PRIMITIVE ROOTS IN A FINITE FIELD

BY

L. CARLITZ

1. **Introduction.** A number $\beta \in GF(p^n)$, $\beta \neq 0$, is a primitive root of the field if $k = p^n - 1$ is the smallest positive integer such that $\beta^k = 1$; the number of primitive roots is $\phi(p^n - 1)$, where $\phi(m)$ is the Euler function. Ore [6] has introduced an analogous concept in the following manner. For each $\gamma \in GF(p^n)$ there exists a "linear" polynomial

$$a(x) = \sum_{r=0}^{m} a^r x^{p^r} \qquad (a_r \in GF(p),\ a_m \neq 0) \tag{1.1}$$

with minimum m such that $a(\gamma) = 0$; γ is said to *belong* to $a(x)$. In particular if $a(x) = x^{p^n} - x$, Ore calls γ a primitive root. It is easy to see that the two varieties of primitive roots are not identical; for example in the $GF(2^4)$ defind by $\theta^4 + \theta + 1$, θ is a primitive root in the original sense but not in Ore's sense (since it belongs to $x^8 + x^4 + x^2 + x$). On the other hand it can be verified that θ^3 is primitive according to Ore but belongs to the numerical exponent 5. To avoid confusion we shall refer to ordinary primitive roots as primitive roots of the first kind, while those satisfying Ore's definition will be called roots of the second kind. Ore proved that primitive roots of the second kind exist; indeed there are precisely $\Phi(x^n - 1) \in GF(p^n)$, where Φ now denotes the Euler function for $GF[p, x]$. The equivalent result in terms of the existence of a normal basis (see §2) had been proved by Hensel.

It is natural to ask whether one can find a number $\beta \in GF(p^n)$ which is simultaneously a primitive root of both the first and second kinds. More generally if $e \mid p^n - 1$ and $a(x) \mid x^{p^n} - x$, can one find a number β belonging to the numerical exponent e and the linear polynomial $a(x)$? We shall show that the first question is answered in the affirmative for p^n sufficiently large; the second question also admits of an affirmative answer provided p^n is large and $e \deg a(x)$ is sufficiently large. The method of proof is suggested by the proof of Vinogradoff's theorem that the least primitive root of a prime p is $O(p^{1/2+\epsilon})$; see [5, p. 178], also [3].

In the opposite direction we show (Theorem 4) that for given p, r there exist infinitely many irreducible polynomials P such that no polynomial of degree $\leqq r$ can be a primitive root of the second kind (mod P). Finally (Theorem 6) we obtain a bound for

$$N_r(e, a(x)) - \frac{\phi(e)}{p^n - 1} N_r(a(x)),$$

Presented to the Society, February 23, 1952; received by the editors January 4, 1952.

where $N_r(e, a(x))$ is the number of polynomials of degree $<r$ belonging simultaneously to e and $a(x)$, and $N_r(a(x))$ is the number of polynomials of degree $<r$ belonging to $a(x)$.

2. Notation. Following Ore, we shall generalize slightly the concepts defined above. For $\gamma \in GF(p^{nm})$, let

$$(2.1) \qquad a(x) = \sum_{r=0}^{k} a_r x^{p^{nr}} \qquad (a_r \in GF(p^n),\ a_m \neq 0)$$

be a "linear" polynomial of minimal order k such that $a(\gamma)=0$; γ is said to *belong* to $a(x)$. If $A=A(x)=a_0+a_1x+\cdots+a_mx^k$, we say that $a(x)$ *corresponds* to $A(x)$. Let $B=B(x)$ be another polynomial $\in GF[p^n, x]$ and $b(x)$ the corresponding linear polynomial; then if $C=AB$ and $c(x)$ corresponds to $C(x)$ we have $c(x)=a(b(x))=b(a(x))$. If $A(x)\,|\,x^m-1$, then there are precisely $\Phi(A)$ numbers $\in GF(p^{nm})$ which belong to $a(x)$, where $\Phi(A)$ now denotes the Euler function for $GF[p^n, x]$.

