ACTA ARITHMETICA
XXXI (1976)

Elementary methods in the theory of L-functions, I*
Hecke's theorem

by

J. PINTZ (Budapest)

1. The first elementary results in the theory of Dirichlet's L-functions are due to Mertens, who gave direct elementary proofs for the non-vanishing of $L(1, \chi)$ in case of a real non-principal character χ (see Landau [7], § 106). Later several authors proved this fact in an elementary way. A very important elementary achievement about real L-functions was Linnik's proof [8], of the famous theorem of Siegel [17], that for any $\varepsilon > 0$

$$L(1, \chi) > D^{-\varepsilon}. \tag{1.1}$$

From this it easily follows (see Walfisz [20]) that

$$L(s, \chi) \neq 0 \quad \text{for} \quad s \in [1-D^{-\varepsilon}, 1] \tag{1.2}$$

for a real primitive character χ (mod D), provided that D exceeds an ineffective constant $D_0(\varepsilon)$ depending on ε. (The author [15] gave a simpler elementary proof of Siegel's theorem using the ideas of Linnik [8].)

Another partly elementary result due to Davenport [1], states that for a real non-principal character

$$L(s, \chi) \neq 0 \quad \text{for} \quad s \in \left[1-\frac{c}{\sqrt{D}\log\log D}, 1\right] \tag{1.3}$$

with a computable absolute constant c [1].

The other important results concerning real zeros of real L-functions,

---

* The results of this series were presented with detailed proofs in the seminar of the Department of Complex Function Theory of the Mathematical Institute of the Hungarian Academy of Sciences, September–October 1974.

(1) In connection with Davenport's result we must mention a paper of W. Haneke: *Über die reellen Nullstellen der Dirichletschen L-Reihen*, Acta Arith. 23 (1973), pp. pp. 391–421, where he asserts

$$L(s, \chi) \neq 0 \quad \text{for} \quad s \in \left[1-\frac{C}{\sqrt{D}}, 1\right].$$

But the proof is incorrect as just in the last of his 23 lemmata, estimating the sum $\sum_{p \leq D^2} (1+\chi(p))p^{-1}$ he neglects those primes for which $\chi(p) = 0$, i.e. $p|D$. If we correct this fault, Haneke's paper gives only Davenport's result (1.3) (proved in another way).

which are unavoidable in studying the distribution of primes in arithmetic progressions, namely Hecke's, Landau's and Page's theorems were proved until now only by the use of complex analysis.

Hecke's theorem states that if the L-function belonging to the real primitive character $\chi \pmod D$ does not vanish in the interval

$$\left[1-\frac{c}{\log D},\, 1\right] \tag{1.4}$$

then

$$L(1,\chi) > \frac{b(c)}{\log D} \tag{1.5}$$

(the proof is in Landau [6]). (Here c is a constant and $b(c)$ is another constant depending on c.)

Landau's theorem [6] asserts that if

$$L(1-\delta_1,\chi_1) = L(1-\delta_2,\chi_2) = 0 \tag{1.6}$$

for real primitive characters $\chi_1 \not\equiv \chi_2 \pmod{D_1}$ resp. $\pmod{D_2}$, then

$$\max(\delta_1,\delta_2) > \frac{c}{\log D_1 D_2} \tag{1.7}$$

with an absolute constant c.

Page [14] proved the theorem of Landau mentioned above for the case $\chi_1 = \chi_2 \equiv \chi \pmod D$, i.e. when $L(s,\chi_D)$ has at most one simple zero in the interval

$$\left[1-\frac{c}{\log D},\, 1\right]. \tag{1.8}$$

In the direction of the effectivization of Siegel's theorem ((1.1) and (1.2)) besides Davenport's result (1.3) another interesting theorem is due to Tatuzawa [19], who proved that one can determine with at most one exception all the real primitive characters for which (1.1) and (1.2) fail.

The great interest for real L-functions can be attributed to the fact that they play a fundamental role in the theory of quadratic fields as well as in prime number theory.

Thus these theorems of Hecke, Landau, Siegel, Tatuzawa have their analogue for class numbers of imaginary quadratic fields, which one can get from the cited forms of the theorems by using Dirichlet's class number formula and in fact they were originally formulated in this way. (In the case of Landau's theorem we get this analogue if we use Hecke's theorem as well.)

