*Glasgow Math. J.* **42** (2000) 225–237. © Glasgow Mathematical Journal Trust 2000. Printed in the United Kingdom

# ON THE RATIONAL POINTS ON CUBIC SURFACES

C. HOOLEY

*School of Mathematics, University of Wales, Cardiff, Senghennydd Road, Cardiff CF2 4YN*

(Received 27 July, 1998)

**Abstract.** It is shewn that, if $N(P)$ be the number of solutions of the indeterminate equation

$$ax^3 + by^3 + cz^3 + dw^3 = 0 \qquad (a, b, c, d \neq 0)$$

for which $|x|, |y|, |z|, |w| \leq P$, then

$$N(P) = KP^2 + o(P^2),$$

where, to within a term $O(P)$, $KP^2$ is the contribution to $N(P)$ corresponding to the rational lines in the projective surface defined by the equation. This proves a conjecture made by Heath-Brown, who has studied $N(P)$ under the assumption of the Riemann Hypothesis for certain Hasse-Weil $L$-functions. The remainder term $o(P^2)$ in the formula represents $O(P^{\frac{4}{3}+\varepsilon})$, $O(P^{\frac{5}{3}+\varepsilon})$, or $O(P^2/\sqrt[3]{\log P})$ according as the surface contains three, one, or no rational lines.

1991 *Mathematics Subject Classification*. 11P99.

Developing inter alia an idea introduced by the author in [**8**], Heath-Brown [**3**] has used his important new version of the circle method to obtain a remarkable conditional theorem on the rational points on (non-singular) projective cubic surfaces defined by quaternary diagonal cubic forms, namely, *subject to the Riemann Hypothesis for certain Hasse-Weil L-functions, the equation*

$$ax^3 + by^3 + cz^3 + dw^3 = 0 \qquad (a, b, c, d \neq 0) \tag{1}$$

*has only* $O(P^{\frac{3}{2}+\varepsilon})$ *solutions in integers of magnitude not exceeding P save for those that correspond to points on rational lines in the surface* $\mathcal{C}$ *the equation defines*. In other words, if $N(P)$ denote the total number of solutions for which $|x|, |y|, |z|, |w| \leq P$, then

$$N(P) = KP^2 + O(P^{\frac{3}{2}+\varepsilon}), \tag{2}$$

where, to within a term $O(P)$, $KP^2$ is the contribution to $N(P)$ due to any rational lines in the surface, where $K$ is easily calculated in terms of $a, b, c, d$, and where of course $K = 0$ when there are no such rational lines. Among the notable features of the method, we should especially mention the unusual way in which the main term of the formula arises from arcs in the circle method that correspond to rationals with large denominators.

To gauge the significance of the result and the extent of its departure from the relatively trival, we should briefly indicate the expanse of our previous knowledge on

the matter. First, since the number of representations of a number $m$ by a (non-degenerate) binary cubic form is $O\{d_3(m)\}$ (see our paper [**7**] for the irreducible case, the reducible case being much easier), we immediately gain the estimate

$$N(P) = O(P^{2+\varepsilon}),$$

which we might be inclined through elaborate divisor sum methods to refine to

$$N(P) = O(P^2 \log^E P)$$

were it not for there being more favourable avenues to follow. Indeed, letting $r(n)$ be the number of representations of $n$ as the sum of two cubes of either sign, we should mention that the superior bound

$$N(P) = O(P^2) \tag{3}$$

flows from Hölder's inequality and the estimate

$$\sum_{n \leq x} r^2(n) = O(x^{\frac{2}{3}}) \tag{4}$$

that is a corollary of asymptotic formulae of the form

$$\sum_{n \leq x} r^2(n) = 2E_1 x^{\frac{2}{3}} + o(x^{\frac{2}{3}}) \tag{5}$$

obtained in several of our earlier papers (see, in particular, [**5**] and [**6**]). Easily deduced from (4) in several ways (perhaps the most transparent method is through the use of the exponential sum $f(\theta) = \sum_{|m| \leq P} e^{2\pi i m^3 \theta}$ and the product $f(a\theta) f(b\theta) f(c\theta) f(d\theta)$), the formula (3) is actually best possible as a universal order relation because of the barrier to further improvement in the exponent of $P$ presented by the contribution $N_1(P)$ to $N(P)$ due to solutions corresponding to rational lines on $\mathcal{C}$. The significance of Heath-Brown's theorem is therefore that it gives a useful conditional estimate for the difference

$$N_0(P) = N(P) - N_1(P) \tag{6}$$

that is substantially less than the estimate $O(P^2)$ implied by what has already been stated, a result that had been only known both unconditionally and more or less explicitly for diagonal forms in situations derived from the case $a, b, c, d = \pm 1$ that is associated with (5); in particular, an improvement in the order relation (3) is implied when there are no rational lines on $\mathcal{C}$.

