto 0$ otherwise, can be written as

$$(9) \qquad e_{\mathcal{K}_q}(xa/q) = \sum_{\chi \in \mathscr{K}_q} \left(\frac{1}{|\mathcal{K}_q|} \sum_{k \in \mathcal{K}_q} e(ka/q)\overline{\chi(k)} \right) \chi(x).$$

All this construction has been designed for the following application. Let $(\varphi_n)_{n \le N}$ be a sequence of complex numbers such that

$$(10) \qquad \forall n \le N, \left[a_n \neq 0 \implies \forall q \in \mathcal{Q}, n \in \mathcal{K}_q \right].$$

We define

$$(11) \qquad S(\alpha) = \sum_{n \le N} \varphi_n e(n\alpha) \quad , \quad (\alpha \in \mathbb{R}/\mathbb{Z})$$

and

$$(12) \qquad S(\chi) = \sum_{n \le N} \varphi_n \chi(n) \quad , \quad (\chi \in \mathscr{K}_q, q \in \mathcal{Q}),$$

distinction between (11) and (12) being clear from the context. Let us note that (10) ensures the fundamental equality $S(\chi) = S(\chi')$ whenever χ and χ' are induced by a same character.

By (9), we check that

$$(13) \qquad \sum_{a \bmod_K^* q} |S(a/q)|^2 = \frac{q}{|\mathcal{K}_q|} \sum_{\chi \in \mathscr{K}_q} |S(\chi)|^2$$

from which we infer

$$\sum_{K|d|q} \sum_{a \bmod_K^* d} |S(a/d)|^2 = \frac{q}{|\mathcal{K}_q|} \sum_{K|f|q} \sum_{\chi \in \mathscr{K}_f^*(K)} |S(\chi)|^2,$$

from which Moebius inversion formula yields

$$\boxed{\sum_{a \bmod_K^* q} |S(a/q)|^2 = \sum_{K|f|q} \left(\sum_{d|q/f} \mu(\frac{q}{df}) \frac{df}{|\mathcal{K}_{df}|} \right) \sum_{\chi \in \mathscr{X}_f^*(K)} |S(\chi)|^2.} \tag{14}$$

This equation was our main objective here. It turns out that it is one of the main ingredients of Bombieri & Davenport's [3] proof of the Brun-Titchmarsh inequality. Note the reason why we can reach such a generality is that we dispense here with the value of the Gauss sums. Note that usually, the factor of $\sum_{\chi \in \mathscr{X}_f^*(K)} |S(\chi)|^2$ is non-negative

All this is of no use if no orthonormal system for $\mathcal{K}$ exists. We now provide a sufficient condition usually satisfied. If $K = 1$, our condition is the split multiplicativity introduced in [26], a condition that is inherited by induced system, as defined above, and this would be enough for the application we have in mind. We propose here an intrinsic definition. Let $\sigma_{q \to \ell}$ be the canonical surjection from $\mathbb{Z}/q\mathbb{Z}$ to $\mathbb{Z}/\ell\mathbb{Z}$ when $\ell | q$. We consider the fibered product

$$\mathbb{Z}/q_1\mathbb{Z} \times_K \mathbb{Z}/q_2\mathbb{Z} = \Big\{ (x_1, x_2) / \sigma_{q_1 \to K}(x_1) = \sigma_{q_2 \to K}(x_2) \Big\} \tag{15}$$

whenever K divides q_1 and q_2 and the somewhat generalized Chinese remainder map

$$\begin{array}{rcl} \rho : \mathbb{Z}/(q_1q_2/K)\mathbb{Z} & \rightarrow & \mathbb{Z}/q_1\mathbb{Z} \times_K \mathbb{Z}/q_2\mathbb{Z} \\ x & \mapsto & \big(\sigma_{q_1q_2/K \to q_1}(x), \sigma_{q_1q_2/K \to q_2}(x)\big) \end{array} \tag{16}$$

which is a ring isomorphism whenever $(q_1, q_2) = K$ (it is trivially injective and a cardinality argument concludes). Once this is set, we say that $\mathcal{K}$ is *K-multiplicatively split* if $\mathcal{K}_{q_1q_2/K}$ is isomorphic to $\mathcal{K}_{q_1} \times_K \mathcal{K}_{q_2}$ via the Chinese remainder map, whenever $(q_1, q_2) = K$. In case $K = 1$, this only means that $\mathcal{K}_q$ is isomorphic to the product of the $\mathcal{K}_{p^\nu}$ for all $p^\nu \| q$.

