and

$$T(n) = \sum_{r\geq 1}' N_r.$$

Applying the Cauchy-Schwarz inequality we get

$$\Big(\sum_{r\geq 1}' rN_r\Big)^2 \leqslant \sum_{r\geq 1}' r^2 N_r \cdot \sum_{r\geq 1}' N_r,$$

so

$$\sum_{r\geq 1}' r^2 N_r \geqslant \frac{\big(S(n)\big)^2}{T(n)}.$$

Since

$$Q(n) \geqslant \sum_r' r(r-1) N_r = \sum_r' r^2 N_r - \sum_r' rN_r,$$

inequality (2) follows and the theorem is proved.

We remark that our argument may also be applied to some "dual" problems dealt with in the last section of the paper by Bredihin and Linnik [2].

References

[1] Б. М. Бредихин, Ю. В. Линник, *Некоторые диофантовые уравнения с простыми числами*, Математические Заметки 12 (3) (1972).

[2] B. M. Bredihin and Yu. V. Linnik, *Remarks on some new applications of the dispersion method*, Acta Arith., this volume, pp. 409-410.

OKAYAMA UNIVERSITY
Okayama, Japan

Received on 7. 11. 1971 (233)

ACTA ARITHMETICA
XXI (1972)

Additive problems involving squares, cubes and almost primes

by

Yu. V. Linnik

We consider here certain additive problems of the binary type in the sense of [3] § 1, namely the representation of large numbers by the sums of two squares and two cubes, two squares and three cubes, one square and a ternary cubic form and a product of two primes and a ternary cubic form. Only in the case of two squares and three cubes we succed in solving the corresponding equation for all large numbers; in other cases we solve the equations for certain large classes of numbers. No asymptotic is obtained, only certain crude lower estimates are obtained. However in same cases the possibility of obtaining asymptotic formulae with help of the dispersion method [3] is indicated.

§ 1. Consider the diophantine equations:

$$n = \xi^2+\eta^2+x^3+y^3, \tag{1.1}$$

$$n = \xi^2+\eta^2+x^3+y^3+z^3 \tag{1.2}$$

with non-negative ξ, η, x, y, z.

There are many reasons to believe that the equation (1.1) is solvable for all large numbers n, but we cannot prove it. We shall consider here only even numbers $n = 2N_1$. We can represent any even number n, in the form $n = 2^{3\mu}3^{6\nu}2^{\alpha}3^{\beta}n_1$ where $1 \leqslant \alpha \leqslant 3$; $0 \leqslant \beta \leqslant 5$; $\mu \geqslant 0$, $\nu \geqslant 0$, $(n_1, 6) = 1$. We shall call the corresponding number $2^{\alpha}3^{\beta}n_1$ the kernel of even number n. Clearly if $2^{\alpha}3^{\beta}n_1$ is representable in the form (1.1) so is n. Therefore we shall consider only the kernels of the even numbers n.

In what follows, $c_0, c_1, c_2, \ldots, K_0, K_1, K_2, \ldots$ will be positive constants, $\varepsilon_0, \varepsilon_1, \ldots$ small positive constants.

THEOREM 1. *Let $\Gamma(K_0, K_1, K_2)$ be the set of all even numbers n subject to conditions*: 1) *the kernels* $2^{\alpha}3^{\beta}n_1 \geqslant K_0$; 2) *the number* n_1 *has* *a divisor $\delta = u^2+v^2$ which is the sum of two squares and satisfies the inequalities*

$$(1.3)\qquad \frac{\sqrt[3]{n_1}}{K_2} \leqslant \delta \leqslant \frac{\sqrt[3]{n_1}}{K_1}.$$

Then, K_1 and $K_2 > K_1$ being given and sufficiently large, $K_0 = K_0(K_1, K_2)$ being sufficiently large, the number $n \epsilon \Gamma(K_0, K_1, K_2)$ can be represented in the form (1.1) *with the representation number tending to infinity as $n_1 \to \infty$. Moreover, in the representation* (1.1) $\operatorname{arctg}\frac{\eta}{\xi}$ *can be chosen within ε_0 ($\varepsilon_0 > 0$) from any given angle $\varphi \epsilon \left(0, \frac{\pi}{2}\right)$.*

