Consequently if we put

$$(6.5)\qquad F_r = \begin{cases} B_k(nx) & \text{for} \quad r=0, \\ k\dfrac{\overline{\varphi}_{k-1}(n,x\,\varepsilon^s)}{\varepsilon^r-1} & \text{for} \quad r=1,\ldots,n-1, \end{cases}$$

it follows that the matrix

$$(6.6)\qquad (F_{s-r}) \quad (r,s=0,1,\ldots,n-1)$$

has the characteristic roots

$$(6.7)\qquad n^k\overline{B}_k\left(x-\frac{r}{n}\right) \quad (r=0,1,\ldots,n-1).$$

In particular we can evaluate the determinants of (6.3) and (6.5).

References

[1] L. Carlitz, *Some cyclotomic determinants*, Bulletin of the Calcutta Mathematical Society, 49 (1957), p. 49-51.

[2] R. Fricke, *Lehrbuch der Algebra*, vol. 1, Braunschweig 1924.

[3] G. Frobenius, *Über die Bernoulli'schen Zahlen und die Euler'schen Polynome*, Sitzungsberichte der Preussischen Akademie der Wissenschaften (1910), p. 809-847.

[4] E. Landau, *Vorlesungen über Zahlentheorie*, Leipzig 1927.

[5] D. H. Lehmer, *On certain character matrices*, Pacific Journal of Mathematics 6 (1956), p. 491-499.

DUKE UNIVERSITY

Reçu par la Rédaction le 27. 12. 1958

ACTA ARITHMETICA
V (1959)

A note on the real zeros of Dirichlet's *L*-functions

by

P. Turán (Budapest)

1. For $s=\sigma+it$, the L-functions of Dirichlet belonging to a modulus k are defined for $\sigma>1$ by

$$(1.1)\qquad L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s},$$

where $\chi(n)$ are the characters of the group of the reduced residue-classes $\bmod k$. It is well known that the study of zeros of these functions give the key to the distribution of primes in the arithmetical progressions $\bmod k$ and the essentially new difficulties, compared to those connected with the zeros of the Riemann zeta-function, are due to the appearance of real zeros. Concerning them we know[1] that for a suitable positive[2] c_1 at most one of the $L(s,\chi)$-functions $\bmod k$ can vanish in the interval

$$(1.2)\qquad 1-\frac{c_1}{\log k}\leqslant s\leqslant 1$$

and, if such an exceptional $L(s,\chi)$ exists, it has here a single simple zero (called *exceptional zero* and denoted by β). The possibility of an exceptional zero gives a lot of trouble in the number-theory. A typical example is furnished by the formula (Page, [2]), valid for $\chi\neq\chi_0$

$$(1.3)\qquad \Big|\sum_{n\leqslant x}\Lambda(n)\chi(n)\Big|\leqslant\begin{cases} c_2(xe^{-c_3\sqrt{\log x}}+x^{\beta}) \\ c_2xe^{-c_3\sqrt{\log x}}, \end{cases}$$

χ is an exceptional character or not, respectively; here $\Lambda(n)$ stands for the known Dirichlet symbol and $\varphi(k)$ is the usual Euler function.

(1) This is essentially due to E. Landau [1].

(2) In what follows, $c_1, c_2, \ldots$ stand for explicitly calculable positive numerical constants; as an exception $c_4=c_4(\varepsilon)$ is not and depends on ε.

