DÉCEMBRE / DECEMBER 2000

IN THIS ISSUE / DANS CE NUMÉRO

22
No 4

C. R. Math. Rep. Acad. Sci. Canada Vol. 22 (4), 2000 pp. 129–146

THE LEAST PRIME IN A CONJUGACY CLASS

V. KUMAR MURTY, FRSC

ABSTRACT. We discuss the generalization to number fields of Linnik's famous theorem on primes in arithmetic progressions. We formulate two conjectural bounds, both of which capture all known cases. We also formulate some natural conjectures on the zeros of Artin L-functions which would imply these bounds.

RÉSUMÉ. Nous nous intéressons à la généralisation aux corps de nombres du théorème célèbre de Linnik sur les nombres premiers dans une progression arithmétique. Nous formulons deux conjectures sur des bornes qui toutes les deux couvrent tous les cas classiques connus. Nous formulons aussi quelques conjectures naturelles sur les zéros de fonctions L d'Artin qui impliquent les bornes ci-dessus.

1. Introduction. A classical theorem of Dirichlet asserts that given an arithmetic progression $a \pmod k$ with $(a,k) = 1$, there are infinitely many primes $p \equiv a \pmod k$. The problem of estimating the least such prime is an extremely difficult one. Let us denote by $P(k,a)$ the least such prime. It is known that the Riemann Hypothesis for Dirichlet L-functions implies that

$$P(k,a) \ll \phi(k)^2 (\log k)^2$$

where $\phi(k)$ denotes Euler's function. A famous conjecture of Chowla [2] asserts that

$$P(k,a) \ll k^{1+\epsilon}.$$

As there are $\phi(k)$ coprime progressions $a \pmod k$ and the $\phi(k)$-th prime is $\gg \phi(k)\log\phi(k)$, we know that

$$\max_a P(k,a) \gg \phi(k)\log\phi(k).$$

Thus, Chowla's conjecture is close to the best possible. A deep theorem of Linnik [7] asserts that there is an absolute constant $c > 0$ such that

$$P(k,a) \ll k^c.$$

Received by the editors September 1, 2000.

This paper was written while the author was visiting the Institute of Mathematical Sciences, Chennai. He would like to thank the Institute for its hospitality. Research was partially supported by a grant from NSERC.

AMS subject classification: Primary: 11R42, 11R44, 11R45; secondary: 11M41, 11R29.

Key words and phrases: Chebotarev Density Theorem, Artin L-functions, zeros of Dedekind zeta functions.

The present article is about generalizations of this result to number fields.

Let K be a number field and L a finite Galois extension of K. For any prime ideal $\mathfrak{p}$ of K which is unramified in L, and a prime ideal $\mathfrak{q}$ of L which divides $\mathfrak{p}$, we have the Frobenius automorphism $(\mathfrak{q}, L/K)$ which is an element of $G = \mathrm{Gal}(L/K)$. It is the unique element of G which on the residue field of $\mathfrak{q}$ induces the map $x \mapsto x^{\mathrm{N}\mathfrak{p}}$. (For basic properties of Frobenius automorphisms, see Lang [6, Ch. X, §1].) The set

$$\{(\mathfrak{q}, L/K) : \mathfrak{q}|\mathfrak{p}\}$$

forms a full conjugacy class in G which we denote $\mathrm{Fr}_{\mathfrak{p}} = \mathrm{Fr}_{\mathfrak{p}}(L/K)$.

Let C be a conjugacy class in G. We define

$$\pi_C(x, L/K) = \#\{\mathfrak{p} \text{ degree one} : \mathrm{N}_{K/\mathbb{Q}}\mathfrak{p} \leq x, \mathfrak{p} \text{ unramified in } L, \mathrm{Fr}_{\mathfrak{p}} = C\}.$$

Here, $\mathfrak{p}$ ranges over degree one primes of K, that is over primes $\mathfrak{p}$ of K with the property that $\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p}$ is a rational prime. By the Chebotarev density theorem, we know that as $x \longrightarrow \infty$,

$$\pi_C(x, L/K) \sim \frac{|C|}{|G|}\pi_K(x)$$

where $\pi_K(x)$ denotes the number of prime ideals of K of norm $\leq x$. In particular, $\pi_C(x, L/K)$ is positive for sufficiently large x.

We are interested in estimating the least value of x for which

$$\pi_C(x, L/K) > 0.$$

Let us denote this value of x by $P(C, L/K)$. Note that x is necessarily the norm of a degree one prime of K which is unramified in L. Let us also set

$$P(L/K) = \max_C P(C, L/K).$$

Consider the case $K = \mathbb{Q}$ and L a cyclotomic field, say $L = \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m-th root of unity. Then

$$(\mathbb{Z}/m)^\times \simeq \mathrm{Gal}(L/K)$$

with the map given explicitly by

$$a \pmod m \mapsto (\zeta_m \mapsto \zeta_m^a).$$

If C denotes the element of the Galois group corresponding to $a \pmod m$ under the above isomorphism, then $P(C, \mathbb{Q}(\zeta_m)/\mathbb{Q})$ is the least prime $p \equiv a \pmod m$ and by the theorem of Linnik [7] quoted above, we have

$$P(C, \mathbb{Q}(\zeta_m)/\mathbb{Q}) \leq m^c. \tag{1}$$

Since d_L is approximately m^m, this led Lagarias and Odlyzko [9, p. 415] to conjecture the following generalization of Linnik's theorem.

CONJECTURE 1.1. There is an absolute constant $c_1 > 0$ such that

$$P(L/K) \ll (\log d_L)^{c_1}.$$

Here d_L denotes the absolute value of the discriminant of $L/\mathbb{Q}$.

There is a large body of literature on generalizations of Linnik's theorem to number fields. (See for example, Rieger [18] and Fogels [3].) In particular, Fogels showed that there exists a constant $c_2 = c(n_K) > 0$ with the following property. Let $\mathfrak{f}$ be an integral ideal of K and α a residue class modulo $\mathfrak{f}$. Then, there exists a prime ideal $\mathfrak{p}$ of K with $\mathfrak{p} \equiv \alpha \pmod{\mathfrak{f}}$ and

$$\mathbb{N}_{K/\mathbb{Q}}\mathfrak{p} \leq (d_K \mathbb{N}\mathfrak{f})^{c_2}.$$

Note that corresponding to $\mathfrak{f}$, there is an Abelian extension L of K, namely the $\mathfrak{f}$-ray class field, whose Galois group corresponds to the the ray classes modulo $\mathfrak{f}$. In particular, the degree of L/K is equal to the ray class number $h(\mathfrak{f})$. Moreover, if we assume for simplicity that $\mathfrak{f}$ is a prime ideal, then

$$d_L \doteq d_K^{h(\mathfrak{f})} (\mathbb{N}\mathfrak{f})^{h(\mathfrak{f})-1}.$$

Thus, the above bound of Fogels can be stated in our notation as

$$P(L/K) \ll d_L^{c_2 n_K / n_L}.$$

The constant c_2 here is *not* absolute but depends (in an unspecified way) on the degree n_K of the base field.

There are other results, but for the most part, they deal with Abelian extensions only and give estimates in which the dependence on the fields involved is not made explicit.

The first effective results which addressed the general case are due to Lagarias and Odlyzko. Assuming the GRH, that is the Riemann Hypothesis for the Dedekind zeta function $\zeta_L(s)$, they showed that

$$P(L/K) \ll (\log d_L)^2. \tag{2}$$

Unconditionally, Lagarias, Odlyzko and Montgomery [8] showed that there is an absolute constant $c_3 > 0$ such that

$$P(L/K) \ll d_L^{c_3}. \tag{3}$$

They remark that this is probably the best result that can be proved by present techniques since in the case $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$ a quadratic extension, and $C \neq \{1\}$, the best result known (due to Burgess [1]) is

$$P(C, L/K) \ll d_L^{\frac{1}{4\sqrt{e}}}. \tag{4}$$

An old conjecture of I. M. Vinogradov asserts that for any $\epsilon > 0$, the right hand side in (4) can be replaced by d_L^{ϵ}.

In this paper, we shall reexamine the problem of estimating $P(C, L/K)$. We formulate two conjectures (Conjecture 2.1 and Conjecture 5.1) which we believe are the natural generalizations of Linnik's theorem and which fit more accurately than (3) with the known cases of cyclotomic fields (1) and quadratic fields (4). The first conjecture will involve the discriminant d_L of the field and the second conjecture will be formulated in terms of the Artin conductors of the characters of $\mathrm{Gal}(L/K)$.

2. Conjectures in terms of the discriminant.

CONJECTURE 2.1. There are absolute constants $a, b > 0$ so that

$$P(L/K) \ll d_L^{an_K/n_L} (\log d_L)^b.$$

Here, $n_K = [K : \mathbb{Q}]$ and $n_L = [L : \mathbb{Q}]$.

REMARK. As pointed out by Odlyzko, a factor such as $(\log d_L)^b$ is necessary as one sees by considering a field K and a sequence of fields L/K for which the root discriminant $\exp\{\frac{1}{n_L} \log d_L\}$ is constant.

If we assume the GRH, we should actually expect a better estimate than the one cited above (2).

CONJECTURE 2.2. Assume the GRH. Then

$$P(C, L/K) \ll \frac{1}{|C|} (\log d_L)^2.$$

The new feature in this conjecture is the appearance of the size of the conjugacy class. Indeed, it is reasonable to expect that if we are seeking primes whose Frobenius class is a large conjugacy class, it should be easier to find them.

3. The zeta function and Artin L-functions.

The Dedekind zeta function factors [15, Chapter 2] into L-functions associated to irreducible characters of $\mathrm{Gal}(L/K)$. Thus

$$\zeta_L(s) = \prod L(s, \chi)^{\chi(1)}.$$

As is generally seen in analytic number theory, factorization of a zeta function usually leads to stronger estimates. The difficulty in using the above factorization, however, is that it has not been proved that the individual factors $L(s, \chi)$ are holomorphic. The assertion that they indeed are holomorphic is Artin's Conjecture (AC). The one exception to this is that the L-function corresponding to the trivial character, namely the zeta function $\zeta_K(s)$ has a (simple) pole at $s = 1$.

If we assume both the GRH and Artin's holomorphy conjecture (AC), then a slightly weaker version of Conjecture 2.2 can be proved.

THEOREM 3.1. *Assume both the GRH and AC. Let* $n = n_L/n_K = [L : K]$. *Then*

$$P(C, L/K) \ll \frac{n_K^2}{|C|}(n \log n + \log d_L)^2.$$

All of the above can be formulated for conjugacy sets (*i.e.*, a union of conjugacy classes). In the case that $C = G - \{1\}$, an estimate which is sharper than that of Conjecture 2.2 was proved in [12]. Indeed, it was shown that assuming the GRH,

$$P(G - \{1\}, L/K) \ll \left(\frac{\log d_L}{|G| - 1}\right)^2.$$

It would be of interest to consider whether this could be true in general. That is, given any conjugacy set C, is it true that

$$P(C, L/K) \ll \left(\frac{\log d_L}{|C|}\right)^2?$$

4. Conjectures on zeros of the zeta function. All proofs of Linnik's theorem require delicate information about zeros of (Abelian) L-functions. It is therefore reasonable to expect that such information about Dedekind zeta functions or about Artin L-functions would enable us to establish the analogue of Linnik's theorem in our general setting of the least prime in a conjugacy class.

We formulate two conjectures about zeros of the Dedekind zeta function near $s = 1$ which would suffice to imply Conjecture 2.1. The first of these is [14, Conjecture 3.2].

CONJECTURE 4.1. There is an absolute constant $c_5 > 0$ such that the region

$$\sigma \geq 1 - \frac{c_5 n_L}{\log d_L}, \quad |t| \leq \frac{c_5 n_L}{\log d_L}$$

contains at most one zero of $\zeta_L(s)$. This zero, if it exists, is real and simple.

