IRREDUCIBLE CONGRUENCES OVER $GF(p)$

C. B. HANNEKEN

1. **Introduction.** In this paper we shall classify the irreducible m-ic congruences

$$C_m(z) = z^m + a_1 z^{m-1} + \cdots + a_{m-1} z + a_m \equiv 0 \pmod{p} \tag{1.1}$$

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

$$T\colon z = (az' + b)/(cz' + d) \tag{1.2}$$

with coefficients belonging to the same field. Two irreducible m-ic congruences are said to belong to the same conjugate set if one of them can be transformed into the other by a transformation of G. The number of distinct irreducible congruences in a conjugate set will be referred to as the order of the conjugate set. Since the order of the group G is $p(p^2-1)$, it follows that the order of any conjugate set will be at most $p(p^2-1)$.

A classification of the irreducible binary modular forms under the group of all binary linear homogeneous transformations of determinant unity in the field $GF(p^n)$ has been done by Dickson[**4**]. Since an irreducible binary modular form over $GF(p)$ of degree m in x and y defines an irreducible m-ic congruence $C(z)$ over $GF(p)$ with roots $\lambda^{p^i} = (x/y)^{p^i}$, $(i=0, 1, 2, \cdots, m-1)$, in the Galois field $GF(p^m)$, it follows that Dickson's results provide a classification of the irreducible m-ic congruences over $GF(p)$ under the subgroup G' of transformations of G with determinant a square in $GF(p)$. Clearly, G' is a proper subgroup of G if $p>2$, and a conjugate set C under the group G will consist of, at most, two conjugate sets C_1', C_2' under the smaller group G', i.e., $C = C_1' \cup C_2'$. It is shown in §2 that if $\sigma_1 \in GF(p^m)$ characterizes the set C_1' under G', then $-\sigma_1$ will characterize the set C_2' under G' and σ_1^2 will characterize the conjugate set C under the group G.

In studying the irreducible binary modular forms over $GF(p^n)$, Dickson lists two relative invariants, namely,

$$Q = (x^{p^{2n}-1} - y^{p^{2n}-1})/(x^{p^n-1} - y^{p^n-1}),$$

and

$$L = x^{p^n} y - x y^{p^n}.$$

Received by the editors March 29, 1958.

It is also shown in this paper that the invariant π_m $(m>2)$ is an absolute invariant under the group $\overline{G}$ of all binary transformations in $GF(p^n)$, and that π_m is expressible homogeneously in terms of J and K, where

$$(1.3) \qquad J = Q^{p^n+1} = q^r, \quad \text{and} \quad K = L^{p^n(p^n-1)} = l^r,$$

and where $r=1$ if $p=2$, $r=2$ if $p>2$. The above invariants are invariants under the group G provided $n=1$ and, hence, may be applied directly in our problem.

The recursion formula

$$(1.4) \qquad F_t = QF_{t-1}^{p^n} - KF_{t-2}^{p^{2n}} \qquad (F_1 = 1, F_2 = Q)$$

given by Dickson and the fact that

$$(1.5) \qquad \pi_m = \frac{F_m \pi F_{m/q_iq_j} \pi F_{m/q_iq_jq_kq_l} \cdots}{\pi F_{m/q_i} \pi F_{m/q_iq_jq_k} \cdots}$$

where $m = q_1^{\alpha_1} q_2^{\alpha_2} q_3^{\alpha_3} \cdots q_u^{\alpha_u}$ and where $q_1, \cdots, q_u$ are distinct prime factors >1 of m make it possible to express π_m explicitly as a function of J and K for any degree m.

The need for such a classification as that given in this paper arises in the study of the metabelian subgroups in the holomorph of an Abelian group of order p^s and type $1, 1, \cdots$ each having commutator subgroup of order p^m.[1] A classification of the irreducible m-ic congruences over $GF(p^n)$ under the group $\overline{G}$ of linear fractional transformations with coefficients in $GF(p^n)$ may be obtained by generalizing the results of this paper. Since the group problem does not require such a generalization, and since such a generalization would be quite simple to make, we do not offer it in this paper. Consequently, we make use of a special case of Dickson's results; namely, that where $n=1$. Furthermore, if $n=1$, $p=2$, then $G=G'$ and Dickson's classification applies directly, hence, in the sequel we restrict p to be greater than 2.

