ACTA ARITHMETICA
XXI (1972)

On the μ-invariants of cyclotomic fields

by

KENKICHI IWASAWA (Princeton, N.J.)

Let p be an odd prime. For each $n \geqslant 0$, let k_n denote the cyclotomic field of p^{n+1}-th roots of unity and let p^{e_n}, $e_n \geqslant 0$, be the highest power of p which divides the class number of k_n. It is known (see [1]) that for all sufficiently large n, the exponent e_n is given by a formula

$$e_n = \lambda n + \mu p^n + \nu$$

where λ, μ, and ν are integers ($\lambda, \mu \geqslant 0$), independent of n. In the present paper, we shall prove that

$$\mu < p-1.$$

Let $\boldsymbol{Z}_p$ denote the ring of p-adic integers and let Λ be the ring of all formal power series in an indeterminate T with coefficients in $\boldsymbol{Z}_p$: $\Lambda = \boldsymbol{Z}_p[[T]]$. We shall first prove a lemma on Λ-modules [1].

A Λ-module Y is called *elementary* if Y is the direct sum of a finite number of Λ-modules of the form Λ/P^m, $m \geqslant 0$, where P are prime ideals of height 1 in Λ. Let X be a noetherian torsion Λ-module. Then there exist an elementary Λ-module Y and a morphism

$$f\colon X \to Y$$

such that both the kernel and the cokernel of f are finite modules. Let

$$Y = \sum_i \Lambda/P_i^{m_i}$$

be the direct decomposition for Y and let

$$\mu = \sum{}' m_i,$$

where the sum is taken over all indices i such that $P_i = p\Lambda$. The integer μ is then uniquely determined for X by the above and hence is denoted by $\mu(X)$.

[1] For the theory of Λ-modules, see [3].

LEMMA. *Let X be a noetherian torsion Λ-module with $\mu = \mu(X)$. Then the order of X/TX is at least equal to p^μ.*

Proof. Let $f\colon X \to Y$ be as above and let $Z = f(X)$, the image of f. It is clear that the order of X/TX is not less than the order of Z/TZ.

Now, if Y/TY is infinite, then so is X/TX and the lemma holds trivially. Hence we may assume that Y/TY is finite. In such a case, we see easily that $P_i \neq T\Lambda$ for every index i in the direct decomposition of Y so that the map

$$Y \to Y,$$
$$y \to Ty$$

is injective and that

$$Y/Z \simeq TY/TZ.$$

Since Y/Z and Y/TY are both finite, it follows that the order of Z/TZ is equal to that of Y/TY. Therefore it is sufficient to show that the order of Y/TY is at least equal to p^μ. However, this is an immediate consequence of the fact that if $U = \Lambda/p^m\Lambda$, $m \geqslant 0$, then the order of U/TU is equal to p^m.

Now, let $k = k_0$ and let K denote the union of all k_n, $n \geqslant 0$. K is a Galois extension of k and its Galois group is isomorphic to the additive group of the compact ring $\boldsymbol{Z}_p$. Let L be the maximal unramified abelian p-extension over K and let X be the Galois group of L/K. Since L/k is also a Galois extension, Γ acts on the abelian group X in the obvious manner. Fixing a topological generator γ of the compact group Γ, we can then make X into a Λ-module module so that $(1+T)x = \gamma x$ for every x in X. Furthermore, we can show (cf. [1] and [3]) that X is a noetherian torsion Λ-module and its invariant $\mu(X)$ is equal to the second coefficient μ in the formula for e_n mentioned above: $\mu = \mu(X)$.

Let J denote the automorphism of L which maps each α in L to its complex-conjugate $\bar{\alpha}$. Clearly J also acts on X. Let X^+ (resp. X^-) be the set of all x in X such that $Jx = x$ (resp. $Jx = -x$). Then X^+ and X^- are Λ-submodules of X and

$$X = X^+ \oplus X^-.$$

Hence we have

$$\mu = \mu(X) = \mu^+ + \mu^-$$

where $\mu^+ = \mu(X^+)$ and $\mu^- = \mu(X^-)$. It is also known (cf. [2]) that

$$\mu^+ \leqslant \mu^-.$$

Therefore

$$\mu \leqslant 2\mu^-.$$

Let h^- denote the so-called first factor of the class number of k, the cyclotomic field of pth roots of unity. It is proved (see [1] and [2]) that the order of X^-/TX^- is just equal to the highest power of p which divides h^-. Hence, applying the above lemma for X^-, we see that