The purpose of the present communication is to provide an unconditional proof of a version of Heath-Brown's theorem in which the remainder term in (2) is usually weaker than the $O(P^{\frac{3}{2}+\varepsilon})$ appearing therein but is always superior to the uninteresting $O(P^2)$; in particular, therefore, his conjecture (1.4) in [**3**] will be substantiated. More or less both obvious and known when there are three rational lines on $\mathcal{C}$, the proof increasingly depends on new features not explicitly present in previous literature on the subject as the number of rational lines decreases, the treatment

https://doi.org/10.1017/S0017089500020073 Published online by Cambridge University Press

when there are no such lines being almost entirely new and constituting the most important part of the exposition. Beyond this we need say no more at present, since what we do and its connections with other work will be clear from the relevant portions of the text.

In what follows $E_1, E_2, \ldots$ denote positive constants depending at most on $a, b, c, d$, the constants implied by the $O$-notation being of this type except when they also depend on an arbitrarily small positive constant $\epsilon$; the letter $P$ denotes a positive variable that is to be regarded as tending to infinity; from time to time we shall express non-zero integers such as $h$ uniquely in the form $h_1 h_2^3$, where $h_1$ is positive, cube-free, and termed the positive cube-free part of $h$; the notation $p||h$ means as usual that $p$ is the highest power of the (positive) prime $p$ that divides $h$; $(a_1, \ldots, a_r)$ denotes the (positive) highest common factor of integers $a_1, \ldots, a_r$ when this is defined. Also during the proof it may obviously be assumed that

$$(a, b, c, d) = 1 \tag{7}$$

although this restriction is irrelevant to the final conclusions.

With the aid of the numbers $A = \sqrt[3]{a}$, $B = \sqrt[3]{b}$, $C = \sqrt[3]{c}$, $D = \sqrt[3]{d}$, and a complex cube root of unity $\omega$, we classify the surfaces $\mathcal{C}$ and their modes of treatment according to how many of the 27 lines on each surface are rational. Since the lines

$$\begin{aligned} &Ax + \omega^i By = 0,\ Cz + \omega^j Dw = 0 \qquad (0 \le i, j \le 3);\\ &Ax + \omega^i Cz = 0,\ By + \omega^j Dw = 0 \qquad (0 \le i, j \le 3);\\ &Ax + \omega^i Dz = 0,\ By + \omega^j Cw = 0 \qquad (0 \le i, j \le 3); \end{aligned}$$

clearly lie on $\mathcal{C}$ and are in number 27, they exhaust all the lines on the surface, the only possible rational ones being therefore

$$Ax + By = 0, \qquad Cz + Dw = 0; \tag{8}$$

$$Ax + Cz = 0, \qquad By + Dw = 0; \tag{9}$$

$$Ax + Dw = 0, \qquad By + Cw = 0. \tag{10}$$

If all three of the above lines be rational, then $A, B, C, D$ are in rational ratio and conversely, in which case

$$A^3 : B^3 : C^3 : D^3 :: \kappa^3 : \lambda^3 : \mu^3 : \nu^3$$

with $(\kappa, \lambda, \mu, \nu) = 1$ so that $A, B, C, D$ are integers by (7). Thus in this instance the equation of $\mathcal{C}$ takes the form

$$(Ax)^3 + (By)^3 + (Cz)^3 + (Dw)^3 = 0. \tag{11}$$

To continue the classification we note that there cannot be exactly two rational lines. This is because, if, say, the first line (8) were rational, then the rationality of any plane occurring in (9) or (10) would imply that $A, B, C, D$ were in rational ratio and hence that there were three rational lines. We must therefore next consider the

https://doi.org/10.1017/S0017089500020073 Published online by Cambridge University Press

case where there is just one rational line, which may be taken typically to be (8) by an appropriate ordering of the terms in the diagonal form. Thus now each of the pairs $A, B$ and $C, D$ are in rational ratio whereas $A, C$; $A, D$; $B, C$; $B, D$ are not. Hence common positive cube-free parts $\lambda_1$ and $\lambda_2$ are shared by $a, b$ and $c, d$, respectively, whence

$$a = \lambda_1 a_1^3, \quad b = \lambda_1 b_1^3, \quad c = -\lambda_2 c_1^3, \quad d = -\lambda_2 d_1^3, \tag{12}$$

where $\lambda_1 \neq \lambda_2$ and where also

$$(\lambda_1, \lambda_2) = 1 \tag{13}$$

by (7). Consequently in this situation the equation of $\mathcal{C}$ can be thrown into the form

$$\lambda_1\{(a_1 x)^3 + (b_1 y)^3\} - \lambda_2\{(c_1 z)^3 + (d_1 w)^3\} = 0. \tag{14}$$

There remains the instance where there is no rational line on $\mathcal{C}$. This is examined by considering separately the cases where at least one of the planes in (8), (9), and (10) is rational and where none of them is. Taking for the moment only the former as being the easier to treat, we may suppose that $Cz + Dw = 0$ is a rational plane by an appropriate arrangement of terms with the consequence that $c = -\lambda_2\, c_1^3$, $d = -\lambda_2\, d_1^3$ as in (12); the equation can thus be cast into the shape

$$ax^3 + by^3 - \lambda_2\{(c_1 z)^3 + (d_1 w)^3\} = 0 \tag{15}$$

in which $ax^3 + by^3$ is an irreducible form.

