ACTA ARITHMETICA
XXVI (1975)

Examples of Iwasawa invariants, II

by

ROBERT GOLD (Columbus, Ohio)

Let l be an odd rational prime and $k = Q(\sqrt{-m})$ an imaginary quadratic number field with $(l, m) = 1$. Let K be the cyclotomic (or fundamental) Z_l-extension of k and $\lambda_l(k)$, $\mu_l(k)$ the Iwasawa invariants of K/k. In an earlier paper, [3], we showed how one could compute the values of these invariants in the case $\left(\frac{-m}{l}\right) = -1$. Our purpose below is to extend this method to the case $\left(\frac{-m}{l}\right) = +1$ and to give the results of some computations in this case.

Let ζ be a primitive l^n-th root of unity and P_n the unique subfield of $Q(\zeta_{n+1})$ of index $l-1$. Set $k_n = k_0 \cdot P_n$. Then k_n is cyclic of degree l^n over k_0 and $K = \bigcup_{n=0}^{\infty} k_n$. Let e_n be the exact power of l dividing the class number of k_n. By the fundamental result of Iwasawa, [4], for all sufficiently large n,

$$e_n = \lambda_l(k)n + \mu_l(k)l^n + c \quad \text{for} \quad c \in Z \text{ independent of } n,$$
$$\lambda_l(k),\ \mu_l(k) \in N.$$

Using the results of [1], [3] we have programmed a computation of e_1, e_2 in the case $(m, l) = 1$. In [3] we showed that a knowledge of e_0, e_1, e_2 is sufficient in many cases (all of those examined) to determine λ, μ when $\left(\frac{-m}{l}\right) = -1$. This assertion is based on a result of which Theorem 1, below, is a restatement.

Let $\Lambda = Z_l[[T]]$, the power series ring over the l-adic integers. Let M be a discrete Λ-module and $\hat{M} = \mathrm{Hom}_Z\left(M, \frac{Q_l}{Z_l}\right)$, the Pontryagin dual. If $\hat{M}$ is a noetherian torsion Λ-module, then $\hat{M}$ is isogenous to a Λ-module of the form $\bigoplus_{i=1}^{t} \frac{\Lambda}{(f_i^{s_i})}$ where $s_i \in N$ and each f_i is either

l or an irreducible distinguished polynomial of Λ ([7], [8], [10]).

Let $\omega_n = 1-(1-T)^{l^n} \in \Lambda$ and, for any Λ-module X, let $X^{\Gamma_n} = \{x \in X \mid \omega_n x = 0\}$. Call X strictly finite if $\frac{X}{\omega_n X}$ is finite.

See [3] for a proof of the following:

THEOREM 1. *If X is a strictly finite compact Λ-module with no finite submodule and X is isogenous to $\bigoplus_{i=1}^{t} \frac{\Lambda}{(f_i^{s_i})}$, then*

$$\#(\hat{X}^{\Gamma_0}) = \prod_{i=1}^{t} [\boldsymbol{Z}_l \colon (f_i(0)^{s_i})],$$

$$\#(\hat{X}^{\Gamma_n})/\#(\hat{X}^{\Gamma_{n-1}}) = \prod_{i=1}^{t} [\boldsymbol{Z}[\zeta_n] \colon (f_i(1-\zeta_n)^{s_i})].$$

Let A_n be the l-primary part of the ideal class group of k_n. Let $A = \varinjlim A_n$, where the limit is taken over the natural extension maps. This A is the Iwasawa module for K/k. When $\left(\frac{-m}{l}\right) = -1$, there is a unique ramified prime in K/k and $\hat{A}$ satisfies the hypotheses of Theorem 1. When $\left(\frac{-m}{l}\right) = +1$, however, there are two ramified primes in K/k and $\hat{A}$ is no longer strictly finite. We will find a strictly finite module by reducing A modulo the classes generated by ramified primes.

