ON THE REPRESENTATIONS OF NUMBERS BY BINARY CUBIC FORMS

by C. HOOLEY

In honorem Professoris Roberti Rankin annos LXX nati.

There are not a few situations in the theory of numbers where it is desirable to have as sharp an estimate as possible for the number $r(n)$ of representations of a positive integer n by an irreducible binary cubic form

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3.$$

A variety of approaches are available for this problem but, as they stand, they are all defective in that they introduce unwanted factors into the estimate. For instance, an estimate involving the discriminant of $f(x, y)$ is obtained if we adopt the Lagrange procedure [**5**] of using congruences of the type $f(\sigma, 1) \equiv 0$, mod n, to reduce the problem to one where $n = 1$. Alternatively, following Oppenheim (vid. [**2**]), Greaves [**3**], and others, we may appeal to the theory of factorization of ideals, which leads to unwanted logarithmic factors owing to the involvement of algebraic units. Having had need, however, in some recent work on quartic forms [**4**] for an estimate without such extraneous imperfections, we intend in the present note to prove that

$$r(n) = O\{d_3(n)\}$$

uniformly with respect to the coefficients of $f(x, y)$, where $d_s(n)$ denotes the number of ways of expressing n as a product of s factors.

We use a refinement of Lagrange's method, indicating at appropriate places where the original procedure is modified. At the beginning, in contrast with the classical development, we restrict our attention to primitive representations and consequently define $\rho(n)$ to be the number of solutions of $f(x, y) = n$ for which $(x, y) = 1$. It being sufficient to consider the case where $\rho(n) > 0$ when obtaining a bound for $\rho(n)$, let $n = f(\alpha, \gamma)$ be a primitive representation of n. Then, if β, δ be chosen so that $\alpha\delta - \gamma\beta = 1$, the form $f(x, y)$ is transformed by the unimodular substitution

$$x = \alpha X + \beta Y_1, \qquad y = \gamma X + \delta Y_1$$

into an equivalent form

$$F(X, Y_1) = nX^3 + B_1X^2Y_1 + C_1XY_1^2 + D_1Y_1^3$$

that has leading coefficient n and that represents n primitively $\rho(n)$ times. Next, singling out for each divisor δ of n the $\rho_\delta(n)$ primitive solutions of $F(X, Y_1) = n$ for which $(Y_1, n) = \delta$, we write

$$n = m\delta, \qquad Y_1 = Y\delta, \quad \text{where} \quad (Y, m) = 1, \tag{1}$$

https://doi.org/10.1017/S0017089500006108 Published online by Cambridge University Press

and express the equation of representation as

$$m\delta X^3+B_1\delta X^2Y+C_1\delta^2XY^2+D_1\delta^3Y^3=m\delta$$

and hence, on clearing common factors, as

$$G(X, Y)=NX^3+BX^2Y+CXY^2+DY^3=N, \tag{2}$$

where

$$N \mid m \tag{3}$$

and $G(X, Y)$ is a primitive irreducible form such that no prime divisor of N divides both B and C. Thus $\rho_8(n)$ does not exceed the number of solutions of (2) for which

$$(Y, N)=1. \tag{4}$$

We now break down the problem into one concerning the representation of unity by cubic forms. If N be not already 1, we suppose that (2) and (4) hold and then let M be a suitable divisor of N that exceeds 1. Then, since $(Y, M)=1$, there are integers Ξ, H, σ such that

$$X=M\Xi+\sigma\mathrm{H}, \qquad Y=\mathrm{H}, \tag{5}$$

$$0 \leqq \sigma < M, \qquad (\mathrm{H}, M)=1, \tag{6}$$

from which fact, on setting $\phi(\sigma)=G(\sigma, 1)$, we deduce that

$$\Gamma(\Xi, \mathrm{H})=\tfrac{1}{6}\phi'''(\sigma)M^3\Xi^3+\tfrac{1}{2}\phi''(\sigma)M^2\Xi^2\mathrm{H}+\phi'(\sigma)M\Xi\mathrm{H}^2+\phi(\sigma)\mathrm{H}^3=N. \tag{7}$$

If in this, following Lagrange, we were to take M to be N, we would deduce that $\phi(\sigma)\equiv 0$, mod N, and hence that 1 was represented by the form† $N^{-1}\Gamma(\Xi, \mathrm{H})$ with integral coefficients. Yet this leads to too many possible choices of $\Gamma(\Xi, \mathrm{H})$, and we must therefore attempt to limit these choices by using a smaller value of M.