In §4 we make use of the previous results for the cases $m=2, 3, \cdots, 7$. Although classifications relative to G of the irreducible m-ic congruences for $m=3, 4, 5, 6$ have been done, it seems in order here to show how easily this may be done with the techniques of this paper. In §5 we devote a detailed discussion to the special case for $m=8$.

[1] For a connection between the two problems see Brahana, *Metabelian groups of order p^{n+m} with commutator subgroup p^m*, Trans. Amer. Math. Soc. vol. 34 (1934) pp. 776–792.

2. **A characterization of conjugate sets under** G. Since in (1.3) $r=2$ if $p>2$, it follows that one may express $\pi_m(J, K)$ given by (1.5) and (1.4) in terms of q and l. Corresponding to each irreducible factor Γ_r of degree r over $GF(p)$ of $\pi_m(J, K)$ is a factor γ_{2r} of degree $2r$ of $\pi_m(q, l)$. This factor is factorable over $GF(p)$ into two irreducible factors $\gamma_r^{(1)}$ and $\gamma_r^{(2)}$ each of degree r or is irreducible of degree $2r$ over $GF(p)$ according as the root $\pi = J/K$ of Γ_r is a square or a non-square in $GF(p^r)$. If γ_{2r} is factorable and θ is a root of $\gamma_r^{(1)}$, then $-\theta$ is a root of $\gamma_r^{(2)}$. If γ_{2r} is irreducible and θ is a root, then $-\theta$ is also a root. Conversely, corresponding to any two roots ξ and $-\xi$ of $\pi_m(q, l)$ is an irreducible factor of $\pi_m(J, K)$.

In deciding whether or not two binary forms ϕ_1 and ϕ_2 are conjugate relative to G', Dickson shows that one may employ a root $\mu_1 = x/y$ of $\phi_1 \equiv 0$ and a root $\mu_2 = x/y$ of $\phi_2 \equiv 0$ and determine corresponding values of $\sigma_1 = q_1/l_1$ and $\sigma_2 = q_2/l_2$ for μ_1 and μ_2, respectively. According as these values σ_1 and σ_2 are roots of the same irreducible factor or different irreducible factors of $\pi_m(q, l)$ the given forms ϕ_1 and ϕ_2 belong to the same or different conjugate sets.

Let $C_{\mu_1}(z)$ and $C_{\mu_2}(z)$ be the two irreducible m-ic congruences defined by $\phi_1(x, y)$ and $\phi_2(x, y)$, respectively. Since μ_1 and μ_2 are roots of $C_{\mu_1}(z)$ and $C_{\mu_2}(z)$, respectively, we have, by making use of (1.3) and the fact that $z = x/y$, the following important result:

$$(1.6)\qquad \begin{aligned} (J/K)_i = (q_i/l_i)^2 = \sigma_i^2 = \pi\mu_i &= \frac{(\mu_i^{p^2} - \mu_i)(\mu_i^{p} - \mu_i^{p^3})}{(\mu_i^{p^2} - \mu_i^{p^3})(\mu_i^{p} - \mu_i)} \\ &= (\mu_i^{p^2}\mu_i^{p}, \mu_i\mu_i^{p^3}), \qquad (i = 1, 2). \end{aligned}$$

If $C_{\mu_1}(z)$ and $C_{\mu_2}(z)$ are conjugate under G and if $\mu_1 T = \mu_2$ for $T \in G$, then, since the cross ratio π is an invariant under G, we have $\sigma_1^2 = \sigma_2^2$. If, further, $C_{\mu_1}(z)$ and $C_{\mu_2}(z)$ are not conjugate under G', then σ_1 and σ_2 are not roots of the same irreducible factor of $\pi_m(q, l)$ and $\sigma_1 \neq \sigma_2$. It follows since $\sigma_1^2 = \sigma_2^2$ that $\sigma_1 = -\sigma_2$, and that σ_1 and σ_2 are roots of $\gamma_r^{(1)}$ and $\gamma_r^{(2)}$, respectively.

