Comm. Korean Math. Soc. **16** (2001), No. 4, pp. 595–606

DETERMINATION OF CLASS NUMBERS OF THE SIMPLEST CUBIC FIELDS

JUNG SOO KIM

ABSTRACT. Using p-adic class number formula, we derive a congruence relation for class numbers of the simplest cubic fields which can be considered as a cubic analogue of Ankeny-Artin-Chowla's theorem. Furthermore, we give an elementary proof for an upper bound for the class numbers of the simplest cubic fields.

1. The simplest cubic fields

The motivation of this paper is to find a cubic analogue of the *Ankeny-Artin-Chowla Theorem* (cf. [1]) for the simplest cubic fields. In this section, we shall introduce the notion of the simplest cubic fields and develop basic materials which will be used later. Let m be a nonnegative integer such that m^2+3m+9 is a prime. Consider the following polynomial

$$f(X) = X^3 + mX^2 - (m+3)X + 1,$$

which is irreducible over $\mathbb{Q}$. Let ρ be the negative root of $f(X)$. Then $\rho' = \dfrac{1}{1-\rho}$ and $\rho'' = 1 - \dfrac{1}{\rho}$ are the other roots of $f(X)$, therefore $K = \mathbb{Q}(\rho)$ is a totally real cyclic cubic field. K is called the simplest cubic field and the arithmetic of these fields were studied in [3], [6]. Note that

$$-m-2 < \rho < -m-1 < 0 < \rho' < 1 < \rho'' < 2.$$

Let $p = m^2+3m+9$. Then we can easily check that $p \equiv 1 \pmod 6$. In [6], Washington showed that the discriminant of K is p^2 and $\{-1, \rho, \rho'\}$ generates the full group of units of K. Since $K/\mathbb{Q}$ is a cyclic cubic extension, its associated character group Y is generated by a cubic character χ, i.e., $Y = \{1, \chi, \bar{\chi}\}$. By the Conductor-Discriminant formula(cf. [5]),

Received March 6, 2001. Revised July 28, 2001.
2000 Mathematics Subject Classification: 11R16, 11R29.
Key words and phrases: simplest cubic field, class number.
The present work was supported by Com^{2}MaC.

$f_\chi = f_{\bar{\chi}} = p$, so $K \subset \mathbb{Q}(\zeta_p)$ by *Kronecker-Weber Theorem.* Here ζ_p (or simply ζ) denote a primitive p-th root of unity. Let X denote the Dirichlet character group associated to $\mathbb{Q}(\zeta)$ and ω be a generator of X satisfying $\omega^{(p-1)/3} = \chi$. Let $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $R = Gal(\mathbb{Q}(\zeta)/K)$. If we identify G with $(\mathbb{Z}/p\mathbb{Z})^*$, then R becomes a subgroup of G consisting of cubic residues modulo p. Consider the pairing

$$\begin{aligned} Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \times X &\longrightarrow \mathbb{C} \\ (\sigma, \psi) &\longrightarrow \psi(\sigma). \end{aligned}$$

It is well known (cf. [5]) that there is a one-to-one correspondence between subgroups of X and subfields of $\mathbb{Q}(\zeta)$. Under this paring, Y corresponds to the fixed field of $Y^\perp(= R)$, i.e., the field generated by $\sum_{r\in R} \zeta^r$. Obviously, this field should be K. Therefore we have a correspondence as in the following diagram:

$$\begin{array}{ccccc} \text{Number field} & & \text{Galois group} & & \text{Dirichlet character group} \\ \\ \mathbb{Q}(\zeta) & \longleftrightarrow & 1 & \longleftrightarrow & X \\ | & & | & & | \\ K & \longleftrightarrow & R & \longleftrightarrow & Y \\ | & & | & & | \\ \mathbb{Q} & \longleftrightarrow & G & \longleftrightarrow & 1 \end{array}$$