We are ready to dispose of our problem in all situations saving the last one left undiscussed in the previous paragraph. In the first one where (11) is applicable, $N_0(P)$ in (6) evidently does not exceed the number of solutions of

$$X^3 + Y^3 + Z^3 + W^3 = 0$$

for which $|X|, |Y|, |Z|, |W| \leq E_2\, P$ and for which none of $X + Y$, $Z + W$, $X + Z$, $Y + W$, $X + W$, $Y + Z$ is zero. This matter was treated by the author ([**5**] and [**6**]; see especially the comment in the antepenultimate paragraph of the introduction to the former) and then considerably later by Wooley [**9**] and Heath-Brown [**2**], whose successive results imply that

$$N_0(P) = O(P^{\eta+\varepsilon}) \tag{16}$$

for the exponents $\frac{5}{3}, \frac{5}{3}, \frac{4}{3}$, respectively.

In the second situation where (14) is relevant, $N_0(P)$ does not exceed the number of solutions of

$$\lambda_1(X^3 + Y^3) = \lambda_2(Z^3 + W^3) \tag{17}$$

in integers $X, Y, Z, W$ for which $|X|, |Y|, |Z|, |W| \leq E_3\, P$ and $X + Y$, $Z + W$ are non-zero. Hence, save for the presence of the cube-free coefficients $\lambda_1$, $\lambda_2$, the subject of bounding $N_0(P)$ seems much the same as before and, in particular therefore, to the one regarding solutions of

$$l^3 + m^3 = \lambda^3 + \mu^3; \quad \lambda \neq l, m; \quad \mu \neq l, m$$

that was raised in our already cited [**5**]. Yet, although the solution of the latter problem was also contained in the following paper [**6**] on sums of two $h$-th powers for odd values of $h \geq 3$, it is important to note that the method of the later paper cannot suit our present needs because the appearance of $\lambda_1$, $\lambda_2$ in (17) means that substitutions akin to (9) in [**6**] are no longer available; in like manner, the methods of Wooley and Heath-Brown in [**9**] and [**2**], respectively, are not applicable in these more general circumstances. We therefore briefly indicate the initial transformations that are needed to prepare (17) for the operation of the method in [**5**], then summarizing for completeness the interconnection between [**6**] and both $N_0(P)$ and [**5**].

Since in bounding the order of magnitude of $N_0(P)$ we may clearly restrict attention to the case where $X - Y, Z - W \geq 0$, we set

$$r' = X + Y, \quad s = X - Y, \quad \rho' = Z + W, \quad \sigma = Z - W$$

much as in (4) of [**5**] and, having deduced that $0 < r', \rho' \leq E_4\, P$ and $0 \leq s, \sigma \leq E_4\, P$, obtain the two equivalent equations

$$\lambda_1 r'(r'^2 + 3s^2) = \lambda_2 \rho'(\rho'^2 + 3\sigma^2) \tag{18}$$

and

$$3\lambda_1 r' s^2 - 3\lambda_2 \rho' \sigma^2 = \lambda_2 \rho'^3 - \lambda_1 r'^3 \tag{19}$$

in the second of which the right-hand side is non-zero because $\lambda_1$, $\lambda_2$ are unequal cube-free numbers. Next, if $(r', \rho') = \delta$, let

$$r' = \delta r'', \rho' = \delta \rho'', \quad \text{where } (r'', \rho'') = 1, \tag{20}$$

and then set $(r'', \lambda_2) = \delta_2$ and $(\rho'', \lambda_1) = \delta_1$ so that

$$r'' = \delta_2\, r, \rho'' = \delta_1 \rho, \lambda_1 = \delta_1 \lambda_1', \lambda_2 = \delta_2 \lambda_2', (r, \lambda_2') = 1, (\rho, \lambda_1') = 1$$

and

$$0 < r \leq E_4 P/\delta\delta_2, \quad 0 < \rho \leq E_4 P/\delta\delta_1.$$

Then, for each set of relevant values of $\delta, \delta_1, \delta_2$, we consider either the derivatives

$$\lambda_1' r(\delta^2 \delta_2^2 r^2 + 3s^2) = \lambda_2' \rho(\delta^2 \delta_1^2 \rho^2 + 3\sigma^2), \quad (\lambda_1' r, \lambda_2' \rho) = 1$$

of (18) and (13) or the derivative

$$3\lambda_1' r s^2 - 3\lambda_2' \rho \sigma^2 = \delta^2(\lambda_2' \delta_1^2 \rho^3 - \lambda_1' \delta_2^2 r^3)$$