Since any conjugate set under G consists of, at most, two distinct conjugate sets under G', and since there are as many conjugate sets of irreducible m-ic congruences under G' as there are distinct irreducible factors of $\pi_m(q, l)$, we have along with the above results the following:

THEOREM 2.1. *There are as many distinct conjugate sets of irreducible m-ic congruences over $GF(p)$ under the group G of linear fractional trans-*

formations with coefficients in $GF(p)$ as there are distinct irreducible factors over $GF(p)$ of the invariant $\pi_m(K, L)$.

Since the corresponding value $\sigma_\mu = q/l$ of a root μ of an irreducible m-ic $C_\mu(z)$ is a root of $\pi_m(q, l)$ and is in $GF(p^m)$ and, conversely, since any root $\sigma_\mu = q/l$ of $\pi_m(q, l)$ defines an irreducible m-ic congruence having a root μ whose corresponding value of q/l is equal to σ_μ, it follows that any root $\pi = J/K$ of $\pi_m(J, K)$ will define an irreducible m-ic congruence $C_\mu(z)$ having a root μ such that

$$\pi_\mu = (\mu^{p^2}\mu^p, \mu\mu^{p^3}). \tag{1.7}$$

Conversely, the cross ratio $\pi_\mu = (\mu^{p^2}\mu^p, \mu\mu^{p^3})$ of the roots $\mu, \mu^p, \cdots, \mu^{p^{m-1}}$ of an irreducible m-ic $C_\mu(z)$ will be a root of an irreducible factor of $\pi_m(K, L)$. This gives the following:

THEOREM 2.2. *Two irreducible m-ic congruences $C_{\mu_1}(z)$ and $C_{\mu_2}(z)$ having roots μ_1 and μ_2, respectively, are conjugate under G if, and only if, the corresponding cross ratios π_{μ_1} and π_{μ_2} as defined by* (1.6) *are roots of the same irreducible polynomial over $GF(p)$.*

Since the value $\sigma = q/l$ for a root $\mu = x/y$ of an irreducible binary form $\phi(x, y)$ belongs to $GF(p^m)$ and since $\pi_\mu = \sigma^2$, it follows that any irreducible factor Γ_r of $\pi_m(J, K)$ is of degree m or a divisor of m, i.e., $r \mid m$. If the root $\pi_\mu = J/K$ of Γ_r is a square in $GF(p^r)$, then Γ_r defines two distinct irreducible factors $\gamma_r^{(1)}$ and $\gamma_r^{(2)}$ of $\pi_m(q, l)$. These factors each define distinct conjugate sets relative to G'. Hence, in this case the conjugate set defined by Γ_r under G splits into two distinct ones relative to G'. If, however, π_μ is a nonsquare in $GF(p^r)$, then the corresponding factor γ_{2r} of $\pi_m(q, l)$ is irreducible over $GF(p)$ and the corresponding conjugate set defined by Γ_r does not split into two distinct sets relative to G'. This gives the following:

THEOREM 2.3. *Let S be a conjugate set of irreducible m-ic congruences over $FG(p)$ under the group G of all linear fractional transformations with coefficients belonging to $GF(p)$ and let $C_\mu(z)$ having a root μ be any congruence belonging to S. Let the cross ratio $\pi_\mu = (\mu^{p^2}\mu^p, \mu\mu^{p^3})$ be a root of the irreducible polynomial Γ_r of degree r over $GF(p)$. Then S will split into two distinct conjugate sets under the subgroup G' of all transformations of G whose determinant is a square if, and only if, the mark π_μ of $GF(p^r)$ is a square in $GF(p^r)$.*

