LINEAR HOMOGENEOUS EQUATIONS OVER FINITE RINGS

HARLAN STEVENS

1. Introduction. The intent of this paper is to apply the following theorem in several particular instances:

THEOREM 1. *For any finite ring $\mathfrak{R}$ of q elements, let $\{\mathfrak{H}_i\}$ be a collection of s subsets of $\mathfrak{R}$, each containing h_i $(i = 1, 2, \ldots, s)$ members, and let $D(\mathfrak{H}_i)$ denote the set of all differences $d' - d''$ with d' and d'' from $\mathfrak{H}_i$, including $d' = d''$. Furthermore, suppose that*

$$\prod_{i=1}^{s} h_i > q^r \qquad (r < s). \tag{1.1}$$

Then the system of r linear equations

$$\sum_{i=1}^{s} a_{ji} x_i = 0 \qquad (j = 1, 2, \ldots, r), \tag{1.2}$$

where $a_{ji} \in \mathfrak{R}$ or is a rational integer, has a non-trivial solution such that $x_i \in D(\mathfrak{H}_i)$ $(i = 1, 2, \ldots, s)$.

Such a theorem seems appropriate in that it points out the algebraic foundation for several more or less familiar results for $\mathfrak{R} = J_q$, the ring of integers (mod q). ("Integer" and "prime" will always mean "rational integer" and "rational prime.") Moreover, it allows easy extension of these results to other finite rings. Its proof in §2 consists essentially of not much more than the Dirichlet box principle.

In particular, *suppose that the positive real numbers f_i $(i = 1, 2, \ldots, s)$, each less than the integer q, are such that*

$$\prod_{i=1}^{s} f_i > q^r \qquad (r < s).$$

Then as one consequence of Theorem 1 we have:

The system of r linear congruences

$$\sum_{i=1}^{s} a_{ji} x_i \equiv 0 \pmod{q} \qquad (j = 1, 2, \ldots, r) \tag{1.3}$$

has a non-trivial solution in integers $x_1, x_2, \ldots, x_s$ such that

$$|x_i| < f_i \ (i = 1, 2, \ldots, s).$$

Received May 13, 1963.

To see this, one merely need take $\mathfrak{H}_i$ as the set $0, 1, \ldots, f_i^*$, where f_i^* is the greatest integer less than f_i.

Indeed, this last result, due to A. Brauer and T. L. Reynolds **(1)**, motivates the present discussion. Furthermore, if in the latter theorem $r = 1$, $s = 2$, and $f_1 = \sqrt{q}$, $f_2 = \delta + \sqrt{q}$, where $\delta > 0$ is arbitrarily small, then there exists a solution of (1.3) such that $|x_1| < \sqrt{q}$, $|x_2| \leqslant \sqrt{q}$. This is a familiar conclusion usually attributed to Thue. A more extensive history of the theorem, along with complete references, is also included in **(1)**.

In addition, there appears in **(1)** an extension of the Brauer-Reynolds theorem to higher congruences and rings of matrices, but only for the case $r = 1$, $s = 2$. As suggested before, we can now do the same for arbitrary r and s; this is shown in §2.

Perhaps one should not expect very sharp applications from a statement as general as Theorem 1. Nevertheless, it is well known that Thue's theorem implies that primes of the form $4N + 1$ are representable as the sum of two squares. Further, the Brauer-Reynolds generalization has been employed in **(1)** and **(2**, pp. 20–29**)** to derive elementary estimates for primitive roots and nth power non-residues, modulo a prime. Following the lead of these papers, in §§3 and 4 we obtain some information about the distribution of primitive roots and nth power non-residues in the Galois field $\mathrm{GF}(p^k)$. For the present, we shall let the following example suffice.

Let $P = P(x)$ be any irreducible polynomial of degree k in $\mathrm{GF}[p, x]$, the domain of polynomials in x over $\mathrm{GF}(p) = J_p$, where p is a prime. In addition, let

$$A = A(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} \qquad (a_i \in \mathrm{GF}(p))$$

be any member of $\mathrm{GF}(p^k) = \mathrm{GF}[p, x] \pmod P$. Then in §4 we show that for any arbitrarily specified set of coefficients $\{a_i\}$, $k' = k - [(k + 2)/2]$ in number, there exists an A which is an nth power non-residue $\pmod P$ such that these particular k' coefficients are zero. (As usual, $[\alpha]$ denotes the greatest integer function.) This implies, of course, that the non-residue of least degree has degree at most $[k/2]$.

