Ist $c \equiv 2 (\mathrm{mod}\,4)$, so läßt γ_3 offenbar keine Nullstelle von $x^n - a$ oder $x^{2n} + 2^n a^2$ fest. Ist $c \equiv 0 (\mathrm{mod}\,8)$, so gilt $\gamma_3(\sqrt{2}) = \sqrt{2}$, und γ_3 läßt eine Nullstelle von $x^n - a$ bzw. $x^{2n} + 2^n a^2$ genau dann fest, wenn es ein $j_4 \equiv 2 (\mathrm{mod}\,4)$ gibt mit

$$c \cdot j_4 \equiv -8 j_3 (\mathrm{mod}\,4n),$$

bzw. ein $j_5 \equiv 1 (\mathrm{mod}\,2)$ mit

$$c \cdot j_5 \equiv -8 j_3 (\mathrm{mod}\,4n).$$

Beides ist genau dann der Fall, wenn $(c, 4n) | 8 j_3$. Ist $c \equiv 4 (\mathrm{mod}\,8)$ so gilt $\gamma_3(\sqrt{2}) = -\sqrt{2}$. Dann läßt γ_3 eine Nullstelle von $x^n - a$ fest genau dann, wenn es ein $j_4 \equiv 2 (\mathrm{mod}\,4)$ gibt mit

$$c j_4 \equiv -8 j_3 (\mathrm{mod}\,4n),$$

also genau dann, wenn

$$(c, 4n) | 8 j_3.$$

Eine Nullstelle von $x^{2n} + 2^n a^2$ bleibt genau dann fest, wenn es ein $j_5 \equiv 1 (\mathrm{mod}\,2)$ gibt mit

$$c j_5 \equiv -8 j_3 + 2n (\mathrm{mod}\,4n),$$

also genau dann, wenn

$$(c, 4n) | (-8 j_3 + 2n).$$

Beide Teilerbedingungen sind gleichwertig. Nach Hilfssatz 1 ergibt sich also die Behauptung. Damit ist Satz 4 bewiesen.

Literaturverzeichnis

[1] N. C. Ankeny and C. A. Rogers, *A conjecture of Chowla*, Ann. of Math. 53 (1951), S. 541–550.

[2] H. Flanders, *Generalisation of a theorem of Ankeny and Rogers*, ibid. 57 (1953), S. 392–400.

[3] I. Gerst, *On the theory of n-th power residues and a conjecture of Kronecker*, Acta Arith. 17 (1970), S. 121–139.

[4] A. Schinzel, *A refinement of a theorem of Gerst on power residues*, ibid. 17 (1970), S. 161–168.

[5] V. Schulze, *Die Verteilung der Primteiler von Polynomen auf Restklassen II*, Journ. Reine Angew. Math. 281 (1976), S. 126–148.

[6] E. Trost, *Zur Theorie der Potenzreste*, Nieuw Arch. Wiskunde 18 (1934), S. 58–61.

Eingegangen am 13. 2. 1976
und in revidierter Form am 14. 5. 1976 (815)

ACTA ARITHMETICA
XXXIII (1977)

An explicit bound for Iwasawa's λ-invariant

by

BRUCE FERRERO (Cambridge, Mass.)

For each finite extension k of the field $\boldsymbol{Q}$ of rational numbers, and for each prime number p, Iwasawa has defined a non-negative integer $\lambda_p(k)$ (see [4] for a description of the meaning of this invariant). We will give an explicit bound for $\lambda_p(k)$, for all p, when k is one of the ten imaginary quadratic fields described below. The method used is a refinement of a technique of Metsänkylä [5].

THEOREM. *Let $k = \boldsymbol{Q}(\sqrt{-d})$ be the imaginary quadratic field of discriminant $-d$, where $d \leqslant 20$, $d = 24$, or $d = 40$. Then for each prime number p, we have $\lambda_p(k) < p^{3(p-1)/2}$.*

Proof. If $p \leqslant 7$ and $p \leqslant d$, if $p = d = 11$, or if $p = d = 19$, then the validity of the theorem may be checked by calculating the exact value of $\lambda_p(k)$ (usually 0 or 1) by the formulas of [2]. We will therefore assume that $p \nmid d$ and that p is greater than the minimum of d and 7.