Theorem 2 *If $\mathcal{K}$ is K-multiplicatively split and verifies the Johnsen-Gallagher condition (JG) then there exists an orthonormal system for $\mathcal{K}$. A partial converse is that if an orthonormal system exists then the Johnsen-Gallagher condition is verified.*

Proof : Let us start with the sufficiency. By K-split multiplicativity, it is enough to build such a system on $\mathcal{K}_{p^\nu K}$. We first select an orthonormal system $\mathscr{X}_K$ in $\mathscr{F}_K$. Let us note that

$$|\mathcal{K}_{p^\nu K}| = \frac{|\mathcal{K}_{pK}|}{|\mathcal{K}_K|} \frac{|\mathcal{K}_{p^2K}|}{|\mathcal{K}_{pK}|} \cdots \frac{|\mathcal{K}_{p^\nu K}|}{|\mathcal{K}_{p^{\nu-1}K}|} \tag{17}$$

Let us proceed by induction on $\nu \geq 0$. For $\nu = 0$, $\mathscr{K}_K$ has already been built (and is thus the same for every p). Let us assume that $\mathscr{K}_{p^{\nu-1}M}$ has been built. We first consider $\mathscr{K}'$ the set of all pull-backs from $\mathscr{K}_{p^{\nu-1}M}$ over $\mathbb{Z}/p^\nu M\mathbb{Z}$. We have

$$(18)\quad \forall (\chi_1,\chi_2)\in\mathscr{K}',\ \sum_{a\ mod p^\nu M}\chi_1(a)\overline{\chi_2(a)} = \sum_{b\in\mathcal{K}_{p^{\nu-1}M}}\chi_1(b)\overline{\chi_2(b)}\sum_{\substack{a\in\mathcal{K}_{p^\nu M}\\ a\equiv b[p^{\nu-1}M]}} 1$$

and (JG) together with (17) tell us that property (c) is verified on $\mathscr{K}'$. It is then enough to complete $\mathscr{K}'$ in an orthonormal base of $\mathscr{F}p^\nu M$.

Conversely, let $W_d^q(x)$ be the number of points of $\mathcal{K}_q$ that are congruent to x modulo d, when $d|q$. Let χ_1 and χ_2 be two characters modulo d. By writing their scalar product modulo d, we get

$$\sum_{x\in\mathcal{K}_d} W_d^q(x)\chi_1(x)\overline{\chi_2(x)} = \delta_{\chi_1=\chi_2}|\mathcal{K}_q|.$$

However the orthogonality of these characters also gives

$$\sum_{x\in\mathcal{K}_d}\chi_1(x)\overline{\chi_2(x)} = \delta_{\chi_1=\chi_2}$$

from which it is not difficult to conclude that $W_d^q(x)/|\mathcal{K}_q|$ should be constant and thus equal to $1/|\mathcal{K}_d|$. $\diamond\diamond\diamond$

6 Products of primes covering every reduced residue class

Lemma 6 *For $X \geq 4$, we have*

$$\sum_{\substack{d\leq X\\ (d,6)=1}}\frac{\mu^2(d)}{\phi(d)} \geq \tfrac{1}{3}\operatorname{Log} X + 0.6.$$

(and $\frac{1}{3}\operatorname{Log} X + 0.463$ if one wants $X \geq 1$).