As a direct result of this theorem we see that if π_μ is a nonsquare of $GF(p^r)$ then $2r \mid m$ since the degrees of the irreducible factors of $\pi_m(q, l)$ must divide m. Hence, m must be even. Conversely, if m is odd, then every root of $\pi_m(K, L)$ must be a square. This along with Theorem 2.3 gives

THEOREM 2.4. *If m is an odd degree, then every conjugate set S relative to G splits into two distinct conjugate sets relative to G' and the number of distinct conjugate sets relative to G is one-half the number relative to G'.*

3. **Number of conjugate sets of a given order relative to G.** Since the group G is of order $p(p^2-1)$ it follows that any conjugate set S will have order at most $p(p^2-1)$. If S contains less than $p(p^2-1)$ distinct m-ics, then there exist transformations of G that carry each m-ic into itself. Such transformations must be of order d where $d|m$. If d is the largest order of a transformation that carries an m-ic into itself, then S must be of order $p(p^2-1)/d$. Let $m=r\cdot d$ and S be a conjugate set of order $p(p^2-1)/d$ containing $S_\mu(z)$. Then there exists a transformation $T\in G$ of order d that transforms $S_\mu(z)$ into itself and, hence, $\mu\cdot T=\mu^{p^r}$, $\mu^p\cdot T=\mu^{p^{r+1}}$, $\cdots$. By making use of (1.6) we see that

$$(3.1) \qquad \pi_\mu = \pi_{\mu^{p^r}} = (\mu^{p^{r+2}}\mu^{p^{r+1}}, \mu^{p^r}\mu^{p^{r+3}}) = (\mu^{p^2}\cdot T\mu^p\cdot T, \mu\cdot T\mu^{p^3}\cdot T).$$

Hence, $\pi_\mu\in GF(p^r)\subset GF(p^m)$ and is a root of an irreducible polynomial of degree r over $GF(p)$. This gives

THEOREM 3.1. *If $m=rd$, then the irreducible factors of $\pi_m(K, L)$ of degree r define distinct conjugate sets of order $p(p^2-1)/d$. Conversely, the conjugate sets of order $p(p^2-1)/d$ are defined by the irreducible factors of $\pi_m(K, L)$ of degree r.*

4. **Number of conjugate sets of irreducible m-ics for $m=3, 4, \cdots, 7$.** Clearly, if $m=1$, 2 the m-ic congruences are all conjugate relative to G. For $m=3$ we see by Theorem 2.3 that there exists only one conjugate set relative to G since there are in all exactly two conjugate sets relative to G'. This is in accordance with Brahana's *On cubic congruences* [1].

For $m=4$ we have $\pi_4=J^p-J^{p-1}K-K^p$ Dickson [4]. Setting $t=J/K$ we see that π_4 vanishes only if $t^p-t^{p-1}-1\equiv 0 \bmod p$. From this we see that $t^p=t/(t-1)$ and $t^{p^2}=t^p/(t^p-1)=t$. Hence, any root of π_4 must be in $GF(p^2)$, and the irreducible factors of π_4 must be of degree at most two. If $t\in GF(p)$ then the only root of π_4 is $t=2$. Since π_4 is of degree p the irreducible factors of π_4 consist of one linear and $(p-1)/2$ quadratic factors. This along with Theorem 3.1 gives

THEOREM 4.1. *The irreducible quartic congruences belonging to $GF(p)$ constitute $(p+1)/2$ conjugate sets under G of which there are*

$(p-1)/2$ conjugate sets of order $p(p^2-1)/2$ and exactly one of order $p(p^2-1)/4$.

The above theorem is in accordance with Brahana's, *Note on irreducible quartic congruences* [2]. Furthermore, we might add that if $p=7$, then $\pi_4=(t-2)(t^2+5t+2)(t^2+2t+5)(t^2+t+6)$.

