DIOPHANTINE EQUATIONS IN DIVISION ALGEBRAS*

BY

RALPH G. ARCHIBALD

1. Introduction. A type of division algebras of order n^2, defined over a field F,—called algebras of type D—has been given by Professor L. E. Dickson.† A further division algebra of order sixteen has lately been given by Professor F. Cecioni.‡ A great advance in the problem of the determination of all division algebras has been made in Dickson's recent paper on *New division algebras*.§ In that paper it is shown how to construct algebras Γ of order p^2q^2 over a field F, corresponding to the Galois group, of order $n=pq$, of an equation $f(x)=0$, of degree n, irreducible in the field F. General conditions that algebras Γ be associative are derived; and, in particular, associativity conditions are deduced for algebras Γ whose group for the field F is abelian and has two generators. In §12 of his paper Dickson gives necessary and sufficient conditions, for the case $p=q=2$, that an algebra Γ, whose group is abelian for the field F, be an associative division algebra.

It is the object of the present paper to obtain necessary and sufficient conditions for the solvability, in integers, of the diophantine equations which arise in an attempt to satisfy the associativity conditions for an algebra Γ based on the quartic equation $x^4+px^2+n^2=0$ irreducible in the field of rational numbers. In §2 it is noted that, in view of a known theorem on Tschirnhausen transformations, quite a general situation is being considered when the quartic equation is assumed to be of the above form. In §3 a diophantine equation in six unknowns is obtained which, by simple change of variables (in §4), simplifies to

$$U^2 - a_1R_0^2 = (A_0^2 - a_1b_1B_0^2)(F_1^2 - b_1C_0^2),$$

where each of $a_1=2n-p$, $b_1=-2n-p$, a_1b_1 is an integer different from a perfect square. In §5, by the use of Dickson's result on the integral solutions of $x^2-my^2=zw$, the nature of the problem is modified; in §7 necessary and sufficient conditions for the solvability, in integers, of the diophantine equation are obtained and simplified; and, finally, in §9 numerical examples

* Presented to the Society, October 29, 1927; received by the editors in December, 1927.

† *Algebras and their Arithmetics*, §47, p. 65.

‡ Rendiconti del Circolo Matematico di Palermo. vol. 47 (1923), pp. 209–254.

§ These Transactions, vol. 28 (1926), pp. 207–234.

are given which, incidentally, show that the conditions obtained are not inconsistent.

2. **Quartic equation irreducible in the field of rational numbers.** It is known* that, by means of a rational quadratic Tschirnhausen transformation, a quartic equation with rational coefficients, irreducible in the field of rational numbers, whose Galois group for the field of rational numbers is the group

$$G_4 = \{I, (12)(34), (13)(24), (14)(23)\},$$

can be brought to the form

$$x_1^4 + p_1 x_1^2 + n_1^2 = 0,$$

where p_1 and n_1 are rational numbers.

Write $n_1 = n_2/n_3$, $p_1 = p_2/p_3$, where n_2, n_3, p_2, p_3 are integers. Multiplying the resulting equation through by $(p_3 n_3)^4$ and introducing the new variable $x = p_3 n_3 x_1$, we obtain

$$x^4 + px^2 + n^2 = 0, \tag{1}$$

where $p = p_2 p_3 n_3^2$, $n = n_2 n_3 p_3^2$ are both integers.

The following theorem can be easily established.

THEOREM 1. *Necessary and sufficient conditions for the irreducibility, in the field of rational numbers, of the equation* (1) *with p and n rational, are that each of*

$$p^2 - 4n^2, \quad 2n - p, \quad -2n - p \tag{2}$$

be different from a perfect square in the field of rational numbers.

3. **Associativity conditions for a division algebra Γ of order sixteen.** Let us consider an equation (1) which is irreducible in the field of rational numbers and in which p and n are integers. It is proposed to develop algebras of type Γ, of order sixteen, on the basis of this equation (1).

Since this equation is irreducible in the field of rational numbers, $n \neq 0$; thus the roots of (1) are

$$x_1 = i, \quad x_2 = \theta_1(i) = -i, \quad x_3 = \theta_2(i) = \frac{i^3 + pi}{n} = -\frac{n}{i},$$

$$x_4 = \theta_3(i) \equiv \theta_1[\theta_2(i)] = \theta_2[\theta_1(i)] = \frac{-i^3 - pi}{n} = \frac{n}{i}.$$

* See R. J. Garver, *A normal form for certain quartics*, Messenger of Mathematics, vol. 56, No. 12, pp. 184–6.

Moreover, the Galois group of equation (1) for the field of rational numbers is

$$G_4 = \{I,\ \Theta_1,\ \Theta_2,\ \Theta_3 \equiv \Theta_1\Theta_2 = \Theta_2\Theta_1\},$$

where

$$\Theta_1 = (12)(34), \quad \Theta_2 = (14)(23).$$

In view of Dickson's memoir on *New division algebras*, §12, consider the quartic equation (1) irreducible in the field R of rational numbers. The roots $i, \theta_1(i), \theta_2(i), \theta_3(i)$ of equation (1) are rational functions of i with coefficients in R such that

$$\theta_1\theta_1 = \theta_2\theta_2 = \theta_3\theta_3 = i, \quad \theta_1\theta_2 = \theta_2\theta_1 = \theta_3, \quad \theta_1\theta_3 = \theta_3\theta_1 = \theta_2, \quad \theta_2\theta_3 = \theta_3\theta_2 = \theta_1,$$

where $\theta_r\theta_s$ denotes $\theta_r[\theta_s(i)]$. Under the law of multiplication

$$(a + bj_1)(c + dj_1) = ac + gbd(\theta_1) + [ad + bc(\theta_1)]j_1,$$

where a, b, c, d, g are in $R(i)$, the elements $a+bj_1$ form an associative algebra Σ if and only if g is in the field $R(i^2)$ (that is, if and only if $g=g(\theta_1)$), and they form an associative division algebra Σ if and only if g is in the field $R(i^2)$, but is not the norm, relative to $R(i^2)$, of any number of $R(i)$. For $A=a+bj_1$, write $A'=a(\theta_2)+b(\theta_2)\alpha j_1$, where α and γ (as defined in Dickson's paper) are in $R(i)$. Under the law of multiplication

$$(A_0 + A_1j_2)(B_0 + B_1j_2) = (A_0B_0 + A_1B_1'\gamma) + (A_0B_1 + A_1B_0')j_2,$$

where A_0, A_1, B_0, B_1 are in Σ, the elements $A_0+A_1j_2$ form an associative algebra Γ, when Σ is one, if and only if

$$\alpha\alpha(\theta_1)g = g(\theta_2), \qquad \alpha\alpha(\theta_2)\gamma(\theta_1) = \gamma = \gamma(\theta_2),$$

and they form an associative division algebra Γ, when Σ is one, if and only if

$$\gamma \neq X'X \text{ for any } X \text{ in } \Sigma,$$

and

$$\alpha\alpha(\theta_1)g = g(\theta_2), \qquad \alpha\alpha(\theta_2)\gamma(\theta_1) = \gamma = \gamma(\theta_2).$$

