TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 153, January 1971

IRREDUCIBLE CONGRUENCES OF PRIME POWER DEGREE(1)

BY
C. B. HANNEKEN

Abstract. The number of conjugate sets of irreducible congruences of degree m belonging to $GF(p)$, $p>2$, relative to the group G of linear fractional transformations with coefficients belonging to the same field has been determined for $m\leqq 8$. In this paper the irreducible congruences of prime power degree q^α, $q>2$, are considered and the number of conjugate sets relative to G is determined.

1. **Introduction.** The conjugate sets of irreducible m-ic congruences

$$C_m(x) = x^m+a_1x^{m-1}+\cdots+a_{m-1}x+a_m\equiv 0 \pmod p \tag{1.1}$$

belonging to the modular field defined by a prime p under the group G of linear fractional transformations

$$T\colon x = (ax'+b)/(cx'+d), \qquad a, b, c, d\in GF(p), \tag{1.2}$$

have been classified in terms of the irreducible factors of an absolute invariant $\pi_m(J, K)$ [4]. In this classification it was shown that there is a 1-1 correspondence between irreducible factors of $\pi_m(J, K)$ of degree r and conjugate sets of order $p(p^2-1)/d$ where $d=m/r$. Since the roots $\pi_\mu=J/K$ of $\pi_m(J, K)$ are given by

$$\pi_\mu = (\mu^{p^2}\mu^p, \mu\mu^{p^3}) = (\mu^{p^2}-\mu)(\mu^p-\mu^{p^3})/(\mu^{p^2}-\mu^{p^3})(\mu^p-\mu) \tag{1.3}$$

where μ is a root of an irreducible m-ic congruence and since $\pi_m(J, K)$ contains no multiple roots then the degree r of an irreducible factor of $\pi_m(J, K)$ must be a divisor of m(2).

Although the conjugate sets of m-ic congruences relative to G have been classified relative to the factors of $\pi_m(J, K)$ there still remains the problem of determining the degrees of these factors and hence the number of conjugate sets of the various

Received by the editors February 25, 1970.

AMS 1969 *subject classifications*. Primary 1076, 1225; Secondary 1077, 1230, 1006.

Key words and phrases. Congruences, linear fractional transformation, matrix representation, conjugate set, transform of a q^α-ic congruence, conjugate under G, self-conjugate congruence, order of a conjugate set, marks of $GF(p^{q^r})$, complementary function, normal form of a congruence, characteristic polynomial, completely reducible, normalizer of a subgroup.

(1) The preparation of this paper was partially supported by a Summer Faculty Fellowship sponsored by Marquette University (1969).

(2) For the degree d_m of $\pi_m(J, K)$ see [2, equation (11), p. 5] in the special case of $n=1$.

orders. This is important in determining the number of nonisomorphic subgroups of Class II (the metabelian subgroups) in the holomorph of an elementary abelian group of order p^{n+m} each having commutator subgroup of order p^m(3).

Any hope of determining the number of conjugate sets of m-ic congruences relative to G where $m=q_1^{\alpha_1}q^{\alpha_2}\cdots q_t^{\alpha_t}$ and therefore the corresponding number of metabelian subgroups necessitates considering the more restricted cases for m, namely those for which the number t of distinct prime factors is 1. These are the cases which we shall be concerned with in this paper. We shall therefore determine the number of conjugate sets of irreducible m-ic congruences over $GF(p)$ where m is a power of a prime q, say $m=q^\alpha$.

A study of the irreducible congruences of prime power degree over $GF(p^n)$ relative to G may be made by generalizing the results of this paper. Since the group problem does not require such a generalization and since it would be relatively simple to make we do not offer it in this paper. Moreover, since the cases $p=2$ and $q=2$ require special treatment we assume them to be greater than 2.

Since the divisors of $m=q^\alpha$ are of the form $d=q^s$, $0\leqq s\leqq\alpha$, and since the group G is of order $o(G)=p(p^2-1)$ then the orders of conjugate sets are of the form $p(p^2-1)/q^s$. Thus, if $q^r=(q^\alpha, p(p^2-1))$, the g.c.d. of q^α and $o(G)$, then conjugate sets of order $p(p^2-1)/q^s$ may exist where $s=0, 1, \ldots, r$. In all, there are $(p^{q^\alpha}-p^{q^{\alpha-1}})/q^\alpha$ distinct q^α-ic congruences over $GF(p)$. If C_s denotes a set of order $p(p^2-1)/q^s$ and if K_s denotes the number of such sets then

$$(1.4)\qquad \begin{aligned}\frac{p^{q^\alpha}-p^{q^{\alpha-1}}}{q^\alpha} &= K_0p(p^2-1)\\ &\quad+K_1\frac{p(p^2-1)}{q}+\cdots+K_s\frac{p(p^2-1)}{q^s}+\cdots+K_r\frac{p(p^2-1)}{q^r}.\end{aligned}$$

To determine the number of conjugate sets of the various orders we consider separately the two possible values for r in $q^r=(q^\alpha, p(p^2-1))$, namely $r=0$ and $r>0$. The cases for which $r=0$ are quickly disposed of in §2. For $r>0$, two cases must be considered, namely that for which $q|p$, in which case $q=p$, and that for which $q|(p^2-1)$, in which case $q|(p+1)$ or $q|(p-1)$ but not both since $q>2$. These two cases are considered in §§3 and 4 respectively.

For convenience we use the standard notation $IQ[m, p^k]$ for an irreducible monic congruence of degree m over $GF(p^k)$. We shall use $\{IQ[m, p^k]\}^{p^j}$ to denote the congruence of degree m whose coefficients are respectively the p^jth powers of those of $IQ[m, p^k]$ and $\{IQ[m, p^k]\}^{p^j+p^w}$ will mean the product of $\{IQ[m, p^k]\}^{p^j}$ and $\{IQ[m, p^k]\}^{p^w}$. Moreover, $GF^*(p^k)$ will be used to denote the set of marks of the field $GF(p^k)$ which do not belong to any proper subfield. Finally, if $T\in G$ is given by (1.2) then we shall say that T is identified by the matrix $M(T)=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ and

(3) For a connection between the two problems see Brahana [1].

that this matrix defines T. If $f(x)$ is an $IQ[m, p^k]$ and $T \in G$ then $f(x)T=f'(x)$ will denote the transform of $f(x)$ by T. In particular, $f(x)T=f'(x)$ is the monic polynomial congruence in x obtained from $f((ax+b)/(cx+d))$. If $f(x)T=f(x)$ then we refer to $f(x)$ as being self-conjugate under T.