THEOREM 2. *All large numbers n can be represented in the form* (1.2) *with the representation number exceeding $c_\varepsilon n^{2/3-\varepsilon}$. Moreover,* $\operatorname{arctg}\frac{\eta}{\xi}$ *can be chosen within ε_0 from a given angle $\varphi \epsilon \left(0, \frac{\pi}{2}\right)$ with the same estimate of the representation number.*

Theorem 2 is an easy consequence of Theorem 1. The method of the proof of Theorem 1 is essentially the same as that of the theorem on the representation of numbers by six cubes (see [2], pp. 58–70). We pass now to the proof of Theorem 1. Putting $H_1 = x+y$, replacing the number $n \epsilon \Gamma(K_0, K_1, K_2)$ by its kernel $2N_1 = 2^\alpha 3^\beta n_1$, we get the equation:

$$2N_1 = H_1^3/4 + 3H_1(x - H_1/2)^2 + \xi^2 + \eta^2.$$

If K_0 is sufficiently large and

$$(1.4)\qquad H_1 \epsilon [(2N_1)^{1/3}(1-\tfrac{1}{10})^{1/3}, (2N_1)^{1/3}(1+\tfrac{1}{10})^{1/3}]$$

the numbers x and y in (1.1) are non-negative (see [2], pp. 59–60). Define now H_1' as follows: H_1' is the largest uneven divisor of $\delta = u^2+v^2$. As $2N_1 \not\equiv 0 \pmod{16}$, we have: $\delta/8 \leqslant H_1' \leqslant \delta$, and H_1' is the sum of two squares. In subsequent reasonings there will be however a case when we shall be obliged to multiply H_1' thus defined by an uneven bounded factor which is also a sum of two squares and use the number thus obtained as H_1'. We put now: $2N_1 = 2H_1'N_2$. The number H_1' is uneven, and the number $2H_1' = u_1^2+v_1^2$ is the sum of two squares. For sufficiently large K_1, K_2 and $K_0 = K_0(K_1, K_2)$, we can find as many primes $P \geqslant 3$ as we wish in any prescribed (admisssible) arithmetic progression such that $H_1 = 2H_1'P$ and H_1 satisfies (1.4). Hence, (1.1) is reduced to solving the equation

$$(1.5)\qquad 2H_1'N_2 = 2H_1'^3P^3 + 3\cdot 2H_1'Px_1^2 + \xi^2 + \eta^2$$

in integer x_1, ξ, η (we put $x - H_1/2 = x_1 > 0$; H_1 is even and so x_1 is integer). Now, $2H_1' = u_1^2+v_1^2$, we can put: $\xi^2+\eta^2 = (u_1^2+v_1^2)(\xi_1^2+\eta_1^2) = 2H_1'(\xi_1^2+\eta_1^2)$ and reduce (1.7) to the equation:

$$(1.6)\qquad N_2 - H_1'^2P^3 = 3Px_1^2 + \xi_1^2 + \eta_1^2,$$

where $N_2 - H_1'^2P^3 \geqslant \frac{1}{6}N_2$ as easily seen, i.e. to the representation of a positive number by a positive ternary quadratic form. The asymptotic theory of such representation was worked out by the author and A. V. Malyshev. The complete account of this theory is given in A. V. Malyshev's work [5]; for the ergodic background of the theory see [4]. We need the following theorem of A. V. Malyshev ([5], p. 175):

THEOREM (A. V. Malyshev). *Let $f = f(x_1, x_2, x_3)$ be a positive primitive ternary quadratic form with uneven relatively prime invariants $[\Omega, \Delta]$. Let q be a prime not dividing 2Δ, let g be a positive integer such that $(g, 2\Omega\Delta) = 1$, b_1, b_2, b_3 integers such that $(g, b_1, b_2, b_3) = 1$. Consider a positive integer m such that $(m, q) = 1$ for which the congruence:*

$$(1.7)\qquad f(x_1, x_2, x_3) \equiv m \pmod{8\Omega^2\Delta m}$$

is primitively solvable and the conditions $f(b_1, b_2, b_3) \equiv m \pmod{g}$, and