This Γ is an algebra over the field R with the sixteen basal units i^rj_s $(r, s=0, 1, 2, 3)$, where $j_3=j_1j_2$, $j_0=1$. On the other hand, the algebra Γ may be regarded as an algebra of order four over the field $R(i)$ with the basal units

$$1, j_1, j_2, j_3 = j_1j_2.$$

Special cases of the laws of multiplication give

$$j_1^2 = g, \ j_2^2 = \gamma, \ j_2j_1 = \alpha j_1j_2, \ j_ri = \theta_r(i)j_r, \ j_r\phi(i) = \phi[\theta_r(i)]j_r \ (r = 0,1,2,3).$$

Necessary and sufficient conditions that the algebra Γ be associative are the following:

(3) $$j_1^2 = g(i) = g(\theta_1),$$

(4) $$j_2^2 = \gamma(i) = \gamma(\theta_2),$$

(5) $$\alpha\alpha(\theta_1)g = g(\theta_2),$$

(6) $$\alpha\alpha(\theta_2) = \gamma(i)\gamma^{-1}(\theta_1),$$

where α, g, γ are rational functions of i with coefficients in R.

Being an even function of i, g must be of the form

(7) $$g = ai^2 + b,$$

where a and b are both rational numbers. Also, since $\gamma = \gamma(\theta_2)$,

$$\gamma(i) = \gamma\left(-\frac{n}{i}\right);$$

whence, where c, d, e, f are all rational numbers,

$$\gamma = ci^3 + di^2 + ei + f$$
$$= i^3\left(\frac{e}{n} - \frac{cp}{n}\right) + i^2(-d) + i\left(cn - \frac{cp^2}{n} + \frac{ep}{n}\right) + (f - dp).$$

Equating coefficients and combining results, we have

$$d = 0, \quad \frac{e}{n} = c\left(1 + \frac{p}{n}\right).$$

Therefore

(8) $$\gamma = ci^3 + c(n + p)i + f.$$

Define a number η of $R(i)$ in terms of α, g, γ as follows:

(9) $$j_3^2 = j_1j_2j_1j_2 = j_1(\alpha j_1)j_2j_2 = \alpha(\theta_1)j_1^2j_2^2 = \alpha(\theta_1)g\gamma = \eta.$$

By equations (5) and (6),

$$\alpha\alpha(\theta_1)g\gamma\gamma(\theta_1) = g(\theta_2)\gamma\gamma(\theta_1) = g(\theta_2)\alpha\alpha(\theta_2)\gamma(\theta_1)\gamma(\theta_1).$$

Hence, since α and γ are both different from zero,

$$\alpha(\theta_1)g\gamma = \alpha(\theta_2)g(\theta_2)\gamma(\theta_1).$$

Therefore, by definition of η, $\eta = \eta(\theta_1\theta_2)$. Moreover, by equation (5),

$$\eta\eta(\theta_1) = g\alpha\alpha(\theta_1)g\gamma\gamma(\theta_1) = gg(\theta_2)\gamma\gamma(\theta_1).$$

The associativity conditions (3)-(6) are now replaced by

(3′) $$j_1^2 = g = g(\theta_1),$$

(4′) $$j_2^2 = \gamma = \gamma(\theta_2),$$

(5′) $$j_3^2 = \eta = \eta(\theta_3),$$

(6′) $$\eta\eta(\theta_1) = gg(\theta_2)\gamma\gamma(\theta_1).$$

Evidently η is of the form

$$\eta = ri^3 + si^2 + ti + u,$$

where r, s, t, u are rational numbers. Therefore, in view of (5′),

$$ri^3 + si^2 + ti + u = i^3\left(\frac{rp}{n} - \frac{t}{n}\right) - si^2 + i\left(\frac{rp^2}{n} - \frac{tp}{n} - rn\right) + u - sp.$$

As a result of equating coefficients of like powers of i, we obtain

$$\eta = ri^3 + r(p - n)i + u. \tag{10}$$

Equation (6′) imposes a condition which becomes, on simplification,

$$r^2(n^2p - 2n^3) + u^2 = (a^2n^2 - abp + b^2)(c^2n^2p + 2c^2n^3 + f^2). \tag{11}$$

The problem of satisfying the associativity conditions (3′)-(6′) now becomes the problem of satisfying equation (11) with rational values for r, u, a, b, c, f.

4. **A type of diophantine equation.** When we write

$$\begin{aligned} h &= n^2p - 2n^3, & U_1 &= u, & C_1 &= c, \\ l &= n^2p + 2n^3, & A_1 &= a, & F_1 &= f, \\ R_1 &= r, & B_1 &= b, & & \end{aligned}$$

equation (11) becomes

$$hR_1^2 + U_1^2 = (n^2A_1^2 - pA_1B_1 + B_1^2)(lC_1^2 + F_1^2), \tag{12}$$

where n and p are regarded as parameters and the capital letters as variables. It will now be proved that all *rational* solutions of equation (12) are known when all *integral* solutions are known.

Consider any rational solution:

$$R_1 = R/D,\ U_1 = U/D,\ A_1 = A/D,\ B_1 = B/D,\ C_1 = C/D,\ F_1 = F/D, \tag{13}$$

where R, U, A, B, C, F, D are integers. Therefore, placing these values in equation (12) and multiplying through by D^4, we obtain

$$h(DR)^2 + (DU)^2 = (n^2A^2 - pAB + B^2)(lC^2 + F^2).$$

Therefore,

$$R_1 = DR,\ U_1 = DU,\ A_1 = A,\ B_1 = B,\ C_1 = C,\ F_1 = F \tag{14}$$

is an integral solution of (12). Consequently, any rational solution (13) is obtained from an appropriate integral solution (14) by dividing the first two values in (14) by D^2, and the last four by D.