Actually, Davenport **(4)** and Carlitz **(3)** have already made considerations similar to the last mentioned for $\mathrm{GF}(p^k)$. They employ deeper methods due to Vinogradov, however, and their results are stated in terms of a "sufficiently large" degree k or prime p. On the other hand, our procedure is elementary, and all results are for arbitrary irreducibles $P(x)$, of fixed degree over a fixed $\mathrm{GF}(p)$.

2. Proof of Theorem 1; corollaries. The notation of matrix theory is convenient for us. Let $\mathfrak{P}$ represent the set of all r-vectors (column matrices) with components from $\mathfrak{R}$. Clearly, $\mathfrak{P}$ consists of q^r elements. Now, if C is the coefficient matrix of the system (1.2) and $Y = \mathrm{col}[y_1, y_2, \ldots, y_s]$, consider all possible vectors CY formed by taking y_i from $\mathfrak{H}_i$ $(i = 1, 2, \ldots, s)$. From

https://doi.org/10.4153/CJM-1964-054-8 Published online by Cambridge University Press

(1.1) there are more than q^r, so that by the box principle, $CY_1 = CY_2$ for some $Y_1 \neq Y_2$. Hence, $X = Y_1 - Y_2$ is the required non-trivial solution.

As an obvious corollary of Theorem 1 we have the following theorem.

THEOREM 2. *If $\mathfrak{H}$ is a module of $\mathfrak{R}$ containing h elements, and $h^s > q^r$, then there exists a non-trivial solution of* (1.2) *such that $x_i \in \mathfrak{H}$ $(i = 1, 2, \ldots, s)$.*

Now let $J_m[x]$ be the ring of all polynomials over J_m, and let $M = M(x)$ in $J_m[x]$ be monic of degree k. Then if $\mathfrak{R}$ is $J_m[x] \pmod{M}$, it consists of $q = m^k$ elements, and as another consequence of Theorem 1, we obtain the following theorem.

THEOREM 3. *Let $\{f_{ij}\}$ $(i = 1, 2, \ldots, s; j = 0, 1, \ldots, k-1)$ be a collection of sk positive numbers such that*

$$\prod_{j=0}^{k-1} \prod_{i=1}^{s} f_{ij} > m^{kr} \qquad (s > r).$$

Then there exists a non-trivial solution

$$Y_i'(x) = \sum_{j=0}^{k-1} e_{ij} x^j \qquad (i = 1, 2, \ldots, s)$$

of the linear homogeneous system

$$\sum_{i=1}^{s} a_{li}(x) Y_i(x) \equiv 0 \pmod{M} \qquad (l = 1, 2, \ldots, r)$$

such that $|e_{ij}| < f_{ij}$ $(i = 1, 2, \ldots, s; j = 0, 1, \ldots, k-1)$.

Proof. Take $\mathfrak{H}_i$ in Theorem 1 to be the set of all polynomials

$$B_i(x) = \sum_{j=0}^{k-1} b_{ij} x^j$$

and such that b_{ij} is one of the numbers $0, 1, \ldots, f_{ij}^*$, where again f_{ij}^* means the greatest integer less than f_{ij}. Then

$$\prod_{i=1}^{s} h_i = \prod_{i=1}^{s} \prod_{j=0}^{k-1} (f_{ij}^* + 1) > m^{kr},$$

from which the theorem follows.

A similar assertion holds for the ring $\mathfrak{R}$ of square matrices of order v with elements from J_m. Thus, $q = m^{v^2}$ and, as another corollary, we obtain the following theorem.

THEOREM 4. *Let $\{f_{jk}^{(i)}\}$, defined for all $1 \leqslant i \leqslant s$, $1 \leqslant j, k \leqslant v$, be a collection of sv^2 positive numbers less than m such that*

$$\prod_i \prod_j \prod_k f_{jk}^{(i)} > m^{rv^2} \qquad (r < s).$$

Let $A_\mu^{(i)}$ $(i = 1, 2, \ldots, s)$ *be fixed and in* $\mathfrak{R}$. *Then there are matrices* $B^{(i)} = (b_{jk}^{(i)})$, *not all* $\equiv 0 \pmod m$, *which satisfy*

$$\sum_{i=1}^{s} A_\mu^{(i)} B^{(i)} \equiv 0 \pmod m \qquad (\mu = 1, 2, \ldots, r)$$

and such that $|b_{jk}^{(i)}| < f_{jk}^{(i)}$ *for every* i, j, k.

3. Distribution of primitive roots in $GF(p^k)$. Now let $G = G(x)$ be a primitive root (mod P), where $P = P(x)$ is an irreducible member of GF$[p, x]$ of degree k. Consequently, G generates the multiplicative group of the corresponding GF(p^k).