If θ belongs to the linear polynomial $x^{p^{nm}}-x$, then the numbers θ, $\theta^{p^n}, \cdots, \theta^{p^{n(m-1)}}$ form a *normal basis* of $GF(p^{nm})$ relative to $GF(p^n)$; we shall say that θ generates the basis. There are $\Phi(x^m-1)/m$ such normal bases; indeed if $\alpha=a(\theta)$, where $a(x)$ has the same meaning as above, then α generates a normal basis if and only if $(A(x), x^m-1)=1$. If $(A(x), x^m-1)=D(x)$ and $x^m-1=D(x)B(x)$, then $\alpha=a(\theta)$ belongs to $b(x)$, where $b(x)$ corresponds to $B(x)$; in particular if $x^m-1=A(x)B(x)$, then α belongs to $b(x)$.

3. The λ-functions. We now define a set of functions $\lambda(\alpha)$ as follows. Let $c_0, c_1, \cdots, c_{m-1}$ be m arbitrary numbers of $GF(p^n)$ and let θ generate a normal basis of $GF(p^{nm})$ relative to $GF(p^n)$. Put

$$(3.1) \qquad \alpha = a_0\theta + a_1\theta^{p^n} + \cdots + a_{m-1}\theta^{p^{n(m-1)}} \qquad (a_r \in GF(p^n)).$$

Then we define

$$(3.2) \qquad \lambda(\alpha) = \lambda_c(\alpha) = \zeta^{t(a_0c_0+\cdots+a_{m-1}c_{m-1})},$$

where $\zeta = 2^{2\pi i/p}$ and

$$t(a) = a + a^p + \cdots + a^{p^{n-1}},$$

so that $t(a) \in GF(p)$. It follows at once that

$$(3.3) \qquad \lambda(\alpha+\beta) = \lambda(\alpha)\lambda(\beta), \qquad \lambda(0) = 1.$$

There are evidently p^{nm} distinct λ-functions; the function $\lambda_0(\alpha)\equiv 1$ corresponds to $c_0=\cdots=c_{m-1}=0$.

The λ's are evidently characters of the additive group of $GF(p^n)$. Note that for $\lambda \neq \lambda_0$,

$$(3.4) \qquad \sum_{\beta\in GF(p^{nm})} \lambda(\alpha\beta) = \begin{cases} p^{nm} & (\alpha = 0) \\ 0 & (\alpha \neq 0); \end{cases}$$

also that for $a \in GF(p^n)$, the sum

$$\sum_{b \in GF(p^n)} \zeta^{t(ab)} = \begin{cases} p^n & (a = 0) \\ 0 & (a \neq 0). \end{cases} \tag{3.5}$$

Next let $\beta_1, \cdots, \beta_r \in GF(p^{nm})$ and be linearly independent relative to $GF(p^n)$. The numbers

$$\beta = b_1\beta_1 + \cdots + b_r\beta_r \qquad (b_i \in GF(p^n))$$

define a module M_r of rank r. We now state without proof some lemmas which can be obtained by standard arguments.

LEMMA 1. *For* $\lambda \neq \lambda_0$, $\alpha \in GF(p^{nm})$,

$$\sum_{\beta \in M_r} \lambda(\alpha\beta) = \begin{cases} p^{nr} & (\alpha \in M'_{m-r}) \\ 0 & (\alpha \notin M'_{m-r}), \end{cases} \tag{3.6}$$

where M'_{m-r} *is a certain module of rank* $m-r$.

In the next place we have

$$\sum_{\lambda} \lambda(\alpha) = \begin{cases} p^{nm} & (\alpha = 0) \\ 0 & (\alpha \neq 0), \end{cases} \tag{3.7}$$

where the summation is over all p^{nm} λ's.

Suppose now that as in §2, $x^m - 1 = A(x)B(x)$ and $a(x)$ corresponds to $A(x)$. We consider the set of functions λ such that

$$\lambda(a(\gamma)) = \lambda_0(\gamma). \tag{3.8}$$

LEMMA 2. *The number of* λ's *satisfying* (3.8) *is* p^{nk}, *where* $k = \deg A(x)$.

