Токуо J. Матн. Vol. 28, No. 1, 2005

# On a Higher Class Number Formula of Z<sub>p</sub>-Extensions

# Satoshi FUJII

Waseda University

(Communicated by Y. Yamada)

## 1. Introduction

Let p be a prime number and k a number field of finite degree over  $\mathbf{Q}$ , the rational number field. Let  $\mathbf{Z}_p$  be the additive group of p-adic integers, and K/k a  $\mathbf{Z}_p$ -extension over k. For an integer  $n \ge 0$ , we denote by  $k_n$  the n-th layer of the extension K/k, namely  $k_n$  is the unique intermediate field of K/k such that  $[k_n : k] = p^n$ . Recently, Ozaki studied the maximal unramified pro-p extensions  $\tilde{L}$  of K and  $\tilde{L}_n$  of  $k_n$  as in what follows. Let  $\tilde{G} = \text{Gal}(\tilde{L}/K)$ and  $\tilde{G}_n = \text{Gal}(\tilde{L}_n/k_n)$  for all non-negative n. We define the subgroups  $C_i(\tilde{G})$  of  $\tilde{G}$  by the descending central series

$$\tilde{G} = C_1(\tilde{G}) \supseteq C_2(\tilde{G}) \supseteq \cdots \supseteq C_i(\tilde{G}) \supseteq \cdots, \ C_{i+1}(\tilde{G}) = \overline{[C_i(\tilde{G}), \tilde{G}]}.$$

Then we consider the modules  $X^{(i)} = C_i(\tilde{G})/C_{i+1}(\tilde{G})$ , and call  $X^{(i)}$  the *i*-th Iwasawa module. We define the subgroups  $C_i(\tilde{G}_n) \subseteq \tilde{G}_n$  and the modules  $X_n^{(i)}$  similar to  $C_i(\tilde{G})$  and  $X^{(i)}$ , respectively. Note that  $X_n^{(1)}$  is isomorphic to the Sylow *p*-subgroup of the ideal class group  $A_{k_n}$  of  $k_n$  and that  $X^{(1)}$  is the Iwasawa module  $X_K$  of K/k which is defined as the projective limit  $\lim_{k \to \infty} A_{k_n}$  with respect to the norm maps. By definition, the complete group ring  $\Lambda_{K/k} = \mathbb{Z}_p[[\mathrm{Gal}(K/k)]]$  acts on  $X^{(i)}$  in the natural way, namely  $\mathrm{Gal}(K/k)$  acts via the inner automorphism. For i = 1, Iwasawa studied the  $\Lambda_{K/k}$ -module structure of  $X_K$  and deduced the following celebrated formula:

THEOREM A. There exist non-negative integers  $\lambda(K/k)$ ,  $\mu(K/k)$  and an integer  $\nu(K/k)$  such that

$$#A_{k_n} = p^{\lambda(K/k)n + \mu(K/k)p^n + \nu(K/k)}$$

for all sufficiently large n.

Received September 12, 2003; revised April 28, 2004 2000 Mathematics Subject Classification. Primary 11R23, 11R29. Key words and phrases. Iwasawa's class number formula, higher Iwasawa modules.

### SATOSHI FUJII

These integers  $\lambda(K/k)$ ,  $\mu(K/k)$  and  $\nu(K/k)$  are called the Iwasawa invariants of K/k. We remark that  $\lambda(K/k)$  and  $\mu(K/k)$  are the invariants of the  $\Lambda_{K/k}$ -module  $X_K$ . If  $\mu(K/k) = 0$ , then  $X_K$  is a finitely generated  $\mathbb{Z}_p$ -module with rank $\mathbb{Z}_p X_K = \lambda(K/k)$ , and  $X^{(i)}$  is also a finitely generated  $\mathbb{Z}_p$ -module. When  $\mu(K/k) = 0$ , we define the *i*-th  $\lambda$ -invariant of K/k by  $\lambda^{(i)}(K/k) = \operatorname{rank}_{\mathbb{Z}_p} X^{(i)}$ . Now we raise the following question on the higher Iwasawa modules  $X^{(i)}$ :

QUESTION. Suppose  $\mu(K/k) = 0$ . Then, for each  $i \ge 2$ , does there exist an integer  $\nu^{(i)}(K/k)$  such that  $\#X_n^{(i)} = p^{\lambda^{(i)}(K/k)n + \nu^{(i)}(K/k)}$  for all sufficiently large n?