In this endeavour, we note the identical congruences

$$\phi(\sigma)\equiv B\sigma^2+C\sigma+D \bmod N, \quad \phi'(\sigma)\equiv 2B\sigma+C \bmod N,$$

where the determinant C^2-4BD of $B\sigma^2+C\sigma+D$ is denoted by Δ. Next, writing

$$N=\prod_{p \mid N} p^{\alpha}$$

and defining γ for any prime divisor p of N by $p^{\gamma} \parallel \Delta$ with the convention that $\gamma=\infty$ when $\Delta=0$, we consider these congruences in conjunction with (7) in order to determine

$$M=\prod_{p \mid N} p^{\beta}$$

suitably in terms of α and γ.

If a prime divisor p of N divide B, we set $\beta=\alpha$ with the result that $\phi(\sigma)\equiv 0, \bmod p^{\alpha}$, by (6) and (7), all the coefficients in $\Gamma(\Xi, \mathrm{H})$ being divisible by p^{α}. Moreover,

† We have not felt it desirable to distinguish notationally between indeterminates in a form and their numerical specializations.

https://doi.org/10.1017/S0017089500006108 Published online by Cambridge University Press

this congruence has at most one root, mod p^β, since $p \nmid C$ and since therefore the congruence

$$\phi(\sigma_1)-\phi(\sigma_1)\equiv(\sigma_1-\sigma_2)\{B(\sigma_1+\sigma_2)+C\}\equiv 0, \bmod p^\beta,$$

implies that $\sigma_1\equiv\sigma_2$, mod p^β.

We assume that β satisfies the inequality $\frac{1}{2}\alpha\leqq\beta\leqq\alpha$ when we discuss its choice for the other prime divisors of N, the case where p is odd being considered first. Then, since M^2 and M^3 are divisible by p^α, we infer from (7) that

$$4\mathrm{H}^3(B\sigma^2+C\sigma+D)+4M\Xi\mathrm{H}^2(2B\sigma+C)\equiv 0, \bmod p^\alpha, \tag{8}$$

whence

$$(T^2-\Delta)+4M\Xi\bar{\mathrm{H}}BT\equiv 0, \bmod p^\alpha, \tag{9}$$

and then

$$W^2\equiv\Delta, \bmod p^\alpha, \tag{10}$$

where

$$T=2B\sigma+C, \qquad W=T+2M\Xi\bar{\mathrm{H}}B, \tag{11}$$

and $\bar{\mathrm{H}}$ is a solution of $\mathrm{H}\bar{\mathrm{H}}\equiv 1, \bmod p^\alpha$. To count the number of incongruent solutions of (10), consider first the case $\gamma<\alpha$ including that where $\gamma=0$. Here $p^\gamma \parallel W^2$ so that we deduce in turn that γ is even,

$$W=p^{\gamma/2}W_1, \text{ say}, \tag{12}$$

and

$$W_1^2\equiv\Delta p^{-\gamma}, \bmod p^{\alpha-\gamma},$$

where $p \nmid \Delta p^{-\gamma}$. Having at most two incongruent solutions, mod $p^{\alpha-\gamma}$, the last congruence shows via (11) that the solutions of (8) in σ form at most two residue classes, mod $p^{\alpha-\gamma/2}$, wherefore we set $\beta=\alpha-\frac{1}{2}\gamma$ in conformity with the pre-assigned condition $\beta\geqq\frac{1}{2}\alpha$. On the other hand, if $\gamma\geqq\alpha$, then (10) is equivalent to $W^2\equiv 0, \bmod p^\alpha$, whose solutions are given by

