SUMS OF TWO CUBES

Trevor D. Wooley*

In the course of investigations concerning sums of two cubes, Hooley [2] has obtained estimates for the function $\nu(x)$, which he defines to be the number of positive integers not exceeding x that have at least two essentially distinct representations as the sum of two non-negative cubes. Some thirty years ago Hooley [2] used a sieve method to show that $\nu(x) = O(x^{2/3} \log\log x (\log x)^{-1/2})$, thus proving that the representation of a number as the sum of two non-negative cubes is almost always essentially unique. In a subsequent tour de force, Hooley [3] devised an ingenious method, utilising Deligne's resolution of the Riemann hypothesis for varieties over finite fields inside the large sieve, and thereby obtained the improved estimate $\nu(x) = O_\epsilon(x^{5/9+\epsilon})$. In this note we provide an elementary proof of Hooley's theorem, using nothing more profound than simple properties of binary quadratic forms.

Theorem 1. *One has* $\nu(x) = O_\epsilon(x^{5/9+\epsilon})$.

Following Hooley, we establish Theorem 1 by estimating the number of non-trivial solutions of an auxiliary equation. We note that $\nu(x)$ is bounded above by the number of integral solutions of the simultaneous inequalities

$$0 < u_1^3 + u_2^3 = v_1^3 + v_2^3 \le x \quad \text{and} \quad 0 \le u_2 < v_1 \le v_2 < u_1 \le x^{1/3}. \tag{1}$$

Let $S(P)$ denote the number of solutions of the equation $x_1^3 + x_2^3 = x_3^3 + x_4^3$ with $0 \le x_i \le P$ $(1 \le i \le 4)$ and $x_1 \ne x_j$ $(j = 3, 4)$. Then it follows from (1) that $\nu(x)$ is bounded above by $S(x^{1/3})$, wherefore Theorem 1 follows from the estimate for $S(P)$ contained in the following theorem.

Theorem 2. *One has* $S(P) \ll_\epsilon P^{5/3+\epsilon}$.

Proof. Let $T(P, h)$ denote the number of solutions of the simultaneous equations

$$\begin{aligned} x_1^3 + x_2^3 &= x_3^3 + x_4^3 \\ x_1 + x_2 &= x_3 + x_4 + h \end{aligned} \tag{2}$$

with $0 \le x_i \le P$ $(1 \le i \le 4)$. When $h = 0$, it follows easily from (2) that $x_1 = x_3$ or $x_1 = x_4$. Thus

$$S(P) = \sum_{1 \le |h| \le 2P} T(P, h) \ll (\log 2P) \max_{1 \le H \le P} \sum_{H \le |h| \le 2H} T(P, h). \tag{3}$$

Let h be non-zero, and let $\mathbf{x}$ be a solution of the system (2) counted by $T(P, h)$. Notice that by relabelling variables we may suppose that $x_3 = \min_{1 \le i \le 4} x_i$. Also, one has

$$(x_1 + x_2 - x_3)^3 - (x_1^3 + x_2^3 - x_3^3) = (x_4 + h)^3 - x_4^3. \tag{4}$$

Moreover, on making the substitution

$$u_1 = x_1 + x_2, \quad u_2 = x_1 - x_3, \quad u_3 = x_2 - x_3, \quad y = 2x_4 + h,$$

* Research supported in part by NSF grant DMS-9303505, an Alfred P. Sloan Research Fellowship, and a Fellowship from the David and Lucile Packard Foundation.

Internat. Math. Res. Notices (1995), 181–185

Typeset by $\mathcal{AMS}$-TEX

one readily deduces that the x_i are uniquely determined from the u_j, y and h. Thus we deduce from (2) and (4) that $T(P,h)$ is bounded above by $U(P,h)$, where $U(P,h)$ denotes the number of solutions of the system

$$\begin{aligned} 12u_1u_2u_3 &= h(3y^2+h^2) \\ u_1+u_2+u_3 &= y+h \end{aligned} \tag{5}$$

with

$$1 \le u_i \le 2P \quad (1 \le i \le 3), \quad 1 \le y \le 4P.$$

We note for future reference that if, for any i, one has $h = u_i$ in (5), then by relabelling variables, $h = u_3$. On eliminating y, one obtains $h^2 + 3(u_1 - u_2)^2 = 0$, whence $h = 0$. Consequently, in any solution counted by $U(P,h)$ one has $h \ne u_i$ $(1 \le i \le 3)$.