Ozaki found infinitely many fields where the above question is affirmatively answered for i = 2, 3.

THEOREM B. Let p be an odd prime number and K/k the cyclotomic  $\mathbb{Z}_p$ -extension over a CM-field k with the maximal real subfield  $k^+$ . Assume that the following conditions are satisfied:

(1) the Iwasawa  $\mu$ -invariant of K/k is 0,

(2) the class number of  $k^+$  is prime to p,

(3) there is a unique prime of  $k^+$  lying over p.

Then there is an integer  $\nu^{(i)}(K/k)(i = 2, 3)$  such that  $\#X_n^{(i)} = p^{\lambda^{(i)}(K/k)n + \nu^{(i)}(K/k)}$  for all sufficiently large *n*.

For example, all imaginary quadratic fields satisfy the assumptions of Theorem B. In this paper, we will prove an asymptotic formula of  $\#X_n^{(2)}$  in terms of  $p^{\lambda^{(2)}(K/k)n}$ , namely;

THEOREM. Suppose that  $\mu(K/k) = 0$  and p does not split in  $K/\mathbb{Q}$ . Then  $\#X_n^{(2)} = p^{\lambda^{(2)}(K/k)n+O(1)}$ .

#### 2. Lemmas

To prove this Theorem, we use the following lemmas. For a number field F, let  $E_F$  be the unit group of F. Denote by  $A_F$  the Sylow p-subgroup of the ideal class group of F. Let L be a finite Galois extension of F and Gal(L/F) its Galois group. Then we denote by  $H_i(L/F, M)$  the *i*-th homology group of a Gal(L/F)-module M for a non-negative integer i. We regard the additive group of p-adic integers  $\mathbb{Z}_p$  as a Gal(L/F)-module with trivial action. We denote by  $M^{\text{Gal}(L/F)}$  and  $M_{\text{Gal}(L/F)}$  the Gal(L/F)-invariant submodule and the Gal(L/F)-co-invariant module of M, respectively. For a  $\mathbb{Z}_p$ -module N, let  $\text{Tor}_{\mathbb{Z}_p}N$  be the maximal  $\mathbb{Z}_p$ -torsion submodule of N and put  $N[p] = \{x \in N | px = 0\}$ .

LEMMA 2.1. Let F be a number field of finite degree and L/F an unramified finite p-extension of finite degree such that L contains the Hilbert p-class field of F and let G = Gal(L/F) (p-extension means a Galois extension with p-power degree). Put

 $\mathcal{H}_{L/F} = E_F/E_F \cap N_{L/F}L^{\times}$ . Then we have the exact sequence

$$0 \longrightarrow \mathcal{H}_{L/F} \longrightarrow H_2(L/F, \mathbf{Z}_p) \longrightarrow (A_L)_G \longrightarrow 0.$$

Furthermore, for any subfield k of F such that L/k and F/k are Galois extensions, the above sequence is exact as Gal(F/k)-modules.

PROOF. This lemma is well known as the central class field theory. For example, see Fröhlich [1].  $\hfill \Box$ 

Let  $L_n = L_n^{(1)} = \tilde{L}_n^{C_2(\tilde{G}_n)}$  and  $L_n^{(2)} = \tilde{L}_n^{C_3(\tilde{G}_n)}$ . Then  $L_n$  is the Hilbert *p*-class field of  $k_n$ and  $L_n^{(2)}$  is the central *p*-class field of  $L_n/k_n$ , respectively. It follows from the definition of  $X_n^{(2)}$  that  $X_n^{(2)} = \text{Gal}(L_n^{(2)}/L_n) \simeq (A_{L_n})_{\text{Gal}(L_n/k_n)}$ . Since  $L_n/k_n$  is an abelian extension, we have  $H_2(L_n/k_n, \mathbb{Z}_p) \simeq A_{k_n} \wedge A_{k_n}$ , where  $\wedge$  means the exterior product. For  $m \ge n \ge 0$ , let  $N'_{m,n} : A_{k_m} \wedge A_{k_m} \to A_{k_n} \wedge A_{k_n}$  be the homomorphisms induced by the norm maps. Note that the diagram

$$\begin{array}{cccc} H_2(L_m/k_m, \mathbf{Z}_p) & \stackrel{\sim}{\longrightarrow} & A_{k_m} \wedge A_{k_m} \\ & & & \\ d_{m,n} \downarrow & & & N'_{m,n} \downarrow \\ H_2(L_n/k_n, \mathbf{Z}_p) & \stackrel{\sim}{\longrightarrow} & A_{k_n} \wedge A_{k_n} \end{array}$$