of (19) according as $\delta \leq P^{\frac{1}{2}}$ or $\delta > P^{\frac{1}{2}}$. These are the central elements in the estimation of sums that are closely analogous, respectively, to $v^{\dagger}(x, \delta)$ and $v^{**}(x)$ in [**5**], the effect of the bounded parameters $\lambda_1'$, $\lambda_2'$, $\delta_1$, $\delta_2$ being merely to bring in some unimportant complication into the previous treatment. We therefore end up with the estimate

https://doi.org/10.1017/S0017089500020073 Published online by Cambridge University Press

$$N_0(P) = O(P^{\frac{5}{3}+\varepsilon}) \tag{21}$$

that generalizes Theorem 1 in [**5**].

An advantage of the later paper [**6**] over [**5**] is the generality of the method used for the estimation of exponential seems. We may therefore with some advantage substitute this treatment in both [**5**] and our proof of (21) but otherwise leave the structure of [**5**] intact.

In the first case of the third situation where (15) is the underlying equation, $N_0(P)$ does not exceed the number of solutions

$$ax^3 + by^3 = \lambda_2(Z^3 + W^3)$$

satisfying $|x|, |y| \leq P$ and $|Z|, |W| \leq E_5\, P$. The cardinality of those for which $Z + W = 0$ being $O(P)$ by the irreducibility of $ax^3 + by^3$, we may restrict $Z + W$ to be positive when determining the order of magnitude of the number $N_2(P)$ of the remaining solutions. Hence, writing

$$\rho = Z + W, \sigma = Z - W, \quad \text{where } 0 < \rho \leq 2E_5\, P,$$

we are faced with the equation

$$4(ax^3 + by^3) = \lambda_2\rho(\rho^2 + 3\sigma^2), \tag{22}$$

of which, having set $x = \Delta x'$, $y = \Delta y'$, $\rho = \Delta\rho'$, $\sigma = \Delta\sigma'$ where $(x', y', \rho', \sigma') = 1$ and then having suppressed the (notational) primes, we investigate the primitive solutions that are subject to the inequalities

$$|x|, |y| \leq P/\Delta, \qquad 0 < \rho \leq 2E_5P/\Delta. \tag{23}_{P/\Delta}$$

Then, since certainly

$$(x, y, \rho) \Big| 3\lambda_2 \tag{24}$$

in the situation we have reached, we deduce that

$$N_0(P) = O\left(\sum_{\Delta \leq P} N_2(P/\Delta)\right) + O(P),$$

where $N_2(P')$ is the number of solutions of (22) for which $(23)_{P'}$ and (24) hold. The replacement of (18) by (22) actually makes the treatment of $N_2(P')$ easier than the previous one for $N_0(P)$ because the work no longer involves a transformation of type (20) with a consequent split of the analysis into two parts. Indeed, on replacing $\sigma^2$ by a member of a set obtained by eliminating quadratic non-residues, modulis various primes $p$, we can follow closely with the participation of (22) the treatment of [**5**, Section 4 onwards] to arrive at the conclusion that

$$N_2(P') = O(P'^{\frac{5}{3}+\varepsilon}),$$

https://doi.org/10.1017/S0017089500020073 Published online by Cambridge University Press

whence

$$N_0(P) = O\left(P^{\frac{5}{3}+\varepsilon} \sum_{\Delta \leq P} \frac{1}{\Delta^{\frac{5}{3}}}\right) + O(P) = O(P^{\frac{5}{3}+\varepsilon}). \tag{25}$$

In particular, hardly any change is needed in the examination by Deligne's theories of the exponential sums appertaining to products $d$ of the primes $p$ featuring in the large sieve process.

The cases so far examined have been settled for the most part by fairly transparent modifications of some of the author's earlier methods, although we should stress that in one instance a superior result stems from Heath-Brown's method in [**2**]. In contrast, the final and most important case must be treated by another method, the description of which is the most significant part of this paper. To initiate the proceedings, we state some presumably familiar properties of pure cubic fields and include their proofs for convenience. Let $\theta_1 = \sqrt[3]{D_1}$, $\theta_2 = \sqrt[3]{D_2}$, where neither $\theta_1$ nor $\theta_2$ is rational. Then *the pure cubic fields* $R_1 = \mathbb{Q}(\theta_1)$, $R_2 = \mathbb{Q}(\theta_2)$ *are the same if and only if either* $\theta_2/\theta_1$ *or* $\theta_2/\theta_1^2$ *be rational* (the rationality of $\theta_2/\theta_1^2$ is obviously equivalent to that of $\theta_2^2/\theta_1$). The sufficiency of the condition being clear, let us suppose that $R_1$ and $R_2$ be the same so that there are rational numbers $a, b, c$ such that

