ACTA ARITHMETICA
LII (1989)

Some problems in multidimensional analytic number theory

by

W. DUKE (New Brunswick, N. J.)

Introduction. The purpose of this work is to give some new applications of Hecke zeta functions with Grössencharaktere, hereafter known as Hecke characters, to rational primes with special properties. These properties typically restrict the primes to a set of zero density in the set of all primes.

As an example, consider for $\delta \geqslant 0$ the set of primes

$$\mathscr{P}_\delta = \{p = a_p^2 + b_p^2 \text{ where } |a_p| \leqslant p^{1/2-\delta}\}$$

and its counting function for $x \geqslant 0$

$$\pi_\delta(x) = \#\{p \leqslant x;\ p \in \mathscr{P}_\delta\}.$$

As an approximation to the famous problem of showing that n^2+1 is prime infinitely often Kubilius (see [M2]) obtained the following theorem for some $\delta_0 > 0$.

THEOREM (Kubilius). *For* $0 \leqslant \delta < \delta_0$

$$\pi_\delta(x) \sim \frac{cx^{1-\delta}}{\log x}$$

for $c > 0$ *some absolute constant.*

The largest value of δ_0 which has been obtained is given in [M1] as $\delta_0 = 12/37$, while under an appropriate density hypothesis we would have $\delta_0 = 1/2$, which is almost as good as what would follow under the appropriate GRH (see [K3]).

The applications are to two types of generalizations of this problem to higher dimensional cases. The most obvious is to replace x^2+y^2 by an arbitrary norm form over a number field $\boldsymbol{k}$ of degree n:

$$f(x) = f(x_1, \ldots, x_n) = N\Big(\sum_{i=1}^{n} \alpha_i x_i\Big) N(\mathfrak{a})^{-1}$$

defined with respect to an ideal $\mathfrak{a}$ with integral basis $\{\alpha_i\}$ of a special type.

Let for $\delta \geqslant 0$ and some m such that $1 \leqslant m \leqslant n$ and $\alpha_m > 0$

$$\mathscr{P}_\delta^f = \{p = f(x);\ |x_i| \leqslant p^{1/n-\delta} \text{ for } i \neq m\}$$

and $\pi_\delta^f(x) = \#\{p \leqslant x;\ p \in \mathscr{P}_\delta^f\}$.

We prove in Section 3.2

THEOREM 3.2. *For* $0 \leqslant \delta < (3n)^{-1}$,

$$\pi_\delta^f(x) \approx \frac{x^{1-(n-1)\delta}}{\log x}$$

where $\approx$ *means* $\ll$ *and* $\gg$ *with implied constants depending only on* $\boldsymbol{k}$.

A more interesting generalization is to consider primes p for which $|a_p| \ll p^{1/2-\delta}$ where a_p is the "error term" in the number of solutions mod p of a general diagonal curve

$$X\colon\ ax^\alpha + by^\beta = c,$$

where $\alpha, \beta, a, b, c \in \mathbf{Z}\setminus\{0\}$ [with $\alpha \geqslant \beta \geqslant 2$] and. $p \equiv 1 \pmod m$, where $m = \operatorname{lcm}(\alpha, \beta)$. For g depending only on X let

$$\mathscr{P}_\delta = \mathscr{P}_\delta^X = \{p \equiv 1\,(m);\ p \not| abc \text{ and } |a_p| \leqslant 2gp^{1/2-\delta}\}$$

and $\pi_\delta^X(x)$ be the associated counting function. In Section 3.3 we prove

THOEOREM 3.3. *For* $0 \leqslant \delta < (3\phi(m))^{-1}$, ϕ = *Euler's function*

$$\pi_\delta^X(x) \gg \frac{x^{1-\delta\phi(m)/2}}{\log x}$$

with the constant depending only on X.

In the special case $y^2 = x^l + d$ for $l > 3$ prime and $d \neq 0$ we obtain in Section 4 a sharp upper bound for the counting function $\pi_\delta(x)$ of

$$\{p \equiv 1\,(l);\ p \not| d,\ |a_p| > (l-1)\,p^{1/2}(1 - Ap^{-\delta})\}$$

for $A > 0$ constant and suitable $\delta > 0$. Explicitly, we have

THEOREM 3.4. *For* $0 \leqslant \delta < 1/(3l-3)$

$$\pi_\delta(x) \approx \frac{x^{1-\delta(l-1)/2}}{\log x}$$

where the constants depend only on l *and* d.

The first two sections contain the analytic results concerning Hecke zeta-functions which are needed to prove these theorems.

Acknowledgements. This paper constitutes essentially my Ph. D. dissertation. I am indebted to my advisor Peter Sarnak for his guidance. I also want to thank Prof. P. X. Gallagher for several useful suggestions.

1. The large sieve for Grössencharaktere

1.0. Conventions and statement of results. Let $\boldsymbol{k}/\boldsymbol{Q}$ be a number field of degree $n = r_1 + 2r_2$, $\mathfrak{q}$ an integral ideal with $N(\mathfrak{q}) = q$, and $\chi\lambda^m = \lambda$ an arbitrary Hecke character mod $\mathfrak{q}$. Here $m \in \mathbf{Z}^{n-1}$ and

$$\lambda^m = \lambda_1^{m_1} \dots \lambda_{n-1}^{m_{n-1}}$$

where $\{\lambda_i\}$ forms a basis for the torsion-free Hecke characters mod $\mathfrak{q}$ (see [H2]) and χ is a narrow class character mod $\mathfrak{q}$.

Unless otherwise indicated, implicit constants depend only on $\boldsymbol{k}$ and the expression $x \approx y$ means $|x| \leqslant Ay$ and $x \geqslant By$ for constants $A, B > 0$ which depend only on $\boldsymbol{k}$. A, B, and C denote such constants and their values may differ in different expressions. Ideals in $\boldsymbol{k}$ will be denoted by german letters, $\mathfrak{p}$ being always a prime ideal and $\mathfrak{a}$ integral. As immediate corollaries to the main result of this chapter, which is Theorem 1.3, we state the following mean value theorems for Dirichlet series over $\boldsymbol{k}$ twisted by Hecke characters.

THEOREM 1.1. *Let* $c(\mathfrak{a}) \in \mathbf{C}$ *be arbitrary for* $N(\mathfrak{a}) \leqslant N$ *and write*

$$\|c\|^2 = \sum_{N(\mathfrak{a}) \leqslant N} |c(\mathfrak{a})|^2.$$

Then

$$\text{(i)}\quad \sum_{\chi \bmod \mathfrak{q}} \sum_{|m| \leqslant T} \int_{-T}^{T} \Big|\sum_{N(\mathfrak{a}) \leqslant N} c(\mathfrak{a})\,\chi\lambda^m(\mathfrak{a})\,N(\mathfrak{a})^{it}\Big|^2 dt \ll (N + qT^n)\log^A qT\,\|c\|^2,$$

$$\text{(ii)}\quad \sum_{q \leqslant Q} \sum_{\chi \bmod \mathfrak{q}}^{*} \sum_{|m| \leqslant T} \int_{-T}^{T} \Big|\sum_{N(\mathfrak{a}) \leqslant N} c(\mathfrak{a})\,\chi\lambda^m(\mathfrak{a})\,N(\mathfrak{a})^{it}\Big|^2 dt \ll (N + Q^2T^n)\log^A QT\,\|c\|^2.$$

Here and throughout * *restricts to primitive* χ.

It is unfortunate that the range of $|m|$ and $|t|$ must be the same and it seems reasonable to conjecture that if the range for $|m|$ is $|m| \leqslant M$ then the left-hand side of (i) should be

$$\ll \sum_{N(\mathfrak{a}) \leqslant N} \big(N(\mathfrak{a}) + qM^{n-1}T\big)|c(\mathfrak{a})|^2$$

while that of (ii) should be

$$\ll \sum_{N(\mathfrak{a}) \leqslant N} \big(N(\mathfrak{a}) + Q^2M^{n-1}T\big)|c(\mathfrak{a})|^2$$

so that they reduce to Gallagher's [G2] results when $\boldsymbol{k} = \boldsymbol{Q}$.

1.1. Duality. In this section the interpretation of large sieve inequalities as norm estimates for Dirichlet operators as given by [F-V] will be generalized to number fields.

A generalized Hecke character

$$\omega(\mathfrak{a}) = \chi(\mathfrak{a})\lambda^m(\mathfrak{a})N(\mathfrak{a})^{it} \tag{1.1.1}$$

is a multiplicative function from ideals in k to C of the above form. Set

$$\|\omega\| = q^{1/n}(|t|+1+|m|) \tag{1.1.2}$$

where $q = N(\mathfrak{q})$ and let Ω be a finite set of generalized Hecke characters with cardinality $|\Omega|$. We shall parameterize Ω by the "width"

$$D = D(\Omega) = \max_{\omega_1,\omega_2\in\Omega} \|\bar{\omega}_1\omega_2\|. \tag{1.1.3}$$

A standard ideal counting argument shows

Lemma 1.1.1. *If the t's belonging to each $\omega\in\Omega$ are spaced by some positive absolute constant, then $|\Omega| \ll D^{2n}$.*

Ω is said to be *δ-well spaced* if for each $\omega_1, \omega_2 \in \Omega$, $\omega_1 \neq \omega_2$, where

$$\omega_i = \chi_i\lambda^{m_i}N^{it_i}, \quad i = 1, 2$$

we have either

$$\text{(i)}\quad |t_1-t_2| \geqslant \delta \text{ or} \tag{1.1.4}$$
$$\text{(ii)}\quad \chi_1\bar{\chi}_2\lambda^{m_1-m_2} \text{ is nonprincipal.}$$

For a set $\mathcal{N}$ of integral ideals define the *Dirichlet operator*

$$\mathcal{D} = \mathcal{D}_k(\mathcal{N}, \Omega)\colon L^2(\mathcal{N}) \to L^2(\Omega)$$

by

$$\mathcal{D}(c) = \sum_{\mathfrak{a}\in\mathcal{N}} c(\mathfrak{a})\omega(\mathfrak{a}). \tag{1.1.5}$$

The reason this operator is interesting is that an estimate for its norm $\|\mathcal{D}\|$ gives the *mean value inequality*

$$\sum_{\omega\in\Omega}\Big|\sum_{\mathfrak{a}\in\mathcal{N}} c(\mathfrak{a})\omega(\mathfrak{a})\Big|^2 \leqslant \|\mathcal{D}\|^2\|c\|^2 \tag{1.1.6}$$

for arbitrary c.