Multiply equation (12) through by 4 and rewrite it in the form

$$h(2R_1)^2 + (2U_1)^2 = \{n^2(2A_1)^2 - p(2A_1)(2B_1) + (2B_1)^2\}\{lC_1^2 + F_1^2\}. \tag{15}$$

Make now the following substitutions in (15):

$$\begin{aligned} A_1 &= B_0, & 2R_1 &= R_2, \\ 2B_1 &= -A_0 + pB_0, & 2U_1 &= U, \\ p^2 - 4n^2 &= -m. \end{aligned} \tag{16}$$

Equation (15) then becomes

$$hR_2^2 + U^2 = (A_0^2 + mB_0^2)(hC_1^2 + F_1^2). \tag{17}$$

All integral solutions of (12) give rise, by virtue of relations (16), to integral solutions of (17). Moreover, the totality of those integral solutions of (17) for which are satisfied the following conditions (18), give rise to all the integral solutions of (12):

$$R_2 \equiv 0,\ U \equiv 0,\ A_0 \equiv pB_0 \pmod 2. \tag{18}$$

Placing

$$a_1 = 2n - p,\ b_1 = -2n - p,\ R_0 = nR_2,\ C_0 = nC_1, \tag{19}$$

we bring equation (17) to the form

$$U^2 - a_1R_0^2 = (A_0^2 - a_1b_1B_0^2)(F_1^2 - b_1C_0^2). \tag{20}$$

All integral solutions of (12) are obtained by securing all integral solutions of (20) for which the following conditions (21) are satisfied:

$$\begin{aligned} R_0 &\equiv 0 \pmod{2n}, & U &\equiv 0 \pmod 2, \\ C_0 &\equiv 0 \pmod n, & A_0 &\equiv pB_0 \pmod 2. \end{aligned} \tag{21}$$

The problem is now reduced to that of considering the solution* in integers (not all zero) of equation (20), where, in view of conditions (2), each of a_1, b_1, a_1b_1 is different from a perfect square.

5. **Modification of the problem.** In the Bulletin of the American Mathematical Society, vol. 29 (1923), pp. 464–7, Dickson derived† the result that all integral solutions of the equation

$$x^2 - my^2 = zw$$

are given by

$$\begin{aligned} z &= s(el^2 + 2flq + gq^2), & w &= s(en^2 - 2fnt + gt^2), \\ x &= \pm s(eln + fnq - flt - gqt), & y &= s(lt + nq), \end{aligned} \tag{22}$$

* This problem in diophantine analysis cannot be solved by the known methods of composition of forms. For, to obtain solutions by composition, the determinants of $U^2 - a_1R_0^2$, $A^2 - a_1b_1B_0^2$, and $F^2 - b_1C_0^2$ must be in the ratios of three integral squares (cf. C. F. Gauss, *Disquisitiones Arithmeticae*, art. 235). That is, a_1b_1/a_1 = perfect square. This is contrary to restrictions (2) placed on b_1.

† See also a paper by Dickson in the same Bulletin, vol. 27 (1920–21), pp. 353–365. In that paper Dickson was led to the present theorem by the theory of ideals.

where s ranges over the set of rational integers and where e, f, g take only those sets of integral values (finite in number) for which the form $el^2+2flq+gq^2$ is a reduced* quadratic form having the same discriminant $4m$ as x^2-my^2, so that

$$f^2 - eg = m.$$

Consider equation (20) in which it is assumed that each of the integers a_1, b_1, a_1b_1 is different from a perfect square. Let a_0^2, b_0^2 be the greatest integral squares contained in a_1, b_1, and let c be the greatest common divisor of a_1/a_0^2, b_1/b_0^2. Write

$$a_1 = aca_0^2, \qquad b_1 = bcb_0^2.$$

Consequently, we can state the restrictions on a, b, c as follows:

(23) c is positive; no one of a, b, c possesses a square factor (other than 1); no two of a, b, c have a common factor greater than 1; and, moreover, whenever $c=1$, both a and b are different from 1.

Equation (20) can be written as

$$(20') \qquad U^2 - ac(a_0R_0)^2 = \{A_0^2 - ab(ca_0b_0B_0)^2\}\{F_1^2 - bc(b_0C_0)^2\}.$$

Place

$$(24) \qquad R = a_0R_0,\ A = A_0,\ B = ca_0b_0B_0,\ F = F_1,\ C = b_0C_0.$$

Equation (20′) now becomes

$$(25) \qquad U^2 - acR^2 = (A^2 - abB^2)(F^2 - bcC^2),$$

where a, b, c are subject to conditions (23).

All integral solutions of equation (20) are obtained from all those integral solutions of equation (25) which satisfy conditions (26) following:

$$(26) \qquad R \equiv 0 \pmod{a_0},\ B \equiv 0 \pmod{ca_0b_0},\ C \equiv 0 \pmod{b_0}.$$

Let $U=u$, $R=r$, $A=\bar{a}$, $B=\bar{b}$, $F=\bar{f}$, $C=\bar{c}$ be an integral solution of (25). Then $U=ua_0^2b_0^2c$, $R=ra_0^2b_0^2c$, $A=\bar{a}a_0^2b_0c$, $B=\bar{b}a_0^2b_0c$, $F=\bar{f}b_0$, $C=\bar{c}b_0$ is a solution of (25) satisfying conditions (26). Therefore, equations (20) and (25) are *simultaneously* solvable (in integers, not all zero), or not solvable. The same is true also of equations (12) and (20), and, consequently, of equations (12) and (25).

Placing

$$Z = A^2 - abB^2, \quad W = F^2 - bcC^2,$$

* That is, a single form—in fact, not necessarily reduced—is employed from each class of quadratic forms of discriminant $4m$.

we may write equation (25) as

$$U^2 - acR^2 = ZW\ ;$$

hence, in view of Dickson's solution of the equation $x^2-my^2=zw$, it is seen that solving equation (25) in integers is equivalent to solving in integers

$$A^2 - abB^2 = s(eL_1^2 + 2fL_1Q_1 + gQ_1^2), \tag{27a}$$

$$F^2 - bcC^2 = s(eN_1^2 - 2fN_1T_1 + gT_1^2). \tag{27b}$$

After multiplying equations (27a), (27b) through by e, making the transformation

$$L = eL_1 + fQ_1,\ N = eN_1 - fT_1,\ Q = Q_1,\ T = T_1, \tag{28}$$

and replacing f^2-eg by its value ac, we have equations (27a), (27b) replaced by

$$eA^2 - eabB^2 - sL^2 + sacQ^2 = 0, \tag{29a}$$

$$eF^2 - ebcC^2 - sN^2 + sacT^2 = 0. \tag{29b}$$

All integral solutions of (27a), (27b) are obtained from all those integral solutions of (29a), (29b) such that the following conditions hold:

$$L \equiv fQ\ ;\ N \equiv -fT \pmod{e}. \tag{30}$$

Since equation (25) and equations (29a), (29b) are simultaneously solvable, or not solvable, it is now our purpose to obtain necessary and sufficient conditions for the solvability in integers of equations (29a), (29b).

6. **Meyer's solution of $ax^2+by^2+cz^2+du^2=0$.** A set of necessary and sufficient conditions for the solvability of the equation

$$ax^2 + by^2 + cz^2 + du^2 = 0 \tag{31}$$

in integers (not all zero), where a, b, c, d are all non-zero integers, has been obtained by A. Meyer.*

It is assumed that a, b, c, d are not only non-zero but also without square factors, and that they are such that no three have a common factor (greater than 1). The greatest common divisor of a and b is designated by (a, b). Let

$$a = (a,b)(a,c)(a,d)\alpha, \qquad b = (b,a)(b,c)(b,d)\beta,$$

$$c = (c,a)(c,b)(c,d)\gamma, \qquad d = (d,a)(d,b)(d,c)\delta.$$

---

* Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich, vol. 29 (1884), pp. 209–222. Cf. also P. Bachmann, *Zahlentheorie*, Part IV, *Die Arithmetik der Quadratischen Formen*, I, pp. 259–266.

