ACTA ARITHMETICA
118.4 (2005)

An explicit seven cube theorem

by

O. Ramaré (Lille)

1. Introduction. In 1941, Yu. Linnik proved that every large integer is a sum of seven non-negative cubes. Here and throughout, all cubes are cubes of non-negative integers. Linnik's proof was awfully intricate and G. L. Watson in [15] offered a drastically simpler one. The latter was made effective simultaneously by K. S. McCurley [4] and R. J. Cook [2] in 1984, and explicit only in [4]. We follow here a similar path while improving some steps. Roughly speaking, E. Maillet introduced in 1895 an identity in this context, but it is arithmetically too rigid to be effective for sums of seven cubes. Maillet himself proved only that fewer than thirteen cubes were enough. Linnik succeeded in putting this identity to use by introducing arithmetical perturbations. A key point of his proof is to find a prime number of size X in an arithmetic progression to a modulus of size about $(\log X)^9$. Watson follows the same path but relies on much easier perturbations. However his proof requires a prime in a progression to a modulus of size $(\log X)^{12}$. The identity (1) below due to E. Bombieri is different (a symmetric version of Watson's in fact) and leads to a similar problem but to a modulus of size $(\log X)^6$, which explains most of our improvement on McCurley's result. Some further numerical care accounts for the final result:

Theorem 1.1. *Every integer* $\geq \exp(205\,000)$ *is a sum of seven non-negative cubes.*

McCurley in [4] had 1 077 334 instead of 205 000.

Concerning the number of representations, let us recall that in 1922 G. H. Hardy and J. E. Littlewood used the circle method to get the number of distinct representations of an integer as a sum of nine cubes. It is only in 1986 that by sharpening this method R. C. Vaughan obtained in [11] the number of representations of a large integer as a sum of eight cubes. In 1989, in [12] and [13], he also showed the number of representations of a large integer as a sum of seven cubes to be of the expected order of magnitude.

2000 *Mathematics Subject Classification*: Primary 11P05.

Though what “large” means in the above results is not known, there is little doubt that small integers will not be covered by them.

As a consequence of the work [3] of J.-M. Deshouillers, F. Hennecart and B. Landreau, and a kind of greedy algorithm performed in Lemma 3 from [1] by F. Bertault, the current author and P. Zimmermann, we now know that every integer between 455 and $2.50 \cdot 10^{26}$ is a sum of seven cubes.

NOTES. Most of this paper has been written when I was invited at the Institute of Advanced Study in 1992. E. Bombieri introduced me to this problem and proposed me kindly to see if I could make some progress by using the identity (1) below. I thank him here for his concern. I thought at the time I could prove every integer $\geq \exp(177\,000)$ is a sum of seven cubes, a fact I claimed in several subsequent talks. There was a numerical mistake and I have to apologize for this claim, though the theorem proved here is only marginally weaker.

2. A modified form of G. L. Watson's lemma. We state and prove a lemma similar to the one used by Watson. The core identity is however different, though we still add summands of 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. Watson's lemma as well as ours rely on the fact that every integer congruent to 3 modulo 8 is a sum of three squares, while Linnik introduced coefficients in the resulting ternary quadratic form to encompass all possible residue classes.

LEMMA 2.1. *Let n, a, u, v and w be positive integers and t a non-negative integer. Assume that*

(1) $1 \leq u \leq v \leq w \leq (3/4)^{1/3} uv/24$,

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

(3) *u, v, w and a are pairwise coprime*,

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

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

(6) $\begin{cases} 4(n-t^3) \equiv v^6 w^6 a^3\ [u^2], \\ 4(n-t^3) \equiv u^6 w^6 a^3\ [v^2], \\ 4(n-t^3) \equiv u^6 v^6 a^3\ [w^2]. \end{cases}$

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

$$0 \leq \frac{uv}{6w}\left(\frac{n}{u^6 v^6 a^3} - \delta - \frac{3}{4}\right)^{1/3} \leq \frac{t}{6uvwa} \leq \frac{uv}{6w}\left(\frac{n}{u^6 v^6 a^3} - \delta\right)^{1/3}$$