For $m=5$ we have $\pi_5=J^{p^2+1}-J^{p^2}K-J^{p^2-p+1}K^p+K^{p^2+1}$, which vanishes for $t=J/K$ if

$$t^{p^2+1} - t^{p^2} - t^{p^2-p+1} - t + 1 \equiv 0 \pmod{p}. \tag{4.1}$$

A root t of (4.1) is either in $GF(p)$ or $GF(p^5)$. If $t \in GF(p)$ then (4.1) vanishes if t satisfies

$$t^2 - 3t + 1 \equiv 0 \pmod{p}. \tag{4.2}$$

If $p=5$, then $t=-1$ is a double root of (4.2) and it follows that there exist only one distinct linear factor and exactly $p^2/5=5$ irreducible fifth degree factors of π_5. If $p=5K\pm 2$ then (4.2) is irreducible, hence, there are no linear factors. If $p=5K\pm 1$ then (4.2) is factorable into two distinct linear factors. In this case π_5 factors into two linear factors and $(p^2-1)/5$ irreducible fifth degree factors. Using Theorem 3.1 with the above results gives

THEOREM 4.2. *The irreducible quintic congruences belonging to $GF(p)$ constitute* 6, $(p^2+9)/5$, $(p^2+1)/5$ *distinct conjugate sets under G according as $p=5$, $p=5K\pm 1$, $p=5K\pm 2$.*

The above theorem is in accordance with C. B. Hanneken's, *Irreducible quintic congruences*, [5].

For $m=6$ we have

$$\pi_6 = J^{p^3+p-1} - J^{p^3-p^2+p-1}K^{p^2} - J^{p-1}K^{p^3} - K^p\left(\frac{J^{p^3}-K^{p^3}}{J-K}\right),$$

which vanishes for $t=J/K$ if

$$t^{p^3+p-1} - t^{p^3-p^2+p-1} - t^{p-1} - \frac{t^{p^3}-1}{t-1} \equiv 0 \pmod{p}. \tag{4.3}$$

$t=1$ is not a root of (4.3) and for $p=2$ or 3, there is no root in $GF(p)$, while for $p>3$ the only root is $t=3$. The roots t of (4.3) that belong to the subfield $GF(p^2)$ must be roots of the irreducible quadratics over $GF(p)$ of the form $t^2+t(s-1)+s^2\equiv 0 \pmod{p}$, where $s\in GF(p)$, and, conversely, any root of this irreducible quadratic is a root of (4.3). It follows that there are $(p-3)/2$ irreducible quadratic factors of π_6 if $p=6K+5$, and $(p-1)/2$ if $p=3$ or $p=6K+1$.

Corresponding to each of these factors is a conjugate set of order $p(p^2-1)/3$.

The roots of (4.3) that belong to $GF(p^3)$ must satisfy the equation

$$\frac{1}{t}+\frac{1}{t^p}+\frac{1}{t^{p^2}}=1. \tag{4.4}$$

Conversely, any root of (4.4) belongs to $GF(p^3)$ and, except for $t=3$, does not belong to $GF(p)$. It follows that the irreducible cubic factors of π_6 are of the form $\rho^3-\rho^2+\cdots$, where $\rho=1/t$, and their number is 3 if $p=3$ or $(p^2-1)/3$ if $p>3$.

Since the degree of (4.3) is p^3+p-1, it follows that the number of sixth degree factors of π_6 is $(p^3-p^2+2)/6$ for $p=6K-1$ and $(p^3-p^2)/6$ for $p=3$ or $p=6K+1$. Corresponding to each of these factors is a conjugate set of order $p(p^2-1)$. This gives

THEOREM 4.3. *The irreducible sextic congruences belonging to $GF(p)$ constitute $(p^3+p^2+3p+1)/6$ distinct conjugate sets under G if $p=6K+1$, and $(p^3+p^2+3p-3)/6$ conjugate sets if $p=6K-1$ or $p=3$.*

The above theorem is in accordance with C. B. Hanneken's, *Irreducible sextic congruences*, [6].

