ACTA ARITHMETICA
XXXII (1977)

Elementary methods in the theory of L-functions, VII
Upper bound for $L(1,\chi)$

by

J. PINTZ (Budapest)

1. If χ is a real nonprincipal character $(\bmod D)$, then the upper bound which one can give for $L(1,\chi)$ is closely connected with the upper bound of

$$S_\chi = \max_{1\leqslant a<b\leqslant D}\Big|\sum_{n=a}^{b}\chi(n)\Big|. \tag{1.1}$$

Using the trivial $S_\chi\leqslant D$ one can easily prove $L(1,\chi)\leqslant \log D+O(1)$; by means of the Pólya–Vinogradov inequality $S_\chi\leqslant c\sqrt{D}\log D$

$$L(1,\chi)\leqslant \big(\tfrac{1}{2}+o(1)\big)\log D \tag{1.2}$$

(see Pólya [7]) can be proved.

If $D=p$ is a prime, χ a real nonprincipal character $(\bmod p)$, then making use of Burgess's inequality [1]

$$\Big|\sum_{n=N+1}^{N+H}\chi(n)\Big|\leqslant \varepsilon H \quad \text{for} \quad H>p^{1/4+\varepsilon},\ p>p_0(\varepsilon), \tag{1.3}$$

S. Chowla [4] in 1964 proved the inequality

$$L(1,\chi_p)\leqslant \big(\tfrac{1}{4}+o(1)\big)\log p. \tag{1.4}$$

Burgess [2] showed in 1966 that

$$L(1,\chi_p)<0.2456\ldots\log p. \tag{1.5}$$

Wirsing (unpublished) improved it to

$$L(1,\chi_p)<\tfrac{1}{2}\big(\sqrt{2}-1+o(1)\big)\log p\approx 0.207\log p. \tag{1.6}$$

P. J. Stephens [8] showed in 1972 using a method of Wirsing that

$$L(1,\chi_p)<\tfrac{1}{2}\Big(1-\frac{1}{\sqrt{e}}+o(1)\Big)\log p\approx 0.197\log p. \tag{1.7}$$

Now we give an elementary proof of Stephens's result (using Burgess's inequality) generalizing it for real primitive characters, whose modulus is not nessecarily prime, and improve (1.2) for real non-principal characters. Our result will follow from the following general theorem.

THEOREM 1. *If θ is a completely multiplicative function, which takes only the values $+1$, 0, -1, x a real number for which*

$$\sum_{n\leqslant x}\theta(n)\leqslant \varepsilon x \tag{1.8}$$

then

$$\sum_{d\leqslant x}\frac{\theta(d)}{d}\leqslant 2\left(1-\frac{1}{\sqrt{e}}+\delta\right)\log x \tag{1.9}$$

where $\delta=\delta(\varepsilon, x)\to 0$ if $x\to\infty$ and $\varepsilon\to 0$.

Theorem 1 is the best possible, because if we choose

$$\theta(p)=\begin{cases}1 & \text{for}\quad p\leqslant x^{1/\sqrt{e}},\\ -1 & \text{for}\quad p> x^{1/\sqrt{e}}\quad (p \text{ is a prime})\end{cases}$$

then it is easy to see that (1.8) is true with $\varepsilon=o(1)$ and that in (1.9) equality holds with $\delta=o(1)$.

But Burgess [3] proved that if χ is a nonprincipal character (mod D), then

$$\Big|\sum_{n=N+1}^{N+H}\chi(n)\Big|\leqslant \varepsilon H \quad \text{for}\quad H\geqslant D^{\tau_\chi+\varepsilon};\ D>D_0(\varepsilon) \tag{1.10}$$

where if χ is a primitive character then $\tau_\chi=1/4$ and for an arbitrary χ, $\tau_\chi=3/8$. Thus using (1.10) we have by partial summation

$$\Big|\sum_{D^{\tau_\chi+\varepsilon}<d\leqslant D}\frac{\chi(d)}{d}\Big|\leqslant \varepsilon\log D \tag{1.11}$$

and using the trivial estimation $S_\chi\leqslant D$ by means of Abel's inequality we get

$$\Big|\sum_{d>D}\frac{\chi(d)}{d}\Big|\leqslant 1. \tag{1.12}$$

So using Theorem 1 with $x=D^{\tau_\chi+\varepsilon}$ we have from (1.11) and (1.12)