$$\theta_2 = a\theta_1^2 + b\theta_1 + c, \tag{26}$$

whence, on taking conjugates, we also have

$$\omega^*\theta_2 = a\omega^2\theta_1^2 + b\omega\theta_1 + c, \tag{27}$$

and

$$\omega^{*2}\theta_2 = a\omega\theta_1^2 + b\omega^2\theta_1 + c, \tag{28}$$

for complex cube roots of unity $\omega$ and $\omega^*$. If $\omega^* = \omega$, the linear combination (26) + $\omega^2$ (27) + $\omega$ (28) yields

$$3\theta_2 = a(1 + \omega + \omega^2)\theta_1^2 + 3b\theta_1 + c(1 + \omega^2 + \omega) = 3b\theta_1$$

and $\theta_2/\theta_1$ is therefore rational; alternatively, if $\omega^* = \omega^2$, the rationality of $\theta_2/\theta_1^2$ is implied by the combination (26) + $\omega$ (27) + $\omega^2$ (28) that is tantamount to

$$3\theta_2 = 3a\theta_1^2 + b(1 + \omega^2 + \omega)\theta_1 + c(1 + \omega + \omega^2) = 3a\theta_1^2.$$

Also, if $R_1$, $R_2$ *be distinct, then the degree of* $S = \mathbb{Q}(\theta_1, \theta_2)$ *over* $\mathbb{Q}$ *is* 9 *and the degree of* $T = \mathbb{Q}(\theta_1, \theta_2, \omega)$ *over* $\mathbb{Q}$ *is* 18. To establish the first part it suffices to prove that the degree of $\theta_2$ over $R_1$ is 3 and therefore that it is not 2. But, if this degree were in fact 2, then $\theta_2$ would satisfy a quadratic equation with real coefficients, which property is impossible because the only real quadratic factor of the minimum polynomial of $\theta_2$ over $\mathbb{Q}$ has purely imaginary zeros. The last part follows because $\omega$ cannot belong to the real field $S$.

Because of the present assumption that all the planes in (8), (9), and (10) are non-rational, each pair of terms on the left of (1) such as $ax^3$ and $by^3$ give rise to a pure cubic field, which in the example chosen is the field $\mathbb{Q}\left(\sqrt[3]{\frac{a}{b}}\right) = \mathbb{Q}\left(\sqrt[3]{\frac{b}{a}}\right)$

https://doi.org/10.1017/S0017089500020073 Published online by Cambridge University Press

$= \mathbb{Q}\left(\sqrt[3]{a^2b}\right)$ generated by the real root of the equation $au^3 + b = 0$. If the fields corresponding to each side of the equation

$$ax^3 + by^3 = -cz^3 - dw^3$$

were the same, then $a^2b$ would have the same cube-free part as either $c^2d$ or $cd^2$, it being possible to insist on the former occurrence by rearranging the last two terms on the left of (1) if necessary. Next, if likewise the fields related to each side of

$$ax^3 + dw^3 = -by^3 - cz^3$$

were also identical, then $a^2d$ would have the same cube-free part as either $b^2c$ or $bc^2$. In the former instance, we would altogether deduce that both

$$\frac{a^2b}{c^2d}\frac{a^2d}{b^2c} = \frac{a^3}{c^3}\frac{a}{b} \text{ and } \frac{a^2b}{c^2d}\frac{b^2c}{a^2d} = \frac{b^3}{cd^2} = \frac{b^3}{d^3}\frac{d}{c}$$

were rational cubes, while in the latter instance we similarly would see that

$$\frac{a^2b}{c^2d}\frac{a^2d}{bc^2} = \frac{a^3}{c^3}\frac{a}{c} \text{ and } \frac{a^2b}{c^2d}\frac{bc^2}{a^2d} = \frac{b^2}{d^2} = \frac{b^3}{d^3}\frac{d}{b}$$

were rational cubes. Hence either $a/b$ and $c/d$ or $a/c$ and $b/d$ would be rational cubes in opposition to the prevailing circumstances. Thus, by a suitable permutation of the terms in (1), we may certainly assume that the equation of the surface $\mathcal{C}$ can be expressed as

$$ax^3 + by^3 = -cz^3 - dw^3,$$

where the pure cubic fields $R_1 = \mathbb{Q}\left(\sqrt[3]{a^2b}\right)$ and $R_2 = \mathbb{Q}\left(\sqrt[3]{c^2d}\right)$ are distinct.