It is fundamental that $\|\mathcal{D}^*\| = \|\mathcal{D}\|$, where $\mathcal{D}^*$ is the adjoint of $\mathcal{D}$. In its equivalent dual form (1.1.6) is called a *large sieve inequality*

$$\sum_{\mathfrak{a}\in\mathcal{N}}\Big|\sum_{\omega\in\Omega} c(\omega)\bar{\omega}(\mathfrak{a})\Big|^2 \leqslant \|\mathcal{D}^*\|^2\|c\|^2 \tag{1.1.7}$$

again for arbitrary c.

The fact that $\|\mathcal{D}\| = \|\mathcal{D}^*\|$ allows us to bound $\|\mathcal{D}\|$ in terms of a smoothed product of ω's.

Lemma 1.1.2. *Let $\varphi\colon \mathbf{R}^+ \to \mathbf{R}^+$ satisfy*

(i) *$\varphi(N(\mathfrak{a})) \geqslant 1$ for $\mathfrak{a}\in\mathcal{N}$,*

(ii) *φ is rapidly decreasing.*

Then, letting $\Phi(\omega_1, \omega_2) = \sum_{\mathfrak{a}} \varphi(N(\mathfrak{a}))\bar{\omega}_1\omega_2(\mathfrak{a})$ we have

$$\|\mathcal{D}\|^2 \leqslant \max_{\omega\in\Omega}|\Phi(\omega, \omega)| + |\Omega| \max_{\omega_1\neq\omega_2}|\Phi(\omega_1, \omega_2)|.$$

Proof.

$$\sum_{\mathcal{N}}\Big|\sum_{\Omega} c(\omega)\bar{\omega}(\mathfrak{a})\Big|^2 \leqslant \sum_{\mathfrak{a}}\varphi(N(\mathfrak{a}))\Big|\sum_{\Omega} c(\omega)\bar{\omega}(\mathfrak{a})\Big|^2$$
$$= \sum_{\Omega\times\Omega}\Big(\sum_{\mathfrak{a}}\varphi(N(\mathfrak{a}))\bar{\omega}_1\omega_2(\mathfrak{a})\Big)c(\omega_1)c(\omega_2)$$
$$\leqslant \|c\|^2 \max\Big(\sum_{\omega_1\in\Omega}\Big|\sum_{\omega_2\in\Omega}\sum_{\mathfrak{a}}\varphi(N(\mathfrak{a}))\bar{\omega}_1\omega_2(\mathfrak{a})\Big|\Big)$$

so

$$\|\mathcal{D}^*\|^2 = \|\mathcal{D}\|^2 \leqslant \max_{\omega_1}\sum_{\omega_2}|\Phi(\omega_1, \omega_2)|$$
$$\leqslant \max_{\omega}|\Phi(\omega, \omega)| + |\Omega| \max_{\omega_1\neq\omega_2}|\Phi(\omega_1, \omega_2)|. \quad\blacksquare$$

To apply this lemma we first need to establish a uniform estimate for Hecke zeta functions in a left half-plane.

1.2. A uniform estimate for Hecke zeta functions. In this section we establish a uniform estimate for a Hecke zeta function in the half-plane $\mathrm{Re}\, s \leqslant \delta_0 < 0$. Let

$$\zeta(s, \chi\lambda^m) = \zeta(s, \lambda) = \sum_{\mathfrak{a}}\chi(\mathfrak{a})\lambda^m(\mathfrak{a})N(\mathfrak{a})^{-s}$$

for $\mathrm{Re}\, s > 1$. ζ has an Euler product

$$\zeta(s, \lambda) = \prod_{\mathfrak{p}\nmid\mathfrak{q}}(1-\chi(\mathfrak{p})\lambda^m(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1},$$

by unique factorization of $\mathfrak{a}$ into prime ideals $\mathfrak{p}$, also for $\mathrm{Re}\, s > 1$. If χ is not primitive then it is induced by χ^*, a primitive character mod $\mathfrak{f}$, where $\mathfrak{f}\mid\mathfrak{q}$, and $\chi^*\lambda^m$ is a primitive Hecke character mod $\mathfrak{f}$ (see [H2]). Further,

$$\zeta(s, \chi\lambda^m) = \zeta(s, \chi^*\lambda^m)\prod_{\mathfrak{p}\mid\mathfrak{q}}(1-\chi^*\lambda^m(\mathfrak{p})N(\mathfrak{p})^{-s}) \tag{1.2.1}$$
$$= \zeta(s, \chi^*\lambda^m)\sum_{\substack{\mathfrak{a}\mid\mathfrak{q}\\(\mathfrak{a},\mathfrak{f})=1}}\mu(\mathfrak{a})\chi^*\lambda^m(\mathfrak{a})N(\mathfrak{a})^{-s}$$

and $\zeta(s, \chi^* \lambda^m)$ satisfies the functional equation (write $\lambda^* = \chi^* \lambda^m$)

(1.2.2) $$\zeta(s, \lambda^*) = w(\lambda^*) A^{1-2s} G(1-s, m. \hat{\chi}) \zeta(1-s, \bar{\lambda}^*)$$

where $|w| = 1$, $A^2 = |d| N(\mathfrak{f}) \pi^{-n} 2^{-r_2}$, d the discriminant of k.

Here $\hat{\chi}$ is the sign character induced by χ^* and

(1.2.3) $$G(s, m, \hat{\chi}) = \prod_{q=1}^{r_1} \frac{\Gamma(\frac{1}{2}(s+a_q-ib_q))}{\Gamma(\frac{1}{2}(1-s+a_q+ib_q))} \prod_{q=r_1+1}^{r_1+r_2} \frac{\Gamma(s+\frac{1}{2}|a_q|-ib_q)}{\Gamma(1-s+\frac{1}{2}|a_q|+ib_q)}$$

where $a_1, \ldots, a_{r_1} \in \{0, 1\}$ are determined by $\hat{\chi}$ while $a_{r_1+1}, \ldots, a_{r_1+r_2} \in \mathbf{Z}$, $b_1, \ldots, b_{r_1+r_2} \in \mathbf{R}$, these values depending only on m. We will write

$$\|\lambda\| = \max_{q=1,\ldots,r_1+r_2} |\varepsilon_q| a_q|/2 + ib_q|$$

where

$$\varepsilon_q = \begin{cases} 0, & q = 1, \ldots, r_1, \\ 1, & q = r_1+1, \ldots, r_1+r_2. \end{cases}$$

It is easily seen that $\|\lambda\| \approx |m|$ where $\approx$ means $\ll$ and $\gg$. In other words, the parametrization by m reflects truly the gamma factor parameters up to constants depending only on k.

THEOREM 1.2. *For* $\operatorname{Re} s \leqslant \delta_0 < 0$

$$|\zeta(s, \chi\lambda^m)| \ll_{k,\delta_0} (Aq^{1/n}(1+|s|+|m|))^{n(1/2-\sigma)}.$$

Proof. After reduction to primitive χ^* the proof requires, in view of the functional equation (1.2.2), estimates for three types of Γ function quotients.

LEMMA 1.2.1. *For* $\sigma = \operatorname{Re} s > 0$

$$\left|\frac{\Gamma(\frac{1}{2}s)}{\Gamma(\frac{1}{2}(1-s))}\right| \leqslant 2\left|\frac{s}{2}\right|^{\sigma-1/2} (1+O(1/|s|)).$$

Proof. By the reflection principle we may assume $t \geqslant 0$. Now

$$\frac{\Gamma(\frac{1}{2}s)}{\Gamma(\frac{1}{2}(1-s))} = \pi^{-1/2} 2^{1-s} \cos(\tfrac{1}{2}\pi s) \Gamma(s).$$

By Stirling's formula (with $s = \sigma+it$, $\sigma = r\cos\theta$, and $t = r\sin\theta$):

$$\log \Gamma(s) = (s-\tfrac{1}{2}) \log s - s + \tfrac{1}{2}\log 2\pi + O(1/r)$$

so

$$\log|\Gamma(s)| = (\sigma-\tfrac{1}{2}) \log r - (\theta t+\sigma) + \tfrac{1}{2}\log 2\pi + O(1/r),$$

which implies that

$$|\Gamma(s)| = \sqrt{2\pi}\, r^{\sigma-1/2} e^{-(\theta t+\sigma)} (1+O(1/r))$$

so

$$|\pi^{-1/2} 2^{1-s} \cos(\tfrac{1}{2}\pi s) \Gamma(s)|$$
$$= 2^{1/2-\sigma} |e^{i(\pi/2)(\sigma+it)-(\theta t+\sigma)} + e^{-i(\pi/2)(\sigma+it)-(\theta t+\sigma)}| r^{\sigma-1/2}(1+O(1/r))$$
$$= A|s/2|^{\sigma-1/2}(1+O(1/|s|))$$

and we are done if $A \leqslant 2$.

Now

$$A \leqslant e^{-[(\theta+\pi/2)t+\sigma]} + e^{-[(\theta-\pi/2)t+\sigma]} \leqslant 1 + e^{-[(\theta-\pi/2)t+\sigma]}$$

since $t, \theta, \sigma \geqslant 0$.

Finally,

$$(\theta-\pi/2)t+\sigma = (\theta-\pi/2) r\sin\theta + r\cos\theta \geqslant 0 \quad \text{for } 0 \leqslant \theta \leqslant \pi/2.$$

LEMMA 1.2.2. *For* $\sigma = \operatorname{Re} s \geqslant 0$

$$\left|\frac{\Gamma(\frac{1}{2}(1+s))}{\Gamma(\frac{1}{2}(2-s))}\right| \leqslant 2|s/2|^{\sigma-1/2}(1+O(1/|s|)).$$

Proof. Same as above using

(1.2.4) $$\frac{\Gamma(\frac{1}{2}(1+s))}{\Gamma(\frac{1}{2}(2-s))} = \pi^{-1/2} 2^{1-s} \sin(\tfrac{1}{2}\pi s) \Gamma(s).$$

LEMMA 1.2.3. *For* $\sigma \geqslant 1$, $a \geqslant 0$

$$\left|\frac{\Gamma(s+a)}{\Gamma(1-s+a)}\right| \ll |s+a|^{2\sigma-1}.$$

Proof. First note that by Stirling's formula, for $\varepsilon \in [0, 1]$

$$\left|\frac{\Gamma(\sigma+a+ic)}{\Gamma(\sigma+a+\varepsilon+ic)}\right| \ll e^{\varepsilon-(\theta_1-\theta_2)c} |\sigma+a+ic|^{-\varepsilon}$$

where $\theta_1 = \arg(\sigma+a+ic)$, $\theta_2 = \arg(\sigma+a+\varepsilon+ic)$ so that $(\theta_1-\theta_2)c \geqslant 0$ and hence above is

