COMPOSITIO MATHEMATICA

L. CARLITZ

Sets of primitive roots

Compositio Mathematica, tome 13 (1956-1958), p. 65-70

<http://www.numdam.org/item?id=CM_1956-1958__13__65_0>

Sets of primitive roots

by

L. Carlitz

1. **Introduction.** As a special case of a more general result [1, Theorem 1] the writer has proved that if a is a fixed integer $\geqq 1$, then the number of integers x, $1 \leqq x \leqq p-1$, such that x and $x+a$ are both primitive roots (mod p) is equal to

$$\frac{\varphi^2(p-1)}{p-1} + O(p^{\frac{1}{2}+\varepsilon}) \qquad (\varepsilon > 0), \tag{1.1}$$

where $\varphi(p-1)$ is the Euler function. The more general result referred to is concerned with the number of solutions in primitive roots (mod p) of

$$a_1x_1 + \cdots + a_rx_r \equiv a \quad (\text{mod } p). \tag{1.2}$$

It is natural to raise the following question. Let $a_1, \cdots, a_{r-1}$ be fixed integers $\geqq 1$. We seek the number of integers x (mod p) such that

$$x,\ x+a_1, \cdots, x+a_{r-1} \tag{1.3}$$

are all primitive roots. If N_r denote this number we show that

$$N_r \sim \frac{\varphi^r(p-1)}{p^{r-1}} \qquad (p \to \infty). \tag{1.4}$$

The proof of (1.4) depends on some results of Davenport [2].

Indeed we can prove rather more. Let

$$f_1(x),\ f_2(x), \cdots, f_r(x) \tag{1.5}$$

denote polynomials with integral coefficients (mod p); there is no loss in generality in assuming that each $f_i(x)$ is of degree $\geqq 1$. Moreover we assume that the $f_i(x)$ are relatively prime (mod p) in pairs and none is divisible by the square of a polynomial (mod p). If now N_r denotes the number of integers x (mod p) such that all the numbers (1.5) are primitive roots, then again (1.4) holds.

We also prove that if the polynomials $g_j(x)$ satisfy the previous hypotheses then M_r, the number of integers x (mod p) such that

$$\left(\frac{g_j(x)}{p}\right) = \varepsilon_j \qquad (j = 1, \cdots, r), \tag{1.6}$$

where (a/p) is the Legendre symbol and $\varepsilon_j = \pm 1$, satisfies

$$2^r M_r \sim p \qquad (p \to \infty). \tag{1.7}$$

More generally if $f_1(x), \cdots, f_r(x), g_1(x), \cdots, g_s(x)$ are polynomials satisfying the previous hypotheses and $N_{r,s}$ is the number of integers (mod p) such that simultaneously all $f_i(x)$ are primitive roots and (1.6) is satisfied, then

$$2^s N_{r,s} \sim \frac{\varphi^r(p-1)}{p^{r-1}} \qquad (p \to \infty). \tag{1.8}$$

It should be noted that in these results the numbers r, s, $\deg f_i$, $\deg g_j$ are kept fixed as $p \to \infty$.

Since it is no more difficult, we prove the above results for arbitrary finite fields $GF(q)$. Moreover in place of primitive roots we deal with numbers belonging to an exponent e, where $e \mid q-1$. For the precise statement of the more general results see the theorems in §§ 3, 4.

2. Let $GF(q)$, $q = p^n$, denote an arbitrary finite field and put $q-1 = ef$. Numbers of $GF(q)$ will be denoted by lower case Greek letters $\alpha, \beta, \gamma, \cdots, \xi, \eta, \zeta$. Let $\chi(\alpha)$ denote a character of the multiplicative group of $GF(q)$, and let $\chi_0(\alpha)$ denote the principal character. We now define a function $\omega(\xi)$ by means of

$$\omega(\xi) = \frac{1}{f} \sum_{d \mid e} \frac{\mu(d)}{d} \sum_{\chi^{df} = \chi_0} \chi(\xi), \tag{2.1}$$

where $\mu(d)$ is the Möbius function and inner sum is over the df character χ such that $\chi^{df} = \chi_0$. Then we have the following easily proved result.

LEMMA 1. *If ξ belongs to the exponent e, then $\omega(\xi) = 1$; for all other ξ, $\omega(\xi) = 0$.*

It is convenient to transform (2.1) by means of

LEMMA 2. *The function $\omega(\xi)$ defined by (2.1) satisfies*

$$\omega(\xi) = \frac{\varphi(e)}{q-1} \sum_{z \mid q-1} \frac{\mu(z_1)}{\varphi(z_1)} \sum_{\chi^{(z)}} \chi(\xi) \qquad \left(z_1 = \frac{z}{(z, f)}\right), \tag{2.2}$$

where the inner sum is over the $\varphi(z)$ characters belonging to the exponent z.