For $m=7$ we may use Theorem 2.3 along with the number of classes of irreducible septic forms relative to the subgroup G' of G and obtain

THEOREM 4.4. *The irreducible septic congruences over $GF(p)$ constitute* 351, $(p^4+p^2+19)/7$, $(p^4+p^2+1)/7$ *conjugate sets according as $p=7$, $p=7K\pm1$ or $p\neq 7K\pm1$.*

5. **A classification of the irreducible octic congruences.** For the irreducible octic congruences we find by making use of (1.4) and (1.5) that

$$\pi_8=(J-K)^{p^6+p^3}-J^{p^6-p^4+p^3}K^{p^4}-(J-K)^{p^3-p^2+p-1}K^{p^2}\pi_4^{p^4-1}. \tag{5.1}$$

Setting $J=\rho K$ we see that π_8 vanishes if ρ satisfies

$$(\rho-1)^{p^6+p^3}-\rho^{p^6-p^4+p^3}-(\rho-1)^{p^3-p^2+p-1}\cdot\frac{(\rho-1)^{p^6}-\rho^{p^6-p^4}}{(\rho-1)^p-\rho^{p-1}}\equiv 0 \pmod{p}. \tag{5.2}$$

The irreducible factors of (5.1) are of degree 1, 2, 4, or 8. To determine the number of factors of each of these degrees we use the fact that $\rho\in GF(p^8)$. We shall first determine the number of factors of degree 4 or less. If $\rho \in GF(p^4)$, then $\rho^{p^4} = \rho$ and we see that ρ must satisfy the following relation:

$$\begin{aligned}(5.3)\quad \rho^{p^3+p^2+p+1} - \rho^{p^2+p+1} - \rho^{p^3+p^2+1} - \rho^{p^2+1} - \rho^{p^3+p^2+p} \\ - \rho^{p^3+p+1} + \rho^{p^3+p} \equiv 0 \pmod{p}.\end{aligned}$$

Setting $\lambda = 1/\rho$, multiplying by $\lambda^{p^3+p^2+p+1}$, and simplifying we obtain

$$(5.4)\qquad 1 - (\lambda + \lambda^p + \lambda^{p^2} + \lambda^{p^3}) + \lambda\lambda^{p^2} + (\lambda\lambda^{p^2}) \equiv 0 \pmod{p}.$$

Clearly, any solution λ of (5.4) will define a solution ρ of (5.3).

Let μ be a fixed nonsquare of $GF(p^2)$ not in $GF(p)$. Then any mark of $GF(p^4)$ is of the form $\lambda = A + B\mu^{1/2}$, where A, B are marks of $GF(p^2)$. It follows that $\lambda^{p^2} = A - B\mu^{1/2}$, $\lambda + \lambda^{p^2} = 2A$, $\lambda\lambda^{p^2} = A^2 - B^2\mu$ and upon substitution into (5.4) we have after simpliyfing

$$(5.5)\qquad [(A-1)^2 - B^2\mu] + [(A-1)^2 - B^2\mu]^p = 1.$$

Since A, B, $\mu \in GF(p^2)$, then $(A-1)^2 - B^2\mu = \xi \in GF(p^2)$, and $\xi = \gamma_1 + \gamma_2\delta^{1/2}$, where γ_1, $\gamma_2 \in GF(p)$ and δ is a nonsquare of $GF(p)$. (5.5) then gives $\xi + \xi^p = 1$ which implies that $\gamma_1 = 1/2$. From this it follows that

$$(5.6)\qquad (A-1)^2 - B^2\mu = 1/2 + \gamma_2\delta^{1/2},$$

where, of course, $\gamma_2 \in GF(p)$. Since μ is a nonsquare, and since γ_2 may assume any one of p different values of $GF(p)$, it follows that there exist $p(p^2+1)$ distinct sets (A, B) satisfying (5.5). If $B \neq 0$, then λ is a root of an irreducible quartic, and, hence, defines an irreducible quartic factor of π_8. If $B = 0$, then $\lambda \in GF(p^2)$ and will define a linear factor of π_8 or a quadratic factor of π_8 according as $\lambda \in GF(p)$ or $\lambda \notin GF(p)$. To determine the number of such factors we set $B = 0$ in (5.5), thus obtaining