Let $\boldsymbol{Z}_p$ and $\boldsymbol{Q}_p$ denote respectively the ring of p-adic integers and field of p-adic numbers. Let χ be the Dirichlet character for k; then χ has conductor d, is defined on the rational integers $\boldsymbol{Z}$, and assumes the values -1, 0, and 1. Let $\omega\colon \boldsymbol{Z} \to \boldsymbol{Z}_p$ be the Dirichlet character of conductor p which satisfies the congruence $\omega(a) \equiv a (\mathrm{mod}\,p)$, for all $a \in \boldsymbol{Z}$. Let $L_p(s; \chi\omega)$ be the p-adic L-function for the character $\chi\omega$ (see [3] for the definition). Then $L_p(s; \chi\omega)$ is defined for $s \in \boldsymbol{Z}_p$ and takes values in $\boldsymbol{Z}_p$ for such s. The main step in the proof consists in showing that if n is a nonnegative integer such that $\lambda_p(k) \geqslant p^n$, then $L_p(s; \chi\omega)$ is divisible by p^{n+1}, for all $s \in \boldsymbol{Z}_p$.

Let w be the number of roots of 1 in k. Define, for any $b, c \in \boldsymbol{Z}$, a rational number $h(b, c)$ by

$$h(b, c) = (-w/2d) \sum_{j=1}^{d-1} j \chi(b + cj).$$

Then the following properties are easily verified:

(i) $h(b, c) = \chi(c) h(b', 1)$, if $b' \in \boldsymbol{Z}$ and $b \equiv b'c (\mathrm{mod}\,d)$;

(ii) If $b > 0$, then

$$h(b, 1) = h(0, 1) - (w/2) \sum_{j=0}^{b-1} \chi(j);$$

(iii) $h(0, 1) = h(k)$, the class number of k.

In particular, $h(b, c) \in \boldsymbol{Z}$ if $(c, d) = 1$.

For each $n \geqslant 0$, and each $a \in \boldsymbol{Z}_p$, define $s_n(a) \in \boldsymbol{Z}$ by the conditions

$$0 \leqslant s_n(a) < p^{n+1}, \quad s_n(a) \equiv a(\operatorname{mod} p^{n+1}\boldsymbol{Z}_p).$$

Define $V' = \{\omega(a): 1 \leqslant a \leqslant (p-1)/2\}$. For each $a \in \boldsymbol{Z}$, and each $n \geqslant 0$, define

$$H(a, n) = \sum_{v \in V'} h\big(s_n(av), p^{n+1}\big).$$

Iwasawa [3] constructed a power series $f(T; \chi\omega) \in \Lambda = \boldsymbol{Z}_p[[T]]$ satisfying

$$L_p(s; \chi\omega) = 2f\big((1+pd)^s - 1; \chi\omega\big), \quad \text{for all } s \in \boldsymbol{Z}_p.$$

Furthermore, his construction gives, for each $n \geqslant 0$, the congruence:

$$(w/2)f(T; \chi\omega) \equiv \sum_{i=0}^{p^n-1} H(c_i, n)(1+T)^i (\operatorname{mod} \omega_n \Lambda),$$

where $c_i = (1+pd)^{p^n - i}$, and $\omega_n = (1+T)^{p^n} - 1 \in \Lambda$.

By the properties (i)–(iii) above, this congruence may be rewritten as follows:

(1) $$\big(\chi(p^{n+1})(w/2)\big) f(T; \chi\omega) \equiv \sum_{i=0}^{p^n-1} a_i (1+T)^i (\operatorname{mod} \omega_n \Lambda),$$

where

$$a_i = \sum_{v \in V'} \big(h(k) - (w/2) t_{i,v}\big),$$

and where $t_{i,v}$ is a "partial sum" of χ, i.e., a sum of the form

$$\sum_{j=0}^{r} \chi(j),$$

for some positive integer r (r depends on i, v, and n).