(1.2.5) $$\ll |\sigma+a+ic|^{-\varepsilon}.$$

Next, the functional equation $\Gamma(s+1) = s\Gamma(s)$ gives

(1.2.6) $$|\Gamma(\sigma+a+\varepsilon+ic)|$$
$$= |\sigma+a+\varepsilon-1+ic| \ldots |\sigma+a+\varepsilon-[2\sigma]+ic|\, |\Gamma(\sigma+a+\varepsilon-[2\sigma]+ic)|.$$

Choose $\varepsilon \in (0, 1]$ such that $[2\sigma]-\varepsilon = 2\sigma-1$ and thus $\sigma+a+\varepsilon-[2\sigma] = 1-\sigma+a$. Also, $|1-\sigma+a| \leqslant |\sigma+a+\varepsilon-1|$ for $\sigma \geqslant 1$ so by (1.2.5) and (1.2.6)

$$\left|\frac{\Gamma(\sigma+a+ic)}{\Gamma(1-\sigma+a-ic)}\right| \ll |\sigma+a+ic|^{-\varepsilon} |\sigma+a+ic|^{[2\sigma]} \left|\frac{\Gamma(1-\sigma+a+ic)}{\Gamma(1-\sigma+a-ic)}\right|$$
$$= |\sigma+a+ic|^{2\sigma-1}.$$

Proof of Theorem 1.2. Returning to (1.2.1) we have for $\sigma \leqslant \delta_0 < 0$:

$$|\zeta(s, \chi\lambda^m)| \leqslant |\zeta(s, \chi^* \lambda^m)| \sum_{\substack{\mathfrak{a}|\mathfrak{q} \\ (\mathfrak{a},\mathfrak{f})=1}} N(\mathfrak{a})^{-\sigma} \ll_k |\zeta(s, \chi^* \lambda^m)| \, N(\mathfrak{q}/\mathfrak{f})^{1/2-\sigma}$$

and by the functional equation (1.2.2)

(1.2.7) $$|\zeta(s, \chi\lambda^m)| \ll_{k\delta_0} |dN(\mathfrak{f}) \, N(\mathfrak{q}/\mathfrak{f}) \, \pi^{-n} 2^{-2r_2}|^{1/2-\sigma} |G(1-s, m, \hat{\chi})|.$$

By Lemmas 1.2.1 and 1.2.2,

$$\prod_{q=1}^{r_1} \left| \frac{\Gamma(\frac{1}{2}(1-s+a_q-ib_q))}{\Gamma(\frac{1}{2}(s+a_q+ib_q))} \right| \ll \prod_{q=1}^{r_1} \left| \frac{1-s-ib_q}{2} \right|^{1/2-\sigma} \leqslant \left(\tfrac{1}{2}(1+|s|+\|\lambda\|)\right)^{r_1(1/2-\sigma)}.$$

By Lemma 1.2.3

$$\prod_{q=r_1+1}^{r_1+r_2} \left| \frac{\Gamma(1-s+\frac{1}{2}|a_q|-ib_q)}{\Gamma(s+\frac{1}{2}|a_q|+ib_q)} \right| \ll \prod_{q=r_1+1}^{r_1+r_2} |1-\sigma+\tfrac{1}{2}|a_q|-it-ib_q|^{1-2\sigma}$$
$$\ll (1+|s|+\|\lambda\|)^{r_2(1-2\sigma)}.$$

Thus,

$$|G(1-s, m, \hat{\chi})| \ll 2^{-r_1(1/2-\sigma)} (1+|s|+\|\lambda\|)^{n(1/2-\sigma)}$$

so by (1.2.7)

$$|\zeta(s, \lambda)| \ll_{k,\delta_0} |dN(\mathfrak{q})(2\pi)^{-n}|^{1/2-\sigma} (1+|s|+\|\lambda\|)^{n(1/2-\sigma)}$$
$$\ll [Aq^{1/n}(1+|s|+\|m\|)]^{n(1/2-\sigma)}. \quad \blacksquare$$

Remark. For $\delta_0 \leqslant \sigma \leqslant 1-\delta_0$, $0 > \delta_0 \geqslant -1/2$ Phragmén–Lindelöf gives (see [R], p. 204)

(1.2.8) $$|\zeta(s, \lambda)| \ll_\delta [Aq^{1/n}(1+|s|+\|\lambda\|)]^{n(1/2-\sigma/2-\delta_0/2)}.$$

1.3. Estimates for $\|\mathscr{D}\|$. Here we will prove the main result of this chapter, Theorem 1.3, using the analytic method of Halász and Montgomery. We now choose the smoothing function φ to be

(1.3.1) $$\varphi_N(x) = 5\,[e^{-(x/2N)^{3L}} - e^{-(x/N)^{3L}}]$$

where $L = \log D$ and 5 is chosen so that (i) in Lemma 1.1.2 is satisfied for $\mathscr{N}$ with norms contained in $[N, 2N]$. This restriction is assumed to hold throughout this section but it is easily removed for the proof of Theorem 1.1 by a standard trick. With this φ_N recall the notation of Lemma 1.1.2:

(1.3.2) $$\Phi(\omega_1, \omega_2) = \sum_{\mathfrak{a}} \varphi_N(N(\mathfrak{a})) \bar{\omega}_1 \, \omega_2(\mathfrak{a})$$
$$= 5 \sum_{\mathfrak{a}} \bar{\lambda}_1 \lambda_2(\mathfrak{a}) \, N(\mathfrak{a})^{i(t_2-t_1)} [e^{-(N(\mathfrak{a})/2N)^{3L}} - e^{-(N(\mathfrak{a})/N)^{3L}}].$$

Lemma 1.3.1. *For φ_N above if we suppose $N \geqslant (AD\log^2 D)^n$ then for $\lambda = \bar{\lambda}_1 \lambda_2$*

$$\Big|\sum_{\mathfrak{a}} \lambda(\mathfrak{a}) \, N(\mathfrak{a})^{it} \varphi_N(N(\mathfrak{a}))\Big| \ll \varepsilon(\lambda) \, Ne^{-|t|/3\log D} + N^{1/2} D^{-2n}$$

where

$$\varepsilon(\lambda) = \begin{cases} 1, & \lambda \text{ principal}, \\ 0, & \text{otherwise}. \end{cases}$$

Proof. By a standard Mellin pair

(1.3.3) $$\text{LHS} = \frac{5}{2\pi} \left| \int_{\mathrm{Re}\, w=2} \zeta(w+it, \lambda) \, \Gamma\left(\frac{w}{3L}+1\right) \left[\frac{(2N)^w - N^w}{w}\right] dw \right|.$$

Note that $\Gamma(w/3L+1)[\cdot]$ above is analytic for $\mathrm{Re}\, w > -3L$ and so the integrand has a simple pole at $w = 1-it$ if and only if λ is principal, with residue in that case

$$\ll Ne^{-|t|/3L}.$$

Hence

$$\text{LHS} \ll \varepsilon(\lambda) \, Ne^{-|t|/3L} + I$$

where

$$I = \frac{5}{2\pi L} \left| \int_{\mathrm{Re}\, w=-2L} \zeta(w+it, \lambda) \, \Gamma\left(\frac{w}{3L}\right) [(2N)^w - N^w] \, dw \right|$$

which, by Theorem 1.2 and Stirling's formula is

$$\ll N^{-2L} L^{-1} \int_{-\infty}^{\infty} (Aq^{1/n}(1+|-2L+i(u+t)|+|m|))^{n(1/2+2L)} e^{-(\pi/2)|u/3L|} |u/3L|^{-7/6} \, du$$

$$\ll N^{-2L} L^{-1} (Aq^{1/n}(1+|t|+|m|))^{n(1/2+2L)}$$
$$\times \int_0^{\infty} |iu+2L|^{n(1/2+2L)} e^{-(\pi/2)(u/3L)} (u/3L)^{-7/6} \, du$$

$$\ll N^{-2L} L^{-1} (Aq^{1/n}(1+|t|+|m|) \, L)^{n(1/2+2L)} \int_0^{\infty} (u/3L)^{n(1/2+2L)-7/6} e^{-u/3L} \, du$$

$$= N^{-2L} (Aq^{1/n}(1+|t|+|m|) \, L)^{n(1/2+2L)} \, \Gamma(\tfrac{1}{2}n+2L-\tfrac{1}{6})$$
$$\ll N^{-2L} (Aq^{1/n}(1+|t|+|m|) \, L^2)^{n(1/2+2L)} e^{-2nL}.$$

By assumption this is

$$\leqslant N^{-2L} N^{1/2+2L} e^{-2nL} = N^{1/2} D^{-2n}. \quad \blacksquare$$

LEMMA 1.3.2. *If Ω is $6n\log^2 D$-well spaced and $N \gg (AD\log^2 D)^n$ then*

$$\|\mathscr{D}\|^2 \ll N.$$

Proof. In the notation of Lemma 1.1.2 $|\Phi(\omega, \omega)| \ll N$ and $|\Phi(\omega_1, \omega_2)| \ll \varepsilon(\lambda) ND^{-2n} + N^{1/2} D^{-2n}$ by Lemma 1.3.1. Lemmas 1.1.1 and 1.1.2 give

$$\|\mathscr{D}\|^2 \ll N + |\Omega|(ND^{-2n} + N^{1/2} D^{-2n}) \ll N + D^{2n}(ND^{-2n} + N^{1/2} D^{-2n}) \ll N. \ \blacksquare$$

We are now ready to prove the main result of this section.

THEOREM 1.3. *If Ω is $6n\log^2 D$-well spaced then*

$$\|\mathscr{D}\|^2 \ll N + D^n \log^{2n+2} D.$$

Proof. By the previous lemma we may assume

$$N < (AD\log^2 D)^n. \tag{1.3.4}$$

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be a finite set of distinct prime ideals ordered by norm. Write

$$R = (AD\log^2 D)^n (2n\log D) N^{-1};$$

by (1.3.4) $R > 2n\log D$. $\mathfrak{p}_i$ may be chosen to satisfy

(i) $R \leqslant N(\mathfrak{p}_1) \leqslant BR$, B sufficiently large,

(ii) $\prod_{i=1}^{s} N(\mathfrak{p}_i) > D^n$, $s \leqslant 2n\log D/\log N(\mathfrak{p}_1)$.

Since for each ω some $\mathfrak{p}_i$ cannot divide ω's modulus $\mathfrak{q}$ as $D^n \geqslant N(\mathfrak{q})$, we have

$$\sum_{\omega} \Big|\sum_{\mathfrak{a}} c(\mathfrak{a})\omega(\mathfrak{a})\Big|^2 \leqslant \sum_{i=1}^{s} \sum_{\Omega} \Big|\sum_{\mathscr{N}} c(\mathfrak{a})\omega(\mathfrak{p}_i\mathfrak{a})\Big|^2 \leqslant \sum_{i=1}^{s} \|\mathscr{D}(\mathfrak{p}_i\mathscr{N}, \Omega)\|^2 \|c\|^2.$$

We may apply Lemma 1.3.2 to each $\mathscr{D}(\mathfrak{p}_i\mathscr{N})$ by (i) to deduce that

$$\|\mathscr{D}\|^2 \ll N \sum_{i=1}^{s} N(\mathfrak{p}_i) \leqslant NsN(\mathfrak{p}_s). \tag{1.3.5}$$

By the Prime Ideal Theorem the number of prime ideals with norms between $N(\mathfrak{p}_1)$ and $CN(\mathfrak{p}_1)$ is $\gg N(\mathfrak{p}_1)/\log N(\mathfrak{p}_1)$ for C sufficiently large.