So far we have showed that K equals the field generated by $\sum_{r\in R} \zeta^r$ from the above diagram. Now we shall derive this result from computational point of view. Let S and $T(\neq R)$ be cosets of R in $(\mathbb{Z}/p\mathbb{Z})^*$. For example, if we take any $\delta \in (\mathbb{Z}/p\mathbb{Z})^*$ which is not a cubic residue modulo p, then we may take $S = \delta R$ and $T = \delta^2 R$. Let α, β, γ be given by $\alpha = \sum_{r\in R} \zeta^r$, $\beta = \sum_{s\in S} \zeta^s$, $\gamma = \sum_{t\in T} \zeta^t$. By a theorem of Gauss (cf. [4], pp. 111-120), $3\alpha + 1$, $3\beta + 1$, $3\gamma + 1$ are the roots of

$$X^3 = 3pX + pA,$$

where A is uniquely determined by the conditions

$$4p = A^2 + 27B^2, \quad A \equiv 1 (\text{mod } 3).$$

On the other hand, $3\rho + m$, $3\rho' + m$, $3\rho'' + m$ are the roots of

$$X^3 = 3pX - (2m + 3)p.$$

Note that $4p = (2m + 3)^2 + 27$. From the uniqueness of A, it follows that

$$A = \begin{cases} 2m + 3 & \text{if } \ m \equiv -1 \pmod 3, \\ -(2m + 3) & \text{if } \ m \equiv 1 \pmod 3. \end{cases}$$

This implies that

$$\rho = \begin{cases} \min[\alpha,\beta,\gamma] - \dfrac{m-1}{3} & \text{if} \quad m \equiv 1 \pmod 3, \\ \text{-}\max[\alpha,\beta,\gamma] - \dfrac{m+1}{3} & \text{if} \quad m \equiv -1 \pmod 3. \end{cases}$$

For the computation in the next section, we need to fix a prime in K which lies over p. Let $\pi = \prod_{r\in R}(1-\zeta^r)$, $\pi' = \prod_{s\in S}(1-\zeta^s)$, and $\pi'' = \prod_{t\in T}(1-\zeta^t)$.

Then $p = \pi\pi'\pi'' = \pi^3\dfrac{\pi'}{\pi}\dfrac{\pi''}{\pi}$ and $\dfrac{\pi'}{\pi}, \dfrac{\pi''}{\pi}$ are units in K. Thus p is totally ramified in $K/\mathbb{Q}$ and π is a prime of K above p. As a conclusion of this section, we summarize our computation in the following proposition.

PROPOSITION 1.1. *Let m (≥ 0) be an integer such that $p = m^2 + 3m + 9$ is a prime. Let K be the simplest cubic field defined by the irreducible polynomial*

$$f(X) = X^3 + mX^2 - (m+3)X + 1,$$

i.e., $K = \mathbb{Q}(\rho)$ where ρ is the negative root of $f(X)$. Let $\zeta (= \zeta_p)$ be a primitive p-th root of unity and R be the subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ consisting of cubic residues modulo p. We denote S, T ($\neq R$) the cosets of R in $(\mathbb{Z}/p\mathbb{Z})^*$ and put

$$\alpha = \sum_{r\in R}\zeta^r, \quad \beta = \sum_{s\in S}\zeta^s, \quad \gamma = \sum_{t\in T}\zeta^t,$$

and

$$\pi = \prod_{r\in R}(1-\zeta^r), \quad \pi' = \prod_{s\in S}(1-\zeta^s), \quad \pi'' = \prod_{t\in T}(1-\zeta^t).$$

Then we have

(1) *$K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\gamma)$.*

(2) $$\rho = \begin{cases} \min[\alpha,\beta,\gamma] - \dfrac{m-1}{3} & \textit{if} \quad m \equiv 1 \pmod 3; \\ \text{-}\max[\alpha,\beta,\gamma] - \dfrac{m+1}{3} & \textit{if} \quad m \equiv -1 \pmod 3. \end{cases}$$

(3) *π is a prime element of K above p.*

2. Congruence for class numbers of the simplest cubic fields

In this section, we shall prove the following congruence relation for the class numbers of the simplest cubic fields.

