THE LINEAR CONGRUENCE GROUP MODULO \( n \)

F. A. LEWIS

The symbol \( GLH[m, n] \) will be used to represent the order of \( GLH(m, n) \), the group of linear transformations on \( m \) variables whose coefficients are taken modulo \( n \) in such a way that the determinant of each transformation is prime to \( n \). In this note we state four theorems on congruence groups, which may be obtained by modifying proofs of corresponding theorems\(^1\) on groups of transformations with coefficients in a Galois field \( GF[p^s] \). Theorem 5 gives a set of defining relations for a related abstract group.

**Theorem 1.** \( GLH[m, n] = \prod_{i=1}^{m} n^{-1} \phi_i(n) \), where \( \phi_i(n) \) represents the \( i \)th totient of \( n \).

**Theorem 2.** The matrix of every transformation of \( GLH(m, n) \) of determinant \( s \) equals \( BD_s \), where \( B \) is derived from \( B_{r,c,\lambda} \) and \( D_s \) is the diagonal matrix \((1, 1, \cdots, s)\).

**Theorem 3.** \( SLH[m, n] = GLH[m, n]/\phi(n) \).

**Corollary.** \( SLH[2, n] = n\phi_2(n) \).

**Theorem 4.** \( SLH(2, n) = \{ V, W \} \), where \( V \) and \( W \) are, respectively, the following transformations: \( x_1' = -x_2, x_2' = x_1 \) and \( x_1' = x_1, x_2' = x_1 + x_2 \).

**Theorem 5.** If \( n > 2 \), \( SLH(2, n) \) is simply isomorphic with the abstract group whose generators \( V \) and \( W \) satisfy

(a) \( V^2 = I \),

(b) \( W^n = I, WV^2 = V^2W \),

(c) \( W^\lambda VW\mu VW^{(\lambda + 1)/(\mu = 1)} VW^{(\lambda - 1)} V = I \), for all values of \( \lambda \) and \( \mu \) such that \( \lambda \mu - 1 \) is prime to \( n \).

Let \( g \) be the order of \( G = \{ V, W \} \). Since (a), (b), and (c) are satisfied by the generators of \( SLH(2, n) \), \( g \geq n\phi_2(n) \).

If \( \mu \) is prime to \( n \), the substitutions \( \lambda = \alpha(1 + 1/\beta) \) and \( \mu = 1/\alpha \) in (c) yield

(c') \( W^{a + a/\beta} VW^{1/\alpha} VV^{a + a/\beta} VV^{1/\alpha} VV^{\beta + \beta/\alpha} V = I \),

for all \( \alpha \) and \( \beta \) prime to \( n \).

In order to simplify the computation, we define

---

Received by the editors August 4, 1950 and, in revised form, August 9, 1951.

1 See Dickson, Linear groups, pp. 77–82, for statement of corresponding theorems and explanation of notation.

2 The corresponding theorem on \( SLH(2, p^s) \) is due to E. H. Moore; Dickson, loc. cit., p. 300.

367
\[ R_a = W^{1/a}VW^aVW^{1/a}V \]

for all values of \( \alpha \) prime to \( n \). The following properties of the operator \( R \) may be established:

(d) \( R_I = I \),

(e) \( (R_a V)^2 = V^2 \),

(f) \( W^\rho R_a = R_a W^{\rho a^2} \), where \( \alpha \) is prime to \( n \) and \( \rho \) is arbitrary.

(f') \( R_a V = VR_1/a \),

(g) \( R_{ab} = R_a R_b \).

Consider the following set of elements

\[ W^{(e+dz)/(a+bx)} R_{a+bz} V^{-1} W^{-b/(a+bx)} V W^{-x} \]

where \( (a, b) \) is prime to \( n \), \( x \) is any integer such that \( a+bx \) is prime to \( n \), and \( ad-bc \equiv 1 \mod n \). The condition

\[ W^{(e+dz)/(a+bx)} R_{a+bz} V^{-1} W^{-b/(a+bx)} V W^{-x} = W^{(e+dy)/(a+by)} R_{a+by} V^{-1} W^{-b/(a+by)} V W^{-y} \]

for all values of \( x \) and \( y \) for which \( a+bx \) and \( a+by \) are prime to \( n \) reduces to an equivalent form of (c). Hence a different choice of \( x \) yields the same set (h). Therefore, the number of distinct elements in the set is at most \( n\phi_2(n) \).

If we multiply the set on the right by \( W \), the product has the same form as (h). Applying \( V \) as a right-hand multiplier, the product of any element of the set by \( V \) is an element of the set if

\[ W^{(e+dz)/(a+bx)} R_{a+bz} V^{-1} W^{-b/(a+bx)} V W^{-x} V = W^{(d-cy)/(b-ay)} R_{b-ay} V^{-1} W^{a/(b-ay)} V W^{-y}, \]

where \( b-ay \) is prime to \( n \). This condition may be reduced to (c') by means of (c) and the fact that \( x \) and \( y \) may be chosen so that \( a+bx \), \( b-ay \), and \( 1+xy \) are each relatively prime to \( n \). Hence \( g = n\phi_2(n) \) and the theorem is proved.

The University of Alabama