Proof : Lemma 3.4 of [22] yields for $X > 0$

$$\sum_{\substack{d\leq X\\ (d,6)=1}}\frac{\mu^2(d)}{\phi(d)} = \tfrac{1}{3}\operatorname{Log} X + c + \mathcal{O}^*(4.58X^{-1/3})$$

with

$$c = \frac{1}{3}\left(c_0 + \frac{\operatorname{Log} 2}{2} + \frac{\operatorname{Log} 3}{3}\right) = 0.68178665394 + \mathcal{O}^*(10^{-10}).$$

This proves our estimate if $X \geq 10\,000$. For smaller X we use the following GP script.

```
{res=0.0; cmin=1.0;
for(d=1,1000,
   if (issquarefree(d)&&(d%2==1)&&(d%3!=0),
        res+=1/eulerphi(d),);
   if(d>4,cmin=min(cmin,res-log(d+1)/3),));
cmin}
```

◇◇◇

Lemma 7 *For $X > 0$ and $3.32A \geq X$, we have*

$$\sum_{\substack{d \leq X \\ (d,6)=1}} \frac{A\mu^2(d)}{(A+d)\phi(d)} \geq \tfrac{1}{3}\operatorname{Log} X$$

Proof : This is obviously true if $X \leq 4$ so we are now only considering the case $X \geq 4$. Call $G(X)$ the function of lemma 6, or the one we study here but with $A = \infty$. With $c = 0.6$, we find that

$$\begin{aligned}\sum_{\substack{d \leq X \\ (d,6)=1}} \frac{A\mu^2(d)}{(A+d)\phi(d)} &= \frac{AG(X)}{X+A} + A\int_1^X \frac{G(t)dt}{(t+A)^2} \\ &\geq \frac{Ac}{A+1} + \tfrac{1}{3}\operatorname{Log}\frac{X(1+A)}{X+A} + A\int_1^4 \frac{\big(G(t) - \tfrac{1}{3}\operatorname{Log} t - c\big)dt}{(t+A)^2}.\end{aligned}$$

When t varies from 1 to 4, $G(t)$ is 1, and

$$A\int_1^4 \frac{\big(1 - \tfrac{1}{3}\operatorname{Log} t - c\big)dt}{(t+A)^2} = \frac{3A(1-c)}{(4+A)(1+A)}.$$

The function of X

$$\tfrac{1}{3}\operatorname{Log}\frac{1+A}{X+A} + \frac{Ac}{A+1} + \frac{3A(1-c)}{(4+A)(1+A)}$$

decreases as X increases and some numerical analysis tells us that it is positive if $A \geq 10$. For smaller A and X, in fact for $X \leq 10\,000$, we use the following script to show our difference to be ≥ 0.02.

```
{Getc(Amin)=
   exp(log(1+1/Amin)+3*Amin*0.6/(Amin+1)
       +3*Amin*intnum(t=1,4,(0.4-log(t)/3)/(t+Amin)))-1}

{f(X)=
   local(res = 0.0, d);
   for(d = 1, X, if((moebius(d) != 0)&&(gcd(d,6) == 1),
                    res += 1/eulerphi(d)/(1+3.32*d/X),));
   return(res)}

{Check(borneX)=
   local(X, res = 1000);
   forstep(X = borneX, 1, -1,
           res = min(res, f(X)-log(X+1)/3);
           if(res > 0, print1("."),
                       print(X," gives troubles")));
   return(res)}
```

◇ ◇ ◇

Theorem 3 *Let $(k_i)_{i\in I}$ be a set of moduli, all of them divisible by K, prime to 6. We further assume that the k_i/K are two by two coprime. Let $\mathcal{P}$ be a set of prime numbers all not more than X', contained in an interval of length $X > K$, and containing only primes congruent to 5 modulo 6 and prime to all k_i's. For every modulus k, we set*

$$\Delta(k,K) = \phi(k) \sum_{a \mod {}^*k} \Bigl| \sum_{\substack{p\equiv a[k],\\ p\in\mathcal{P}}} 1 \Bigr|^2 - \phi(K) \sum_{a \mod {}^*K} \Bigl| \sum_{\substack{p\equiv a[K],\\ p\in\mathcal{P}}} 1 \Bigr|^2$$

and $\Theta = \sum_{p\in\mathcal{P}} \operatorname{Log} p$; Then

$$\sum_i \left(1 - \frac{2\operatorname{Log}(k_i/K)}{\operatorname{Log}(X/K)-1}\right) \Delta(k_i,K)/\Theta^2 \le \frac{(X+6)\operatorname{Log} X'}{\Theta\bigl(\operatorname{Log}(X/K)-1\bigr)} - 1.$$