Let us set

$$N_L(\sigma, T) = \#\{\rho : \zeta_L(\rho) = 0, \sigma \leq \Re\rho \leq 1, |\Im\rho| \leq T\}.$$

We know that

$$N_L(0, T) \sim \frac{n_L}{2\pi} T \log T.$$

CONJECTURE 4.2. There is an absolute constant $\lambda > 0$ such that for any $\epsilon > 0$, and $\sigma > 1/2$, we have

$$N_L(\sigma, T) \ll_\epsilon (d_L^{1/n_L} T)^{(\lambda+\epsilon)(1-\sigma)}.$$

It should be possible to deduce Conjecture 2.1 assuming Conjectures 4.1 and 4.2.

In terms of what can be proved in the direction of Conjectures 4.1 and 4.2, we have the following result about zeros near $s = 1$.

THEOREM 4.1. *In the region 4.1, there is no zero of multiplicity* $> n_L^{2/3}$.

Regarding the conjecture on the zero-density estimate, Heath-Brown [5] has shown that

$$N_L(\sigma, T) \ll_{\epsilon, L} T^{(n_L+\epsilon)(1-\sigma)}(\log T)^{\gamma}$$

for $n_L \geq 3$ and an absolute constant $\gamma > 0$. In its present form, this estimate is essentially unusable for our purposes since the implied constant depends on the field in an undetermined way. It is probable that one can prove

$$N_L(\sigma, T) \ll_{\epsilon} (d_L T)^{(n_L+\epsilon)(1-\sigma)}(\log d_L T)^{\gamma}.$$

5. **Conjectures in terms of Artin conductors.** Again, exploiting the factorization

$$\zeta_L(s) = \prod_{\chi} L(s, \chi)^{\chi(1)}$$

we can formulate refinements of the conjectures of the previous sections. Associated to each χ is the Artin conductor A_χ. It is given by

$$A_\chi = d_K^{\chi(1)} \mathbb{N}\mathfrak{f}_\chi.$$

Here $\mathfrak{f}_\chi$ is an ideal of K which is supported on primes at which χ ramifies. Let $\mathfrak{p}$ be a prime of K and let G_0 denote the inertia group at any prime $\mathfrak{q}$ of L dividing $\mathfrak{p}$. There is a descending filtration

$$G_0 \supseteq G_1 \supseteq G_2 \cdots$$

in which G_i is defined to be the subgroup of G_0 which acts trivially on $O_L/\mathfrak{q}^{i+1}$. (Here, O_L is the ringer of integers of L.) If V is the representation space underlying χ, then the power of $\mathfrak{p}$ dividing $\mathfrak{f}_\chi$ is given by

$$n(\mathfrak{p}, \chi) = \sum_i \frac{|G_i|}{|G_0|} \operatorname{codim} V^{G_i}.$$

The factorization of the zeta function into the Artin L-functions is mirrored in the conductor-discriminant formula

$$d_L = \prod A_\chi^{\chi(1)}.$$

We now state a conjectural estimate for the least prime in a conjugacy class in terms of Artin conductors. In the next section, we shall state some natural hypotheses on zeros of Artin L-functions from which this is likely to follow.

Let us set

$$A = A(L/K) = \max A_\chi$$

and

$$d = \max \chi(1).$$

CONJECTURE 5.1. There is an absolute constant $c > 0$ so that

$$P(L/K) \ll A^c.$$

REMARK. Let us compare this with the classical Linnik theorem. Here $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_m)$. Every character of the Galois group of L/K has conductor dividing m. Moreover, there exist characters whose conductor is equal to m, and so $A = m$.

REMARK. It is not unreasonable to expect that Conjecture 5.1 can be proved for Abelian extensions L/K using existing technology.

REMARK. Suppose L/K is unramified. Then, for every χ, we have $A_\chi = d_K^{\chi(1)}$ and Conjecture 5.1 asserts that there is an absolute constant $c > 0$ such that

$$P(L/K) \ll d_K^{cd}.$$

We have the following implication between Conjecture 2.1 and the above conjecture. Denote by $k(G)$ the number of conjugacy classes of a finite group G.

PROPOSITION 5.1. *Conjecture 2.1 implies that there are absolute constants* $c_1, c_2 > 0$ *such that*

$$P(L/K) \ll A^{c_1} k(G)^{c_2}.$$

PROOF. The conductor-discriminant formula states that

$$\log d_L = \sum \chi(1) \log A_\chi.$$

From this, we see that

$$\log d_L \leq |G|^{\frac{1}{2}} k(G)^{\frac{1}{2}} (\log A)$$

where $k(G)$ denotes the number of conjugacy classes of G. Thus, with $n = |G|$, we have

$$\frac{1}{n} \log d_L \leq \left(\frac{k(G)}{n}\right)^{\frac{1}{2}} (\log A) \leq \log A. \tag{5}$$

Now, there exists a character χ_1 for which

$$\chi_1(1) \geq \left(\frac{|G|}{k(G)}\right)^{\frac{1}{2}}$$

since

$$\sum \chi(1)^2 = |G|.$$

By Minkowski's theorem, if $K \neq \mathbb{Q}$, we have $\log d_K \gg n_K$. Hence, for any χ, we have

$$\log A_\chi \geq \chi(1) \log d_K \gg \chi(1) n_K.$$

In particular,

$$\log A_{\chi_1} \gg \chi_1(1) \geq \left(\frac{|G|}{k(G)}\right)^{\frac{1}{2}}.$$

On the other hand, if $K = \mathbb{Q}$, then again by Minkowski's theorem and using the conductor-discriminant formula, we have

$$n_L \ll \log d_L = \sum \chi(1) \log A_\chi.$$

Hence, there exists a character χ for which

$$\log A_\chi \gg \left(\frac{|G|}{k(G)}\right)^{\frac{1}{2}}.$$

Thus, in all cases,

$$\log A \gg \left(\frac{|G|}{k(G)}\right)^{\frac{1}{2}}.$$

Thus,

$$\log d_L \ll k(G)(\log A)^2.$$

Hence

$$d_L^{a/n}(\log d_L)^b \ll A^a k(G)^b (\log A)^{2b} \ll A^{c_1} k(G)^{c_2}.$$

This proves the result.

6. **Conjectures on zeros of Artin L-functions.** Now consider three statements about zeros of Artin L-functions.

CONJECTURE 6.1. There is an absolute constant $0 < c_1 < 1$ such that $\prod L(s,\chi)$ does not vanish in the region

$$1 - \frac{c_1}{\log\left(A(|t|+2)^{dn_K}\right)} \leq \sigma \leq 1$$

except possibly for one zero. If this zero exists, it is real and simple.

We will also need a hypothesis about the exceptional zero in case it occurs.

CONJECTURE 6.2. Set

$$\Delta(t) = \log A + dn_K \log(|t|+2).$$

There are absolute and effective constants $0 < c_2, c_3 < 1$ such that the following holds. If ρ_0 is a zero (real or complex) of an $L(s,\chi)$ then any other zero $\rho = \sigma + it$ of an $L(s,\chi)$ satisfies

$$\beta < 1 - c_2 \frac{\log \frac{c_3}{|1-\rho_0|\Delta(t)}}{\Delta(t)}.$$

For the next statement, let us set

$$N(\chi,\sigma,T) = \#\{\rho : L(\rho,\chi) = 0, |\Re\rho| \geq \sigma, |\Im\rho| \leq T\}.$$

CONJECTURE 6.3. There is an absolute constant $\mu > 0$ such that for $\sigma > 1/2$, we have

$$\sum_{\chi} N(\chi, \sigma, T) \ll (AT)^{\mu(1-\sigma)}.$$

The bound (5) shows that Conjecture 4.1 implies Conjecture 6.1 and Conjecture 4.2 implies Conjecture 6.3.

It is likely that Conjecture 5.1 will follow if we assume the truth of Conjectures 6.1, 6.2 and 6.3.

In the direction of Conjecture 6.1, the best result that is known is the following [13]. Assuming Artin's conjecture, there is at most one zero of $\prod L(s, \chi)$ in the region

$$1 - \frac{c_1}{d^3 \log\bigl(A(|t|+2)^{n_K}\bigr)} \leq \sigma \leq 1$$

where d is the maximum of the character degrees. In the direction of Conjecture 6.2, the best result that is known (assuming Artin's conjecture) is due to Mahmoudian [10]. It states that the the estimate of Conjecture 6.2 holds with $\Delta(t)$ replaced with

$$\Delta_1(t) = d\Bigl(\log A + dn_K \log\bigl((|t|+2)\bigr)\Bigr).$$

There does not seem to be any result in the direction of Conjecture 6.3.

7. **Some functorial properties.** In this section, we establish some properties of $P(C, L/K)$ when we pass to subgroups or quotients of $G = \mathrm{Gal}(L/K)$.

PROPOSITION 7.1. *Let M be a subfield of L containing K. Let H be the subgroup of G fixing M. Let C be a conjugacy class which has a non-trivial intersection with H. Then either*

$$P(C, L/K) = \min_{C_0 \subseteq C \cap H} P(C_0, L/M)$$

or the right hand side divides the discriminant $\mathbb{N}d_{M/K}$. In the above, the minimum ranges over conjugacy classes C_0 of H which are contained in $C \cap H$.

PROOF. Let $\mathfrak{p}$ be a degree one prime of K, unramified in L, with $\mathrm{Fr}_{\mathfrak{p}}(L/K) = C$, and let $\mathfrak{b}$ be a prime of L dividing $\mathfrak{p}$. Then, $(\mathfrak{b}, L/K) \in C$ and every element of $\mathrm{Fr}_{\mathfrak{p}}$ is of the form $g(\mathfrak{b}, L/K)g^{-1}$ for some element $g \in G$. By assumption, one of these lies in H, say $(\mathfrak{b}, L/K)$ itself. Let C_0 denote its conjugacy class in H. Let $\mathfrak{q}$ be the prime of M below $\mathfrak{b}$. Then $\mathrm{Fr}_{\mathfrak{q}}(L/M) = C_0$ and $\mathbb{N}_{M/K}\mathfrak{q} = \mathfrak{p}$. Moreover, $\mathfrak{q}$ is unramified in L. Hence

$$P(C_0, L/M) \leq P(C, L/K).$$

Conversely, suppose $\mathfrak{q}$ is a degree one prime of M, unramified in L and with $\mathrm{Fr}_{\mathfrak{q}}(L/M)$ a class, say C_0, in $C \cap H$. Let $\mathfrak{p}$ be the prime of K over which it lies.

Then $\mathfrak{p}$ is a degree one prime of K, and *if* it is unramified in L, then $\mathrm{Fr}_{\mathfrak{p}}(L/K) = C$. Hence

$$P(C, L/K) \leq P(C_0, L/M).$$

On the other hand, if $\mathfrak{p}$ ramifies in L, it must also ramify in M and thus the right hand side divides the different.

PROPOSITION 7.2. *Let H be a normal subgroup of G and let M denote its fixed field. Suppose that C is a conjugacy class of G with the property that $CH \subseteq C$. Then either*

$$P(C, L/K) = P(\overline{C}, M/K)$$

or the right hand side divides the discriminant of L/K. In the above, $\overline{C}$ denotes the image of C in $\mathrm{Gal}(M/K) = G/H$.