LEMMA 3. *If* λ *runs through the* p^{nk} *solutions of* (3.8), *then the sum*

$$\sum_{\lambda} \lambda(\beta) = \begin{cases} p^{nk} & (b(\beta) = 0) \\ 0 & (b(\beta) \neq 0). \end{cases} \tag{3.9}$$

In the next place if $\chi(\alpha)$ denotes a multiplicative character for $GF(p^{nm})$, we put

$$\tau = \tau(\lambda, \chi) = \sum_{\alpha} \lambda(\alpha)\chi(\alpha). \tag{3.10}$$

Then by a familiar argument, if $\lambda \neq \lambda_0$, $\chi \neq \chi_0$,

$$\begin{aligned} |\tau|^2 &= \sum_{\alpha,\beta \neq 0} \lambda(\alpha - \beta)\chi(\alpha)\bar{\chi}(\beta) \\ &= \sum_{\alpha,\beta} \lambda((\alpha - 1)\beta)\chi(\alpha) = \sum_{\alpha} \chi(\alpha) \sum_{\beta} \lambda((\alpha - 1)\beta). \end{aligned}$$

Since by (3.4) the inner sum vanishes unless $\alpha = 1$, we have

$$|\tau| = p^{nm/2} \qquad (\lambda \neq \lambda_0,\ \chi \neq \chi_0). \tag{3.11}$$

In addition it is evident that

$$\tau(\lambda_0, \chi) = 0 \qquad (\chi \neq \chi_0), \tag{3.12}$$

$$\tau(\lambda, \chi_0) = -1 \qquad (\lambda \neq \lambda_0). \tag{3.13}$$

4. **The main theorem.** Let $p^{nm}-1=ef$ and consider the function

$$\omega(\beta) = \frac{1}{f}\sum_{d|e}\frac{\mu(d)}{d}\sum_{\chi^{df}=\chi_0}\chi(\beta), \tag{4.1}$$

where the inner sum is restricted to the df characters such that $\chi^{df}=\chi_0$. Now it is clear that

$$\sum_{\chi^f=\chi_0}\chi(\beta) = \begin{cases} f & (\beta^e = 1) \\ 0 & (\beta^e \neq 1), \end{cases}$$

so that for $d|e$

$$\frac{1}{df}\sum_{\chi^{df}=\chi_0}\chi(\beta) = \begin{cases} 1 & (\beta^{e/d} = 1) \\ 0 & (\beta^{e/d} \neq 1). \end{cases}$$

Hence if $\beta^e \neq 1$ it follows that $\omega(\beta)=0$. If β belongs to the exponent e, then $d=1$ is the only value of d that need be considered in (4.1) and we see that $\omega(\beta)=1$. Finally if β belongs to the exponent e/s, $s>1$, then (4.1) becomes

$$\omega(\beta) = \sum_{d|s}\mu(d) = 0.$$

This proves

LEMMA 4. *If β belongs to the exponent e, then $\omega(\beta)=1$; for all other β, $\omega(\beta)=0$.*

In the next place we put $x^m-1=A(x)B(x)$ and define

$$\Omega(\beta) = \frac{1}{|B|}\sum_{D|A}\frac{\mu(D)}{|D|}\sum_{\lambda^{(DB)}}\lambda(\beta) \qquad (|B| = p^{n\deg B}), \tag{4.2}$$

where the inner sum is restricted to the λ's such that $\lambda(h(\gamma))=\lambda_0(\gamma)$, where $h(x)$ is the linear polynomial corresponding to $H(x)=D(x)B(x)$. We shall prove

LEMMA 5. *If β belongs to the linear polynomial $a(x)$, then $\Omega(\beta)=1$; for all other β, $\Omega(\beta)=0$.*