The results of Hecke and Landau were the first steps towards the proof of Gauss's conjecture [3], that the class number $h(-D)$ of the imaginary quadratic field belonging to the fundamental discriminant $-D<0$ tends to $+\infty$ as $D\to\infty$. Gauss's conjecture was proved by Mordell [13] (improving a result of Deuring [2]) under the assumption that the classical Riemann-hypothesis is not true, and a little later by Heilbronn [5] assuming the falsity of the general Riemann-hypothesis. Heilbronn's result showed the truth of Gauss's conjecture, as by the theorem of Hecke the conjecture is obviously true if special real zeros of real L-functions (see (1.4)) do not exist. The values of real L-functions in the point $s=1$ (and in the neighbourhood of $s=1$) are further closely connected with the class numbers and fundamental units of real quadratic fields and with the distribution of quadratic residues and non-residues modulo a prime.

Thus Linnik and A. I. Vinogradov [11] proved, using Siegel's theorem (and also Burgess's inequality), that for the least quadratic prime residue $P(p) \pmod p$ (where p is a prime)

$$P(p) < p^{1/4+\varepsilon} \quad \text{if} \quad p > p_0(\varepsilon) \tag{1.9}$$

with a $p_0(\varepsilon)$ ineffective constant depending only on ε.

D. Wolke [21] proved that if $P(p) > p^{\varepsilon}$, then

$$L(1,\chi_p) = \sum_{n=1}^{\infty}\left(\frac{n}{p}\right)n^{-1} \leqslant \frac{c}{\varepsilon^2 \log p}, \tag{1.10}$$

where c is a computable absolute constant.

These questions are in connection with the old conjecture of I. M. Vinogradov that $P(p) < c(\varepsilon)p^{\varepsilon}$. The upper bounds for $L(1,\chi_p)$ are similarly connected with the least quadratic non-residue $\pmod p$. (See the work of Linnik and Rényi [10].)

The best known upper bounds for $L(1,\chi)$ (χ primitive) are due to P. J. Stephens [18], who proved

$$L(1,\chi_p) \leqslant \frac{1}{2}\left(1-\frac{1}{\sqrt{e}}+o(1)\right)\log p \quad (p \text{ prime}), \tag{1.11}$$

using Burgess's inequality, and, for general D, to Pólya [15]

$$L(1,\chi_D) \leqslant \left(\tfrac{1}{2}+o(1)\right)\log D. \tag{1.12}$$

By Dirichlet's class number formulae these estimates imply upper bounds for class numbers and (in the case of real fields) for fundamental units of quadratic fields.

2. In this series of papers we give elementary proofs for all the results mentioned; in some cases we prove even more. In this paper we prove Hecke's theorem. In papers II and III we investigate $L(s, \chi)$ belonging to the real primitive character $\chi(n) = \left(\frac{-D}{n}\right)$ where $D > 0$, and $h(-D)$ is low (which means in these papers $h(-D) \leqslant (\log D)^{3/4}$). In paper II we determine the distance δ of the real zero $1-\delta$ of $L(s, \chi)$ from the point $s_0 = 1$ up to a factor $1+o(1)$. This makes it possible to improve Davenport's result (1.3) in an effective way to

$$\delta > \frac{12-o(1)}{\pi\sqrt{D}} \tag{2.1}$$

and to show what further results in the $h(-D) = 4$ problem are necessary to improve (2.1).

In paper III we show that if $h(-D)$ is low then, except for the exceptive real zero mentioned above, neither the corresponding $L(s, \chi)$ function nor $\zeta(s)$ has a zero in a great domain T of the complex plane and we determine up to a factor $1+o(1)$ the values of $L(s, \chi)$ in this domain T, i.e. we show for $s \in T$ that

$$L(s, \chi) = (1+o(1))\frac{\zeta(2s)}{\zeta(s)}\prod_{p|D}\left(1+\frac{1}{p^s}\right). \tag{2.2}$$

This also proves Mordell's theorem in the weakened form that if $\zeta(s)$ has a zero in the half-plane $\mathrm{Re}\, s > \frac{3}{4}$, then $h(-D) \to \infty$.

In paper IV we prove a weakened form of Linnik's theorem concerning exceptional zeros [9], i.e. the Heilbronn–Deuring phenomenon, and from this we derive Siegel's theorem in the somewhat effectivized form proved by Tatuzawa (loc. cit.).