Note that in the proof we shall require the condition $k_i \le \frac{7}{11}\sqrt{XK}$ but that it is superfluous in the statement, for otherwise the coefficient of $\Delta(k_i,K)$ is ≤ 0.

Proof : For typographical simplicity, let us introduce the function f on primes that is $\operatorname{Log} p$ if $p\in\mathcal{P}$ and 0 otherwise. We set

$$V(q) = \sum_{a \mod {}^*q} \Bigl| \sum_p f(p)\ e(ap/q) \Bigr|^2 .$$

The weighted large sieve inequality of Montgomery & Vaughan in [17] as improved by [20] gives us

$$\sum_{\substack{q\le Q\\(q,6)=1}} \frac{V(q)}{N+\rho KqQ} \le \sum_{p\in\mathcal{P}} \operatorname{Log}^2 p$$

where N is a real number that majorizes the number of integers $\equiv 5[6]$ in the interval that contains $\mathcal{P}$; and $\rho = \sqrt{1+\frac{2}{3}\sqrt{6/5}}$. Let us further set

$$W_K(q) = \sum_{\chi \mod {}^*_K Kq} \left|\sum_p f(p)\ \chi(p)\right|^2$$

and (14) gives us

$$V(q) = \sum_{\substack{d|q,\\(q/d,Kd)=1}} \frac{\mu^2(q/d)}{\phi(q/d)} \frac{d}{\phi(d)} W_K(d)$$

so that

$$\sum_{\substack{d\le Q\\(d,6)=1}} \tilde{G}_K(d,Q) W(d) \le \Theta \operatorname{Log} X'$$

with

$$\tilde{G}_K(d,Q) = \frac{Kd}{\phi(Kd)} \sum_{\substack{q\le Q/d\\(q,6Kd)=1}} \frac{\mu^2(q)}{(N+\rho KQdq)\phi(q)}.$$

We follow the classical treatment of [28] to write

$$\sum_{\delta|dK} \sum_{\substack{q\le Q/d\\(q,6dK)=\delta}} \frac{\mu^2(q)}{(N+\rho KQdq)\phi(q)} \le \sum_{\delta|dK} \frac{\mu^2(\delta)}{\phi(\delta)} \sum_{\substack{q\le Q/d\\(q,6dK)=1}} \frac{\mu^2(q)}{(N+\rho KQdq)\phi(q)},$$

so that

$$\begin{aligned}\tilde{G}_K(d,Q) &\ge \sum_{\substack{q\le Q/d\\(q,6)=1}} \frac{\mu^2(q)}{(N+\rho KQdq)\phi(q)} = \frac{1}{N} \sum_{\substack{q\le Q/d\\(q,6)=1}} \frac{\mu^2(q)N/(\rho KdQ)}{(N/(\rho KdQ)+q)\phi(q)}\\ &\ge \frac{\operatorname{Log}(Q/d)}{3N}\end{aligned}$$

provided $KQ^2 \leq 3.32N/\rho$ et $d \leq Q$. Hence

$$\sum_{\substack{d \leq Q \\ (d,6)=1}} \operatorname{Log}(Q/d) W_K(d) \leq 3N\Theta \operatorname{Log} X'.$$

At last note that for any k

$$\sum_{d|k/K} W_K(d) = \phi(k) \sum_{a \mod {}^*k} \left| \sum_{p \equiv a[k]} f(p) \right|^2 \geq \Theta^2.$$