$$\left(\frac{-\Delta m}{q}\right) = +1$$

are fulfilled. Let $\Lambda_{f,m}$ be a domain on the ellipsoid $f(x_1, x_2, x_3) = m$ consisting of a bounded number of convex domains and subtending an f-elliptic solid angle $\lambda \geqslant \lambda_0 > 0$ from the centre of the ellipsoid. Denote by $r_{g;b_1,b_2,b_3}(\Lambda_{f,m})$ the number of primitive representations (x_1, x_2, x_3) of the number m by the form f, for which the conditions

$$(x_1, x_2, x_3) \epsilon \Lambda_{f,m}; \quad (x_1, x_2, x_3) \equiv (b_1, b_2, b_3) \pmod{g}$$

are fulfilled. Then there exist positive constants m_0, $\varkappa > 0$, $\varkappa' > 0$ depending only upon $\Omega, \Delta, q, g, \lambda$ and the shape of the domain $\Lambda_{f,m}$ such that for $m \geqslant m_0$

$$\varkappa h(-\Delta m) < r_{g;b_1,b_2,b_3}(\Lambda_{f,m}) < \varkappa' h(-\Delta m)$$

where $h(-\Delta m)$ is the class number of properly primitive positive binary quadratic forms of determinant Δm.

Hence we must verify the conditions of this theorem in the case (1.6) for suitably chosen H_1' and P, N_2 being equal to $\frac{2N_1}{2H_1'}$. The ternary quadratic form on the right hand side of (1.6) has the invariants: $\Omega = 1$; $\Delta = 3P$; hence the congruence (1.7) has the form:

$$3Px_1^2+x_2^2+x_3^2 \equiv m \pmod{24Pm} \tag{1.8}$$

where $m = N_2 - H_1'^2P^3$. Here the relevant moduli are 8, 3 and P as it is seen from elementary considerations. Let us fix now P as a prime number $P \equiv 1 \pmod 4$, so that $P = a^2+b^2$; $(a, b) = 1$. Then the congruence $3Px_1^2+x_2^2+x_3^2 \equiv n \pmod P$ is primitively solvable for $n \not\equiv 0 \pmod P$. For $n \equiv 0$ a primitive solution will be $(0, a, b)$. Hence for such moduli there are always primitive solutions. Now as regards the modulus 3, we have chosen the number H_1' so that $H_1' \not\equiv 0 \pmod 3$. Now $P^3 \equiv P \pmod 3$ and hence $N_2 - H_1'^2P^3 \equiv N_2 - P \pmod 3$. If $N_2 \equiv 0 \pmod 3$ then $N_2 - P \equiv 1$ or $2 \pmod 3$, and the congruence $3Px_1^2+x_2^2+x_3^2 \equiv N_2 - H_1'^2P \pmod 3$ will have the primitive solutions $(0, 1, 0)$ or $(0, 1, 1)$ respectively. If $N_2 \not\equiv 0 \pmod 3$, we can chose the prime number P in the progression with the difference 12 so that $N_2 - H_1'^2P \equiv 1 \pmod 3$ and the congruence is again primitively solvable.

Consider now the modulus 8; we shall prove that the prime P always can be chosen (mod 24) so that the congruence

$$3Px_1^2+x_2^2+x_3^2 \equiv N_2 - H_1'^2P^3 \pmod 8$$

is primitively solvable. As H_1' and P are uneven, we can replace our congruence by:

$$3Px_1^2+x_2^2+x_3^2 \equiv N_2 - P \pmod 8. \tag{1.9}$$

We shall consider all possible cases of the residuacity of $N_2 \pmod 8$:

1° $N_2 \equiv 1 \pmod 8$. Take $P \equiv 5 \pmod 8$; $N_2 - P \equiv 4 \pmod 8$ and $4 \equiv 15\cdot 1^2+1^2+2^2 \pmod 8$.

2° $N_2 \equiv 3 \pmod 8$. Take $P \equiv 1 \pmod 8$; $N_2 - P \equiv 2 \equiv 1^2+1^2 \pmod 8$.

3° $N_2 \equiv -3 \pmod 8$. Take $P \equiv 1 \pmod 8$; $N_2 - P \equiv 4 \equiv 3\cdot 1^2+1^2 \pmod 8$.