In paper V (applying only elements of real analysis) we prove Landau's and Page's theorems ((1.7) resp. (1.8)). In the case of Page's theorem we improve the constant in (1.8).

In paper VI we demonstrate the results of Linnik, A. I. Vinogradov and Wolke, about the least quadratic prime residue (mod p).

In paper VII we prove Stephens's result (1.10) and we generalize it to a primitive character χ (mod D), where D is not a prime, i.e. we improve Pólya's result (1.11). We also demonstrate the consequences of Stephens's and our results concerning the class numbers and units of quadratic fields.

Finally, in paper VIII we prove in a simple unified way (which is mainly elementary and is distinct from the methods of papers I–VII) the basic results concerning real zeros of real L-functions, i.e. the theorems of Hecke, Landau, Page, Siegel and Tatuzawa mentioned above. As the investigation of zeros of complex L-functions, and complex zeros of real L-functions require other methods, our proof makes possible to discuss at least the real zeros of real L-function in a unique and more direct way, and to get a clearer look on these problems. (It allows us e.g. to improve the constant in Landau's theorem from 0.1 (see Miech [12]) to $1+o(1)$.)

3. In our series we use only the following results of number theory:

(a) Dirichlet's class number formulae in papers II and III (but it is unavoidable only in Theorem 3 of paper II) and further to demonstrate the consequences of our results concerning quadratic fields (in papers IV, VII and VIII);

(b) 3 easy lemmas from the theory of quadratic fields (in papers II, III, VII);

(c) The easy elementary effective lower bound

$$|L(1, \chi_D)| \gg \frac{1}{\sqrt{D}\log^2 D}$$

due to Gelfond [4] (in papers II and V);

(d) The Pólya–Vinogradov inequality (in papers II and III and only to get a better constant in V);

(e) Burgess's inequality for character sums, where it plays a fundamental role in the theorem, i.e. in papers VI and VII (and once in paper V to get a better constant). We note that an elementary proof of A. Weil's theorem from which Burgess deduced his inequality is due to W. Schmidt [16];

(f) Simple properties of the zeta function and the easy estimate for it in the critical strip (in paper III), namely for $1 \neq s = 1-\tau+it$, $0 \leqslant \tau \leqslant \frac{1}{2}$

$$|\zeta(s)| \ll |s|^\tau \log(|s|+1)\max\left(1, \frac{1}{|1-s|}\right);$$

(g) 3 easy lemmas from the elementary theory of numbers.

As to analysis, besides some easy lemmas of real elementary analysis, we make use of simple properties of real continuous functions and (in papers III and V) of their derivatives. In paper VIII, which regarding the applied methods is different from the other papers of this series, we use also some complex analysis (namely the notion of the analytic continuation).

The papers will be almost independent, only in paper IV we apply Hecke's theorem (proved in paper I) and Landau's theorem (proved later in paper V of course without recourse to the results of paper IV), further we use Theorem 2 of paper II in paper III, Lemma 1 of paper II in papers III, IV and VI, and Lemma 2 of paper II in paper V.

Finally the author would like to express his gratitude to Prof. P. Turán for many helpful advices.

4. Now we shall prove the theorem of Hecke, i.e. we shall show the following

THEOREM. *If an L-function belonging to the real non-principal character* $\chi \pmod D$ *(where* $D \geq 200$*) has no zero in the interval* $[1-\alpha, 1]$, *where* $0 < \alpha < (20\log D)^{-1}$, *then*

$$L(1, \chi) > 0.23\,\alpha.$$

Proof. We shall use the following

LEMMA OF REAL ELEMENTARY ANALYSIS. *For an arbitrary* τ, *for which* $0<\tau<1$, *there exists a* c_τ, $0<c_\tau<1$, *such that for all* $u \geq 1$

$$\sum_{m\leq u}\frac{1}{m^{1-\tau}} = \frac{1}{\tau}(u^\tau - 1) + c_\tau + \frac{\vartheta}{u^{1-\tau}} \qquad (|\vartheta| \leq 1). \tag{4.1}$$

Let

$$x = \frac{D}{\alpha}100 \left(<\frac{D^2}{\alpha}\right), \qquad g(n) = \sum_{d|n}\chi(d). \tag{4.2}$$

Then

$$g(n) = \prod_{p^\beta \| n}\big(1+\chi(p)+\ldots+\chi^\beta(p)\big) \geq 0, \qquad g(m^2) \geq 1. \tag{4.3}$$