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

Proof. Our proof is similar to Watson's but relies on an identity due to Bombieri. We put $N = 8(n - t^3)$. Our hypotheses give us

$$N = 2(u^6v^6 + v^6w^6 + w^6u^6)a^3 + 6au^2v^2w^2c$$

where $c \equiv 3$ [8]. Our size condition on t is also equivalent to

$$0 \le c \le (u^2v^2a/w)^2.$$

We can then write c as a sum of three non-negative squares: $c = x^2 + y^2 + z^2$. Next notice that

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

where the cubes involved are non-negative due to the upper bound on c. This gives an expression of N as six non-negatives cubes, all of them even. The lemma follows readily. ■

3. Reduction to finding a prime in an arithmetic progression. To use Lemma 2.1, 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 u, v and w being primes $\equiv 5$ [6], every invertible residue class modulo $u^2v^2w^2$ is indeed a cube. Select a prime number $a \equiv 5$ [6] with $a \equiv \ell$ $[u^2v^2w^2]$. Finally, select $t \equiv 0$ $[uvw]$ so that $t^3 \equiv n - 1$ [2] and $t^3 \equiv n$ $[6a]$, which can again be achieved because a is a prime $\equiv 5$ [6]. It is possible to choose t in the stated interval if it contains more than $6auvw$ integers, which is certainly true if its length is larger than $6auvw + 1$. This means

$$(2) \qquad \left(\frac{n}{u^6v^6a^3} - \delta\right)^{1/3} - \left(\frac{n}{u^6v^6a^3} - \delta - \frac{3}{4}\right)^{1/3} \ge \frac{6w}{uv}(1 + \varrho)$$

with $\varrho = 1/(6auvw)$. 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 to n, the best we can do is to take them of size $\log n$. This means that δ will be about constant in size and ϱ will be very small. Since

$$(3) \qquad x^{1/3} - (x - 3/4)^{1/3} \ge 1/(4x^{2/3}) \quad \text{for } x \ge 3/4$$

it is enough to require $u^6v^6a^3 \le n/(\delta + 3/4)$ and

$$(4) \qquad 1 \ge 24(1 + \varrho)\,\frac{w}{uv}\left(\frac{n}{u^6v^6a^3} - \delta\right)^{2/3},$$

which reads

$$n^{1/3}/(3/4+\delta)^{1/3} \geq au^2v^2 \geq n^{1/3}\Big/\left(\left(\frac{uv}{24(1+\varrho)w}\right)^{3/2}+\delta\right)^{1/3}. \tag{5}$$

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

4. Creating a non-exceptional modulus. To apply the prime number theorem modulo $k = 6u^2v^2w^2$ to get a prime of size $n^{1/3}$, we need this modulus to be non-exceptional (see below). We could avoid this condition by invoking Linnik's theorem, but this would ruin any hope for reasonable bounds. Instead, we use the fact that exceptional moduli are rare: we are going to create *two* moduli, and one of them will be non-exceptional. Using this trick in this context is due to McCurley.

The main result we shall use is the following one.

Lemma 4.1 (McCurley). *If χ_1 and χ_2 are two distinct real primitive characters modulo k_1 and k_2 respectively and if β_1 (resp. β_2) is a real zero of $L(s,\chi_1)$ (resp. $L(s,\chi_2)$), then*

$$\min(\beta_1,\beta_2) \leq 1 - 1/(R_1 \log\max(13, k_1k_2/17)),$$

where $R_1 = (5-\sqrt{5})/(15-10\sqrt{2})$.

Definition 4.1. An integer $k \geq 2$ is said to be *exceptional in the sense of McCurley* if there exists a (not necessarily primitive) character modulo k such that the associated L-function has a real zero β satisfying $\beta > 1 - 1/(R\log k)$ where $R = 9.645908801$.

Such a character if it exists is real-valued by McCurley (see [6]). This definition is different from the one that is often used and whose definition reads as above except the lower bound is $\beta > 1 - 1/(R\log f)$ where f is the conductor of χ. Our definition is adapted to studying the error term in the prime number theorem, which is indeed our aim. We shall drop the "in the sense of McCurley" part, as is customary, but the reader should remember this definition depends on R.