THEOREM 2.1. *Let K, m, and p be as in Proposition 1 and h be the class number of K. Then*

$$h \equiv -\frac{27}{4} B_{\frac{p-1}{3}} B_{\frac{2(p-1)}{3}} \pmod{p},$$

where B_n denotes the n-th Bernoulli number.

PROOF. By p-adic class number formula, we have

$$\frac{4hR_p(K)}{p} = L_p(1,\chi)L_p(1,\bar{\chi}). \tag{1}$$

From basic congruence relation for p-adic L-function (cf. [5]), we obtain

$$\begin{aligned} L_p(1,\chi)L_p(1,\bar{\chi}) &\equiv L_p(1-\frac{p-1}{3},\chi)L_p(1-\frac{2(p-1)}{3},\bar{\chi}) \\ &\equiv \frac{9}{2} B_{\frac{p-1}{3}} B_{\frac{2(p-1)}{3}} \pmod{\mathrm{p}}. \end{aligned} \tag{2}$$

By definition of p-adic regulator, we can write

$$R_p(K) = \log_p^2(\rho) - \log_p(\rho)\log_p(\rho-1) + \log_p^2(\rho-1). \tag{3}$$

Since $3\rho+m$, $3\rho'+m$, $3\rho''+m$ are roots of $X^3 = 3pX - (2m+3)p$, we have

$$(3\rho+m)(3\rho'+m)(3\rho''+m) = -(2m+3)p. \tag{4}$$

Note that $(2m+3,p) = 1$. Now let R_π be the ring of π-adic integral elements of K_π. Then we have

$$(3\rho+m)(3\rho'+m)(3\rho''+m) = (p) = (\pi)^3 \text{ in } R_\pi.$$

Since $3\rho^{'}+m, 3\rho^{''}+m$ are conjugates of $3\rho+m$, by the uniqueness of prime factorization of ideals, we conclude that

$$(3\rho+m) = (\pi).$$

Hence we can write

$$3\rho+m = \pi\xi, \tag{5}$$

for some $\xi \in R_\pi^*$. Since $\mathbb{Q}_p(\rho)/\mathbb{Q}_p$ is totally ramified at p, it follows that

$$\mathbb{Z}_p[\rho]/\pi\mathbb{Z}_p[\rho] \cong \mathbb{Z}/p\mathbb{Z}. \tag{6}$$

Hence we can write

$$\xi = a + b\pi + c\pi^2 \pmod{\pi^3}, \tag{7}$$

where $a, b, c \in \mathbb{Z}$ and $p \nmid a$.

From (5), it follows that

$$\log_p(\rho) = \log_p(-\frac{m}{3}) + \log_p(1 - \frac{\pi\xi}{m}), \tag{8}$$

and by combining (7) and (8), we obtain

$$\log_p(\rho) \equiv -\frac{a\pi}{m} - (\frac{b}{m} + \frac{a^2}{2m^2})\pi^2 \pmod{\pi^3}. \tag{9}$$

In verification of (9), we have used the following fact: if $q \in \mathbb{Q}$, then $\log_p q \equiv 0 \pmod{p}$, so $\log_p q \equiv 0 \pmod{\pi^3}$.