For β we know at present only the estimation[3]

$$\beta < 1 - c_4(\varepsilon)/k^{\varepsilon}$$

for $0 < \varepsilon \leqslant 1$, where — curiously enough — no *explicit* form of $c_4(\varepsilon)$ is known and also that the exceptional k-values (i. e. those with an exceptional $L(s, \chi)$) if they exist at all lie very dispersed (see Landau [1]). Taking into account all these it is of some interest to note that for the greatest real zero $\gamma = \gamma(\chi) \geqslant \frac{1}{2}$ of *any* $L(s, \chi)$ function belonging to the modulus k (if there exists such a zero) only the "small" primes are responsible. More exactly we shall prove the following

THEOREM. *With* $P = e^{(\log k \log\log k)^2}$ *we have for* $k > c_5$ *the inequality*

$$\left(\tfrac{1}{2} \leqslant\right) \gamma(\chi) \leqslant 2\frac{\log\log\log k}{\log\log k} + \frac{1}{\log P} \max_{1 \leqslant X \leqslant P} \log\Big|\sum_{n \leqslant X} \Lambda(n)\chi(n)\Big|$$

for each $\chi \neq \chi_0 (\operatorname{mod} k)$ *(if there are any real zeros of* $L(s, \chi)$*).*

By more careful treatment of the details one could have the constants in the theorem replaced by smaller numerical values and the estimation refined so that it could be used also for numerical calculations with prime tables. We shall not do this. The proof of the theorem will be based, as in many former applications, on the following theorem[4].

For any arbitrary non-negative integer m and complex b_j, z_j-numbers with

(1.4) $$1 = |z_1| \geqslant |z_2| \geqslant \ldots \geqslant |z_n|$$

there is an integer ν with

(1.5) $$m+1 \leqslant \nu \leqslant m+n$$

and

(1.6) $$\Big|\sum_{j=1}^{n} b_j z_j^{\nu}\Big| \geqslant \left(\frac{n}{8e(m+n)}\right)^n \min_j |b_1 + \ldots + b_j|.$$

This theorem will be applied here in the case $b_1 = b_2 = \ldots = b_n = 1$ in the following form (which can easily be derived from (1.4)-(1.5)-(1.6)).

If $m > 0$ and $\max_j |z_j| \geqslant 1$ and $2 \leqslant n \leqslant N$, then

(1.7) $$\max_{\substack{m \leqslant \nu \leqslant m+N \\ \nu \text{ integer}}} |z_1^{\nu} + \ldots + z_n^{\nu}| \geqslant \left(\frac{N}{22(m+N)}\right)^N.$$

The proof of our present theorem is in principle similar to a previous one[5] on the remainder-term of the prime-number formula but the appearance of the parameter k necessitates unexpected changes in the choice of the parameters of the proof.

2. We turn to the proof of the theorem. We fix an arbitrary $\chi(n)$ mod k and suppose that $L(s, \chi)$ has real zeros and $\gamma \geqslant \frac{1}{2}$ is the maximal one. We shall make repeated use of the fact that for $k > c_6$ and any real τ the number of zeros of $L(s, \chi)$ in the parallelogram

(2.1) $$\sigma \geqslant \tfrac{1}{4}, \quad \tau \leqslant t \leqslant \tau + 1$$

does not exceed

(2.2) $$c_7 \log k(|\tau| + 1).$$

The integer ω will be exactly determined later; at this moment we require only

(2.3) $$\log^2 k \log\log k \leqslant \omega + 1 \leqslant \log^2 k(\log\log k + 3c_7).$$

Further let M be such that

(2.4) $$e^{\frac{(\log k \log\log k)^2}{\log^2 k(\log\log k + 3c_7) + 1}} < M \leqslant e^{\frac{(\log\log k)^2}{\log\log k + 3c_7}}$$

and then fixed; further let

(2.5) $$\xi = M^{\omega+1};$$

then owing to (2.4) and (2.3) we have

(2.6) $$\xi \leqslant e^{(\log k \log\log k)^2} = P.$$

Finally let

(2.7) $$J(\chi) = \frac{1}{2\pi i} \int_{(2)} \frac{\xi^s}{s^{\omega+1}} \cdot \frac{L'}{L}(s, \chi)\, ds.$$

---

[3] C. L. Siegel [3]. Alternative proofs are given independently by S. Chowla and T. Esterman.