Let $\mathfrak{l}_n, \bar{\mathfrak{l}}_n$ be the two primes of k_n which lie over l. Then $\mathfrak{l}_n\bar{\mathfrak{l}}_n$ is an ideal of P_n and hence l-principal. Also $\mathfrak{l}_n^{l^n} = \mathfrak{l}_0$ and, if $\mathfrak{l}_0$ has l-order l^a in A_0, then the l-order of $\mathfrak{l}_n$ in A_n is l^{a+n}, [2]. Let $S = \{\mathfrak{l}_n, \bar{\mathfrak{l}}_n\}$, where the value of n will vary with the context. Let B_n be the quotient of A_n modulo the cyclic subgroup of A_n generated by the classes of $\mathfrak{l}_n, \bar{\mathfrak{l}}_n$. So $\#(A_n) = \#(B_n)\cdot l^{n+a}$. The natural extension $A_n \to A_m$, $m \geq n$, induces a map $B_n \to B_m$ which is injective, [2]. Let $B = \varinjlim B_n$ under these maps. We will show that $\hat{B}$ satisfies the hypotheses of Theorem 1. Clearly B is a quotient of A and therefore $\hat{B}$ can be imbedded in $\hat{A}$. Since $\hat{A}$ is a noetherian torsion Λ-module without finite submodule, [5], [6], [7], it follows that $\hat{B}$ has these properties as well. It remains to show that $\hat{B}$ is strictly finite.

Let $G = G_{n,m} = \mathrm{Gal}(k_m/k_n) \cong \boldsymbol{Z}_{l^{m-n}}$. Let I_m^S, E_m^S be, respectively, the ideals of k_m prime to ideals of S, the $S \cup S_\infty$-units of k_m (S_∞ = set of infinite primes). Map k_m to I_m^S by $a \mapsto (a)$ and then delete from (a) all occurrence of primes of S. The image, to be denoted by P_m^S, consists of all ideals principal modulo powers of $\mathfrak{l}_m, \bar{\mathfrak{l}}_m$. The following exact sequences of G-modules are immediate:

$$0 \to E_m^S \to k_m \to P_m^S \to 0, \qquad 0 \to P_m^S \to I_m^S \to B_m \to 0.$$

In the usual manner one pastes together cohomology sequences to arrive at

$$0 \to H^1(G, E_m^S) \to (I_m^S)^G/P_n^S \to (B_m)^G \to H^0(G, E_m^S) \to H^0(G, k_m).$$

Noting that $(I_m^S)^G = I_n^S$, we have

$$0 \to H^1(G, E_m^S) \to B_n \to (B_m)^G \to H^0(G, E_m^S) \to H^0(G, k_m).$$

The map $B_n \to (B_n)^G$ is the natural extension which, as we have remarked above, is injective. Hence $H^1(G, E_m^S) = \{0\}$. Moreover, the Herbrand quotient of E_m^S is computable (e.g.[9]) and shows that $\#(H^0(G, E_m^s)) = l^{m-n}$. We can, in fact, determine the structure of $H^0(G, E_m^s) = E_n^s/N(E_m^s)$. Since $\mathfrak{l}_n\bar{\mathfrak{l}}_n$ is an ideal of P_n, there is a g, relatively prime to l, such that $(\mathfrak{l}_n\bar{\mathfrak{l}}_n)^g = (\varrho_n)$ for some $\varrho_n \in P_n$. Furthermore, $\mathfrak{l}_n^{l^{n+a}} = \mathfrak{l}_0^{l^a}$ which is l-principal and l^{n+a} is the exact l-order of $\mathfrak{l}_n$ in A_n. For some g, prime to l, $(\mathfrak{l}_0^{l^a})^g = (\lambda)$, $\lambda \in k_0$. It is clear that E_n^s is generated by E_n (the units of k_n), ϱ_n, and λ. Every unit in k_n is the norm of a unit of k_m, [6]. Also $(\varrho_n) = (\mathfrak{l}_n\bar{\mathfrak{l}}_n)^g = N(\mathfrak{l}_m\bar{\mathfrak{l}}_m)^g = (N(\varrho_m))$. Hence $\varrho_n \in N(E_m^s)$. Hence $E_n^s/N(E_m^s)$ is generated by the class of λ and, since $\mathfrak{l}_m$ has exact l-order l^{m+a} in A_m, λ has order l^{m-n} modulo $N(E_m^s)$.