4° $N_2 \equiv -1 \pmod 8$. Take $P \equiv 5 \pmod 8$; $N_2 - P \equiv 2 \equiv 1^2+1^2 \pmod 8$.

5° $N_2 \equiv 2 \pmod 8$. Take $P \equiv 1 \pmod 8$; $N_2 - P \equiv 1 \equiv 1^2 \pmod 8$.

6° $N_2 \equiv 4 \pmod 8$. Take $P \equiv 1 \pmod 8$; $N_2 - P \equiv 3 \equiv 3\cdot 1^2 \pmod 8$.

Now, $8 \nmid N_2$ in view of the properties of the kernel $2^\alpha 3^\beta n_1$, so we have enumerated all possible cases. We must now find a prime $q \nmid 24P$ satisfying the condition

$$\left(\frac{-3P(N_2+H_1'^2\cdot P^3)}{q}\right) = +1. \tag{1.10}$$

Let $K_3 = K_3(K_1, K_2)$ be a large constant; consider a given sequence of some primes: $q_i \equiv 1 \pmod 4$; $q_i \leqslant K_3$, $q_1 < q_2 < \ldots < q_r \leqslant K_3$. Consider the initial number $2N_1 = 2H_1'N_2$. Let $2N_1 = q_1^{\gamma_1}q_2^{\gamma_2}\ldots q_r^{\gamma_r}M$ where $(M, q_1\ldots q_r) = 1$, $\gamma_i \geqslant 0$ $(i = 1, 2, \ldots, r)$. We can write: $2N_1 = (q_1^{\delta_1}\ldots q_r^{\delta_r})^6 \times \times q_1^{\nu_1}\ldots q_r^{\nu_r}M$; $0 \leqslant \nu_i \leqslant 5$. Clearly, if the equation (1.1) is solvable for the number $q_1^{\nu_1}\ldots q_r^{\nu_r}M = 2N'$ it is solvable for the number $2N_1$, and if K_3 is sufficiently large, so is $2N'$, and $2N' \in \Gamma(K_0, K_1, K_2)$ for sufficiently large values of $2N_1$. Hence we can replace $2N$ by $2N'$ in our reasonings. If all the numbers ν_i are $\geqslant 1$, we can include $q_{i_0}^{\nu_{i_0}}$ into the factor $2H_1'$ of the number $2N'$, and so in (1.10) q_{i_0} will not divide N_2. We take then $q = q_{i_0}$. If a number $\nu_i = 0$, $q_i \nmid N_2$ and we take $q = q_i$. So we can suppose $q \nmid N_2$ in the relation (1.10). Now, by a well known estimate of André Weil

$$\left|\sum_{\xi=0}^{q-1}\left(\frac{-3\xi(N_2+H_1'^2\xi^3)}{q}\right)\right| \leqslant c_0\sqrt{q}$$

if $N_2 \not\equiv 0 \pmod q$. Hence, for sufficiently large q, we can choose $P \pmod{24q}$ so as to satisfy the condition (1.10).

Hence, all the conditions of A. V. Malyshev's theorem are satisfied and (1.6) is primitively solvable. The number of solutions will be $\geqslant C_\varepsilon N^{\frac{1}{2}-\varepsilon}$ and so will tend to infinity as $n = 2N_1 \to \infty$. Moreover, in virtue of the same theorem $\operatorname{arctg}\frac{\eta_1}{\xi_1}$ can be made equal to any angle $\varphi \in \left(0, \frac{\pi}{2}\right)$ up to $\varepsilon_0 > 0$ and so also $\operatorname{arctg}\frac{\eta}{\xi}$. Theorem 1 is thus proved.