PROOF. The condition $CH \subseteq C$ ensures that the image $\overline{C}$ of C in G/H is still a conjugacy class. Let $\mathfrak{p}$ be a prime of K with $\mathrm{Fr}_{\mathfrak{p}}(L/K) = C$. Let $\mathfrak{q}$ be a prime of M dividing $\mathfrak{p}$ and $\mathfrak{b}$ a prime of L dividing $\mathfrak{q}$. Then

$$(\mathfrak{b}, L/K)|_M = (\mathfrak{q}, M/K).$$

On the other hand,

$$(\mathfrak{b}, L/K)|_M = (\mathfrak{b}, L/K)H.$$

Hence, $(\mathfrak{q}, M/K) \in \overline{C}$ and so $\mathrm{Fr}_{\mathfrak{p}}(M/K) = \overline{C}$. Thus,

$$P(\overline{C}, M/K) \leq P(C, L/K).$$

The reverse inequality follows in a similar way except if $P(\overline{C}, M/K)$ ramifies in L.

8. **Examples.** If we assume Conjecture 5.1 for Abelian extensions and use the properties of the previous section, we can get sharper bounds than (3) in some cases. We indicate some examples in this section.

EXAMPLE. Let p be a prime and a a rational integer which is not a p-th power. Let α be a p-th root of a. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_p, \alpha)$. Then we can identify

$$\mathrm{Gal}(L/K) \simeq \left\{ \begin{pmatrix} u & v \\ 0 & 1 \end{pmatrix} u \in \mathbb{F}_p^{\times}, v \in \mathbb{F}_p \right\}.$$

The subgroup in which $u = 1$ forms a conjugacy class, C say. Then

$$P(C, L/K) = P\big(1, \mathbb{Q}(\zeta_p)/\mathbb{Q}\big) \ll p^c$$

by Linnik's theorem. Note that

$$d_L = p^{p(p-1)} a^{p-1}.$$

Thus,

$$P(C, L.K) \ll d_L^{c/n_L}.$$

EXAMPLE. Let ℓ be a rational prime. Let $K = \mathbb{Q}$ and L an extension with $\mathrm{Gal}(L/K) = \mathrm{GL}_2(\mathbb{Z}/\ell)$. Such extensions arise from elliptic curves, and more generally from modular forms. Indeed, let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Let L be the field obtained by adjoining the coordinates of all points of order dividing ℓ in $E(\overline{\mathbb{Q}})$. Then it follows from a result of Serre that for ℓ sufficiently large, the field L is of the above type.

For each prime p not dividing the conductor N, we set as usual

$$a_p = p + 1 - \#E(\mathbb{F}_p).$$

Now fixing a and b, we can ask for the least prime $p = P(a, b)$ such that

$$a_p \equiv a \pmod{\ell}, \quad p \equiv b \pmod{\ell}.$$

The discriminant d_L satisfies

$$\ell^4 \log \ell N \ll \log d_L \ll \ell^4 \log \ell N.$$

Thus, Conjecture 1.1 predicts that

$$P(a, b) \ll (\ell^4 \log \ell N)^{c_1}.$$

The theorem of Lagarias, Montgomery and Odlyzko (3) gives only the exponentially weaker bound

$$P(a, b) \ll \exp\{c_3 \ell^4 (\log \ell N)\}.$$

The Artin conductors can be estimated and one finds that

$$\log A \ll \ell \log \ell N.$$

Thus, Conjecture 5.1 predicts that

$$P(a, b) \ll \exp\{c\ell \log \ell N\}.$$

Using the functorial properties described in the previous section, we can actually prove the above estimate in some cases. Suppose that the roots of the quadratic polynomial

$$T^2 - aT + b$$

lies in $\mathbb{Z}/\ell$. Then the conjugacy set of matrices of trace a and determinant b intersects non-trivially the subgroup B of upper triangular matrices. Moreover, the set of upper triangular matrices of trace a and determinant b is stable under right multiplication by unipotent matrices (that is, matrices in B with diagonal entries equal to 1). Denote by U the set of unipotent matrices in B. It is in fact a normal subgroup of B. Thus, if we let M be the subfield of L fixed by B and N the subfield of L fixed by U, then N/M is Galois and even Abelian, the group being the set of diagonal matrices.

Now, if we assume Conjecture 5.1 for Abelian extensions, then by the properties of the previous section, it follows that

$$P(a,b) \ll \exp\{c\ell \log \ell N\}$$

and we see that this is the bound predicted by Conjecture 5.1 and it is an improvement over the bound given by (3).

9. Proofs of Theorem 3.1 and Theorem 4.1. In this section, we give proofs of two of the results stated in Sections 3 and 4.

PROOF OF THEOREM 3.1. This follows along standard lines so we just sketch it. If we assume both AC and GRH, then we have by [16, Corollary 3.7] the estimate

$$\pi_C(x, L/K) = \frac{|C|}{|G|} \operatorname{Li} x + \mathbf{O}(|C|^{\frac{1}{2}} n_K x^{\frac{1}{2}} \log Mx)$$

where

$$\log M = \log \frac{n_L}{n_K} + \frac{1}{n_K} \log d_K + \sum_{p \in P(L/K)} \log p.$$

Here, $P(L/K)$ is the support of $\mathfrak{N}_{K/\mathbf{Q}} d_{L/K}$.

Now consider the function

$$k(s) = k(s; x, y) = \left(\frac{y^{s-1} - x^{s-1}}{s-1} \right)^2$$

for $y > x > 1$. Then the inverse Mellin transform

$$\hat{k}(u) = \hat{k}(u; x, y) = \frac{1}{2\pi i} \int_{(2)} k(s) u^{-s}\, ds$$

is given by the formula (see [8])

$$\hat{k}(u) = \begin{cases} \frac{1}{u} \log \frac{u}{x^2} & \text{if } x^2 \le u \le xy \\ \frac{1}{u} \log \frac{y^2}{u} & \text{if } xy \le u \le y^2 \\ 0 & \text{otherwise.} \end{cases}$$

Let us set

$$F_C(s) = \frac{|C|}{|G|} \sum_{\chi} \overline{\chi(C)} \left(-\frac{L'}{L}(s, \chi) \right)$$

where the sum ranges over the irreducible characters χ of G and $L(s, \chi)$ denotes the Artin L-function associated to χ. Then the integral

$$\frac{1}{2\pi i} \int_{(2)} F_C(s) k(s; x, y)\, ds \tag{6}$$

can be evaluated in two different ways. On the one hand, it is equal to

$$\sum_{\substack{\mathfrak{p}^m:\mathfrak{p}\text{ unramified in } L\\ \mathrm{Fr}_{\mathfrak{p}^m}=C}} \frac{\log \mathbb{N}\mathfrak{p}}{\mathbb{N}\mathfrak{p}^m}\hat{k}(\mathbb{N}\mathfrak{p}^m;x,y)+\mathbf{O}\left(\frac{1}{x^2}\log\frac{y}{x}\right) \tag{7}$$

where the error term comes from ramified primes. On the other hand, moving the line of integration to the left, we see that (6) is equal to

$$\frac{|C|}{|G|}\left(\log\frac{y}{x}\right)^2-\frac{|C|}{|G|}\sum_{\chi}\overline{\chi(C)}\sum_{\rho_\chi}\left(\frac{y^{\rho_\chi-1}-x^{\rho_\chi-1}}{\rho_\chi-1}\right)^2$$

where ρ_χ runs over all (trivial and non-trivial) zeros of $L(s,\chi)$. Assuming AC and GRH, we know that the Riemann Hypothesis holds for each $L(s,\chi)$ (see [4, Corollary 1]). Moreover, the number $N(t,\chi)$ of zeros ρ_χ of $L(s,\chi)$ with $|\gamma_\chi - t|\le 1$ satisfies the estimate [16, (3.5.5)]

$$N(t,\chi)\ll \log A_\chi+\chi(1)n_K\log(|t|+2).$$

Here,

$$A_\chi = d_K^{\chi(1)}\mathbb{N}_{K/\mathbb{Q}}\mathfrak{f}_\chi$$

where $\mathfrak{f}_\chi$ is the Artin conductor of χ (see [16, §2.4]). Hence,

$$\sum_{\rho_\chi}\left(\frac{y^{\rho_\chi-1}-x^{\rho_\chi-1}}{\rho_\chi-1}\right)^2 \ll x^{-1}\sum_{j=1}^{\infty}\frac{1}{j^2}\left(\log A_\chi+\chi(1)n_K\log(j+2)\right)$$

and this is

$$\ll x^{-1}\left(\log A_\chi+\chi(1)n_K\right).$$

Hence,

$$\frac{|C|}{|G|}\sum_{\chi}\overline{\chi(C)}\sum_{\rho_\chi}\left(\frac{y^{\rho_\chi-1}-x^{\rho_\chi-1}}{\rho_\chi-1}\right)^2$$

is

$$\ll \frac{|C|}{|G|}\frac{1}{x}\sum_{\chi}|\chi(C)|\left(\log A_\chi+\chi(1)n_K\right).$$

Now, by orthogonality of characters,

$$\sum_{\chi}|\chi(C)|^2=\frac{|G|}{|C|}.$$

Moreover, using the estimate of [16, Proposition 2.5], we have

$$\log A_\chi+\chi(1)n_K\ll\chi(1)(\log d_K+n_K\log M).$$

Hence, using these estimates and the Cauchy-Schwarz inequality, we deduce that

$$\frac{|C|}{|G|}\sum_{\chi}\overline{\chi(C)}\sum_{\rho_\chi}\left(\frac{y^{\rho_\chi-1}-x^{\rho_\chi-1}}{\rho_\chi-1}\right)^2 \ll \frac{|C|^{\frac{1}{2}}}{|G|^{\frac{1}{2}}}\frac{1}{x}|G|^{\frac{1}{2}}(\log d_K + n_K\log M).$$

Now choose

$$x = \frac{|G|}{|C|^{\frac{1}{2}}}n_K\log M$$

and $y = \alpha x$ for a large constant $\alpha > 0$. This forces

$$\frac{|C|}{|G|}\left(\log\frac{y}{x}\right)^2 > \frac{|C|}{|G|}\left|\sum_{\chi}\overline{\chi(C)}\sum_{\rho_\chi}\left(\frac{y^{\rho_\chi-1}-x^{\rho_\chi-1}}{\rho_\chi-1}\right)^2\right| + \delta\frac{1}{x^2}\log\frac{y}{x}$$

where δ is the implied constant in the error term of (7). We can aslo estimate the contribution of prime powers to the main term of (7) and show that it is negligible. Hence, there exists a prime $\mathfrak{p}$ with $\mathrm{Fr}_{\mathfrak{p}} = C$ and

$$\mathbb{N}\mathfrak{p} \le y^2 = \alpha^2\frac{n_K^2}{|C|}(|G|\log M)^2.$$

By [19], Proposition 5, (7), we know that

$$\sum_{p\in P(L/K)}\log p \le \frac{2}{n}\log d_L.$$

Hence,

$$|G|\log M \le n\log n + \frac{n}{n_K}\log d_K + 2\log d_L \ll n\log n + \log d_L.$$

This completes the proof of Theorem 3.1.