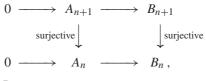
is commutative for  $m \ge n \ge 0$ . Here, we denote by  $d_{m,n}$  the map induced by the restriction map  $\text{Gal}(L_m/k_m) \to \text{Gal}(L_n/k_n)$  ( $\sigma \mapsto \sigma|_{L_n}$ ). By Lemma 2.1, we have the following:

LEMMA 2.2. The following diagram is exact and commutative as  $\Gamma$ -modules for  $m \ge n \ge 0$ :

The action of  $\sigma \in \Gamma$  on  $A_{k_n} \wedge A_{k_n}$  is given by  $\sigma(x \wedge y) = (\sigma x) \wedge (\sigma y)$  for  $x, y \in A_{k_n}$ .

The next lemma tells us that the knowledge of  $A_{k_n} \wedge A_{k_n}$  gives information about  $\mathcal{H}_{L_n/k_n}$ and  $X_n^{(2)}$ .

LEMMA 2.3. Let  $\{A_n\}$  and  $\{B_n\}$   $(n \ge 0)$  denote projective systems of finite abelian *p*-groups with the following exact commutative diagram:



and let  $A = \lim_{n \to \infty} A_n$ ,  $B = \lim_{n \to \infty} B_n$ .

#### SATOSHI FUJII

(1) Suppose that B is a finitely generated  $\mathbb{Z}_p$ -module. Then  $\mathfrak{B} = \operatorname{Tor}_{\mathbb{Z}_p} B$  is isomorphic to a subgroup of  $B_n$  for all sufficiently large n.

(2) Suppose that B is a finitely generated  $\mathbb{Z}_p$ -module and

$$\operatorname{Ker}(B_{n+1}/\mathfrak{B} \to B_n/\mathfrak{B}) = (B_{n+1}/\mathfrak{B})[p]$$

for all sufficiently large n. Then there exist integers a and b such that

$$#A_n = p^{\lambda(A)n+a},$$
$$#B_n = p^{\lambda(B)n+b}$$

for all sufficiently large n. Here we denote by  $\lambda(M)$  the  $\mathbb{Z}_p$ -rank of a finitely generated  $\mathbb{Z}_p$ -module M.

PROOF. (1) Let  $\mathfrak{b}_n = \operatorname{Ker}(B \to B_n)$ . Then  $\{\mathfrak{b}_n\}$  is a system of fundamental neighborhoods of *B*. Since  $\mathfrak{B}$  is finite, there is  $n_0$  such that  $\mathfrak{b}_n \cap \mathfrak{B} = 0$  for  $n \ge n_0$ . It follows from the finiteness of  $B_n$  that  $\mathfrak{b}_n$  is a free  $\mathbb{Z}_p$ -module of rank  $\lambda(B)$  for all sufficiently large *n*. From the freeness of  $\mathfrak{b}_n$ , we see that  $\mathfrak{B}$  maps to  $B_n$  injectively and  $B_n$  is a product of the image of  $\mathfrak{B}$  and some subgroup of  $B_n$ .

(2) Let  $B' = B/\mathfrak{B}$ . By (1), we have

$$0 \longrightarrow \mathfrak{b}_n \longrightarrow B' \longrightarrow B_n/\mathfrak{B} \longrightarrow 0 \quad (\text{exact}) \,,$$

and  $\dim_{F_p}(B_n/\mathfrak{B})/p(B_n/\mathfrak{B}) = \lambda(B)$  for all sufficiently large *n*, where  $F_p$  is the finite field of *p* elements. By the commutative diagram

and the snake lemma, we have  $\operatorname{Ker}(B_{n+1}/\mathfrak{B} \to B_n/\mathfrak{B}) = (B_{n+1}/\mathfrak{B})[p] \simeq \mathfrak{b}_n/\mathfrak{b}_{n+1}$ . It follows from  $(B_{n+1}/\mathfrak{B})[p] \simeq (B_{n+1}/\mathfrak{B})/p(B_{n+1}/\mathfrak{B}) \simeq F_p^{\oplus \lambda(B)}$  that  $\mathfrak{b}_{n+1} = p\mathfrak{b}_n$ .

