FACTORIZATION AND CONGRUENCE IN THE ARITHMETICS OF CAYLEY'S ALGEBRA

by P. J. C. LAMONT

(Received 7 December, 1989)

This paper treats factorization and congruence in the arithmetics of Cayley's algebra C. Results, proved by Rankin **[10]**, on the number of factorizations of a given element in the nonmaximal arithmetics H_0 and J_0 are reviewed. Further, new results on congruence are established and are used to find the number of factorizations of a prescribed element in the remaining arithmetics, including the maximal arithmetics J_w. When computer factorizing a given element, the congruence results can be used as a heuristic device to prune the search tree.

Let J be any arithmetic of Cayley's algebra C. If, for any two elements ζ, ξ of an arithmetic J of C, there exists an element η of J such that

$$\zeta = \xi\eta \tag{1}$$

ζ is said to be divisible by ξ on the left in J and ξ is said to divide ζ on the left in J. Similarly we define ζ to be divisible by η on the right in J if there exists an ξ of J such that (1) holds. In both cases ζ is said to have the factorization $\xi\eta$ in J and ξ, η are called factors of ζ in J. We write

$$\zeta = \xi\eta \quad \text{in } J.$$

For example, an element ρ of norm 1 in J, henceforth called a unit of J, divides any element ζ of J on the left and on the right in J. Also, clearly, a rational integer m divides an element ζ of J on the right in J if and only if m divides ζ on the left in J.

An element $\zeta$of J is said to be a Cayley *prime* for J if, for all factorizations $\xi\eta$ of ζ in J, either $N\xi = 1$ or $N\eta = 1$. For example, suppose that ζ has norm a rational prime p, say. Then it follows, since $N\zeta = N\xi\, N\eta = p$, that either ξ or η has norm 1. In this case, ζ is a Cayley prime.

If, for given quaternions α, β, γ,

$$\alpha = \beta\gamma$$

it follows, by the associative law of multiplication for quaternions, that for any quaternion δ

$$\alpha = (\beta\delta)(\delta^{-1}\gamma).$$

Thus if β divides α on the left in a quaternion arithmetic H' of C, it follows that for any unit δ belonging to H', $\beta\delta$ divides α on the left in H'.

If ζ, ξ, η are Cayley numbers and $\zeta = \xi\eta$ the relation

$$\zeta = (\xi\delta)(\delta^{-1}\eta)$$

in general only holds when δ is a nonzero real number.

Suppose that, for $N\xi = N\xi'$ and $N\eta = N\eta'$,

$$\zeta = \xi\eta = \xi'\eta'$$

are two different factorizations in arithmetic J of an element ζ of J. Then, from **[9]**, it follows that no explicit relation corresponding to a principal isotopism of C can exist

https://doi.org/10.1017/S001708950000820X Published online by Cambridge University Press

between (ξ, η) and (ξ', η') other than

$$\xi = -\xi', \qquad \eta = -\eta'$$

unless ζ of ζu is a quaternion for some unit u of C or ζ is of some other special form.

We shall see that the factors of a given element of J_w can be characterized up to a factor of ±1 by considering congruence modulo 2 in J_w.

For any rational integer $m > 0$ and Cayley integers ξ, η of J_w, we define ξ to be congruent to η modulo m in J_w if $\xi - \eta$ is divisible by m in J_w. We then write

$$\xi \equiv \eta \quad (\text{modulo } m \text{ in } J_w)$$

or, when no confusion can arise,

$$\xi \equiv \eta \quad (\operatorname{mod} m).$$

It is clear that for this definition congruence is well defined in the sense that it is an equivalence relation.

If

$$\xi \equiv \xi_1 \quad (\operatorname{mod} m), \qquad \eta \equiv \eta_1 \quad (\operatorname{mod} m)$$

then

$$\xi\eta \equiv \xi_1\eta_1 \quad (\operatorname{mod} m).$$

We only consider modulus m for m a rational integer.