We are now to get rid of N and Q. We can take $N = (X+6)/6$ and $Q = \sqrt{3.32N/(\rho K)} \geq \frac{7}{11}\sqrt{X/K}$, which yields the result. ⋄⋄⋄

We are to observe that a minimization argument readily yields

$$\Delta(k,1) \geq \Theta^2 \left(\frac{\phi(k)}{|\mathcal{A}(k)|} - 1 \right). \tag{19}$$

We take $K = 1$ and deduce that for one i, we have

$$|I| \left(1 - \frac{2 \operatorname{Log} k_i}{\operatorname{Log} X - 1} \right) \left(\frac{\phi(k_i)}{|\mathcal{A}(k_i)|} - 1 \right) \leq \frac{X+6}{\sum_p \operatorname{Log} p} \frac{\operatorname{Log} X'}{\operatorname{Log} X - 1} - 1. \tag{20}$$

7 A first simple approach for large n

We are first to note that we will take w as upper bounds for the u and the v that appear on the denominator of Y, which means that we should rather write it in the form

$$Y = \frac{n^{1/3}}{w^4 \left(\frac{3u^6v^6\gamma}{4w^{12}} + \frac{u^6v^6}{w^{12}}\delta \right)^{1/3}}.$$

Since $3u^6v^6\gamma/4w^{12}$ and

$$\frac{u^6v^6\delta}{w^{12}} = \frac{1}{4} \left(\frac{u^6v^6}{w^{12}} + \frac{u^6}{w^6} + \frac{v^6}{w^6} \right) \tag{21}$$

are both largest when u/w and v/w are smallest, we have

$$Y \geq \frac{n^{1/3}}{(3(\gamma+1)/4)^{1/3} B_1^4} = Y'. \tag{22}$$

To derive a lower bound, we write the quantity Y/κ in the form

$$\frac{n^{1/3}}{u^4\left(\left(\frac{v^5\gamma}{24(1+\rho')u^3w}\right)^{3/2}+((v/u)^6+(vw/u^2)^6+(w/u)^6)/4\right)^{1/3}},$$

$$\leq \frac{n^{1/3}}{u^4\left(\left(\frac{u\gamma}{24(1+\rho')}\right)^{3/2}+\frac{3}{4}\right)^{1/3}}.$$

We set

$$\kappa' = \alpha^{-4}((C+1)/(\gamma+1))^{1/3}, \quad C = (2^{1/3}A^-/(3(1+\rho')))^{3/2}$$

and we are to find our product of two primes in $[Y'/\kappa', Y']$. We anticipate the final result: we have not been able to produce any noticeable improvement by acting on the parameter γ. The trivial value $\gamma = 1$ yields results that are only slightly worse, but simplifies scripts quite a lot. Thus, from now on, we shall only consider this case. A final note: one could try to select special sets of u, v and w were this parameter could be taken appreciably larger than 1; in the present case, n is still too large and the sets considered too big.

8 Base final argument

We write $s = \hat{s}\check{s}$ with

$$\hat{s}, \check{s} \in [\sqrt{Y'/\kappa'}, \sqrt{Y'}].$$

We know that

$$\vartheta(X;6,5) = \frac{X}{2}(1+\mathcal{O}^*(0.0023)) \quad (X \geq 612\,477) \tag{23}$$

from [25]: directly from the table there for $X \geq 10^{10}$ and then by using the bounds for the restricted range ($\leq 1.8/\sqrt{X_0}$).

