TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 193, 1974

IRREDUCIBLE CONGRUENCES OVER $GF(2)$ (1)

BY

C. B. HANNEKEN

ABSTRACT. In characterizing and determining the number of conjugate sets of irreducible congruences of degree m belonging to $GF(p)$ relative to the group $G(p)$ of linear fractional transformations with coefficients belonging to the same field, the case $p = 2$ has been consistently excluded from considerations. In this paper we consider the special case $p = 2$ and determine the number of conjugate sets of m-ic congruences belonging to $GF(2)$ relative to $G(2)$.

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 the prime p under the group 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 $\pi_m(J, K)$ [2]. In this classification and in the various studies of conjugate sets that have followed, the most recent being that for which the degree m is a power of an odd prime [3], the case $p = 2$ has been excluded as a possible characteristic for the base field $GF(p)$ because of the special considerations and treatments that would have been required. In this paper we consider this special case and therefore determine the number of conjugate sets of m-ic congruences over $GF(2)$ relative to $G(2) = G$.

For convenience we shall henceforth use p rather than 2 for the characteristic 2 of our fields and we shall use the standard notation $IQ[m, p^k]$ for an irreducible monic congruence of degree m over $GF(p^k)$. $GF'(p^k)$ will denote the subset of marks of $GF(p^k)$ which do not belong to any proper subfield and an m-ic over $GF'(p^k)$ will be regarded as a monic congruence of degree m over $GF(p^k)$ with at

Received by the editors September 13, 1972.

AMS (MOS) subject classifications (1970). Primary 12C05; Secondary 12E05, 12C30.

Key words and phrases. Congruences, conjugate sets, transform of an m-ic congruence, conjugate under G, self-conjugate, mark of $GF(p^k)$, irreducible and reducible congruences.

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

least one coefficient belonging to $GF'(p^k)$. We shall use $\{IQ[m, p^k]\}^{p^j}$ or $\{f(x)\}^{p^j}$ to denote the congruence of degree m whose coefficients are respectively the p^jth powers of those of $IQ[m, p^k] = f(x)$. $\{IQ[m, p^k]\}^{p^j + p^w}$ will mean the product of $\{f(x)\}^{p^j}$ and $\{f(x)\}^{p^w}$.

For $p = 2$ the group $G = G(2)$ is of order $p(p^2 - 1) = 6$ and may be easily recognized as the substitution group on three letters. If $T \in G$ is given by (1.2) then we shall say that T is identified by the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and that this matrix defines T. We will find it convenient to identify the transformations of G by the six nonsingular 2×2 matrices over $GF(2)$ given as follows:

$$(1.3) \qquad G: \quad \begin{array}{ll} I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & L = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \\ K = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, & \overline{L} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ K^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, & \overline{\overline{L}} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = LK^2. \end{array}$$

Clearly the order of K, $o(K) = 3$; $o(L) = o(\overline{L}) = o(\overline{\overline{L}}) = 2$ and the generators K and L of G satisfy the condition $KLK = L$.

Finally, if $f(x)$ is an $IQ[m, p^k]$ and $T \in G$ then $f(x)T = f'(x)$ will be called the transform of $f(x)$ by T and is the monic polynomial congruence in x obtained from $f((ax + b)/(cx + d))$. The set $\{f(x)T\colon T \in G\}$ is called a conjugate set relative to G and the members of the set are said to be conjugate. If $f(x)T = f(x)$ then $f(x)$ is said to be self-conjugate under T. If η is a root of a congruence $f(x)$ over $GF(p^k)$ and if $T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ then $\eta T = (a\eta + b)/(c\eta + d)$ is called the transform of η by T. Clearly $\eta^{p^i}T = (\eta T)^{p^i}$ for all $i \geq 0$.

Since $o(G) = 6$ then the orders of conjugate sets of m-ics are of the form $6/d$ where $d|m$. Thus, conjugate sets may be of order 6, 3, 2 or 1. To determine the number of conjugate sets of each possible order we consider separately the number of order 1, 2 and 3. In §2 we show that there can be no set of order 1 if $m > 2$ and the numbers C_2 and C_3 of sets of order 2 and 3 are considered in §3 and §4, respectively. The number C_6 of order 6 is the easily determined from the total number of irreducible m-ics over $GF(p)$.