THEOREM 2. *If χ is a real primitive character* (mod D), *then*

$$L(1,\chi)\leqslant \frac{1}{2}\left(1-\frac{1}{\sqrt{e}}+o(1)\right)\log D \tag{1.13}$$

if χ is a real nonprincipal character (mod D), *then*

$$L(1,\chi)\leqslant \frac{3}{4}\left(1-\frac{1}{\sqrt{e}}+o(1)\right)\log D. \tag{1.14}$$

(1.13) is in the following sense the best possible for $D=p$: If the least quadratic non-residue (mod p),

$$N(p)\geqslant p^{\frac{1}{4\sqrt{e}}-o(1)}$$

then it is easy to see that in (1.13) the equality is valid. Thus any improvement of (1.13) is only possible if we improve Burgess's theorem [1] concerning the least quadratic non-residue (mod p) to

$$N(p)=O(p^\eta) \tag{1.15}$$

with an $\eta<\dfrac{1}{4\sqrt{e}}$.

The upper bound of $L(1,\chi)$ is in connection with the class number and fundamental unit of quadratic fields. Using (1.4) S. Chowla ([4], [5]) proved that if p is a prime $\equiv 1\ (4)$, then for the class number $h(p)$, and fundamental unit $\varepsilon>1$ of $Q(\sqrt{p})$ one has

$$h(p)\leqslant \left(\tfrac{1}{4}+o(1)\right)\log p \tag{1.16}$$

and

$$\varepsilon\leqslant e^{\left(\frac{1}{8}+o(1)\right)\sqrt{p}\log p}. \tag{1.17}$$

He also proved [5] that if p is a prime $\equiv 3\ (4)$, then for the class number $h(-p)$ of $Q(\sqrt{-p})$

$$h(-p)\leqslant\left(\frac{1}{4\pi}+o(1)\right)\sqrt{p}\log p \tag{1.18}$$

holds. If D or $-D$, respectively is not a prime but a fundamental discriminant the best known upper bounds for class numbers of quadratic fields belonging to the discriminant D or $-D$ respectively, are due to Landau [6], who proved the inequalities

$$h(D)\leqslant\left(\tfrac{1}{2}+o(1)\right)\sqrt{D}\qquad (D>0) \tag{1.19}$$

and

$$h(-D)\leqslant\left(\frac{1}{2\pi}+o(1)\right)\sqrt{D}\log D\qquad (-D<0). \tag{1.20}$$

Taking into account the well-known class number formulae

$$2h(D)\log\varepsilon=\sqrt{D}L(1,\chi)\quad\left(\chi(n)=\left(\frac{D}{n}\right),\ D>0\right),\tag{1.21}$$

$$h(-D)=\frac{\sqrt{D}}{\pi}L(1,\chi)\quad\left(\chi(n)=\left(\frac{-D}{n}\right),\ -D<-4\right)\tag{1.22}$$

and the inequality

$$\varepsilon\geqslant\tfrac{1}{2}(\sqrt{D}+1),\tag{1.23}$$

Theorem 2 gives the following improvements of the results of S. Chowla and Landau ((1.16)–(1.20)):

THEOREM 3. *For the class number $h(D)$ and for the fundamental real unit $\varepsilon>1$ of the real quadratic field belonging to the fundamental discriminant $D>0$ the inequalities*

$$h(D)\leqslant\frac{1}{2}\left(1-\frac{1}{\sqrt{e}}+o(1)\right)\sqrt{D}\tag{1.24}$$

and

$$\varepsilon\leqslant e^{\frac{1}{4}\left(1-\frac{1}{\sqrt{e}}+o(1)\right)\sqrt{D}\log D}\tag{1.25}$$

hold.

THEOREM 4. *For the class number $h(-D)$ of the imaginary quadratic field belonging to the fundamental discriminant $-D<0$ the inequality*

$$h(-D)\leqslant\frac{1}{2\pi}\left(1-\frac{1}{\sqrt{e}}+o(1)\right)\sqrt{D}\log D\tag{1.26}$$

holds.