2. **Case for** $(q^\alpha, p(p^2-1))=1$. These are the cases for which (i) $q>p$ or (ii) $q<p$ and $q\nmid(p^2-1)$. Here $r=s=0$ and every conjugate set is a C_0 set. The number K_0 of such sets is easily determined by making use of (1.4). We have therefore

THEOREM 2.1. *If* $(q^\alpha, p(p^2-1))=1$ *then all conjugate sets of irreducible q^α-ic congruences over $GF(p)$ are of order $p(p^2-1)$ and there are*

$$K_0 = (p^{q^\alpha}-p^{q^{\alpha-1}})/q^\alpha p(p^2-1)$$

such sets.

3. **Case for** $p=q$. In this case $(q^\alpha, p(p^2-1))=q^r$ implies that $r=1$ and hence $s=0$ or 1. Thus conjugate sets may be of orders $p(p^2-1)$ and $p(p^2-1)/p=p^2-1$. To determine the exact number of each order we consider separately the cases for $\alpha=1$, $\alpha=2$ and $\alpha>2$.

(i) $\alpha=1$. For this case $\pi_m(J, K)$ is of degree $d_m=(p^{p-1}-1)/(p^2-1)$ and since this is prime to p then $\pi_m(J, K)$ must contain at least one linear factor. Thus there exists at least one conjugate set of order p^2-1. Furthermore since the factors of $\pi_m(J, K)$ are all distinct there can be no more than $p-1$ linear factors and hence no more than $p-1$ conjugate sets of order p^2-1.

If R and S denote the number of conjugate sets of order p^2-1 and $p(p^2-1)$ respectively then it follows that

$$d_m = (p^{p-1}-1)/(p^2-1) = p^{p-3}+p^{p-5}+\cdots+p^2+1 = R+pS. \tag{3.1}$$

Obviously $R\equiv 1 \pmod p$ and since $1\leqq R\leqq(p-1)$ then $R=1$ and hence $S=p(p^{p-3}-1)/(p^2-1)$ (4). Thus we have

THEOREM 3.1. *If $m=p$ then there exists one conjugate set of p-ic congruences over $GF(p)$ of order p^2-1 and $p(p^{p-3}-1)/(p^2-1)$ conjugate sets of order $p(p^2-1)$.*

An interesting characterization of the conjugate set C_1 of order p^2-1 may now be given. Since $o(G)=p(p^2-1)$ and $p|o(G)$ then G contains a transformation, say $\bar{T}$, of order p and C_1 contains a congruence, say $\bar{f}(x)$, which is self-conjugate under $\bar{T}$. Since $o(\bar{T})=p$ then there exist $L\in G$ such that $L^{-1}\bar{T}L=T$ where

$$M(T) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad a \neq 0. \tag{3.2}$$

(4) We note here that $S=0$ if and only if $p=3$. Thus all cubic congruences over $GF(3)$ are conjugate under G. The order of this conjugate set is p^2-1 which is in agreement with the number of irreducible cubics over $GF(3)$ as given by Dickson [3, p. 18].

Now if $\bar{f}(x)L=f(x)$ then $f(x)T=f(x)(L^{-1}\bar{T}L)=\bar{f}(x)(\bar{T}L)=\bar{f}(x)L=f(x)$ and $f(x)$ is self-conjugate under T. If η is a root of $f(x)$ then $\eta T=\eta^p=\eta+a$ is also a root and the p roots of $f(x)$ are

$$\eta,\ \eta^p = \eta+a,\ \eta^{p^2} = \eta+2a, \dots,\ \eta^{p^{p-1}} = \eta+(p-1)a. \tag{3.3}$$

It follows upon expansion that

$$f(x) = \prod_{j=0}^{p-1} (x-\eta^{p^j}) = x^p-x+\beta, \qquad \beta \neq 0. \tag{3.4}$$

Clearly $f(x)$ is irreducible over $GF(p)$ for any nonzero $\beta \in GF(p)$. Moreover, all congruences of this form are not only invariant under T but are conjugate under T' where $M(T')=\left(\begin{smallmatrix} k & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Substituting (3.3) into (1.3) and simplifying we find $\pi_\eta=(\eta^{p^2}\eta^p, \eta\eta^{p^3})=4$ which characterizes this set C_1. Since $J/K=\pi_\eta=4$ then $J-4K$ is the linear factor of $\pi_m(J, K)$.

(ii) $\alpha=2$. It is well known that any $IQ[m, p^n]$ is factorable over $GF(p^{n\sigma})$ into δ factors each an $IQ[m/\delta, p^{n\sigma}]$ where δ is the g.c.d. of m and σ [3, p. 33]. For $n=1$ and $m=q^\alpha$ we have

$$IQ[q^\alpha, p] = \prod_{j=1}^{q^{\alpha-1}} IQ_j[q, p^{q^{\alpha-1}}], \tag{3.5}$$

where, in fact, $IQ_j[q, p^{q^{\alpha-1}}]=\{IQ[q, p^{q^{\alpha-1}}]\}^{p^j}$ for some $IQ[q, p^{q^{\alpha-1}}]$. Thus

$$IQ[q^\alpha, p] = \{IQ[q, p^{q^{\alpha-1}}]\}^{1+p+p^2+\cdots+p^{q^{\alpha-1}-1}} \tag{3.6}$$

for some $IQ[q, p^{q^{\alpha-1}}]$.