[4] This is an improved form of Theorem IX of my book [5] where the theorem stands with $(n/24e^2(m+2n))^n$ instead of $(n/8e(m+n))^n$. The improvement is contained in the paper [6] (and also in the rewritten and enlarged Chinese edition of my book in 1956). As E. Makai proved (see his forthcoming paper in Acta Math. Hung.) the estimation (1.6) is no more true replacing the constant $8e$ by any one $< 2e$. The improvement of the constant $8e$ will be of significance in some applications (not here).

Added in proof. Suitable modifications lead to the following form of the theorem (again no care is given to best-possible constants).

If $k > c_5$, $\omega > c_5$ *and* $P_1 = k^{(1+\log\omega)e^{2\omega}}$ *then with* $U(x) = \sum_{n \leqslant x} \Lambda(n)\chi(n)$

$$\left(\tfrac{1}{2} \leqslant\right) \gamma(\chi) \leqslant \frac{4}{1+\log\omega} + \frac{1}{\log P_1} \max_{1 \leqslant x \leqslant P_1} \log|U(x)|.$$

The proof will be given in the forthcoming English edition of my book.

[5] See § 9 of the German edition of my book [5].

Owing to the well-known coefficient formula we have

$$J(\chi)=\frac{1}{\omega!}\sum_{n\leqslant\xi}\Lambda(n)\chi(n)\log^{\omega}\frac{\xi}{n}.$$

Putting

$$\sum_{n\leqslant v}\Lambda(n)\chi(n)=U(v,\chi) \tag{2.8}$$

we obtain

$$J(\chi)=\frac{1}{\omega!}\int_1^{\xi}\log^{\omega}\frac{\xi}{v}\,dU(v,\chi)=-\frac{1}{\omega!}\int_1^{\xi}U(v,\chi)\,d_v\log^{\omega}\frac{\xi}{v},$$

i. e. from (2.6) and (2.3)

$$\begin{aligned}|J(\chi)|&\leqslant\frac{\log^{\omega}\xi}{\omega!}\max_{1\leqslant v\leqslant\xi}|U(v,\chi)|\\&\leqslant\left(2e\frac{\log^2 k(\log\log k)^2}{\omega+1}\right)^{\omega+1}\max_{1\leqslant v\leqslant P}|U(v,\chi)|\\&\leqslant(2e\log\log k)^{\omega+1}\max_{1\leqslant v\leqslant P}|U(v,\chi)|.\end{aligned} \tag{2.9}$$

3. Using (2.2) and the known fact (see [4]) that if $\varrho=\sigma_\varrho+it_\varrho$ stand for the zeros of an $L(s,\chi)$ with any fixed χ, then for $\sigma\geqslant\frac{1}{4}$ and any real t the inequality

$$\left|\frac{L'}{L}(s,\chi)-\sum_{\substack{|t_\varrho-t|\leqslant 2\\ \sigma_\varrho\geqslant 1/5}}\frac{1}{s-\varrho}\right|\leqslant c_8\log k(|t|+1) \tag{3.1}$$

holds, we easily get the existence of a connected broken line V, consisting of segments alternately parallel to the axes, all lying in the infinite vertical strip

$$\tfrac{1}{3}\leqslant\sigma\leqslant\tfrac{1}{3}+\frac{1}{(\log k\log\log k)^2}, \tag{3.2}$$

on which the inequality

$$\left|\frac{L'}{L}(s,\chi)\right|\leqslant c_9\log^5 k(|t|+1) \tag{3.3}$$

holds. For later reasons let us observe that V does not depend upon the choice of ω. Using this and the other known fact that for any real τ with $|\tau|\geqslant 2$ we have between τ and $\tau+1$ a $t=t_\tau$ so that on the segment

$$0\leqslant\sigma\leqslant 2,\qquad t=t_\tau$$

the inequality

$$\left|\frac{L'}{L}(s,\chi)\right|\leqslant c_{10}\log^3(k|\tau|)$$

holds, we infer by usual contour integration that

$$J(\chi)=\sum_{\substack{\varrho\text{ right}\\ \text{from }V}}\frac{\xi^{\varrho}}{\varrho^{\omega+1}}+\frac{1}{2\pi i}\int_{(V)}\frac{\xi^{s}}{s^{\omega+1}}\frac{L'}{L}(s,\chi)\,ds$$