2. Conjugate sets of order 1. If $m = 2$ then $x^2 + x + 1 = IQ[2, p]$ is the only irreducible congruence and necessarily belongs to a set of order 1. It is, therefore, invariant under G.

If $m > 2$ and if $f(x) = IQ[m, p]$ belongs to a conjugate set of order 1, then $f(x)T = f(x)$ for every $T \in G$ and it follows that $m = 6k$ for some $k \geq 1$. Thus, $f(x)$ is the product of k distinct $IQ[6, p^k]$, each of which is self-conjugate under every transformation $T \in G$ [1, p. 33]. If $s(x)$ denotes one of these factors, then

$$f(x) = \prod_{i=0}^{5} \{s(x)\}^{p^i};$$

and, if μ is a root of $s(x)$, then its roots are

$$\mu, \quad \mu^{p^k}, \quad \mu^{p^{2k}}, \quad \mu^{p^{3k}}, \quad \mu^{p^{4k}}, \quad \mu^{p^{5k}}.$$

Since $s(x)$ is irreducible over $GF(p^k)$, these roots are all distinct and belong to $GF'(p^{6k})$.

Now this irreducible sextic $s(x)$ over $GF(p^k)$ is the product of two cubics $c_1(x)$ and $c_2(x) = \{c_1(x)\}^{p^3}$, each irreducible over $GF(p^{2k})$ and self-conjugate under K, the transformation of G of order 3 given by (1.3). The roots of these two cubics are

$$\mu, \quad \mu^{p^{2k}}, \quad \mu^{p^{4k}} \quad \text{and} \quad \mu^{p^k}, \quad \mu^{p^{3k}}, \quad \mu^{p^{5k}},$$

respectively. Now, since $s(x)$ is self-conjugate under G, $s(x)L = s(x)$ implies that $c_1(x)L = c_2(x)$ and we conclude that $\mu L = \mu^{p^{3k}}$ since $o(L) = 2$. We may assume that $\mu K = \mu^{p^{2k}}$. Then, since $\overline{L} = LT$, we have

$$\mu\overline{L} = \mu(LT) = (\mu T)\,L = \mu^{p^{2k}}L = \mu^{p^{5k}}$$

and, since $o(\overline{L}) = 2$, it follows that

$$\mu = \mu\overline{L}^2 = (\mu\overline{L})\overline{L} = (\mu^{p^{5k}})\overline{L} = \mu^{p^{10k}} = \mu^{p^{4k}}$$

since $\mu^{p^{6k}} = \mu$. Thus $\mu = \mu^{p^{2k}}$, which implies that $\mu \in GF(p^{2k})$ and hence that $s(x)$ is reducible. Since $s(x)$ is irreducible we conclude that there exist no irreducible sextic over $GF(p^k)$ that is self-conjugate under G and hence no conjugate set of order 1. We state these results in

Theorem 2.1. *For $p = 2$ there exist no conjugate sets of irreducible m-ic congruences over $GF(p)$ of order 1 relative to G if $m > 2$ and only one set of order 1 if $m = 2$.*

3. Conjugate sets of order 2. Since there exist no $IQ[m, p]$ invariant under G then any $IQ[m, p] = f(x)$ that is self-conjugate under K must necessarily belong to a set of order 2 and $f(x)L = f'(x)$ will be the other m-ic belonging to the set. That $f'(x)$ is also self-conjugate under K is given by

Theorem 3.1. *Any $IQ[m, p] = f(x)$ that is self-conjugate under K belongs to a set of order 2 and $f(x)L$ is likewise self-conjugate under K.*

Proof. Suppose $IQ[m, p] = f(x)$ is self-conjugate under K and let $f'(x) = f(x)L$. Then $f(x) \not\equiv f'(x)$, for otherwise $f(x)$ would belong to a set of order 1. Now $f(x)K = f(x)$ implies that

$$f(x)KL = (f(x)K)L = f(x)L = f'(x)$$

and, since $KLK = L$,

$$f'(x)K = (f(x)KL)K = f(x)(KLK) = f(x)L = f'(x).$$

Thus $f'(x)$ is self-conjugate under K. Since

$$f(x)\overline{L} = f(x)(LK) = (f(x)L)K = f'(x)K = f'(x)$$

and

$$f(x)\overline{\overline{L}} = f(x)(LK^2) = f'(x)K^2 = (f'(x)K)K = f'(x)K = f'(x),$$

we conclude that $f(x)$ belongs to a set of order 2.