$$(5.7)\qquad (A-1)^2 + (A-1)^{2p} = 1.$$

Setting $A = a + b\delta^{1/2}$, a, $b \in GF(p)$, into (5.7) and simplifying, we obtain

$$(5.8)\qquad (a-1)^2 + \delta b^2 = 1/2.$$

Since -1 is a square or a nonsquare according as p is of the form $4K+1$ or $4K-1$, we have

LEMMA 5.1. (a) *If $p = 4K+1$, then there are $p+1$ solutions (a, b) of* (5.8); (b) *If $p = 4K-1$, then there are $p-1$ solutions (a, b) of the Equation* (5.8).

Each of these solutions (a, b) will define $A \in GF(p^2)$ satisfying

(5.7). Since there are $p(p^2+1)$ distinct solutions (A, B) satisfying (5.5), the following theorem is immediate:

THEOREM 5.1. (a) *If* $p=4K+1$, *then there exist* $[p(p^2+1)-(p+1)]/4 = [p^3-1]/4$ *distinct irreducible quartic factors of* π_8;

(b) *If* $p=4K-1$, *then there exist* $[p(p^2+1)-(p-1)]/4=[p^3+1]/4$ *distinct irreducible quartic factors of* π_8.

To determine the number of irreducible quadratic factors of π_8 we turn to the solutions (a, b) of (5.8). Clearly, $b\neq 0$ unless 2 is a square. If $b=0$, then $\lambda\in GF(p)$ and will define a linear factor of π_8. The mark 2 is a square or a nonsquare according as $p=8K\pm 1$, or $p=8K\pm 3$. This, along with Lemma 5.1, will give the number of linear and quadratic factors of $\pi_8(J, K)$.

Since $\pi_8(J, K)$ is of degree p^5+p^3, we may determine the exact number of irreducible factors of degree 8 of π_8. We summarize the above results in the following table giving the number of irreducible factors of $\pi_8(J, K)$:

p	Linear	Quadratic	Quartic	Octic	Total Number
$8K+1$	2	$(p-1)/2$	$(p^3-1)/4$	$(p^5-p)/8$	$(p^5+2p^3+3p+10)/8$
$8K-1$	2	$(p-3)/2$	$(p^3+1)/4$	$(p^5-p)/8$	$(p^5+2p^3+3p+6)/8$
$8K+3$	0	$(p-1)/2$	$(p^3+1)/4$	$(p^5-p)/8$	$(p^5+2p^3+3p-2)/8$
$8K-3$	0	$(p+1)/2$	$(p^3-1)/4$	$(p^5-p)/8$	$(p^5+2p^3+3p+2)/8$

Theorem 3.1 enables one to find the exact number of conjugate sets of irreducible octic congruences of a given order, e.g., if $p=8K+1$, then there exist 2 conjugate sets of order $p(p^2-1)/8$, $(p-1)/2$ conjugate sets of order $p(p^2-1)/4$, $(p^3-1)/4$ conjugate sets of order $p(p^2-1)/2$, and $(p^5-p)/8$ conjugate sets of order $p(p^2-1)$.

REFERENCES

1. H. R. Brahana, *On cubic congruences*, Bull. Amer. Math. Soc. vol. 39 (1933) pp. 962–969.

2. ———, *Note on irreducible quartic congruences*, Trans. Amer. Math. Soc. vol. 38 (1935) pp. 395–400.

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

4. ———, ibid., p. 6, where $n=1$.

5. C. B. Hanneken, *Irreducible quintic congruences*, Duke Math. J. vol. 22 (1955) pp. 107–118.

6. ———, *Irreducible sextic congruences*. This paper has been offered to the Duke Mathematical Journal.

MARQUETTE UNIVERSITY