2. To prove Theorem 1 first we note that if

$$g(n)=\sum_{d\mid n}\theta(d)\tag{2.1}$$

then as $\theta(d)=O(1)$, we get

$$\sum_{n\leqslant x}g(n)=\sum_{d\leqslant x}\theta(d)\left[\frac{x}{d}\right]=x\sum_{d\leqslant x}\frac{\theta(d)}{d}+O(x).\tag{2.2}$$

Let P,Q,T denote the sets of those primes, $\leqslant x$, for which

$$P=\{p;\,\theta(p)=-1\},\quad Q=\{q;\,\theta(q)=0\},\quad T=\{t;\,\theta(t)=1\}.\tag{2.3}$$

Let $d(n)$ denote the number of divisors of n.

Then we shall prove

LEMMA 1. *With the notations (2.1)–(2.3) we have*

$$\sum_{n\leqslant x}g(n)\leqslant\sum_{n\leqslant x}d(n)-2\sum_{p\in P}\sum_{\substack{p\mid n\\ n\leqslant x}}d\left(\frac{n}{p}\right)+2\sum_{p\in P}\sum_{\substack{p^2\mid n\\ n\leqslant x}}d\left(\frac{n}{p^2}\right)+$$
$$+2\sum_{p'\in P}\sum_{p''\in P}\sum_{\substack{p'p''\mid n\\ n\leqslant x}}d\left(\frac{n}{p'p''}\right)-\sum_{q\in Q}\sum_{\substack{q\mid n\\ q\leqslant x}}d\left(\frac{n}{q}\right)+2\sum_{q\in Q}\sum_{p\in P}\sum_{\substack{pq\mid n\\ n\leqslant x}}d\left(\frac{n}{pq}\right).\tag{2.4}$$

Proof. Let $c(n)d(n)$ be the sum of those terms on the right side which belong to the number n (i.e. the sum of those terms which have the form $d(n/s)$).

We can write n in the form $n=abm$,

$$m=p_1^{\alpha_1}\ldots p_r^{\alpha_r},\quad b=q_1^{\beta_1}\ldots q_s^{\beta_s},\quad a=t_1^{\gamma_1}\ldots t_u^{\gamma_u}\tag{2.5}$$

where $p_i\in P$, $q_i\in Q$, $t_i\in T$. Then we have

$$c(n)=1-2\sum_{i=1}^{r}\frac{\alpha_i}{\alpha_i+1}+2\sum_{i=1}^{r}\frac{\alpha_i-1}{\alpha_i+1}+2\sum_{i=1}^{r}\sum_{\substack{j=1\\ j\neq i}}^{r}\frac{\alpha_i\alpha_j}{(\alpha_i+1)(\alpha_j+1)}-$$
$$-\sum_{j=1}^{s}\frac{\beta_j}{\beta_j+1}+2\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{\beta_j\alpha_i}{(\beta_j+1)(\alpha_i+1)}$$
$$=1+A+B=C+B\tag{2.6}$$

where

$$A=2\sum_{i=1}^{r}\frac{1}{\alpha_i+1}\left(\alpha_i\sum_{\substack{j=1\\ j\neq i}}^{r}\frac{\alpha_j}{\alpha_j+1}-1\right)\tag{2.7}$$

and

$$B=\sum_{j=1}^{s}\frac{\beta_j}{\beta_j+1}\left(2\sum_{i=1}^{r}\frac{\alpha_i}{\alpha_i+1}-1\right).\tag{2.8}$$

Now let us regard the following cases:

I. If $r=0$, i.e. $m=1$, then

$$c(n)=1-\sum_{j=1}^{s}\frac{\beta_j}{\beta_j+1}\geqslant\prod_{j=1}^{s}\frac{1}{\beta_j+1}=\frac{1}{d(b)}.$$

If $r\geqslant 1$ then from (2.7) $B\geqslant 0$ and so $c(n)\geqslant C$.

