ON CUBIC CONGRUENCES*

BY H. R. BRAHANA

1. *Introduction.* In the consideration of metabelian groups G of order p^{n+3} which contain a given abelian group H of order p^n and type 1, 1, $\cdots$, there enters an irreducible cubic congruence

$$x^3 + \gamma x^2 - \alpha x + \beta \equiv 0, \pmod{p}. \tag{1}$$

It is necessary to determine how many congruences (1) are distinct under certain transformations on the generators of G.†

Let the generators of H be $s_1, s_2, \cdots, s_n$, and let U_1, U_2, U_3 be three operators of order p from the group of isomorphisms of H. Let the operators $s_1, \cdots, U_3$ be permutable except for the relations

$$\begin{aligned} &U_1^{-1}s_1U_1 = s_1s_3,\ U_2^{-1}s_1U_2 = s_1s_5,\ U_3^{-1}s_1U_3 = s_1s_3^{\alpha}s_4^{\beta}s_5^{\gamma}, \\ &U_1^{-1}s_2U_1 = s_2s_4,\ U_2^{-1}s_2U_2 = s_2s_3,\ U_3^{-1}s_2U_3 = s_2s_5. \end{aligned} \tag{2}$$

Such operators U_1, U_2, U_3 obviously exist. The condition that $\{U_1, U_2, U_3\}$ contain no operator permutable with any operator, except identity, of $\{s_1, s_2\}$ is readily seen to be that (1) be irreducible, (mod p).

The group $G = \{H, U_1, U_2, U_3\}$ is a subgroup of the holomorph of H. For the sake of simplicity in the subsequent computations we shall show that generators of G may be chosen so that $\gamma = 0$, provided $p > 3$. Let $s_1' = s_1s_2^{-1}$, $U_2' = U_1^{-1}U_2$, and $U_3' = U_1U_2^{-2}U_3$. The operators $s_1', s_2, \cdots, s_n, U_1, U_2', U_3'$ generate G, and satisfy (2) with new numbers α', β', γ', where

$$\begin{aligned} \alpha' &= 2\gamma + \alpha - 3, \\ \beta' &= \alpha + \beta + \gamma - 1, \\ \gamma' &= \gamma - 3. \end{aligned}$$

Hence by repeating this transformation we may reduce γ to

* Presented to the Society, October 28, 1933.

† See my paper, *On the metabelian groups which contain a given group H as a maximal invariant abelian subgroup.* This paper has been offered to the American Journal of Mathematics.

zero provided $p \neq 3$. We may therefore assume that γ in (2) is zero. The congruence (1) then becomes

$$x^3 - \alpha x + \beta \equiv 0, \pmod{p}. \tag{3}$$

There are many pairs α, β such that (3) is irreducible and each such pair determines a group of the type in question. It is necessary to determine how many of these groups are distinct. We shall show that there is just one such group by proving the following theorem.

THEOREM 1. *In any given group whose generators satisfy* (2) *with* $\gamma = 0$ *and no relations which are not consequences of* (2), *generators may be chosen to satisfy* (2) *with* $\gamma' = 0$ *and* α' *and* β' *the coefficients of an arbitrary irreducible cubic of the form* (3).

We consider the following choice of generators of G, not the most general on account of the complexity of the required computations. We take

$$\begin{aligned} s_1' &= s_1 s_2^a, \qquad s_2' = s_1^b s_2^c, \\ U_1' &= U_1, \qquad U_2' = U_1^k U_2^l U_3^m \qquad U_3' = U_1^{k_1} U_2^{l_1} U_3^{m_1}. \end{aligned} \tag{4}$$

We require $a, \cdots, m_1$ to be such that the new generators satisfy (2), with $\gamma = 0$. The transformation misses complete generality only because of U_1'. The requirement that the commutator of U_2' and s_2' be the same as that of U_1' and s_1' gives

$$\begin{aligned} bk + cl + \alpha bm &\equiv 1, \\ ck \qquad + \beta bm &\equiv a, \\ bl + \quad cm &\equiv 0, \pmod{p}. \end{aligned}$$