Similarly, we get

$$\log_p(\rho - 1) \equiv -\frac{a\pi}{m+3} - \left\{\frac{b}{m+3} + \frac{a^2}{2(m+3)^2}\right\}\pi^2 \pmod{\pi^3}. \tag{10}$$

From (3), (9), and(10), it follows that

$$R_p(K) \equiv -\frac{(2m+3)a^3\pi^3}{2 * 3^4} \pmod{\pi^4}. \tag{11}$$

Now let $p = \pi^3\epsilon, \epsilon \in R_\pi^*$. From(6), we can find $t \in \mathbb{Z}$ such that

$$\epsilon \equiv t \pmod{\pi}. \tag{12}$$

By (1), (2), and (11), it follows that

$$-\frac{4(2m+3)a^3h}{t} \equiv 3^6 B_{\frac{p-1}{3}} B_{\frac{2(p-1)}{3}} \pmod{\pi}. \tag{13}$$

Since every term on both sides of (13) is rational, we may replace π by p, and therefore, we get

$$-\frac{4(2m+3)a^3h}{t} \equiv 3^6 B_{\frac{p-1}{3}} B_{\frac{2(p-1)}{3}} \pmod{p}. \tag{14}$$

Now choose δ in $(\mathbb{Z}/p\mathbb{Z})^*$ such that $S = \delta$R and T=$\delta^2 R$. From the choice of π (cf. Proposition 1), we can write

$$\epsilon = \frac{\pi'\pi''}{\pi^2} = \prod_{r \in R} \frac{(1-\zeta^{r\delta})(1-\zeta^{r\delta^2})}{(1-\zeta^r)^2}. \tag{15}$$

Note that $\dfrac{(1-\zeta^{r\delta})}{(1-\zeta^r)} = \sum_{k=0}^{\delta-1}\zeta^{kr} \equiv \sum_{k=0}^{\delta-1} 1 \equiv \delta \pmod{\wp}$, where $\wp = (1-\zeta)$. Hence

$$\prod_{r\in R}\frac{(1-\zeta^{r\delta})}{(1-\zeta^r)} \equiv \delta^{\frac{p-1}{3}} \pmod{\wp}. \tag{16}$$

Similarly, we have

$$\prod_{r\in R}\frac{(1-\zeta^{r\delta^2})}{(1-\zeta^r)} \equiv \delta^{\frac{2(p-1)}{3}} \pmod{\wp}. \tag{17}$$

From (12), (15), (16), and (17), it follows that

$$\epsilon \equiv t \equiv \delta^{p-1} \equiv 1 \pmod{\wp}.$$

Since $t \in \mathbb{Z}$, we have

$$t \equiv 1 \pmod{p}. \tag{18}$$

By (5) and (7), we can write

$$(3\rho+m)(3\rho'+m)(3\rho''+m) \equiv \pi\pi'\pi'' a^3 \pmod{\pi^4}. \tag{19}$$

Therefore, by (4) and (19), it follows that $-(2m+3)p \equiv p\,a^3 \pmod{\pi^4}$, so that $-(2m+3) \equiv a^3 \pmod{\pi}$. Consequently, we obtain

$$-(2m+3) \equiv a^3 \pmod{p}. \tag{20}$$

From (14), (18), and (20), we get the desired congruence relation as in the Theorem 2.1. □

3. Upper bound for class number

In this section, we shall obtain the following upper bound for class numbers of the simplest cubic fields.

THEOREM 3.1. *Let h be the class number of K as in Theorem 2.1. Then,*

$$h < p.$$

PROOF. Let $L = \dfrac{p-1}{2}$. By the class number formula, we get

$$\frac{4Rh}{p} = L(1,\chi)L(1,\bar{\chi}) = |L(1,\chi)|^2, \tag{21}$$

where $R = \log^2(1-\rho) - \log(1-\rho)\log(-\rho) + \log^2(-\rho)$ is the regulator of K. Since $\rho < -m-1$, we obtain

$$R \geq \frac{3}{4}\log^2(-\rho) \geq \frac{3}{4}\log^2(m+1). \tag{22}$$

From (21) and (22), it follows that

$$\frac{3h\log^2(m+1)}{p} \leq |L(1,\chi)|^2. \tag{23}$$

Now we shall find an upper bound for $|L(1,\chi)|^2$. Note that

$$L(1,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n} = \sum_{n=1}^{L}\frac{\chi(n)}{n} + \sum_{n=L+1}^{\infty}\frac{\chi(n)}{n}. \tag{24}$$