Necessary conditions for the solvability of equation (31) in integers not all zero are the following:

I: a, b, c, d are not all of the same sign.

II: $-(a, c)(a, d)(b, c)(b, d)\gamma\delta$ is a quadratic residue of (a, b);
$-(a, b)(a, d)(c, b)(c, d)\beta\delta$ " " " " " (a, c);
$-(a, b)(a, c)(d, b)(d, c)\beta\gamma$ " " " " " (a, d);
$-(b, a)(b, d)(c, a)(c, d)\alpha\delta$ " " " " " (b, c);
$-(b, a)(b, c)(d, a)(d, c)\alpha\gamma$ " " " " " (b, d);
$-(c, a)(c, b)(d, a)(d, b)\alpha\beta$ " " " " " (c, d).

Necessary and sufficient conditions are: Conditions I and II above, and

III: either

(i) $abcd \equiv 2, 3, 5, 6, 7 \pmod 8$; or

(ii) $abcd \equiv 1$ and $a+b+c+d \equiv 0 \pmod 8$; or

(iii) $abcd \equiv 4 \pmod 8$, and, if a and b are even and c and d odd, either $\frac{1}{4}abcd \equiv 3, 5, 7 \pmod 8$, or $\frac{1}{4}abcd \equiv 1 \pmod 8$ and $a/2+b/2+c+d \equiv \{(cd)^2-1\}/2 \pmod 8$.

7. Necessary and sufficient conditions for the solvability of the diophantine equation. Necessary and sufficient conditions will here be derived for the solvability in integers of equations (29a), (29b), and hence for the solvability of the original diophantine equation (20).

Now, $e \neq 0$ since ac is not a perfect square; moreover, it is initially assumed that $s \neq 0$ since in the contrary case the problem becomes a trivial one. Where ϵ^2, σ^2 are the greatest integral squares contained in e, s, respectively, write

$$\begin{aligned} e &= e_1\epsilon^2, & s &= s_1\sigma^2, \\ e_1 &= (e_1, s_1)e_2, & s_1 &= (e_1, s_1)s_2, \\ e_2 &= (e_2, a)(e_2, b)e_3, & ab &= (e_2, a)(e_2, b)a_2b_2, \\ s_2 &= (s_2, a)(s_2, c)s_3, & ac &= (s_2, a)(s_2, c)a_3c_1. \end{aligned}$$

Noting that $(e_3, c_1) = (e_3, c) = (e_2, c)$ and $(b_2, s_3) = (b_2, s_2) = (b, s_2)$, we write

$$e_3 = (e_2, c)e_4, \quad c_1 = (e_2, c)c_2, \quad b_2 = (b, s_2)b_3, \quad s_3 = (b, s_2)s_4.$$

Moreover, place

$$\begin{aligned} A_2 &= \epsilon A, & B_3 &= \epsilon B, & L_2 &= \sigma L, \\ Q_2 &= \sigma Q, & B_4 &= (e_2, a)(e_2, b)B_3, & Q_3 &= (s_2, a)(s_2, c)Q_2, \\ & & L_2 &= (e_2, c)L_3, & A_2 &= (b, s_2)A_3. \end{aligned}$$

Equation (29a) then becomes

$$(e_2,a)(e_2,b)(b,s_2)e_4A_3^2 - e_4a_2b_3B_4^2 - (s_2,a)(s_2,c)(e_2,c)s_4L_3^2 + s_4a_3c_2Q_3^2 = 0. \tag{29a'}$$

Let $e_1, s_1, e_2, s_2, s_3, a_3, c_1$ be defined as above, and write

$$e_2 = (e_2,b)(e_2,c)e_5, \quad bc = (e_2,b)(e_2,c)b_2c_3,$$

where $c_3 = (s_2, c)c_2$. Moreover, since $(e_5, a_3) = (e_5, a) = (e_2, a_3) = (e_2, a)$ and since $(e_5, c_1) = (e_5, c) = 1$, write

$$e_5 = (e_2,a)e_4, \quad a_3 = (e_2,a)a_4, \quad b_2 = (b,s_2)b_3, \quad s_3 = (b,s_2)s_4,$$

where $a_2 = (s_2,a)a_4$. Also place

$$F_2 = \epsilon F, \quad C_3 = \epsilon C, \quad N_2 = \sigma N,$$
$$T_2 = \sigma T, \quad C_4 = (e_2,b)(e_2,c)C_3, \quad T_3 = (s_2,a)(s_2,c)T_2,$$
$$N_2 = (e_2,a)N_3, \quad F_2 = (b,s_2)F_3.$$

Equation (29b) then becomes

$$(e_2,b)(e_2,c)(b,s_2)e_4F_3^2 - e_4b_3c_3C_4^2 - (s_2,a)(s_2,c)(e_2,a)s_4N_3^2 + s_4a_4c_1T_3^2 = 0. \tag{29b'}$$

All integral solutions of equations (29a), (29b) are obtained by securing all integral solutions A_3, B_4, L_3, Q_3; F_3, C_4, N_3, T_3 of equations (29a'), (29b'), respectively, such that

$$\begin{aligned} &(b,s_2)A_3 \equiv 0 \pmod{\epsilon}, && B_4 \equiv 0 \pmod{(e_2,a)(e_2,b)\epsilon}, \\ &(e_2,c)L_3 \equiv 0 \pmod{\sigma}, && Q_3 \equiv 0 \pmod{(s_2,a)(s_2,c)\sigma}, \\ &(b,s_2)F_3 \equiv 0 \pmod{\epsilon}, && C_4 \equiv 0 \pmod{(e_2,b)(e_2,c)\epsilon}, \\ &(e_2,a)N_3 \equiv 0 \pmod{\sigma}, && T_3 \equiv 0 \pmod{(s_2,a)(s_2,c)\sigma}. \end{aligned} \tag{32}$$

Meyer's *preliminary conditions* are satisfied by both equations (29a'), (29b'). In the notation of Meyer, for equations (29a'), (29b'), respectively, we have the following two sets of four equations each:

$$\begin{aligned} (e_2,b)(b,s_2)e_4 &= |\,e_4\,|\,\alpha, \\ -e_4a_2b_3 &= |\,e_4\,|\,(s_2,a)\,|\,a_4\,|\,\beta, \\ -(s_2,c)(e_2,c)s_4 &= |\,s_4\,|\,\gamma, \\ s_4a_3c_2 &= (e_2,a)\,|\,a_4\,|\cdot|\,s_4\,|\,\delta\,; \\ (e_2,b)(b,s_2)e_4 &= |\,e_4\,|\,\alpha_1, \\ -e_4b_3c_3 &= |\,e_4\,|\,(s_2,c)c_2\beta_1, \\ -(s_2,a)(e_2,a)s_4 &= |\,s_4\,|\,\gamma_1, \\ s_4a_4c_1 &= (e_2,c)c_2\,|\,s_4\,|\,\delta_1. \end{aligned}$$

CONDITION* I. Either s and e are of the same sign; or s and e are of opposite sign, and either a is positive and b negative, or a and b are both positive.