We can bound exceptional k's from below:

Lemma 4.2. *No L-function attached to a real character to a modulus $k \leq 1\,000$ has a real zero in the strip $0 < \Re s < 1$.*

These computations were carried out by J. B. Rosser in [9] and [10]. Note that M. Watkins in [14] shows that we can even take $k \leq 300\,000\,000$ if we restrict our attention to odd characters.

Lemma 4.3. *Let $B \geq A \geq 1$ be two real numbers. There are more than $M \geq 1$ prime numbers in $[A, B]$ prime to the integer n and congruent to b modulo q if*

$$\vartheta(B; q, b) - \vartheta(A; q, b) \geq \log n + M \log B.$$

Proof. The product P of primes $p \equiv b\ [q]$ in $]A, B]$ and dividing n satisfies

$$\log P \leq \log n.$$

The condition thus ensures the existence of at least M other primes in the above interval. ■

We shall only need the case $q = 6$, $b = 5$ and $y = x$ of the following lemma due to the current author and R. Rumely in [8], but it is no more effort to state it in general.

Lemma 4.4. *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 4.5. *There are more than 24 prime numbers coprime to n and congruent to 5 modulo 6 lying in the interval $[0.161 \log n, 2.18 \log n]$ if $\log n$ is larger than 50 000.*

The constants 0.161 and 2.18 are chosen to minimize the lower bound for $\log n$ reached in Lemma 5.3. The difference could not be taken smaller than $2 = \phi(6)$.

Proof. We have to verify the hypothesis of Lemma 4.3 with $q = 6$ and $b = 5$. We need to check that

$$\frac{B - A}{2} - 2.072(\sqrt{A} + \sqrt{B}) \geq \log n + 24 \log B,$$

which is readily done. ■

Lemma 4.6. *Let $\alpha = (2.18/0.161)^{1/4}$. There exists an interval $[A, \alpha A]$ with A in $[0.161 \log n, (2.18/\alpha) \log n]$ which contains more than six primes coprime to n and congruent to 5 modulo 6 if $\log n$ is larger than 50 000.*

Proof. Set $A_0 = 0.161 \log n$. Among the four intervals $[\alpha^j A_0, \alpha^{j+1} A_0]$ with $j \in \{0, 1, 2, 3\}$, one contains more than six primes in the proper congruence class by Lemma 4.5. The lemma follows readily. ■

Let $u_1 < v_1 < w_1 < u_2 < v_2 < w_2$ be the six primes satisfying the hypothesis of Lemma 4.6. Let k_1 be one of $\{3(u_1 v_1 w_1)^2, 3(u_2 v_2 w_2)^2\}$ and k_2 be the other one. We show that k_1 or k_2 is non-exceptional.

Let χ_1 (resp. χ_2) be a real character of conductor $f_1 \mid k_1$ (resp. $f_2 \mid k_2$) whose Dirichlet L-function admits a real zero β_1 (resp. β_2), if two such characters exist. If not, we are done. Note these two characters are necessarily distinct since otherwise one would have $f_1 = f_2 = 3$, an impossibility according to Lemma 4.5. Assume β_1 is smaller than β_2. By Lemma 4.1, we have

$$\beta_1 \le 1 - 1/(R_1 \log(k_2 k_1/17)) \tag{6}$$

and this is $\le 1 - 1/(R \log k_1)$ because

$$k_1^{R/R_1 - 1} \ge k_2/17, \tag{7}$$

an inequality that is true if $\log n \ge 100$ (3 would even be enough!).

