MATHEMATICS

1962

SovietRxiv

Abstract

Full Text

MATHEMATICS

A. A. KISELEV and I. Sh. SLAVUTSKII

ON SOME CONGRUENCES FOR THE NUMBER OF REPRESENTATIONS BY SUMS OF AN ODD NUMBER OF SQUARES

(Presented by Academician V. I. Smirnov on 10 XI 1961)

1. In this work a series of congruences is established for the number of representations of a natural number by sums of an odd number of integer squares. The simplest special cases of these results were obtained in (^{1}).

The investigations of Hardy (^{2,3}), Suetuna (^{4}), and Bateman (^{5}) allow one to conclude that the principal term $\rho_s(n)$ containing the singular series in the formula for the number of representations $r_s(n)$ of a natural number n by sums of an odd number s of integer squares ($s = 2\sigma + 1,\ \sigma \geqslant 1$) is equal to

$$\rho_s(n) = (-1)^{[\sigma/2]+1} \frac{2^{2\sigma} n^{\sigma-1} f}{(2^{2\sigma}-1)|B_{2\sigma}|} \frac{2^\sigma - \left(\dfrac{D}{2}\right)}{2^\alpha} \chi_2(n) T_\sigma(n) \sum_{r=1}^{|D|} \left(\frac{D}{r}\right) B_\sigma\left(\frac{r}{|D|}\right). \tag{1}$$

Here, in order to carry out the summation in finite form, one has to use the Cauchy–Dirichlet methods, the expansions of Bernoulli polynomials in Fourier series, and the values of Gauss sums. Here $n = f^2 t = 2^\gamma u$, t is squarefree, $\gamma \geqslant 0$, $(2, u) = 1$; $\left(\dfrac{D}{r}\right)$ is the Kronecker symbol, with $\left(\dfrac{D}{r}\right) = 0$ when $(D, r) = \delta > 1$;

$$D = \begin{cases} \eta t, & \eta(t) \equiv 1 \pmod 4, \\ 4\eta t, & \eta(t) \equiv 2, 3 \pmod 4, \end{cases} \qquad \eta = (-1)^\sigma; \qquad \alpha = \begin{cases} 1, & 2/D, \\ 0, & 2 \nmid D; \end{cases}$$

B_k and $B_k(x)$ are the Bernoulli numbers and polynomials, defined respectively by the symbolic equality $(B+1)^k = B^k$ and by the relation

$$B_k(x) = \sum_{r=0}^{k} C_k^r B_r x^{k-r};$$

respectively;

$$T_\sigma(n) = \prod_{p/f}\left(1 - \left(\frac{\eta t}{p}\right)p^{-\sigma}\right)\prod_{p/n}\left(1 - p^{1-2\sigma}\right)^{-1}\prod_{\substack{p/n \\ 2\nmid a}}\left(1 - p^{(1-2\sigma)\frac{a+1}{2}}\right)\times$$

$$\times\prod_{\substack{p/n \\ 2/a}}\left(1 + \frac{(\eta v/p) - p^{1-\sigma}}{1 - (\eta v/p)p^{-\sigma}}p^{(1-2\sigma)\frac{a}{2}-\sigma}\right);$$

p is an odd prime; $v = np^{-a}$, where $p^a \mid n$, but $p^{a+1} \nmid n$;

$$1 \mp \frac{1}{2^\sigma - 2^{1-\sigma}} \pm \frac{2 - 2^{1-2\sigma}}{2 - 2^{1-\sigma}}2^{(1-2\sigma)\frac{\gamma-1}{2}}, \qquad \gamma \geqslant 1, \quad (2,\gamma) = 1;$$

$$1 \mp \frac{1}{2^\sigma - 2^{1-\sigma}} \pm \frac{2 - 2^{1-2\sigma}}{2 - 2^{1-\sigma}}2^{(1-2\sigma)\frac{\gamma}{2}}, \qquad \eta u \equiv 3 \pmod 4, \quad 2/\gamma;$$

$$1 \mp \frac{1}{2^\sigma - 2^{1-\sigma}} \pm \frac{1 + 2^{-\sigma} - 2^{1-2\sigma}}{1 - 2^{1-2\sigma}}2^{(1-2\sigma)\frac{\gamma+2}{2}}, \qquad \eta u \equiv 5 \pmod 8, \quad 2/\gamma;$$

$$1 \mp \frac{1}{2^\sigma - 2^{1-\sigma}} \mp \frac{1 - 2 - 2^{1-2\sigma}}{1 - 2^{1-2\sigma}}2^{(1-2\sigma)\frac{\gamma+2}{2}}, \qquad \eta u \equiv 1 \pmod 8, \quad 2/\gamma,$$

where the upper signs are taken for $\sigma \equiv 1, 2$, and the lower signs for $\sigma \equiv 3, 0 \pmod 4$.