THEOREM 2. *B is strictly finite; $\#(B^{\Gamma_n}) = l^{e_n-n-a+t}$ for some fixed $t \geq 0$.*

Proof. B^{Γ_n} is the inductive limit of groups $(B_m)^{G_{n,m}}$ over increasing m. By the preceding remarks we have an exact sequence

$$(*) \qquad 0 \to B_n \to (B_m)^G \to \mathrm{Ker}\big(E_n^s/N(E_m^s) \to k_n/N(k_m)\big) \to 0.$$

We proceed to determine the size of this kernel. Let $s(n, m)$ denote the minimal s such that λ^{l^s} in k_n is the norm of an element of k_m. This power of λ generates the kernel and hence the kernel has order $l^{\varkappa(n,m)}$ where $\varkappa(n, m) = (m-n) - s(n, m)$.

LEMMA 1. (i) *If $n' \geq n$, then $s(n, m) \leq s(n', m) + (n'-n)$ and $\varkappa(n, m) \geq \varkappa(n', m)$.*

(ii) *If $m' \geq m$, then $s(n, m') \leq s(n, m) + (m'-m)$ and $\varkappa(n, m') \geq \varkappa(n, m)$.*

Proof. Let $N_{m,n}$ be the norm from k_m to k_n. If $m \geq n' \geq n$ and $\lambda^{l^s} = N_{m,n'}(\beta)$, $\beta \in k_m$, then $\lambda^{l^{s+(n'-n)}} = N_{m,n}(\beta)$. Hence $s(n, m) \leq s(n', m) + (n'-n)$. The inequality in (ii) follows in exactly the same manner and the statements for $\varkappa(n, m)$ follow by definition.

LEMMA 2. *The conductor of P_m/P_n is $\mathfrak{l}_n^f\bar{\mathfrak{l}}_n^f$ where*

$$f = f(P_m/P_n) = (m-n)l^n + \left(\frac{l^n-1}{l-1}\right) + 1.$$

Proof. The discriminant of $Q(\zeta_{n+1})/Q$ is well known. Since $Q(\zeta_{n+1})/P_n$ is tamely ramified, it is easy to compute the discriminant of P_n/Q and therefore also of P_m/P_n. If $d(P_m/P_n)$ denotes the exact power of $\mathfrak{l}_n\bar{\mathfrak{l}}_n$ dividing the discriminant of P_m/P_n, then

$$f(P_m/P_n) = \varphi(l^{m-n})^{-1}[d(P_m/P_n) - d(P_{n-1}/P_n)]$$

by the conductor-discriminant formula. The expression of Lemma 2 is the result of this computation.

LEMMA 3. *Let* $\nu_{\mathfrak{l}_0}(\lambda^{l-1}-1) = t+1$. *Then for each* n, $\varkappa(n, m) = t$ *for all sufficiency large* m.

Proof. Since k_m/k_n is cyclic, $\lambda^{l^s} \in N(k_m)$ iff λ^{l^s} is locally a norm everywhere. If $\mathfrak{p} \neq \mathfrak{l}_n, \bar{\mathfrak{l}}_n$, then λ is a $\mathfrak{p}$-unit and $\mathfrak{p}$ is unramified in k_m/k_n. Hence λ is a local norm at $\mathfrak{p}$. By the norm symbol product theorem, the smallest power of λ which is locally a norm at $\bar{\mathfrak{l}}_n$ is the smallest power of λ which is globally a norm. The completion of k_n at $\bar{\mathfrak{l}}_n$ equals the completion of P_n at $\mathfrak{l}_n\bar{\mathfrak{l}}_n$, the unique prime over l. In these completions, λ is a local unit.