By (i) $N(\mathfrak{p}_1) \geqslant 2n\log D$ so by (ii) $s \leqslant N(\mathfrak{p}_1)/\log N(\mathfrak{p}_1)$ and

$$N(\mathfrak{p}_s) \leqslant CN(\mathfrak{p}_1). \tag{1.3.6}$$

Hence by (1.3.5), (1.3.6), (i) and (ii)

$$\|\mathscr{D}\|^2 \ll D^n \log^{2n+2} D. \ \blacksquare$$

2. Zero density of Hecke zeta-functions

2.0. Statement of result. In this chapter an average zero density estimate of Ingham's type for Hecke zeta-functions is given. This, when combined with the strong zero-free region of Urbialis [U] for general Hecke zeta-functions, yields nontrivial unconditional results about primes with "nonlinear" constraints, as discussed in the introduction. Montgomery (see [M3]) obtained the q-versions of the following theorem in the case $\boldsymbol{k} = \boldsymbol{Q}$, and our treatment is based on the simplification of Montgomery's method by Bombieri [B]. From now on unless indicated otherwise implied constants depend on q and $\boldsymbol{k}$. Also, we sometimes write $\lambda = \chi\lambda^m$.

THEOREM 2.1. *For A depending only on $\boldsymbol{k}$ and $\chi \bmod \mathfrak{q}$ fixed*

$$\sum_{|m| \leqslant T} N(\sigma, T, \chi\lambda^m) \ll T^{\frac{3n}{2-\sigma}(1-\sigma)} \log^A T$$

where $N(\sigma, T, \chi\lambda^m)$ is the number of zeros of $\zeta(s, \chi\lambda^m)$ in $\mathrm{Re}\, s \geqslant \sigma$, $|\mathrm{Im}\, s| \leqslant T$ for $\sigma \in [0, 1]$.

The constant $3n/(2-\sigma)$ is poor near $\sigma = 1$ and by applying the Halász method directly Montgomery and others have improved this constant in case $\boldsymbol{k} = \boldsymbol{Q}$. Such methods may be extended in general to give better constants in our applications than those stated. The essential ingredients are a good average bound for the fourth power moment of $\zeta(s, \lambda)$ on its critical line and the large sieve. It is remarked that a sharp mean square estimate as given in [S1] gives the density results with the constant replaced by $4/(3-2\sigma)$.

We note that for $\zeta_k(s)$, the Dedekind zeta-function, Heath-Brown [H1] has given the following density estimate.

THEOREM (Heath-Brown). *For any $\varepsilon > 0$ there is a $c = c(\varepsilon, \boldsymbol{k})$ such that*

$$N(\sigma, T, 1) \ll_k T^{(n+\varepsilon)(1-\sigma)} \log^c T$$

for $n \geqslant 3$. For $n = 2$, $(n+\varepsilon)$ must be replaced by $8/3$.

Since the sum over m is over $\gg T^{n-1}$ terms we see that Theorem 2.1 is an improvement on "average" of this result, of the same type as Ingham's result for $\zeta(s)$. It is also possible to keep the estimate uniform in q and to sum over $q \leqslant Q$ so as to generalize Montgomery's results for Dirichlet L-functions. Without summing over the m-aspect this has been done by Hinz [H4].

Another class of density estimates first gotten by Fogels [F1] and Gallagher [G2] (see also [B]) for Dirichlet L-functions have no log factors but large multiples of $(1-\sigma)$. Used in conjunction with the Deuring-Heilbronn phenomenon they may be used to prove Linnik's theorem and other q-effective results. The presence of the log factor also necessitates the use of a strong zero-free region of Vinogradov's type. Since this has been obtained for Hecke zeta functions, Theorem 2.1 gives reasonably small constants in the applications.

2.1. The fourth power moment. In order to apply a mean value inequality to $\zeta^2(s, \lambda)$ we must approximate it by a finite Dirichlet series. This is done conveniently on $\operatorname{Re} s = 1/2$ by a smoothed approximate functional equation in conjunction with Theorem 1.1 to yield the following average estimate.

THEOREM 2.2. *For χ and $\mathfrak{q}$ fixed*

$$\sum_{|m| \leqslant T} \int_{-T}^{T} |\zeta(\tfrac{1}{2}+it, \chi\lambda^m)|^4\, dt \ll T^n \log^A T.$$

The assumption that $|m|$ is in the same range as $|t|$ is essential for the method used. For k imaginary quadratic Sarnak [S3] has shown how to replace the right-hand side when $\mathfrak{q} = (1)$ by the sharp estimate $T^2 \log^4 T$. It is interesting that the same assumption about the range of $|m|$ is crucial for his argument as well, which uses Eisenstein series over k.

Proof. By a standard trick we may reduce the problem to proving

$$\sum_{|m| \leqslant T} \int_{BT}^{2BT} |\zeta|^4 \ll T^n \log^A T$$

for B a large constant.

By the approximate functional equation given in [H5] as Theorem 2 we have for $BT \leqslant t \leqslant 2BT$ and $|m| \leqslant T$

$$\zeta^2(\tfrac{1}{2}+it, \lambda^*) = \sum_{\mathfrak{a}} d(\mathfrak{a})\lambda^*(\mathfrak{a}) N(\mathfrak{a})^{-1/2-it} c(N(\mathfrak{a})/x)$$

$$+O\big(\sum_{\mathfrak{a}} d(\mathfrak{a})\overline{\lambda^*}(\mathfrak{a}) N(\mathfrak{a})^{-1/2+it} c'(N(\mathfrak{a})/y)\big)+O(1)$$

where $\lambda^* = \chi^* \lambda^m$ is primitive mod $\mathfrak{f}$.

Here c and c' have compact support (see [H4]) and

$$xy = \big(|d|\, N(\mathfrak{f})(|t|/2\pi)^n\big)^2.$$

Thus $\zeta^2(1/2+it, \lambda^*)$ may be approximated by two finite Dirichlet series with $\approx T^n$ terms in the given range with bounded error. Using the usual techniques to deal with the dependence on t the result follows by Theorem 1.1(i) and (1.2.1). ∎

2.2. Proof of Theorem 2.1. For x real and large let

$$M_x = M_x(s, m, \chi) = \sum_{N(\mathfrak{a}) \leqslant x} \mu(\mathfrak{a})\chi\lambda^m(\mathfrak{a}) N(\mathfrak{a})^{-s}$$

and set

$$b(\mathfrak{a}) = \sum_{\substack{\mathfrak{b}|\mathfrak{a} \\ N(\mathfrak{b}) \leqslant x}} \mu(\mathfrak{b}). \tag{2.2.1}$$

Here μ is the Möbius function on ideals $\mathfrak{a}$. Then

$$M_x\zeta = 1+ \sum_{N(\mathfrak{a})>x} b(\mathfrak{a})\chi\lambda^m(\mathfrak{a}) N(\mathfrak{a})^{-s}$$

for $\operatorname{Re} s > 1$. Next introduce another large parameter y and smooth to get

$$e^{-1/y}+ \sum_{N(\mathfrak{a})>x} b(\mathfrak{a})\chi\lambda^m(\mathfrak{a}) N(\mathfrak{a})^{-s} e^{-N(\mathfrak{a})/y} \tag{2.2.2}$$

$$= \zeta(s, \lambda) M_x(s, m, \chi)+\frac{1}{2\pi i}\int_{\operatorname{Re} w = 1/2-\sigma} \zeta(s+w, \lambda) M_x(s+w, m, \chi)\, \Gamma(w)\, y^w\, dw$$

where $\sigma \in (1/2, 1]$ and λ is not trivial. If λ is trivial a term must be added but its effect is negligible due to the exponential decay of $\Gamma(2-s)$ as $|\operatorname{Im} s| \to \infty$.

Now suppose $\varrho = \beta+i\gamma$ is a zero of $\zeta(s, \lambda)$ with $\beta \geqslant \sigma$, $|\gamma| \leqslant T$. From (2.2.2)

$$\Big|\sum_{N(\mathfrak{a})>x} b(\mathfrak{a})\chi\lambda^m(\mathfrak{a}) N(\mathfrak{a})^{-\varrho} e^{-N(\mathfrak{a})/y}\Big| + y^{1/2-\sigma}\int_{\gamma-(\log T)^2}^{\gamma+(\log T)^2} |\zeta(\tfrac{1}{2}+it, \lambda)|\,|M_x|\, dt \gg 1. \tag{2.2.3}$$

There are three possibilities for ϱ:

1. $\Big|\sum_{N(\mathfrak{a})>x} b(\mathfrak{a})\chi\lambda^m(\mathfrak{a}) N(\mathfrak{a})^{-\varrho} e^{-N(\mathfrak{a})/y}\Big| \gg 1.$

2. For some t_ϱ such that $|t_\varrho-\gamma| < \log^2 T$
$$|M_x(\tfrac{1}{2}+it_\varrho, \chi, m)| > x^{\sigma-1/2}.$$

3. $\displaystyle\int_{\gamma-\log^2 T}^{\gamma+\log^2 T} |\zeta(\tfrac{1}{2}+it, \lambda)|\, dt \gg (y/x)^{\sigma-1/2}.$

Let N_i, $i = 1, 2, 3$, be the number of zeros ϱ satisfying conditions 1, 2, 3 resp. We choose a subset R_i of zeros from each class for which the associated set of generalized Hecke characters

$$\Omega_i = \{\omega(\mathfrak{a}) = \chi\lambda^m(\mathfrak{a}) N(\mathfrak{a})^{-i\gamma}\colon |m| \leqslant T,\ \varrho \in R_i\}$$

is $\gg \log^2 T$ well spaced and is such that

$$N_i \ll |R_i| \log^3 T, \quad i = 1, 2, 3. \tag{2.2.4}$$

R_1: By Cauchy's inequality,

$$|R_1| \ll \sum_{\Omega_1} \Big|\sum b(\mathfrak{a})\omega(\mathfrak{a}) N(\mathfrak{a})^{-\beta}\Big|^2 \ll \log T \sum_k \sum_{\Omega_1} \Big|\sum_{I_k} b(\mathfrak{a})\omega(\mathfrak{a}) N(\mathfrak{a})^{-\beta}\Big|^2$$

where $\{I_k\}$ cover $[x, y]$ by $\ll \log T$ intervals of the form $[N_k, 2N_k]$. By Theorem 1.3 and partial summation

$$|R_1| \ll \log T \sum_k (|I_k| + T^n \log^A T) \sum_{I_k} |b(\mathfrak{a})|^2 N(\mathfrak{a})^{-2\sigma} \tag{2.2.5}$$

$$\ll \sum_k (|I_k| + T^n \log^A T)\, |I_k|^{1-2\sigma} \log^A T \ll (y^{2-2\sigma} + T^n x^{1-2\sigma}) \log^A T.$$