Solving this system for k, l, and m, we have

$$\begin{aligned} k &= [a\rho + \beta b^2(c - ab)]/(c\rho), \\ l &= c(c - ab)/\rho, \\ m &= -b(c - ab)/\rho, \end{aligned} \tag{5}$$

where $\rho = c^3 - \alpha b^2 c + \beta b^3$, which cannot be zero because (3) is irreducible. The operator $U_2' = U_1^k U_2^l U_3^m$ is not a power of U_1' because s_1' and s_2' are independent, which makes $c - ab$ different from zero. We may now compute the exponents of $s_5' = s_3^r s_4^s s_5^t$, the commutator of U_2' and s_1'. They are

$$r = \{a\rho + (c - ab)[\beta b^2 + ac^2 - \alpha bc]\}/(c\rho),$$
$$s = [a^2\rho - \beta b(c - ab)^2]/(c\rho),$$
$$t = (c - ab)^2/\rho.$$

Computing the commutator of U_3' and s_2' and requiring it to be s_5', we get the system

$$\begin{aligned} bk_1 + cl_1 + \alpha bm_1 &\equiv r, \\ ck_1 \qquad + \beta bm_1 &\equiv s, \\ bl_1 + \quad cm_1 &\equiv t, \pmod{p}. \end{aligned}$$

We avoid the solution of this system by taking account of the fact that if the commutator of U_3' and s_1' is expressible in terms of the commutators of U_1' and s_1' and s_2', as it must be if the resulting cubic takes the form (3), it must be independent of s_5, and hence

$$l_1 + am_1 \equiv 0, \pmod{p}.$$

Using this congruence with the last two of the system above, we get

$$\begin{aligned} k_1 &= [a^2\rho - \beta b(c - ab)(2c - ab)]/(c^2\rho), \\ l_1 &= -a(c - ab)/\rho, \\ m_1 &= (c - ab)/\rho. \end{aligned} \tag{6}$$

The first congruence of the system above then takes the form of a condition on a, b, and c. It becomes

$$3ac^2 - \alpha ab^2 + 3\beta b^2 - 2\alpha bc \equiv 0, \pmod{p}. \tag{7}$$

Hence if a, b, and c are chosen to satisfy (7), k, l, and m are determined by (5) and k_1, l_1, and m_1 by (6) so that the new generators of G satisfy (2) and the corresponding cubic, which must still be irreducible, is in the form (3). The condition that U_1', U_2', and U_3' be independent is that the determinant of the exponents of U_1, U_2, and U_3 in the expressions for them be not zero. This determinant is $(c-ab)^3/\rho^2$ and the condition is satisfied.

If we denote the transformed cubic by

$$x^3 - \alpha' x + \beta' \equiv 0, \tag{8}$$

and examine the exponents of s_3 and s_4 in the commutator of U_3' and s_1', we obtain the following congruences:

$$\begin{aligned} k_1 + al_1 + \alpha m_1 &\equiv \alpha' + b\beta', \\ ak_1 \qquad + \beta m_1 &\equiv a\alpha' + c\beta', \end{aligned}$$

which we may solve for α' and β'. The result is

$$\begin{aligned} \alpha' &= (2ab - 3\beta b + \alpha c - 3a^2c)/\rho, \\ \beta' &= (a^3 - \alpha a + \beta)/\rho. \end{aligned} \tag{9}$$

We next take the irreducible congruence (3) and consider the effect of a linear fractional transformation on the variable x. Let this transformation be

$$x' = (-x + a)/(bx - c). \tag{10}$$

If the coefficients a, b, and c are residues (mod p) and if they satisfy (7), the transformation changes (3) into

$$x'^3 - \alpha' x' + \beta' \equiv 0,$$

where β' and α' are given by (9). In fact the condition (7) is the condition that the coefficient of x'^2 in the transformed congruence be zero. Hence the transformation (10) on the variable x is the same as the transformation (4) on the generators of G. We may then study all transformations (4) by studying transformations (10).

Now the irreducible congruence (3) defines a Galois field $GF(p^3)$ in which the congruence has three roots. Any other irreducible cubic congruence, for example (8), defines a $GF(p^3)$ simply isomorphic with the first. The congruence (8) is therefore reducible in the $GF(p^3)$ defined by (3). If X is one of the roots of (8), then the three roots are*

$$X,\ X^p, \text{ and } X^{p^2}.$$

Any mark X in the $GF(p^3)$ may be written

$$\gamma x^2 + \delta x + \epsilon, \tag{11}$$

where x is a root of (3) and γ, δ, and ϵ are rational, that is, in the $GF(p)$. Then in order to prove our theorem we need only to show that rational numbers a, b, and c can be found such that (10)