First let $n = 0$. Since the conductor exponent for P_m/P_0, by Lemma 2 or as is well-known, is $m+1$, a unit of $(P_0)_l = Q_l$ is locally a norm from P_m if and only if, up to $(l-1)$-st roots of unity, it is congruent to 1 modulo l^{m+1}. Hence, if $\nu_{\mathfrak{l}_0}(\lambda^{l-1}-1) = t+1$, then $s(0, m) = m-t$ for all $m \geq t$. Therefore $\varkappa(0, m) = t$ for $m \geq t$.

For general n, by Lemma 1, we have $\varkappa(n, m) \leq \varkappa(0, m) = t$ for $m \geq t$. On the other hand, if $\nu_{\mathfrak{l}_0}(\lambda^{l-1}-1) = t+1$, then $\nu_{\mathfrak{l}_n}(\lambda^{l-1}-1) = (t+1)l^n$. The exponent of the conductor of P_{n+t}/P_n is $tl^n + \left(\frac{l^n-1}{l-1}\right)+1$ by Lemma 2. This is less than $(t+1)l^n$. Hence λ is a local norm from P_{n+t} to P_n. So $s(n, n+t) = 0$ or $\varkappa(n, n+t) = t$. Applying Lemma 1 again, we see that, for $m \geq n+t$, $t = \varkappa(n, n+t) \leq \varkappa(n, m) \leq \varkappa(0, m) = t$. So for every n and $m \geq n+t$, $\varkappa(n, m) = t$.

Returning to (*) and the proof of Theorem 2, we see that for all sufficiently large m,

$$\#[(B_n)^G] = \#(B_n)\cdot l^t = \#(A_n)\cdot l^{-(n+a)}\cdot l^t = l^{e_n-n-a+t}.$$

Let ε_n be the exact power of l dividing $\#[B^{\Gamma_n}]$. Then

$$\varepsilon_n = e_n - n - a + t \quad \text{and} \quad \varepsilon_n - \varepsilon_{n-1} = e_n - e_{n-1} - 1.$$

COROLLARY OF THEOREM 1 (see [3]). *If for some* $n \geq 1$, $\varepsilon_n - \varepsilon_{n-1} < \varphi(l^n)$, *then*

$$\mu(B) = 0 \quad \textit{and} \quad \lambda(B) = \varepsilon_n - \varepsilon_{n-1}.$$

The exact sequence $0 \to \boldsymbol{Z}/l^{n+a}\boldsymbol{Z} \to A_n \to B_n \to 0$ gives rise, in the limit, to $0 \to \boldsymbol{Z}_l \to A \to B \to 0$. Hence, by [3], $\mu_l(k) = \mu(A) = \mu(B)$ and $\lambda_l(k) = \lambda(A) = \lambda(B)+1$. Thus follows:

COROLLARY. *If* $(-m/l) = +1$ *and for some* $n \geq 1$, $e_n - e_{n-1} \leq \varphi(l^n)$, *then*

$$\mu_l(Q(\sqrt{-m})) = 0$$

and

$$\lambda_l(Q(\sqrt{-m})) = e_n - e_{n-1}.$$

Explanation of Tables

Table 1. For each $l = 3, 5, 7$, and 11 and for each d with $0 < d \leq 264$ and $(-d/l) = +1$ the computed values of e_0, e_1, e_2 are given. Recall e_i is the l-order of the class number of the ith layer of the $\boldsymbol{Z}_l$-extension of $Q(\sqrt{-d})$. The computational formula is that of [3].