We first prove

THEOREM 1. *For any elements η and η' of J_w such that*

$$\eta \equiv \eta' \quad (\text{modulo } 2 \textit{ in } J_w)$$

$N\eta$ and $N\eta'$ are either both even or both odd rational integers.

We have $\eta = \eta' + 2\zeta$ where ζ is an element of J_w. Therefore,

$$N\eta = N\eta' + 4N\zeta + 2R(2\eta'\bar{\zeta}).$$

But $n'\bar{\zeta}$ is an element of J_w. Hence $R(2\eta'\bar{\zeta})$ must be an integer. The result follows.

Also we have

THEOREM 2. *Any element ζ of maximal arithmetic J_w is congruent modulo 2 in J_w to an element τ of an arithmetic J, containing J_0, of C if and only if ζ is itself an element of J.*

We have

$$\zeta \equiv \tau \quad (\text{modulo } 2 \text{ in } J_w).$$

Thus

$$\zeta = \tau + 2\alpha$$

where α is an element of J_w. Thus 2α is contained in J_0. Hence ζ belongs to J if and only if τ belongs to J.

We now prove the more difficult

THEOREM 3. *Any element ξ of odd norm of a maximal arithmetic J_w of Cayley's algebra C is congruent modulo 2 in J_w to an element, unique apart from sign, of norm 1 of J_w.*

Let ξ be any given element of odd norm in J_w. Then, from the definition of J_w, it follows, since ξ has odd norm, that, with the notation of [3],

$$\xi = \alpha_0 + \delta_1 \xi_{(w)}$$

where α_0 is an element of J_0, $\xi_{(w)}$ equals ξ_u, ξ_u^*, $\xi_{w,v}$ or $\xi_{w,v}^*$ and u is a basic unit assigned to an associative triad containing w, and v is a basic unit assigned to a triad not containing w.

Suppose that $\delta_1 = 0$. Then $\xi = \alpha_0$ and

$$\alpha_0 \equiv \sum_{s=0}^{7} a_s i_s \quad (\text{mod } 2)$$

where each a_s is 0 or 1. Since $N\alpha_0$ is odd, the numer r of coefficients for which $a_s = 1$ $(0 \leq s \leq 7)$ must be odd.

If $r = 1$ the result follows.

If $r = 3$ we have

$$\alpha_0 \equiv i_{s_1} + i_{s_2} + i_{s_3} \quad (\text{mod } 2).$$

It is easy to prove that there exists a basic unit i_t of C for which $\frac{1}{2}(i_t + i_{s_1} + i_{s_2} + i_{s_3})$ is contained in J_w. But for any such set (u_1, u_2, u_3, u_4)

$$\sum_{l=1}^{4} u_l \equiv 0 \quad (\text{mod } 2).$$

Thus in this case

$$\alpha_0 \equiv i_t \quad (\text{mod } 2).$$

If $r = 5$ we have, since

$$\sum_{l=0}^{7} i_l \equiv 0 \quad (\text{mod } 2),$$

α_0 congruent modulo 2 in J_w to the sum of three different basic units of C. The case $r = 5$ has thus been reduced to the case $r = 3$.

Similarly the result follows if $r = 7$.

If $\delta_1 = 1$, we have

$$\xi = \alpha_0 + \xi_{(w)}.$$

From above we see that if $N\alpha_0$ is odd, α_0 is congruent modulo 2 in J_w to a basic unit i_t, say, of J_0. Now write

$$\xi_{(w)} = \tfrac{1}{2} \sum_{l=1}^{4} w_l$$

where w_s $(1 \leq s \leq 8)$ are the eight basic units of J_0.
Then we have $i_t = w_{l_1}$ for some l_1 $(1 \leq l_1 \leq 4)$ for if not ξ is congruent modulo 2 in J_w to an element of even norm of J_w which cannot be true. Thus

$$\xi \equiv \tfrac{1}{2}(-w_{l_1} + w_{l_2} + w_{l_3} + w_{l_4}) \quad (\text{mod } 2)$$

and the result follows.