$$W\equiv 0, \bmod p^{\alpha'}, \tag{13}$$

where α' is the least integer that is not less than $\frac{1}{2}\alpha$. Since the corresponding solutions of (8) then belong to a single residue class, mod $p^{\alpha'}$, we therefore in this case set $\beta=\alpha'$. Finally, in both the above cases, (12), (13), (11), and (8) shew that the chosen values of σ endow the form $\Gamma(\Xi, \mathrm{H})$ with coefficients that are divisible by p^α.

Little change in the above argument is needed when $p=2$. If C be even and equal to $2C^*$, say, we can use (8) and the procedure that followed it without introducing the factor 4, the conclusions being similar save that four incongruent solutions for σ, mod p^β, may occur. If, however, C be odd, we take $\beta=\alpha$ and deduce from (7) that $\phi(\sigma)\equiv 0$, mod p^α, which congruence has at most two incongruent solutions, mod p^β, because Δ is also odd; in this situation, the coefficients of $\Gamma(\Xi, \mathrm{H})$ are obviously still divisible by p^α.

In summation, considering the incongruent values of σ, mod M, we see that the solutions of (2) and (4) correspond to representations of unity by a set of not more than

https://doi.org/10.1017/S0017089500006108 Published online by Cambridge University Press

$2^{\omega(N)+1}$ integral irreducible forms $N^{-1}\Gamma(\Xi, \mathrm{H})$ that appertain to the admissible transformations of type (5). Since Delone and Siegel [**1**] have shewn for negative and positive discriminants, respectively, that the number of ways of expressing unity through an irreducible binary cubic is absolutely bounded, we therefore deduce that

$$\rho_\delta(n) = O(2^{\omega(n/\delta)})$$

because of (1) and (3).

Our result is now immediate from this and the equations

$$\rho(n) = \sum_{\delta \mid n} \rho_\delta(n), \qquad r(n) = \sum_{\delta_1^3 \mid n} \rho(n/\delta_1^3),$$

which give

$$\begin{aligned} r(n) &= O\left\{\sum_{\delta_1^3 \mid n} \sum_{\delta \mid n/\delta_1^3} 2^{\omega(n/\delta\delta_1^3)}\right\} = 0\left\{\sum_{\delta_1^2 \mid n} \sum_{\delta \mid n/\delta_1^2} 2^{\omega(n/\delta\delta_1^2)}\right\} \\ &= O\left\{\sum_{\delta \mid n} \sum_{\delta_1^2 \mid n/\delta} 2^{\omega(n/\delta\delta_1^2)}\right\} \\ &= O\left\{\sum_{\delta \mid n} d(n/\delta)\right\} = O\{d_3(n)\}. \end{aligned}$$

We have therefore proved the following

THEOREM. *Let $r(n)$ be the number of representations of a positive integer n by an irreducible binary cubic form. Then we have*

$$r(n) = O\{d_3(n)\},$$

uniformly with respect to the coefficients of the form.

REFERENCES

1. B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, Vol. 10, American Math. Soc. (1964).

2. C. J. A. Evelyn and E. H. Linfoot, On a problem in the additive theory of numbers, *J. reine angew. Math.* **164** (1931), 131–140.

3. G. Greaves, On the representation of a number of a sum of two fourth powers, *Math. Z.* **94** (1966), 233–234.

4. C. Hooley, On binary quartic forms (*to appear*).

5. J. L. Lagrange, Nouvelle méthode pour résoudre les problèmes indeterminées en nombres entires, *Mémoires de Berlin*, **24** (1770).

DEPARTMENT OF PURE MATHEMATICS,
UNIVERSITY COLLEGE,
CARDIFF.

https://doi.org/10.1017/S0017089500000610 Published online by Cambridge University Press