In the first place it follows from Lemma 3 that for $D|A$,

$$\frac{1}{|DB|}\sum_{\lambda^{(DB)}}\lambda(\beta) = \begin{cases} 1 & (k(\beta) = 0) \\ 0 & (k(\beta) \neq 0), \end{cases}$$

where $k(x)$ corresponds to $K(x)=A(x)/D(x)$. Hence if $a(\beta)\neq 0$ the inner sum in the right member of (4.2) vanishes for all D and therefore $\Omega(\beta)=0$. If β belongs to $a(x)$ then $D=1$ is the only value of D that need be considered and it follows that $\Omega(\beta)=1$. Finally if β belongs to a linear polynomial that corresponds to $A(x)/S(x)$, $S(x)\neq 1$, it is clear that (4.2) becomes

$$\Omega(\beta) = \sum_{D\mid S} \mu(D) = 0.$$

This completes the proof of the lemma.

Combining Lemmas 4 and 5 it is evident that $\omega(\beta)\,\Omega(\beta)$ vanishes unless β simultaneously belongs to the numerical exponent e and the polynomial $a(x)$. Hence the number of such β's is given by

$$N(e, a(x)) = \sum_{\beta\in GF(p^{nm})} \omega(\beta)\Omega(\beta). \tag{4.3}$$

By (4.1), (4.2), (3.10) the right member of (4.3)

$$= \frac{1}{f\,|B|}\sum_{d\mid e} \frac{\mu(d)}{d}\sum_{D\mid A} \frac{\mu(D)}{|D|} \sum_{\chi^{df}=\chi_0}\ \sum_{\lambda^{(DB)}} \tau(\lambda, \chi). \tag{4.4}$$

Now for $\lambda=\lambda_0$, $\chi=\chi_0$ we get

$$\frac{1}{f\,|B|}\,\frac{\phi(e)}{e}\,\frac{\Phi(A)}{|A|}\,(p^{nm}-1) = \frac{\phi(e)\Phi(A)}{p^{nm}}. \tag{4.5}$$

The remaining part of (4.4)

$$\begin{aligned} &\leqq \frac{1}{f\,|B|}\sum_{d\mid e} \frac{\mu^2(d)}{d}\sum_{D\mid A} \frac{\mu^2(D)}{|D|}\cdot df\cdot |DB| \cdot |\tau(\lambda, \chi)| \\ &\leqq p^{nm/2}\sum_{d\mid e} \mu^2(d) \sum_{D\mid A} \mu^2(D), \end{aligned} \tag{4.6}$$

by Lemma 2 and (3.15), (3.12), (3.13). Hence substituting from (4.4), (4.5), (4.6) in (4.3) we have

$$\left| N(e, a(x)) - \frac{\phi(e)\Phi(A)}{p^{nm}}\right| \leqq p^{nm/2}\delta(e)\Delta(A), \tag{4.7}$$

where

$$\delta(e) = \sum_{d\mid e} \mu^2(d), \qquad \Delta(A) = \sum_{D\mid A} \mu^2(D).$$

It therefore follows that

$$N(e, a(x)) = \frac{\phi(e)\Phi(A)}{p^{nm}} + O(p^{nm(1/2+\epsilon)}) \qquad (p^{nm}\to\infty), \tag{4.8}$$

where we have used

$$\delta(m) = O(m^\epsilon), \qquad \Delta(M) = O(|M|^\epsilon).$$

The first of these is familiar, the second can be proved in a similar way.

For the applications (4.7) and (4.8) are of interest mainly when the product $\phi(e)\cdot\Phi(A)$ is not too small; roughly the product should be larger than $p^{3nm/2}$. Now it is well known that

$$(4.9) \qquad m/\phi(m) = O(m^\epsilon);$$

the analogous estimate

$$(4.10) \qquad M/\Phi(M) = O(|M|^\epsilon)$$

is easily proved. If therefore $e|A| > p^{cnm}$, where $c > 3/2$, it follows from (4.9) and (4.10) that

$$\frac{\phi(e)\Phi(A)}{p^{nm}} \geqq C(\epsilon)p^{nm(c-1-\epsilon)},$$

where $C(\epsilon)$ is a positive number depending only on ϵ. Comparison with (4.8) now shows that $N \neq 0$.