Now suppose that $N\alpha_0$ is even. Then

$$\alpha_0 \equiv \sum_{s=0}^{7} a_s i_s \quad (\text{mod } 2)$$

where each $a_s = 0$ or 1. Since $N\alpha_0$ is even the number r of coefficients $a_s = 1$ must be even.

https://doi.org/10.1017/S001708950000820X Published online by Cambridge University Press

If $r=0$ or 8 the result follows at once.

If $r=2$ or 6 we have

$$\xi \equiv i_{s_1} + i_{s_2} + \xi_{(w)} \pmod 2$$

where as before

$$\xi_{(w)} = \tfrac{1}{2} \sum_{l=1}^{4} w_l$$

and the w's form a set D, say, of four basic units of C. Precisely one of i_{s_1} and i_{s_2} cannot occur in D, for ξ must be congruent modulo 2 in J_w to an element of odd norm. If neither i_{s_1} nor i_{s_2} occurs in D the result follows as before. We now suppose that both i_{s_1} and i_{s_2} occur in the set D. In this case it is easy to prove that there exist two elements w_{s_1}, w_{s_2} of D for which

$$\tfrac{1}{2}(i_{s_l} + i_{s_2} + w_{s_l} + w_{s_2})$$

is a contained in J_w.

We deduce that

$$i_{s_1} + i_{s_2} \equiv w_{s_1} + w_{s_2} \pmod 2.$$

Hence

$$\xi \equiv \tfrac{1}{2}(-w_{s_1} - w_{s_2} + w_{s_3} + w_{s_4}) \pmod 2.$$

Finally we suppose that $r=4$. Then

$$\xi \equiv i_{s_1} + i_{s_2} + i_{s_3} + i_{s_4} + \tfrac{1}{2}(w_1 + w_2 + w_3 + w_4) \pmod 2.$$

Clearly the sets $(i_{s_1}, i_{s_2}, i_{s_3}, i_{s_4})$ and (w_1, w_2, w_3, w_4) must have an even number of elements in common for otherwise ξ is congruent modulo 2 in J_w to an element of even norm. If the sets have no element in common or four elements in common the results is immediate. If they have precisely two elements in common the argument reduces to the previous case.

Thus for any element ξ contained in J_w

$$\xi \equiv \rho \quad (\text{modulo } 2 \text{ in } J_w)$$

where ρ is an element of norm 1 of J_w. If also

$$\xi \equiv \rho' \quad (\text{modulo } 2 \text{ in } J_w)$$

where $N\rho' = 1$ it follows that $\rho = \pm\rho'$. Theorem 3 has thus been proved.

As an example we consider the element

$$\xi = 1 + i_1 + \tfrac{1}{2}(i_4 + i_5 + i_6 - i_7).$$

Since the characteristic unit [3] $x(\xi) = 1$ and

$$\xi = 1 + i_1 + \tfrac{1}{2}(1 + i_1 + i_2 + i_3)i_4 = \alpha_0 + \xi_{(w)}$$

where $\alpha_0 = 1 + i_1$ and $\xi_{(w)} = \xi^*_{i_4}$, we can take $w = i_1$, i_2 or i_3. In J_{i_3} we have

$$\beta = 1 - i_1 + i_4 + i_6 \equiv 0 \pmod 2$$

since $x(\tfrac{1}{2}\beta) = i_3$. Thus in J_{i_3}

$$\xi \equiv -i_4 - i_6 + \tfrac{1}{2}(i_4 + i_5 + i_6 + i_7) \pmod 2$$
$$\equiv \tfrac{1}{2}(-i_4 + i_5 - i_6 + i_7) \pmod 2$$

while in J_{i_1} we have

$$\xi \equiv \tfrac{1}{2}(+i_4 + i_5 - i_6 - i_7) \pmod 2.$$

Next we deduce from Theorem 3

https://doi.org/10.1017/S001708950000820X Published online by Cambridge University Press

THEOREM 4. *Any element η of even norm of a maximal arithmetic J_w of Cayley's algebra C is congruent modulo 2 in J_w to the sum of two elcments of J_w of norm 1 or to zero.*

This follows since any such element η can be written as $\eta_1+\eta_2$ where η_1 and η_2 are linear combinations of disjoint defining sets of units for J_w and are such that $N\eta_1$ and $N\eta_2$ are odd.