A character χ *belongs* to the exponent k if k is the least integer

$\geqq 1$ such that $\chi^k = \chi_0$. We shall sketch the proof of the equivalence of (2.1) and (2.2). It is clear from (2.1) that

$$\omega(\xi) = \frac{1}{f}\sum_{d|e}\frac{\mu(d)}{d}\sum_{z|df}\sum_{\chi^{(z)}}\chi(\xi), \tag{2.3}$$

where $\chi^{(z)}$ has the same meaning as in (2.2). In the next place the right member of (2.3) is equal to

$$\frac{1}{f}\sum_{z|q-1}\sum_{\chi^{(z)}}\chi(\xi)\sum_{z|df|q-1}\frac{\mu(d)}{d},$$

where the innermost sum is over all d satisfying the indicated conditions. Now put $z_0 = (z, f)$, $z = z_0 z_1$, $f = z_0 f_1$; $z|df$ is equivalent to $z_1|d$. Put $d = z_1 u$; then

$$\sum_{z|df|q-1}\frac{\mu(d)}{d} = \sum_{u|ez_1^{-1}}\frac{\mu(z_1u)}{z_1u} = \frac{\mu(z_1)}{z_1}\sum_{\substack{u|ez_1^{-1}\\(u,z_1)=1}}\frac{\mu(u)}{u}$$

$$= \frac{\mu(z_1)}{z_1}\frac{\varphi(e)}{e}\frac{z_1}{\varphi(z_1)} = \frac{\varphi(e)}{e}\frac{\mu(z_1)}{\varphi(z_1)}.$$

This evidently proves (2.2).

LEMMA 3. *Let $\chi_1, \cdots, \chi_r$ denote non-principal multiplicative characters and let $f_1(x), \cdots, f_r(x)$ denote quadratfrei polynomials with coefficients in $GF(q)$ that are relatively prime in pairs and of degree $\geqq 1$. Put*

$$S = S(f, \chi) = \sum_{\alpha\varepsilon GF(q)}\chi_1(f_1(\alpha))\cdots\chi_r(f_r(\alpha)). \tag{2.4}$$

Then

$$|S(f, \chi)| \leqq (k-1)q^{1-\theta_k}, \tag{2.5}$$

where $k = \deg f_1 + \cdots + \deg f_r$ *and*

$$\theta_3 = \frac{1}{4}, \qquad \theta_k = \frac{3}{2(k+4)} \qquad (k\geqq 4). \tag{2.6}$$

For proof see Davenport [2].

As a matter of fact by a theorem of André Weil [3], we may take $\theta_k = \frac{1}{2}$; however we shall not make use of this deeper result.

3. Let $e_1, \cdots, e_r$ be integers such that $e_i|q-1$ and let N_r denote the number of $\alpha\varepsilon\, GF(q)$ such that $f_i(\alpha)$ belongs to the exponent e_i for $i = 1, \cdots, r$; here the $f_i(x)$ are polynomials with coefficients in $GF(q)$. Extending the definition (2.1) in an obvious way we define the set of functions $\omega_1(\xi), \cdots, \omega_r(\xi)$ such that $\omega_i(\xi) = 1$ if ξ belongs to the exonent e_i, while $\omega_i(\xi) = 0$ otherwise. Then it

is clear that

$$N_r = \sum_{\alpha} \omega_1(f_1(\alpha)) \cdots \omega_r(f_r(\alpha)). \tag{3.1}$$

Put $e_i f_i = q-1$, $i = 1, \cdots, r$. Substituting from (2.2) in (3.1) we get

$$N_r = \frac{\varphi(e_1) \cdots \varphi(e_r)}{(q-1)^r} \sum_{\substack{z_1, \cdots, z_r \\ z_i \mid q-1}} \frac{\mu(z_1') \cdots \mu(z_r')}{\varphi(z_1') \cdots \varphi(z_r')} \cdot \sum_{\chi_1^{(z_1)}, \cdots, \chi_r^{(z_r)}} \sum_{\alpha} \chi_1(f_1(\alpha)) \cdots \chi_r(f_r(\alpha)), \tag{3.2}$$

where χ_i runs through the $\varphi(z_i)$ characters belonging to the exponent z_i, and