Having cast the equation of $\mathcal{C}$ into a suitable form, we continue by first letting $r_{e,f}(n) = r_{e,f}(-n) = r_{e,f,P}(n)$ be the number of representations of the number $n$ by the irreducible form $el^3 + fm^3$ for which $|l|, |m| \leq P$ and by then defining $\rho_{e,f}(n)$ to be 1 or 0 according as $n$ (and therefore $-n$) is representable by the form or not. Then, by these definitions and the Cauchy-Schwarz inequality,

$$\begin{aligned} N_0(P) &= \sum_n r_{a,b}(n) r_{c,d}(n) = \sum_n r_{a,b}(n)\rho_{c,d}(n) r_{c,d}(n)\rho_{a,b}(n) \\ &\leq \left(\sum_n r_{a,b}^2(n)\rho_{c,d}(n)\right)^{\frac{1}{2}} \left(\sum_n r_{c,d}^2(n)\rho_{a,b}(n)\right)^{\frac{1}{2}} \\ &= (S_1 S_2)^{\frac{1}{2}}, \text{ say,} \end{aligned} \tag{29}$$

it being sufficient in what follows to unfold the estimation of $S_1$. Next

https://doi.org/10.1017/S0017089500020073 Published online by Cambridge University Press

$$\begin{aligned} S_1 &= \sum_n r_{a,b}(n)\rho_{c,d}(n) + \sum_n \big(r_{a,b}^2(n) - r_{a,b}(n)\big)\rho_{c,d}(n) \\ &\le \sum_n r_{a,b}(n)\rho_{c,d}(n) + \sum_n \big(r_{a,b}^2(n) - r_{a,b}(n)\big) \\ &= S_3 + S_4, \text{ say,} \end{aligned} \tag{30}$$

in which the sum $S_4$ is bounded by the earlier methods in the paper. In fact, since

$$\begin{aligned} \sum_n r_{a,b}^2(n) &= \sum_{\substack{ax^3+by^3=az^3+bw^3 \\ |x|,|y|,|z|,|w|\le P}} 1 = \sum_{|x|,|y|\le P} 1 + \sum_{\substack{ax^3+by^3=az^3+bw^3 \\ |x|,|y|,|z|,|w|\le P \\ x\ne z; y\ne w}} 1 \\ &= \sum_n r_{a,b}(n) + \sum_{\substack{ax^3+by^3=az^3+bw^3 \\ |x|,|y|,|z|,|w|\le P \\ x\ne z; y\ne w}} 1, \end{aligned}$$

we deduce, on altering the signs of $y$ and $z$, that $S_4$ is the number of solutions of

$$a(x^3 + z^3) = b(y^3 + w^3) \tag{31}$$

for which $|x|, |y|, |z|, |w| \le P$ and $x + z, y + w \ne 0$. Hence, by the second case considered above, we deduce that

$$S_4 = O(P^{\frac{5}{3}+\varepsilon}) \tag{32}$$

since the surface (31) has only one rational line within it.

The estimation of $S_3$ begins by our developing a weak criterion for deciding whether $\rho_{c,d}(n)$ be non-zero or zero. To this end, let $p$ denote any prime satisfying

$$p \nmid abcd, \qquad p \equiv 1 \pmod 3. \tag{33}$$

Then, if $c\lambda^3 + d\mu^3$ be divisible by $p$ but not by $p^2$, we infer that both $\lambda$ and $\mu$ are indivisible by $p$ and hence that the congruence

$$c\Omega^3 + d \equiv 0 \pmod p$$

is not only soluble but has three distinct roots, mod $p$, which state of affairs by a principle due to Dedekind is tantamount to the prime $p$ being a product of three distinct linear prime ideals in the corpus $\mathbb{Q}(\sqrt[3]{c^2d})$. Consequently, rephrasing this deduction to suit the method to follow, we infer that any number $n$ representable by $c\lambda^3 + d\mu^3$ does not have the property that it is divisible by $p$ but indivisible by $p^2$ for any prime $p$ satisfying (33) that does not split totally into three distinct prime ideals in $\mathbb{Q}(\sqrt[3]{c^2d})$. (Note this is valid when $n = 0$.) The ground has thus been laid for the application of a sieve method to the majorization of $S_3$ in (30). Let $\delta$ denote, generally, a positive square-free number composed entirely of primes $p$ corresponding to the unwanted properties and then let the notation $\delta || n$ indicate the conjunction of the conditions $p || n$ for all prime divisors $p$ of $\delta$. Then, by Brun's method (see, for example, our tract [**4**] and Halberstam and Richert [**1**]; the former work describes a general situation covering the present type of sieving, while the latter gives full

https://doi.org/10.1017/S0017089500020073 Published online by Cambridge University Press

details of Brun's method when it is applied in circumstances that are slightly different from those here), there is a suitable modification $\mu'(\delta)$ of the Möbius function such that

(i) $\mu'(\delta) = \mu(\delta)$ or 0,

(ii) $\mu'(\delta) = 0$ for $\delta > P^{\alpha} = Q$, where $0 < \alpha < 1$,

(iii) $\rho_{c,d}(n) \leq \sum_{\delta||n} \mu'(\delta)$,

(iv) $\mu'(\delta)$ has properties that enable equation (39) below to be substantiated in the light of what we shall shortly discover about a function $\Psi(\delta)$ to be introduced.