Theorems 3 and 4 are used to characterize and count the number of distinct factors in maximal arithmetic J_w of a given element ζ of J_w. However, we must first relate the number of representations of odd rational integer mn as $\sum_{s=0}^{7} z_s^2$, where $\sum_{s=0}^{7} z_s i_s$ is an element of J_w, to the number of representations of rational integers m and n of this form.

We define $r_h(m)$ to be the number of different representations of m as $\sum_{s=0}^{7} x_s^2$ where $\sum_{s=0}^{7} x_s i_s$ is contained in fixed arithmetic J_h of C for h an integer between 0 and 7 or one of the seven basic units of C other than 1. Further we write $r_0(m)=r(m)$. Clearly,

$$r_s(m)=r_t(m) \quad \text{and} \quad r_{i_s}(m)=r_{i_t}(m)$$

for s and t between 1 and 7. For example, $r(1)=16$, and $r_s(1)=48$ and $r_{i_s}=240$ for $1\le s\le 7$.

We state without proof some results on the number of distinct representations of a rational integer as the norm of an element of any fixed arithmetic of C containing the eight basic units of C.

THEOREM 5.

(i) *For an odd rational integer*

$$r_h(m)r(1)=r(m)r_h(1).$$

(ii) *For m, n odd rational integers such that $(m,n)=1$*

$$r_h(m)r_h(n)=r_h(mn)r_h(1).$$

(iii) *For p a rational prime and integer $t>0$*

$$r_h(p)=r_h(1)(1+p^3)$$

and

$$r_h(1)r_h(p^{t+1})=r_h(p)r_h(p^t)-r_h(1)p^3r_h(p^{t-1}).$$

(iv) *For integer $t>0$*

$$r(2^t)=16\left\{\sum_{s=1}^{t} 2^{3s}-1\right\}$$

where in each case h may take any one of the values $0,1,\ldots,7,i_1,i_2,\ldots,i_7$.

The results for $r(m)$ are given in Rankin's paper [**10**]. Then it follows that, for m odd,

$$r(4m)=\tfrac{1}{16}r(4)r(m)=71r(m).$$

Hence the number of representations of $4m$ as a sum of eight squares of integers, four of

https://doi.org/10.1017/S001708950000820X Published online by Cambridge University Press

which are odd, is $70r(m)$. Thus, from Theorem 5(i), it follows that

$$r_{i_s}(m) = 15r(m)$$

and

$$r_s(m) = 3r(m) \quad \text{for} \quad 1 \le s \le 7.$$

An independent proof of Theorem 5 can be given by means of the methods indicated by Rankin.

We now prove

THEOREM 6. *Any element ζ of maximal arithmetic J_w of C for which $N\zeta = mn$ where m, n are positive rational integers such that $(m, n) = 1$ has precisely 240 different factorizations $\xi\eta$ in J_w for which $N\xi = m$ and $N\eta = n$.*

If $N\xi_1 = m = N\xi_2$ and $\xi_1 \ne \pm\xi_2$ then the absolute value of $R(\bar{\xi}_1, \xi_2)$ is less than m. For if

$$\xi_t = \sum_{s=0}^{7} x_{ts} i_s \quad (t = 1, 2)$$

we have

$$N(\xi_1 \pm \xi_2) = \sum_{s=0}^{7} (x_{1s} \pm x_{2s})^2 < 2 \sum_{s=0}^{7} (x_{1s}^2 \pm x_{2s}^2) = 4m.$$