We pass now to the proof of Theorem 2. Let n be a large number; we consider the numbers $n - z^3$; $\frac{1}{4}n^{1/3} \leqslant z \leqslant \frac{1}{2}n^{1/3}$ and try to choose such numbers z as to make $n - z^3$ belong to $\Gamma(K_0, K_1, K_2)$ for some suitably chosen $K_1, K_2, K_0 = K_0(K_1, K_2)$. For sufficiently large K_1 and $K_2 > K_1$, we consider prime numbers $\delta \equiv 5 \pmod{12}$ subject to condition (1.3). The number of them is larger than $C_1\frac{n^{1/3}}{\ln n}$. As $\delta - 1 \not\equiv 0 \pmod 3$, z^3 will run over all the residues of δ, and so it can be chosen such that $n - z^3 \equiv 0 \pmod\delta$; moreover, δ is the sum of two squares. Now $z^3 \equiv z \pmod 3$ and so z can be chosen so that $n - z^3 \equiv 0 \pmod 3$ but $n - z^3 \not\equiv 0 \pmod 9$. Hence in choosing the prime numbers P (as in the proof of Theorem 1), we need not take the progressions mod 24, but only mod 8. Now if n is uneven, we take z to be uneven so that $z^3 \equiv z \pmod 8$ and so we can make $n - z^3 \equiv 2 \pmod 8$. If n is even, we take $z \equiv 2 \pmod{16}$, so $z^3 \equiv 8 \pmod{16}$, then $n - z^3$ is even but $n - z^3 \not\equiv 0 \pmod{16}$, so the kernel of n is $2N_1 \geqslant \frac{n}{24}$. The choice of the prime number $P \equiv 1 \pmod 4$ can be made so that $n-z^3 \not\equiv 0 \pmod{P}$, and the number q in the relation (1.10) can be chosen so that $n-z^3 \not\equiv 0 \pmod{q}$ and the relation (1.10) is satisfied. Different values of δ correspond to different values of $x+y$ and so to different representations. By the theorem of A. V. Malyshev, even if we fix $\operatorname{arctg}\frac{\eta_1}{\xi_1}$ up to a given $\varepsilon_0 > 0$, the representation number for given P, H_1' of the number $N_2 - H_1'^2 P^3 > \frac{1}{6}N_2 > c_1 n^{2/3}$, will be $\geqslant c_6 n^{\frac{1}{3}-\varepsilon}$. Hence the total representation number will be $\geqslant c_8 n^{\frac{2}{3}-\varepsilon}$ and Theorem 2 is proved.

The method applied to the equations (1.1) and (1.2) is applicable also to the more general equations: $n = Q_2(\xi,\eta)+Q_3(x,y)$, where $Q_2(\xi,\eta)$ is a positive (in general non-primitive) binary quadratic form and $Q_3(x,y)$ a cubic form with a rational root and the corresponding equation $n = Q_2(\xi,\eta)+Q_3(x,y)+Az^3$ $(A \geqslant 0)$. But if $Q_3(x,y)$ has only irrational roots as, say, in the case of the equations $n = Q_2(\xi,\eta)+x^3+5y^3$, the method does not work.

There is a well known hypothesis relating to the form $x^3+y^3+z^3$: if $\psi_3(m)$ is the solution number of the equation: $n = x^3+y^3+z^3$; $x \geqslant 0$, $y \geqslant 0$, $z \geqslant 0$, then

$$\sum_{m=1}^{n} (\psi_3(m))^2 = O(n^{1+\varepsilon}) \tag{1.11}$$

This hypothesis, though highly probable one is not yet proved or disproved. However, on this hypothesis the application of the dispersion method [3] to the equation (1.2) would be possible; namely considering the equation:

$$n = \xi^2+\eta^2+\varrho^3(x^3+y^3+z^3) \tag{1.12}$$

in non-negative integer variables, we make ϱ^3 and $x^3+y^3+z^3$ run independently over the corresponding segments $[0, n^{\varepsilon_1}]$ and $[0, n^{1-\varepsilon_1}]$, $\varepsilon_1 > 0$ being a small constant. Then we apply the dispersion method taking $\varphi = \xi^2+\eta^2$; $\nu = \varrho^3$; $D' = x^3+y^3+z^3$ and consider the equation $n = \varphi + D'\nu$ (see [3]). An asymptotic formula for (1.12) on the hypothesis (1.11) can thus be obtained. The form $\xi^2+\eta^2$ in (1.12) can be replaced by any positive binary quadratic form.