PROOF OF THEOREM 4.1. Let $\rho = \beta + i\gamma$ be a zero of multiplicity m. For $\sigma > 1$, we have the inequality

$$\frac{m}{\sigma-\beta} < \frac{1}{\sigma-1} + \frac{1}{2}\log d_L \tag{8}$$

which follows from Stark [20]. Indeed, write $n_L = [L:\mathbb{Q}] = r_1 + 2r_2$ where r_1 (resp. r_2) denote the number of real (resp. complex) embeddings of L. The function

$$s(s-1)d_L^{s/2}\left(\pi^{-s/2}\Gamma(s/2)\right)^{r_1}\left((2\pi)^{-s}\Gamma(s)\right)^{r_2}\zeta_L(s)$$

is entire and is of order one. Thus it has a Hadamard factorization of the form

$$e^{A+Bs}\prod_{\rho}\left(1-\frac{s}{\rho}\right)e^{s/\rho}.$$

Logarithmically differentiating this and using the fact that the zeros of the above function have real part in $[0,1]$, one derives an inequality [20, pp. 139–140, (9) and (10)] for $\sigma > 1$,

$$\sum_{\rho} \frac{1}{\sigma - \rho} \leq \frac{1}{\sigma - 1} + \frac{1}{2}\log d_L + \left(\frac{1}{\sigma} - \frac{n_L}{2}\log \pi\right) + \frac{r_1}{2}\frac{\Gamma'(s/2)}{\Gamma(s/2)} + r_2\left(\frac{\Gamma'(s)}{\Gamma(s)} - \log 2\right).$$

Now the inequality stated above (8) is an easy consequence of this. Choose $\sigma = 1 + (c\log d_L)^{-1}$. Then we get

$$\beta < 1 - \left(\frac{m}{c + \frac{1}{2}} - \frac{1}{c}\right)\frac{1}{\log d_L}.$$

The quantity in parentheses on the right is positive when

$$c > (2m - 2)^{-1}.$$

Subject to this condition, it is maximized (as a function of c) by taking

$$c = \frac{1 + \sqrt{m}}{2(m-1)}.$$

This gives

$$\beta < 1 - \frac{c_0 m^{3/2}}{\log d_L}.$$

Hence, if

$$\beta > 1 - \frac{c_5 n_L}{\log d_L}$$

then

$$m \ll n_L^{2/3}.$$

10. **Some other bounds.** Denote by $k(G)$ the number of conjugacy classes of G. We have

$$P(L/K) \gg k(G)\log k(G).$$

This follows from the fact that the $k(G)$-th prime is $\gg k(G)\log k(G)$.

REMARK. If we take into account the fact that our primes are in fact the norms of degree one primes of K, then it is possible that we can obtain a lower bound of the form $n_K k(G)\log k(G)$. However, we do not pursue that here.

It is a result of Pyber [17] that for any group G of order $n \geq 4$, we have

$$k(G) \gg \frac{\log n}{(\log\log n)^8}.$$

In particular, let us apply this to $G = \mathrm{Gal}(L/K)$. By Serre [19, p. 128], we know that

$$\log d_L \leq n\log d_K + n_L \sum_{p \in P(L/K)} \log p + n_L \log n$$

where $n_L = [L:\mathbb{Q}]$, $n_K = [K:\mathbb{Q}]$ and $n = [L:K] = n_L/n_K$. (In the notation of an earlier section, the right hand side is $n_L \log M$.) Then

$$k(G) \gg \frac{\log \frac{\log d_L}{n_K \log M}}{(\log\log \frac{\log d_L}{n_K \log M})^8}.$$

In particular, if $K = \mathbb{Q}$ and we consider a family of fields L which are ramified at a fixed set $S = P(L/\mathbb{Q})$ of primes, then,

$$k(G) \gg_S \frac{\log\log d_L}{(\log\log\log d_L)^8}$$

and

$$P(L/\mathbb{Q}) \gg_S \frac{\log\log d_L}{(\log\log\log d_L)^7}.$$

Stronger lower bounds for $k(G)$ are known for nilpotent groups. It is a result of P. Hall that

$$k(G) \gg (\log n)$$

Thus for any nilpotent extension $L/\mathbb{Q}$ which is unramified outside S, we have

$$P(L/\mathbb{Q}) \gg_S \log\log d_L.$$

The Frattini subgroup of a group G is the intersection of the maximal subgroups of G. If G is a solvable group of order $n \geq 4$ with trivial Frattini subgroup then a result of Pyber [17] states that

$$k(G) \geq \exp\left\{c\frac{\log n}{(\log\log n)^2}\right\}$$

for some $c > 0$. In particular, if $L/\mathbb{Q}$ is a solvable extension with trivial Frattini and unramified outside S, then there is a constant $c_2 = c_2(S)$ such that

$$P(L/K) \gg (\log d_L)^{\frac{c_2}{(\log\log d_L)^2}}.$$

On the other hand, there exists a conjugacy class C with

$$|C| \geq |G|/k(G).$$

Hence, by Theorem 3.1, we see that the GRH and AC together imply that for this C,

$$P(C, L/K) \ll \frac{n_K^2 k(G)}{|G|}(n\log n + \log d_L)^2.$$

Again assuming $K = \mathbb{Q}$ for simplicity, and using the bound for d_L in terms of n_L and M, we have for this C,

$$P(C, L/K) \ll nk(G)(\log nM)^2.$$

A slightly better bound can be obtained as follows.

PROPOSITION 10.1. *Assume the GRH and AC. Then there exists a conjugacy class $C \subseteq G$ such that*

$$P(C, L/K) \ll B(\log B)^2$$

where

$$B = n_K n_L (\log M)^2.$$

In particular, if $K = \mathbb{Q}$ and we fix a set of primes S and consider Galois extensions L which are unramified outside S, then

$$P(C, L/K) \ll_S (\log d_L)(\log\log d_L).$$

PROOF. We have the estimate [16, Proposition 3.6]

$$\sum_{C \subseteq G} \frac{1}{|C|} \left(\psi_C(x) - \frac{|C|}{|G|}x\right)^2 \ll n_K^2 x (\log Mx)^2 (\log x)^2.$$

If $\psi_C(x) = 0$ for all C, then the left hand side is

$$\sum \frac{1}{|C|} \frac{|C|^2}{|G|^2} x^2 = \frac{1}{|G|} x^2.$$

This implies that

$$x \ll n_K^2 |G| (\log x)^2 \big((\log M)^2 + (\log x)^2\big).$$

This proves the first part.

Now if $K = \mathbb{Q}$ and we fix the ramification locus S, then

$$\log M \ll_S \log n = \log n_L \ll \log\log d_L.$$

Moreover,

$$n_L \log M \ll \log d_L.$$

This proves the second part.

REFERENCES

1. D. A. Burgess, *The distribution of quadratic residues and non-residues.* Mathematika **4**(1957), 106–112.
2. S. Chowla, *On the least prime in an arithmetic progression.* J. Indian Math. Soc. **1**(1934), 1–3.
3. E. Fogels, *On the distribution of prime ideals.* Acta Arith. **7**(1961/1962), 255–269.
4. R. Foote and V. Kumar Murty, *Zeros and poles of Artin L-series.* Math. Proc. Camb. Phil. Soc. **105**(1989), 5–11.
5. R. Heath-Brown, *On the density of zeros of the Dedekind zeta function.* Acta Arith. **33**(1977), 169–181.
6. S. Lang, *Algebraic Number Theory.* Springer Verlag, New York, 1986.
7. Ju. V. Linnik, *On the least prime in an arithmetic progression, I: The basic theorem.* Mat. Sb. **15**(1947), 139–178; *II: The Deuring-Heilbronn phenomenon.* Mat. Sb. **15**(1947), 347–368.

8. J. C. Lagarias, H. Montgomery and A. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem.* Invent. Math. **54**(1979), 271–296.
9. J. C. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem.* In: Algebraic Number Fields (ed. A. Fröhlich), Academic Press, New York, 1977, 409–464.
10. K. Mahmoudian, *A non-Abelian analogue of the least character non-residue.* Ph. D. thesis, University of Toronto, 1998.
11. V. Kumar Murty, *Non-vanishing of L-functions and their derivatives.* In: Automorphic forms and analytic number theory (ed. R. Murty), Univ. Montreal, Montreal, 1990, 89–113.
12. ———, *The least prime which does not split completely.* Forum Math. **6**(1994), 555–565.
13. ———, *Modular forms and the Chebotarev density theorem, II.* In: Analytic Number Theory (ed. Y. Motohashi), Cambridge Univ. Press, Cambridge, 1997, 287–308.
14. ———, *Stark zeros in certain towers of fields.* Math. Res. Letters **6**(1999), 511–520.
15. M. Ram Murty and V. Kumar Murty, *Non-vanishing of L-functions and Applications.* Progr. Math. **57**, Birkhauser, Boston, 1997.
16. M. Ram Murty, V. Kumar Murty and N. Saradha, *Modular forms and the Chebotarev density theorem.* Amer. J. Math. **110**(1988), 253–281.
17. L. Pyber, *Finite groups have many conjugacy classes.* J. London Math. Soc. **46**(1992), 239–249.
18. G. J. Rieger, *On the prime ideals of smallest norm in an ideal class* (mod $\mathfrak{f}$) *of an algebraic number field.* Bull. Amer. Math. Soc. **67**(1961), 314–315.
19. J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev.* Inst. Hautes Études Sci. Publ. Math. **54**(1981), 123–201.
20. H. M. Stark, *Some effective cases of the Brauer-Siegel theorem.* Invent. Math. **23**(1974), 135–152.

Department of Mathematics
University of Toronto
100 St. George Street
Toronto, ON M5S 3G3
email: murty@math.toronto.edu

C. R. Math. Rep. Acad. Sci. Canada Vol. **22** (4), 2000 pp. 147–150

A METRIC SYMBOL FOR PAIRS OF POLYNOMIALS OVER LOCAL FIELDS

ALEXANDRU ZAHARESCU

Presented by M. Ram Murty, FRSC

ABSTRACT. We define a metric symbol $(\frac{g}{f})$ for pairs (f,g) of polynomials of prime degree over a local field and prove an irreducibility criterion, a transitivity property and a reciprocity law.

RÉSUMÉ. Nous définissons un symbole métrique $(\frac{g}{f})$ pour une paire (f,g) de polynômes de degré un nombre premier à coéfficients dans un corps local. Nous démontrons un critère d'irreductibilité, une proprieté de transitivité et une loi de réciprocité.

1. Introduction. Let (K,v) be a local field and let q be a prime number. We consider pairs of monic polynomials $f,g \in K[X]$ of degree q. For such a pair we define a metric symbol $(\frac{g}{f})$ by the following rule:

$$\left(\frac{g}{f}\right) = \begin{cases} 1 & \text{if } v(R(f,g)) > \frac{q}{q-1} v(\Delta(f)) \\ -1 & \text{else} \end{cases}$$

where $\Delta(f)$ denotes the discriminant of f and $R(f,g)$ denotes the resultant of f and g. Although the above definition is not symmetric in f and g this metric symbol has some nice properties. We have the following:

THEOREM 1.

(i) (Irreducibility criterion): If f is irreducible and $(\frac{g}{f}) = 1$ then g is also irreducible.

(ii) (Transitivity): If f is irreducible and $(\frac{g}{f}) = (\frac{h}{g}) = 1$ then $(\frac{h}{f}) = 1$.

(iii) (Reciprocity Law): If f and g are irreducible then:

$$\left(\frac{g}{f}\right) = \left(\frac{f}{g}\right).$$

As an application we show that for any positive integer n the diophantine equation

$$(1.1) \quad (X^2+Y^2-Z^2-n)^2 + 4(Y-Z)(YZ^2 - X^2Y - Y^2Z + nZ) = 0$$

satisfies the local-global principle. More precisely we have:

Received by the editors October 26, 1999.
AMS subject classification: 11S05.

THEOREM 2. *Let $n \geq 0$ be an integer. The following are equivalent:*
(i) Equation (1.1) has solutions in $\mathbb{Z}$.
(ii) Equation (1.1) has solutions in $\mathbb{Z}_p$ for any prime p.
(iii) Equation (1.1) has solutions modulo $16n^3$.
(iv) n is a square.