Further, suppose that ζ is dividisible on the left by ξ_1 and ξ_2 in J_w where $N\xi_1 = N\xi_2 = m$. Write

$$\zeta = \xi_1\eta_1 \quad \text{and} \quad \zeta = \xi_2\eta_2.$$

Then

$$\zeta\bar{\eta}_2 = (\xi_2\eta_2)\bar{\eta}_2 = \xi_2 n.$$

Similarly,

$$\eta_1\bar{\zeta} = n\bar{\xi}_1.$$

Thus

$$n^2\bar{\xi}_1\xi_2 = (\eta_1\bar{\zeta})(\zeta\bar{\eta}_2).$$

Hence,

$$n^2 R(\bar{\xi}_1\xi_2) = N\zeta R(\eta_1\bar{\eta}_2).$$

But $(m, n) = 1$. Therefore,

$$R(\bar{\xi}_1\xi_2) = 0 \quad \text{or} \quad \pm\tfrac{1}{2}m.$$

Suppose further that

$$\xi_1 \equiv \xi_2 \quad (\text{mod } 2 \text{ in } J_w).$$

Then

$$\bar{\xi}_1\xi_2 \equiv 1 \quad (\text{mod } 2 \text{ in } J_w). \tag{2}$$

Thus, by Theorem 2, $\bar{\xi}_1\xi_2$ is contained in J_0. Hence

$$R(\bar{\xi}_1\xi_2) = 0. \tag{3}$$

Now $N(\bar{\xi}_1\xi_2) = m^2$ and m is odd. Therefore, $\bar{\xi}_1\xi_2$ has one or five odd rational integral components. It is easy to show that any set of five basic units of C contains a basic defining set of units for J_w. Thus the sum of any five such basic units is congruent modulo 2 in J_w to one of the five units. Hence

$$\bar{\xi}_1\xi_2 \equiv i_t \quad (\text{mod } 2) \tag{4}$$

for some t, $(1 \le t \le 7)$.

https://doi.org/10.1017/S001708950000820X Published online by Cambridge University Press

But (2) and (4) cannot both hold. Hence

$$\xi_1 \not\equiv \xi_2 \pmod 2. \tag{5}$$

From (5), Theorem 3 and the fact that

$$r_w(1) = 240,$$

it follows that any ζ of odd norm mn where $(m, n) = 1$ has at most 240 factorizations $\xi\eta$ in J_w such that $N\xi = m$, $N\eta = n$.

Now suppose that there exists a ζ in J_w of norm mn with less than 240 such factorizations. For all such ζ for which $N\zeta = mn$ the number of factorizations of this form is given by $r_w(m)r_w(n)$.

We deduce that

$$r_w(m)r_w(n) < 240 \sum_{N\zeta = mn} 1 = 240 r_w(mn).$$

But this contradicts Theorem 5(ii) with $h = w$. This completes the proof of Theorem 6.

Next we prove

THEOREM 7. *Any element ζ of maximal arithmetic J_w of C for which $N\zeta = p^{l+1}$ where p is an odd rational prime and $l > 0$ has precisely*

(i) $240(1 + p^3)$ *distinct factorizations $\xi\eta$ in J_w for which $N\xi = p$ and $N\eta = p^l$ if p divides ζ in J_w or*

(ii) 240 *such factorizations if p does not divide ζ in J_w.*

Proof. (i) Suppose that p divides ζ in J_w. Then $\zeta = p\zeta'$ where ζ' is contained in J_w. Let ξ be any element of J_w of norm p and suppose that $\eta = \bar{\xi}\zeta'$. Then η is contained in J_w. Also

$$\xi\eta = \xi(\bar{\xi}\zeta') = p\zeta' = \zeta.$$

Thus ζ has as many distinct factorizations $\xi\eta$ with $N\xi = p$ and $N\eta = p^l$ as there are distinct elements of norm p in J_w. The result follows from (iii) of Theorem 5.