Now suppose that $f(x) = IQ[m, p]$ is self-conjugate under K. Then, since $3|m$, we have $m = 3^t k$, $(3, k) = 1$, $t \geq 1$ and $f(x)$ is the product of $s = 3^{t-1}k$ distinct irreducible cubics over $GF(p^s)$ [1, p. 33]

$$IQ[m, p] = f(x) = \prod_{i=0}^{s-1} \{c(x)\}^{p^i},$$

each cubic $\{c(x)\}^{p^i}$ of which is self-conjugate under K. It follows therefore that there exist an $IQ[m, p]$ that is self-conjugate under K and hence a conjugate set of order 2, provided there exist an irreducible cubic $c(x)$ over $GF(p^s)$ that is self-conjugate under K. The number of such cubics may then be used to determine the number of $IQ[m, p]$'s that are self-conjugate under K and, hence, the number of conjugate sets of order 2.

Suppose therefore that $c(x)$ is any cubic over $GF(p^s)$ (reducible or irreducible) that is self-conjugate under K. Then if μ is a root of $c(x)$ its roots are μ, μK, μK^2; and if we set $\alpha = \mu + \mu K + \mu K^2$ then

$$\alpha = \mu + \frac{\mu + 1}{\mu} + \frac{1}{\mu + 1} = \frac{\mu^3 + \mu + 1}{\mu^2 + \mu}. \tag{3.1}$$

Hence $\mu^3 + \alpha\mu^2 + (\alpha + 1)\mu + 1 = 0$, and we conclude that μ, μK, and μK^2 are roots of

$$c(x) = x^3 + \alpha x^2 + (\alpha + 1)x + 1. \tag{3.2}$$

Thus we have the following

Theorem 3.1. *Any cubic $c(x)$ over $GF(p^s)$ that is self-conjugate under $K = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ is of the form* (3.2) *where $\alpha \in GF(p^s)$. Conversely, any cubic over $GF(p^s)$ of the form* (3.2) *is self-conjugate under K.*

If $\alpha \in GF'(p^s)$ then the roots μ, $\mu K = (\mu + 1)/\mu$, and $\mu K^2 = 1/(\mu + 1)$ of $c(x)$ necessarily belong to $GF'(p^s)$ or $GF'(p^{3s})$, according as $c(x)$ is reducible or irreducible. If these roots are not distinct then $\mu = \mu K$, $\mu = \mu K^2$, or $\mu K = \mu K^2$ each implies that $\mu^2 + \mu + 1 = 0$, from which we conclude that $\mu \in GF'(p^2)$ since $x^2 + x + 1$ is the only irreducible quadratic over $GF(p)$. Thus, $s = 2 = 3^{t-1}k$ and hence $m = 3s = 6$. This gives

Theorem 3.2. *The roots μ, μK and μK^2 of the cubic $c(x)$ over $GF'(p^s)$ are all distinct if and only if $s \neq 2$.*

All m-ics whose degree $m = 3s$ is a multiple of 3 may now be considered by taking separately the three cases for s, namely, $s = 1$, $s = 2$, or $s > 2$.