§ 2. There are ternary cubic forms for which the analogon of the hypothesis (1.11) can be proved. Consider for instance the ternary cubic form:

$$V_3(x,y,z) = x^3+y^3+z^3+(x+y-z)^3 \tag{2.1}$$

under conditions:

$$x \geqslant 0, \quad y \geqslant 0, \quad z \geqslant 0, \quad x+y-z \geqslant 0. \tag{2.2}$$

$V_3(x,y,z)$ is a ternary cubic form which is the sum of four positive cubes. Now, to prove the analogon of the hypothesis (1.11) it is sufficient to prove that the equation

$$V_3(x,y,z) - V_3(x',y',z') = 0 \tag{2.3}$$

under conditions that all its variables run independently over the interval $[0, N]$ has no more than $O(N^{3+\varepsilon})$ solutions. In fact, putting $x+y = H_1$; $x'+y' = H_2$ and fixing H_1, H_2 we obtain the equation of the type:

$$12H_1(u_1^2+v_1^2) - 12H_2(u_2^2+v_2^2) = H_2^3 - H_1^3 \tag{2.4}$$

u_i, v_i being of order $O(N)$ and $H_i = O(N)$; $H_i \geqslant 0$. Now $u_i^2+v_i^2$ run over $O(N^2)$ values with no more than $O(N^\varepsilon)$ repetitions. Thus we can replace (2.4) by the equation:

$$H_1X_1 + H_1^3 = H_2X_2 + H_2^3,$$

where $X_i = O(N^2)$ with $O(N^\varepsilon)$ possible repetitions, $X_i \geqslant 0$, $H_i \geqslant 0$. Fixing now H_2 and X_2 we obtain $O(N^\varepsilon)$ such solutions for the equation (2.4) and $O(N^{3+\varepsilon})$ for the number of all solutions of (2.3). Hence we can apply the dispersion method [3] for finding the asymptotic formula for the number of solutions of the equation:

$$n = Q_2(\xi,\eta) + V_3(\varrho x, \varrho y, \varrho z), \tag{2.5}$$

where $Q_2(\xi,\eta)$ is a positive binary quadratic form and $0 \leqslant \varrho \leqslant n^{\varepsilon_1}$; $0 \leqslant x, y, z \leqslant n^{\frac{1-\varepsilon_1}{3}}$, $\varepsilon_1 > 0$ being a small constant, ϱ independent upon x, y, z and $x+y-z \geqslant 0$. But if $Q_2(\xi,\eta)$ is replaced by a single square, the dispersion method fails to work. Consider the equation:

$$n = \xi^2 + V_3(x,y,z) \tag{2.6}$$

under conditions (2.2). We shall study this equation with the method of § 1 for certain sets of large numbers n. We consider again the numbers $n \equiv 0 \pmod 4$, represented in the form: $n = 2^{6\mu}3^{6\nu}2^\alpha 3^\beta n_1$ where $2 \leqslant \alpha \leqslant 5$, $0 \leqslant \beta \leqslant 5$, $(n_1, 6) = 1$ and call $2N_1 = 2^\alpha 3^\beta n_1$ the kernel of the number n. It is sufficient to solve the equation (2.6) for kernel numbers. Let K_1, $K_2 > K_1$ be given large constants and $\Gamma'(K_0, K_1, K_2)$ be the set of all numbers $n \equiv 0 \pmod 4$ such that 1) the kernels $2^\alpha 3^\beta n_1 \geqslant K_0 = K_0(K_1, K_2)$; 2) the number n_1 has an even square divisor δ^2 satisfying

$$\frac{\sqrt[3]{n_1}}{K_2} \leqslant \delta^2 \leqslant \frac{\sqrt[3]{n_1}}{K_1};$$

3) there is a prime q_0, $3 \leqslant q_0 < K_3(K_1, K_2)$ such that $q_0 \,\Big|\, \dfrac{n_1}{\delta^2}$, $(\delta, q_0) = 1$;

4) in each of the two progressions $24m+1$ and $24m-7$ there exist primes P such that

$$P \nmid n_1; \qquad \left(\frac{-2P}{q_0}\right) = +1$$

and

$$P \in \left[\frac{(2N_1)^{1/3}}{\delta^2}\left(1-\frac{1}{10}\right)^{1/3}, \frac{(2N_1)^{1/3}}{\delta^2}\left(1+\frac{1}{10}\right)^{1/3}\right].$$