II. If $r=1$, then

$$C=1-\frac{2}{\alpha_1+1}=\frac{\alpha_1-1}{\alpha_1+1}\ (\geqslant 0).$$

III. If $r=2$, and $a_1=1$ or $a_2=1$, say $a_1=1$, then

$$C=1-2\left(\frac{1}{2}+\frac{1}{a_2+1}\right)+2\cdot 2\cdot\frac{1}{2}\cdot\frac{a_2}{a_2+1}=\frac{2(a_2-1)}{a_2+1}\geqslant 0.$$

IV. If $r=2$, and $a_i\geqslant 2$ for $i=1,2$ or $r\geqslant 3$, then for an arbitrary $i\leqslant r$

$$a_i\sum_{\substack{j=1\\ j\neq i}}^{r}\frac{a_j}{a_j+1}\geqslant 1$$

and so $A\geqslant 0$, $C\geqslant 1$.

On the other hand, one has

$$g(n)=\sum_{d|n}\theta(d)=\prod_{p^\gamma\|n}\big(1+\theta(p)+\ldots+\theta^\gamma(p)\big). \tag{2.9}$$

Hence

$$g(n)=g(a)g(b)g(m)=\begin{cases}d(a) & \text{if}\quad m=l^2,\\ 0 & \text{if}\quad m\neq l^2.\end{cases}$$

So in the following cases we have:

I. $g(n)=d(a)=\dfrac{d(n)}{d(b)}\leqslant c(n)d(n)$;

II. if a_1 is odd, then $0=g(n)\leqslant C\leqslant c(n)\leqslant c(n)d(n)$,

if a_1 is even, then $g(n)=d(a)\leqslant\dfrac{d(n)}{a_1+1}\leqslant Cd(n)\leqslant c(n)d(n)$;

III. $0=g(n)\leqslant C\leqslant c(n)\leqslant c(n)d(n)$;

IV. $g(n)\leqslant d(a)\leqslant d(n)\leqslant Cd(n)\leqslant c(n)d(n)$.

Thus in all cases $g(n)\leqslant c(n)d(n)$ which proves Lemma 1.

Now let $S=P\cup Q$, and for $s\in S$, let

$$\mathbf{s}=\begin{cases}s & \text{if}\quad s\in P,\\ 2s & \text{if}\quad s\in Q.\end{cases} \tag{2.10}$$

Then using the well-known relations

$$\sum_{\substack{n\leqslant x\\ l|n}}d\left(\frac{n}{l}\right)=\sum_{m\leqslant x/l}d(m)=\frac{x}{l}\log\frac{x}{l}+O\left(\frac{x}{l}\right),$$

$$\sum_{\substack{p\leqslant x\\ p\ \text{prime}}}\frac{1}{p}=o(\log x),\qquad \sum_{\substack{p\leqslant x\\ p\ \text{prime}}}\ \sum_{\substack{p'\leqslant x\\ p'\ \text{prime}}}\frac{1}{pp'}=o(\log x),$$

if we add to the right side of (2.4)

$$\frac{1}{2}\sum_{q\in Q}\sum_{\substack{q'\in Q\\ qq'\leqslant x}}\frac{x}{qq'}\log\frac{x}{qq'}\geqslant 0,$$

then we have with the notation (2.10) the following

COROLLARY. *We have*

$$\sum_{n\leqslant x}g(n)\leqslant x\log x\left(1-\frac{2}{\log x}U+o(1)\right) \tag{2.11}$$

where

$$U=\sum_{s\in S}\frac{1}{\mathbf{s}}\log\frac{x}{s}-\sum_{s\in S}\sum_{\substack{s'\in S\\ ss'\leqslant x}}\frac{1}{\mathbf{ss'}}\log\frac{x}{ss'}. \tag{2.12}$$

Thus we have to estimate U from below.