Table 2. For each $l = 3, 5, 7$, and 11 and each d, $0 < d \leq 264$, the entry in the table gives the sign of $(-d/l)$ and the nonnegative integer $\lambda_l(Q(\sqrt{-d}))$. In all cases $\mu_l(Q(\sqrt{-d})) = 0$. The class number of $Q(\sqrt{-d})$ is given under h. For $(-d/l) = +1$ the values in this table are read off from Table 1 by application of the above corollary. In all cases $e_2 - e_1$ was sufficiently small to imply that $\mu = 0$ and $\lambda = e_2 - e_1$. For $(-d/l) = -1$ the values given are copied from [3]. For the case $l|d$, one may use the fact that if $e_0 = 0$ and l does not decompose as a product of distinct primes in $Q(\sqrt{-d})$, then all $e_n = 0$. The entries for $l|d$ are left blank in the table.

We note also that, as a consequence of Corollary 4 of [3], the formula $e_n = \lambda_n + e_0$ is valid for all $n \geq 0$ for all values of l and d in this table with the single exception $l = 3$, $d = 239$. In this exceptional case we have instead $e_n = 6n-2$ for $n \geq 1$.

Table 3. This table gives some values of the invariant t described in Theorem 2 and in Lemma 3. Note that if $e_0 = 0$, then $t = 0$ if and only if all $e_n = n$, [2].

References

[1] R. Gold, *Γ-extensions of imaginary quadratic fields*, Pacific J. Math. 40 (1972), pp. 83–88.
[2] — *The nontriviality of certain $\boldsymbol{Z}_l$-extensions*, to appear in J. Number Theory.
[3] — *Examples of Iwasawa invariants*, Acta Arith. 26 (1974), pp. 21–32.
[4] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. 65 (1959), pp. 183–226.
[5] — *On some properties of Γ-finite modules*, Ann. of Math. 70 (1959), pp. 291–312.
[6] — *On the theory of cyclotomic fields*, Ann. of Math. 70 (1959), pp. 530–561.
[7] — *On $\boldsymbol{Z}_l$-extensions of algebraic number fields*, Ann. of Math. 98 (1973), pp. 246–326.
[8] Yu. Manin, *Cyclotomic fields and modular curves* (Russian), Uspehi Matem. Nauk. 26 (6) (162) (1971), transl: Russian Math. Surveys, 26 (1971), pp. 7–77.
[9] M. Rosen, *Two theorems on Galois cohomology*, Proc. Amer. Math. Soc. 17 (1968), pp. 1183–1185.
[10] J. P. Serre, *Classes des corps cyclotomiques*, Sem. Bourbaki, 174 (1958), pp. 1–11.

Table 1

$l = 3$

d	e_0	e_1	e_2
8	0	1	2
11	0	1	2
20	0	1	2
23	1	2	3
35	0	2	4
47	0	2	4
56	0	2	4
59	1	2	3
68	0	1	2
71	0	1	2
83	1	2	3
95	0	1	2
104	1	2	3
107	1	3	5
116	1	2	3
119	0	1	2
131	0	1	2
143	0	1	2
152	1	2	3
155	0	1	2
164	0	3	6
167	0	1	2
179	0	1	2
191	0	1	2
203	0	1	2
212	1	2	3
215	0	1	2
227	0	2	4
239	1	4	10
248	0	1	2
251	0	1	2
260	0	2	4
263	0	1	2

$l = 5$

d	e_0	e_1	e_2
4	0	1	2
11	0	2	4
19	0	1	2
24	0	1	2
31	0	1	2
39	0	1	2
51	0	2	4
56	0	1	2
59	0	1	2
71	0	1	2
79	1	2	3
84	0	1	2
91	0	1	2
104	0	2	4
111	0	1	2
116	0	1	2
119	1	2	3
131	1	2	3
136	0	2	4
139	0	1	2
151	0	1	2
159	1	2	3
164	0	2	4
179	1	2	3
184	0	1	2
191	0	1	2
199	0	1	2
211	0	1	2
219	0	1	2
231	0	1	2
239	1	2	3
244	0	1	2
251	0	1	2
259	0	1	2
264	0	1	2

