

Ist $c \equiv 2 \pmod{4}$, so läßt γ_3 offenbar keine Nullstelle von $x^n - a$ oder $x^{2n} + 2^n a^2$ fest. Ist $c \equiv 0 \pmod{8}$, 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 $j_4 \equiv 2 \pmod{4}$ gibt mit

$$c \cdot j_4 \equiv -8j_3 \pmod{4n},$$

bzw. ein $j_5 \equiv 1 \pmod{2}$ mit

$$c \cdot j_5 \equiv -8j_3 \pmod{4n}.$$

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

$$c j_4 \equiv -8j_3 \pmod{4n},$$

also genau dann, wenn

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

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

$$c j_5 \equiv -8j_3 + 2n \pmod{4n},$$

also genau dann, wenn

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

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)

An explicit bound for Iwasawa's λ -invariant

by

BRUCE FERRERO (Cambridge, Mass.)

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

Proof. If $p \leq 7$ and $p \leq d$, 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 \mathbf{Z}_p and \mathbf{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 \mathbf{Z} , and assumes the values $-1, 0$, and 1 . Let $\omega: \mathbf{Z} \rightarrow \mathbf{Z}_p$ be the Dirichlet character of conductor p which satisfies the congruence $\omega(a) \equiv a \pmod{p}$, for all $a \in \mathbf{Z}$. 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 $s \in \mathbf{Z}_p$ and takes values in \mathbf{Z}_p for such s . The main step in the proof consists in showing that if n is a nonnegative integer such that $\lambda_p(k) \geq p^n$, then $L_p(s; \chi\omega)$ is divisible by p^{n+1} , for all $s \in \mathbf{Z}_p$.

Let w be the number of roots of 1 in k . Define, for any $b, c \in \mathbf{Z}$, 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 $b' \in \mathbf{Z}$ and $b \equiv b'c \pmod{d}$;

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

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

$$0 \leq s_n(a) < p^{n+1}, \quad s_n(a) \equiv a \pmod{p^{n+1} \mathbf{Z}_p}.$$

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

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

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

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

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

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

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

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

$$(1) \quad (\chi(p^{n+1})(w/2))f(T; \chi\omega) \equiv \sum_{i=0}^{p^n-1} a_i(1+T)^i \pmod{\omega_n \mathcal{A}},$$

where

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

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 $\lambda_p(k) \geq p^n$. Then by [2] (see also [3], § 7) we have $f(T; \chi\omega) \equiv 0 \pmod{p\mathcal{A} + T^{p^n}\mathcal{A}}$. Since $\omega_n \in p\mathcal{A} + T^{p^n}\mathcal{A}$, it follows from (1) by a simple argument that p divides a_i . The ten fields k in question all have the property that

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

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

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

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

$$f(T; \chi\omega) \equiv 0 \pmod{\omega_n \mathcal{A}},$$

and consequently

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

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

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

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 $F \subseteq \mathbf{Q}_p$ is the number field generated over \mathbf{Q} by the values of the character ω . By fixing an embedding of F into the complex numbers \mathbf{C} , we may also view $\chi\omega$ as a character with values in \mathbf{C} ; then ([3], § 2) we have the equality of complex numbers:

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

where $L(2; \chi\omega)$ is the value at 2 of the usual (\mathbf{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 $|L_i|$ ($1 \leq i \leq [F:\mathbf{Q}]/2$) be the complex absolute values of F . From (3), we find

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

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

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

Let R be the ring of integers of F , and let $\mathfrak{p} = R \cap p\mathbf{Z}_p$, 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 $\lambda_p(k) \leq 1$ for all $p \leq 349$ (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	this	this
321 ₄	$f((r+1)n/m)$	$f([(r+1)n/m])$

Les volumes IV et suivants sont à obtenir chez
 Volumes from IV on are available at
 Die Bände IV und folgende sind zu beziehen durch
 Томы IV и следующие можно получить через

Ars Polona, Krakowskie Przedmieście 7, 00-068 Warszawa

Les volumes I–III sont à obtenir chez
 Volumes I–III are available at
 Die Bände I–III sind zu beziehen durch
 Томы I–III можно получить через

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

BOOKS PUBLISHED BY THE POLISH ACADEMY OF SCIENCES
 INSTITUTE OF MATHEMATICS

- S. Banach, *Oeuvres*, vol. I, 1967, 381 pp.
 S. Mazurkiewicz, *Travaux de topologie et ses applications*, 1969, 380 pp.
 W. Sierpiński, *Oeuvres choisies*, vol. I, 1974, 300 pp.; vol. II, 1975, 780 pp.; vol. III, 1976, 678 pp.
 S. Banach, *Oeuvres*, vol. II, in print.
 J. P. Schauder, *Oeuvres*, in print.

MONOGRAFIE MATEMATYCZNE

41. H. Rasiowa and R. Sikorski, *The mathematics of metamathematics*, 3rd ed., revised, 1970, 520 pp.
 43. J. Szarski, *Differential inequalities*, 2nd ed., 1967, 256 pp.
 44. K. Borsuk, *Theory of retracts*, 1967, 251 pp.
 45. K. Maurin, *Methods of Hilbert spaces*, 2nd ed., 1972, 570 pp.
 47. D. Przeworska-Rolewicz and S. Rolewicz, *Equations in linear spaces*, 1968, 380 pp.
 50. K. Borsuk, *Multidimensional analytic geometry*, 1969, 443 pp.
 51. R. Sikorski, *Advanced calculus. Functions of several variables*, 1969, 460 pp.
 52. W. Ślebodziński, *Exterior forms and their applications*, 1970, 427 pp.
 53. M. Krzyżański, *Partial differential equations of second order I*, 1971, 562 pp.
 54. M. Krzyżański, *Partial differential equations of second order II*, 1971, 407 pp.
 57. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 1974, 630 pp.
 58. C. Bessaga and A. Pełczyński, *Selected topics in infinite-dimensional topology*, 1975, 353 pp.
 59. K. Borsuk, *Theory of shape*, 1975, 379 pp.
 60. R. Engelking, *General topology*, 1977, 626 pp.

BANACH CENTER PUBLICATIONS

- Vol. 1. *Mathematical control theory*, 1976, 166 pp.
 Vol. 2. *Mathematical foundations of computer science*, 1977, 260 pp.
 Vol. 3. *Mathematical models and numerical methods*, in print.
 Vol. 4. *Approximation theory*, in print.
 Vol. 5. *Probability theory*, in print.