Choosing $y = x^{3/2}$, $x = T^{n/(2-\sigma)}$ we get

$$|R_1| \ll T^{\frac{3n}{2-\sigma}(1-\sigma)} \log^A T. \tag{2.2.6}$$

R_2: As for R_2, in a similar manner we get

$$|R_2| \ll (x+T^n) \log^A Tx^{1-2\sigma} \ll T^{\frac{3n}{2-\sigma}(1-\sigma)} \log^A T. \tag{2.2.7}$$

R_3: Write $l_\varrho = (\gamma - \log^2 T, \gamma + \log^2 T)$ so

$$|R_3| x^{2\sigma-1} \ll \sum_{\varrho \in R_3} \Big(\int_{l_\varrho} |\zeta(\tfrac{1}{2}+it, \lambda)| \, dt\Big)^4 \ll \log^A T \sum_{R_3} \int_{l_\varrho} |\zeta|^4 \, dt$$

by Hölder's inequality, so

$$|R_3| \ll x^{1-2\sigma} \log^A T \sum_{|m| \leqslant T} \int_{-2T}^{2T} |\zeta(\tfrac{1}{2}+it, \lambda)|^4 \, dt \ll x^{1-2\sigma} T^n \log^A T$$

by Theorem 2.2, and this is

$$\ll T^{\frac{3n}{2-\sigma}} \log^A T. \tag{2.2.8}$$

To complete the proof, we have

$$\sum_{i=1}^{3} N_i \ll \sum R_i \log^3 T \ll T^{\frac{3n}{2-\sigma}(1-\sigma)} \log^A T$$

by (2.2.4), (6), (7), and (8). Finally,

$$\sum_{\chi} \sum_{|m| \leqslant T} N(\sigma, T, \chi\lambda^m) \leqslant \sum_{i=1}^{3} N_i$$

since every zero ϱ satisfies 1, 2, or 3. ∎

3. Applications to primes and character sums

3.0. Previous results. In order to place the applications given in this chapter in perspective, I will give a brief survey of some motivating results given (in some cases only implicitly) previously.

Let $F(x)$ be an integral polynomial of degree n which is square-free. Consider the character sum

$$a_p = -\sum_{x \bmod p} \left(\frac{F(x)}{p}\right)$$

where $(\div)$ is the Legendre symbol and p is an odd prime not dividing any coefficient of F. The Weil estimate is

$$|a_p| \leqslant 2\left[\frac{n-1}{2}\right] p^{1/2}, \quad \text{where } [x] = \text{greatest integer contained in } x.$$

For $n > 2$, little else is known in general concerning the distribution of $|a_p|$ as $p \to \infty$.

If we suppose that $y^2 = F(x)$ is an elliptic curve E with complex multiplication by the integers in $\boldsymbol{k} = \boldsymbol{Q}(\sqrt{d})$ where $d = d_k$ is the discriminant, then much more can be said. By the theory of complex multiplication $\boldsymbol{k}$ must have class number one in this case [G3].

Let Δ = discriminant of E and for any $\delta \geqslant 0$ define the set of primes

$$\mathscr{P}_\delta^E = \left\{p \nmid \Delta;\ \left(\frac{d}{p}\right) = 1 \text{ and } |a_p| \leqslant 2p^{1/2-\delta}\right\}$$

and its counting function

$$\pi_\delta^E(x) = \#\{p \leqslant x;\ p \in \mathscr{P}_\delta^E\}.$$

By combining the results of Deuring [D3] and Kubilius [K3] we can infer that for some $\delta_0 > 0$ the following holds.

THEOREM. *For $0 \leqslant \delta < \delta_0$, as $x \to \infty$*

$$\pi_\delta^E(x) \sim c \frac{x^{1-\delta}}{\log x} \tag{3.0.1}$$

where $0 < c \leqslant 1/2$ depends only on E.

The best value of δ_0 known to this author is $\delta_0 = 12/37$ given in [M1]. If we assume the density hypothesis for $\zeta(s, \chi\lambda^m)$ over $\boldsymbol{k}$ in the form

$$\sum_{|m| \leqslant M} N(\sigma, T, \chi\lambda^m) \ll (M^{n-1} T)^{2(1-\sigma)} \log^A MT$$

then (3.0.1) holds with $\delta_0 = 1/2$, and this is essentially as strong as what can be shown assuming the GRH for these functions. As mentioned in the introduction this was pointed out by Kubilius [K3] in case

$$F(x) = x(x^2+1),$$

where he showed that under the appropriate GRH there are infinitely many $p \equiv 1 \pmod 4$ such that

$$|a_p| \ll \log p. \tag{3.0.2}$$

This is in view of Jacobsthal's evaluation of a_p as the unique solution of

$$4p = a_p^2 + b_p^2, \quad a_p \equiv -1 \pmod 4.$$

That for certain other $F(x)$ the appropriate version of the above theorem holds is implicit in the uniform PNT for certain biquadratic extensions given in [G1]. Examples of such $F(x)$ are

$$F(x) = x^8+1,\ x^{12}+1,\ x(x^{12}+1)$$

as provided in [B-E], and for these such a theorem holds for $\delta_0 = 1/11$.

For $F(x) = x^5+1$ Sarnak [S2] has given the analogue of Kubilius' result (3.0.2) for infinitely many $p \equiv 1 \pmod 5$ under the appropriate GRH. However, his methods do not seem to extend due to an uncertainty principle in the harmonic analysis involved.

The "Problems" referred to in the title are to establish results of the type discussed above in higher dimensional situations unconditionally. In the next section a general form of the theorem above is formulated as Theorem 3.1. Then in Section 2 this is applied to counting primes represented by norm forms with all but one coordinate small. Section 3 contains the main result, which is a (weak) generalization of the above theorem to arbitrary diagonal curves. Finally, in Section 4, more detailed information is given concerning the distribution of p with $|a_p|$ large in case $F(x) = x^l+d$ where $l > 3$ is prime and $d \neq 0$.

3.1. A uniform estimate for certain primes. First we estimate a smoothed von Mangoldt sum which picks out prime ideals in a given narrow ideal class which satisfy a condition in some Grossencharakter variables which is uniform in a certain range. This results in Theorem 3.1, upon which our applications are based.

Suppose $k/\mathbf{Q}$ is a number field of degree n and choose $H = \{\lambda_1, \ldots, \lambda_e\}$, a fixed set of independent Hecke characters mod $\mathfrak{q}$, so $e \leqslant n-1$. If $e = 1$ suppose λ_1 has infinite order.

As usual, unless otherwise specified, all implied constants depend only on $\mathfrak{q}$. Define for a prime ideal $\mathfrak{p} \nmid \mathfrak{q}$

$$\theta_H(\mathfrak{p}) = \theta(\mathfrak{p}) \in \mathbf{R}^e/\mathbf{Z}^e = \mathbf{T}^e$$

by

(3.1.1) $$\lambda_j(\mathfrak{p}) = e^{2\pi i \theta_j(\mathfrak{p})}, \quad j = 1, \ldots, e.$$

Let I be a narrow ideal class mod $\mathfrak{q}$ and write $q = N(\mathfrak{q})$. For $\theta_0 \in \mathbf{T}^e$, $A > 0$ fixed consider the following set of rational primes parametrized by $\delta \geqslant 0$:

(3.1.2) $$\mathscr{P}_\delta = \{p = N(\mathfrak{p}) \text{ for some } \mathfrak{p} \in I \text{ with } \|\theta(\mathfrak{p}) - \theta_0\| \leqslant Ap^{-\delta}\}$$

where $\|\cdot\|$ is Euclidean distance on $\mathbf{T}^e$, and its counting function $\pi_\delta(x) = \pi_\delta^I(x)$.

After Hecke we have $\pi_0(x) \sim cx/\log x$ for some $c > 0$. In this section we will prove

THEOREM 3.1. *For $\mathfrak{q}$ fixed and $0 \leqslant \delta < 1/3n$ we have*

(3.1.3) $$\pi_\delta(x) \approx_q \frac{x^{1-e\delta}}{\log x}$$

where $\approx$ means $\ll$ and $\gg$.

Proof. We will show only that LHS $\gg$ RHS by smoothing under, the other following similarly by smoothing over.

Let $\varphi(t) \geqslant 0$ be an even smooth function supported in $[-\frac{1}{2}\log 2, \frac{1}{2}\log 2]$ and such that $\hat{\varphi} \geqslant 0$ and $\hat{\varphi}(0) = 1$. Set

$$g_x(t) = g(t) = \varphi\left(\log \frac{t}{x\sqrt{2}}\right)$$

so that $\operatorname{supp} g \subset [x, 2x]$. Also, let $f\colon \mathbf{R}^e \to \mathbf{R}$ be smooth and supported in $B(0, 1/2)$ with $\hat{f}(0) = 1$ and as usual write for $\varepsilon > 0$, $\theta \in \mathbf{R}^e$

(3.1.4) $$f_\varepsilon(\theta) = \varepsilon^{-e} f(\theta/\varepsilon),$$

and consider f_ε as defined on $\mathbf{T}^e$ for ε small.

Now define the smoothed von Mangoldt sum for $x \geqslant 0$

(3.1.5) $$\Psi_I(x, \varepsilon) = \sum_{\mathfrak{a} \in I} \Lambda(\mathfrak{a}) g_x(N(\mathfrak{a})) f_\varepsilon(\theta(\mathfrak{a}) - \theta_0)$$

where $\Lambda(\mathfrak{a})$ is the generalized von Mangoldt function defined by

$$\Lambda(\mathfrak{a}) = \begin{cases} \log N(\mathfrak{p}), & \mathfrak{a} = \mathfrak{p}^k, \\ 0, & \text{otherwise}. \end{cases}$$

$\Psi_I(x, \varepsilon)$ may be used in the standard way to underestimate $\pi_\delta(x)$ by taking

(3.1.6) $$\varepsilon \approx x^{-\delta}$$

and summing over $2^{-k}x$ and summing by parts. Specifically we need

(3.1.7) $$\Psi_I(x, \varepsilon) \gg x$$

subject to (3.1.6) since $|f_\varepsilon| \ll \varepsilon^{-e} \ll x^{e\delta}$.