(ii) Suppose now that p does not divide ζ in J_w. Let ζ have distinct factorizations $\xi_1\eta_1$ and $\xi_2\eta_2$ in J_w for which

$$N\xi_1 = N\xi_2 = p \quad \text{and} \quad N\eta_1 = N\eta_2 = p^l.$$

Suppose that

$$\xi_1 \equiv \xi_2 \quad (\text{mod } 2 \text{ in } J_w).$$

Then

$$\xi_1\bar{\xi}_2 \equiv 1 \quad (\text{mod } 2 \text{ in } J_w).$$

Thus, by Theorem 2, $\xi_1\bar{\xi}_2$ is an element of J_0.

Now, we have

$$R\{\xi_1(\bar{\xi}_1\zeta) + (\bar{\zeta}\xi_1)\bar{\xi}_2\} = R(\zeta)2R(\xi_1\bar{\xi}_2).$$

But,

$$\xi_1(\bar{\xi}_2\zeta) = p\xi_1\eta_2 \quad \text{and} \quad (\bar{\zeta}\xi_1)\bar{\xi}_2 = p\bar{\eta}_1\bar{\xi}_2.$$

Therefore, p divides $2R(\zeta)R(\xi_1\bar{\xi}_2)$. Since odd prime p does not divide ζ in J_w it does not divide $2R(\zeta)$. Therefore, p divides $R(\xi_1\bar{\xi}_2)$. But $R(\xi_1\bar{\xi}_2)$ is an integer and $N(\xi_1\bar{\xi}_2) = p^2$.

https://doi.org/10.1017/S001708950000820X Published online by Cambridge University Press

Now $\xi_1 \neq \pm\xi_2$. Therefore $\xi_1\bar{\xi}_2 \neq p$. Hence $R(\xi_1\bar{\xi}_2)=0$ and $\xi_1\bar{\xi}_2$ has one or five odd rational integral components. Thus, as in the proof of Theorem 6, $\xi_1\bar{\xi}_2$ is congruent modulo 2 in J_w to a basic unit of J_0 other than ± 1. Therefore each element of ξ of norm p which divides ζ on the left in J_w is congruent modulo 2 to a distinct element of norm 1 of J_w. Hence there exist at most 240 distinct factorizations $\xi\eta$ in this case. For all ζ of norm p^{l+1} in J_w the number of factorizations of this form is given by

$$r_w(p)r_w(p^l).$$

Suppose that there exists a ζ in J_w of norm p^{l+1} which is not divisible by p in J_w with less than 240 factorizations of the type described. Then

$$\begin{aligned} r_w(p)r_w(p^l) &< 240 \sum_{N\zeta=p^{l+1}, p\nmid\zeta} 1 + 240(1+p^3)\sum_{N\zeta=p^{l+1}, p\mid\zeta} 1 \\ &= 240\{r_w(p^{l+1}) - r_w(p^{l-1})\} \\ &\quad + 240(1+p^3)r_w(p^{l-1}) \\ &= 240r_w(p^{l+1}) + 240p^3r_w(p^{l-1}) \\ &= r_w(p)r_w(p^l). \end{aligned}$$

Hence no such ζ exists. The result has thus been proved by contradiction. This completes the proof of Theorem 7.

Let ζ be any element of an arithmetic J_h for some h ($h=0,1,\ldots,7,i_1,i_2,\ldots,i_7$) of C. Suppose that $N\zeta=mn\neq 0$. We use a notation suggested by that of Rankin [**10**] and define

$$\Omega_h(\zeta;m,n)=\Omega_h(\zeta)$$

to be the set of all factorizations $\xi\eta$ of ζ in J_h for which $N\xi=m$ and $N\eta=n$. Also we define

$$S_h(\zeta;m,n)=S_h(\zeta)$$

to be the number of such factorizations.

Thus we have proved, for w a basic unit of C other than 1, the following result.

THEOREM 6. *For m, n odd positive rational integers such that $(m,n)=1$,*

$$S_w(\zeta;m,n)=240.$$

Also we have proved

THEOREM 7. *For p an odd rational prime and $l>0$*

(i) *if p divides ζ in J_w*

$$S_w(\zeta;p,p^l)=240(1+p^3), \quad \textit{or}$$

(ii) *if p does not divide ζ in J_w*

$$S_w(\zeta;p,p^l)=240.$$

From Theorems 6 and 7 we deduce the following results.