As for $r_s(n)$, for $s = 3, 5, 7$, as is known, $r_s(n) = \rho_s(n)$ (Gauss' s formula and the Smith-Minkowski formulas), while for $3 \leqslant s \leqslant 23$

$$r_s(n) = \rho_s(n) + \alpha_s(n),$$

where the remainder term $\alpha_s(n)$ is a certain arithmetical sum ([6],[7]).

Finally, when n is free of squares ($f = 1$) and, consequently, all representations are proper, the structure (1) is simplified; in particular,

$$T_\sigma(n) = 1.$$

2. For the Bernoulli numbers B_χ^k introduced by Berger and Leopoldt, belonging to a character χ with conductor $F > 1$*, from Voronoi' s generalized congruence ([8],[9]) one may obtain a congruence of Kummer type

$$\frac{B_\chi^a}{a} \equiv \frac{B_\chi^b}{b} \pmod{p^l},$$

where

$$\sum_{r=1}^{F} \chi(r)\, te^{rt}/(e^{Ft}-1) = \sum_{k=0}^{\infty} B_\chi^k t^k/k!;$$

a, b, l are natural numbers,

$$a \equiv b \pmod{(p-1)p^{l-1}}, \qquad l > \min\langle a, b\rangle, \qquad (p, F) = 1.$$

Then the quantities $\rho_{2a+1}(n)$ and $\rho_{2b+1}(n)$ turn out to be connected, since

$$B_\chi^k = F^{k-1} \sum_{r=1}^{F} \chi(r) B_k\left(\frac{r}{F}\right),$$

if one takes $\chi(r) = \left(\frac{F}{r}\right)$. Let, for definiteness, $\eta u \equiv 3 \pmod 4$; then, for example:

$$\frac{1}{T_3(n)}\rho_7(n) \equiv \frac{1}{3T_5(n)}\rho_{11}(n) \pmod 3, \qquad (3, n) = 1;$$

$$\frac{1}{5T_2(n)}\rho_5(n) \equiv \frac{1}{5T_6(n)}\rho_{13}(n) \pmod 5, \qquad (5, n) = 1;$$

$$\frac{1}{7T_3(n)}\rho_7(n) \equiv \frac{5}{T_9(n)}\rho_{19}(n) \pmod 7, \qquad (7, n) = 1;$$

$$\frac{1}{T_2(n)}\rho_5(n) \equiv -\frac{1}{3T_8(n)}\rho_{17}(n) \pmod 9, \qquad (3, n) = 1.$$

In the case when $3 \leqslant s \leqslant 23$, from similar congruences one can also derive congruences for the quantities $r_s(n)$; in this way 20 independent congruences modulo $3, 5, 7, 9$ are obtained.

3. If one takes into account that for the number of classes $H(df^2)$ of binary quadratic forms (positive for $d < 0$) of the form $ax^2 + bxy + cy^2$, where $(a, b, c) = 1$, the following congruences hold (see $(^{8-11})$):

$$H(df^2)\frac{U_{(f),l}}{p^{l-1}} \equiv -\chi T_{(f),l} \prod_{q/f}\left(1-\left(\frac{d}{q}\right)\frac{1}{q}\right)\frac{B_\chi^m}{m} \pmod{p^l}$$

$$\text{for } d = np > 0, \quad n \geqslant 1, \quad \chi \bmod n;$$

$$H(df^2)\frac{\overline{U}_{(f),l}}{p^{l}} \equiv -\chi \overline{T}_{(f),l} \prod_{q/f}\left(1-\left(\frac{d}{q}\right)\frac{1}{q}\right)\frac{B_\chi^{2m}}{2m} \pmod{p^l}$$

$$\text{for } d > 0, \quad p \nmid df, \quad \chi \bmod d;$$

$$H(df^2)\frac{U_{(f),l}}{p^{l-1}} \equiv -\chi T_{(f),l} \prod_{q/f}\left(1-\left(\frac{d}{q}\right)\frac{1}{q}\right)\frac{B_\chi^{2m}}{2m} \pmod{p^l}$$

$$\text{for } d > 0, \quad p \nmid d, \quad (p, f_0) = 1, \quad f = p^c f_0, \quad c \geqslant 1, \quad \chi \bmod d;$$

$$H(df^2) \equiv -f \prod_{q/f}\left(1-\left(\frac{d}{q}\right)\frac{1}{q}\right)\frac{B_\chi^{m+1}}{m+1} \pmod{p^l}$$

$$\text{for } d = -np < -4, \quad n \geqslant 1, \quad \chi \bmod n;$$

$$\left(1-\left(\frac{d}{p}\right)\right)H(df^2) \equiv f \prod_{q/f}\left(1-\left(\frac{d}{q}\right)\frac{1}{q}\right)\frac{B_\chi^{2m+1}}{2m+1} \pmod{p^l}$$

$$\text{for } d < -4, \quad p \nmid d, \quad \chi \bmod |d| \; **.$$

* For more details on this, see the note to (12).