Remember that we are sure to have T primes congruent to 5 modulo 6 and prime to n in an interval $[A, \alpha A]$. Once this is set, the values of Y' and Y'/κ' are defined, and we are simply to select the proper u, v and w. We assume that T is divisible by 3 and group them 3 by 3. This gives us $T/3$ moduli $k = u^2v^2w^2$, all of them prime to the other. The number of classes reached is at least for one of the k's

$$\frac{|\mathcal{A}|}{\phi(k)} \geq \left(1+\frac{\frac{L+6}{\Theta}\frac{\frac{1}{2}\operatorname{Log} Y'}{\operatorname{Log} L-1}-1}{T/3\left(1-\frac{12\operatorname{Log} B}{\operatorname{Log} L-1}\right)}\right)^{-1} \tag{24}$$

where $L = \sqrt{Y'}(1-\sqrt{1/\kappa'})+1$ and $\Theta = \sqrt{Y'}(\frac{1}{2}(1-\sqrt{1/\kappa'})-\varepsilon(1+\sqrt{1/\kappa'}))-\operatorname{Log} n$ with $\varepsilon = 0.0023$. We need this density to be at least 1/2, which translates into

$$\frac{L+6}{\Theta}\frac{\frac{1}{2}\operatorname{Log} Y'}{\operatorname{Log} L-1}-1<\frac{T}{3}\left(1-\frac{12\operatorname{Log} B}{\operatorname{Log} L-1}\right). \tag{25}$$

This way we show that integers larger than exp(780) are sums of seven cubes. Parameters: $\beta = 1.9$, $T = 51$ and $M = 2T$.

9 Refinement number I

We now assume $\operatorname{Log} n$ to be not more than 750. Using $\beta \operatorname{Log} n = A^-$ as a lower bound, we find B such that the the interval $[A^-, B]$ contains more than M primes congruent to 5 modulo 6 and prime to n, and find a subinterval that contains T such primes. This step only differs from the previous one by the fact that we compute B exactly. Then we can build Y' and Y'/κ' as before but this time select u, v and w more shrewdly. Select first t_1 in this set such that

$$\Delta(t_1^2, 1) \le \frac{D-\operatorname{Log} X+1}{T\big(\operatorname{Log} X-1-4\operatorname{Log} B\big)}. \tag{26}$$

with $D = (X+6)\operatorname{Log}(X)/\Theta$. Having this t_1, we select t_2 again in this set but distinct from t_1 and such that

$$\Delta(t_1^2t_2^2, 1) \le \frac{D-\operatorname{Log} X+2\operatorname{Log} B+1}{(T-1)\big(\operatorname{Log} X-1-6\operatorname{Log} B\big)}+\frac{D-\operatorname{Log} X+1}{T\big(\operatorname{Log} X-1-4\operatorname{Log} B\big)}$$

And finally, we select t_3 again in this set and distinct from t_1 and t_2 and such that

$$\begin{aligned}\Delta(t_1^2t_2^2t_3^2, 1) \le \frac{D-\operatorname{Log} X+4\operatorname{Log} B+1}{(T-2)\big(\operatorname{Log} X-1-8\operatorname{Log} B\big)} \\ +\frac{D-\operatorname{Log} X+2\operatorname{Log} B+1}{(T-1)\big(\operatorname{Log} X-1-6\operatorname{Log} B\big)} \\ +\frac{D-\operatorname{Log} X+1}{T\big(\operatorname{Log} X-1-4\operatorname{Log} B\big)}\end{aligned} \tag{27}$$

We simply reorder t_1, t_2 and t_3 to get u, v and w and use again (19) to get a lower bound for the number of classes attained.

We show this way that integers larger than exp(536) are sums of seven cubes by selecting the parameters as follows: $\beta = 2.2$, $T = 33$ and $M = 2T$.

10 Refinement number II

For small values of n, we compute ξ exactly and we reach $\mathrm{Log}\, n \geq 524$ by selecting the parameters as follows: $\beta = 1.79$, $T = 34$, $M = 2T$.

References

[1] F. Bertault, O. Ramaré, and P. Zimmermann. On Sums of Seven Cubes. *Math. Comp.*, 68:1303–1310, 1999.

[2] J. Bohman and C.E. Fröberg. Numerical investigations of waring's problem for cubes. *BIT*, 21:118–122, 1981.

[3] E. Bombieri and H. Davenport. On the large sieve method. *Abh. aus Zahlentheorie und Analysis zur Erinnerung an Edmund Landau*, Deut. Verlag Wiss., Berlin:11–22, 1968.