We shall now employ a method of Brauer **(2)**. G belongs to the exponent $p^k - 1 \pmod P$. Suppose, for fixed k and p, that $p^k - 1$ has τ distinct prime divisors $p_1, p_2, \ldots, p_\tau$. Let $u_1, \ldots, u_\nu$ represent the $\nu = 2^\tau$ possible products of distinct primes from the p_i, including $u_1 = 1$; assume also that $u_\nu = p_1 p_2 \ldots p_\tau$. Further, let $Y_0, Z_0^{(1)}, \ldots, Z_0^{(\nu-1)}$ be a solution of the linear homogeneous system in ν unknowns

$$Z^{(i)} \equiv G^{\mu_i} Y \pmod P \qquad (i = 1, 2, \ldots, \nu - 1). \tag{3.1}$$

Then either Y_0 or one of the $Z_0^{(i)}$ is a primitive root. For if Y_0 is not, then $Y_0 \equiv G^\alpha \pmod P$, where α and $p^k - 1$ have common prime divisors, say, $p_1, p_2, \ldots, p_\eta$. Then, if $u_\beta = p_{\eta+1} \ldots p_\tau$, we have

$$Z_0^{(\beta)} \equiv G^{\alpha + u_\beta} \pmod P.$$

Since $\alpha + u_\beta$ and $p^k - 1$ are relatively prime, it follows that $Z_0^{(\beta)}$ is a primitive root (mod P).

We may now apply Theorem 3 to (3.1). If all the numbers f_{ij} are set equal to $p^{(\nu-1)/\nu} + \delta$, where $\delta > 0$ is arbitrarily small, then

$$\prod_{j=0}^{k-1} \prod_{i=1}^{\nu} (p^{(\nu-1)/\nu} + \delta) > p^{(\nu-1)k} + \delta > p^{(\nu-1)k}.$$

Therefore, by virtue of the preceding argument, we have:
There exists a primitive root

$$G \equiv \sum_{i=0}^{k-1} g_i x^i \pmod P \tag{3.2}$$

such that

$$|g_i| < p^{(\nu-1)/\nu} \qquad (i = 0, 1, \ldots, k - 1). \tag{3.3}$$

If $p = 4N + 1$, or $p = 4N - 1$ and k is even, then it is easily shown that $-G$ is also a primitive root. To this end, assume that $-G$ belongs to the exponent $e \pmod P$. Then

$$G^e \equiv (-1)^e \pmod P,$$

where e divides $p^k - 1$. Clearly, it cannot be that $2e < p^k - 1$; likewise, since $p^k - 1 = 4M$, it follows that $e \neq (p^k - 1)/2$. Thus $e = p^k - 1$. Consequently, we may conclude that there exists at least one G such that any arbitrarily chosen coefficient g_ϕ shall satisfy

$$0 \leqslant g_\phi < p^{(\nu-1)/\nu}. \tag{3.4}$$

Sometimes we can take advantage of Theorem 2. Suppose that π is a positive integer that satisfies

$$\nu(k - \pi) > k(\nu - 1), \tag{3.5}$$

where ν has the same significance as before. Then consider the module $\mathfrak{H}$ composed of all those polynomials where some particular π of the coefficients are specified as zero. $\mathfrak{H}$ consists then of $h = p^{k-\pi}$ elements. Hence, by Theorem 2, along with (3.5) and the argument above, $\mathfrak{H}$ contains at least one primitive root (mod P).

This occurs, for instance, when $p = 3$, $k = 9$, $\pi = 1$; then $3^9 - 1 = 2.13.757$, so that $\nu = 2^3$ and (3.5) obtains. In particular, if P is an arbitrary irreducible polynomial of degree 9 in GF[3, x], it possesses a primitive root of degree $\leqslant 7$.

Summarizing, we can state the following theorem.

THEOREM 5. *For an arbitrary prime p, let P be any irreducible member of* GF[p, x] *of degree k. Then there exists at least one primitive root G* (mod P), *where G is represented by* (3.2), *such that* (3.3) *holds. If k is even, or $p = 4N + 1$, then for any fixed coefficient g_ϕ there is a G such that* (3.3) *and* (3.4) *hold. When* (3.5) *is true, there is a G such that any π arbitrarily chosen coefficients are zero.*

In some cases one can do a little better. Let $p = 4N - 1$; then $P = x^2 + 1$ is irreducible in GF[p, x], and $a + bx \leftrightarrow a - bx$ is an automorphism of GF[p, x] (mod $x^2 + 1$). Thus, since k is even, either none or all of the four expressions $\pm g_0 \pm g_1 x$ are primitive roots; hence we have the following theorem.