* Dickson, *Linear Groups*, p. 20.

transforms a root of (3) into (11). Setting (11) equal to the right-hand side of (10), we obtain

$$\begin{aligned} a &= (\beta\gamma^2 + \delta\epsilon)/(\alpha\gamma^2 - \delta^2 + \gamma\epsilon), \\ b &= \gamma/(\alpha\gamma^2 - \delta^2 + \gamma\epsilon), \\ c &= \delta/(\alpha\gamma^2 - \delta^2 + \gamma\epsilon). \end{aligned} \tag{12}$$

This shows that (4) may be chosen so that (3) is transformed into (8), where α' and β' are any numbers such that (8) is irreducible, and hence completes the proof of Theorem 1.

2. *A Special Transformation.* Much interesting information about irreducible cubics is obtained by considering special transformations of the form (4). Let $s_1' = s_1^k$, $U_2' = U_2^k$, $U_3' = U_3^{k^2}$.* This leaves G invariant and the transform of the congruence (3) corresponding to the generators s_1', s_2, U_1, U_2', U_3' is

$$x^3 - \alpha k^2 x + \beta k^3 \equiv 0. \tag{13}$$

By means of this transformation we are able to classify all cubic congruences of the form (3) in three types: those for which (a) $\alpha = 0$; (b) $\alpha = 1$; and (c) α is a particular number not a square, (mod p).

Let us consider the possibility of transforming (3) into an irreducible congruence of the same form except that $\alpha = 0$. By means of (7) we may change the value of α' in (9) to

$$\alpha' = (c - ab)[\alpha(c + ab) - 3\beta b]/(c\rho). \tag{14}$$

Hence if α' is to be zero, then a, b, and c must be chosen so that

$$[\alpha(c + ab) - 3\beta b] \equiv 0.$$

Using this with (7) to eliminate b we obtain

$$c(3\alpha a^2 - 9\beta a + \alpha^2) \equiv 0.$$

If $c = 0$ and (7) is satisfied, we must have $a = 3\beta/\alpha$ and excepting the case where $\alpha = 2$ these values require b to be zero if α' is to be zero. Therefore, in general, we must have

$$3\alpha a^2 - 9\beta a + \alpha^2 \equiv 0.$$

Since a must be rational it follows that

* This is a special case of a transformation which only *appears* to be more general than (4).

$$81\beta^2 - 12\alpha^3 \tag{15}$$

is a square. Conversely if (15) is a square, a, b, and c may be found such that α' is zero, in which case the irreducible congruence takes the form

$$x^3 + \beta' \equiv 0. \tag{16}$$

Irreducible congruences of the form (16) exist when p is of the form $6k+1$ and do not exist when p is of the form $6k-1$. The irreducibility of the congruence (3) says that the group $\{s_1, s_2\}$ contains no operator permutable with any operator of $\{U_1, U_2, U_3\}$, a property independent of the choice of generators of the two groups. Hence the irreducibility of (3) implies the irreducibility of (16). Therefore (15) is a square when p is of the form $6k+1$ and is not a square when p is of the form $6k-1$. The quantity (15) is the product of -3 and the discriminant of (3). Now -3 is or is not a square according as p is of the form $6k+1$ or $6k-1$, and consequently the discriminant of an irreducible cubic is always a square.*

3. *Method of Writing all Irreducible Cubics of the Form* (3). The following considerations give an easy method of writing all the irreducible cubics of the form (3) when p is of the form $6k+1$. Start with any irreducible cubic in the form (16). Since $\alpha=0$, the transformation (4) will have its coefficients subjected to (7) changed to

$$ac^2 + \beta b^2 \equiv 0.$$

The first relation of (9), or (14), becomes

$$\alpha' = 3ac(c - ab)/(b\rho).$$

Setting $\alpha'=1$ and combining these two relations to eliminate β, we have

$$c(c - ab)(3a - bc) \equiv 0.$$

Therefore if $\alpha'=1$, we have $3a=bc$ and we may solve for a and b in terms of c. This gives

$$a = -c^4/(9\beta), \quad b = -c^3/(3\beta). \tag{17}$$

The determinant $c-ab$ could be zero only if $c(27\beta^2-c^6)$ were zero which is impossible since β is not a cube. Hence c may be

* See Dickson, *Criteria for the irreducibility of functions in a finite field*, this Bulletin, vol. 13 (1906–7), p. 1.