We now state

THEOREM 1. *Let $p^{nm}-1=ef$, $x^m-1=A(x)B(x)$; let $N=N(e, a(x))$ denote the number of β's in $GF(p^{nm})$ which simultaneously belong to e, $a(x)$. Then N satisfies* (4.7) *and* (4.8). *In particular if $e|A| > p^{cnm}$, $c > 3/2$, then $N > 0$ for p^{nm} sufficiently large; indeed*

$$N \sim \phi(e)\Phi(A)/p^{nm}.$$

For example, the theorem applies when

$$e = (p^{nm} - 1)/(p^n - 1), \qquad A = (x^m - 1)/(x - 1).$$

If $e = p^{nm}-1$, $A(x) = x^m - 1$, we get as an immediate corollary:

THEOREM 2. *Let N' denote the number of β's that are simultaneously primitive roots of the first and second kind; then*

$$N' = \frac{\phi(p^{nm} - 1)\Phi(x^m - 1)}{p^{nm}} + O(p^{nm(1/2+\epsilon)}).$$

It follows, therefore, that $N' > 0$ if p^{nm} exceeds a certain numerical bound. Whether there are any exceptions for small values of p^{nm} is not known.

When the condition on $e|A|$ in Theorem 1 is not satisfied we have

THEOREM 3. *If, with the notation of Theorem* 1, $e|A| = O(p^{nm(3/2+\epsilon)})$, *then*

$$N = O(p^{nm(1/2+\epsilon)}).$$

5. **Some other results.** It will now be convenient to use the concrete representation $GF[p^n, x]/P(x)$ for the $GF(p^{nm})$, where $P(x)$ is an irreducible

polynomial$\in GF[p^n, x]$ of degree m. Thus the results of §4 can be expressed in terms of polynomials (mod $P(x)$). Davenport [3] showed that for large p, one can always find primitive roots of the first degree. It does not seem possible to carry over the proof for the type of problem considered in this paper, even if we allow the required polynomial to be of degree $\leqq m/2$, say. The difficulty appears for example in the problem of primitive roots of the second kind of a given degree. It would suffice to have a nontrivial estimate for

$$S_r = S_r(\lambda) = \sum_{\deg A<r} \lambda(A) \qquad (\lambda \neq \lambda_0), \tag{5.1}$$

where the summation is over all A (including 0) of degree $<r$, and $\lambda(A)$ is defined in accord with the definition of $\lambda(\alpha)$ in §3. It follows from (5.1) that

$$|S_r|^2 = \sum_{\deg A<r,\ \deg B<r} \lambda(A-B) = p^{nr} \sum_{\deg A<r} \lambda(A) = p^{nr}S_r. \tag{5.2}$$

Thus $S_r=0$ or p^{nr}. We have also, using (3.9),

$$\sum_\lambda S_r = \sum_{\deg A<r} \sum_\lambda \lambda(A) = p^{nm}.$$

Hence for $p^{n(m-r)}$ λ's we have $S_r(\lambda)=p^{nr}$, for the remaining functions $S_n(\lambda)=0$. However this information apparently does not suffice for the problem mentioned above. We shall instead prove the following result in the opposite direction (compare [3, Theorem 2]).

THEOREM 4. *For given p^n, $r \geqq 0$, there exist infinitely many irreducible $P \in GF[p^n, x]$ such that $a(R)\equiv 0$ (mod P) for all $R \in GF[p^n, x]$,* deg $M \leqq r$, *where $a(x)$ corresponds to $A(x)=(x^m-1)/(x-1)$, $m=$*deg P.

It follows that no polynomial R of degree $\leqq r$ can be a primitive root of the second kind (mod P).

To prove the theorem, we note first that the condition $a(R)\equiv 0$ is equivalent to the existence of a polynomial U such that

$$U^{p^n} - U \equiv R \pmod{P}. \tag{5.3}$$

It is possible to make use of some known results [2, §11] concerning the congruence (5.3); however it is perhaps simpler to give a direct proof of the following theorem.