and thus using (2.6), (3.2), and (2.3) for $k>c_{11}$

$$\left|J(\chi)-\sum_{\substack{\varrho\text{ right}\\ \text{from }V}}\frac{\xi^{\varrho}}{\varrho^{\omega+1}}\right|\leqslant c_{12}P^{1/3}\log^5 k\cdot 3^{\omega+1}<\tfrac{1}{2}P^{2/5}.$$

This and (2.9) give — taking in account also (2.5) and $\gamma\leqslant 1$ — the inequality

$$\begin{aligned}&\max_{1\leqslant v\leqslant P}|U(v,\chi)|\\&\geqslant(2e\log\log k)^{-(\omega+1)}\cdot\left\{-\tfrac{1}{2}P^{2/5}-\sum_{\substack{|t_\varrho|\geqslant\log k\\ \sigma_\varrho\geqslant 1/3}}\left|\frac{\xi^{\varrho}}{\varrho^{\omega+1}}\right|+\xi^{\gamma}\left|\sum_{\substack{\varrho\text{ right}\\ \text{from }V,\\ |t_\varrho|<\log k}}\left(M^{\varrho-\gamma}\frac{\gamma}{\varrho}\right)^{\omega+1}\right|\right\}.\end{aligned} \tag{3.4}$$

4. Owing to (2.2) and (2.3) the first sum on the right of (3.4) does not exceed

$$\begin{aligned}2c_7\sum_{n\geqslant\log k}\frac{\xi}{n^{\omega+1}}\log kn&<c_{13}\frac{P\log k}{(\log k)^{\omega}}<c_{13}\frac{P\log^2 k}{(\log k)^{\log^2 k\log\log k}}\\&=c_{13}\log^2 k<\tfrac{1}{2}P^{2/5}.\end{aligned} \tag{4.1}$$

As to the factor ξ^{γ} in (3.4), we have for $k>c_{14}$ from (2.5), (2.4) and (2.3)

$$\begin{aligned}\xi^{\gamma}&>e^{\frac{(\log k\log\log k\log k)^2}{\log^2 k(\log\log k+3c_7)+1}\gamma\log^2 k\log\log k}\\&>P^{\gamma\frac{1}{1+(3c_7+1)/\log\log k}}>P^{\gamma\left(1-\frac{3c_7+1}{\log\log k}\right)}>P^{\gamma}e^{-\frac{3c_7+1}{\log\log k}}.\end{aligned} \tag{4.2}$$

We estimate the remaining sum

$$\left|\sum_{\substack{\varrho\text{ right from }V,\\ |t_\varrho|<\log k}}\left(M^{\varrho-\gamma}\frac{\gamma}{\varrho}\right)^{\omega+1}\right|\equiv|Z| \tag{4.3}$$

from below by a proper choice of ω (so that the requirement (2.3) should not be violated); this will be done by the theorem quoted in (1.7), where the role of the numbers z_j is played by the numbers $M^{\varrho-\gamma}\cdot\gamma/\varrho$ and

$$m=\log^2 k\log\log k. \tag{4.4}$$

Since the line V does not depend upon ω and the numbers $M^{\varrho-\gamma}\cdot\gamma/\varrho$ either, Z is a power-sum of fixed complex numbers indeed, where the number of terms is also independent of ω. Obviously γ is among the ϱ's so that the condition $\max_j|z_j|\geqslant 1$ is satisfied. Owing to (2.2) the number n of the terms in Z is for $k > c_{15}$

$$\leqslant 2\log k \cdot c_7 \log\big(k(1+\log k)\big) < 3c_7 \log^2 k. \tag{4.5}$$