Thus we have

$$1.5 \leq \sum_{m^2\leq x}\frac{1}{m^2} \leq \sum_{n\leq x}\frac{g(n)}{n} < \sum_{n\leq x}\frac{g(n)}{n^{1-\alpha}} \tag{4.4}$$
$$= \sum_{d\leq x}\frac{\chi(d)}{d^{1-\alpha}}\sum_{m\leq x/d}\frac{1}{m^{1-\alpha}} = \sum_{d\leq x}\frac{\chi(d)}{d^{1-\alpha}}\left\{\frac{1}{\alpha}\left(\frac{x^\alpha}{d^\alpha}-1\right)+c_\alpha+\frac{d^{1-\alpha}\vartheta_d}{x^{1-\alpha}}\right\}$$
$$\leq \frac{x^\alpha}{\alpha}\sum_{d\leq x}\frac{\chi(d)}{d} + \left(c_\alpha - \frac{1}{\alpha}\right)\sum_{d\leq x}\frac{\chi(d)}{d^{1-\alpha}} + \sum_{d\leq x}\frac{1}{x^{1-\alpha}}.$$

Use being made of $\left|\sum_{d=a}^{b}\chi(d)\right| < D$, the Abel inequality gives

$$\frac{x^\alpha}{\alpha}\left|\sum_{d>x}\frac{\chi(d)}{d}\right| < \frac{x^\alpha}{\alpha}\cdot\frac{D}{x} = 0.01x^\alpha, \tag{4.5}$$

and further

$$\left(\frac{1}{\alpha}-c_\alpha\right)\left|\sum_{d>x}\frac{\chi(d)}{d^{1-\alpha}}\right| < \frac{1}{\alpha}\cdot\frac{D}{x^{1-\alpha}} = 0.01x^\alpha. \tag{4.6}$$

On the other hand as $L(s,\chi)$ is continuous and $L(1,\chi)>0$

$$L(1-\alpha, \chi) > 0, \tag{4.7}$$

and as $\alpha < 0.01$

$$x^\alpha < (D^2)^{1/20\log D}\left(\frac{1}{\alpha}\right)^\alpha < e^{1/10}(100)^{1/100} < 1.2. \tag{4.8}$$

So we have from the formulae (4.4)–(4.8) (as $1/\alpha - c_\alpha > 0$)

$$1.5 < \frac{x^\alpha}{\alpha}L(1,\chi) + 0.01x^\alpha - \left(\frac{1}{\alpha}-c_\alpha\right)L(1-\alpha,\chi) + 0.01x^\alpha + x^\alpha \tag{4.9}$$
$$< x^\alpha\left(\frac{L(1,\chi)}{\alpha}+1.02\right) < 1.2\left(\frac{L(1,\chi)}{\alpha}+1.02\right).$$

Thus (4.9) proves the theorem.

Added in proof (28. 6. 1976). In the meantime I was informed by Prof. Haneke that with some modification his proof for

$$L(s,\chi) \neq 0 \quad \text{for} \quad s \in \left[1-\frac{C}{\sqrt{D}}, 1\right]$$

could be completed [see the present issue of Acta Arithmetica, pp. 99–100].

References

[1] H. Davenport, *Eine Bemerkung über Dirichlets L-Funktionen*, Göttinger Nachrichten, 1966, pp. 203–212.

[2] M. Deuring, *Imaginär quadratische Zahlkörper mit der Klassenzahl* 1, Math. Zeitschr. 37 (1933), pp. 405–415.

[3] C. F. Gauss, *Disquisitiones Arithmeticae*, *Werke*, vol. 1, Göttingen 1870.

[4] A. O. Gelfond, *On an elementary approach to some problems from the field of distribution of prime numbers* (Russian), Vestnik Moskov. Univ. Ser. Mat.-Fiz. Nauk 8 (1953), pp. 21–26.

[5] H. Heilbronn, *On the class number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. 5 (1934), pp. 150–160.

[6] E. Landau, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Göttinger Nachrichten, 1918, pp. 285–296.

[7] — *Handbuch der Lehre von der Verteilung der Primzahlen*, 1 Bd., Teubner, Leipzig 1909.

[8] Yu. V. Linnik, *Elementary proof of Siegel's theorem based on a method of I. M. Vinogradov* (Russian), Izv. Akad. Nauk SSSR, Ser. Mat., 14 (1950), pp. 327–342.