Here we shall use the supposition $\sum_{d\leqslant x}\theta(d)\leqslant\varepsilon x$ from which

$$o(1)x\geqslant\sum_{d\leqslant x}\theta(d)=[x]-2\sum_{\substack{d\leqslant x\\ \theta(d)=-1}}1-\sum_{\substack{d\leqslant x\\ \theta(d)=0}}1$$

$$\geqslant 2\sum_{p\in P}\frac{x}{p}-\sum_{q\in Q}\frac{x}{q}=x\left(1-2\sum_{s\in S}\frac{1}{\mathbf{s}}\right)-1$$

follows. Hence

$$\sum_{s\in S}\frac{1}{\mathbf{s}}\geqslant\frac{1}{2}-o(1). \tag{2.13}$$

Let

$$S=\{s_1<s_2<\ldots<s_k\}$$

and

$$S'=\left\{s_1<s_2<\ldots<s_l:\ \sum_{i=1}^{l+1}\frac{1}{\mathbf{s}_i}>\frac{1}{2}\geqslant\sum_{i=1}^{l}\frac{1}{\mathbf{s}_i}\right\}. \tag{2.14}$$

(If $\sum_{s\in S}\frac{1}{\mathbf{s}}\leqslant\frac{1}{2}$ then let $S'=S$.)

Now we define a $\theta'(n)$ completely multiplicative function for $n\leqslant x$ with

$$\begin{aligned}\theta'(p)&=-1 &&\text{if}\quad p\in P\cap S',\\ \theta'(q)&=0 &&\text{if}\quad q\in Q\cap S',\\ \theta'(t)&=1 &&\text{if}\quad t\in T\cup(S\setminus S').\end{aligned}$$

Thus we have from (2.9) for an arbitrary n

$$\sum_{d|n}\theta(d) = g(n) \leqslant g'(n) = \sum_{d|n}\theta'(d). \tag{2.15}$$

So we shall use the Corollary for $\theta'(n)$ and we shall estimate the corresponding U', i.e. we shall prove

LEMMA 2. *We have*

$$U' = \sum_{s}\frac{1}{\mathbf{s}}\log\frac{x}{s} - \sum_{s}\sum_{s'\leqslant x/s}\frac{1}{\mathbf{s}\mathbf{s}'}\log\frac{x}{ss'} \geqslant \left(\frac{1}{\sqrt{e}}-\frac{1}{2}+o(1)\right)\log x \tag{2.16}$$

where the summation in Lemma 2 runs always through $s, s' \in S'$.

Proof. If in the definition of S' in (2.14) $s_{l+1} \leqslant \log x$, and $\mathbf{s} \neq s$ then as $\sum_{s}\frac{1}{\mathbf{s}} > \frac{1}{6}$, we get

$$U' \geqslant \sum_{s}\frac{1}{\mathbf{s}}\log x\big(1-o(1)\big) - \log x\sum_{s}\sum_{s'}\frac{1}{\mathbf{s}\mathbf{s}'}$$

$$\geqslant \big(1-o(1)\big)\log x\left(\sum_{s}\frac{1}{\mathbf{s}}\right)\left(1-\sum_{s'}\frac{1}{\mathbf{s}'}\right) \geqslant \left(\frac{1}{6}\cdot\frac{5}{6}-o(1)\right)\log x$$

which implies (2.16).

If $s_{l+1} > \log x$, or $\mathbf{s} = s'$ let

$$\alpha = \sum_{s\leqslant\sqrt{x}}\frac{1}{\mathbf{s}}, \qquad \beta = \sum_{\sqrt{x}<s\leqslant x}\frac{1}{\mathbf{s}}. \tag{2.17}$$

Then as $1/s_{l+1} = o(1)$, we have

$$\tfrac{1}{2} - o(1) \leqslant \alpha+\beta \leqslant \tfrac{1}{2}. \tag{2.18}$$