THEOREM 5. *Put $P=x^m+c_1x^{m-1}+\cdots+c_m$, $c_j\in GF(p^n)$. Then a necessary and sufficient condition that*

$$a(R) = R + R^{p^n} + \cdots + R^{p^{n(m-1)}} \equiv 0 \pmod{P}$$

for all R of degree $\leqq r$ is furnished by

$$p \mid m; \qquad c_s = 0 \qquad (1 \leqq s \leqq r,\ p \nmid s). \tag{5.4}$$

Let u be an additional indeterminate; then we have

$$P(u) \equiv \prod_{s=0}^{m-1} (u - x^{p^{ns}}) \pmod{P(x)},$$

from which it follows on differentiating that

$$\begin{aligned} P'(u) &\equiv \sum_s \frac{P(u)}{u - x^{p^{ns}}} \equiv \sum_s \frac{P(u) - P(x^{p^{ns}})}{u - x^{p^{ns}}} \\ &\equiv \sum_{r=1}^{m} \sum_{s=0}^{m-1} c_{m-r} \frac{u^r - x^{rp^{ns}}}{u - x^{p^{ns}}} \qquad (c_0 = 1) \\ &\equiv \sum_{r=1}^{m} \sum_{s=0}^{m-1} c_{m-r}(u^{r-1} + x^{p^{ns}} u^{r-2} + \cdots + x^{(r-1)p^{ns}}) \\ &\equiv \sum_{r=1}^{m} \sum_{i=1}^{r} c_{m-r} u^{i-1} a(x^{r-i}) \\ &\equiv \sum_{i=1}^{m} u^{i-1} \sum_{r=i}^{m} c_{m-r} a(x^{r-i}) \pmod{P(x)}. \end{aligned}$$

On the other hand since

$$P'(u) = mu^{m-1} + (m-1)c_1 u^{m-2} + \cdots + c_{m-1},$$

comparison of coefficients leads to the following set of congruences:

$$\begin{aligned} m &\equiv a(1), \\ (m-1)c_1 &\equiv c_1 a(1) + a(x), \\ (m-2)c_2 &\equiv c_2 a(1) + c_1 a(x) + a(x^2), \\ &\cdots\cdots, \\ (m-r)c_r &\equiv c_r a(1) + c_{r-1} a(x) + \cdots + a(x^r). \end{aligned} \tag{5.5}$$

If we now assume

$$a(1) \equiv a(x) \equiv \cdots \equiv a(x^r) \equiv 0 \pmod{P}, \tag{5.6}$$

then (5.4) holds. Indeed $p \mid m$ follows from the first congruence, while the remainder of (5.4) is true since nothing is asserted when $p \mid s$. Conversely if (5.4) holds, then (5.6) as is clear from (5.5) and the fact that $a(x^{rp}) \equiv a^p(x^r)$; consequently $a(R) \equiv 0$ for all R, deg $R \leqq r$. This completes the proof of Theorem 5.

Returning to the proof of Theorem 4 it is now necessary only to show the existence of irreducibles of degree m for which (5.4) holds. Put

$$P^*(x) = x^m P\left(\frac{1}{x}\right) = 1 + c_1 x + \cdots + c_m x^m.$$

Then by Artin's refinement [1, p. 246] of Kornblum's theorem [4] we can assert the existence of irreducibles P^* of sufficiently high degree such that

$$P^*(x) \equiv G(x) \pmod{x^r},$$

where $G(x)$ is an arbitrary polynomial subject only to $x \nmid G(x)$. In particular then the conditions (5.4) can be satisfied. Theorem 4 now follows immediately.

Returning to the problem mentioned at the beginning of this section, the following result may be of some interest.