In the special case of $\alpha=2$ and $p=q$ we have

$$f(x) = IQ[p^2, p] = \{IQ[p, p^p]\}^{1+p+p^2+\cdots+p^{p-1}} = \prod_{j=0}^{p-1} \{IQ[p, p^p]\}^{p^j}. \tag{3.7}$$

If η is a root of $f(x)=IQ[p, p^p]$ then $\eta \in GF^*(p^{p^2})$ and the roots of $f(x)$ are

$$\eta, \eta^{p^p}, \eta^{p^{2p}}, \dots, \eta^{p^{(p-1)p}}.$$

Now if $T \in G$ transforms $f(x)=IQ[p^2, p]$ into itself, in which case $f(x)$ belongs to a conjugate set of order p^2-1, then T is of order p and it follows by making use of (3.7) that either

$$IQ[p, p^p]T = IQ[p, p^p] \tag{1}$$

or

$$IQ[p, p^p]T = \{IQ[p, p^p]\}^{p^j}, \tag{2}$$

for some $j=1, 2, \dots, p-1$. That is, T either leaves each factor of $f(x)$ fixed or it permutes them. We now show that (2) cannot hold. Suppose therefore that (2) holds for some $j<p$. Then $IQ[p, p^p]T^2=\{IQ[p, p^p]\}^{p^j}T=\{IQ[p, p^p]\}^{p^{2j}}$, $IQ[p, p^p]T^3$

$=\{IQ[p,p^p]\}^{p^{3j}},\ldots$. Thus T transforms the roots of $IQ[p,p^p]$ into the roots of $\{IQ[p,p^p]\}^{p^j}$ and hence $\eta T=\eta^{p^{kp+j}}$ for some $k=0,1,2,\ldots,p-1$. Since $\eta^{p^t}T=\eta^{p^{kp+j+t}}$ for all t, we have

$$\eta T^2 = (\eta T)T = (\eta^{p^{kp+j}})T = \eta^{p^{2kp+2j}},\ldots,\eta T^p = \eta I = \eta = \eta^{p^{kp^2+pj}} = \eta^{p^{pj}},$$

and since $j<p$ it follows that $\eta\in GF(p^p)$. This, of course, contradicts the irreducibility of $IQ[p,p^p]$. Hence (2) does not hold.

Thus, the problem of determining the number of conjugate sets of $IQ[p^2,p]$ of order p^2-1 under G resolves itself to that of determining the number of conjugate sets of $IQ[p,p^p]$ of order p^2-1 under G. Now any $IQ[p,p^p]$ in a C_1 set is conjugate to an $f'(x)=IQ[p,p^p]$ which is self-conjugate under a transformation T of G given by (3.2). Without loss of generality we choose $a=1$. Then if η is a root of $f'(x)$, its set of roots is

$$S_\eta = \{\eta, \eta^{p^p} = \eta+1, \eta^{p^{2p}} = \eta+2,\ldots,\eta^{p^{(p-1)p}} = \eta+(p-1)\}$$

and, hence, $f'(x)=IQ[p,p^p]=\prod_{i=0}^{p-1}(\delta-i)$, where $\delta=x-\eta$. From this we obtain

$$IQ[p,p^p] = f'(x) = \delta^p-\delta = x^p-x-(\eta^p-\eta) = x^p-x-\sigma,$$

where $\eta^p-\eta=\sigma$. Since $f'(x)$ is an irreducible p-ic over $GF(p^p)$ then σ must belong to $GF^*(p^p)$ while $\eta\in GF^*(p^{p^2})$ since η is also a root of $f(x)=IQ[p^2,p]$.

To determine the number of $IQ[p,p^p]$ of the form $f'(x)=x^p-x-\sigma$ suppose that $\beta\in GF(p^p)$ and let $\gamma=\beta^p-\beta$. Then β is a root of $x^p-x-\gamma=g(x)$ and since $g(x)$ is transformed into itself by T: $\left(\begin{smallmatrix}1 & a\\ 0 & 1\end{smallmatrix}\right)$, its roots are $\beta,\beta+1,\ldots,\beta+(p-1)$. Therefore, $g(x)$ is reducible over $GF(p^p)$. If β and $\bar\beta$ produce the same expression γ, that is, if $\beta^p-\beta=\bar\beta^p-\bar\beta=\gamma$ then $(\beta-\bar\beta)^p=\beta-\bar\beta \pmod p$ and, hence, $\beta-\bar\beta=c\in GF(p)$. Thus β and $\bar\beta$ produce the same expression γ if and only if their difference lies in $GF(p)$. From this we conclude that there are p^{p-1} distinct expressions γ of the form $\gamma=\beta^p-\beta$ where $\beta\in GF(p^p)$. All of these γ's belong to $GF^*(p^p)$ except the one, namely 0, obtained by choosing $\beta\in GF(p)$. Hence there are $p^{p-1}-1$ distinct expressions $\gamma=\beta^p-\beta\in GF^*(p^p)$, $\beta\in GF(p^p)$. Let Γ denote this set. Since x^p-x-k is irreducible for any nonzero $k\in GF(p)$ the $p-1$ nonzero marks of $GF(p)$ belong to Γ. Thus there are $(p^{p-1}-1)-(p-1)=p^{p-1}-p$ distinct marks of $GF^*(p^p)$ belonging to Γ and hence $(p^p-p)-(p^{p-1}-p)=p^{p-1}(p-1)$ marks of $GF^*(p^p)$ not in Γ. Obviously, if σ is one of these, then $x^p-x-\sigma=f'(x)$ is irreducible over $GF(p^p)$ and its root η necessarily belongs to $GF(p^{p^2})$. Now the transformation defined by the matrix $\left(\begin{smallmatrix}a & 0\\ 0 & 1\end{smallmatrix}\right)$ transforms $x^p-x-\sigma$ into $x^p-x-\sigma/a$ and since a may assume any one of $p-1$ values we see that each conjugate set of $IQ[p,p^p]$ of order p^2-1 contains $p-1$ irreducible congruences of the form $x^p-x-\sigma$. Since there are in all $p^{p-1}(p-1)$ such congruences and since any conjugate set of order p^2-1 contains $p-1$ of these we have

LEMMA 3.1. *There are exactly p^{p-1} distinct conjugate sets of irreducible p-ic congruences over $GF(p^p)$ of order p^2-1 under the group G.*

If $x^p-x-\sigma$ is an $IQ[p, p^p]$ then so is $x^p-x-\sigma^{p^i}$, $i=0, 1, \ldots, p-1$. Since an $IQ[p^2, p]$ in a conjugate set of order p^2-1 is conjugate to an $IQ[p^2, p]$ of the form

$$IQ[p^2, p] = \prod_{i=0}^{p-1} (x^p-x-\sigma^{p^i}),$$

where $x^p-x-\sigma^{p^i}$ is an $IQ[p, p^p]$, and conversely, then it follows that p conjugate sets of $IQ[p, p^p]$ of order p^2-1 combine to form one set of $IQ[p^2, p]$ of order p^2-1. This gives

LEMMA 3.2. *There exist $p^{p-1}/p=p^{p-2}$ distinct conjugate sets of irreducible p^2-ic congruences over $GF(p)$ of order p^2-1.*