Let $\mathbf{u}$, y be a solution of the system (5). Notice now that by relabelling variables we may suppose that the pairwise common factors of the u_i and h satisfy the condition $(u_3,h) = \max_{1\le i\le 3}(u_i,h)$. Write

$$d_3 = (u_3,h), \quad d_2 = (u_2, h/d_3), \quad d_1 = (u_1, h/(d_2d_3)),$$

$$g = h/(d_1d_2d_3), \quad f = 12/g, \quad \text{and} \quad v_i = u_i/d_i \quad (1 \le i \le 3).$$

From (5) we see that f and g are integers. Thus, on recalling the above observation, together with the concluding remark of the preceding paragraph,

$$h = gd_1d_2d_3, \quad fg = 12, \quad d_3 = \max_{1\le i\le 3} d_i, \quad v_3 \ne gd_1d_2, \tag{6}$$

and $u_i = v_id_i$ $(1 \le i \le 3)$. On substituting into (5), and eliminating y by using the linear equation, we deduce that $U(P,h)$ is bounded above by $V(P,h)$, where $V(P,h)$ denotes the number of solutions of the equation

$$fv_1v_2v_3 = 3(d_1v_1 + d_2v_2 + d_3v_3 - gd_1d_2d_3)^2 + (gd_1d_2d_3)^2, \tag{7}$$

with $\mathbf{v}$, $\mathbf{d}$, f and g satisfying (6), and

$$1 \le v_i \le 2P/d_i \quad (1 \le i \le 3). \tag{8}$$

Let $W(P;\mathbf{d},f,g,v_3)$ denote the number of solutions of the equation (7) with v_1 and v_2 satisfying (8). Then we may conclude thus far that

$$S(P) \ll (\log 2P) \max_{1\le H\le P} \sum_{gf=12} \sum_{H\le |h|\le 2H} \sum_{\substack{gd_1d_2d_3=h \\ d_3=\max_{1\le i\le 3} d_i}} \sum_{\substack{1\le v_3\le 2P/d_3 \\ v_3\ne gd_1d_2}} W(P;\mathbf{d},f,g,v_3). \tag{9}$$

For fixed $\mathbf{d}$, f, g and v_3 arising in the summation of (9), the equation (7) may be written in the form

$$6d_1^2v_1^2 + 6d_2^2v_2^2 + 2Av_1v_2 + 12d_1Bv_1 + 12d_2Bv_2 + C = 0,$$

where

$$A = 6d_1d_2 - fv_3, \quad B = d_3v_3 - gd_1d_2d_3 \quad \text{and} \quad C = 6B^2 + 2(gd_1d_2d_3)^2.$$

On completing the square, we obtain $X^2 + DY^2 = n$, where

$$D = 36d_1^2d_2^2 - A^2, \quad n = (36d_1^2d_2B - 6d_1AB)^2 - D(6d_1^2C - 36d_1^2B^2),$$

and

$$X = Dv_2 + 36d_1^2d_2B - 6d_1AB, \quad Y = 6d_1^2v_1 + Av_2 + 6d_1B. \tag{10}$$

Following a little computation, one finds that

$$n = 3(fd_1d_3)^2v_3(v_3 - gd_1d_2)\left(3(2v_3 - gd_1d_2)^2 + (gd_1d_2)^2\right),$$

and so n is non-zero, since for values of v_3, g, d_1 and d_2 occurring in the summation, one has $v_3 \ne gd_1d_2$. A little further calculation reveals that

$$D = -f^2v_3(v_3 - gd_1d_2),$$

whence D is also non-zero. Consequently, the map $(v_1, v_2) \to (X, Y)$ described by (10) is one-to-one. It follows that $W(P; \mathbf{d}, f, g, v_3)$ is bounded above by the number of solutions of the equation $X^2 + DY^2 = n$ with $|X| \le KP^3$ and $|Y| \le KP^3$, for a suitable absolute constant K. However, the elementary theory of binary quadratic forms (see, for example, Hua [1, Chapter 11] or Vaughan and Wooley [4, Lemma 3.5]) shows that the latter number is $O_\epsilon((DnP)^\epsilon)$. Thus we obtain

$$W(P; \mathbf{d}, f, g, v_3) \ll_\epsilon P^\epsilon. \tag{11}$$

On combining (9) and (11), we obtain

$$S(P) \ll P^{2\epsilon} \max_{1 \le H \le P} \sum_{gf=12} \sum_{H \le |h| \le 2H} \sum_{\substack{gd_1d_2d_3=h \\ d_3=\max\{d_1,d_2,d_3\}}} P/d_3.$$

The summation condition on d_3 ensures that $d_3 \gg H^{1/3}$, whence by using an elementary estimate for the divisor function we finally deduce that

$$S(P) \ll P^{3\epsilon} \max_{1 \le H \le P} H(PH^{-1/3}) \ll P^{5/3+3\epsilon},$$

which completes the proof of the theorem.

References

1. L.-K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin, 1982.
2. C. Hooley, *On the representation of a number as a sum of two cubes*, Math. Z. **82** (1963), 259–266.
3. C. Hooley, *On the numbers that are representable as the sum of two cubes*, J. Reine Angew. Math. **314** (1980), 146–173.
4. R. C. Vaughan and T. D. Wooley, *Further improvements in Waring's problem*, Acta Math. **174** (1995), 147–240.

Mathematics Department, University of Michigan, Ann Arbor, Michigan, 48109-1003
E-mail address: wooley@math.lsa.umich.edu