Case $s = 3^{t-1}k = 1$. In this case we have $m = 3s = 3$, and the roots of the cubic $c(x) = x^3 + \alpha x^2 + (\alpha + 1)x + 1$ over $GF(p)$ are distinct. Since $o(GF(p)) = 2$ it follows that $c(x)$ is irreducible. Moreover, since there are exactly $(p^3 - p)/3 = (8 - 2)/3 = 2$ irreducible cubics over $GF(p)$ in all, they are identified by the choices $\alpha = 0$ and $\alpha = 1$ of $GF(p)$. Therefore we have

Theorem 3.3. *For $p = 2$ there exists one conjugate set of irreducible cubics over $GF(p)$ of order 2, and this set represents the only conjugate set of cubics over $GF(p)$.*

Case $s = 3^{t-1}k = 2$. In this case $m = 3s = 6$ and we have $\mu = \mu K = \mu K^2 \in GF'(p^2)$. This implies that $\alpha = \mu + \mu + \mu = \mu$ and identifies the reducible cubic $c(x) = x^3 + \mu x^2 + (\mu + 1)x + 1$ over $GF'(p^2)$. Moreover, $\mu^p = \mu + 1$, the only other mark of $GF'(p^2)$, likewise determines a reducible cubic, namely,

$$c'(x) = \{c(x)\}^p = x^3 + \mu^p x^2 + (\mu^p + 1)x + 1$$

which is also self-conjugate under K. Since $o(GF'(p^2)) = 2$, there are no irreducible cubics over $GF'(p^2)$ that are self-conjugate under K and hence no irreducible sextics over $GF(p)$ that are self-conjugate under K. Thus,

Theorem 3.4. *For $p = 2$ there exist no conjugate sets of irreducible sextics over $GF(p)$ of order 2 relative to $G = G(p)$.*

Case $s = 3^{t-1}k > 2$. For any choice of $\alpha \in GF'(p^s)$ the cubic $c(x)$ given by (3.2) may or may not be irreducible. If $S = o(GF'(p^s))$ then there are S distinct choices for α and hence this many cubics $c(x)$ over $GF'(p^s)$ that are self-conjugate under K. The number of irreducible ones may be obtained by deciding the number of choices for $\alpha \in GF'(p^s)$ that determine reducible ones.

Since $\alpha \in GF'(p^s)$, the roots μ, μK, μK^2 each belong to $GF'(p^s)$ or $GF'(p^{3s})$. Suppose $\mu \in GF'(p^s)$. Then μ, μK, μK^2 are distinct and, since each belongs to $GF'(p^s)$, they are roots of irreducible s-ics over $GF(p)$. Now their sum $\alpha = \mu + \mu K + \mu K^2$ is clearly a mark of $GF(p^s)$ and may or may not belong to $GF'(p^s)$. If $\alpha \notin GF'(p^s)$ then $\alpha \in GF'(p^r)$ where $GF(p^r)$ is a proper subfield of $GF(p^s)$. Then the cubic $c(x)$ defined by α is a cubic over $GF'(p^r)$ whose roots $\mu, \mu K, \mu K^2$ belong to $GF'(p^s)$. Therefore, $c(x)$ is an irreducible cubic over $GF'(p^r)$ and, since $\mu \in GF'(p^s)$, we have $r = s/3$. Thus, the marks of $GF'(p^s)$ that are roots of irreducible cubics over $GF'(p^{s/3})$ that are self-conjugate under K determine a mark α of $GF'(p^r)$ where $r = s/3$. Now if L_r is the number of irreducible cubics over $GF'(p^r)$ that are self-conjugate under K then the roots $\mu, \mu K, \mu K^2$ of any such cubic each belong to $GF'(p^s)$ and their sum $\alpha \in GF'(p^r)$. It follows that there are $3L_r$ distinct marks $\mu \in GF'(p^s)$ that identify an α in $GF'(p^r)$. Then the other marks μ of $GF'(p^s)$ determine an α belonging to $GF'(p^s)$. Since $S = o(GF'(p^s))$ there are $(S - 3L_r)/3$ distinct choices for α in $GF'(p^s)$ each determined by the set $\{\mu, \mu K, \mu K^2\}$. These α's determine cubics $c(x)$ over $GF'(p^s)$ whose roots belong to $GF'(p^s)$ and therefore are reducible cubics. Now any mark α of $GF'(p^s)$ not among this collection of $(S - 3L_r)/3$ distinct marks will determine a cubic $c(x)$ over $GF'(p^s)$ of the form (3.2) that is irreducible. There are therefore

$$L_{3r} = L_s = S - [(S - 3L_r)/3] = L_r + 2S/3$$

distinct irreducible cubics over $GF'(p^s)$ that are self-conjugate under K for each $r \geq 1$. Thus we have

Theorem 3.5. *For $p = 2$, if L_r is the number of irreducible cubics over $GF'(p^r)$ of the form* (3.2), $r = 1, 2, 3, \cdots$, *then there are*

$$L_{3r} = L_r + 2 \cdot o(GF'(p^{3r})/3 \tag{3.3}$$

distinct irreducible cubics over $GF'(p^{3r})$ of the form (3.2).