Next, by (30),

$$\begin{aligned} S_3 &\leq \sum_n r_{a,b}(n) \sum_{\delta||n} \mu'(\delta) = \sum_{|l|,|m|\leq P} \sum_{\delta||(al^3+bm^3)} \mu'(\delta) \\ &= \sum_{\delta\leq Q} \mu'(\delta) \sum_{\substack{\delta||(al^3+bm^3) \\ |l|,|m|\leq P}} 1 \\ &= \sum_{\delta\leq Q} \mu'(\delta)\ \Psi(\delta, P), \text{ say,} \end{aligned} \tag{34}$$

to proceed from which we must investigate $\Psi(\delta, P)$ and the associated function $\Psi(\delta)$ that is the number of solutions of $\delta||(al^3 + bm^3)$ satisfying $0 < l, m \leq \delta^2$.

Since the solutions of $p||(al^3 + bm^3)$ arrange themselves in residue classes (mod $p^2$), we infer first that $\Psi(\delta)$ is a multiplicative function of $\delta$ and then that

$$\begin{aligned} \Psi(\delta, P) &= \sum_{\substack{\delta||(ah^3+bk^3) \\ 0<h,k\leq\delta^2}} \sum_{\substack{|l|,|m|\leq P \\ l-h\equiv m-k\equiv 0 \ (\mathrm{mod}\ \delta^2)}} 1 \\ &= \sum_{\substack{\delta||(ah^3+bk^3) \\ 0<h,k\leq\delta^2}} \left(\frac{2P+1}{\delta^2} + O(1)\right)\left(\frac{2P+1}{\delta^2} + O(1)\right) \\ &= \frac{4P^2\Psi(\delta)}{\delta^4} + O\left(\frac{P\Psi(\delta)}{\delta^2}\right) \end{aligned} \tag{35}$$

for $\delta \leq Q$ and $\alpha \leq \frac{1}{2}$. Secondly, to examine $\Psi(\delta)$ we study $\Psi(p)$, whose non-vanishing by an argument previously applied to $c\lambda^3 + d\mu^3$ implies that the congruence

$$a\Omega^3 + b \equiv 0 \ (\mathrm{mod}\ p)$$

is soluble and hence that $p$ is a product of three distinct linear ideals in $\mathbb{Q}(\sqrt[3]{a^2b})$. Also, in these circumstances, the numbers of incongruent solutions, modulis $p$ and $p^2$, of

$$ah^3 + bk^3 \equiv 0 \ (\mathrm{mod}\ p), \qquad ah^3 + bk^3 \equiv 0 \ (\mathrm{mod}\ p^2)$$

for which $p \nmid hk$ are $3(p-1)$ and $3p(p-1)$, respectively, so that

https://doi.org/10.1017/S0017089500020073 Published online by Cambridge University Press

$$\Psi(p) = 3p^2(p-1) - 3p(p-1) = 3p(p-1)^2. \tag{36}$$

Hence, returning to (34), we get

$$\begin{aligned} S_3 &\leq 4P^2 \sum_{\delta \leq Q} \frac{\mu'(\delta)\Psi(\delta)}{\delta^4} + O\left(P \sum_{\delta \leq Q} 3^{\omega(\delta)}\delta\right) \\ &= 4P^2 \sum_{\delta \leq Q} \frac{\mu'(\delta)\Psi(\delta)}{\delta^4} + O(PQ^2 \log^2 Q) \\ &= 4P^2 \sum\nolimits_1 + O(P^{\frac{7}{4}}), \text{ say,} \end{aligned} \tag{37}$$

if we choose $\alpha$ to be $\frac{1}{3}$.

The sieving primes in the process are thus those satisfying (33) which split totally into three distinct linear prime ideals in $\mathbb{Q}(\sqrt[3]{a^2b})$ but not in $\mathbb{Q}(\sqrt[3]{c^2d})$ and which therefore belong to the set $\mathcal{A} = \mathcal{A}_1 - \mathcal{A}_2$, where $\mathcal{A}_1$ is the set of primes in (33) splitting totally into three distinct linear prime ideals in $\mathbb{Q}(\sqrt[3]{a^2b})$ and $\mathcal{A}_2$ is the set in (33) splitting totally into three distinct linear prime ideals in both $\mathbb{Q}(\sqrt[3]{a^2b})$ and $\mathbb{Q}(\sqrt[3]{c^2d})$. The condition $p \equiv 1 \pmod 3$ is seen to be superfluous in the definitions of $\mathcal{A}_1, \mathcal{A}_2$ but serves to remind us that $p$ splits totally into three distinct linear prime ideals in $\mathbb{Q}(\omega)$, whereupon we are prompted to define the members of $\mathcal{A}_1, \mathcal{A}_2$ with reference to their factorizations in the *normal* corpora $U_1 = \mathbb{Q}(\sqrt[3]{a^2b}, \omega)$ and $U_2 = \mathbb{Q}(\sqrt[3]{a^2b}, \sqrt[3]{c^2d}, \omega)$ of respective degrees 6 and 18. The condition that $p$ belong to $\mathcal{A}_i$ being that it split totally into distinct linear prime ideals $\mathfrak{p}_i$ in $U_i$ by the theory of ideals, we can employ the prime ideal theorem in a familiar way to yield