THEOREM 8. *For m, n odd positive rational integers such that $(m,n)=1$*

$$S_0(\zeta;m,n)=16.$$

https://doi.org/10.1017/S001708950000820X Published online by Cambridge University Press

THEOREM 9. *For p an odd rational prime and $l > 0$*

(i) *if p divides ζ in J_0*

$$S_0(\zeta; p, p^l) = 16(1 + p^3), \quad \textit{or}$$

(ii) *if p does not divide ζ in J_0*

$$S_0(\zeta; p, p^l) = 16.$$

THEOREM 10. *For m, n odd positive rational integers such that $(m, n) = 1$ and any t* $(1 \le t \le 7)$

$$S_t(\zeta; m, n) = 48.$$

THEOREM 11. *For p an odd rational prime, $l > 0$, and any t* $(1 \le t \le 7)$

(i) *if p divides ζ in J_t*

$$S_t(\zeta; p, p^l) = 48(1 + p^3), \quad \textit{or}$$

(ii) *if p does not divide ζ in J_t*

$$S_t(\zeta; p, p^l) = 48.$$

The methods used to establish Theorems 6 and 7 were first used by Rankin **[10]** to establish Theorems 8 and 9 above. We have used the idea of congruence modulo 2 in J_w, while Rankin used the fact that the eight basic units of C are linearly independent and generate J_0 over the rational integers.

We have already see that J_0 occurs as a subset of J_w for any basic unit w of C other than 1 and that J_t $(1 \le t \le 7)$ occus as a subset of J_w for three basic unis w of C for which $w \neq 1$. Further, the elements of J_w which belong to J_s $(0 \le s \le 7)$ are characterized as the elements of J_w congruent modulo 2 in J_w to an element of J_s of norm 1. Thus Theorems 8 and 10 follow from Theorems 5 and 6, while from Theorems 5 and 7 we deduce Theorem 9 and 11.

REFERENCES

1. F. van der Blij, *History of the octaves*, Wis- en Natuurkundig Tijdschrift (= Simon Stevin) **34,** III (1961), 106–125.

2. F. Van der Blij and T. A. Springer, *The arithmetics of the octaves and of the group G_2*, Nederl. Akad. Wetensch. Proc. (= Indag. Math.) **62A** (1959), 406–418.

3. P. J. C. Lamont, *Arithmetics in Cayley's algebra*, Proc. Glasgow Mathematical Assoc. **6** (1963), 99–106.

4. P. J. C. Lamont, *Ideals in Cayley's algebra*, Nederl. Akad. Wetensch. Proc. (= Indag. Math.) **66A** (1963), 394–400.

5. P. J. C. Lamont, *Approximation theorems for the group G_2*, Nederl. Akad. Wetensch. Proc. (= Indag. Math.) **67A** (1964), 187–192.

6. P. J. C. Lamont, *Factorization and arithmetic functions for orders in composition algebras*, Glasgow Mathematical Journal **14** (1973), 86–95.

7. P. J. C. Lamont, *The number of Cayley integers of given norm*, Proc. Edinburgh Math. Soc. **25** (1982), 101–103.

8. P. J. C. Lamont. *Computer generated natural inner automorphisms of Cayley's algebra*, Glasgow Mathematical Journal **23** (1982), 187–189.

9. P. J. C. Lamont, *The nonexistence of a factorization formula for Cayley numbers*, Glasgow Mathematical Journal **24** (1983), 131–132.

https://doi.org/10.1017/S001708950000820X Published online by Cambridge University Press

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

11. O. Taussky, *Sums of squares*, Am. Math. Monthly **77** (1970), 805–830.

Department of Computer Science
College of Applied Sciences
Western Illinois University
Macomb, Illinois 61455

https://doi.org/10.1017/S001708950000820X Published online by Cambridge University Press