In all there are $(p^{p^2}-p^p)/p^2$ distinct p^2-ics over $GF(p)$. By Lemma 3.1 and the fact that conjugate sets are of orders p^2-1 and $p(p^2-1)$ we have

THEOREM 3.2. *There are p^{p-2} distinct conjugate sets of irreducible p^2-ic congruences of order p^2-1 under G and $(p^{p^2-3}-p^{p-1})/(p^2-1)$ conjugate sets of order $p(p^2-1)$.*

(iii) $\alpha > 2$. This case is simply a generalization of the cases $\alpha=1$ and $\alpha=2$. We first determine the number of conjugate sets of order p^2-1. Any such set must contain an $IQ[p^\alpha, p]$ which is self-conjugate under a transformation T of order p. Since $IQ[p^\alpha, p]$ is the product of $p^{\alpha-1}$ distinct irreducible p-ic congruences over $GF(p^{p^{\alpha-1}})$ and since

$$IQ[p^\alpha, p] = \prod_{j=0}^{p^{\alpha-1}-1} \{IQ[p, p^{p^{\alpha-1}}]\}^{p^j}$$

for some $f'(x)=IQ[p, p^{p^{\alpha-1}}]$ then T either leaves the factors fixed or it permutes them. In a manner similar to the case for $\alpha=2$ one may show that the latter does not occur and hence T leaves each factor fixed. If η is a root of $f'(x)=IQ[p, p^{p^{\alpha-1}}]$ then $\eta T=\eta^{p^{sp^{\alpha-1}}}$ for some $s=1, 2, \ldots, p-1$. Without loss of generality we may assume that $s=1$ and that $M(T)=\left(\begin{smallmatrix}1 & a\\ 0 & 1\end{smallmatrix}\right)$. Then the roots of $f'(x)$ are

$$\eta,\ \eta+a=\eta^{p^{p^{\alpha-1}}},\ \eta+2a = \eta^{p^{2p^{\alpha-1}}}, \ldots, \eta+(p-1)a=\eta^{p^{(p-1)p^{\alpha-1}}},$$

and it readily follows that $f'(x)$ is of the form

$$f'(x) = IQ[p, p^{p^{\alpha-1}}] = x^p-x-(\eta^p-\eta) = x^p-x-\sigma.$$

Clearly $f'(x)$ is irreducible over $GF(p^{p^{\alpha-1}})$ if and only if $\sigma \in GF^*(p^{p^{\alpha-1}})$ and is not of the form $\sigma=\beta^p-\beta$ for $\beta \in GF(p^{p^{\alpha-1}})$. In a manner similar to the case $\alpha=2$ one may show that there are

$$p^{p^{\alpha-1}}-p^{p^{\alpha-1}-1} = p^{p^{\alpha-1}-1}(p-1)$$

marks σ satisfying the prescribed conditions and, hence, as many irreducible p-ics over $GF(p^{p^{\alpha-1}})$ of the form $x^p-x-\sigma=f'(x)$. Now $x^p-x-\sigma$ is conjugate to

$x^p - x - k\sigma$ for any nonzero $k \in GF(p)$ and, hence, there are $p^{p^{\alpha-1}-1}$ conjugate sets of p-ics over $GF(p^{p^{\alpha-1}})$ of order p^2-1. Since $p^{\alpha-1}$ of these sets go together to form one set of irreducible p^α-ics over $GF(p)$ of order p^2-1 then there are

$$K_1 = p^{p^{\alpha-1}-1}/p^{\alpha-1} = p^{p^{\alpha-1}-\alpha}$$

distinct C_1 sets. The number K_0 of C_0 sets is now easily determined. We state these results in

THEOREM 3.3. *There are $K_1 = p^{p^{\alpha-1}-\alpha}$ distinct conjugate sets of irreducible p^α-ics over $GF(p)$ of order p^2-1 under the group G and $K_0 = (p^{p^\alpha} - p^{p^{\alpha-1}+2})/p^{\alpha+1}(p^2-1)$ conjugate sets of order $p(p^2-1)$ under G.*

4. **Case for** $(q^\alpha, p(p^2-1)) = q^r$, $r > 1$, $q < p$. In these cases $q|(p^2-1)$ and since $2 < q$ then $q|(p+1)$ or $q|(p-1)$ but not both. Since $r > 1$ then C_s sets may exist for $s = 0, 1, 2, \ldots, r$ and our problem is to determine the number K_s of C_s sets of their respective order $p(p^2-1)/q^s$ according as $q|(p \pm 1)$.

Let $f_s(x)$ be any given $IQ[q^\alpha, p]$ which belongs to a C_s set. Then $f_s(x)T = f_s(x)$ for some $T \in G$ of order q^s and let

$$f_s(x) = IQ[q^\alpha, p] = \prod_{j=0}^{q^{\alpha-s}-1} \{IQ[q^s, p^{q^{\alpha-s}}]\}^{p^j} = \{q_s(x)\}^{1+p+\cdots+p^{q^{\alpha-s}-1}},$$

for some $q_s(x) = IQ[q^s, p^{q^{\alpha-s}}]$. We shall show that $q_s(x)$ and hence each factor $\{q_s(x)\}^{p^j}$ of $f_s(x)$ is self-conjugate under T. If η is a root of $q_s(x)$ (and, hence, of $f_s(x)$) then its roots are

$$\eta, \eta^{p^{q^{\alpha-s}}}, \eta^{p^{2q^{\alpha-s}}}, \ldots, \eta^{p^{q^{\alpha-s+1}}}, \ldots, \eta^{p^{(q^s-1)q^{\alpha-s}}}$$

and the relation $f_s(x)T = f_s(x)$ implies that $\eta T = \eta^{p^k}$ for some k. Now, since $\eta^{p^h}T = (\eta^{p^k})^{p^h} = \eta^{p^{h+k}}$ for all h and since $\eta T^2 = (\eta T)T = \eta^{p^k}T = \eta^{p^{2k}}$ and, hence, $\eta T^j = \eta^{p^{jk}}$ for all j, then $\eta T^{q^s} = \eta = \eta^{p^{q^s k}}$ implies that $q^s k = q^\alpha$ since $\eta \in GF^*(p^{q^\alpha})$ and, hence, $k = q^{\alpha-s}$. Thus $\eta T = \eta^{p^{q^{\alpha-s}}}$ and we have $q_s(x)T = q_s(x)$. Therefore each factor of $f_s(x)$ in this factorization is self-conjugate under T.