$$\sum_{\substack{p \leq u \\ p \in \mathcal{A}_1}} 1 = \frac{1}{6} \sum_{\mathrm{N}\mathfrak{p}_i \leq u} 1 + O(u^{\frac{1}{2}}) = \frac{1}{6} \mathrm{li}\, u + O\left(ue^{-E_6\sqrt{\log u}}\right)$$

and

$$\sum_{\substack{p \leq u \\ p \in \mathcal{A}_2}} 1 = \frac{1}{18} \sum_{\mathrm{N}\mathfrak{p}_i \leq u} 1 + O(u^{\frac{1}{2}}) = \frac{1}{18} \mathrm{li}\, u + O\left(ue^{-E_6\sqrt{\log u}}\right)$$

because in a normal corpus a rational prime $p$ has a linear prime ideal factor if and only if it split totally into a product of such ideals (which will be distinct when $p$ does not divide the discriminant). Consequently

$$\sum_{\substack{p \leq u \\ p \in \mathcal{A}}} 1 = \frac{1}{9} \mathrm{li}\, u + O\left(ue^{-E_6\sqrt{\log u}}\right). \tag{38}$$

The sieving procedure and the remainder of the estimation are quickly completed. By Brun's procedure and what has been said earlier about the function $\mu'(\delta)$, the sum $\sum_1$ in (37) does not exceed

https://doi.org/10.1017/S0017089500020073 Published online by Cambridge University Press

$$E_7 \prod_{\substack{p \le Q \\ p \in A}} \left(1 - \frac{\Psi(p)}{p^4}\right) = E_7 \prod_{\substack{p \le Q \\ p \in A}} \left(1 - \frac{3(p-1)^2}{p^3}\right)$$
$$\le E_8 \prod_{\substack{p \le Q \\ p \in A}} \left(1 - \frac{3}{p}\right) \tag{39}$$
$$\le \frac{E_9}{\sqrt[3]{\log Q}} \quad \le \frac{E_{10}}{\sqrt[3]{\log P}}$$

owing to (36) and (38), from which inequality and (37) we conclude that

$$S_3 = O\left(\frac{P^2}{\sqrt[3]{\log P}}\right). \tag{40}$$

Then, going back to (29), we first infer from (30), (32), and (40) that

$$S_1, S_2 = O\left(\frac{P^2}{\sqrt[3]{\log P}}\right)$$

because $S_2$ is a sum of type $S_1$. Hence, finally,

$$N_0(P) = O\left(\frac{P^2}{\sqrt[3]{\log P}}\right), \tag{41}$$

with which estimate we end the analysis of the final case to be considered.

We then arrive via (16), (21), (25), and (41) at our

THEOREM. *Let $N(P)$ be the number of solutions of the indeterminate equation*

$$ax^3 + by^3 + cz^3 + dw^3 = 0 \qquad (a, b, c, d \neq 0)$$

*for which $|x|, |y|, |z|, |w| \le P$. Then*

$$N(P) = KP^2 + o(P^2),$$

*where, to within a correcting term $O(P)$, the contribution to $N(P)$ from the rational lines on the surface* (1) *is $KP^2$. Also, according as the surface contains three, one, or no rational lines, the remainder term $o(P^2)$ is actually*

$$O\left(P^{\frac{4}{3}+\varepsilon}\right), \quad O\left(P^{\frac{5}{3}+\varepsilon}\right), \quad \text{or } O\left(\frac{P^2}{\sqrt[3]{\log P}}\right),$$

*respectively.*

https://doi.org/10.1017/S0017089500020073 Published online by Cambridge University Press

## REFERENCES

**1.** H. Halberstam and H.-E. Richert, *Sieve Methods* (Academic Press, 1975).

**2.** D. R. Heath-Brown, The density of rational points on cubic surfaces, *Acta Arith.* **79** (1997), 17–30.

**3.** D. R. Heath-Brown, The circle method and diagonal cubic forms, *Phil. Trans. Royal Soc. London A* **356** (1998), 673–699.

**4.** C. Hooley, *Applications of sieve methods to the theory of numbers* (Cambridge University Press, 1976).

**5.** C. Hooley, On the numbers that are representable as the sum of two cubes, *J. Reine Angew. Math.* **314** (1980), 146–173.

**6.** C. Hooley, On another sieve method and the numbers that are a sum of two *h*th powers, *Proc. London Math. Soc. (3)* **43** (1981), 73–109.

**7.** C. Hooley, On the representation of numbers by binary cubic forms, *Glasgow Math. J.* **27** (1985), 95–98.

**8.** C. Hooley, On Waring's problem, *Acta Math.* **157** (1986), 49–97.

**9.** T. D. Wooley, Sums of two cubes, *Internat. Math. Res. Notes* **4** (1995), 181–184 (electronic).