If $G(s) = \int_0^\infty g(t) t^s \frac{dt}{t}$ then G is entire of exponential type and the following estimate holds.

LEMMA 3.1.1. *For any $l \in \mathbf{Z}^+$*

$$|G(\sigma+it)| \ll_l \begin{cases} (2x)^\sigma (1+|s|)^{-l}, & \sigma \geqslant 0, \\ x^\sigma (1+|s|)^{-l}, & \sigma < 0. \end{cases}$$

Proof. $G(s) = (\sqrt{2}x)^s \int_{-\infty}^{\infty} \varphi(t) e^{st}\, dt$ and the result follows by integrating by parts l times using the smoothness and compact support of φ.

Thus, by Mellin inversion, for any $l > 0$

$$g(N(\mathfrak{a})) = \frac{1}{2\pi i} \int_{2-iT}^{2+iT} G(s) N(\mathfrak{a})^{-s}\, ds + O_l(N(\mathfrak{a})^{-2} x^2 T^{-l})$$

so

(3.1.8)
$$\Psi_I(x,\varepsilon)=\sum_{\mathfrak{a}\in I}\Lambda(\mathfrak{a})\frac{1}{2\pi i}\int_{2-iT}^{2+iT}G(s)N(\mathfrak{a})^{-s}ds\cdot f_\varepsilon(\theta(\mathfrak{a})-\theta_0)+O_l(x^2T^{-l}\varepsilon^{-e}).$$

We may expand f_ε in its Fourier series
$$f_\varepsilon(\theta(\mathfrak{a}))=\sum_{m\in\mathbf{Z}^e}\hat{f}(\varepsilon m)\lambda_H^m(\mathfrak{a}),$$
so
$$f_\varepsilon(\theta(\mathfrak{a})-\theta_0)=\sum\hat{f}(\varepsilon m)e^{-2\pi i m\cdot\theta_0}\lambda_H^m(\mathfrak{a}),$$
where $\lambda_H^m=\lambda_1^{m_1}\ldots\lambda_e^{m_e}$. Cutting this series off at $|m|=T$, the above large parameter, we have for any $l\in\mathbf{Z}^+$

(3.1.9)
$$f_\varepsilon(\theta(\mathfrak{a})-\theta_0)=\sum_{|m|\leqslant T}\hat{f}(\varepsilon m)e^{-2\pi i\theta_0\cdot m}\lambda_H^m(\mathfrak{a})+O_l((\varepsilon T)^{e-l}\varepsilon^{-e})$$

by the rapid decay of $\hat{f}$. This shows we should take

(3.1.10)
$$\varepsilon T=T^{\varepsilon_0}$$

for some $\varepsilon_0>0$. If this holds then also $T=x^\alpha$ for some $\alpha>0$ so by (3.1.8) and (3.1.9)
$$\Psi_I(X,\varepsilon)=\beta\sum_\chi\bar{\chi}(I)\sum_{\mathfrak{a}}\chi\lambda_H^m(\mathfrak{a})\Lambda(\mathfrak{a})\frac{1}{2\pi i}\int_{2-iT}^{2+iT}G(s)N(\mathfrak{a})^{-s}ds$$
$$\times\sum_{|m|\leqslant T}\hat{f}(\varepsilon m)e^{-2\pi i\theta_0\cdot m}+o(1),$$
where χ runs over all narrow class characters mod $\mathfrak{q}$ and $\beta^{-1}=2^r h\phi(\mathfrak{q})$, h = class number of $\mathbf{k}$, and $r\leqslant r_1$.

Thus subject to (3.1.10)

(3.1.11)
$$\Psi_I(x,\varepsilon)=\beta\sum_\chi\bar{\chi}(I)\sum_{|m|\leqslant T}\hat{f}(\varepsilon m)e^{-2\pi i m\cdot\theta_0}\frac{1}{2\pi i}\int_{2-iT}^{2+iT}G(s)\frac{\zeta'(s,\chi\lambda_H^m)}{\zeta(s,\chi\lambda_H^m)}ds+o(1).$$

LEMMA 3.1.2. *Notation as above and assuming* (3.1.10)
$$\Psi_I(x,\varepsilon)=\frac{c_1}{\phi(\mathfrak{q})}x+O\Big(\sum_\chi\sum_{|m|\leqslant T}\sum_{|\mathrm{Im}\,\varrho|\leqslant T}x^{\mathrm{Re}\,\varrho}\Big)+O(qT^e)$$
where $c_1>0$ is absolute and ϱ runs over nontrivial zeros of $\zeta(s,\chi\lambda_H^m)$. For this lemma implied constants depend only on $\mathbf{k}$.

Proof. The proof proceeds along classical lines. First replace the vertical contours in (3.1.11) by horizontal ones which go from $2\pm iT$ to $-\infty\pm iT$ and thus pick up contributions from the zeros (and pole at $s=1$ if $\chi\lambda_H^m$ is trivial) of $\zeta(s,\chi\lambda_H^m)$. Of course the T must be chosen so as to avoid as much as possible any ordinate of a zero for $|m|\leqslant T$. As in the classical case when $n=1$ we base the estimates for zeros of $\zeta(s,\chi\lambda_H^m)$ and for $|\zeta'/\zeta|$ needed in this proof on the following lemma. Here λ^m runs over all torsion-free Hecke characters mod $\mathfrak{q}$.

LEMMA 3.1.3. *Let ϱ run over nontrivial* ($\mathrm{Re}\,\varrho>0$) *zeros of $\zeta(s,\chi\lambda^m)$. Then for $t\in\mathbf{R}$*
$$\sum_\varrho\frac{1}{1+(t-\mathrm{Im}\,\varrho)^2}\ll_k\log q(|t|+|m|+2).$$

Proof. This is proved as in [D1], p. 103 for the case of Dirichlet L-functions after first reducing to primitive χ^*, since $\zeta(s,\chi\lambda^m)$ and $\zeta(s,\chi^*\lambda^m)$ have the same nontrivial zeros by (1.2.1). The difference is that Stirling's formula must be applied to the more general factor. ∎

As a consequence, there are $\ll_k qT^e\log qT$ zeros ϱ for $|m|\ll T$ such that
$$|\mathrm{Im}\,\varrho-T|<1$$
so there is a gap of length $\gg q^{-1}T^{-e}\log^{-1}qT$, provided T is large.

Also, for $-1\leqslant\sigma\leqslant 2$ and $|m|\ll T$

(3.1.12)
$$\frac{\zeta'(\sigma+iT,\chi\lambda^m)}{\zeta(\sigma+iT,\chi\lambda^m)}=\sum_{|\mathrm{Im}\,\varrho-T|<1}(\sigma+iT-\varrho)^{-1}+O(\log qT)$$

if T avoids any zero ordinate. By varying T by a bounded amount we can be assured that on the contours from $2\pm iT$ to $-1\pm iT$ (we must avoid trivial zeros as well)
$$\sum_\chi\sum_{|m|\leqslant T}\left|\frac{\zeta'(s,\chi\lambda^m)}{\zeta(s,\chi\lambda^m)}\right|\ll q^2T^{2e}\log^2 qT.$$

By the rapid decay of $G(\sigma+iT)$ in T we see that

(3.1.13)
$$\sum_\chi\sum_{|m|\leqslant T}\hat{f}(\varepsilon m)\int_{-1\pm iT}^{2\pm iT}|G(s)\zeta'(s,\lambda)/\zeta(s,\lambda)|\,ds=o(1),$$

writing $\lambda=\chi\lambda^m$. Also, since $(s-1)\zeta(s,\chi\lambda^m)$ is entire of order 1, by Lemma 3.1.1 the same holds for the contours from $-\infty\pm iT$ to $-1\pm iT$.

Clearly the first term in Lemma 3.1.2 comes from the pole of $\dfrac{\zeta'(s,1)}{\zeta(s,1)}$ at $s=1$.

Since $\operatorname*{res}_{s=1}\dfrac{\zeta'(s,1)}{\zeta(s,1)}=1$, $\hat{f}(0)=1$, and $G(1)=\sqrt{2}x\int_{-\infty}^{\infty}\varphi(t)e^t\,dt$, we see that $c_1>0$ is absolute.

The second term bounds the contribution of the nontrivial zeros since

$$|G(\varrho)| = |(\sqrt{2}x)^{\varrho} \int_{-\infty}^{\infty} \varphi(t) e^{\varrho t} dt| \ll x^{\mathrm{Re}\,\varrho}.$$

To complete the proof it is enough by (3.1.10) to show that the trivial zeros contribute $O(q \log q \cdot \varepsilon^{-e})$. These occur at the poles of the gamma factor and include zeros contributed by nonprimitive χ on $\mathrm{Re}\, s = 0$. The first kind are at negative integral or even integral translates of a fixed set of complex numbers with nonpositive real parts, for each $\chi\lambda_H^m$. By Lemma 3.1.1 and (1.2.1)

$$\sum_{\chi} \sum_{|m| \leqslant T} |\hat{f}(\varepsilon m)| \sum_{\substack{\tilde{\varrho}\,\mathrm{trivial} \\ |\mathrm{Im}\,\tilde{\varrho}| \leqslant T}} |G(\tilde{\varrho})| \ll \log q \sum_{\chi} \sum_{|m| \leqslant T} |\hat{f}(\varepsilon m)| \ll q \log q \cdot \varepsilon^{-e}.$$

Finally, we note that the effect of varying T by a bounded amount is to change the sum in the second term of the lemma over ϱ by $O(qT^{\varepsilon} \log qT)$ terms and each term is $O(T^{-l}x)$ for all $l > 0$ by Lemma 3.1.1 so the restriction on T may be removed. This completes the proof of Lemma 3.1.2. ∎

To complete the proof of Theorem 3.1 we need to apply the zero density estimate Theorem 2.1 as well as the following strong zero-free region for $\zeta(s, \chi\lambda^m)$ which follows in a standard way from Lemma 5 in [U].

THEOREM (Urbialis). *$\zeta(s, \chi\lambda^m)$ has no zeros for $|\mathrm{Im}\, s| \leqslant T$ and*

$$\mathrm{Re}\, s \geqslant 1 - c_3 \log^{-c_2} T \tag{3.1.14}$$

if $|m| \leqslant T$, $T \geqslant 2$, and $c_2 > 5/7$. Here $c_3 > 0$ depends only on **k**, *q, and c_2.*

LEMMA 3.1.4. *Suppose*

$$\sum_{|m| \leqslant T} N(\sigma, T, \chi\lambda^m) \ll T^{nb(1-\sigma)} \log^A T.$$

If $T = x^{\delta}$ and $0 < \delta < (bn)^{-1}$ then

$$\sum_{|m| \leqslant T} \sum_{|\mathrm{Im}\,\varrho| \leqslant T} x^{\varrho} = o(x),$$

where ϱ runs over nontrivial zeros of $\zeta(s, \chi\lambda^m)$.