$l = 7$

d	e_0	e_1	e_2
3	0	1	2
19	0	1	2
20	0	1	2
24	0	1	2
31	0	1	2
40	0	1	2
47	0	1	2
52	0	1	2
55	0	1	2
59	0	1	2
68	0	1	2
83	0	1	2
87	0	1	2
103	0	1	2
104	0	1	2
111	0	2	4
115	0	1	2
131	0	1	2
132	0	1	2
136	0	2	4
139	0	1	2
143	0	3	6
152	0	1	2
159	0	1	2
164	0	1	2
167	0	1	2
187	0	1	2
195	0	2	4
199	0	1	2
215	1	2	3
223	1	2	3
227	0	1	2
244	0	1	2
248	0	1	2
251	1	2	3
255	0	1	2
264	0	1	2

$l = 11$

d	e_0	e_1	e_2
7	0	1	2
8	0	1	2
19	0	2	4
24	0	1	2
35	0	1	2
39	0	1	2
40	0	1	2
43	0	1	2
51	0	1	2
52	0	1	2
68	0	1	2
79	0	1	2
83	0	1	2
84	0	1	2
87	0	1	2
95	0	1	2
107	0	2	4
116	0	1	2
120	0	1	2
123	0	1	2
127	0	2	4
131	0	1	2
139	0	1	2
151	0	1	2
164	0	1	2
167	0	1	2
183	0	1	2
184	0	1	2
195	0	1	2
211	0	1	2
215	0	1	2
219	0	1	2
227	0	2	4
228	0	1	2
239	0	1	2
244	0	2	4
248	0	1	2
255	0	1	2
259	0	1	2
260	0	1	2
263	0	1	2

Table 2

d	h	$l = 3$	5	7	11	d	h	$l = 3$	5	7	11
3	1		−0	+1	−0	132	4		−0	+1	
4	1	−0	+1	−0	−0	136	4	−0	+2	+2	−0
7	1	−0	−0		+1	139	3	−1	+1	+1	+1
8	1	+1	−0	−0	+1	143	10	+1	−1	+3	
11	1	+1	+2	−0		148	2	−0	−0	−0	−0
15	2			−0	−0	151	7	−0	+1	−3	+1
19	1	−0	+1	+1	+2	152	6	+1	−0	+1	−0
20	2	+1		+1	−0	155	4	+1		−0	−0
23	3	+1	−0	−0	−0	159	10		+1	+1	−0
24	2		+1	+1	+1	163	1	−0	−0	−0	−0
31	3	−1	+1	+1	−0	164	8	+3	+2	+1	+1
35	2	+2			+1	167	11	+1	−0	+1	+1
39	4		+1	−0	+1	168	4		−0		−0
40	2	−0		+1	+1	179	5	+1	+1	−0	−0
43	1	−0	−0	−0	+1	183	8		−0	−0	+1
47	5	+2	−1	+1	−0	184	4	−0	+1	−0	+1
51	2		+2	−0	+1	187	2	−0	−0	+1	
52	2	−0	−0	+1	+1	191	13	+1	+1	−0	−0
55	4	−0		+1		195	4			+2	+1
56	4	+2	+1		−0	199	9	−1	+1	+1	−0
59	3	+1	+1	+1	−0	203	4	+1	−0		−0
67	1	−0	−0	−0	−0	211	3	−2	+1	−0	+1
68	4	+1	−0	+1	+1	212	6	+1	−0	−0	−0
71	7	+1	+1	−1	−0	215	14	+1		+1	+1
79	5	−0	+1	−0	+1	219	4		+1	−0	+1
83	3	+1	−0	+1	+1	223	7	−0	−0	+1	−0
84	4		+1		+1	227	5	+2	−1	+1	+2
87	6		−0	+1	+1	228	4		−0	−0	+1
88	2	−0	−0	−0		231	12		+1		
91	2	−0	+1		−0	232	2	−0	−0	−0	−0
95	8	+1		−0	+1	235	2	−0		−0	−0
103	5	−0	−1	+1	−0	239	15	+6	+1	−0	+1
104	6	+1	+2	+1	−0	244	6	−1	+1	+1	+2
107	3	+2	−0	−0	+2	247	6	−1	−0	−0	−0
111	8		+1	+2	−0	248	8	+1	−0	+1	+1
115	2	−0		+1	−0	251	7	+1	+1	+1	−0
116	6	+1	+1	−0	+1	255	12			+1	+1
119	10	+1	+1		−0	259	4	−0	+1		+1
120	4			−0	+1	260	8	+2		−0	+1
123	2		−0	−0	+1	263	13	+1	−0	−0	+1
127	5	−0	−2	−0	+2	264	8		+1	+1	
131	5	+1	+1	+1	+1						