CONDITION II.

(33a)	ac	is a quadratic residue of	$\lvert e_4 \rvert$.
(33b)	$-(s_2, c)e_3s_4a_4b_3$	" " " " "	(e_2, a).
(33c)	$-(s_2, a)e_5s_4b_3c_2$	" " " " "	(e_2, c).
(33d)	$-(e_2, b)e_4s_3a_4c_2$	" " " " "	$(s_2, a)\ (s_2, c)$.
(33e)	e_2s_2	" " " " "	$\lvert a_4 \rvert c_2$.
(33f)	ab	" " " " "	$\lvert s_4 \rvert$.
(33g)	bc	" " " " "	$\lvert s_4 \rvert$.

Conditions (33a)-(33e) are equivalent, respectively, to the following conditions (33a')-(33e'):

(33a') For every (positive) odd prime factor of $\lvert e_4 \rvert$, a and c are simultaneously quadratic residues or simultaneously quadratic non-residues of the chosen odd prime factor of $\lvert e_4 \rvert$.

(33b') For every odd prime factor of (e_2, a), exactly an even number (including zero) of $-(s_2, c)$, e_3, s_4, a_4, b_3 are quadratic non-residues of the chosen odd prime factor of (e_2, a).

(33c') For every odd prime factor of (e_2, c), exactly an even number (including zero) of $-(s_2, a)$, e_5, s_4, b_3, c_2 are quadratic non-residues of the chosen odd prime factor of (e_2, c).

(33d') For every odd prime factor of (s_2, ac), exactly an even number (including zero) of $-(e_2, b)$, e_4, s_3, a_4, c_2 are quadratic non-residues of the chosen odd prime factor of (s_2, ac).

(33e') For every odd prime factor of $\lvert a_4 \rvert c_2$, e_2 and s_2 are simultaneously quadratic residues or simultaneously quadratic non-residues of the chosen odd prime factor of $\lvert a_4 \rvert c_2$.

Let s_j $(j=6, 7, \cdots, \mu+5)$ be the distinct (positive) odd prime factors of $\lvert s_4 \rvert$, and let a_i $(i=5, 6, \cdots, \lambda+4)$, b_i $(i=5, 6, \cdots, \rho+4)$, and c_i $(i=5, 6, \cdots, \nu+4)$ be the distinct (positive) odd prime factors of a, b, c, respectively.

* We lay aside the trivial case in which one (or both) of equations (29a'), (29b') has merely the zero solution.

Conditions (33f), (33g) can be combined and replaced by the equivalent statement that, for every positive odd prime factor of $|s_4|$, each of a, b, c is simultaneously a quadratic residue or simultaneously a quadratic non-residue of the chosen odd prime factor of $|s_4|$. This condition will be given in another form. The condition (on $|s_4|$) that a, b, c be simultaneously quadratic residues of a chosen s_j, is treated first, under four separate cases. Similarly, the alternative condition, that a, b, c be simultaneously quadratic non-residues of a chosen s_j, is treated later.

Case 1A. $a=2a_5a_6\cdots a_{\lambda+4}$.

Now a is a quadratic residue of $|s_4|$ if and only if each of the Legendre symbols

$$\left(\frac{a}{s_6}\right),\left(\frac{a}{s_7}\right),\cdots,\left(\frac{a}{s_{\mu+5}}\right)$$

has the value $+1$. Now

$$\left(\frac{a}{s_j}\right)=\left(\frac{2}{s_j}\right)\left(\frac{a_5}{s_j}\right)\left(\frac{a_6}{s_j}\right)\cdots\left(\frac{a_{\lambda+4}}{s_j}\right)$$

$$=(-1)^{\zeta}\left(\frac{s_j}{a_5}\right)\left(\frac{s_j}{a_6}\right)\cdots\left(\frac{s_j}{a_{\lambda+4}}\right),$$

where $\zeta=(s_j^2-1)/8+\frac{1}{4}(s_j-1)\{\sum_{i=5}^{\lambda+4}a_i-\lambda\}$. Hence

(34a) either $s_j^2+2(s_j-1)\{\sum_{i=5}^{\lambda+4}a_i-\lambda\}\equiv 1 \pmod{16}$, and s_j is a quadratic non-residue of exactly an even number (including zero) of the prime factors of $a/2$; or $s_j^2+2(s_j-1)\{\sum_{i=5}^{\lambda+4}a_i-\lambda\}\equiv 9 \pmod{16}$, and s_j is a quadratic non-residue of exactly an odd number of the prime factors of $a/2$.

Case 1B. $a=-2a_5a_6\cdots a_{\lambda+4}$.

In this case the condition, designated by (34b), is the same as condition (34a) when λ of (34a) is replaced (except in the upper limit of summation) by $\lambda-2$ and a by $-a$.

Case 1C. $a=a_5a_6\cdots a_{\lambda+4}$.

(34c) Either $(s_j-1)\{\sum_{i=5}^{\lambda+4}a_i-\lambda\}\equiv 0 \pmod 8$, and s_j is a quadratic non-residue of exactly an even number (including zero) of the prime factors of a; or $(s_j-1)\{\sum_{i=5}^{\lambda+4}a_i-\lambda\}\equiv 4 \pmod 8$, and s_j is a quadratic non-residue of exactly an odd number of the prime factors of a.

Case 1D. $a=-a_5a_6\cdots a_{\lambda+4}$.

The condition in this case, designated by (34d), is the same as (34c) after λ has been replaced (except in the upper limit of summation) by $\lambda-2$ and a by $-a$.

The corresponding conditions for b, denoted by (35a), (35b), (35c), (35d), are obtained from conditions (34a), (34b), (34c), (34d), respectively, by replacing a by b, λ by ρ, a_i by b_i.

The corresponding conditions for c, denoted by (36a), (36c), are obtained from conditions (34a), (34c), respectively, by replacing a by c, λ by ν, a_i by c_i.

The alternative condition, that a, b, c are simultaneously quadratic non-residues of a chosen s_j, will now be given in more suitable form.

Case 2A. $a=2a_5a_6\cdots a_{\lambda+4}$.