2. Proof of Theorems 1 and 2. As in the Introduction, let (K, v) be a local field. We denote by $\bar{K}$ a fixed algebraic closure of K and continue to denote by v the unique extension to $\bar{K}$ of the valuation v on K. Let $G_K = \mathrm{Gal}(\bar{K}/K)$. For the general theory of local fields, see [Ar], [B-Ch] or [S]. In particular, we will need the following well known

LEMMA 3 (KRASNER'S LEMMA). *Let $\alpha, \beta \in \bar{K}$, α separable over K and assume that*

$$v(\beta - \alpha) > v\big(\sigma(\alpha) - \alpha\big)$$

for any $\sigma \in G_K$ for which $\sigma(\alpha) \neq \alpha$. Then $K(\alpha) \subseteq K(\beta)$.

For a proof, see [Ar, Ch. 2, Section 6, Theorem 8]. We will also need the following:

LEMMA 4. *Let $f \in K[X]$ be irreducible, separable and of prime degree q. Then the distance between any two distinct roots of f is the same.*

PROOF. Let $S = \{\theta_1, \theta_2, \ldots, \theta_q\}$ be the set of roots of f. Denote:

$$\delta = \min_{1 \leq i,j \leq q} v(\theta_i - \theta_j).$$

For any $j \in \{1, 2, \ldots, q\}$ consider the set

$$A_j = \{\theta_i \in S; v(\theta_i - \theta_j) > \delta\}.$$

It is easy to see that any two such sets A_{j_1} and A_{j_2} are either equal or disjoint. Moreover all these sets A_j have the same number of elements. Indeed, if A_{j_1} has more elements than A_{j_2} let $\sigma \in G_K$ be such that $\sigma(\theta_{j_1}) = \theta_{j_2}$. On one hand we know that σ induces a permutation on S. On the other hand σ is an isometry so it will send any element of A_{j_1} to an element of A_{j_2}. Hence σ induces an injection $A_{j_1} \hookrightarrow A_{j_2}$ which contradicts the above assumption on A_{j_1} and A_{j_2}. Thus all the sets A_j have the same number of elements, say e, and we obtain a partition of S in subsets with e elements each. Since q is a prime number it now follows that $e = 1$, so $A_j = \{\theta_j\}$ for any j. In conclusion $v(\theta_i - \theta_j) = \delta$ for any $i \neq j$ which concludes the proof of the lemma.

We now proceed to prove Theorem 1.

Let us first express the condition $(\frac{q}{f}) = 1$ in terms of distances between the roots of f and g. Let $f, g \in K[X]$ be monic polynomials of degree q. Denote by $\theta_1, \ldots, \theta_q$ the roots of f and by $\eta_1, \ldots, \eta_q$ the roots of g. We have

$$v\big(R(f,g)\big) = v\Big(\prod_{1 \leq i,j \leq q} (\theta_i - \eta_j)\Big) = \sum_{1 \leq i,j \leq q} v(\theta_i - \eta_j) \tag{2.1}$$

$$v(\Delta(f)) = v\Big(\prod_{1\le i\ne j\le q}(\theta_i-\theta_j)\Big) = \sum_{1\le i\ne j\le q} v(\theta_i-\theta_j). \tag{2.2}$$

The condition $(\frac{q}{f}) = 1$ can be written as follows:

$$\frac{1}{q^2}\sum_{1\le i,j\le q} v(\theta_i-\eta_j) > \frac{1}{q(q-1)}\sum_{1\le i\ne j\le q} v(\theta_i-\theta_j). \tag{2.3}$$

The Left Hand Side of (2.3) is the average value of $v(\theta_i-\eta_j)$ while the Right Hand Side is the average value of $v(\theta_i-\theta_j)$. Thus the condition $(\frac{q}{f}) = 1$ can be interpreted as saying that in average distances between the roots of f and g are smaller than distances between distinct roots of f. We now proceed to prove (i).

Let f be irreducible and $(\frac{q}{f}) = 1$. This implies in particular that $\Delta(f) \ne 0$ so f is separable. By Lemma 4 all the terms in the RHS of (2.3) are equal. Therefore there is a term in the LHS of (2.3), say $v(\theta_1-\eta_1)$, which is larger then any term in the RHS of (2.3). In other words η_1 is closer to θ_1 than any conjugate of θ_1 and from Krasner's Lemma it follows that $K(\theta_1) \subseteq K(\eta_1)$. Since $[K(\theta_1):K] = q$ it now follows: $K(\theta_1) = K(\eta_1)$ and g is irreducible.

(ii) Let f be irreducible and $(\frac{q}{f}) = (\frac{h}{g}) = 1$. From (i) we know that g and h are also irreducible. Let $\theta_1,\dots,\theta_q$ be the roots of f, $\eta_1,\dots,\eta_q$ be the roots of g and $\gamma_1,\dots,\gamma_q$ be the roots of h. From Lemma 4 it follows that for any $i \ne j$ we have $v(\theta_i-\theta_j) = \delta_f$ say, and similarly for g and h: $v(\eta_i-\eta_j) = \delta_g$, $v(\gamma_i-\gamma_j) = \delta_h$ for any $1 \le i \ne j \le q$. From (i) we also know that there is a pair (θ_1,η_1) say, for which we have: $v(\theta_1-\eta_1) > \delta_f$. Now let σ be any element of G_K such that $\sigma(\theta_1) \ne \theta_1$. Since σ is an isometry one has: $v\big(\sigma(\theta_1)-\sigma(\eta_1)\big) = v(\theta_1-\eta_1) > \delta_f$. It follows then immediately that $v\big(\eta_1-\sigma(\eta_1)\big) = v\big(\theta_1-\sigma(\theta_1)\big) = \delta_f$.

This proves two things: firstly, that $\delta_f = \delta_g$ and secondly it shows that for any root $\sigma(\theta_1)$ of f there is a unique root of g which is closer to $\sigma(\theta_1)$ than any conjugate of $\sigma(\theta_1)$, and this root is $\sigma(\eta_1)$. Applying the above reasoning to the pair (g,h) it follows that $\delta_g = \delta_h$ and moreover for each root η_j of g there is a unique root of h which is closer to η_j than any other root of g.

We deduce that for each root θ_i of f there is a unique root of h which is closer to η_1 than any other root of f. From this it follows easily that the corresponding inequality (2.3) for the pair (f,h) holds true and hence we have $(\frac{h}{f}) = 1$.

(iii) Let f and g be irreducible. There are two cases: either $(\frac{q}{f}) = (\frac{f}{g}) = -1$ or at least one of them equals 1. In the second case we know from the proof of (ii) that $\delta_f = \delta_g$. In combination with Lemma 4 this shows that $\Delta(f) = \Delta(g)$ and so $(\frac{q}{f}) = (\frac{f}{g})$ directly from the definition of the metric symbol. This completes the proof of Theorem 1.

REMARK. If one uses the same definition to extend the metric symbol to pairs of polynomials of any degree one loses the nice properties from Theorem 1. For example, property (i) from Theorem 1 fails for the following polynomials of

degree 4 over $K = \mathbb{Q}_p$, where $p \neq 2$: $g(x) = (x^2 - p)^2$ and $f(x)$ is the minimal polynomial of $\theta = \alpha^2 + p\alpha$, where $\alpha^4 = p$. Then $v(R(f,g)) > \frac{4}{3}v(\Delta(f))$, f is irreducible of degree 4 while g is not irreducible. For $p = 2$ one can take the same f and g where this time $\theta = \alpha^2 + 16\alpha$, $\alpha^4 = 2$.

Various metric results concerning distances between the roots of polynomials of any degree over a local field can be found in [P-Z,1], [P-Z,2], [A-P-Z] and [O].

PROOF OF THEOREM 2. Note that if n is a square one can take $Y = Z$ and $X = \sqrt{n}$ in (1.1). Thus (iv) implies (i). Clearly (i) implies (ii) and by the Chinese Remainder Theorem (ii) implies (iii). It remains to show that (iii) implies (iv).

Let $X = a$, $Y = b$, $Z = c$ be a solution of (1.1) modulo $16n^3$. We consider the polynomials $f(x) = x^2 - bx + \frac{b^2-n}{4}$ and $g(x) = x^2 - cx + \frac{c^2-a^2}{4}$. Then $\Delta(f) = n$, $\Delta(g) = a^2$ and $16R(f,g)$ equals the Left Hand Side of (1.1) where X, Y, Z are replaced by a, b and c respectively. Therefore n^3 divides $R(f,g)$.

Now choose a prime divisor p of n. Since

$$v_p(R(f,g)) \geq 3v_p(n) = 3v_p(\Delta(f))$$

it follows from the definition of $(\frac{g}{f})$ over $\mathbb{Q}_p$ that $(\frac{g}{f}) = 1$. Let's assume that f is irreducible over $\mathbb{Q}_p$. Then from Theorem 1 (i) it follows that g is irreducible over $\mathbb{Q}_p$. But g is not irreducible over $\mathbb{Q}_p$ since $\Delta(g)$ is a square. Therefore f is not irreducible over $\mathbb{Q}_p$ and hence $\Delta(f) = n$ is a square in $\mathbb{Q}_p$. This is true for any prime divisor p of n, so n has to be a square in $\mathbb{Z}$.

REFERENCES

[A-P-Z] V. Alexandru, N. Popescu and A. Zaharescu, *On the closed subfields of* C_p. J. Number Theory (2) **68**(1998), 131–150.

[Ar] E. Artin, *Algebraic numbers and algebraic functions.* Gordon and Breach Science Publishers, New York-London-Paris, 1967.

[B-Ch] Z. I. Borevich and I. R. Chafarevitch, *Théorie des nombres.* (Translated from the Russian by Myriam Verley and Jean-Luc Verley.) Reprint of the 1967 French translation. Les Grands Classiques Gauthier-Villars. Éditions Jacques Gabay, Sceaux, 1993.

[O] K. Ota, *On saturated distinguished chains over a local field.* Preprint.

[P-Z,1] N. Popescu and A. Zaharescu, *On the Structure of Irreducible Polynomials Over Local Fields.* J. Number Theory (1) **52**(1995), 98–118.

[P-Z,2] ———, *On the main invariant of an element over a local field.* Portugal. Math. **54**(1997), 73–83.

[S] J-P. Serre, *Corps locaux.* Deuxième édition. Publications de l'Université de Nancago, No. VIII. Hermann, Paris, 1968.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, IL 61801
USA
email: zaharesc@math.uiuc.edu

C. R. Math. Rep. Acad. Sci. Canada Vol. **22** (4), 2000 pp. 151–159

SUR LE COMPORTEMENT ASYMPTOTIQUE DU NOYAU ASSOCIÉ À UNE DIFFUSION DÉGÉNÉRÉE

SERGIO ALBEVERIO, ASTRID HILBERT ET VASSILY KOLOKOLTSOV

Présenté par Vlastimil Dlab, FRSC

ABSTRACT. We consider the asymptotic behaviour for small time of the heat kernel describing the motion of a brownian particle on a Riemannian manifold perturbed by a multiplicative noise. Asymptotic developments for the heat kernel and the trace are given and the first order terms are explicitely calculated.

RÉSUMÉ. On étudie le comportement asymptotique pour les petits temps du noyau associé à un système décrivant le mouvement d'une particule en mouvement sur une variété Riemannienne sous l'action du flot géodésique perturbé par un bruit multiplicatif. Les développements asymptotiques du noyau et de sa trace en puissances du temps sont donnés en général et avec des formules explicites pour les deux premiers termes.

1. Quelques méthodes d'estimation reliés à notre étude. Le problème d'estimer le noyau de la chaleur des diffusions non dégénérées respectivement dégénérées par une borne gaussienne et d'obtenir un développement asymptotique a été discuté dans plusieurs travaux, voir par exemple [15], [6], [1], [12], [4], [13]. Pour des opérateurs qui satisfont à une hypothèse de Hörmander uniformément faible les estimations uniformes pour le noyau de la chaleur ont été données par Léandre [13], par des méthodes d'analyse stochastique. Pour les générateurs hypoelliptiques gaussiens, D. Manankiandrianana d'une part et M. Chaleyat, L. Elie d'autre part (voir les références de [11]) ont classifié la structure des processus associés et donné les fonctionnelles d'action aussi bien que les fonctions "distances" appropriées.