5. Finding a prime in a progression with a large modulus. Set

$$Y = n^{1/3}/(3/4+\delta)^{1/3}, \qquad \kappa^3 = \frac{\left(\dfrac{uv}{24(1+\varrho)w}\right)^{3/2} + \delta}{3/4+\delta},$$

and

$$k = 3(uvw)^2 \ge 3.22 \cdot 10^{27} \quad (\log n \ge 200\,000).$$

We have to find a prime congruent to a given invertible residue class modulo k and in the interval $[Y/\kappa, Y]$. Note first that

$$\varrho \le 1/(6(0.16 \log n)^3) \le 10^{-7} \quad (\log n \ge 1\,000).$$

We can replace ϱ by this upper bound in κ^3. The resulting expression is non-increasing in u and v and non-decreasing in w, as a quotient of such functions and because $uv/(24(1+\varrho)w) \ge (3/4)^{2/3}$. We also use the bound $w/u \le \alpha$. This time the resulting expression is non-decreasing in $\log n$, and this warrants

$$\kappa \ge 9 \qquad (\log n \ge 203\,000).$$

Since κ is sufficiently large, the next lemma is enough to treat the condition $a \ge Y/\kappa$. It is a direct consequence of a theorem of H. Montgomery and R. C. Vaughan in [7].

Lemma 5.1. *For $1 \le q < X$, and b an invertible residue class modulo q, we have*

$$\vartheta(X; q, b) \le \frac{2X}{\phi(q)} \frac{\log X}{\log(X/q)}.$$

Let us recall a theorem of McCurley from [5]:

Lemma 5.2. *If $q \ge 10^{25}$ and b is an invertible residue class modulo q where q is non-exceptional and $\log X \ge 10.88 \log^2 q$, then*

$$|\vartheta(X; q, b) - X/\phi(q)| \le X/(2\phi(q)).$$

LEMMA 5.3. *Assume* $\log n \geq 205\,000$. *For any invertible residue class* ℓ *modulo* k *there is a prime in* $[Y/9, Y]$ *congruent to* ℓ *modulo* k.

Proof. We first verify the inequality

$$\tfrac{1}{3}\log n - \tfrac{1}{3}\log(1+2\alpha^6/4) - 4\log(2.18\log n) \geq 10.88\,(\log 3 + 6\log(2.18\log n))^2,$$

and this is readily done for $\log n \geq 205\,000$. By Lemma 5.2, we infer

$$\vartheta(Y;k,\ell) \geq Y/(2\phi(k))$$

and using Lemma 5.1, we get

$$\vartheta(Y;k,\ell) - \vartheta(Y/9;k,\ell) \geq \frac{Y}{\phi(k)}\left(\frac{1}{2} - \frac{2\log(Y/9)}{9\log(Y/(9k))}\right).$$

We need $9\log k < 5\log(Y/9)$ for the right hand side to be positive, a condition that is easily verified to hold true. ∎

References

[1] F. Bertault, O. Ramaré and P. Zimmermann, *On sums of seven cubes*, Math. Comp. 68 (1999), 1303–1310.

[2] R. J. Cook, *An effective seven cube theorem*, Bull. Austral. Math. Soc. 30 (1984), 381–385.

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

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

[5] —, *Explicit estimates for the error term in the prime number theorem for arithmetic progressions*, Math. Comp. 42 (1984), 265–285.

[6] —, *Explicit zero-free regions for Dirichlet L-functions*, J. Number Theory 19 (1984), 7–32.

[7] H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika 20 (1973), 119–133.

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

[9] J. B. Rosser, *Real roots of Dirichlet L-series*, Bull. Amer. Math. Soc. 55 (1949), 906–913.

[10] —, *Real roots of real Dirichlet L-series*, J. Res. Nat. Bur. Standards 45 (1950), 505–514.

[11] R. C. Vaughan, *On Waring's problem for cubes*, J. Reine Angew. Math. 363 (1986), 122–170.

[12] —, *A new iterative method in Waring's problem*, Acta Math. 162 (1989), 1–71.

[13] —, *On Waring's problem for cubes II*, J. London Math. Soc. 39 (1989), 205–218.

[14] M. Watkins, *Real zeros of real odd Dirichlet L-functions*, Math. Comp. 73 (2004), 415–423.

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

Laboratoire de Mathématique
Université Lille I
59655 Villeneuve d'Ascq, France
E-mail: Olivier.Ramare@math.univ-lille1.fr

Received on 12.10.2004 (4865)