Proof.

$$\sum x^{\varrho} \ll -\int_0^1 x^{\sigma} d\sigma \big(\sum N(\sigma, T, \chi\lambda^m)\big)$$

$$= \sum_{|m| \leqslant T} N(0, T, \chi\lambda^m) + \int_0^1 \log x \cdot x^{\sigma} \sum N \, d\sigma$$

$$\ll T^n \log T + x \log x \int_0^{1-\eta(T)} [T^{nb} x^{-1}]^{1-\sigma} d\sigma$$

where $\eta(T) = c_3 \log^{-c_2} T$ by (3.1.14). The result now follows easily using the condition $\delta < (bn)^{-1}$. ∎

Combining Lemmas 3.1.2 and 3.1.4 and Theorem 1.2, to give $b = 3$ we see that (3.1.7) follows, and this completes the proof of Theorem 3.1.

3.2. Primes represented by norm forms. A general application of Theorem 3.1 is to use it to study primes represented by norms forms for ideals which have all but one coordinate relatively small.

Notation as before, consider for an ideal $\mathfrak{a}$ the integral form in $x = (x_1, \ldots, x_n)$:

$$f(x) = N(\mathfrak{a})^{-1} N\big(\sum_{i=1}^{n} \alpha_i x_i\big)$$

where $\{\alpha_i\}$ is an integral basis which satisfies the additional properties

(i) $$\begin{vmatrix} \alpha_1^{(1)} \ldots \alpha_n^{(1)} \\ \alpha_1^{(n)} \ldots \alpha_n^{(n)} \end{vmatrix} = \sqrt{d_k}\, N(\mathfrak{a}), \text{ with } \sqrt{-1} = +i,$$

where d_k = discriminant of **k**, and

(ii) For some m such that $1 \leqslant m \leqslant n$, $\alpha_m \succ 0$, i.e. α_m is totally positive.

Say two such forms are *narrowly equivalent* if their associated ideals are in the same narrow ideal class I, and denote by f_I the class of all such forms.

In case $\mathbf{k} = \mathbf{Q}(\sqrt{d_k})$ it is classical (see e.g. [H3] and [D1]) that f_I is a class of properly equivalent primitive binary quadratic forms over $\mathbf{Z}$ with discriminant $d_k = b^2 - 4ac$ if

$$f(x, y) = ax^2 + bxy + cy^2, \quad (a, b, c) = 1.$$

Furthermore, every such class of forms (which are positive if $d < 0$) is given by exactly one f_I.

For m fixed let

$$\mathscr{P}_{\delta}^{f} = \{p = f(x),\ x = (x_1, \ldots, x_n) \in \mathbf{Z}^n \text{ such that } |x_i| \leqslant p^{1/n-\delta} \text{ for } i \neq m\},$$

for any $\delta \geqslant 0$.

If $\delta > 1/n$ then of course $\mathscr{P}_{\delta}^{f} = \emptyset$ while if $\delta = 1/n$ then $\mathscr{P}_{\delta}^{f}$ consists of primes represented by finitely many polynomials of degree n. Determining whether or not in this case $\mathscr{P}_{\delta}^{f}$ has infinitely many elements is a difficult and unsolved problem since it includes, in case $\mathbf{k} = \mathbf{Q}(\sqrt{-1})$, the existence question of infinitely many primes p of the form n^2+1.

If $\delta = 0$ it follows from the work of Hecke [H2] that $\mathscr{P}_0^{f}$ has positive density in the set of all primes. That is, for $x \geqslant 0$ let $\pi_{\delta}^{f}(x)$

$= \# \{p \leqslant x;\ p \in \mathscr{P}_\delta^f\}$. Then

$$\pi_0^f(x) \sim c\frac{x}{\log x} \quad \text{for some } 0 < c \leqslant 1.$$

As a more positive attack on the above problem we can now derive from Theorem 3.1

THEOREM 3.2. *For* $0 \leqslant \delta < (3n)^{-1}$

$$\pi_\delta^f(x) \approx \frac{x^{1-(n-1)\delta}}{\log x}$$

where the implied constants depend only on $\boldsymbol{k}$.

Proof. In order to apply Theorem 3.1 observe that

$$p = N\left(\sum x_i \alpha_i\right) N(\mathfrak{a})^{-1} \quad \text{with } \sum x_i \alpha_i \succ 0$$

iff $p = N(\mathfrak{p})$ with some $\mathfrak{p} \in I^{-1}$.

This follows by the correspondence

$$\mathfrak{a}\mathfrak{p} = \left(\sum x_i \alpha_i\right) = (\alpha) \quad \text{with } \alpha \in \mathfrak{a} \text{ and } \alpha \succ 0.$$

Consider now the geometric imbedding into $\boldsymbol{R}^{r_1} \times \boldsymbol{C}^{r_2}$ of θ_k given as usual by

$$\alpha \xrightarrow{\sigma} (\alpha^{(1)}, \ldots, \alpha^{(r_1)}, \alpha^{(r_1+1)}, \ldots, \alpha^{(r_1+r_2)}).$$

The condition $|x_i| \leqslant p^{1/n-\delta}$ for $i \neq m$ is equivalent to the conditions

$$\|\theta(\mathfrak{p}) - \theta_0\| \ll p^{-\delta} \quad \text{and} \quad \sum x_i \alpha_i \succ 0.$$

Here θ is with respect to all torsion-free Hecke characters mod 1 and $\theta_0 = \theta((\alpha_m)) - \theta(\mathfrak{a})$. This follows by the geometric interpretation of θ on principal ideals using that $\alpha_m \succ 0$. Thus by Theorem 3.1 the result follows. ∎

3.3. Application to diagonal curves. Our main application is to the arithmetic of diagonal curves

(3.3.1) $$\boldsymbol{X}\colon\ ax^\alpha + by^\beta \equiv c \pmod p$$

where $\alpha, \beta, a, b, c \in \boldsymbol{Z}\setminus\{0\}$, $2 \leqslant \beta \leqslant \alpha$, $m = \mathrm{lcm}(\alpha, \beta)$, $d = \gcd(\alpha, \beta)$, and $p \equiv 1 \pmod m$. Specifically, the number of (affine) solutions N_p of (3.3.1) may be expressed [D-H]

(3.3.2) $$N_p = p + \mathscr{N}_p - a_p$$

where

$$\mathscr{N}_p = \begin{cases} 1-d, & -a/b \text{ is a } d\text{th power mod } p, \\ 1, & \text{otherwise} \end{cases}$$

is bounded. Define the set of rational primes for $\delta \geqslant 0$

$$\mathscr{P}_\delta^{\boldsymbol{X}} = \{p \equiv 1\,(m);\ p \nmid abc \text{ and } |a_p| \leqslant 2gp^{1/2-\delta}\}$$

where $g = (1/2)[(\alpha-1)(\beta-1)-(d-1)]$ is the genus of $\boldsymbol{X}$ over $\boldsymbol{C}$, and let for $x \geqslant 0$

$$\pi_\delta^{\boldsymbol{X}}(x) = \#\{p \leqslant x;\ p \in \mathscr{P}_\delta^{\boldsymbol{X}}\}.$$

The main result implies that for $\delta < (3\phi(m))^{-1}$, $\mathscr{P}_\delta^{\boldsymbol{X}}$ contains infinitely many primes. Here ϕ is Euler's function.

THEOREM 3.3. *For* $0 \leqslant \delta < (3\phi(m))^{-1}$

$$\pi_\delta^{\boldsymbol{X}}(x) \gg \frac{x^{1-\delta\phi(m)/2}}{\log x}$$

with implied constant depending only on $\boldsymbol{X}$.

Proof. In order to apply Theorem 3.1 we must express a_p in terms of an independent set of Hecke characters. This was accomplished by Weil by expressing a_p in terms of Jacobi sums and then recognizing these as Hecke characters in a cyclotomic field (see [D-H] and [W]). We will only summarize this development here, filling in details in the next section in a special case.

Let $\boldsymbol{k} = \boldsymbol{Q}(e^{2\pi i/m})$ and $\mathfrak{p}$ be a prime in $\boldsymbol{k}$ with $\mathfrak{p} \nmid (abcm)$. Let $(x/\mathfrak{p})_k$ be the kth power residue symbol and define the "generalized" Jacobi sum

(3.3.3) $$J_{abc}\begin{pmatrix}\mu \\ \nu\end{pmatrix}; \mathfrak{p}) = -\sum_{ax+by\equiv c(\mathfrak{p})} \left(\frac{x}{\mathfrak{p}}\right)_\alpha^\mu \left(\frac{y}{\mathfrak{p}}\right)_\beta^\nu.$$

This is denoted $\pi_{abc}(\chi^\mu, \psi^\nu)$ in [D-H] where it is shown that

(3.3.4) $$a_p = -\sum_{\substack{\mu \not\equiv 0(\alpha) \\ \nu \not\equiv 0(\beta) \\ (\mu\beta+\nu\alpha)d^{-1} \not\equiv 0(m)}} J_{abc}\left(\begin{matrix}\mu \\ \nu\end{matrix}; \mathfrak{p}\right)$$

for any $\mathfrak{p}$ over $p \equiv 1\,(m)$. It follows from Weil [W] that

(3.3.5) $$-a_p = 2p^{1/2}\sum_{i=1}^{g} \cos\Big(2\pi \sum_{j=1}^{\phi(m)/2} m_{ij}\theta_i(\mathfrak{p})\Big)$$

where $m_{ij} \in \boldsymbol{Z}$ and θ_i comes from a set of independent Hecke characters mod $\mathfrak{q}$ for some $\mathfrak{q}$ depending on $\boldsymbol{X}$ with $(m^2)|\mathfrak{q}$.