$$z_1' = \frac{z_i}{(z_i, f_i)} \qquad (i = 1, \cdots, r).$$

Consider first the terms in the right member of (3.2) corresponding to principal characters χ_i. Since χ_i belongs to z_i it follows that all $z_i = 1$ and therefore we get

$$\frac{\varphi(e_1) \cdots \varphi(e_r)}{(q-1)^r} \sum_{\alpha} \chi_0(f_1(\alpha)) \cdots \chi_0(f_r(\alpha)) = \frac{\varphi(e_1) \cdots \varphi(e_r)}{(q-1)^r} q + O\left(k \frac{\varphi(e_1) \cdots \varphi(e_r)}{(q-1)^r}\right). \tag{3.3}$$

We now assume that the polynomials f_i satisfy the hypotheses of Lemma 3. Then the remaining terms in (3.2) contribute

$$\frac{\varphi(e_1) \cdots \varphi(e_r)}{(q-1)^r} \sum_{z_i \mid q-1} \frac{\mu(z_1') \cdots \mu(z_r')}{\varphi(z_1') \cdots \varphi(z_r')} \sum_{\chi_i^{(z_i)}} S(f, \chi)$$
$$= O\left\{\frac{\varphi(e_1) \cdots \varphi(e_r)}{(q-1)^r} \sum_{z_i \mid q-1} \frac{1}{\varphi(z_1') \cdots \varphi(z_r)} \sum_{\chi_i^{(z_i)}} |S(f, \chi)|\right\}$$
$$= O\left\{\frac{\varphi(e_1) \cdots \varphi(e_r)}{(q-1)^r} \sum_{z_i \mid q-1} \frac{\varphi(z_1) \cdots \varphi(z_r)}{\varphi(z_1') \cdots \varphi(z_r')} kq^{1-\theta_k}\right\},$$

by (2.5). In the next place we have

$$\sum_{z_i \mid q-1} \frac{\varphi(z_1) \cdots \varphi(z_r)}{\varphi(z_1') \cdots \varphi(z_r')} = O\{f_1 \cdots f_r \sum_{z_i \mid q-1} 1\} = O(f_1 \cdots f_r q^{r\varepsilon}),$$

where $\varepsilon > 0$, and therefore the above estimate becomes

$$O\left\{\frac{\varphi(e_1) \cdots \varphi(e_r)}{(q-1)^r} f_1 \cdots f_r kq^{1-\theta_k + r\varepsilon}\right\} = O(kq^{1-\theta_k + r\varepsilon}). \tag{3.4}$$

Combining (3.2) with (3.3) and (3.4) we get

$$N_r = \frac{\varphi(e_1)\cdots\varphi(e_r)}{(q-1)^r}\,q + O(kq^{1-\theta_k+r\varepsilon}) \qquad (q\to\infty). \tag{3.5}$$

This proves

THEOREM 1. *Let $f_1(x), \cdots, f_r(x)$ denote quadratfrei polynomials with coefficients $\varepsilon GF(q)$ that are relatively prime in pairs and of degree $\geqq 1$; let $e_1, \cdots, e_r$ denote positive integers such that $e_i \mid q-1$, $i = 1, \cdots, r$. Let N_r denote the number of $\alpha\varepsilon GF(q)$ such that $f_i(\alpha)$ belongs to the exponent e_i. Then N_r satisfies* (3.5), *where θ_k is defined by* (2.6) *and $k = \deg f_1 + \cdots + \deg f_r$.*

In particular if all $e_i = q-1$ and k is fixed we get

THEOREM 2. *Let $f_1(x), \cdots, f_r(x)$ satisfy the hypotheses of Theorem 1 and let N'_r denote the number of $\alpha\varepsilon GF(q)$ such that $f_i(\alpha)$ is a primitive root of $GF(q)$ for $i = 1, \cdots, r$. Then for fixed k*

$$N'_r \sim \frac{\varphi^r(q-1)}{q^{r-1}} \qquad (q\to\infty). \tag{3.6}$$

If we take $f_i(x) = x+\alpha_i$, $i = 1, \cdots, r$, where the α_i are distinct, then for $q = p$, (3.6) reduces to (1.4).