Il a été remarqué par Maslov [14] que pour une classe d'équations pseudo différentielles (appelées équations du type "tunnel") données par une classe d'opérateurs pseudoelliptiques linéaires sur $\mathbb{R}^n$, qui contient par exemple les opérateur elliptiques du deuxième ordre, le noyau (la solution fondamentale) $p(t, z, z_0)$, $z, z_0 \in \mathbb{R}^n$, $t > 0$, peut être représenté asymptotiquement pour des temps suffisamment petits et avec h (la "constante de Planck") sous la forme

$$(1) \qquad p(t, z, z_0) = \frac{1}{(2\pi ht)^{\frac{n}{2}}} \exp\Big[-\frac{1}{h} S(t, z, z_0)\Big] \varphi(z, z_0)\big(1 + O(ht)\big),$$

Reçu par les éditeurs le le 26 novembre 1999.
Classification (AMS) par sujet : 35C20, 47D06, 53C17, 58J35, 81Q20.

avec une fonction positive $S(t, z, z_0)$, appelée entropie dans [14]. Dobrokhotov *et al.* [7] présentent une construction effective du développement asymptotique complet du type WKB (avec une phase imaginaire) comme série de puissances en t et h du reste multiplicatif $1 + O(ht)$ dans (1) pour le noyau correspondant à l'opérateur de Schrödinger $-\frac{1}{2}\Delta + V(x)$ avec un potentiel V régulier. Dans leur livre "Idempotent Analysis and its Applications" Kolokoltsov et Maslov (voir les références dans [11]) ont appliqué cette méthode pour obtenir un encadrement et un développement asymptotique du noyau associé à une équation du deuxième ordre dégénérée avec des coefficients de diffusion constants. Le cas de coefficients de diffusion non constants est plus compliqué pour ce qui concerne l'étude du comportement asymptotique ainsi que l'établissement de bornes rigoureuses.

Dans ce travail nous appliquons la méthode WKB avec une phase imaginaire au traitement des equations d'une diffusion dégénérée, dont le générateur est donné par un opérateur regulier du premier rang avec des coefficientes qui sont des fonctions non constantes. Ce génerateur definit un processus de Feller sur T^*M, le "flot géodesique stochastique". Il ne depend que la structure Riemannienne et en temps petits les coefficients du développement de la trace du noyau correspondant sont des invariants de la variété (comme dans le cas du mouvement Brownien sur une variété compacte). Il faut remarquer qu'en général T^*M peut être noncompact, donc à priori l'existence même de la trace pour le modèle consideré n'est pas claire. Une formule bien connue de H. Weyl décrit le comportement asymptotique des valeurs propres associées au problème de Dirichlet pour le Laplacien dans un domaine borné. Ce comportement est relié au comportement asymptotique de la trace $\mathrm{tr}(\exp[\Delta t])$ pour les petits temps. En fait, cette formule de Weyl fournit le terme principal d'un développement de la trace en puissances de t, dont les coefficients dépendent des propriétés géométriques du domaine (voir par exemple [9], [8] et ses références). Les résultats obtenus par Greiner géneralisent ces développement au cas des opérateurs différentiels sur des variétés (relativement) compactes. Notre résultat va au delà de ce contexte et n'est pas dérivable des résultats précédents. En fait sa preuve contient beaucoup d'ingrédients nouveaux et est assez compliquée nous n'en donnons ici qu'une exquisse. Les détails vont être publiés ailleurs.

2. Mouvement stochastique sur une variété riemannienne. La dynamique d'une particule brownienne soumise à une force déterministe est donnée par le système d'équations stochastiques pour $\big(x(t), y(t)\big) \in \mathbb{R}^d \times \mathbb{R}^d$

$$dx = ydt \quad dy = K(x)dt + dw, \tag{2}$$

òu la fonction K décrit la force déterministe et w est le mouvement brownien standard dans $\mathbb{R}^d$. Dans le cas $K = 0$ la position $x(t)$ est simplement l'intégrale du mouvement brownien. Beaucoup d'articles donnent une étude mathématique des systèmes (2), ainsi qu'une extension de ces études au cas de la théorie des

équations aux dérivées partielles stochastiques, voir par exemple [3], [2], [10], [16]. Pour l'étude d'une particule en mouvement sur une variété Riemannienne M de dimension n avec une métrique correspondente à une matrice g il est utile de plonger M dans $\mathbb{R}^m$, $m \geq n$, par une inclusion r, ayant autant de dérivées qu'en demande l'ordre de l'approximation du développement asymptotique. En introduisant des coordonnées locales $(x, y = g(x)\dot{x})$ sur le fibré cotangent T^*M, les équations définissant ce modèle s'écrivent

$$dx = \frac{\partial H}{\partial y}(x,y)dt \quad dy = -\frac{\partial H}{\partial x}(x,y)dt + \frac{\partial}{\partial x}\langle r(x), dw\rangle \tag{3}$$

où $H(x,y) := \frac{1}{2}\langle G(x)y, y\rangle$ est l'Hamiltonien donné par le flot géodésique standard sur M, $G(x) := g^{-1}(x)$ et w est maintenant le mouvement brownien standard sur $\mathbb{R}^m$. Le système (3) décrit donc le flot géodésique sur M perturbé par une force du type bruit multiplicatif, donnée par un bruit blanc avec un coefficient de diffusion dépendant de la position de la particule. L'existence et unicité de la solution de (3) est garantie si on assume que la deuxième dérivée de g existe et M est compacte (les fonctions coefficients sont donc bornées et Lipschitz-continues).

On voit immédiatement [11] que (3) est invariant par rapport au choix de coordonnées locales ainsi que par rapport aux rotations dans l'espace $\mathbb{R}^m$. La diffusion dégénérée (3) sur T^*M correspond à l'equation de la chaleur.

$$\begin{aligned}\frac{\partial}{\partial t}u &= \mathcal{L}_h u \\ &= \left(\left\langle G(x)y, \frac{\partial}{\partial x}\right\rangle - \frac{1}{2}\sum_{j=1}^{n}\left\langle \frac{\partial G(x)}{\partial x_j}y, y\right\rangle \frac{\partial}{\partial y_j} + \frac{h}{2}\sum_{i,j=1}^{n} g_{ij}(x)\frac{\partial^2}{\partial y_i \partial y_j}\right)u \end{aligned} \tag{4}$$

où $h = 1$. Cette équation est indépendante de l'inclusion r de M dans $\mathbb{R}^m$. La solution reflète seulement les propriétés intrinsèques de la géométrie de la variété Riemannienne M, en particulier la trace du noyau de la chaleur correspondant est invariante par rapport aux transformations mentionnées ci-dessus. Suivant la méthode WKB nous definissons un Hamiltonien $\mathcal{H}$ sur $T^*M \times T^*M$ tel que $\mathcal{H}(x, y, -h\frac{\partial}{\partial x}, -h\frac{\partial}{\partial y}) = \mathcal{L}_h$. L'Hamiltonien $\mathcal{H}$ est de dimension $4n$ et régulier du premier rang (dans le sense définit dans [11]). Pour transformer l'opérateur $\mathcal{L}_h$ sous la forme d'une somme de carrés des champs de vecteurs (forme étudiée dans [4], [13]) il faut appliquer un changement d'échelle qui dépend de x. Dans un petit voisinage du point de départ les conditions qui permettent de faire ce changement d'échelle sont semblables à celles d'une condition d'Hörmander faible, voir [13] et ses références (car un changement d'échelle ne change pas l'ordre du développement asymptotique).

3. Résultats. Soit $p(t, x, y, x_0, y_0)$ le noyau associé à l'équation de la chaleur (4) pour $h = 1$. Pour examiner le comportement de p pour les petits temps dans

un voisinage U du point initial $x_0, y_0 \in M$ nous introduisons des coordonnées locales [5] sur la variété M qui sont normales dans U. Pour ces coordonnées nous avons dans U: $x_0 = 0$, $\det g(x) = 1$ et (en utilisant la convention habituelle de sommation sur les indices répétés)

$$g_{kl}(x) = \delta_k^l + g_{kl}^{ij} x^i x^j + O(|x|^3), \tag{5}$$

pour $\forall x \in U$ et certains coefficients réels g_{kl}^{ij} avec $\sum_{i=1}^n g_{kl}^{ii} = 0$ et $\sum_{i,k=1}^n g_{ik}^{ik} = R$, où R est la courbure au point x_0.

THÉORÈME 3.1. *Pour y_0 quelconque fixe et x, $y - y_0$ et t suffisamment petits nous avons*

$$p(t,x,y,0,y_0) = \frac{12^{\frac{n}{2}}}{(2\pi)^n t^{2n}} \exp[-S(t,x,y,y_0)]\varphi(t,x,y,y_0) \tag{6}$$

où

$$\begin{aligned} S(t,x,y,y_0) := {} & \frac{6}{t^3}|x|^2[1 + O(|x|^2) + O(|y-y_0|^2)] + \frac{6}{t^2}\left\langle x, y + y_0 + O(|x|^2)\right\rangle \\ & + \frac{1}{2t}[|y|^2 + \langle y_0, y\rangle + |y_0|^2 + O(|x|^2) + O(|y-y_0|^2)] \end{aligned} \tag{7}$$

et

$$\varphi(t,x,y,y_0) = 1 + O(|x| + |y - y_0| + t). \tag{8}$$

Nous allons indiquer les techniques nouvelles et les étapes les plus importantes de la preuve. Tout d'abord le générateur changé d'échelle $\mathcal{L}_h$ de (4) est associé à l'Hamiltonien modifié $\mathcal{H}(x, y, -h\frac{\partial}{\partial x}, -h\frac{\partial}{\partial y})$. Théorème 2.3.1 [11] montre que les solutions des systèmes dynamiques donnés par l'équation de Hamilton-Jacobi respectivement de Hamilton associées à $\mathcal{H}$ sont les mêmes. Ceci est une conséquence du fait que pour $t \le t_0$, pour un certain $t_0 > 0$, il y a des polydisques suffisamment petits tels que l'application $(p_0, q_0) \mapsto (X_{\mathcal{H}}, Y_{\mathcal{H}})(t, x_0, y_0, p_0, q_0)$ est un difféomorphisme où (x_0, y_0, p_0, q_0) sont les valeurs initiales de l'unique solution $(X_{\mathcal{H}}, Y_{\mathcal{H}}, P_{\mathcal{H}}, Q_{\mathcal{H}})$ de l'equation hamiltonienne donnée par $\mathcal{H}$. De plus ces polydisques contiennent des polydisques centrés en $(X_{\mathcal{H}}, Y_{\mathcal{H}})(t, x_0, y^0, 0, 0)$, voir Théorème 2.3.4 [11]. Après une translation et un changement d'échelle par un polynôme de t, insérés dans le développements de $(x, y)(t)$ et de l'entropie correspondants, on obtient, ordre par ordre, un système fermé d'équations algébriques pour l'entropie. Une procédure analogue appliquée à l'équation du transport fournit le développement de la fonction φ en puissances de t.