Next, the range of the function defined on $\boldsymbol{T}^{\phi(m)/2}$ by

$$g(\theta) = \sum \cos\Big(2\pi \sum m_{ij}\theta_i\Big)$$

is easily seen to be $[-g, g]$ so the hypersurface defined by $g(\theta_0) = 0$ is not empty. Applying Theorem 3.1 with any such θ_0 we get Theorem 3.3. ∎

Remark. Of course, any value of $\alpha \in [-2g, 2g]$ could have been chosen to get Theorem 3.3 for

$$\pi_\delta^\alpha(x) = \#\{p \leqslant x;\ p \equiv 1\,(m),\ p \nmid abc, \text{ and } |a_p p^{-1/2} - \alpha| \leqslant 2gp^{-\delta}\}. \tag{3.3.6}$$

In the next section we will obtain a sharp upper bound for (essentially) $\pi_\delta^{2g}(x)$ in case X is given by (for $l > 3$ prime)

$$y^2 = x^l + d.$$

3.4. Large values of certain Jacobsthal sums. Returning to the example and notation of Section 3.0 suppose $F(x) = x^l + d$ for $l > 3$ prime and $d \neq 0$. Then for $p \nmid d$, $p > 2$

$$a_p = -\sum_{x \bmod p} \left(\frac{x^l + d}{p}\right) \tag{3.4.1}$$

$(-)$ being the Legendre symbol. As before

$$|a_p| \leqslant (l-1)\,p^{1/2}.$$

Consider the set of primes

$$\mathscr{P}_\delta = \{p \equiv 1\ (l);\ p \nmid d \text{ and } |a_p| > (l-1)\,p^{1/2}(1 - Ap^{-\delta})\}$$

for $A > 0$ constant, and its counting function $\pi_\delta(x)$. It follows from a more general result of Korobov [K1] that

$$\pi_1(x) \ll_l 1 \tag{3.4.2}$$

for $A > (l-3)(l-4)/8$, so that a slightly stronger result than the RH holds for all but finitely many p. The question arises as to whether or not this holds for some $\delta < 1$. It follows from the remark following Theorem 3.3 that for $0 < \delta < 1/(3l-3)$ it does not. In this section we show that such exceptional primes p where

$$|a_p| > (l-1)\,p^{1/2}(1 - Ap^{-\delta})$$

form a set of zero density in the set of all primes. More precisely,

THEOREM 3.4. *For* $0 \leqslant \delta < 1/(3l-3)$

$$\pi_\delta(x) \asymp x^{1 - \frac{l-1}{2}\delta}/\log x$$

where the implied constants depend only on l *and* d.

Proof. In view of the following lemma we see that this follows from Theorem 3.1 with $\theta_0 = 0$.

LEMMA 3.4.1. *For any* $\mathfrak{p} \nmid (d)$ *in* $\boldsymbol{Q}(e^{2\pi i/l})$ *over* $p \equiv 1 \pmod l$

$$a_p = -2p^{1/2} \sum_{i=1}^{(l-1)/2} \cos(2\pi\theta_i(\mathfrak{p})),$$

where $\lambda_i = e^{2\pi i \theta_i}$ *is an independent set of Hecke characters* $\bmod (4l^2 d)$.

Proof. Let $\boldsymbol{k} = \boldsymbol{Q}(e^{2\pi i/l})$; for $\mathfrak{p}$ over $p \equiv 1 \pmod l$, $p \nmid d$,

$$\begin{aligned} a_p &= -2p^{1/2} \sum_{i=1}^{(l-1)/2} \cos(2\pi\theta_i(\mathfrak{p})) \\ &= \sum_{x \in (\boldsymbol{O}_k/\mathfrak{p})^*} \left(\frac{x^l + d}{\mathfrak{p}}\right) = \sum \left(\frac{x^l + d}{\mathfrak{p}}\right)_l^{2l} = \sum \left(\frac{x^l + d}{\mathfrak{p}}\right)_{2l}^{l} \sum_{i=1}^{l-1} \left(\frac{x}{\mathfrak{p}}\right)_l^i \\ &= -\sum_i \left(\frac{d}{\mathfrak{p}}\right)\left(\frac{-d}{\mathfrak{p}}\right)_l^i J_{111}\left({1 \atop i}; \mathfrak{p}\right) \end{aligned} \tag{3.4.3}$$

in the notation of (3.3.3) with $\alpha = 2$, $\beta = 1$. Hence by [W] we must show that for $\alpha \in \boldsymbol{O}_k$, the integers in $\boldsymbol{k}$, such that $\alpha \equiv 1\,(4l^2 d)$

$$\left(\frac{d}{\alpha}\right)\left(\frac{-d}{\alpha}\right)_l = \left(\frac{\alpha}{d}\right)\left(\frac{\alpha}{d}\right)_l = 1.$$

This follows by quadratic and Eisenstein reciprocity together with the supplementary laws if $(d, 2l) \neq 1$ ([H3], p. 221, 224, and [I-R], p. 207.), since α is primary in either case.

The independence of $\{\lambda_i\}$ is proved in [D2].

References

[B] E. Bombieri, *Le Grand Crible dans la Théorie Analytique des Nombres*, Astérisque 18 (1973).

[B-E] B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory 11 (1979), 349–398.

[D1] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer, 1980.

[D2] G. P. Davidoff, *Statistical Properties of Certain Exponential Sums*, Thesis, NYU, 1984.

[D3] M. Deuring, *Die Typen der Multiplikatorenringe Elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg, 14 (1941), 197–272.

[D-H] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen*, Journ. für Math. 172 (1934), 2–182.

[F-V] M. Forti and C. Viola, *On Large Sieve Type Estimates for the Dirichlet Series Operator*, Proc. Symp. Pure Math. 24 (1973), 31–49.

[F1] E. Fogels, *On the zeros of L-functions*, Acta Arith. 11 (1965), 67–96.

[F2] –, *On the abstract theory of primes III*, ibid. 11 (1966), 293–331.

[G1] E. Gaigalas, *Distribution of prime numbers in two imaginary quadratic fields, I, II*, Liet. Math. Sb. 19 (1979), 45–60.

[G2] P. X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Inventiones Math. 11 (1970), 329–339.
[G3] B. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, Lecture Notes in Math., #779 (1980).
[H1] R. Heath-Brown, *On the density of the zeros of the Dedekind Zeta-function*, Acta Arith. 33 (1977), 169–181.
[H2] E. Hecke, *Eine Neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen*, Math. Z. 6 (1920), 11–51.
[H3] –, *Lectures on the Theory of Algebraic Numbers*, Springer, 1981.
[H4] J. Hinz, *Über Nullstellen der Heckeschen Zetafunktionen in algebraischen Zahlkörpern*, Acta Arith. 31 (1976), 167–193.
[H5] M. N. Huxley, *The Large Sieve Inequality for Algebraic Number Fields, II, Means of moments of Hecke zeta-functions*, Proc. London Math. Soc. (3) 21 (1970), 108–128.
[I-R] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, 1982.
[K1] N. M. Korobov, *An Estimate of the Sum of the Legendre Symbols*, Dokl. Akad. Nauk. SSSR 196 (1971), 764–767.
[K2] F. B. Kovalcik, *Density Theorems and the Distribution of Primes in Sectors and Progressions*, Sov. Math. Dokl. 15 (1974), 1521–1525.
[K3] I. Kubilius, *On a Problem of the Multidimensional Analytic Theory of Numbers*, Uch. Zap. Vil'nyussk. Univ. Ser. Mat. Fiz.-Khim. Nauk. 4 (1955), 5–43.
[M1] M. Maknys, *Refinement of the remainder term in the law of the distribution of prime numbers of an imaginary quadratic field in sectors*, Liet. Mat. Sb. 17 (1977), 133–137.
[M2] –, *Metric and Analytic Number Theory at Vilnius University*, ibid 20. (1980), 29–38.
[M3] H. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. #227, Springer, 1971.
[R] H. Rademacher, *On the Phragmen–Lindelöf Theorem and Some Applications*, Collected Works, 1958, pp. 496–508.
[S1] P. Sarnak, *Notes on an Approximate Functional Equation, ...*, Preprint.
[S2] –, *On the Number of Points on Certain Curves and an Uncertainty Principle*, Number Theory, New York 1983–84, Lecture Notes in Math. #1135 (1985), pp. 239–253.
[S3] –, *Fourth Moments of Grössencharakter Zeta Functions*, Comm. Pure and Applied Math. 39 (1985), 167–178.
[U] J. Urbialis, *Distribution of Algebraic Primes*, Liet. Mat. Sb. 5 (1965), 504–516.
[W] A. Weil, *Jacobi Sums as 'Grössencharaktere'*, Trans. Amer. Math. Soc. VI, 73 (1952), 487–495.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA, SAN DIEGO
La Jolla, Cal. 92093, U.S.A.

Current address
DEPARTMENT OF MATHEMATICS
RUTGERS UNIVERSITY
New Brunswick, N. J. 08903, U.S.A.

Received on 15.9.1986
and in revised form on 6.11.1987 (1671)

ACTA ARITHMETICA
LII (1989)

Une nouvelle caractérisation des éléments de Pisot dans l'anneau des adèles de Q

par

MARTHE GRANDET-HUGOT (Caen)

Les éléments de Pisot d'un anneau d'adèles de Q ont été introduits par F. Bertrandias [1], elle en a donné une première caractérisation analogue à celle des nombres de Pisot réels.

En appliquant à ces ensembles une méthode voisine de celle qui nous a permis d'améliorer certains résultats de Pisot, dans le cas réel (cf. [4]), nous aboutissons à des caractérisations plus fines.

1. Définitions et notations. Soit $\boldsymbol{P}$ l'ensemble des valeurs absolues de Q, on note $|\cdot|_\infty$ la valeur absolue archimédienne et $|\cdot|_p$ la valeur absolue p-adique normalisée.

On désigne par $\boldsymbol{Q}_p$ le corps des nombres p-adiques, par $\boldsymbol{Z}_p$ son anneau de valuation et par $\boldsymbol{C}_p$ la complétion de sa clôture algébrique (on pose $\boldsymbol{Q}_\infty = \boldsymbol{R}$ et $\boldsymbol{C}_\infty = \boldsymbol{C}$).

On note:

$$D_p(a, r) = \{x \in \boldsymbol{C}_p;\ |x-a|_p < r\},$$

$$\hat{D}_p(a, r) = \{x \in \boldsymbol{C}_p;\ |x-a|_p \leqslant r\},$$

$$C_p(a, r) = \{x \in \boldsymbol{C}_p;\ |x-a|_p = r\}.$$

Soit I un ensemble fini de valeurs absolues de Q, on pose:

$$I^+ = I \cup \{\infty\} \quad \text{et} \quad I^- = I \setminus \{\infty\}.$$

Si I contient la valeur absolue archimédienne, on appelle I-adèle de $\boldsymbol{Q}$ tout élément de l'anneau:

$$\boldsymbol{A}_I = \boldsymbol{R} \prod_{p \in I^-} \boldsymbol{Q}_p;$$

si I ne contient pas la valeur absolue archimédienne, nous désignons par $\boldsymbol{A}_I$ le sous-anneau de $\boldsymbol{A}_{I^+}$ formé des éléments dont la composante réelle est nulle. L'élément unité de $\boldsymbol{A}_{I^+}$ est noté e_I, et pour tout élément $x = (x_p)_{p \in I^+}$ de $\boldsymbol{A}_I$, on note $|x|_p = |x_p|_p$.