$$p^{\mu^-} \leqslant h^-.$$

On the other hand, the classical class number formula for k states that

$$h^- = 2p \prod_{\chi} \left(-\frac{1}{2p} \sum_{a=1}^{p-1} a\chi(a) \right),$$

where the product is taken over all Dirichlet characters χ defined $\bmod p$ with $\chi(-1) = -1$. Since

$$\Big| \sum_{a=1}^{p-1} a\chi(a) \Big| < \sum_{a=1}^{p-1} a = \frac{(p-1)p}{2},$$

we have

$$h^- < 2^{2-p} p (p-1)^{(p-1)/2} \leqslant p^{(p-1)/2}.$$

It then follows that

$$\mu^- < (p-1)/2$$

so that

$$\mu < p-1,$$

q.e.d.

Instead of the above elementary argument, we may estimate h^- also by using

$$|L(1;\chi)| < 2\log p, \quad \chi \neq 1.$$

We then see that for any given real number $c > \frac{1}{2}$, there exists an integer $N(c)$ such that

$$\mu < c(p-1)$$

whenever $p \geqslant N(c)$. It is also clear that by the same method, we can find an upper bound for the μ-invariant of a so-called $\boldsymbol{Z}_p$-extension K/k in many special cases. In particular, if K has only one prime divisor which divides the rational prime p (as in the special case discussed above), then

$$\mu(K/k) \leqslant \log h/\log p,$$

where h is the class number of k.

References

[1] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. 65 (1959), pp. 183–226.
[2] — *On the theory of cyclotomic fields*, Ann. of Math. 70 (1959), pp. 530–561.
[3] J.-P. Serre, *Classes des corps cyclotomiques*, Seminaire Bourbaki, Exposé 174 (1958/1959).

PRINCETON UNIVERSITY

Received on 21. 2. 1971 (147)

ACTA ARITHMETICA
XXI (1972)

О числе решений одного сравнения

Г. И. Перельмутер (Саратов), А. Г. Постников (Москва)

Памяти В. Серпинского

Пусть $n \geqslant 1$, $m_1, \ldots, m_n$ — целые положительные числа

(1) $$F(x, x_1, \ldots, x_n) = f_0(x) + f_1(x)x_1^{m_1} + \ldots + f_n(x)x_n^{m_n},$$

где $f_0, f_1, \ldots, f_n$ — полиномы от неизвестного x с целыми коэффициентами. Мы будем изучать число $N_F(p)$ решений сравнения

(2) $$F(x, x_1, \ldots, x_n) \equiv 0 \pmod p$$

при растущем простом p. Случай, когда все $f_j = \mathrm{const}$, рассматривался А. Вейлем в работе [3].

Для формулировки результата введем некоторые обозначения:

δ_j — Н. О. Д. канонических показателей при разложении полинома $f_j(x)$ на множители над полем рациональных чисел $(0 \leqslant j \leqslant n)$, причем полагаем $\delta_j = 0$, если $f_j = \mathrm{const}$;

допустимая система $a = (a_1, \ldots, a_n)$ — это система рациональных чисел $a_1, \ldots, a_n$, удовлетворяющих условиям:

(3) $$0 < a_j < 1, \quad m_j a_j \equiv 0 \pmod 1, \quad \sum_{j=1}^{n} a_j \not\equiv 0 \pmod 1;$$

$$r_a = \Big(a_1\delta_1, \ldots, a_n\delta_n, \delta_0 \sum_{j=1}^{n} a_j\Big), \text{ т.е.}$$

(4) $$r_a = \prod_q q^{\gamma_q(r_a)}, \quad \text{где} \quad \gamma_q(r_a) = \mathrm{Min}\Big\{\gamma_q(a_1\delta_1), \ldots, \gamma_q(a_n\delta_n), \gamma_q\Big(\delta_0 \sum_j a_j\Big)\Big\}.$$

Будет доказана

Теорема. *Предположим, что выполнены условия:*

1) *Полиномы $f_0(x), \ldots, f_n(x)$ попарно взаимно просты;*

2) *Для всех допустимых систем a (если они существуют)*

(5) $$r_a \not\equiv 0 \pmod 1.$$