THEOREM 6. *Let $N_r(e, a(x))$ denote the number of polynomials A of degree $<r$ which simultaneously belong to e and $a(x)$* (mod P); *let $N_r(a(x))$ denote the number that belong to $a(x)$. Then*

$$N_r(e, a(x)) = \frac{\phi(e)}{p^{nm} - 1} N_r(a(x)) + O(p^{nm(1/2+\epsilon)}). \tag{5.7}$$

Indeed as in §4, we have

$$\begin{aligned} N_r(e, a(x)) &= \sum_{\deg R<r} \omega(R)\Omega(R) \\ &= \frac{1}{f|B|} \sum_{d|e} \frac{\mu(d)}{d} \sum_{D|A} \frac{\mu(D)}{|D|} \sum_{\chi^{df}=\chi_0} \sum_{\lambda^{(DB)}} \tau_r(\lambda, \chi), \end{aligned} \tag{5.8}$$

where

$$\tau_r(\lambda, \chi) = \sum_{\deg R<r} \lambda(R)\chi(R).$$

Similarly

$$N_r(a(x)) = \frac{1}{|B|} \sum_{D|A} \frac{\mu(D)}{|D|} \sum_{\lambda^{(DB)}} \tau_r(\lambda), \tag{5.9}$$

where $\tau_r(\lambda) = \sum_{\deg R<r} \lambda(R)$.

Now for $\lambda \neq \lambda_0$, $\chi \neq \chi_0$, $R \neq 0$,

$$\begin{aligned} \lambda(R)\chi(R)\tau(\bar{\lambda}, \bar{\chi}) &= \sum_{\deg U<m} \lambda(R - U)\chi(R)\bar{\chi}(U) \\ &= \sum_{U} \lambda(R(1 - U))\bar{\chi}(U), \end{aligned}$$

so that

$$\tau_r(\lambda, \chi)\tau(\bar{\lambda}, \bar{\chi}) = \sum_{U} \bar{\chi}(U) \sum_{\deg R<r} \lambda(R(1 - U)).$$

Therefore by (3.6) and (3.11)

$$|\tau_r(\lambda, \chi)| \leqq p^{nm/2} \qquad (\lambda \neq \lambda_0, \chi \neq \chi_0). \tag{5.10}$$

It is also easy to show in the same way that

$$(5.11) \qquad \left| \sum_{\deg R < r} \chi(R) \right| \leqq p^{nm/2} \qquad (\chi \neq \chi_0).$$

Now using (5.8) and (5.9), we have

$$\begin{aligned}
&\left| N_r(e, a(x)) - \frac{\phi(e)}{p^{nm} - 1} N_r(a(x)) \right| \\
&\qquad = \frac{1}{f|B|} \left| \sum_{d|e} \frac{\mu(d)}{d} \sum_{D|A} \frac{\mu(D)}{|D|} \sum_{\lambda^{(DB)}} \left(\sum_{\chi^{df} = \chi_0} \tau_r(\lambda, \chi) - \tau_r(\lambda) \right) \right| \\
&\qquad \leqq \frac{1}{f|B|} \sum_{d|e} \frac{\mu^2(d)}{d} \sum_{D|A} \frac{\mu^2(D)}{|D|} \sum_{\lambda^{(DB)}} \left(\sum_{\chi \neq \chi_0} |\tau_r(\lambda, \chi)| + 1 \right) \\
&\qquad = O(p^{nm(1/2+\epsilon)})
\end{aligned}$$

by (5.10) and (5.11). This completes the proof of (5.7).

In the same way we can prove a theorem like Theorem 6 in which the polynomials belonging to e and $a(x)$ are primary of degree r.

References

1. E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, Math. Zeit. vol. 19 (1924) pp. 153–246.

2. L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. vol. 1 (1935) pp. 137–168.

3. H. Davenport, *On primitive roots in a finite field*, Quart. J. Math. Oxford Ser. vol. 8 (1937) pp. 308–312.

4. H. Kornblum, *Über die Primfunktionen in einer arithmetischen Progression*, Math. Zeit. vol. 5 (1919) pp. 100–111.

5. E. Landau, *Vorlesungen über Zahlentheorie*, vol. II, Leipzig, 1927.

6. O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. vol. 36 (1934) pp. 243–274.

Duke University,
Durham, N. C.