The numbers L_r and hence L_s, $s = 3r = 3^{t-1}k > 2$, $(3, k) = 1$, may now be determined by using the recursion formula (3.3) of the above theorem. First, we consider L_k where $k = 1$ and $k = 2$. Clearly, $L_1 = 2 = p$ since each irreducible cubic over $GF(p)$ is of the form (3.2). Then by (3.3) we have $L_{3\cdot 1} = L_1 + 2(p^3 - p)/3 = 2(p^3 + 1)/3$. Hence

$$L_{3^2\cdot 1} = L_{3\cdot 1} + 2 \cdot o(GF'(p^{3^2}))/3 = 2(p^{3^2} + 1)/3.$$

In general, we have

Lemma 3.1. *For $p = 2$ and $s = 3^{t-1}$, $t \geq 1$, the number L_s of irreducible cubics over $GF'(p^s)$ of the form* (3.2) (*i.e. self-conjugate under K*) *is given by*

$$L_s = 2(p^s + 1)/3. \tag{3.4}$$

Now for $k = 2$ we have $L_k = L_2 = 0$ since there exist no irreducible cubics over $GF'(p^2)$ of the form (3 . 2). Thus

$$L_{3\cdot 2} = L_2 + 2 \cdot o(GF'(p^{3\cdot 2}))/3 = 2(p^{3\cdot 2} - p^3 - p^2 + 1)/3$$

from which it follows that

$$L_{3^2\cdot 2} = L_{3\cdot 2} + 2\cdot o(GF'(p^{3^2\cdot 2}))/3$$
$$= L_{3\cdot 2} + 2(p^{3^2\cdot 2} - p^{3^2} - p^{3\cdot 2} + p^3)/3$$
$$= 2[p^{3^2\cdot 2} - p^{3^2} - p^2 + 1]/3.$$

In general, we have

Lemma 3.2. *For $p = 2$ and $s = 3^{t-1}\cdot 2$, $t > 1$, the number L_s of irreducible cubics over $GF'(p^s)$ of the form* (3.2) *is given by*

(3.5) $$L_s = 2[p^s - p^{s/2} - p^2 + 1]/3.$$

Finally, we determine the number L_k of irreducible cubics over $GF'(p^k)$ that are self-conjugate under K where $k > 2$ and $(3, k) = 1$. Any such cubic is of the form (3.2) where $\alpha \in GF'(p^k)$, and its roots $\mu, \mu K, \mu K^2$ are distinct and belong to $GF'(p^{3k})$. If we choose $\mu \in GF'(p^k)$ and set $\alpha = \mu + \mu K + \mu K^2$ then $\alpha \in GF'(p^k)$ or α belongs to a proper subfield of $GF(p^k)$, say $GF(p^{k'})$. If $\alpha \in GF'(p^{k'})$ then $k'|k$, and the cubic defined by α would be an irreducible cubic over $GF'(p^{k'})$, from which it follows that $3k' = k$ and hence that $3|k$. Since $(3, k) = 1$ we conclude that α cannot belong to a proper subfield of $GF(p^k)$, and hence that $\alpha \in GF'(p^k)$. Now, if we set $K_0 = o(GF'(p^k))$ then there are $K_0/3$ distinct values for $\alpha \in GF'(p^k)$ corresponding to the $K_0/3$ distinct subsets $\{\mu, \mu K, \mu K^2\}$ of $GF'(p^k)$ each of which identifies a reducible cubic over $GF'(p^k)$ of the form (3.2). Therefore, there are $K_0 - K_0/3 = 2K_0/3$ choices for α that determine irreducible ones. Thus we have

Lemma 3.3. *If $k > 2$, $(3, k) = 1$ and $K_0 = o(GF'(p^k))$ then $L_k = 2k_0/3$.*