4. Let the polynomials $f_1(x), \cdots, f_r(x)$ have the same meaning as in Theorem 1. For q odd we define the character $\psi(\alpha)$, $\alpha\varepsilon GF(q)$, as equal to $+1$, -1, 0 according as α is equal to a square, a nonsquare, or zero in $GF(q)$. Let $\varepsilon_j = \pm 1$, $j = 1, \cdots, r$ be assigned. We consider the number of α such that

$$\psi(f_i(\alpha)) = \varepsilon_i \qquad (i = 1, \cdots, r). \tag{4.1}$$

If M_r denotes this number then clearly the sum

$$\sum_{\alpha}\prod_{i=1}^{r}\{1+\varepsilon_i\psi(f_i(\alpha))\} \tag{4.2}$$

differs from $2^r M_r$ by at most k. Expanding the product in (4.2) and applying Lemma 3 we obtain

THEOREM 3. (q odd). *If the polynomials $f_1(x), \cdots, f_r(x)$ satisfy the hypothesis of Theorem 2 and $\varepsilon_i = \pm 1$, $i = 1, \cdots, r$ are assigned, then for fixed k the number of $\alpha\varepsilon GF(q)$ for which* (4.1) *holds satisfies*

$$M_r \sim 2^{-r} q \qquad (q\to\infty). \tag{4.3}$$

It is clear how the theorem can be extended to d-th powers. It should be remarked that some hypothesis on the size of k is necessary. For example when $r = 1$ one can construct a nonconstant polynomial $f(x)$ such that $\psi(f(\alpha)) = 1$ for $q-1$ values of α and therefore (4.3) does not hold.

In the next place it is not difficult to prove a theorem that includes both Theorem 1 and 3. Let $f_1(x), \cdots, f_r(x), g_1(x), \cdots, g_s(x)$ denote polynomials that satisfy the previous hypothesis. Let $e_1, \cdots, e_r$ be divisors of $q-1$ and $\varepsilon_j = \pm 1$, $j = 1, \cdots, s$. We consider the number of $\alpha \varepsilon GF(q)$ such that $f_i(\alpha)$ belongs to the exponent e_i for $i = 1, \cdots, r$ and $\psi(g_j(\alpha)) = \varepsilon_j$ for $j = 1, \cdots, s$. If we call this number $N_{r,s}$ then it is clear that the sum

$$\sum_{\alpha} \prod_{i=1}^{r} \omega_i(f_i(\alpha)) \prod_{j=1}^{s} \{1+\varepsilon_j \psi(g_j(\alpha))\} \tag{4.4}$$

differs from $2^s N_{r,s}$ by at most h, where $I = \deg g_0 + \cdots + \deg g_s$. Hence expanding the second product in the right member of (4.4) proceeding exactly as in the proof of Theorem 1 we get

$$2^s N_{r,s} = \frac{\varphi(e_1) \cdots \varphi(e_r)}{(q-1)^r} q + O(kq^\theta), \tag{4.5}$$

where $\theta < 1$. We may state

THEOREM 4. *Let $f_1(x), \cdots, f_r(x)$, $g_1(x), \cdots, g_s(x)$ denote quadratfrei polynomials that are relatively prime in pairs. Let $e_i \,|\, q-1$* for $i = 1, \cdots, r$; $\varepsilon_j = \pm 1$ for $j = 1, \cdots, s$. *Then $N_{r,s}$, the number of α such that $f_i(\alpha)$ belongs to the exponent e_i and $\psi(g_j(\alpha)) = \varepsilon_j$, satisfies* (4.5), *where* $\theta < 1$, $k = \deg f_1 + \cdots + \deg f_r$, $h = \deg g_1 + \cdots + \deg g_s$.

In particular if all $e_i = q-1$ and k and h are fixed we get

THEOREM 5. *Let $f_1(x), \cdots, f_r(x)$, $g_1(x), \cdots, g_s(x)$ satisfy the hypotheses of Theorem 4 and let $N'_{r,s}$ denote the number of α such that $f_i(\alpha)$ is a primitive root of $GF(q)$ for $i = 1, \cdots, r$ and $\psi(g_j(\alpha)) = \varepsilon_j$ for $j = 1, \cdots, s$. Then for fixed k, h we have*

$$2^s N_{r,s} \sim \frac{\varphi^r(q-1)}{q^{r-1}} \qquad (q \to \infty). \tag{4.6}$$

REFERENCES

L. CARLITZ

[1] Sums of primitive roots in a finite field, Duke Mathematical Journal, vol. 19 (1952), pp. 459—469.

H. DAVENPORT

[2] On character sums in a finite field, Acta Mathematica, vol. 71 (1939), pp. 99—121.

ANDRÉ WEIL

[3] On the Riemann hypothesis in function-fields, Proceedings of the National Academy of Sciences, vol. 27 (1941), pp. 345—347.

Duke University.

(Oblatum 6-10-53).