Since $2\sum_{k=1}^{L}\chi(k) = \sum_{k=1}^{L}\{\chi(k)+\chi(p-k)\} = \sum_{k=1}^{p-1}\chi(k) = 0$,

$$\sum_{k=1}^{L}\chi(k) = \sum_{L+1}^{p-1}\chi(k) = 0. \tag{25}$$

From (25), it follows that

$$|\sum_{k=L+1}^{j}\chi(k)| \leq L, \tag{26}$$

for all j with $j \geq L+1$. Notice that

$$\begin{aligned}\sum_{n=L+1}^{\infty}\frac{\chi(n)}{n} &= \chi(L+1)\Big\{\frac{1}{L+1}-\frac{1}{L+2}\Big\}\\ &\quad+\{\chi(L+1)+\chi(L+2)\}\Big\{\frac{1}{L+2}-\frac{1}{L+3}\Big\}\\ &\quad+\{\chi(L+1)+\chi(L+2)+\chi(L+3)\}\Big\{\frac{1}{L+3}-\frac{1}{L+4}\Big\}\\ &\quad\cdots\end{aligned}$$

(This is not a rearrangement!)

$$= \sum_{j=L+1}^{\infty}\Big\{\sum_{k=L+1}^{j}\chi(k)\Big\}\Big\{\frac{1}{j}-\frac{1}{j+1}\Big\} \tag{27}$$

From (26) and (27), it follows that

$$\Big|\sum_{k=L+1}^{\infty}\frac{\chi(n)}{n}\Big| \leq \sum_{j=L+1}^{\infty}L\Big(\frac{1}{j}-\frac{1}{j+1}\Big) \leq \frac{L}{L+1} < 1. \tag{28}$$

By (24) and (28), we conclude that

$$|L(1,\chi)| < \Big|\sum_{n=1}^{L} \frac{\chi(n)}{n}\Big| + 1. \tag{29}$$

Now let $S_p = \{x \in \mathbb{Z} |\ 1 \le x \le L\}$ and decompose S_p into U, V, W, where

$$\begin{aligned} U &= \{x \in S_p |\ \chi(x) = 1\}, \\ V &= \{x \in S_p |\ \chi(x) = \omega\}, \\ W &= \{x \in S_p |\ \chi(x) = \omega^2\}. \end{aligned}$$

We remark that $|U| = |V| = |W| = (p-1)/6 \in \mathbb{Z}^+$, since $p \equiv 1 \pmod 6$. Recall that Y denotes the character group of the simplest cubic field K, and consider the following term

$$\xi := \sum_{\psi \in Y} \Big|\sum_{n=1}^{L} \frac{\psi(n)}{n}\Big|^2. \tag{30}$$

We notice that

$$\Big|\sum_{n=1}^{L} \frac{\psi(n)}{n}\Big|^2 = \sum_{j=1}^{L}\sum_{k=1}^{L} \frac{\psi(j)\bar{\psi}(k)}{jk} = \sum_{j=1}^{L}\sum_{k=1}^{L} \frac{\bar{\psi}(j^*k)}{jk}, \tag{31}$$

where j^* is uniquely determined in S_p by the condition that $jj^* \equiv \pm 1 \pmod p$. (For $\psi = \chi, \bar{\chi},\ \psi(j) = \bar{\psi}(j^*)$ if and only if $\bar{\psi}(jj^*) = 1$.) From (30) and (31), it follows that

$$\xi = \sum_{j=1}^{L} \frac{1}{j} \sum_{k=1}^{L} \frac{1}{k} \sum_{\psi \in Y} \bar{\psi}(j^*k). \tag{32}$$