Now let n be a non-negative integer such that $\lambda_p(k) \geqslant p^n$. Then by [2] (see also [3], § 7) we have $f(T; \chi\omega) \equiv 0 (\operatorname{mod} p\Lambda + T^{p^n}\Lambda)$. Since $\omega_n \in p\Lambda + T^{p^n}\Lambda$, it follows from (1) by a simple argument that p divides a_i. The ten fields k in question all have the property that

$$|h(k) - (w/2)t| \leqslant 2,$$

where t is any partial sum of χ, and so it follows that

$$|a_i| \leqslant p - 1,$$

and therefore $a_i = 0$, $0 \leqslant i < p^n$. Returning to the congruence (1), we find

$$f(T; \chi\omega) \equiv 0 (\operatorname{mod} \omega_n \Lambda),$$

and consequently

$$L_p(s; \chi\omega) \in \big((1+pd)^{sp^n} - 1\big)\boldsymbol{Z}_p \subseteq p^{n+1}\boldsymbol{Z}_p,$$

for all $s \in \boldsymbol{Z}_p$. If the theorem were false, then, setting $n = 3(p-1)/2$, it would follow in particular that

(2) $$L_p(-1; \chi\omega) \in p^{(3p-1)/2}\boldsymbol{Z}_p.$$

Let $L = L_p(-1; \chi\omega)$. To derive a contradiction to (2), note first that since pd is not a prime power, L is a non-zero algebraic integer in F (see [1] or [3], § 2) where $F \subseteq \boldsymbol{Q}_p$ is the number field generated over $\boldsymbol{Q}$ by the values of the character ω. By fixing an embedding of F into the complex numbers $\boldsymbol{C}$, we may also view $\chi\omega$ as a character with values in $\boldsymbol{C}$; then ([3], § 2) we have the equality of complex numbers:

(3) $$L = -\big(p^2 d^2 / 2\pi^2 \tau(\chi\omega)\big) L(2; \chi\omega),$$

where $L(2; \chi\omega)$ is the value at 2 of the usual ($\boldsymbol{C}$-valued) L-function for $\chi\omega$, and where $\tau(\chi\omega)$ is the Gauss sum

$$\tau(\chi\omega) = \sum_{a=1}^{pd} \chi\omega(a)\exp(2\pi i a/pd).$$

Let $|\ |_i$ $(1 \leqslant i \leqslant [F:\boldsymbol{Q}]/2)$ be the complex absolute values of F. From (3), we find

(4) $$|L|_i = \big((pd)^{3/2}/2\pi^2\big)|L(2; \chi\omega)| < \big((pd)^{3/2}/2\pi^2\big) \sum_{n \geqslant 1} n^{-2} = \frac{1}{12}(pd)^{3/2} < p^3.$$

Let M be the norm of L from F to $\boldsymbol{Q}$; then M is a positive integer, and

(5) $$M = \prod_{i=1}^{[F:\boldsymbol{Q}]/2} |L|_i^2 < (p^6)^{(p-1)/4} = p^{3(p-1)/2}.$$

Let R be the ring of integers of F, and let $\mathfrak{p} = R \cap p\boldsymbol{Z}_p$, a prime ideal of R lying above p. By (2), it follows that $L \in \mathfrak{p}^{(3p-1)/2}$, so that M is divisible by $p^{(3p-1)/2}$, which contradicts (5) and completes the proof.

Remarks. The argument also shows, as in [5], that the invariant $\mu_p(k)$ is 0, for all p, where k is one of the fields of the theorem.

The theorem may also be proved by estimating L (which has a simple expression as a character sum, see [3], § 2-3) directly; however, the method given above provides a better estimate for $\lambda_p(k)$ than that stated in the theorem, as an examination of inequalities (4) and (5) shows. But for $k = Q(\sqrt{-1})$, for example, we have $\lambda_p(k) \leqslant 1$ for all $p \leqslant 349$ (see [2]) which suggests the possibility that $\lambda_p(k)$ may be uniformly bounded independently of p, when k is fixed.

References

[1] L. Carlitz, *Arithmetic properties of generalized Bernoulli numbers*, J. Reine Angew. Math. 202 (1959), pp. 174–182.
[2] B. Ferrero, Thesis, Princeton Univ. (1975).
[3] K. Iwasawa, *Lectures on p-adic L-functions*, Princeton Univ. Press, Princeton 1972.
[4] — *On Z-extensions of algebraic number fields*, Ann. Math. 98 (1973), pp. 246–326.
[5] T. Metsänkylä, *On the Iwasawa invariants of imaginary abelian fields*, to appear.

Received on 10. 3. 1976 (825)

ACTA ARITHMETICA
XXXIII. 4 (1977)

ERRATA

Page, line	For	Read
300^2 and 300_2	$-6\left[\frac{c}{h}\right]$	$-6\left[\frac{c}{h}\right]$
308^{18}	thes	this
321_4	$f([(r+1)n/m])$	$f([(r+1)n/m])$