This lemma along with the recursion formula (3.3) gives

Lemma 3.4. *If $k > 2$, $(3, k) = 1$ and $K_1 = o(GF'(p^{3k}))$ then $L_{3k} = 2(K_0 + K_1)/3$.*

In general, we have

Lemma 3.5. *For $p = 2$, if $s = 3^{t-1}k$ where $k > 2$, $t \geq 1$, $(3, k) = 1$, and if $K_i = o(GF'(p^{3^i k}))$ then*

(3.6) $$L_s = 2\left[\sum_{i=0}^{t-1} K_i\right]\Big/3.$$

Lemmas 3.1, 3.2 and 3.5 now give us the following important

Theorem 3.6. *If* $p = 2$ *and* $s = 3^{t-1}k > 2$ *where* $t \geq 1$ *and* $(3, k) = 1$, *then the number* L_s *of distinct irreducible cubics over* $GF'(p^s)$ *that are self-conjugate under* K *is given by*:

(a) $L_s = 2(p^s + 1)/3$,

(b) $L_s = 2(p^s - p^{s/2} - p^2 + 1)/3$, *or*

(c) $L_s = 2(\sum_{i=0}^{t-1} K_i)/3$, *where* $K_i = o(GF'(p^{3^i k}))$,

according as (a) $k = 1$, (b) $k = 2$, *or* (c) $k > 2$.

We may now determine the number of conjugate sets of irreducible m-ics of order 2 for $m = 3^t k$, where $t \geq 1$, $(3, k) = 1$ and $s = 3^{t-1}k$. First let us note that if $\alpha \in GF'(p^s)$ and determines the irreducible cubic $c(x) = x^3 + \alpha x^2 + (\alpha + 1)x + 1$, then $\alpha + 1 \in GF'(p^s)$ and determines the cubic $c'(x) = x^3 + (\alpha + 1)x^2 + \alpha x + 1$ which is likewise irreducible over $GF'(p^s)$ and self-conjugate under K. Moreover, these two cubics are conjugate since one may easily show that $c(x)L = c'(x)$, where $L = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Now if μ is a root of $c(x)$ then its roots are μ, $\mu K = \mu^{p^s}$, $\mu K^2 = \mu^{p^{2s}}$ and $\mu + 1$, $(\mu + 1)K = \mu^{p^s} + 1$, $(\mu + 1)K^2 = \mu^{p^{2s}} + 1$ are the roots of $c'(x)$. We conclude from this that no p^ith power of $c(x)$ can give us $c'(x)$. Hence it follows that

$$IQ[m, p] = \prod_{i=0}^{s-1} \{c(x)\}^{p^i} \quad \text{and} \quad IQ'[m, p] = \prod_{i=0}^{s-1} \{c'(x)\}^{p^i} = IQ[m, p]L$$

are distinct and constitute the irreducible m-ics over $GF(p)$ belonging to a set of order 2.

Since the s cubic factors of both $IQ[m, p]$ and $IQ'[m, p]$ are each irreducible cubics over $GF'(p^s)$ and of the form (3.2) it follows that there exist $L_s/2s$ distinct conjugate sets of m-ics of order 2 where $m = 3^t k$, $t > 0$, $s = 3^{t-1}k$, $(3, k) = 1$. Thus, since $m = 3s$ we have the following

Theorem 3.7. *If* $p = 2$ *and* $m = 3^t k$, *where* $t > 0$ *and* $(3, k) = 1$, *then the number* C_2 *of conjugate sets of* m*-ic congruences over* $GF(p)$ *of order* 2 *is given by*:

(a) $C_2 = (p^{m/3} + 1)/m$,

(b) $C_2 = (p^{m/3} - p^{m/6} - p^2 + 1)/m$, *or*

(c) $C_2 = (\sum_{i=0}^{t-1} K_i)/m$, $K_i = o(GF'(p^{3^i k}))$,

according as (a) $k = 1$, (b) $k = 2$ *and* $m \neq 6$, *or* (c) $k > 2$. *If* $m = 6$ *then* $C_2 = 0$.