La solution des équations hamiltoniennes correspondantes à $\mathcal{H}$ avec condition initiale $(x_0, y_0, 0, 0)$ est donnée par

$$\tilde{x} = x_0 - y_0 t + O(t^2) \quad \tilde{y} = y_0 + O(t) \quad \tilde{p} = O(t) \quad \tilde{q} = O(t). \tag{9}$$

Nous ne suivons pas la procedure générale donnée par les Théorèmes 2.3.1, 2.3.4 [11] mais adaptons ici une méthode directe qui permet un calcul plus simple

des coefficients paraissants dans (6)–(8). Cherchons d'abord un développement asymptotique pour la solution de l'équation de la chaleur associée à $\mathcal{L}$. Son approximation du premier ordre se trouve dans (1) et est donnée par la méthode WKB sous la forme $\varphi(t,x,y,y_0)\exp[-h^{-1}S(t,x,y,y_0)]$ avec des développements asymptotiques pour φ, et S. Pour développer les algorithmes dessous nous appliquons la représentation des solutions de l'equation aux dérivées partielles linéaire suivante

$$\lambda f(\xi,y) - (\xi,y)M\left(\frac{\partial f}{\partial \xi}(\xi,y), \frac{\partial f}{\partial y}(\xi,y)\right)^t = F(\xi,y) \tag{10}$$

où M est une $d \times d$ matrice avec des blocs de la forme $\left(\begin{smallmatrix}1 & 6\\ 1 & 4\end{smallmatrix}\right)$ avec des valeurs propres 1 et 2 et $\xi, y \in \mathbb{R}^d$.

LEMME 3.2. *Soit F un polynôme homogène de degré q sur $\mathbb{R}^{d\times d}$ et λ un nombre positif. Les uniques solutions de (10) sont des polynômes d'ordre q, combinaisons linéaires des monômes $\xi^I y^J$, où les I, J sont des multiindexes dans $\{0,\dots,q\}$, tels que $|I|+|J| = q$ ($|\cdot|$ décrivant la somme des composantes du multiindex). Plus précisement le coefficient de $\xi^I y^J$ est donné par*

$$\sum_{l_1+\cdots+l_d=\sigma} \sum_{j_1+\cdots+j_d=\kappa} \frac{\partial^q F}{\partial \xi_1^{l_1}\cdots\partial y_{j_d}^{j_d}} A_{\mu\nu}^{\sigma\kappa}.$$

où $\sigma = |I|$, $\kappa = |J|$ et $\mu \in \{1,\dots,\sigma\}$, respectivement $\nu \in \{1,\dots,\kappa\}$, sont égales aux sommes partielles des multiindexes I, respectivement J, qui sont en relation à la transformation qui diagonalize M. De plus $A_{\mu\nu}^{\sigma\kappa}$ sont des constantes. Pour $1 \le q \le 4$ ces constantes sont connues explicitement:

$$\begin{aligned}
\mathbf{q=1}:\ & A_{00}^{01}=\tfrac{1}{6} \quad A_{01}^{01}=0 \quad A_{00}^{10}=-1 \quad A_{10}^{10}=\tfrac{5}{6}\\
\mathbf{q=2}:\ & A_{00}^{02}=\tfrac{1}{30} \quad A_{01}^{02}=\tfrac{-1}{60} \quad A_{02}^{02}=\tfrac{2}{15}, \quad A_{00}^{11}=\tfrac{-1}{5} \quad A_{10}^{11}=\tfrac{3}{20}\\
& A_{01}^{11}=\tfrac{1}{10}, \quad A_{11}^{11}=\tfrac{1}{20}, \quad A_{00}^{20}=\tfrac{6}{5} \quad A_{00}^{20}=\tfrac{-9}{10} \quad A_{20}^{20}=\tfrac{4}{5}\\
\mathbf{q=3}:\ & A_{00}^{03}=\tfrac{1}{140} \quad A_{01}^{03}=\tfrac{-1}{210} \quad A_{02}^{03}=\tfrac{1}{70}, \quad A_{03}^{03}=\tfrac{2}{35} \quad A_{00}^{12}=\tfrac{-3}{70}\\
& A_{10}^{12}=\tfrac{-13}{420}, \quad A_{01}^{12}=\tfrac{1}{35} \quad A_{11}^{12}=\tfrac{-1}{105} \quad A_{02}^{12}=\tfrac{-3}{35}, \quad A_{12}^{12}=\tfrac{9}{70}\\
& A_{00}^{21}=\tfrac{9}{35} \quad A_{10}^{21}=\tfrac{-13}{70} \quad A_{20}^{21}=\tfrac{61}{420} \quad A_{01}^{21}=\tfrac{-6}{35} \quad A_{11}^{21}=\tfrac{2}{35},\\
& A_{21}^{21}=\tfrac{17}{210} \quad A_{00}^{30}=\tfrac{-54}{35} \quad A_{10}^{30}=\tfrac{39}{35} \quad A_{20}^{30}=\tfrac{-61}{70} \quad A_{30}^{30}=\tfrac{113}{140}\\
\mathbf{q=4}:\ & A_{00}^{04}=\tfrac{1}{630} \quad A_{01}^{04}=\tfrac{-1}{840} \quad A_{02}^{04}=\tfrac{1}{420} \quad A_{03}^{04}=\tfrac{1}{840} \quad A_{04}^{04}=\tfrac{2}{35}\\
& A_{00}^{13}=\tfrac{-1}{105} \quad A_{10}^{13}=\tfrac{17}{2520} \quad A_{01}^{13}=\tfrac{1}{140} \quad A_{11}^{13}=\tfrac{-1}{280} \quad A_{02}^{13}=\tfrac{-1}{70}\\
& A_{12}^{13}=\tfrac{11}{840} \quad A_{03}^{13}=\tfrac{-1}{140} \quad A_{13}^{13}=\tfrac{53}{840} \quad A_{00}^{22}=\tfrac{2}{35} \quad A_{10}^{22}=\tfrac{-17}{420}\\
& A_{20}^{22}=\tfrac{19}{630} \quad A_{01}^{22}=\tfrac{-3}{70} \quad A_{11}^{22}=\tfrac{3}{140} \quad A_{21}^{22}=\tfrac{-1}{210} \quad A_{02}^{22}=\tfrac{3}{35}\\
& A_{12}^{22}=\tfrac{-11}{140} \quad A_{22}^{22}=\tfrac{9}{70} \quad A_{00}^{31}=\tfrac{-12}{35} \quad A_{10}^{31}=\tfrac{17}{70} \quad A_{20}^{31}=\tfrac{-19}{105}\\
& A_{30}^{31}=\tfrac{46}{315} \quad A_{01}^{31}=\tfrac{9}{35} \quad A_{11}^{31}=\tfrac{-9}{70} \quad A_{21}^{31}=\tfrac{1}{35} \quad A_{31}^{31}=\tfrac{11}{105}\\
& A_{00}^{40}=\tfrac{72}{35} \quad A_{10}^{40}=\tfrac{-51}{35} \quad A_{20}^{40}=\tfrac{38}{35} \quad A_{30}^{40}=\tfrac{-92}{105} \quad A_{40}^{40}=\tfrac{263}{315}.
\end{aligned}$$

Nous avons en général

$$A_{\mu\nu}^{\sigma\kappa} = \sum_{\ell=0}^{\mu}\sum_{m=0}^{\sigma-\mu}\sum_{n=0}^{\kappa-\nu} C_{\mu}^{\ell}C_{\sigma-\mu}^{m}C_{\kappa-\nu}^{n}C_{\nu}^{\rho}\frac{(-1)^{m-n+\kappa}2^{\rho-1}(-3)^{l-\rho+\nu-\mu}6^{\sigma}}{\lambda+2q-l-m-n-\rho}.$$

Dans cette expression les coefficients explicites, respectivement C_i^j, représentent des coefficients binomiales, respectivement les composantes d'une matrice diagonale par blocs avec des blocs de la forme $\big((1,-2)^t(-1,3)^t\big)$ associés à la transformation de la base, où $(\cdot,\cdot)^t$ sont les colonnes de la matrice. Suivant la méthode WKB nous introduisons l'Ansatz (1) dans l'équation de la chaleur associée à $\mathcal{L}_h$, en séparant les ordres differents du paramètre de développement h. En comparant les termes d'ordre zéro nous arrivons à l'équation de Hamilton-Jacobi

$$\frac{\partial S}{\partial t}+\left\langle G(x)y,\frac{\partial S}{\partial x}\right\rangle-\frac{1}{2}\sum_{j=1}^{n}\left\langle\frac{\partial G(x)}{\partial x}y,y\right\rangle\frac{\partial S}{\partial y_j}+\frac{1}{2}\sum_{i,j=1}^{n}g_{ij}(x)\frac{\partial^2 S}{\partial y_i\partial y_j}=0. \tag{11}$$

Comparant les termes du premier ordre on obtient l'équation de transport:

$$\begin{aligned}\frac{\partial\varphi}{\partial t}&+\left\langle G(x)y,\frac{\partial\varphi}{\partial x}\right\rangle-\frac{1}{2}\sum_{j=1}^{n}\left\langle\frac{\partial G(x)}{\partial x_j}y,y\right\rangle\frac{\partial\varphi}{\partial y_j}\\&+\left\langle G(x)\frac{\partial S}{\partial y},\frac{\partial\varphi}{\partial x}\right\rangle+\frac{1}{2}\operatorname{tr}\left(\frac{\partial^2 S}{\partial y_i\partial y_j}\right)\varphi=0.\end{aligned} \tag{12}$$

Introduisant des coordonnées normales [5] en même temps que les approximations (5) et (9) dans l'équation de Hamilton-Jacobi nous n'arrivons pas à un système fermé d'équations algébrique comme dans le cas nondégéneré. Donc nous changeons l'échelle de façons que $\Sigma(t,\xi,y)\equiv S\big(t,t(\xi+\tilde{x}),y+\tilde{y},x_0,y_0\big)$, où $(\tilde{x},\tilde{y},\tilde{p},\tilde{q})$ est la solution du système hamiltonien associé à $\mathcal{H}$. D'après ce remplacement l'equation Hamilton-Jacobi prend la forme (avec $z_i:=(y_i-y_i^0)$)

$$\begin{aligned}\frac{\partial\Sigma}{\partial t}&-\frac{1}{t}\Big((\xi_i-y_i)-t^2\frac{1}{2}g_{ij}^{kl}(\xi_k-y_k^0)(\xi_l-y_l^0)z_j-y_k^0y_l^0y_j^0\Big)+O(t^3)\Big)\frac{\partial\Sigma}{\partial\xi_i}\\&-\frac{t}{2}\Big(g_{ij}^{kl}\big(y_i^0y_j^0y_l^0+(\xi_l-y_l^0)z_iz_j\big)\Big)+O(t^2)\Big)\frac{\partial\Sigma}{\partial y_k}\\&+\Big(\frac{1}{2}+\frac{t^2}{4}g_{ij}^{kl}(\xi_k-y_k^0)(\xi_l-y_l^0)+O(t^3)\Big)\frac{\partial\Sigma}{\partial y_i}\frac{\partial\Sigma}{\partial y_j}=0.\end{aligned} \tag{13}$$