Now suppose $q(x)$ is any given q^s-ic congruence (irreducible or reducible) over $GF(p^{q^{\alpha-s}})$ which is self-conjugate under a transformation T of order q^s. If $M(T) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and if η is a root then

$$\eta, \eta T = \frac{a\eta + b}{c\eta + d}, \eta T^2 = \frac{(a^2+bc)\eta + (ab+bd)}{(ac+cd)\eta + (bc+d^2)}, \ldots, \eta T^{q^\alpha - 1} = \frac{d\eta - b}{-c\eta + a} \tag{4.1}$$

are all roots of $q(x)$. If $\alpha_s = \eta + \eta T + \eta T^2 + \cdots + \eta T^{q^\alpha-1}$ then

$$\alpha_s = \eta + \frac{a\eta + b}{c\eta + d} + \cdots + \frac{d\eta - b}{-c\eta + a} = \frac{N(\eta)}{D(\eta)} \tag{4.2}$$

and it readily follows that

$$q(x) = N(x) - \alpha_s D(x). \tag{4.3}$$

For convenience we shall refer to (4.3) as the normal form for $q(x)$. The polynomials $N(x)$ and $D(x)$ as defined by (4.2) are called the *complementary functions* of $q(x)$ and obviously depend solely upon the transformation T and its respective powers. Since $N(x)$ and $D(x)$ are of degrees q^s and q^s-1 respectively and since the coefficients of $q(x)$ are linear functions of α_s over $GF(p)$ then $q(x)$ is not irreducible if α_s belongs to a proper subfield of $GF(p^{q^{\alpha-s}})$.

Since any q^s-ic congruence which is self-conjugate under a T of order q^s is expressible in its normal form and since the complementary functions depend upon T then the reducibility or irreducibility of $q(x)$, as well as the number of each type, depends upon the values of α_s. There are $p^{q^{\alpha-s}}-p^{q^{\alpha-s-1}}$, the order of $GF^*(p^{q^{\alpha-s}})$, distinct choices or values which α_s may assume. Obviously, not every one of these choices will identify an irreducible $q(x)$. For any given $\alpha_s \in GF^*(p^{q^{\alpha-s}})$ a root η of $q(x)$ may belong to

$$GF^*(p^{q^{\alpha-s}}),\ GF^*(p^{q^{\alpha-s+1}}), \ldots,\ GF^*(p^{q^{\alpha-1}},\ \text{or}\ GF^*(p^{q^{\alpha}}).$$

If $\eta \in GF^*(p^{q^\alpha})$ then $q(x)$ is an irreducible q^s-ic over $GF(p^{q^{\alpha-s}})$ and this is the only case for which $q(x)$ is irreducible. If, on the other hand, $\eta \in GF^*(p^{q^{\alpha-s}})$ then $q(x)$ is completely reducible over $GF(p^{q^{\alpha-s}})$, that is, $q(x)$ is the product of q^s distinct linear factors over $GF(p^{q^{\alpha-s}})$, namely $q(x)=(x-\eta)(x-\eta T)\cdots(x-\eta T^{q^s-1})$. If, however, $\eta \in GF^*(p^{q^{\alpha-s+1}})$ then η is a root of an irreducible q-ic over $GF(p^{q^{\alpha-s}})$, say $q_1(x)$, which is self-conjugate under $T_1=T^{q^{s-1}}$, a transformation of order q. In this case $q(x)$ would simply be the product of $q_1(x)$ and the q^{s-1} distinct transforms of it by T, that is, $q(x)=\prod_{j=0}^{q^{s-1}} (q_1(x)T^j)$. Moreover, each factor $q_1(x)T^j$ would be an irreducible q-ic over $GF(p^{q^{\alpha-s}})$ which is self-conjugate under T_1.

Similarly, if $\eta \in GF(p^{q^{\alpha-s+2}})$ then it readily follows that η is a root of an irreducible q^2-ic over $GF(p^{q^{\alpha-s}})$ which is self-conjugate under $T_2=T^{q^{\alpha-2}}$ and that $q(x)$ is the product of the q^{s-2} distinct transforms of $q_2(x)$ by T, $q_2(x)T^j$, $j=0, 1, \ldots, q^{s-2}-1$, each of which is self-conjugate under T_2.

In general, if $\eta \in GF(p^{q^{\alpha-s+t}})$, $t=0, 1, 2, \ldots, s-1$, then η is a root of an irreducible q^t-ic over $GF(p^{q^{\alpha-s}})$, say $q_t(x)$, and

$$q(x) = \prod_{j=0}^{q^{s-t}} (q_t(x)T^j), \tag{4.4}$$

each factor of which is an $IQ[q^t, p^{q^{\alpha-s}}]$ which is self-conjugate under $T_t=T^{q^{s-t}}$. The number of $IQ[q^s, p^{q^{\alpha-s}}]$, $s=1, 2, \ldots, r$, which are self-conjugate under T of order q^s may be obtained by determining the number of choices for α_s in (4.3) for which $q(x)$ is reducible.

We remark now that if T is of order q^s then the characteristic polynomial of $M(T)$ has distinct roots belonging to $GF(p)$ or $GF^*(p^2)$ according as $q|(p-1)$ or $q|(p+1)$; and, there corresponds to these roots two distinct marks, say η_1 and η_2, of $GF(p)$ or $GF^*(p^2)$ respectively such that $\eta_1 T=\eta_1$ and $\eta_2 T=\eta_2$. Since $q\neq 2$ then the roots of $q(x)$, as given by (4.1), are all distinct except in the case where $q|(p-1)$ and $\eta=\eta_1$ or η_2. We make use of these facts in the proofs of the following lemmas.

LEMMA 4.1. *There exist* $[(p^{q^n}\pm 1)\mp q^s]/q^s$ *distinct* q^s*-ic congruences over* $GF(p^{q^n})$ *which are completely reducible over* $GF(p^{q^n})$ *and self-conjugate relative to a given fixed transformation* T_s *of order* q^s *according as* $q|(p\pm 1)$.