(37a) Either $s_j^2+2(s_j-1)\{\sum_{i=5}^{\lambda+4}a_i-\lambda\}\equiv 1 \pmod{16}$, and s_j is a quadratic non-residue of exactly an odd number of the prime factors of $a/2$; or $s_j^2+2(s_j-1)\{\sum_{i=5}^{\lambda+4}a_i-\lambda\}\equiv 9 \pmod{16}$, and s_j is a quadratic non-residue of exactly an even number (including zero) of the prime factors of $a/2$.

Case 2B. $a=-2a_5a_6\cdots a_{\lambda+4}$.

In formulating the condition, designated by (37b), for this case, modify the statement of condition (34b) for Case 1B in the same way as the statement of condition (34a) is modified to give condition (37a) for Case 2A.

Case 2C. $a=a_5a_6\cdots a_{\lambda+4}$.

The condition here, designated by (37c), is an analogous modification of condition (34c) for Case 1C.

Case 2D. $a=-a_5a_6\cdots a_{\lambda+4}$.

Similarly, the condition, designated by (37d), for this case is again an analogous modification of condition (34d) for Case 1D.

The corresponding set of conditions for b, denoted by (38a), (38b), (38c), (38d), are obtained from conditions (37a), (37b), (37c), (37d), respectively, by replacing a by b, λ by ρ, a_i by b_i.

The corresponding set of conditions for c, denoted by (39a), (39c), are obtained from conditions (37a), (37c), respectively, by replacing a by c, λ by ν, a_i by c_i.

All the foregoing conditions,—namely, (34a), $\cdots$, (34d), (35a), $\cdots$, (35d), (36a), (36c), (37a), $\cdots$, (37d), (38a), $\cdots$, (38d), (39a), (39c)—are stated for any arbitrarily chosen s_j of the μ distinct positive odd prime factors of $|s_4|$; hence, it is to be understood that in Condition II $j=6, 7, \cdots, \mu+5$.

Define

$$h=(e_2,a)(e_2,b)(b,s_2)e_4-e_4a_2b_3-(s_2,a)(s_2,c)(e_2,c)s_4+s_4a_3c_2,$$

$$k=\tfrac{1}{2}\{(e_2,a)(e_2,b)(b,s_2)e_4-e_4a_2b_3\}-(s_2,a)(s_2,c)(e_2,c)s_4+s_4a_3c_2,$$

$$p=(e_2,b)(e_2,c)(b,s_2)e_4-e_4b_3c_3-(s_2,a)(s_2,c)(e_2,a)s_4+s_4a_4c_1,$$

$$q=\tfrac{1}{2}\{(e_2,b)(e_2,c)(b,s_2)e_4-e_4b_3c_3\}-(s_2,a)(s_2,c)(e_2,a)s_4+s_4a_4c_1.$$

CONDITION IIIA. Either

(i) $e_4^2 s_4^2 a^2bc \equiv 2, 3, 5, 6, 7 \pmod 8$; or

(ii) $e_4^2 s_4^2 a^2bc \equiv 1$ and $h \equiv 0 \pmod 8$; or

(iii) $e_4^2 s_4^2 a^2bc \equiv 4 \pmod 8$, and, if e_4 is even, either $\frac{1}{4}e_4^2 s_4^2 a^2bc \equiv 3, 5, 7 \pmod 8$, or $\frac{1}{4}e_4^2 s_4^2 a^2bc \equiv 1 \pmod 8$ and $k \equiv \frac{1}{2}\{(acs_4^2)^2 - 1\} \pmod 8$.

CONDITION IIIB. Either

(i) $e_4^2 s_4^2 abc^2 \equiv 2, 3, 5, 6, 7 \pmod 8$; or

(ii) $e_4^2 s_4^2 abc^2 \equiv 1$ and $p \equiv 0 \pmod 8$; or

(iii) $e_4^2 s_4^2 abc^2 \equiv 4 \pmod 8$, and, if e_4 is even, either $\frac{1}{4}e_4^2 s_4^2 abc^2 \equiv 3, 5, 7 \pmod 8$, or $\frac{1}{4}e_4^2 s_4^2 abc^2 \equiv 1 \pmod 8$ and $q \equiv \frac{1}{2}\{(acs_4^2)^2 - 1\}$.

The results may now be summarized. Necessary and sufficient conditions for the solvability in integers of equations (29a'), (29b'), when it is assumed that $s \neq 0$, are given as follows:

Condition I and conditions (33a)-(33e), or the equivalent conditions (33a')-(33e'), must hold; and, according to the character of a, b, c, for every odd prime factor of $|s_4|$ *either* one condition must hold from each of the three sets of conditions

$$(34a), \cdots, (34d); \quad (35a), \cdots, (35d); \quad (36a), (36c),$$

or one condition must hold from each of the three sets of conditions

$$(37a), \cdots, (37d); \quad (38a), \cdots, (38d); \quad (39a), (39c).$$

Conditions IIIA, IIIB must hold.

There are combinations among these last conditions (IIIA, IIIB) which are not consistent.

There are twenty-five possible ways of combining a condition of IIIA (i) for equation (29a') with a condition of IIIB (i) for equation (29b'); but it is readily seen that the following twelve combinations are inconsistent:

$$e_4^2 s_4^2 a^2bc \equiv 2,6, \quad e_4^2 s_4^2 abc^2 \equiv 3,5,7 \pmod 8;$$

$$e_4^2 s_4^2 a^2bc \equiv 3,5,7, \quad e_4^2 s_4^2 abc^2 \equiv 2,6 \pmod 8.$$

By taking $e = s = 1$, we find that the remaining thirteen pairs of congruences can be satisfied.

Of the five ways of combining a condition of IIIA (i) with the condition IIIB (ii), it is seen that three give consistent combinations and the remaining two give inconsistent combinations.

Of the twenty-five ways of combining a condition of IIIA (i) with a condi-

tion of IIIB (iii), it is seen that only two give consistent combinations: namely,

$$e_4^2 s_4^2 a^2 bc \equiv 2,6, \quad e_4^2 s_4^2 abc^2 \equiv 4 \pmod 8,$$

where e_4 is odd. These two pairs of congruences can be satisfied by $e=s=1$, $a=1$, $b=17$, $c=2$; $e=s=1$, $a=1$, $b=3$, $c=2$, respectively.

Of the five ways of combining the condition IIIA (ii) with a condition of IIIB (i), three give consistent combinations and two give inconsistent combinations; the combination of condition IIIA (ii) with condition IIIB (ii) is a consistent one; of the five ways of combining the condition IIIA (ii) with a condition of IIIB (iii), all five give inconsistent combinations.

Of the twenty-five ways of combining a condition of IIIA (iii) with a condition of IIIB (i), it is seen that only two give consistent combinations: namely,

$$e_4^2 s_4^2 a^2 bc \equiv 4, \quad e_4^2 s_4^2 abc^2 \equiv 2,6 \pmod 8,$$

where e_4 is odd. These two pairs of congruences can be satisfied by $e=s=1$, $a=2$, $b=17$, $c=1$; $e=s=1$, $a=2$, $b=3$, $c=1$, respectively. All five ways of combining a condition of IIIA (iii) with condition IIIB (ii) give inconsistent combinations.

