Proceedings of the Edinburgh Mathematical Society (1982) **25**, 101–103 ©

THE NUMBER OF CAYLEY INTEGERS OF GIVEN NORM

by P. J. C. LAMONT

(Received 22nd September 1980)

Using results obtained by J. W. L. Glaisher [**1**, **2**] for the number of representations $R_{r,s}(n)$ of n as a sum of r odd and s even squares, formulae are derived for the number of Cayley integers of given norm n in certain orders $\mathcal{O}$. When computer generating order elements of given norm, the formulae can be used to verify that all the required elements have been obtained.

Let $\mathscr{C}$ be the classical Cayley algebra defined over the rationals with basis $\{i_s\}_0^7$ where $\{i_s\}_0^4$ is a basis of a quaternion algebra $\mathscr{H}_4$, $i_0=1$, $i_1i_2i_3=-1$, $i_1i_4=i_5$, $i_2i_4=i_6$, and $i_3i_4=i_7$. For $\xi=\sum_{s=0}^{7} x_s i_s$, $\bar{\xi}=2x_0-\xi$ is called the conjugate of ξ. The real part $R(\xi)$ of ξ is x_0. For $\xi=\xi_0+\xi_1 i_4$ and $\eta=\eta_0+\eta_1 i_4$, where ξ_t and η_t belong to $\mathscr{H}_4$ for $t=0$ and 1, multiplication is defined in $\mathscr{C}$ by

$$\xi\eta=\xi_0\eta_0-\bar{\eta}_1\xi_1+(\eta_1\xi_0+\xi_1\bar{\eta}_0)i_4. \tag{1}$$

The norm $N\xi$ of ξ is $\xi\bar{\xi}$. Hence for any ξ of $\mathscr{C}$

$$\xi^2-2R(\xi)\xi+N\xi=0. \tag{2}$$

We recall the following theorem. [**4**, Theorem 2.1].

(3) *A non-rational Cayley number ρ induces an automorphism $\xi\to\rho\xi\rho^{-1}$ of $\mathscr{C}$ if and only if*

$$4R^2(\rho)=N\rho.$$

A set $\mathcal{O}$ of Cayley numbers is called an *order* if, for any element ξ of $\mathcal{O}$, (2) has rational integral coefficients, and $\mathcal{O}$ is closed under addition and multiplication. Elements of an order $\mathcal{O}$ are called Cayley integers.

Let J be the order of $\mathscr{C}$ spanned by $\{i_s\}_0^7$ over Z. Let J_t be obtained by adjoining

$$\rho_t=\tfrac{1}{2}(1+u_1+u_2+u_3)$$

to J, where $\{u_s\}_1^3$ is a multiplicatively associative set of distinct elements of $\{i_s\}_1^7$ such that $u_1u_2u_3=-1$, and $\{1, u_1, u_2, u_3, i_t, u_1i_t, u_2i_t, u_3i_t\}$ is the basis $\{i_s\}_0^7$ in some order. The set $\{u_s\}_1^3$ determines and is uniquely determined by i_t. For $1\leqq t\leqq 7$, J_t is an order of $\mathscr{C}$. Define J_0 to be the intersection of the seven orders J_t. For $\xi=\sum_{s=0}^{7} x_s i_s$, an element of J_0, the x_s are either all integers or all half odd integers. Let a submodule E of J_0 be defined by the condition:

$$\xi \in E \text{ if and only if } \xi \in J_0 \quad \text{and} \quad \sum_{s=0}^{7} x_s \in 2Z. \tag{4}$$

All elements of E have even norm. J_0 and E are orders of $\mathscr{C}$.

Let i, u, v, w be distinct elements of $\{i_s\}_1^7$ such that $i = u(vw)$. The mapping $\xi \rightarrow \rho\xi\rho^{-1}$ where

$$\rho = \tfrac{1}{2}(1+u+v+w)$$

applied to $\{i_s\}_0^7$ gives a new basis $\{e_s\}_0^7$ of $\mathscr{C}$ that reproduces the multiplication table of the first basis. Let J_i be the order obtained by adjoining $\{e_s\}_1^7$ to J. J_i is independent of the choice of u, v, w for which $u(vw) = i$ and is one of seven isomorphic maximal orders. The orders are obtained by letting i take any value from the set $\{i_s\}_1^7$. For $i = i_s$, we write $J_i = M_s$. Each M_s contains fourteen distinct sets of elements of the form $\sum_{r=1}^{4} x_r v_r$ where the x_r are half odd integers. The v_r take fourteen sets of values from $\{i_s\}_0^7$.