chosen at random (different from zero) and a and b may then be determined so that $\alpha' = 1$. The value of β' is then

$$\beta' = (a^3 + \beta)/\rho = (27\beta^2 + c^6)/(27\beta c^3). \tag{18}$$

The condition that two values of β' given by (18) for two numbers c and c' be the same is

$$27\beta^2(c'^3 - c^3) = c'^3c^3(c'^3 - c^3).$$

Again recalling that β is not a cube, we see that this requires that $c^3 = c'^3$. Therefore, by taking $(p-1)/3$ numbers c whose cubes are distinct, we obtain $(p-1)/3$ distinct numbers β', each of which determines an irreducible cubic of the form $x^3 - x + \beta' \equiv 0$. By means of this transformation and the one which changes (3) into (13), we may obtain all the irreducible cubics (3) for which α is a square from any irreducible cubic of the form (16).

If we let α' be k, instead of 1 as above, and carry through a computation similar to the above, we obtain

$$\beta' = (27\beta^2 + c^6k^3)/(27\beta c^3). \tag{19}$$

Hence we have the following theorem.

THEOREM 2. *The irreducible cubics of the form* (3), *when* p *is of the form* $6k+1$, *are*

$$x^3 - \alpha x + (27\beta^2 + c^6\alpha^3)/(27\beta c^3) \equiv 0,$$

where $x^3 + \beta \equiv 0$ *is any irreducible binomial cubic and* c *and* α *are any numbers from* 1 *to* $p-1$.

This theorem gives a straightforward method of writing without duplications all the irreducible cubics of the form (3) when p is of the form $6k+1$ and a non-cube β is known. In the case of p of the form $6k-1$ we have not been able to obtain a like result. There is, however, one interesting formula which we shall give.

We have given an arbitrary irreducible cubic (3) and we apply the transformation (4) whose exponents are subject to the condition (7). Since a, b, and c are rational, (7) imposes a restriction on a. Also, (7) determines the ratio of c and b in terms of a. If we let $a = 3\beta/\alpha$, we find

$$\alpha' = \frac{81\beta^2}{b^2(4\alpha^3 - 27\beta^2)}. \tag{20}$$

Since the discriminant of the cubic is a square, b can be chosen so that $\alpha' = 1$. The corresponding value of β' is

$$\beta' = \frac{-729\beta^4}{\alpha^3 b^3(4\alpha^3 - 27\beta^2)}.$$

The ratio of β' to α' is $-9\beta^2/(\alpha^3 b)$. If we take α in (3) to be 1 and determine b in (20) so that α' is 1, we have

$$\beta' = -\beta(4 - 27\beta^2)^{1/2}.$$

We have therefore the following theorem.

THEOREM 3. *If p is of the form $6k-1$ and $x^3-x+\beta\equiv 0$ is irreducible, then $x^3-x+\beta(4-27\beta^2)^{1/2}\equiv 0$ is also irreducible.*

If β in the above theorem is not $1/3$, the second cubic is distinct from the first. By repeated applications of the theorem we obtain a set of cubics of the form $x^3-x+\beta\equiv 0$, but in general we do not obtain all of them.

THE UNIVERSITY OF ILLINOIS

THE ALGEBRA OF SELF-ADJOINT BOUNDARY-VALUE PROBLEMS*

BY V. V. LATSHAW

1. *Introduction.* By algebraic processes, D. Jackson† obtained in matrix form the condition for self-adjointness of differential systems of any order. The purpose of this paper is to develop by means of the matrix criterion the explicit conditions for self-adjointness of the boundary conditions associated with self-adjoint and anti-self-adjoint differential equations.

2. *Even-Order Systems.* Let $L(u)$ denote the self-adjoint differential expression‡

$$(1) \qquad L(u) \equiv (p_m u^{(m)})^{(m)} + (p_{m-1}u^{(m-1)})^{(m-1)} + \cdots + p_0 u,$$

where m is any positive integer, $p_i(x)$ is of class C^i, and $p_m(x) \neq 0$ in the interval $(a \leqq x \leqq b)$. Along with

* Presented to the Society, October 31, 1931.

† D. Jackson, Transactions of this Society, vol. 17 (1916), pp. 418–424.

‡ Bounitzky, Journal de Mathématiques, (6), vol. 5 (1909), p. 107.