Fix an integer  $n_0 \ge 0$  such that  $\mathfrak{b}_n \cap \mathfrak{B} = 0$  and  $\mathfrak{b}_{n+1} = p\mathfrak{b}_n$  for all  $n \ge n_0$ . Let  $\#(B_{n_0}/\mathfrak{B}) = p^{\lambda(B)n_0+b'}$  for an integer b'. Since  $\#\operatorname{Ker}(B_{n+1}/\mathfrak{B} \to B_n/\mathfrak{B}) = \#(B_{n+1}/\mathfrak{B})[p] = p^{\lambda(B)}$ , we have  $\#(B_n/\mathfrak{B}) = p^{\lambda(B)n+b'}$  if  $n \ge n_0$ . Then  $\#B_n = \#(B_n/\mathfrak{B})\#\mathfrak{B} = p^{\lambda(B)n+b'}\#\mathfrak{B}$ . Let  $p^b = p^{b'}\#\mathfrak{B}$ . Then  $\#B_n = p^{\lambda(B)n+b}$  for all sufficiently large n.

Let  $\mathfrak{a}_n = \operatorname{Ker}(A \to A_n)$  and  $\mathfrak{A} = \operatorname{Tor}_{\mathbb{Z}_p} A$ . Since  $A \subseteq B$  we have  $\mathfrak{A} = A \cap \mathfrak{B}$ . It follows from the exact commutative diagram

that  $\operatorname{Ker}(A_{n+1}/\mathfrak{A} \to A_n/\mathfrak{A}) = (A_{n+1}/\mathfrak{A})[p]$ . Then  $\mathfrak{a}_{n+1} = p\mathfrak{a}_n$  for all sufficiently large *n*. The remaining part is proved as in the case of  $B_n$ .

LEMMA 2.4. Let K/k be a  $\mathbb{Z}_p$ -extension with a number field k. Assume that the Iwasawa  $\mu$ -invariant of K/k is 0. Then we have the following commutative diagram for all sufficiently large n:

where  $a_1, \dots, a_{\lambda(K/k)}$  are integers independent of *n* and satisfy the inequalities  $a_1 \leq a_2 \leq \dots \leq a_{\lambda(K/k)}$ .

PROOF. For the proof of this lemma, see Grandet–Jaulent [2].

The following is keystone of the proof of main theorem.

LEMMA 2.5. Let K/k be a  $\mathbb{Z}_p$ -extension, and let  $\Gamma_n = \operatorname{Gal}(K/k_n)$ . For  $m \ge n \ge 0$ , let  $B_m^{(n)} = \{c \in A_{k_m} | \exists \mathfrak{a} \in c \text{ s.t. } \sigma \mathfrak{a} = \mathfrak{a} \text{ for all } \sigma \in \Gamma_n\} \subseteq A_{k_m}^{\Gamma_n}$ . If p is not decomposed in  $K/\mathbb{Q}$ , then  $A_{k_m}^{\Gamma_n}/B_m^{(n)} \simeq \hat{H}^0(k_m/k_n, E_{k_m})$ .

PROOF. For the proof of this lemma, see Theorem 1 of Greenberg [3].  $\Box$ 

Here, we give a sketch of the proof of Theorem B for the case i = 2. By Lemma 2.4, we have

$$A_{k_n} \wedge A_{k_n} \simeq \left( \bigoplus_{1 \le i \le \lambda(K/k)} (\mathbf{Z}/p^{a_i+n}\mathbf{Z})^{\oplus(\lambda(K/k)-i)} \right) \oplus D$$