Table 3

d	l	h	t	λ	d	l	h	t	λ
11	3	2	0	1	136	5	4	1	2
11	5	2	1	2	136	7	4	1	2
19	11	1	1	2	143	7	10	1	3
20	3	2	0	1	164	3	8	3	3
35	3	2	1	2	164	5	8	1	2
47	3	5	2	2	227	3	5	1	2
51	5	2	3	2	239	3	15	0	6
56	3	4	1	2	244	11	6	1	2
84	5	4	0	1	248	3	8	0	1
104	5	6	1	2	260	3	8	1	2

DEPARTMENT OF MATHEMATICS
OHIO STATE UNIVERSITY
Columbus, Ohio

Received on 20. 8. 1973 (447)

ACTA ARITHMETICA
XXVI (1975)

Limit theorems for lacunary series and uniform distribution mod 1

by

WALTER PHILIPP (Urbana, Ill.)

Dedicated to Professor Paul Erdös to his 60th birthday

1. Introduction. A sequence $\langle x_n\rangle$ of real numbers is called uniformly distributed mod 1 if its discrepancy

$$(1.1)\qquad D_N = \sup_{0\leqslant a<\beta\leqslant 1} |N^{-1}A(N, a, \beta)-(\beta-a)|\to 0.$$

Here $A(N, a, \beta)$ is the number of indices $n\leqslant N$ with $a\leqslant\{x_n\}<\beta$. (As usual, $\{\varepsilon\}$ denotes the fractional part of ε.) Let $\langle n_k, k\geqslant 1\rangle$ be a lacunary sequence of integers, i.e. a sequence of integers satisfying

$$(1.2)\qquad n_{k+1}/n_k\geqslant q>1 \qquad (k=1,2,\ldots).$$

It is well known (see [8]) that the sequence $\langle n_k x\rangle$ is uniformly distributed mod 1 for almost all x. A much sharper result is due to Erdös and Koksma [3]. They proved that for almost all x

$$(1.3)\qquad ND_N(x) \ll \big(N\log^3 N\log\log N\omega(N)\big)^{1/2}$$

where $\omega(N)$ is any monotone sequence increasing to ∞. In 1954 Erdös and Gaal improved (1.3) to

$$(1.4)\qquad ND_N(x) \ll N^{1/2}(\log\log N)^{5/2+\varepsilon} \quad \text{a.e.}$$

for any $\varepsilon>0$, but their result was never published. (See [1], p. 56.) As a matter of fact most workers in the field expected even a law of the iterated logarithm to hold which would replace the exponent $5/2+\varepsilon$ in (1.4) by $\frac{1}{2}$ which is best possible. The purpose of this paper is to prove this conjecture, often referred to as the Erdös–Gaal conjecture. More precisely, we shall prove the following theorem.

THEOREM 1. *For almost all x*

$$(1.5)\qquad 32^{-1/2}\leqslant \limsup_{N\to\infty}\frac{ND_N(x)}{\sqrt{N\log\log N}}\leqslant C$$