With these notations the following formulae hold

$$D = \sum_{s\leqslant\sqrt{x}}\frac{1}{\mathbf{s}}\log\frac{x}{s} - \sum_{s\leqslant\sqrt{x}}\sum_{s'\leqslant\sqrt{x}}\frac{1}{\mathbf{s}\mathbf{s}'}\log\frac{x}{ss'} \tag{2.19}$$

$$\geqslant \sum_{s\leqslant\sqrt{x}}\frac{1}{\mathbf{s}}\log\frac{x}{s}\left(1-\sum_{s'\leqslant\sqrt{x}}\frac{1}{\mathbf{s}'}\right)$$

$$= (1-\alpha)\log x\cdot\alpha - (1-\alpha)\sum_{s\leqslant\sqrt{x}}\frac{\log s}{\mathbf{s}},$$

$$E = \sum_{s\leqslant\sqrt{x}}\frac{1}{\mathbf{s}}\sum_{\sqrt{x}<s'\leqslant x/s}\frac{1}{\mathbf{s}'}\log\frac{x}{ss'} \leqslant \sum_{\sqrt{x}<s'\leqslant x}\frac{1}{\mathbf{s}'}\sum_{s\leqslant\sqrt{x}}\frac{1}{\mathbf{s}}\log\frac{\sqrt{x}}{s} \tag{2.20}$$

$$= \frac{1}{2}\beta\log x\cdot\alpha - \beta\sum_{s\leqslant\sqrt{x}}\frac{\log s}{\mathbf{s}},$$

$$F = \sum_{s>\sqrt{x}}\frac{1}{\mathbf{s}}\log\frac{x}{s} = \beta\log x - \sum_{\sqrt{x}<s\leqslant x}\frac{\log s}{\mathbf{s}}. \tag{2.21}$$

Here as $U' = D-2E+F$, from formulae (2.18)–(2.21) we get

$$U' \geqslant \log x\big[\alpha(1-\alpha-\beta)+\beta\big] - (1-\alpha-2\beta)\sum_{s\leqslant\sqrt{x}}\frac{\log s}{\mathbf{s}} - \sum_{\sqrt{x}<s\leqslant x}\frac{\log s}{\mathbf{s}} \tag{2.22}$$

$$= \left(\frac{1}{2}-\frac{\alpha}{2}+o(1)\right)\log x - \big(\alpha+o(1)\big)\sum_{s\leqslant\sqrt{x}}\frac{\log s}{\mathbf{s}} - \sum_{\sqrt{x}<s\leqslant x}\frac{\log s}{\mathbf{s}}.$$

On the other hand, it is easy to show that if S' is a set of primes $s \leqslant y$ $(y \neq O(1))$, $\mathbf{s} = s$ or $2s$, and

$$\sum_{s\in S'}\frac{1}{\mathbf{s}} = \gamma + o(1) \qquad (\leqslant 1) \tag{2.23}$$

(γ a given number) then the sum

$$\sum_{s\in S'}\frac{1}{\mathbf{s}}$$

is maximal if the set S' contains all primes in an interval $[z, y]$ and no primes less than z and for all primes s, $\mathbf{s} = s$. So if we use the formulae

$$\sum_{\substack{p\leqslant x\\ p\ \mathrm{prime}}}\frac{\log p}{p} = \log x + O(1), \qquad \sum_{\substack{p\leqslant x\\ p\ \mathrm{prime}}}\frac{1}{p} = \log\log x + C + o(1)$$

where C is an absolute constant, easy computation shows that if (2.23) holds then

$$\sum_{s\in S'}\frac{\log s}{\mathbf{s}} \leqslant \big(1-e^{-\gamma}+o(1)\big)\log y. \tag{2.24}$$

Thus from (2.22) and (2.24) we have

$$U' \geqslant \log x\left(\frac{1}{2}-\frac{\alpha}{2}-\frac{\alpha}{2}(1-e^{-\alpha})-(1-e^{-\beta})-o(1)\right) = G\cdot\log x. \tag{2.25}$$

Here using $\beta = \frac{1}{2} - \alpha + o(1)$, we get with some computation that for $0 \leqslant \alpha \leqslant \frac{1}{2} + o(1)$

$$(2.26) \qquad G = G(\alpha, \beta) = G(\alpha) \geqslant G(0) = \frac{1}{\sqrt{e}} - \frac{1}{2} - o(1),$$

which proves Lemma 2.