for some finite abelian *p*-group *D* independent of *n*. Now we prove the surjectivity of the norm map  $N_{m,n} : E_{k_m} \to E_{k_n}$ , which is equivalent to  $\hat{H}^0(k_m/k_n, E_{k_m}) = E_{k_n}/N_{m,n}E_m = 0$ . Since *k* is a CM-field and *K/k* is the cyclotomic  $\mathbb{Z}_p$ -extension,  $k_n$  is also a CM-field with the maximal real subfield  $k_n^+$ . Because the unit index of  $k_n/k_n^+$  is 1 or 2 and *p* is odd, we have  $\hat{H}^0(k_m/k_n, E_{k_m}) = \hat{H}^0(k_m^+/k_n^+, E_{k_m^+})$ . By the assumptions (2), (3) and Iwasawa's theorem (Iwasawa [4]), the class number of  $k_n^+$  is prime to *p* for  $n \ge 0$ . Therefore,  $\hat{H}^0(k_m^+/k_n^+, E_{k_m^+}) =$ 0 for  $m \ge n \ge 0$  by Lemma 2.5. Applying Lemma 2.3 to  $\mathcal{H}_{L_n/k_n}$  and  $A_{k_n} \land A_{k_n}$ , we see that there is an integer  $\nu^{(2)}(K/k)$  such that  $\#X_n^{(2)} = p^{\lambda^{(2)}(K/k)n+\nu^{(2)}(K/k)}$  for all sufficiently large *n*. The proof of the case i = 3 is much more difficult.

Let  $D_n$  be the subgroup of  $A_{k_n}$  generated by the classes each of which contains a prime above p. We put  $A'_{k_n} = A_{k_n}/D_n$  and define  $A'_{k_n} \to A'_{k_m}$  as the homomorphism induced by the natural inclusion  $k_n \to k_m$ .

### SATOSHI FUJII

LEMMA 2.6. The order of the kernel of the homomorphism  $A'_{k_n} \to A'_{k_m}$  is bounded for  $m \ge n \ge 0$ .

PROOF. For the proof of this lemma, see Iwasawa [5].

# 3. Proof of Theorem

Let  $\mathcal{H} = \varprojlim \mathcal{H}_{L_n/k_n}$ , where the projective limit is taken with respect to the norm maps, and  $\mathcal{I}_n = \operatorname{Im}(\mathcal{H} \to \mathcal{H}_{L_n/k_n})$  the image of the projection map. Applying Lemma 2.3 to  $\mathcal{I}_n$  and  $A_{k_n} \wedge A_{k_n}$ , we see that there exist integers *a* and *b* such that  $\#A_{k_n} \wedge A_{k_n} = p^{\lambda(X_K \wedge X_K)n+a}$ and  $\#\mathcal{I}_n = p^{\lambda(\mathcal{H})n+b}$  for all sufficiently large *n*. By Lemma 2.2, we have

$${}^{k}X_{n}^{(2)} = {}^{\#}A_{k_{n}} \wedge A_{k_{n}}/{}^{\#}\mathcal{H}_{L_{n}/k_{n}}$$
  
=  $p^{\lambda^{(2)}(K/k)n + (a-b)}/[\mathcal{H}_{L_{n}/k_{n}}:\mathcal{I}_{n}].$ 

Hence, we have to prove that  $[\mathcal{H}_{L_n/k_n} : \mathcal{I}_n]$  is bounded for  $n \ge 0$ . We can easily see that  $\mathcal{I}_n = \bigcap_{m \ge n} N_{k_m/k_n} \mathcal{H}_{L_m/k_m}$ . Therefore, if  $\#\hat{H}^0(k_m/k_n, E_{k_m})$  is bounded for  $m \ge n \ge 0$ , then  $[\mathcal{H}_{L_n/k_n} : \mathcal{I}_n]$  is bounded for n according to the following commutative diagram:

$$\begin{array}{cccc} E_{k_m} & \longrightarrow & \mathcal{H}_{L_m/k_m} \\ \text{norm} & & & & & \\ & & & & & \\ E_{k_n} & \longrightarrow & \mathcal{H}_{L_n/k_n} \, . \end{array}$$

Therefore, we have only to prove that  $#\hat{H}^0(k_m/k_n, E_{k_m})$  is bounded for  $m \ge n \ge 0$ . Let  $n_0 \ge 0$  be the integer such that  $k_{n_0}$  is the maximal unramified subextension of K/k. We deal with two cases separately.

Case 1.  $n < n_0 \le m$ .