Introduisant $\Sigma\equiv\Sigma_{-1}t^{-1}+\Sigma_0+\Sigma_1t+\cdots$ dans (13) nous pouvons séparer (13) dans un système d'équations pour les termes de même ordre en t. Nous arrivons comme ça à des équations du type mentionné dans le Lemme 3.2. Les équations homogènes ont solution égale à zéro. Nous commençons avec l'équation fermée en Σ_{-1} (ordre t^-1). L'équation correspondante à t ne dépend que de Σ_{-1} (calculé au premier étape) et Σ_1. Sa inhomogénéité est une somme de polynômes homogènes

d'ordres 2, 3, 4. La linéarité en F des solutions des equations différentielles permet d'appliquer le Lemme 3.2. Cette procedure va marcher pour tous les ordres en t. Pour éviter des formules trop longues nous nous bornons à donner ici le développement jusqu'à l'ordre 1. En utilisant la symétrie de g_{ij}^{kl}, Σ_1 est donné par: $2.5 g_{ij}^{kl} y_i^0 y_j^0 y_k^0 y_l^0 + O(t^3)$, en coordonnées normales. Pour la solution de (13) nous trouvons le développement asymptotique:

$$
\begin{aligned}
\Sigma = {} & \frac{6\xi_i^2 + 6\xi_i y_i + 2y_i^2}{t} \\
& + t\Big(-\frac{14}{15} g_{i,j}^{k,l} y_{0,k} y_{0,l} y_i y_j - \frac{59}{20} g_{i,j}^{k,l} y_{0,k} y_{0,l} \xi_i y_j + \frac{3}{5} g_{i,j}^{k,l} y_{0,k} y_{0,l} \xi_i \xi_j \\
& \quad - \frac{2}{15} g_{i,j}^{k,l} y_{0,j} y_{0,l} y_i y_k + \frac{7}{5} g_{i,j}^{k,l} y_{0,j} y_{0,l} \xi_i y_k + \frac{24}{5} g_{i,j}^{k,l} y_{0,j} y_{0,l} \xi_i \xi_k \\
& \quad + \frac{1}{15} g_{i,j}^{k,l} y_{0,i} y_{0,j} y_l y_k + \frac{11}{20} g_{i,j}^{k,l} y_{0,i} y_{0,j} \xi_k y_l + \frac{3}{5} g_{i,j}^{k,l} y_{0,i} y_{0,j} \xi_k \xi_l \\
& \quad + \frac{7}{10} g_{i,j}^{k,l} y_{0,l} \xi_i y_k y_j - \frac{9}{10} g_{i,j}^{k,l} y_{0,l} \xi_i \xi_j y_k - \frac{3}{2} g_{i,j}^{k,l} y_{0,l} \xi_i \xi_j \xi_k \\
& \quad - \frac{1}{5} g_{i,j}^{k,l} y_{0,j} \xi_i y_l y_k - \frac{6}{5} g_{i,j}^{k,l} y_{0,j} \xi_i \xi_k y_l - 3 g_{i,j}^{k,l} y_{0,j} \xi_i \xi_k \xi_l \\
& \quad - \frac{3}{56} g_{i,j}^{k,l} \xi_i y_l y_k y_j + \frac{1}{7} g_{i,j}^{k,l} \xi_i \xi_j y_l y_k + \frac{5}{7} g_{i,j}^{k,l} \xi_i \xi_j \xi_k y_l + g_{i,j}^{k,l} \xi_i \xi_j \xi_k \xi_l \Big) \\
& + O(t^2).
\end{aligned}
$$

La transformation qui fait passer de Σ à S nous donne (7) et en coordonnées normales $S = 6t^{-1}|y^0| + O(t^3)$. Pour résoudre l'équation de transport nous remplaçons φ par $\psi(t,\xi,y) \equiv t^\alpha \varphi(t, t\xi, y+\tilde{y}, 0, y^0)$ et assumons un développement en t pour $\psi = 1 + t\psi_1 + t^2\psi_2 + \cdots$, où $\alpha = 2n$ garantit que le terme constant est égale à 1. En procédant de la même façon comme pour l'équation de Hamilton-Jacobi nous obtenons:

$$
\begin{aligned}
\psi = {} & 1 + t^2\Big(-\Big(-\frac{3}{56} g_{k,i}^{i,j} \xi_k - \frac{3}{56} g_{k,i}^{j,i} \xi_k - \frac{3}{56} g_{k,j}^{i,i} \xi_k\Big)\xi_j \\
& + \frac{1}{6}\Big(\frac{7}{10} g_{i,j}^{i,k} y_{0,j} - \frac{1}{5} g_{k,j}^{i,i} y_{0,j} - \frac{3}{56} g_{k,i}^{i,j} y_j - \frac{3}{56} g_{k,i}^{j,i} y_j \\
& \quad - \frac{3}{56} g_{k,j}^{i,i} y_j - g_{i,i}^{k,l} y_{0,l}\Big) y_k \\
& + \frac{5}{6}\Big(\frac{7}{10} g_{i,j}^{i,k} y_{0,j} - \frac{1}{5} g_{k,j}^{i,i} y_{0,j} - \frac{3}{56} g_{k,i}^{i,j} y_j - \frac{3}{56} g_{k,i}^{j,i} y_j \\
& \quad - \frac{3}{56} g_{k,j}^{i,i} y_j - g_{i,i}^{k,l} y_{0,l}\Big) \xi_k \qquad (14) \\
& - \frac{1}{6} g_{i,i}^{k,l} y_{0,k} y_l - \frac{5}{6} g_{i,i}^{k,l} y_{0,k} \xi_l + \frac{1}{210} g_{i,j}^{i,k} y_k y_j + \frac{3}{140} g_{i,j}^{i,k} \xi_j y_k \\
& + \frac{4}{35} g_{i,j}^{i,k} \xi_j \xi_k + \frac{1}{30} g_{i,i}^{k,l} y_l y_k + \frac{3}{20} g_{i,i}^{k,l} \xi_k y_l + \frac{4}{5} g_{i,i}^{k,l} \xi_k \xi_l \\
& - \frac{1}{30} g_{i,i}^{k,l} y_{0,k} y_{0,l} + \frac{1}{15} g_{i,j}^{i,k} y_{0,j} y_{0,k} - \frac{1}{30} g_{k,j}^{i,i} y_{0,k} y_{0,j}\Big) + O(t^3).
\end{aligned}
$$

La transformation qui fait passer de ψ à φ nous donne (8). De plus nous pouvons écrire un développement complet pour les fonctions φ et S (nous utilisons ici des bornes uniformes pour les coefficients des terms négligés, en particulier pour les termes donnés par le développement de Duhamel). Le produit de (8) et du developpement de $\exp(S)$ donne le developpement de p d'ordre 2. Sur la diagonale nous obtenons ($x_0 = 0$)

$$\begin{aligned} p(t,0,y_0,0,y_0) &= t^{-2n}\exp[-6t^{-1}|y_0|^2](1 \\ &\quad + t^2\Big(-\frac{15}{280}g^{ji}_{ki}y_{0k}y_{0j} - \frac{15}{280}g^{ij}_{ki}y_{0k}y_{0j} + \frac{41}{280}g^{ii}_{kj}y_{0k}y_{0j} \\ &\quad - \frac{214}{280}g^{ik}_{ij}y_{0j}y_{0k} + \frac{252}{280}g^{kj}_{ii}y_{0k}y_{0j}\Big)(1+O(t^3)). \end{aligned} \tag{15}$$

Les calculations étaient réalisées par MAPLE. D'une façon semblable nous construisons un développement de p à tous les ordre. En reliant $p(t,x,y,x,y)$ à $p(t,0,y_0,x,y)$ et intégrant sur T^*M on obtient (en utilisant la compacticité de M et des bornes données dans [11]):

THÉORÈME 3.3. *Sous les hypothèses du Théorème 3.1, on a le développement asymptotique suivant par rapport au petit parametre t:*

$$\begin{aligned} T(t) &:= \int_{T^*M} p(t,x,y,x,y)\,dx\,dy \\ &= \frac{12^{\frac{n}{2}}}{(2\pi)^n t^{2n}}\big(\operatorname{Vol} M + a_3t^3 + a_4t^4 + \cdots + a_\nu t^\nu + O(t^{\nu+1})\big), \end{aligned}$$

où $\operatorname{Vol} M$ *est le volume de* M. *Le premier coefficient non trivial* a_3 *(proportionnel à la courbure Gaussienne de* M*) est donné par le coefficient de* t^2 *dans (15). Toutes les coefficients* a_j, $j = 3,4,\ldots$ *sont des quantités invariantes de* M *qui peuvent être calculés par la méthode décrite en précédence.*

Nous remarquons pour finir qu'on peut obtenir, comme d'habitude, des estimations pour les temps finis en considérant des convolutions multiples des expressions asymptotiques pour les petits temps.

REMERCIEMENTS. Nous remercions Z. Brzeźniak, D. Elworthy et R. Léandre pour des discussions fructueuses. Nous sommes aussi très reconnaissant à Paul Fischer pour son aide donnant la programmation en MAPLE que nous avons utilisé d'une façon essentielle. Une partie de ce travail a été achevée pendant un séjour de Astrid Hilbert à l'Université de Warwick dans le cadre d'une bourse TMR.

REFERENCES

1. S. Albeverio, A. Boutet de Monvel Berthier and Z. Brzeźniak, *Stationary phase in infinite dimensions by finite dimensional approximations: Application to the Schrödinger equation*. Potential Anal. 4(1995), 469–502.

2. S. Albeverio, A. Hilbert and V. Kolokoltsov, *Transience of stochastically perturbed classical Hamiltonian systems.* Stochastics Stochastics Rep. **60**(1997), 41–55.
3. S. Albeverio, A. Hilbert and E. Zehnder, *Hamiltonian systems with a stochastic force: Nonlinear versus linear, and a Girsanov formula.* Stochastics Stochastics Rep. **39**(1992), 159–188.
4. G. Ben Arous, *Noyau de la chaleur hypoelliptique et géométrie sous-Riemannienne.* In: Proc. Japanese-French Seminar in Stochastic Analysis, Lecture Notes in Math. **1322**, Springer-Verlag, 1988.
5. H. Cycon, R. Froese, W. Kirsch and B. Simon, *Schrödinger Operators with Application to Quantum Mechanics and Global Geometry.* Springer-Verlag, Berlin, 1987.
6. E. B. Davies, *Gaussian upper bounds for the heat kernel of some second order operators on Riemannian manifolds.* J. Funct. Anal. **80**(1988), 16–32.
7. S. Yu. Dobrokhotov, V. N. Kolokoltsov and V. P. Maslov, *The splitting of the low lying energy levels of the Schrödinger operators and the asymptotics of the fundamental solutions of the equation* $hu_t = \left(h^2\ell/2 - v(x)\right)u$. Teoret. Mat. Fiz. (3) **87**(1991), 323–375.
8. P. Gilkey, *Invariance, the heat equation, and the index theorem.* Publish or Perish, Berkeley, 1984.
9. P. Greiner, *An asymptotic expansion for the heat equation.* Arch. Rational Mech. Anal. **41**(1971), 163–218.
10. V. N. Kolokoltsov, *The stochastic HJB equation and stochastic WKB method.* In: Idempotency (ed. J. Gunawardena, Bristol 1994), Publ. Newton Inst. **11** (1998), 285–302.
11. ———, *Semiclassical Asymptotics for Diffusion and Stochastic Processes.* Springer Lecture Notes. Springer Verlag, 1999.
12. S. Kusuoka and D. Stroock, *Application of the Malliavin calculus, III.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **34**(1987), 391–442.
13. R. Léandre, *Uniform upper bounds for hypoelliptic kernels with drift.* J. Math. Kyoto. Univ. (2) **34**(1994), 263–271.
14. V. P. Maslov, *Global exponential asymptotics of the solutions of the tunnel equations and large deviation problems.* Trudy Mat. Inst. Steklov **163**(1985), 150–180.
15. S. A. Molchanov, *Diffusion processes and Riemannian geometry.* Usp. Math. Nauk **30**(1975), 3–59. Translated in Russ. Math. Surv. **30**(1975), 1–63.
16. A. Truman and K. Z. Zhao, *The stochastic Hamilton-Jacobi equation, stochastic heat equations and Schrödinger equations.* In: Stochastic Analysis and Applications (eds. D. Elworthy, I. M. Davies and A. Truman), World Scientific Press, 1996, 441–464.

Institut f. Angew. Mathematik
Universität Bonn
Sergio.Albeverio@uni-bonn.de
CERFIM, Locarno

Institution för Matematik
Luleå Tekniska Universitet
astrid@sm.luth.se

Department of Mathematics
Nottingham Trent University
vk@euler.ntu.ac.uk

Index—Volume 22, 2000