[9] — *On the least prime in an arithmetic progression II. The Deuring–Heilbronn phenomenon* (Russian), Mat. Sb. 15 (57) (1944), pp. 3–12.

[10] Yu. V. Linnik and A. Rényi, *On some hypothesis in the theory of Dirichlet's characters* (Russian), Izv. Akad. Nauk SSSR, Ser. Mat., 11 (1947), pp. 539–546.

[11] Yu. V. Linnik and A. I. Vinogradov, *Hyperelliptic curves and the least prime quadratic residue* (Russian), Dokl. Akad. Nauk SSSR 168 (2) (1966), pp. 259–261.

[12] R. J. Miech, *A number theoretic constant*, Acta Arith. 15 (1968), pp. 119–137.
[13] L. J. Mordell, *On the Riemann hypothesis and imaginary quadratic fields with a given class number*, J. London Math. Soc. 9 (1934), pp. 289–298.
[14] A. Page, *On the number of primes in an arithmetic progression*, Proc. London Math. Soc. 39 (1935), pp. 116–141.
[15] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Göttinger Nachrichten, 1918, pp. 21–29.
[16] W. M. Schmidt, *Zur Methode von Stepanov*, Acta Arith. 24 (1974), pp. 348–367.
[17] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), pp. 83–86.
[18] P. J. Stephens, *Optimizing the size of* $L(1,\chi)$, Proc. London Math. Soc. (3) 24 (1972), pp. 1–14.
[19] T. Tatuzawa, *On a theorem of Siegel*, Japan J. Math. 21 (1951), pp. 163–178.
[20] A. Walfisz, *Zur additiven Zahlentheorie II*, Math. Zeitschr. 40 (1936), pp. 592–607.
[21] D. Wolke, *A note on the least prime quadratic residue* (mod p), Acta Arith. 16 (1969), pp. 85–87.

Received on 7. 2. 1975 (675)

ACTA ARITHMETICA
XXXI (1976)

On the arithmetic of quaternion algebras*

by

ARNOLD PIZER (Rochester, N. Y.)

Introduction. The purpose of this paper is to study the arithmetic of certain (in general) non-maximal orders in definite quaternion algebras over the rational numbers. They are the orders of level m, m a positive integer (see Definition 1). If $m = 1$, they are the maximal orders of the algebra and if m is square free they are the Eichler or hereditary orders and are studied in [3] and [6]. Our goal is to obtain explicit formulas for the "class number" of ideals associated to an order of level m (see Theorem 16) and the "type number" of orders of level m, i.e. the number of isomorphism classes of such orders (see Theorem 26).

1. Foundations. In this section we set our notation and give some basic facts and definitions. The basic reference for the arithmetic of quaternion algebras is [1] in which the reader will find proofs of the facts listed in this section.

$\mathfrak{A}$ will always denote a definite quaternion algebra over Q, the field of rational numbers, i.e. $\mathfrak{A}$ is a central simple algebra of dimension 4 over Q such that $\mathfrak{A}\otimes_Q \boldsymbol{R}$ is Hamilton's Quaternions. Here $\boldsymbol{R}$ denotes the field of real numbers.

For a finite prime p of Q, we let Q_p, v_p, $|\ |_p$ denote respectively the p-adic numbers, the normalized exponential valuation on Q_p, and the normalized valuation ($|a|_p = \left(\frac{1}{p}\right)^{v_p(a)}$) on Q_p. If A is any algebra over Q, $A_p = A\otimes_Q Q_p$ and A^* denotes the invertible elements of A. We also let $Q_\infty = \boldsymbol{R}$, $A_\infty = A\otimes_Q \boldsymbol{R}$, and call the absolute value in Q the infinite prime on Q. If I is any Z module contained in A, we let $I_p = I\otimes_Z Z_p$ where Z (Z_p) denotes the rational (resp. p-adic) integers. Finally, for any subring R of A (or of A_p), $U(R)$ denotes the units of R.

A prime p of Q is said to *ramify* (*split*) in $\mathfrak{A}$ if $\mathfrak{A}_p$ is a division algebra (resp. 2×2 matrices) over Q_p. The set of ramified primes is finite, even in number (if we count the infinite prime) and determines $\mathfrak{A}$ up to isomorphism.

* Written with partial support of NSF GP-42810.