By our assumption that p is not decomposed in  $K/\mathbf{Q}$  and Lemma 2.5, we have

‡

$$\hat{H}^{0}(k_{m}/k_{n}, E_{k_{m}}) = \#A_{k_{m}}^{\Gamma_{n}}/\#B_{m}^{(n)}$$

$$\leq \#A_{k_{m}}^{\Gamma_{n}}$$

$$\leq \#A_{k_{m}}^{\Gamma_{n_{0}}}$$

$$= \#A_{k_{n_{0}}}.$$

Hence the boundedness holds.

Case 2.  $n_0 \leq n$ .

Let  $\mathfrak{p}_n$  be the unique prime of  $k_n$  above p. Since  $\mathfrak{p}_n$  is  $\Gamma$ -invariant and  $\#A_{k_n}^{\Gamma} \leq \#A_{k_n}^{\Gamma_{n_0}} =$  $\#A_{k_{n_0}}$ , we see that  $D_n \subseteq A_{k_n}^{\Gamma}$  and the order of  $D_n$  is bounded. Then there is a constant  $C_1 > 0$ such that  $\#A_{k_n}/\#A'_{k_n} = \#D_n \leq C_1$  for all  $n \geq 0$ . Now we consider the homomorphism  $A'_{k_n} \to A'_{k_m}$  induced by the natural inclusion  $k_n \to k_m$ . Clearly the image of the above map

is contained in  $B_m^{(n)}/D_m$ . Conversely, let  $c \mod D_m$  be an element of  $B_m^{(n)}/D_m$ . Then there is an ideal  $\mathfrak{a} \in c$  of  $k_m$  such that  $\sigma \mathfrak{a} = \mathfrak{a}$  for all  $\sigma \in \Gamma_n$ . Since every  $\Gamma_n$ -invariant ideal of  $k_m$ is a product of a power of the prime above p and an ideal of  $k_n$ , we may assume that the class c contains an ideal of  $k_n$ . Therefore Im $(A'_{k_n} \to A'_{k_m}) = B_m^{(n)}/D_m$ . By Lemma 2.6, there is a constant  $C_2 > 0$  such that  $\#A'_{k_n} \#D_m/\#B_m^{(n)} \le C_2$ . Hence we have

$$\begin{split} #\hat{H}^{0}(k_{m}/k_{n}, E_{k_{m}}) &= #A_{k_{m}}^{\Gamma_{n}}/#B_{m}^{(n)} \\ &\leq \frac{#A_{k_{n}}C_{2}}{#A'_{k_{n}}#D_{m}} \\ &\leq C_{1}C_{2}/#D_{m} \\ &\leq C_{1}C_{2} \,, \end{split}$$

because  $n \ge n_0$ . This completes the proof of Theorem.

ACKNOWLEDGEMENT. I would like to express my thanks to Prof. Manabu Ozaki for his valuable advice in this paper.

**Note added in proof.** After the author submitted, M. Ozaki showed that the Question of this paper is affirmatively answered for each  $i \ge 1$ . See his preprint: Non-abelian Iwasawa Theory of  $\mathbb{Z}_p$ -extensions. His article will be to appear to a journal.

### References

- A. FRÖHLICH, Central extensions, Galois groups, and ideal class groups of number fields, Contemporary Mathematics 24 (1983), American Mathematical Society.
- [2] M. GRANDET and J-F. JAULENT, Sur la capitulation dans une  $\mathbb{Z}_{\ell}$ -extension, J. Reine Angew. Math. 362 (1985), 213–217.
- [3] R. GREENBERG, On the Iwasawa invariants of totally real number fields, Amer. J. Math. 98 (1976), 263–284.
- [4] K. IWASAWA, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257–258.
- [5] K. IWASAWA, On  $\mathbb{Z}_{\ell}$ -extensions of algebraic number fields, Ann. Math. 98 (1973), 246–326.
- [6] M. OZAKI, Non-abelian Iwasawa theory of  $\mathbb{Z}_p$ -extensions, preprint.

Present Address: DEPARTMENT OF MATHEMATICAL SCIENCE, SCHOOL OF SCIENCE AND ENGINEERING, WASEDA UNIVERSITY, OKUBO, SHINJUKU-KU, TOKYO, 169–8555 JAPAN. *e-mail:* fujii@ruri.waseda.jp