Let $\mathcal{O}$ be any one of the orders J, J_0, E, J_s, and M_s $(1 \leqq s \leqq 7)$. Let $r_{\mathcal{O}}(n)$ be the number of Cayley integers of norm n in $\mathcal{O}$. Let $T = \sum_{m=0}^{\alpha} 2^{3m}$ where 2^α is the highest power of 2 dividing n. The formulae listed below hold when summation is taken over all indicated rational integral divisors of the integer n.

$$r_J(n) = r_J(1) \sum_{d|n} (-1)^{n+d} d^3. \tag{5}$$

$$r_{J_0}(n) = r_{J_0}(1) \sum_{d|n} d^3, \quad \text{if } n \text{ is odd.} \tag{6}$$

$$r_{J_0}(2n) = r_{J_0}(1)(1+22T)\Big(\sum_{\substack{d|n \\ d \text{ odd}}} d^3\Big). \tag{7}$$

$$r_E(2n) = r_E(2) \sum_{d|n} d^3. \tag{8}$$

For $\mathcal{O} = J_s$ or M_s,

$$r_{\mathcal{O}}(n) = r_{\mathcal{O}}(1) \sum_{d|n} d^3, \quad \text{if } n \text{ is odd.} \tag{9}$$

$$r_{J_s}(2n) = r_{J_s}(1)(1+12T)\Big(\sum_{\substack{d|n \\ d \text{ odd}}} d^3\Big). \tag{10}$$

$$r_{M_s}(2n) = r_{M_s}(1) \sum_{d|2n} d^3. \tag{11}$$

$$r_E(2n) = r_{M_s}(n). \tag{12}$$

It can be verified that $r_J(1) = r_{J_0}(1) = 16$, $r_{J_s}(1) = 48$, and $r_{M_s}(1) = r_E(2) = 240$. The formulae (5) and (8) are known [**3**, **6**].

We outline the proof of (10). From (5),

$$\begin{aligned} r_J(2n) &= 16 \sum_{d|n} (-1)^d d^3 \\ &= 16(T-2+2^{3\alpha+3})\Big(\sum_{\substack{d|n \\ d \text{ odd}}} d^3\Big). \end{aligned}$$

$R_{8,0}(8n)$ gives the number of representations of $2n$ by 8 half odd integers. From Glaisher [1],

$$R_{8,0}(8n) = 16^2\Delta_3'(n) = 16^2 \cdot 2^{3\alpha}\Big(\sum_{\substack{d|n \\ d \text{ odd}}} d^3\Big).$$

$R_{4,4}(8n)$ gives the number of representations of $2n$ by 4 half odd integers and 4 integers.

$$\begin{aligned} R_{4,4}(8n) &= 1120\Delta_3'(2n) \\ &= 1120 \cdot 2^{3\alpha+3}\Big(\sum_{\substack{d|n \\ d \text{ odd}}} d^3\Big). \end{aligned}$$

$R_{4,4}(8n)/\binom{8}{4}$ gives the corresponding number of representations with the 4 half odd integers in fixed positions. J_s admits 2 such sets of positions. Hence

$$r_{J_s}(2n) = 16(T-2+5 \cdot 2^{3\alpha+3})\Big(\sum_{\substack{d|n \\ d \text{ odd}}} d^3\Big).$$

The result (10) follows.

REFERENCES

1. J. W. L. Glaisher, On the numbers of representations of a number as a sum of $2r$ squares, where $2r$ does not exceed eighteen, *Proc. London Math. Soc.* (2) **5** (1907), 479–490.

2. J. W. L. Glaisher, On the representations of a number as the sum of two, four, six, eight, ten, and twelve squares, *Quarterly J.* **38** (1907), 1–62.

3. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Fourth Edition, Oxford, 1960).

4. P. J. C. Lamont, Arithmetics in Cayley's Algebra, *Proc. Glasgow Math. Assoc.* **6** (1963), 99–106.

5. R. A. Rankin, A certain class of multiplicative functions, *Duke Math. J.* **13** (1946), 281–306.

6. J. P. Serre, *Cours d'Arithmétique* (Paris, 1970).

Department of Quantitative and Information Science
College of Business
Western Illinois University
Macomb
Illinois 61455