Note that

$$\sum_{\psi \in Y} \bar{\psi}(j^*k) = \begin{cases} 3 & \text{if } \ \chi(j^*k) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore we obtain

$$\xi = 3(F^2 + G^2 + H^2), \tag{33}$$

where $F = \sum_{n \in U} \frac{1}{n}$, $G = \sum_{n \in V} \frac{1}{n}$, and $H = \sum_{n \in W} \frac{1}{n}$.
On the other hand, we have

$$\xi = \Big(\sum_{n=1}^{L} \frac{1}{n}\Big)^2 + 2\Big|\sum_{n=1}^{L} \frac{\chi(n)}{n}\Big|^2 = (F+G+H)^2 + 2\Big|\sum_{n=1}^{L} \frac{\chi(n)}{n}\Big|^2. \tag{34}$$

From (33) and (34), it follows that

$$(35) \qquad \Big|\sum_{n=1}^{L} \frac{\chi(n)}{n}\Big|^2 = \frac{1}{2}\{(F-G)^2 + (G-H)^2 + (H-F)^2\}.$$

Now we shall estimate $|F-G|$, $|G-H|$, $|H-F|$. To do this, we need a lemma, which was originally due to Jacobi (cf. [2], pp. 80-81).

LEMMA 3.2. *If p is a prime of the form m^2+3m+9, then 2 is a cubic non-residue modulo p.*

PROOF. Note that $p = (m-3\omega)(m-3\bar{\omega})$ in $\mathbb{Z}[\omega]$ where $\omega = \zeta_3$. Since $3 \nmid m$, $m-3\omega$ and $m-3\bar{\omega}$ are not associated in $\mathbb{Z}[\omega]$. Hence p splits completely in $\mathbb{Z}[\omega]$ and therefore both $m-3\omega$, $m-3\bar{\omega}$ are primes in $\mathbb{Z}[\omega]$. Suppose that 2 is a cubic residue mod p. Then 2 is a cubic residue mod π, where $\pi = m-3\omega$. Note that both 2 and π are primary. By the *cubic reciprocity*, $(\frac{2}{\pi})_3 = (\frac{\pi}{2})_3 = 1$, so by definition $\pi \equiv (\frac{\pi}{2})_3 \equiv 1 \pmod 2$. Hence $\pi = 1+2(s+t\omega)$ for some $s, t \in \mathbb{Z}$. Then $-3 = 2t$. This contradiction completes the proof of lemma. □

Now we return to the proof of the theorem and we may consider only $m \geq 7$. (For the case of $m < 7$, the theorem is trivially true.) We will treat only the case that $F = max[F, G, H]$ and $2 \in V$. (The arguments of remaining cases are similar to this case.) There are two cases to consider. First, we consider the case that $G \geq H$. In this case, we must have that $F \geq G \geq H$. Since $2 \in V$, $G \geq \sum_{n\in U} \frac{1}{2n} = \frac{F}{2}$, and hence we obtain

$$(36) \qquad F - G \leq \frac{F}{2}.$$

Since $4 \in W$, $H \geq \sum_{n\in U} \frac{1}{4n} = \frac{F}{4}$, and hence we have

$$(37) \qquad F - H \leq \frac{3F}{4}.$$

Furthermore, $H \geq \sum_{n\in V} \frac{1}{2n} = \frac{G}{2}$ and hence we have

$$(38) \qquad G - H \leq \frac{G}{2} \leq \frac{F}{2}.$$

Since $\sum_{n=1}^{L} \frac{1}{n} = F + G + H \geq \frac{7}{4}F$, it follows that

$$\frac{4}{7}\Big(\sum_{n=1}^{L} \frac{1}{n}\Big) \geq F. \tag{39}$$

On the other hand,

$$\sum_{n=1}^{L} \frac{1}{n} = 1 + \sum_{n=2}^{L} \frac{1}{n} \leq 1 + \int_{1}^{L} \frac{1}{x} dx = 1 + \log L.$$