Proof. Let T_s be any given transformation of order q^s and let $q_s(x)=N(x)-\alpha_s D(x)$ be a q^s-ic over $GF(p^{q^n})$ which is self-conjugate under T_s and completely reducible over $GF(p^{q^n})$. If η is a root of $q_s(x)$ then $\eta\in GF(p^{q^n})$ and is not among the q^s-1 roots of $D(x)$. There are, therefore, $p^{q^n}-(q^s-1)$ marks of $GF(p^{q^n})$ which are permissible choices for η. These partitions into sets $S_\eta=\{\eta, \eta T, \ldots, \eta T^{q^s-1}\}$ each set constituting the roots of $q_s(x)$ and, therefore, identifying a unique α_s and, hence, a unique $q_s(x)$. Each set S_η consists of q^s distinct marks (roots of $q_s(x)$) except in the case where $q^s|(p-1)$ and η is one of the two marks left fixed by T_s. If η_1 and η_2 denote these marks then $S_{\eta_1}=\{\eta_1\}$, $S_{\eta_2}=\{\eta_2\}$ and it follows that there are

$$[p^{q^n}-(q^s-1)-2]/q^s+2 \;=\; [(p^{q^n}-1)+q^s]/q^s$$

distinct sets S_η, and, hence, this many values for α_s, each of which identifies a $q_s(x)$ possessing the prescribed properties. If $q^s|(p+1)$ then all sets S_η are of order q^s since, in this case, the characteristic roots of $M(T_s)$ belong to $GF^*(p^2)$ and, hence, are not in $GF(p^{q^n})$. It follows that there are

$$[p^{q^n}-(q^s-1)]/q^s \;=\; [(p^{q^n}+1)-q^s]/q^s$$

distinct q^s-ics for this case. Thus the proof is now complete.

LEMMA 4.2. *There exist* $(q-1)(p^{q^n}\pm 1)/q$ *distinct irreducible* q*-ic congruences over* $GF(p^{q^n})$ *which are self-conjugate under a given transformation* T *of order* q *according as* $q|(p\pm 1)$.

Proof. Let T_1 be any given transformation of G of order q and let $q_1(x)=N(x)-\alpha_1 D(x)$ be a q-ic over $GF(p^{q^n})$ which is self-conjugate under T_1. If η is a root of $q_1(x)$ then either $\eta\in GF(p^{q^n})$, in which case $q_1(x)$ is completely reducible, or $\eta\in GF(p^{q^{n+1}})$, in which case $q_1(x)$ is irreducible. The number of irreducible ones is therefore the total number of choices for α_1, namely p^{q^n}, diminished by the number of choices for α_1 for which $q_1(x)$ is reducible, namely those for which $\eta\in GF(p^{q^n})$ and hence $q_1(x)$ completely reducible. Since, by Lemma 4.1, there are $[(p^{q^n}\pm 1)\mp q]/q$ such reducible q-ics there are

$$p^{q^n}-[(p^{q^n}\pm 1)\mp q]/q \;=\; [(q-1)(p^{q^n}\pm 1)]/q$$

irreducible q-ics according as $q|(p\pm 1)$. Thus the lemma.

To illustrate the procedures in the proof of the following important theorem let us determine the number of distinct irreducible q^2-ic congruences over $GF(p^{q^n})$ which are self-conjugate relative to a given transformation T_2 of order q^2. Let T_2 be a given transformation of order q^2 and let $q_2(x)=N(x)-\alpha_2 D(x)$ denote a q^2-ic over $GF(p^{q^n})$ which is self-conjugate relative to T_2. Obviously $\alpha_2\in GF(p^{q^n})$ and any root η of $q_2(x)$ necessarily belongs to $GF(p^{q^{n+2}})$. Since q is prime the only proper subfields of $GF(p^{q^{n+2}})$ to which η may belong are $GF(p^{q^n})$ and $GF(p^{q^{n+1}})$. In either event $q_2(x)$ is reducible and the number of values of α_2 for which $q_2(x)$ is irreducible may be easily determined. Suppose first that $\eta \in GF(p^{q^n})$. Then $q_2(x)$ is completely reducible and, by Lemma 4.1, there are $[(p^{q^n} \pm 1) \mp q^2]/q^2$ such q^2-ics. If $\eta \in GF^*(p^{q^{n+1}})$ then η is a root of an irreducible q-ic over $GF(p^{q^n})$, say $q_1(x)$, which is self-conjugate relative to $T_1 = T_2^q$. Moreover, $q_2(x)$ is the product of the q distinct irreducible q-ics over $GF(p^{q^n})$, namely $q_1(x)T^j$, $j=0, 1, 2, \ldots, q-1$, and each is self-conjugate under T_1. By Lemma 4.2, there are $(q-1)(p^{q^n} \pm 1)/q$ such q-ics, $q_1(x)$, according as $q|(p \pm 1)$; and, since q of these go together to determine one $q_2(x)$, there are

$$(q-1)(p^{q^n} \pm 1)/q^2$$

choices for α_2 for which the root η, and, hence, all roots of $q_2(x)$, belong to $GF^*(p^{q^{n+1}})$. Since α_2 may assume any one of p^{q^n} values there are

$$p^{q^n} - \left[\frac{(p^{q^n} \pm 1) \mp q^2}{q^2} + \frac{(q-1)(p^{q^n} \pm 1)}{q^2}\right] = \frac{(q-1)(p^{q^n} \pm 1)}{q}$$

distinct values for α_2 such that $q_2(x)$ is irreducible and, therefore, this number of irreducible q^2-ics self-conjugate under T_2 of order q^2.

We may now prove the following important

THEOREM 4.1. *If $2 < q < p$, if $q^r = (q^\alpha, p(p^2-1))$ and if T_s is any given transformation of G of order q^s, $1 \leqq s \leqq r$, then there exist $(q-1)(p^{q^n} \pm 1)/q$ distinct irreducible q^s-ic congruences over $GF(p^{q^n})$ which are self-conjugate relative to T_s according as $q|(p \pm 1)$.*

Proof. Let T_s be any given transformation of order q^s, let $T_t = T_s^{q^{s-t}}$, $t = 1, 2, \ldots, s$, and let $q_s(x) = N(x) - \alpha_s D(x)$ be a q^s-ic over $GF(p^{q^s})$ which is self-conjugate under T_s. From previous discussions the theorem is true for $s = 1, 2$. We assume the theorem true for any $t < s$ and prove it true for $t = s$. If η is a root of $q_s(x)$ then $\eta \in GF(p^{q^{n+s}})$ and may belong to any one of the subfields:

$$GF(p^{q^n}), GF(p^{q^{n+1}}, \ldots, GF(p^{q^{n+t}}), \ldots, GF(p^{q^{n+s-1}}), \text{ or } GF(p^{q^{n+s}}).$$