THEOREM 3. *For all numbers $n \in \Gamma'(K_0, K_1, K_2)$ the equation* (2.6) *is solvable with the number of solutions $\geqslant c_\varepsilon n^{\frac{1}{2}-\varepsilon}$.*

Putting $x+y = H_1 \geqslant 0$, we get the equation:

$$n = \xi^2 + \frac{1}{2}H_1^3 + 3H_1\left[\left(x-\frac{H_1}{2}\right)^2 + \left(z-\frac{H_1}{2}\right)^2\right], \tag{2.7}$$

where we must have $y \geqslant 0$, $x+y-z = H_1'-z \geqslant 0$. We choose H_1 subject to conditions (1.4) to meet these requirements. Put $x-\dfrac{H_1}{2} = x_1$, $z-\dfrac{H_1}{2} = y_1$, $2N_1 = 2H_1'N_2$, $H_1 = 2H_1'P$. Here we choose $2H_1' = \delta^2$. P being a prime, we get:

$$2N_1 = 2H_1'N_2 = 4H_1'^3P^3 + 3\cdot 2H_1'P(x_1^2+y_1^2) + \xi^2.$$

Now $2H_1' = \delta^2$; putting $\xi = \delta_1\xi_1$ and dividing by $2H_1'$, we get the equation:

$$N_2 - 2H_1'^2P^3 = \xi_1^2 + 3P(x_1^2+y_1^2), \tag{2.8}$$

where $N_2 - 2H_1'^2P^3 \geqslant \dfrac{N_2}{20}$ as easily seen from the conditions (1.4). We can now apply the theorem of A. V. Malyshev (see § 1) to the equation (2.8). Here the corresponding ternary form has the invariants $\Omega = 3P$, $\Delta = 1$. We must consider the moduli 8, 3, P and a prime modulus $q_0 > 3$ such that:

$$\left(\frac{-(N_2-2H_1'^2P^3)}{q_0}\right) = +1. \tag{2.9}$$

Consider the modulus 8. As $2H_1' = \delta^2$ is a square, we have $N_2-2H_1'^2P^3 \equiv 0 \pmod 8$. Taking $P \equiv 1 \pmod 8$ we have the primitive solution of the congruence: $1^2+3(1^2+2^2) \equiv 0 \pmod 8$. Take the modulus 3. If $2N_1' \equiv 0 \pmod 3$ we choose H_1' prime to 3, hence $N_2-2H_1'^2P^3 \equiv N_2-2P \pmod 3$. If $P \equiv 1 \pmod 3$, $N_2-2P \equiv 1 \pmod 3$. If $2N_1' \not\equiv 0 \pmod 3$, so is $2H_1'$ and we can choose $P \equiv 1 \pmod 3$ or $P \equiv 2 \pmod 3$ to make $N_2-2P \equiv 1 \pmod 3$. Hence we can choose the prime number P in one of the progressions $24m+1$ and $24m-7$ in a suitable way.

Now $q_0 | N_2$, $q_0 \nmid H_1'$ and the symbol at the left hand side of (2.9) is equal to $\left(\dfrac{-2P}{q_0}\right) = +1$ by the conditions of the theorem. This proves the primitive solvability of (2.8) and Theorem 3. The representation number will be $\geqslant c_\varepsilon N_2^{\frac{1}{2}-\varepsilon} > c_\varepsilon' n_1^{\frac{1}{2}-\varepsilon}$.

§ 3. We consider now the equation:

$$n = p_1p_2 + V_3(x, y, z) \tag{3.1}$$

with p_1, p_2 primes, $x \geqslant 0$, $y \geqslant 0$, $z \geqslant 0$, $x+y-z \geqslant 0$. We consider two given constants K_1 and $K_2 > K_1$, and the set $\Gamma''(K_0, K_1, K_2)$ of all numbers n such that 1) $n \geqslant K_0(K_1, K_2)$, 2) n has a prime factor $p \in \left[\dfrac{n^{1/3}}{K_2}, \dfrac{n^{1/3}}{K_1}\right]$. We have the theorem:

THEOREM 4. *Any number $n \in \Gamma''(K_0, K_1, K_2)$ can be represented in the form* (3.1). *The number of representations is $\geqslant c_\varepsilon n^{\frac{2}{3}-\varepsilon}$.*

For proof we write (3.1) in the form:

$$n = p_1p_2 + \tfrac{1}{2}H_1^3 + 3H_1[(x-\tfrac{1}{2}H_1)^2 + (z-\tfrac{1}{2}H_1)^2] \tag{3.2}$$

with $H_1 = x+y$ subject to usual conditions (1.4). Take now $H_1 = 2pP$, where p is the divisor of n of the condition 2), and $P > 3$ a prime number in the interval required by the relations (1.4). Put $p_2 = p$, $x-\dfrac{H_1}{2} = x_1$, $z-\dfrac{H_1}{2} = y_1$ in (3.2); hence we get:

$$\frac{n}{p} - 4p^2P^3 = p_1 + 6P(x_1^2+y_1^2). \tag{3.3}$$

Moreover the left hand side is $\geqslant \dfrac{1}{20}\dfrac{n}{p}$. By the theorems on the generalized Hardy–Littlewood problem, proved by B. M. Bredihin [1], the equation (3.3) is solvable with the number of the solutions $\geqslant c_\varepsilon\left(\dfrac{n}{p}\right)^{1-\varepsilon}$, which proves our theorem.

References

[1] B. M. Bredihin, *Dispersion method and definite binary problems* (Russian), Uspehi Mat. Nauk 20 (2) (1965), pp. 89–130.
[2] Yu. V. Linnik, A. V. Malyshev, *Applications of the arithmetic of quaternions to the theory of ternary quadratic forms and to the decomposition of numbers into cubes* (Russian), Uspehi Mat. Nauk 8 (5) (1953), pp. 3–71.
[3] — *Dispersion method in binary additive problems* (Russian), Leningrad 1961 (American translation, 1963).
[4] — *Ergodic properties of algebraic fields* (Russian), Leningrad 1967 (J. Springer's translation, 1968).
[5] A. V. Malyshev, *On the representation of integers by positive quadratic forms* (Russian), Trudy Mat. Inst. Steklov., 65 (1962).

Received on 20. 9. 1971 (218)

ACTA ARITHMETICA
XXI (1972)

On the analytic theory of quadratic forms

by

K. G. Ramanathan (Bombay)

Dedicated to the memory of W. Sierpiński

1. The analytic theory of quadratic forms, as developed by Siegel [6], leads to a fundamental formula, now called the 'Siegel formula', which is an identity for $m > 4$ between the theta series associated with the genus of a quadratic form in $m > 4$ variables and the Eisenstein-Siegel series associated with it. In a beautiful reworking of the theory, Weil [10] has obtained, among others, a proof of the Siegel formula for $m > 4$ by an analytic method which lends itself to important generalizations (see the recent paper of J. Igusa, Inventiones Math. 1971).

In this note we present a proof of this formula for $m \geqslant 3$ by using an idea due to Hecke [2]. In the case $m = 2$ a similar formula is proved by Hecke [2] for definite forms and by Maass [4] for indefinite forms. However the summation in these cases is over all classes of forms with a given determinant. The result for summation over classes in a given genus is, in general, false. In case $m = 1$, this formula is proved by Siegel [8] and Maass [3]. In [5] Raghavan and Rangachari have extended Weil's methods to the case of quadratic forms in 4 variables with index $\leqslant 1$.

An interesting consequence of the analysis is that one proves, analytically, that the Minkowski–Siegel constant (for semi-simple algebraic groups this is called the Tamagawa number) is two. However one has to prove it first in the case $m = 2$. This is well-known by the classical results of Dirichlet–Minkowski–Siegel.

Generalizations of this formula can be obtained for quadratic or hermitian forms over arbitrary algebraic number fields and over quaternion algebras. The generalization where one deals with representation of matrices by matrices seems difficult and is related to the analytic continuation of Eisenstein series in the Siegel half space.

2. Let S be a semi-integral non-singular m rowed symmetric matrix so that $2S$ is an integral matrix with even diagonal elements. Put

$$d = |2S|. \tag{1}$$