THEOREM 6. *If $p = 4N - 1$, there is a primitive root $G = g_0 + g_1 x$ in* GF[p, x] (mod $x^2 + 1$) *such that $0 \leqslant g_0 < p^{(\nu-1)/\nu}$ and $0 < g_1 < p^{(\nu-1)/\nu}$.*

The following theorem is a straightforward generalization of **(2**, Theorem 3**)**, combined with the arguments above.

THEOREM 7. *Let ω be the maximal length of the sequences of consecutive integers which are not relatively prime to $p^k - 1$. Then Theorem 5 remains true if ν is everywhere replaced by $\omega + 1$.*

Brauer also states in **(2)** that he does not know if $\omega + 1 \leqslant \nu$ always holds.

It may be of interest to compare our results with Davenport's, referred to earlier. He proved that in GF[p, x] every irreducible polynomial P, of fixed degree k, is such that a linear term $x + a$ is a primitive root (mod P), provided p is sufficiently large.

On the other hand, Carlitz showed later in **(3)** that, for a fixed prime p, there are infinitely many irreducible polynomials P such that no primitive root (mod P) is of degree less than r, for any predetermined integer r.

4. Distribution of nth power non-residues in $GF(p^k)$. Now let

$$A = A(x) = a_0 + a_1 + \ldots + a_{k-1}x^{k-1} \qquad (a_i \in \mathrm{GF}(p)). \tag{4.1}$$

If $p^k - 1 = nt$, and $A \equiv G^\alpha \pmod P$, we recall that A is an nth power residue (mod P) if and only if $\alpha \equiv 0 \pmod n$. (For brevity we omit "nth power.") Thus, since G is a non-residue, all the estimates of §3 apply to the set of all non-residues.

Because the product of a residue and a non-residue is clearly a non-residue, we can do considerably better, however. For then any particular solution of

$$Z \equiv BY \pmod P \tag{4.2}$$

will yield a non-residue if $B = G$. From Theorem 3, then, taking each $f_{ij} = \delta + \sqrt{p}$, for very small $\delta > 0$, we easily deduce the existence of a non-residue A, denoted by (4.1), such that

$$|a_i| < \sqrt{p} \qquad (i = 0, 1, \ldots, k-1). \tag{4.3}$$

Moreover, by Euler's criterion extended to $\mathrm{GF}(p^k)$, -1 is a residue if $(p^k - 1)/n$ is even. In this case $-A$ is still a non-residue, and any chosen term a_ϕ can be made to satisfy

$$0 \leqslant a_\phi < \sqrt{p}. \tag{4.4}$$

In particular, this holds if n is odd.

We may apply Theorem 2 to (4.2) in order to verify the example mentioned near the end of §1. If $\mathfrak{H}$ is the module consisting of all polynomials where only $[(k+2)/2]$ specified coefficients are allowed to be non-zero then $\mathfrak{H}$ contains $h = p^{[(k+2)/2]}$ members. Since $r = 1$, $s = 2$, and

$$p^{2[(k+2)/2]} > p^k,$$

a solution of (4.2) is in $\mathfrak{H}$, and the desired result follows. Altogether we have shown the following theorem.

THEOREM 8. *For an arbitrary p, let P be any irreducible member of* $\mathrm{GF}[p, x]$ *of degree k. Then there exists at least one* nth *power non-residue* $A \pmod P$, *where A is represented by* (4.1), *such that if* $(p^k - 1)/n$ *is even, then* (4.3) *and* (4.4) *hold for any specified* a_ϕ. *Also, there exists an A with at most* $[(k+2)/2]$ *arbitrarily specified coefficients not zero.*

Finally, analogous to Theorem 6 we have the following theorem.

THEOREM 9. *If* $p = 4N - 1$ *and* $(p^2 - 1)/n$ *is even, there exists an* nth *power non-residue* $A = a_0 + a_1 x \pmod{x^2 + 1}$ *such that* $0 \leqslant a_0 < \sqrt{p}$ *and* $0 \leqslant a_1 < \sqrt{p}$.

https://doi.org/10.4153/CJM-1964-054-8 Published online by Cambridge University Press

References

1. A. Brauer and T. L. Reynolds, *On a theorem of Aubry-Thue*, Can. J. Math., *3* (1951), 367–374.
2. ——— *Studies in mathematics and mechanics presented to Richard von Mises* (New York, 1954).
3. L. Carlitz, *Distribution of primitive roots in a finite field*, Quart. J. Math., Oxford, *4* (1953), 4–10.
4. H. Davenport, *On primitive roots in finite fields*, Quart. J. Math., Oxford, *8* (1937), 308–312.

The Pennsylvania State University