4. Conjugate sets of order 3. Any conjugate set of order 3 must contain an $IQ[m, p]$ that is self-conjugate under $L = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Moreover, $2|m$, and hence m must be of the form $m = 2^t n$ where $(2, n) = 1$ and $t \geq 1$. In such a case the $IQ[m, p]$ is the product of $2^{t-1}n$ distinct irreducible quadratics $\{q(x)\}^{p^i}$, $i = 0, 1, 2, \cdots, (2^{t-1}n - 1)$, each of which is self-conjugate under L and hence of the form

$$q(x) = x^2 + x + \alpha, \quad \alpha \in GF'(p^{2^{t-1}n}). \tag{4.1}$$

Now let γ be a root of an $IQ[2, p^{2^{t-1}}] = Q(x)$ and without loss of generality suppose $Q(x)$ is of the form

$$Q(x) = x^2 + x + \beta, \quad \beta \in GF'(p^{2^{t-1}}). \tag{4.2}$$

Then the roots of $Q(x)$ are γ and $\gamma^{p^{2t-1}}$ and we have $\gamma + \gamma^{p^{2t-1}} = 1$ and $\gamma \cdot \gamma^{p^{2t-1}} = \beta$. Since $(2, n) = 1$ then any mark η of $GF'(p^{2^t n})$ is uniquely expressible in the form

$$\eta = \phi_1 + \phi_2 \gamma, \quad \phi_1, \phi_2 \in GF'(p^{2^{t-1}n}), \tag{4.3}$$

and if $\eta \in GF'(p^{2^t n})$ then η may be regarded as a root of an irreducible quadratic over $GF'(p^{2^{t-1}n})$.

Since $(2, n) = 1$ implies that $n = 2w + 1$ for some w and hence that $2^{t-1}n = 2^t w + 2^{t-1}$ then

$$\gamma^{p^{2^{t-1}n}} = \gamma^{p^{2^t w + 2^{t-1}}} = [\gamma^{p^{2^t w}}]^{p^{2^{t-1}}} = \gamma^{p^{2^{t-1}}}$$

and we have

$$\eta^{p^{2^{t-1}n}} = (\phi_1 + \phi_2)^{p^{2^{t-1}n}} = \phi_1 + \phi_2 \gamma^{p^{2^{t-1}n}} = \phi_1 + \phi_2 \gamma^{p^{2^{t-1}}}$$

since $\phi_1, \phi_2 \in GF(p^{2^{t-1}n})$.

Now if, in particular, $\eta = \phi_1 + \phi_2 \gamma$ is a root of an irreducible quadratic $q(x)$ of the form (4.1) then

$$\eta + \eta^{p^{2^{t-1}n}} = 1$$

implies that $(\phi_1 + \phi_2 \gamma) + (\phi_1 + \phi_2 \gamma^{p^{2t-1}}) = \phi_2(\gamma + \gamma^{p^{2t-1}}) = \phi_2 \cdot 1 = 1$ and hence that $\nu = \phi_1 + \gamma$. Conversely, if ν is any mark of $GF'(p^{2^t n})$ of the form $\eta = \phi + \gamma$ then η and hence $\eta^{p^{2t-1}n}$ are roots of an irreducible quadratic $q(x)$ over $GF'(p^{2^{t-1}n})$ and, since

$$\eta + \eta^{p^{2^{t-1}n}} = (\phi + \gamma) + (\phi + \gamma^{p^{2^{t-1}n}}) = 1,$$

then $q(x)$ is of the form (4.1) and hence self-conjugate under L. Thus we have

Theorem 4.1. *If $p = 2$ then a necessary and sufficient condition that $\eta = \phi_1 + \phi_2 \gamma$ be a root of an irreducible quadratic $q(x)$ over $GF'(p^{2^{t-1}n})$ that is self-conjugate under L is that $\eta \in GF'(p^{2^t n})$ and be of the form $\eta = \phi + \gamma$ where $\phi \in GF(p^{2^{t-1}n})$.*

Now if $\eta = \phi + \gamma \in GF'(p^{2^t n})$ is a root of $q(x) = x^2 + x + \beta$ then $q(x)L = q(x)$ implies that the roots of $q(x)$ are

$$\eta = \phi + \gamma \quad \text{and} \quad \eta^{p^{2^{t-1}n}} = \eta L = \eta + 1 = (\phi + 1) + \gamma.$$

Thus, if $\phi \in GF(p^{2^{t-1}n})$ defines the root η of the $IQ[2, p^{2^{t-1}n}] = q(x)$ and hence $q(x)$ itself then $\phi + 1$ will likewise define $q(x)$.