Thus we have from formulae (2.2), (2.15), (2.11), (2.12) and (2.16)

$$(2.27) \sum_{d \leqslant x} \frac{\theta(d)}{d} = \frac{1}{x} \sum_{n \leqslant x} g(n) + O(1) \leqslant \frac{1}{x} \sum_{n \leqslant x} g'(n) + O(1)$$
$$\leqslant \log x \left(1 - \frac{2U'}{\log x} + o(1)\right) \leqslant \log x \left(2\left(1 - \frac{1}{\sqrt{e}}\right) + o(1)\right).$$

References

[1] D. A. Burgess, *The distribution of quadratic residues and non residues*, Mathematika 4 (1957), pp. 106–112.

[2] — *Estimating* $L_\chi(1)$, Norske Vid. Selsk. Forh. (Trondheim) 39 (1966), pp. 101–108.

[3] — *On character sums and L-series II*, Proc. London Math. Soc. 12 (1962), pp. 193–206.

[4] S. Chowla, *Bounds for the fundamental unit of a real quadratic field*, Norske Vid. Selsk. Forh. (Trondheim) 37 (1964), pp. 85–87.

[5] — *Application of a theorem of A. Weil to improvement of bounds for class numbers of quadratic fields*, ibid. 38 (1965), pp. 84–85.

[6] E. Landau, *Abschätzungen von Charactersummen, Einheiten und Klassenzahlen*, Göttinger Nachrichten 1918, pp. 79–97.

[7] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, ibid. pp. 21–29.

[8] P. J. Stephens, *Optimizing the size of* $L(1, \chi)$, Proc. London Math. Soc. (3) 24 (1972), pp. 1–14.

EÖTVÖS LORAND UNIVERSITY
DEPARTMENT OF ALGEBRA AND NUMBER THEORY
Budapest, Hungary

Received on 20. 10. 1975 (781)

ACTA ARITHMETICA
XXXII (1977)

The factorization of $Q(L(x_1), \ldots, L(x_k))$ over a finite field where $Q(x_1, \ldots, x_k)$ is of first degree and $L(x)$ is linear

by

L. Carlitz (Durham, N. C.) and A. F. Long, Jr. (Greensboro, N. C.)

1. Introduction. Let $\mathrm{GF}(q)$ denote the finite field of order $q = p^n$ where p is prime and $n \geqslant 1$. Let $\Gamma(p)$ denote the algebraic closure of $\mathrm{GF}(p)$. A polynomial $Q \in \mathrm{GF}[q; x_1, \ldots, x_k]$ is *absolutely irreducible* if Q has no nontrivial factors over $\Gamma(p)$. Throughout this paper, the term irreducible will mean absolutely irreducible.

A polynomial with coefficients in $\mathrm{GF}(q)$ of the form

$$L(x) = \sum_{i=0}^{r} c_i x^{q^i}$$

is called a linear polynomial. The requirement that the coefficients be in $\mathrm{GF}(q)$ insures that the operation of mapping composition for linear polynomials is commutative. Corresponding to the linear polynomial $L(x)$ we have the ordinary polynomial

$$l(x) = \sum_{i=0}^{r} c_i x^i.$$

We shall assume in the following that $c_0 \neq 0$; this avoids multiple factors in $L(x)$ and insures that there is a smallest integer r such that $l(x)$ divides $x^r - 1$. We say that $l(x)$ has *exponent* r.

Let $Q(x_1, \ldots, x_k) = a_1 x_1 + \ldots + a_k x_k + 1$ where $[\deg a_1, \ldots, \deg a_k] = s$ (if $a \in \mathrm{GF}(q^s)$ but $a \notin \mathrm{GF}(q^t)$, $1 \leqslant t < s$, we say that the *degree of* a *relative to* $\mathrm{GF}(q)$ is s and write $\deg a = s$). We shall assume that $\{a_1, \ldots, a_k\}$ are linearly independent over $\mathrm{GF}(q)$; otherwise $Q(x_1, \ldots, x_k)$ can be reduced at once to a polynomial in m variables by suitable first degree transformations, where m is the number of elements in a maximal linearly independent subset of $a_1, \ldots, a_k$.

In this paper we describe the factorization of $Q(L(x_1), \ldots, L(x_k))$. (We note that it is possible to have $Q(L(x_1), \ldots, L(x_k))$ reduce to a polynomial in fewer than k variables even though $\{a_1, \ldots, a_k\}$ are linearly