Of the twenty-five ways of combining a condition of IIIA (iii) with a condition of IIIB (iii), it is found that fifteen give consistent combinations and ten give inconsistent combinations. Here it is somewhat more difficult to determine whether or not a combination is consistent. The following fifteen combinations are the only ones which can be satisfied.

The combination

$$e_4^2 s_4^2 a^2 bc \equiv 4, \quad e_4^2 s_4^2 abc^2 \equiv 4 \pmod 8,$$

where e_4 is odd, can be satisfied by $e=1$, $s=2$, $a=7$, $b=5$, $c=1$.

The combination of

$$e_4^2 s_4^2 a^2 bc \equiv 4, \quad \tfrac{1}{4} e_4^2 s_4^2 a^2 bc \equiv x \pmod 8$$

with

$$e_4^2 s_4^2 abc^2 \equiv 4, \quad \tfrac{1}{4} e_4^2 s_4^2 abc^2 \equiv y \pmod 8,$$

where e_4 is even, is satisfied

by $e=2$, $s=1$, $a=7$, $b=5$, $c=23$, when $x=y=3$;
by $e=2$, $s=1$, $a=7$, $b=3$, $c=1$, when $x=3$, $y=5$;
by $e=14$, $s=a=1$, $b=7$, $c=5$, when $x=3$, $y=7$;
by $e=2$, $s=a=1$, $b=3$, $c=7$, when $x=5$, $y=3$;
by $e=2$, $s=a=1$, $b=5$, $c=17$, when $x=5$, $y=5$;

by $e=14$, $s=a=1$, $b=15$, $c=11$, when $x=5$, $y=7$;
by $e=14$, $s=1$, $a=5$, $b=7$, $c=1$, when $x=7$, $y=3$;
by $e=2$, $s=-1$, $a=11$, $b=7$, $c=1$, when $x=7$, $y=5$;
by $e=2$, $s=a=1$, $b=7$, $c=17$, when $x=7$, $y=7$.

The preceding combination with $y=1$, together with

$$q \equiv \tfrac{1}{2}\{(acs_4^2)^2 - 1\} \pmod 8,$$

is satisfied by $e=14$, $s=a=1$, $b=17$, $c=11$, when $x=3$; by $e=2$, $s=a=1$, $b=17$, $c=7$, when $x=7$. Moreover, the preceding combination with $x=1$, together with

$$k \equiv \tfrac{1}{2}\{(acs_4^2)^2 - 1\} \pmod 8$$

instead of

$$q \equiv \tfrac{1}{2}\{(acs_4^2)^2 - 1\} \pmod 8,$$

is satisfied by $e=14$, $s=1$, $a=11$, $b=17$, $c=1$, when $y=3$; by $e=2$, $s=1$, $a=7$, $b=17$, $c=1$, when $y=7$. The preceding combination with $x=y=1$, together with

$$k \equiv \tfrac{1}{2}\{(acs_4^2)^2 - 1\} \pmod 8$$

and

$$q \equiv \tfrac{1}{2}\{(acs_4^2)^2 - 1\} \pmod 8,$$

is satisfied by $e=2$, $s=1$, $a=-1$, $b=15$, $c=7$.

Since e_4 cannot at the same time be both odd and even, eight combinations are immediately excluded as inconsistent. As is later proved in Theorem 4 of §8, the remaining two ways of combining a condition of IIIA (iii) with a condition of IIIB (iii) give inconsistent combinations.

Finally, out of the 121 combinations of a condition of IIIA for equation (29a′) with a condition of IIIB for equation (29b′), there are exactly thirty-nine consistent combinations and eighty-two inconsistent combinations.

8. **Incompatibility of certain congruences.** It will here be shown, in Theorem 4, that, as stated in the preceding section, certain combinations of a condition from IIIA (iii) with a condition from IIIB (iii) are inconsistent. Theorems 2 and 3 are lemmas for Theorem 4. Under the (additional) restriction that e_2s_2 is relatively prime to abc, Theorems 5, 6, and 7 can be proved. In this case, there are exactly thirty-seven consistent combinations of a condition of IIIA for equation (29a′) with a condition of IIIB for equation (29b′).

Throughout the present section, let e, e_i $(i=1, 2, \cdots, 5)$, s, s_i $(i=1, 2, \cdots, 4)$, a, b, c, p, and q be integers defined as in §7.

THEOREM 2. *If* $e_4=2e_7$, $a\equiv b \pmod 8$, *and* $c\equiv 5a \pmod 8$, *then* $q\equiv 0 \pmod 8$.

By hypothesis,

$$a \equiv (e_2,b)(b,s_2)b_3 \pmod 8,$$
$$c \equiv (e_2,c)(s_2,c)c_2 \equiv 5a \pmod 8.$$

Then

$$a \equiv (e_2,b)(b,s_2)b_3 \equiv 5(e_2,c)(s_2,c)c_2 \pmod 8.$$

Since the square of an odd integer is congruent to 1 modulo 8, on multiplying both sides of the latter congruence by $(e_2, c)e_7b_3$ we obtain

$$(e_2,b)(e_2,c)(b,s_2)e_7 \equiv 5(s_2,c)c_2e_7b_3 \pmod 8$$
$$\equiv 5e_7b_3c_3 \pmod 8.$$

Similarly, since $ac \equiv 5 \pmod 8$,

$$(s_2,a)(s_2,c)(e_2,a)(e_2,c)a_4c_2 \equiv 5 \pmod 8;$$

moreover, multiplying both sides of this congruence by $(e_2, c)s_4a_4c_2$, we obtain

$$(s_2,a)(s_2,c)(e_2,a)s_4 \equiv 5(e_2,c)s_4a_4c_2 \pmod 8$$
$$\equiv 5s_4a_4c_1 \pmod 8.$$

Hence,

$$(e_2,b)(e_2,c)(b,s_2)e_7 - (s_2,a)(s_2,c)(e_2,a)s_4 \equiv 5(e_7b_3c_3 - s_4a_4c_1) \pmod 8;$$

and, since e_4 is relatively prime to a, b, c and e_7 is odd,

$$q \equiv 4(e_7b_3c_3 - s_4a_4c_1) \pmod 8$$
$$\equiv 0 \pmod 8.$$

THEOREM 3. *If* $e_4 = 2e_7$, $b \equiv c \pmod 8$, *and* $a \equiv 5b \pmod 8$, *then* $k \equiv 0 \pmod 8$.

The proof of this theorem is similar to that of the preceding theorem.