The number of conjugate sets of order 3 may now be obtained by determining the number of irreducible quadratics over $GF'(p^{2^{t-1}n})$ that are self-conjugate under L. To do this we must therefore determine the number of distinct marks $\phi \in GF(p^{2^{t-1}n})$ such that $\eta = \phi + \gamma$ belongs to $GF'(p^{2^t n})$. Since $\gamma \in GF'(p^{2^t})$ and since $GF(p^{2^{t-1}n}) \cap GF(p^{2^t}) = GF(p^{2^{t-1}})$ and $(2, n) = 1$ it readily follows that $\eta = \phi + \gamma \in GF'(p^{2^t n})$ if and only if ϕ is a root of any irreducible n-ic over $GF'(p^{2^{t-1}})$.(2) Thus, if $n = q_1^{r_1} \cdot q_2^{r_2} \cdots q_b^{r_b}$ is the standard form for n, then there are

$$(4.4) \qquad nN_{n, p^{2^{t-1}}} = p^{2^{t-1}n} - \sum p^{2^{t-1}n/q_i} + \sum p^{2^{t-1}n/(q_i q_j)} - \cdots$$

distinct choices for ϕ such that $\eta = \phi + \gamma \in GF'(p^{2^t n})$, where the sums Σ are taken for all combinations of the distinct prime factors of n in the numbers indicated [1, p. 18]. [Note that if $n = 1$ then this number given by (4.4) is $p^{2^{t-1}}$.]

Now, since two distinct choices of ϕ identify one quadratic and since $2^{t-1}n$ of these go together to determine one irreducible m-ic $(m = 2^t n)$ over $GF(p)$ that is self-conjugate under L and hence one set of order 3 then the number of sets of order 3 is easily determined. We state this result in the following

Theorem 4.2. *If $p = 2$ and $m = 2^t n$, where $t \geq 1$, $(2, n) = 1$ and if $n = q_1^{r_1} \cdot q_2^{r_2} \cdot \cdots \cdot q_b^{r_b} > 2$ then there exist*

$$C_3 = \left[p^{2^{t-1}n} - \sum p^{2^{t-1}n/q_i} + \sum p^{2^{t-1}n/q_i q_j} - \cdots \right] \Big/ m$$

distinct conjugate sets of irreducible m-ic congruences over $GF(p)$ of order 3. If $n = 1$ then the number of conjugate sets of order 3 is $C_3 = [p^{2^{t-1}}]/m = 2^{2^{t-1}-t}$.

The number of conjugate sets of order 6, say C_6, is now easily determined and is given by the following

---

(2) In fact, if ϕ is a root of an irreducible n-ic over $GF(p)$ then since $\gamma \in GF'(p^{2^t n})$ it is clear that $\eta = \phi + \gamma$ belongs to $GF'(p^{2^t n})$.

Theorem 4.3. *If $p = 2$ then the number of conjugate sets of order 6 is given by $C_6 = [N_{m,p} - 2C_2 - 3C_3]/6$ where C_2 and C_3 are the numbers of sets of order 2 and 3 respectively and $N_{m,p}$ is the total number of irreducible m-ics over $GF(p)$ (see [1, p. 18]).*

BIBLIOGRAPHY

1. L. E. Dickson, *Linear groups*, Teubner, Leipzig, 1901.
2. C. B. Hanneken, *Irreducible congruences over GF(p)*, Proc. Amer. Math. Soc. 10 (1959), 18–26. MR 21 #4130.
3. ———, *Irreducible congruences of prime power degree*, Trans. Amer. Math. Soc. 153 (1971), 167–179. MR 43 #185.

DEPARTMENT OF MATHEMATICS, MARQUETTE UNIVERSITY, MILWAUKEE, WISCONSIN 53233