[4] R.J. Cook. An effective seven cube theorem. *Bull. Aust. Math. Soc.*, 30:381–385, 1984.

[5] J.-M. Deshouillers, F. Hennecart, and B. Landreau. Sums of powers: An arithmetic refinement to the probabilistic model of Erdös and Rényi. *Acta arith.*, 85(1):13–33, 1998.

[6] J.-M. Deshouillers, F. Hennecart, and B. Landreau. 7373170279850 (with an appendix by I. Gusti Putu Purnaba). *Math. Comp.*, 69(229):421–439, 2000.

[7] L.E. Dickson. All integers except 23 and 239 are sums of 8 cubes. *Bull. Amer. Math. Soc.*, 45:588–591, 1939.

[8] L.E. Dickson. *Theory of numbers.* Chelsea Publishing Company, 1971.

[9] P.X. Gallagher. A large sieve density estimate near $\sigma = 1$. *Invent. Math.*, 11:329–339, 1970.

[10] H. Halberstam and K.F. Roth. Sequences. *2nd edition, Springer-Verlag*, page 292pp, 1983.

[11] C. Hooley. On some topics connected with Waring's problem. *J. Reine Angew. Math.*, 369:110–153, 1986.

[12] A.J. Kempner. Über das Waringsche Problem und einige Verallgemeinerungen. *Diss. Göttingen, Extract in Math. Annalen*, 72:387, 1912.

[13] E. Landau. Über die Zerlegung positiver ganzer Zahlen in positive Kuben. *Arch. der Math. u. Phys.*, 18(3):248–252, 1911.

[14] Yu.V. Linnik. On the representation of large numbers as sums of seven cubes. *Mat. Sb., N. Ser.*, 12(54):218–224, 1943.

[15] E. Maillet. Sur la dcomposition d'un nombre entier en une somme de cubes d'entiers positifs. *Assoc. Franç. Bordeaux*, XXIV:242–247, 1895.

[16] K.S. McCurley. An effective seven cube theorem. *J. Number Theory*, 19(2):176–183, 1984.

[17] H.L. Montgomery and R.C. Vaughan. The large sieve. *Mathematatika*, 20(2):119–133, 1973.

[18] Y. Motohashi. Primes in arithmetic progressions. *Invent. Math.*, 44(2):163–178, 1978.

[19] Y. Motohashi. A note on Siegel's zeros. *Proc. Jap. Acad., Ser. A*, 55:190–192, 1979.

[20] E. Preissmann. Sur une inégalité de Montgomery et Vaughan. *Enseign. Math.*, 30:95–113, 1984.

[21] K. Ramachandra, A. Sankaranarayanan, and K. Srinivas. Ramanujan's lattice point problem, prime number theory and other remarks. *Hardy and ramanujan journal*, 19, 1996.

[22] O. Ramaré. On Snirel'man's constant. *Ann. Scu. Norm. Pisa*, 21:645–706, 1995.

[23] O. Ramaré. An explicit seven cube theorem. *Acta Arith.*, 118(4):375–382, 2005.

[24] O. Ramaré. *Arithmetical aspects of the large sieve inequality.* Hindustan Book Agency, 2007.

[25] O. Ramaré and R. Rumely. Primes in arithmetic progressions. *Math. Comp.*, 65:397–425, 1996.

[26] O. Ramaré and I.M. Ruzsa. Additive properties of dense subsets of sifted sequences. *J. Théorie N. Bordeaux*, 13:559–581, 2001.

[27] F. Romani. Computations concerning Waring's problem for cubes. *Calcolo*, 19:415–431, 1982.

[28] J.E. van Lint and H.E. Richert. On primes in arithmetic progressions. *Acta Arith.*, 11:209–216, 1965.

[29] G.L. Watson. A proof of the seven cubes theorem. *J. London Math. Soc.*, 26:153–156, 1951.

[30] A. Wieferich. Beweis des Satzes, dass sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen lässt. *Math. Ann.*, 66:95–101, 1908.