Now, for $t = 0, 1, \ldots, s$, let L_t denote the number of choices for α_s in $GF(p^{q^n})$ such that $q_s(x)$ has a root η (and hence all roots ηT_s^j, $j = 0, 1, \ldots, q^s - 1$) belonging to $GF^*(p^{q^{n+t}})$. To determine L_t for $0 < t < s$ suppose $\eta \in GF^*(p^{q^{n+t}})$. Then η is a root of an irreducible q^t-ic over $GF(p^{q^n})$, say $q_t(x)$, and $q_s(x)$ is the product of the q^{s-t} distinct q^t-ics, $q_t(x)T_s^j$, $j = 0, 1, \ldots, q^{s-t} - 1$, each of which is self-conjugate under T_t. By our assumption there exist $(q-1)(p^{q^n} \pm 1)/q$ distinct choices for $q_t(x)$ and since q^{s-t} of these go together to form one $q_s(x)$ it follows that

$$L_t = [(q-1)(p^{q^n} \pm 1)]/q^{s-t+1}, \qquad 1 \leqq t < s. \tag{4.5}$$

For $t = 0$ it follows from Lemma 4.1 that there are

$$L_0 = [(p^{q^n} \pm 1) \mp q^s]/q^s \tag{4.6}$$

values for α_s such that $q_s(x)$ has its roots in $GF(p^{q^n})$. If $\eta \in GF^*(p^{q^{n+s}})$ then $q_s(x)$ is irreducible and the number L_s is the number of such q^s-ics. Clearly

$$L_s = p^{q^n} - \sum_{t=0}^{s-1} L_t.$$

By direct substitution from (4.5) and (4.6) and simplifying we have

$$L_s = (q-1)(p^{q^n} \pm 1)/q$$

according as $q|(p \pm 1)$. The proof is therefore complete.

Now, since any $f_s(x)$ belonging to a C_s set is factorable into the product of the $q^{\alpha-s}$ distinct irreducible q^s-ic congruences over $GF(p^{q^{\alpha-s}})$, $q_s(x)T^j$, $j=0, 1, \ldots, q^{\alpha-s}-1$, where each factor $q_s(x)T^j$ is an $IQ[q^s, p^{q^{\alpha-s}}]$ which is self-conjugate relative to some fixed transformation T_s of order q^s and since, by the above theorem, there are $(q-1)(p^{q^{\alpha-s}} \pm 1)/q$ such q^s-ics then there are $(q-1)(p^{q^{\alpha-s}} \pm 1)/q^{\alpha-s+1}$ irreducible q^α-ic congruences $f_s(x)$ over $GF(p)$ which are self-conjugate relative to a given T_s. Not all such congruences $f_s(x)$ will belong to C_s sets, for if $s<r$ and if T_{s+1} is a transformation of order q^{s+1} and if $T_{s+1}^q = T_s$ then $f_s(x)$ may be self-conjugate under T_{s+1} and, hence, belong to a C_{s+k} set for some $k \geqq 1$. If so, then

$$f_s(x) = \prod_{j=0}^{q^{\alpha-s-1}-1} q_{s+1}(x)T_{s+1}^j$$

where each factor $q_{s+1}(x)T_{s+1}^j$ is an $IQ[q^{s+1}, p^{q^{\alpha-s-1}}]$ which is self-conjugate relative to T_{s+1}. By Theorem 4.1, there are exactly

$$(q-1)(p^{q^{\alpha-s-1}} \pm 1)/q$$

such q^{s+1}-ics and since each of these is factorable into the product of q irreducible q^s-ics each self-conjugate under $T_{s+1}^q = T_s$ then $(q-1)(p^{q^{\alpha-s-1}} \pm 1)$ of the $(q-1)(p^{q^{\alpha-s}} \pm 1)/q$ choices for $q_s(x)$ identify congruences $f_s(x)$ belonging to C_{s+k} sets, $k \geqq 1$. There are, therefore,

$$(q-1)(p^{q^{\alpha-s}} \pm 1)/q - (q-1)(p^{q^{\alpha-s-1}} \pm 1)$$

q^s-ics, $q_s(x)$, which define $f_s(x)$ belonging to a C_s set, $s<r$. Since $q^{\alpha-s}$ of these q^s-ics go together to form a given $f_s(x)$ we have

THEOREM 4.2. *If* $2<q<p$, *if* $q^r = (q^\alpha, p(p^2-1))$ *and* $0<s<r$ *then there are*

$$Q_s = (q-1)[(p^{q^{\alpha-s}} \pm 1) - q(p^{q^{\alpha-s-1}} \pm 1)]/q^{\alpha-s-1}$$

distinct $IQ[q^\alpha, p]$ *belonging to* C_s *sets each of which is self-conjugate relative to a given transformation* T_s *of order* q^s *according as* $q|(p \pm 1)$.

The number K_s of C_s sets, $0<s<r$, may now be found by determining the exact number of such q^α-ics, $f_s(x)$, in each C_s set. If $f_s(x)$ and $f_s'(x)$ are any two conjugate q^α-ics in a C_s set which are self-conjugate under the same transformation T_s of

order q^s then it is quite clear that $f_s(x)L=f_s'(x)$ if and only if $L^{-1}T_sL=T_s^j$ for some j, that is, if and only if $L\in N_G(\{T_s\})$, the normalizer in G of the cyclic group $\{T_s\}$ generated by T_s. Certainly $T_s^j\in N_G(\{T_s\})$ for each $j=0, 1, \ldots, q^s-1$, and $f_s(x)(LT_s^j)=f_s'(x)T_s^j=f_s'(x)$ implies that the number of distinct images of $f_s(x)$ under $N_G(\{T_s\})$ is $o(N_G(\{T_s\}))/q^s$.