Hence if we determine $\omega+1$ as the exponent realizing the maximum on the left of (1.7) and take

$$N = 3c_7 \log^2 k,$$

(2.3) is not violated and thus

$$|Z| \geqslant \left(\frac{3c_7\log^2 k}{22\,(\log^2 k \log\log k + 3c_7 \log^2 k)}\right)^{3c_7 \log^2 k}$$

or for $k > c_{16}$

$$|Z| > e^{-4c_7 \log^2 k \log\log\log k}$$

Putting this, (4.1) and (4.2) into (3.4) and taking in account that owing to $\gamma \geqslant \frac{1}{2}$ we have for $k > c_{17}$

$$P^{\frac{2}{5}} < \tfrac{1}{2} P^{\frac{1}{2} - \frac{3c_7+1}{\log\log k}} \cdot e^{-4c_7 \log^2 k \log\log\log k} \leqslant \tfrac{1}{2} P^{\gamma - \frac{3c_7+1}{\log\log k}} \cdot e^{-4c_7 \log^2 k \log\log\log k},$$

we get, using also (2.3),

$$\begin{aligned}\max_{1 \leqslant v \leqslant P} |U(v, \chi)| &> (2e\log\log k)^{-(\omega+1)} \tfrac{1}{2} P^{\gamma - \frac{3c_7+1}{\log\log k}} \cdot e^{-4c_7 \log^2 k \log\log\log k} \\ &> P^{\gamma - \frac{4c_7}{\log\log k}} \cdot e^{-\frac{3}{2} \log^2 k \log\log k \log\log\log k} \\ &> P^{\gamma} \cdot e^{-2\log^2 k \log\log k \log\log\log k} = P^{\gamma - 2\frac{\log\log\log k}{\log\log k}},\end{aligned}$$

which proves the theorem.

References

[1] E. Landau, *Über die Klassenzahl imaginärquadratischer Zahlenkörper*, Gött. Nachr. 1918, p. 285-295.

[2] A. Page, *On the numbers of primes in an arithmetical progression*, Proc. of London Math. Soc., Ser. 2, 39.2 (1935) p. 116-142.

[3] C. L. Siegel, *Über die Klassenzahl quadratischer Zahlkörper*, Acta Arithmetica 1 (1935), p. 83-86.

[4] E. C. Titchmarsh, *A divisor problem*, Rend. Circ. Mat. Palermo 54 (1930), p. 414-429.

[5] P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen*, Budapest 1953.

[6] — and Vera T. Sós, *On some new theorems in the theory of diophantine approximations*, Acta Math. Hung. VII. 3-4 (1955), p. 241-255.

Reçu par la Rédaction le 2. 1. 1959

ACTA ARITHMETICA
V (1959)

On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two

by

B. Segre (Rome)

Summary

§ 1. Introduction

The study of the geometry of a *Galois space* $S_{r,q}$, i. e. of a projective r-dimensional space over a Galois field of order

$$q = p^h,$$

where p, h are positive integers and p is a prime (the characteristic of the field), has recently been pursued and developed along new lines (1). In it, both algebraic-geometric and arithmetical methods have been applied, including the use of electronic calculating machines; moreover, some of the problems dealt with are deeply connected with information theory, especially with the construction of q-ary error-correcting codes. It is actually a chapter of *arithmetical geometry*, which reduces to the investigation of certain questions on congruences mod p in the particular case when $h = 1$.

A set of k distinct points of $S_{r,q}$, no three of which lie on a line, is denoted by $k_{r,q}$ and called a *k-arc* if $r = 2$ and a *k-cap* if $r \geqslant 3$; any such $k_{r,q}$ is said to be *complete* when it is not a subset of a $(k+1)_{r,q}$. For given r and q, a $k_{r,q}$ having maximum k is called an *oval* if $r = 2$ and an *ovaloid* if $r \geqslant 3$, and then it is consequently always complete.

(1) See especially [8]; further historical and bibliographical informations are contained in [7].