Therefore it follows that

$$\sum_{n=1}^{L} \frac{1}{n} \leq 1 + \log L. \tag{40}$$

From (39) and (40), we get

$$F \leq \frac{4}{7}(1 + \log L). \tag{41}$$

By (35), (36), (37), (38), and (41), it follows that

$$\Big|\sum_{n=1}^{L} \frac{\chi(n)}{n}\Big|^2 < \frac{17}{98}(1 + \log L)^2 < \Big(\frac{3}{7}\Big)^2 (1 + \log L)^2. \tag{42}$$

By combining (29) and (42), we obtain

$$|L(1, \chi)| < \frac{3}{7}\,\big(\log L + \frac{10}{3}\big). \tag{43}$$

From (23) and (43), we deduce that

$$\frac{3\,h\, \log^2(m+1)^2}{4p} < \Big(\frac{3}{7}\Big)^2 \Big(\log L + \frac{10}{3}\Big)^2. \tag{44}$$

Note that

$$L = \frac{(m^2 + 3m + 8)}{2} \leq (m+1)^2 \quad \text{for all } \ m \geq 2. \tag{45}$$

If $m \geq 7$, then

$$\begin{aligned} \frac{3}{4} \log^2(m+1)^2 &> \Big(\frac{11}{14}\Big)^2 \log^2(m+1)^2 \\ &> \Big(\frac{3}{7}\Big)^2 \Big\{\log(m+1)^2 + \frac{10}{3}\Big\}^2. \end{aligned} \tag{46}$$

By comparison of (44), (45), and (46), we finally have

$$h < p.$$

Next, we consider the case that $H > G$. Since $G \geq \sum_{n\in U} \frac{1}{2n} = \frac{F}{2}$, we have

$$H > G \geq \frac{F}{2} \text{ and } F - H < \frac{F}{2}.$$

Note that $F - G \leq \frac{F}{2}$ and $H - G \leq F - G < \frac{F}{2}$. Therefore we get

$$\sum_{n=1}^{L} \frac{1}{n} = F + G + H > 2F. \tag{47}$$

By combining (40) and (47), it follows that

$$F < \frac{1}{2}(1 + \log L). \tag{48}$$

We plug (48) in (35) and obtain

$$\Big|\sum_{n=1}^{L} \frac{\chi(n)}{n}\Big|^2 < \frac{3}{32}(1 + \log L)^2 < \Big(\frac{3}{7}\Big)^2 (1 + \log L)^2. \tag{49}$$

By the same argument as in the first case (compare (42) and (49)), we conclude that $h < p$. This completes the proof of the theorem. $\square$

REMARK 3.1. By *Staudt-Clausen theorem* (cf. [5]),

$$B_{\frac{p-1}{3}} B_{\frac{2(p-1)}{3}} \in \mathbb{Z}_p.$$

Hence the congruence in Theorem 2.1 is always solvable. Furthermore, by Theorem 3.1, the unique positive integer less than p which satisfies the congruence in Theorem 2.1, is actually the class number of the simplest cubic field.

As an illustration of our result, we consider the simplest cubic field with $m = 11$. In this case, $p = m^2 + 3m + 9 = 163$. By Theorem 2.1,

$$h \equiv \frac{-27}{4} B_{54} B_{108} \equiv \frac{-27 * 69 * 58}{4 * 146 * 118} \equiv 4 \pmod{163}.$$

By Theorem 3.1, $h < 163$, and therefore we conclude that $h = 4$.

References

[1] N. C. Ankeny, E. Artin, and S. Chowla, *The class number of real quadratic fields*, Ann. of Math. **56** (1952), 479–493.
[2] D. A. Cox, *Primes of the form* $x^2 + ny^2$, John Willy and Sons, New York, 1989.
[3] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.
[4] J. H. Silvermann and J. Tate, *Rational points on elliptic curves*, Springer-Verlag, New York, 1985.
[5] L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1980.
[6] ———, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), 371–384.

Department of Mathematics
Pohang University of Science and Technology
Pohang 790-784, Korea
E-mail: integer@euclid.postech.ac.kr