Now if $M(T_s)$ is the matrix representation of T_s and if $\bar{G}=GL(2,p)$ then $M(T_s)\in\bar{G}$ and the order of the normalizer of the cyclic group generated by $M(T_s)$ in $\bar{G}$ is $2(p^2-1)$ or $2(p-1)^2$ according as $q|(p+1)$ or $q|(p-1)$ (see [5]). Since $G=\bar{G}/C(\bar{G})$, where $C(\bar{G})$ is the center of $\bar{G}$, and since $o(C(\bar{G}))=p-1$ then it follows that $o(N_G(\{T_s\}))$ is $2(p\pm 1)$ according as $q|(p\pm 1)$. We state these results in

THEOREM 4.3. *In each C_s set, $0<s<r$, there exist $2(p\pm 1)/q^s$ q^α-ic congruences which are self-conjugate under a given transformation T_s of G of order q^s according as $q|(p\pm 1)$.*

The number K_s of C_s sets, $0<s<r$, is therefore the number Q_s, as given by Theorem 4.2, divided by $2(p\pm 1)/q^s$. We state this as

THEOREM 4.4. *If $2<q<p$ and $q^r=(q^\alpha, p(p^2-1))$ then the number K_s of conjugate sets of irreducible q^α-ic congruences over $GF(p)$ of order $p(p^2-1)/q^s$, $0<s<r$, is*

$$K_s = Q_s/[2(p\pm 1)/q^s] = \frac{q^s(q-1)[(p^{q^{\alpha-s}}\pm 1)-q(p^{q^{\alpha-s-1}}\pm 1)]}{2(p\pm 1)q^{\alpha-s+1}}$$

according as $q|(p\pm 1)$.

There remains the cases $s=r$ and $s=0$ which were excluded in the above theorem.

(i) *Case $s=r$.* If $s=r$ then conjugate sets of order $p(p^2-1)/q^r$ exist and must contain q^α-ic congruences of the form

$$f(x) = \prod_{j=0}^{q^{\alpha-r}-1} q_r(x)T^j,$$

where each factor $q_r(x)T^j$ is an $IQ[q^r, p^{q^{\alpha-r}}]$ which is self-conjugate under some T_r of order q^r. By Theorem 4.1, there are $(q-1)(p^{q^{\alpha-r}}\pm 1)/q$ such q^r-ics according as $q|(p\pm 1)$. Since $q^{\alpha-r}$ of these form one q^α-ic over $GF(p)$ and since $2(p\pm 1)/q^r$ belong to each C_r we have

THEOREM 4.5. *If $2<q<p$ and $q^r=(q^\alpha, p(p^2-1))\neq 1$ then there are*

$$K_r = [(q-1)(p^{q^{\alpha-r}}\pm 1)/q]/[2(p\pm 1)/q^rq^{\alpha-r}] = \frac{q^r(q-1)(p^{q^{\alpha-r}}\pm 1)}{2(p\pm 1)q^{\alpha-r+1}}$$

conjugate sets of q^α-ic congruences over $GF(p)$ of order $p(p^2-1)/q^r$ according as $q|(p\pm 1)$.

(ii) *Case $s=0$.* The number K_0 of C_0 sets is the number of sets of order $p(p^2-1)$. These are sets no congruence of which is left fixed by any transformation of G. Since any $IQ[q^\alpha, p]$ is expressible as the product of $q^{\alpha-1}$ distinct $IQ[q, p^{q^{\alpha-1}}]$ we may determine the number of q^α-ics belonging to C_0 sets by determining the number of irreducible q-ics over $GF(p^{q^{\alpha-1}})$ which are not self-conjugate under any T of G of order q. There are $(q-1)(p^{q^{\alpha-1}})/q$ irreducible q-ics over $GF(p^{q^{\alpha-1}})$ which are self-conjugate under a given T of order q and, hence, under the group $\{T\}$. Since there are $p(p\mp 1)/2$ distinct subgroups of G of order q according as $q|(p\pm 1)$ (see [5]) then there are

$$\frac{p(p\mp 1)}{2}\cdot\frac{(q-1)(p^{q^{\alpha-1}}\pm 1)}{q} = p(p\mp 1)(q-1)(p^{q^{\alpha-1}}\pm 1)/2q$$

irreducible q-ics over $GF(p^{q^{\alpha-1}})$ which are self-conjugate under some T of order q. Since there are $(p^{q^\alpha}-p^{q^{\alpha-1}})/q$ irreducible q-ics over $GF(p^{q^{\alpha-1}})$ altogether then there are

$$R = \frac{p^{q^\alpha}-p^{q^{\alpha-1}}}{q} - \frac{p(p\mp 1)(q-1)(p^{q^{\alpha-1}}\pm 1)}{2q}$$

irreducible q-ics over $GF(p^{q^{\alpha-1}})$ which are not self-conjugate under any T of G. Now $q^{\alpha-1}$ of these are needed to form one q^α-ic over $GF(p)$ belonging to a C_0 set and, hence, there are $R/q^{\alpha-1}$ q^α-ics belonging to C_0 sets. Since C_0 is of order $p(p^2-1)$ then the number K_0 of conjugate sets of order $p(p^2-1)$ is $R/q^{\alpha-1}p(p^2-1)$ Thus

THEOREM 4.6. *If $2<q<p$ and $q^r=(q^\alpha, p(p^2-1))\neq 1$ then the number K_0 of conjugate sets of order $p(p^2-1)$ is*

$$K_0 = \frac{1}{p(p^2-1)}\left[\frac{p^{q^\alpha}-p^{q^{\alpha-1}}}{q^\alpha} - \frac{p(p\mp 1)(q-1)(p^{q^{\alpha-1}}\pm 1)}{2q^\alpha}\right]$$

according as $q|(p\pm 1)$.

The total number $K=\sum_{i=0}^r K_i$ of conjugate sets is now readily obtainable by making use of Theorems 4.6, 4.4 and 4.5. Substituting and simplifying we have

$$K = \sum_{i=0}^{r} K_i = \frac{p^{q^\alpha}-p^{q^{\alpha-1}}}{q^\alpha p(p^2-1)} + \frac{(q-1)^2}{2(p\pm 1)q^\alpha}\cdot\sum_{i=1}^{r} q^{2i-2}(p^{q^{\alpha-i}}\pm 1)$$

according as $q|(p\pm 1)$.

REFERENCES

1. H. R. Brahana, *Metabelian groups of order p^{n+m} with commutator subgroup of order p^m*, Trans. Amer. Math. Soc. **34** (1934), 776–792.

2. L. E. Dickson, *An invariant investigation of irreducible binary modular forms*, Trans. Amer. Math. Soc. **12** (1911), 1–18.

3. ———, *Linear groups*, Teubner, Leipzig, 1901.

4. C. B. Hanneken, *Irreducible congruences over GF(p)*, Proc. Amer. Math. Soc. **10** (1959), 18–26. MR **21** #4130.

5. ———, *Polynomial subrings of matrices and the linear fractional group* (submitted).

MARQUETTE UNIVERSITY,
MILWAUKEE, WISCONSIN 53233