THEOREM 4. *If* $e_4 = 2e_7$, *the set of congruences*

$$e_4^2s_4^2a^2bc \equiv 4 \pmod 8, \qquad e_4^2s_4^2abc^2 \equiv 4 \pmod 8,$$
$$\tfrac{1}{4}e_4^2s_4^2a^2bc \equiv x \pmod 8, \qquad \tfrac{1}{4}e_4^2s_4^2abc^2 \equiv y \pmod 8$$

is inconsistent with the congruence $q \equiv \frac{1}{2}\{(acs_4^2)^2 - 1\} \pmod 8$ *when* $x = 5, y = 1$, *and is inconsistent with the congruence* $k \equiv \frac{1}{2}\{(acs_4^2)^2 - 1\} \pmod 8$ *when* $x = 1$, $y = 5$.

Since the square of an odd integer is congruent to 1 modulo 8, it is seen that, when $x = 5$, $y = 1$,

$$bc \equiv 5, \qquad ab \equiv 1 \pmod 8.$$

Therefore

$$a \equiv b, \qquad c \equiv 5b \equiv 5a, \qquad \tfrac{1}{2}\{(acs_4^2)^2 - 1\} \equiv 4 \pmod 8.$$

Then

$$q \equiv \tfrac{1}{2}\{(acs_4^2)^2 - 1\} \equiv 4 \pmod 8.$$

By Theorem 2 it is seen that $q \equiv 0 \pmod 8$. Hence Theorem 4 is proved when $x=5$, $y=1$.

If $x=1$, $y=5$,

$$b \equiv c, \qquad a \equiv 5b, \qquad \tfrac{1}{2}\{(acs_4^2)^2 - 1\} \equiv 4 \pmod 8.$$

Then

$$k \equiv \tfrac{1}{2}\{(acs_4^2)^2 - 1\} \equiv 4 \pmod 8.$$

By Theorem 3 it is seen that $k \equiv 0 \pmod 8$. Thus Theorem 4 is proved when $x=1$, $y=5$.

The following theorems are of interest when it is assumed that e_2s_2 is relatively prime to abc.

THEOREM 5. *If $e_4 = 2e_7$ and if e_2s_2 is relatively prime to abc, then a necessary condition that each of e, e_i $(i=1, \cdots, 5)$, s, s_i $(i=1, \cdots, 4)$, a, b, c, as defined in §7, satisfy conditions* (23), (33a), (33e), (33f), (33g), *is that*

$$\zeta = \frac{a^2+c^2-2}{8} + \frac{|s_2|-1}{2}\cdot\frac{a-1}{2} + \frac{c-1}{2}\cdot\frac{s_2-1}{2} + \frac{e_7-1}{2}\cdot\frac{c-1}{2} + \frac{a-1}{2}\cdot\frac{|e_7|-1}{2} + \xi + \eta$$

be even, when we define

$$\xi = 0 \text{ if } s \text{ is positive}, \quad = \{|a|-1\}/2 \text{ if } s \text{ is negative};$$
$$\eta = 0 \text{ if } e \text{ is positive}, \quad = \{|a|-1\}/2 \text{ if } e \text{ is negative}.$$

THEOREM 6. *If the integers e, e_i $(i=1, \cdots, 5)$, s, s_i $(i=1, \cdots, 4)$, a, b, c, as defined in §7, satisfy conditions* (23), (33a), (33e), (33f), (33g), *and condition* I *of §7, and if, when $e_4 = 2e_7$, e_2s_2 is relatively prime to abc, then the congruences*

$$c \equiv 5a \pmod 8, \quad a^2 + c^2 \equiv 10 \pmod{16}$$

are inconsistent.

THEOREM 7. *If e, e_i $(i=1, 2, 3, 5)$, $e_4 = 2e_7$, s, s_i $(i=1, \cdots, 4)$, a, b, c have the same significance and satisfy the same restrictions as stated in Theorem* 6, *the set of congruences*

$$e_i^2 s_i^2 a^2 bc \equiv 4 \pmod 8, \qquad e_i^2 s_i^2 abc^2 \equiv 4 \pmod 8,$$
$$\tfrac{1}{4}e_i^2 s_i^2 a^2 bc \equiv h \pmod 8, \qquad \tfrac{1}{4}e_i^2 s_i^2 abc^2 \equiv k \pmod 8$$

is inconsistent when $h=3$ and $k=7$, $h=7$ and $k=3$, $h=5$ and $k=1$, or $h=1$ and $k=5$.

9. **Numerical examples.** Solutions* of equation (25) will now be given for a few values of n and p:

$$U^2 - acR^2 = (A^2 - abB^2)(F^2 - bcC^2), \tag{25}$$

where

$$a_1 = 2n - p = aca_0^2, \quad b_1 = -2n - p = bcb_0^2.$$

	n	p	a	b	c	U	R	A	B	F	C
(i)	-2	-1	-3	5	1	4	4	1	1	3	1
(ii)	1	-5	7	3	1	14	2	-7	1	3	1
(iii)	-4	-3	-5	11	1	10	6	1	1	4	1
(iv)	-4	-3	-5	11	1	0	80	-5	1	24	4
(v)	-2	1	-5	3	1	2	2	3	1	7	4
(vi)	-3	1	-7	5	1	12	60	2	-2	14	2
(vii)	1	-31	33	29	1	0	$30B$	$-33B$	arb. int.	6	3
(viii)	-4	3	-11	5	1	0	32	11	1	12	4
(ix)	-105	-294	3	2	7	315	35	30	5	28	7

Raymond J. Garver,† using different methods and different notation, obtained criteria for the solvability in integers of equation (25) when

$$U = 0, \quad ca_0b_0A = (p - 2)B, \quad \text{and} \quad cb_0R \equiv 0 \pmod{2B}. \tag{40}$$

By imposing further restrictions on p and n, Garver treated the norm conditions for a division algebra and set up examples of division algebras of order sixteen satisfying all his conditions. All conditions (40) are satisfied by examples (iv) and (vii) above. In examples (ii) and (vi) all except the first of conditions (40) are satisfied. In example (viii) only the first and the third of conditions (40) are satisfied. In examples (i), (iii), (v), and (ix) (in which $a_0=2$, $b_0=6$), only the last of conditions (40) is satisfied. On taking $e=s=1$ we see that example (iv) satisfies all our previous conditions and, without modification, gives rise to a solution of equations (25) and (20), and of the original equation (12).

---

* When one solution of equation (25) is known for a given n and a given p, an infinite number of solutions are known; for, if $U=\lambda$, $R=\mu$, $A=\nu$, $B=\rho$, $F=\sigma$, $C=\tau$ is an integral solution, then also is $U=r_1r_2\lambda$, $R=r_1r_2\mu$, $A=r_1\nu$, $B=r_1\rho$, $F=r_2\sigma$, $C=r_2\tau$, where r_1 and r_2 are arbitrary integers.

† R. J. Garver, (I) *On Tschirnhausen Transformations*, (II) *Division Algebras of Order Sixteen*, Dissertation, Chicago, 1926.

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.