** The last of the congruences in (8) is given only for $l = 1$, but in the general case it can also be obtained from Voronoi' s generalized congruence (8,9).

where $m = \frac{p-1}{2}p^{l-1}$; $\chi(r)$ coincides with the corresponding Kronecker symbol; $\varkappa = 1$ for $N(E_1) = -1$, $\varkappa = 2$ for $N(E_2) = 1$; $N(E_1)$ is the norm of $T_1 + U_1\sqrt{d}$ in the quadratic field $R(\sqrt{d})$; T_1, U_1 are the least positive solution of the equation $T^2 - U^2 d = \pm 1$ in integers or half-integers; under the same restrictions $T_{(f),l}, U_{(f),l}$ is a solution of $T^2 - U^2 df^2 = \pm 1$;

$$E_{(f),l} = T_{(f),l} + U_{(f),l} f\sqrt{d} = E_{(f),1}^{p^{l-1}}$$

and

$$\bar{E}_{(f),l} = \bar{T}_{(f),l} + \bar{U}_{(f),l} f\sqrt{d} = E_{(f),l}^{\left(p-\left(\frac{d}{p}\right)\right)p^{\,l-1}}; \qquad \frac{B_{\chi}^{k}}{k}$$

is p-integral for $(p, F) = 1$ and $F > 1$.* Then it is easy to obtain congruences that relate the number of classes $H(df^2)$ of binary quadratic forms of determinant df^2 and the principal term $\rho_s(n)$ of the number of representations $r_s(n)$, where df^2 is some divisor of the number n, and s is taken in the form $m,\ m+1,\ 2m,\ 2m+1$. They have the simplest form when n is free of squares, for example,

$$H(19n)\,U_1 \equiv 16T_1\rho_{19}(n) \pmod{19} \qquad \text{for } (19, n) = 1,\ n \equiv 7 \pmod 8;$$

$$H(-3n) \equiv 7\rho_{21}(n) \pmod{27} \qquad \text{for } (3, n) = 1,\ n \equiv 5 \pmod 8.$$

If, however, $s \leq 23$, then relations between $H(df^2)$ and $r_s(n)$ can be established; in this case one obtains 36 congruences modulo primes (and also some of their powers) for $p \leq 23$. We indicate some of them, still assuming that n is free of squares:

$$H(12n)\,U_1 \equiv 2T_1\,\frac{r_3(n)}{3} \pmod 3 \qquad \text{for } n \equiv 1 \pmod 4,\ (3, n) = 1;$$

$$H(20n)\,U_1 \equiv \varkappa T_1\,\frac{r_5(n)}{5} \pmod 5 \qquad \text{for } n \equiv 2, 3 \pmod 4,\ (5, n) = 1;$$

$$H(12n)\,\frac{U_2^2}{3} \equiv 2T_2^{[[unclear:exponent]]}\,\frac{r_7(n)}{7} \pmod 9 \qquad \text{for } n \equiv 1 \pmod 4,\ (3, n) = 1.$$

In conclusion we note that the relations obtained are certain analogues of Gauss' s classical results on the representation of numbers by three squares; moreover, the latter are contained in (1), if one takes $s = 3$.

Received10 X 1961

CITED LITERATURE

1. A. A. Kiselev, *Uch. zap. LGU, ser. matem. nauk*, vol. 16, 20 (1949).
2. G. H. Hardy, *Proc. Nat. Acad. Sci. USA*, 4, 189 (1918).
3. G. H. Hardy, *Trans. Am. Math. Soc.*, 21, 255 (1920).
4. Z. Suetuna, *J. Fac. Sci. Imp. Univ. Tokio*, sect. I, 1, part 9 (1927).
5. P. T. Bateman, *Trans. Am. Math. Soc.*, 71, 70 (1951).
6. G. A. Lomadze, *Tr. Tbilissk. matem. inst.*, 16, 231 (1948).
7. G. A. Lomadze, ibid., 17, 281 (1949).
8. A. A. Kiselev, I. Sh. Slavutskii, *DAN*, 126, No. 6, 1191 (1959).
9. I. Sh. Slavutskii, *Uch. zap. Leningradsk. ped. inst. im. A. I. Gertsena*, 218, 179 (1961).
10. I. Sh. Slavutskii, *Izv. Vyssh. uchebn. zaved., Matematika*, No. 4, 173 (1960).
11. L. Carlitz, *Comm. Math. Helv.*, 27, No. 4, 338 (1953).
12. G. V. Leopold, *RZhMat.*, abstract No. 9758 (1959).

* This follows easily, for example, from the generalized Voronoi congruence.

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.