Primary components of the ideal class group of the $\mathbf{Z}_p$-extension over $\mathbf{Q}$ for typical inert primes

By Kuniaki Horie

Department of Mathematics, Tokai University
1117, Kitakaname, Hiratsuka, Kanagawa 259-1292

(Communicated by Shigefumi Mori, m. j. a., March 14, 2005)

Abstract: Let p be an odd prime, $\mathbf{Z}_p$ the ring of p-adic integers, and l a prime number different from p. We have shown in [1] that, if l is a sufficiently large primitive root modulo p^2, then the l-class group of the $\mathbf{Z}_p$-extension over the rational field is trivial. We shall modify part of the proof of the above result and see, in the case $p \leq 7$, that the result holds without assuming l to be sufficiently large.

Key words: $\mathbf{Z}_p$-extension; ideal class group.

Introduction. Let p be an odd prime number, $\mathbf{Z}_p$ the ring of p-adic integers, and $\mathbf{Q}_\infty$ the $\mathbf{Z}_p$-extension over the field $\mathbf{Q}$ of rational numbers, i.e., the unique abelian extension over $\mathbf{Q}$ whose Galois group over $\mathbf{Q}$ is topologically isomorphic to the additive group of $\mathbf{Z}_p$. Let l be a prime number different from p. Theorem 3 of [1] states that the l-class group of $\mathbf{Q}_\infty$ is trivial if l is a primitive root modulo p^2 and if

$$l \geq \frac{3}{2\log 2}(p-1)\varphi(p-1)(\log p + \log(\log p)).$$

Here φ denotes as usual the Euler function. In this note, we shall review or improve some preliminary results of [1] for the proof of the theorem, and as a consequence we shall see that, when p is 5 or 7, the theorem holds without the second condition in the above statement (for the case $p = 3$, cf. Lemma 10 of [1]).

1. For each integer $m \geq 0$, let h_m denote the class number of the subfield of $\mathbf{Q}_\infty$ with degree p^m. Since p is totally ramified for $\mathbf{Q}_\infty/\mathbf{Q}$, class field theory shows that h_{u-1} divides h_u for every positive integer u. Furthermore, by the definition of the l-class group of $\mathbf{Q}_\infty$, we immediately have the following

Lemma 1. *The l-class group of $\mathbf{Q}_\infty$ is trivial if and only if l does not divide h_u/h_{u-1} for any positive integer u.*

Let ν be the number of distinct prime divisors of $(p-1)/2$, let

$$\frac{p-1}{2} = q_1 \cdots q_\nu$$

where $q_1, \ldots, q_\nu$ are prime-powers > 1 pairwise relatively prime, and let V be the subset of the cyclic group $\langle e^{2\pi i/(p-1)} \rangle$ consisting of

$$e^{\pi i m_1/q_1} \cdots e^{\pi i m_\nu/q_\nu}$$

for all ν-tuples $(m_1, \ldots, m_\nu)$ of integers with $0 \leq m_1 < q_1, \ldots, 0 \leq m_\nu < q_\nu$. We understand that $V = \{1\}$ if $p = 3$. Denoting by $\mathbf{Z}$ the ring of (rational) integers as usual, let Φ denote the set of maps

$$z : V \to \{u \in \mathbf{Z} \mid 0 \leq u \leq 2l\}$$

such that, for some $\xi \in V$,

$$l \nmid z(\xi) \quad \text{or} \quad z(\xi) > 0$$

according as $l > 2$ or $l = 2$, and

$$l \mid z(\xi') \quad \text{for all} \quad \xi' \in V \setminus \{\xi\}.$$

We then put

$$M = \max_{z \in \Phi} \left| \mathfrak{N}\left(\sum_{\xi \in V} z(\xi)\xi - 1 \right) \right|.$$

Here $\mathfrak{N}$ denotes the norm map from $\mathbf{Q}(e^{2\pi i/(p-1)})$ to $\mathbf{Q}$. For each algebraic number α, we let $\|\alpha\|$ denote the maximum of the absolute values of all conjugates of α over $\mathbf{Q}$.

Now, let n be any positive integer, which will be fixed henceforth. Put

$$\zeta = e^{2\pi i/p^{n+1}}, \quad t = p^n + 1,$$

2000 Mathematics Subject Classification. Primary 11R20; Secondary 11R23, 11R29.

and put

$$\eta = \prod_a \frac{\zeta^a - \zeta^{-a}}{\zeta^{ta} - \zeta^{-ta}} = \prod_a \frac{\sin(2\pi a/p^{n+1})}{\sin(2\pi ta/p^{n+1})},$$

with a ranging over the positive integers $< p^{n+1}/2$ such that $a^{p-1} \equiv 1 \pmod{p^{n+1}}$. We easily see that η is a unit in the subfield of $\mathbf{Q}_\infty$ with degree p^n.

Lemma 2. *Assume that l is a primitive root modulo $p^{\min(2,n)}$, namely, a primitive root modulo p^n. If*

$$p^n > M \quad or \quad l \geq \frac{\log \|\eta\|}{\log 2},$$

then l does not divide h_n/h_{n-1}.

Proof. This follows from Lemmas 2, 3 and 8 of [1]. □

Remark. If $p = 3$ and if $l \equiv 2$ or $5 \pmod 9$, i.e., l is a primitive root modulo 9, then one has

$$M = 2l - 2 \quad \text{or} \quad M = 3$$

according as $l > 2$ or $l = 2$, Lemma 4 of [1] yields

$$\|\eta\| < \frac{3^{n+1}}{\pi} \sin\frac{\pi}{3} = \frac{3^{n+1}\sqrt{3}}{2\pi},$$

and hence, by Lemmas 1 and 2, the l-class group of $\mathbf{Q}_\infty$ is trivial as Lemma 10 of [1] has stated.

Let $\mathfrak{p}$ be a prime ideal of $\mathbf{Q}(e^{2\pi i/(p-1)})$ dividing p. Let I be the set of positive integers $a < p^{n+1}$ such that there exist elements ξ of V with $a \equiv \xi \pmod{\mathfrak{p}^{n+1}}$, and let $\mathfrak{F}$ be the family of all maps from I to the set $\{0, l\}$. For each $a \in I$, let $\mathfrak{G}_a$ denote the family of maps $j : I \to \mathbf{Z}$ such that $\min(l-2, 1) \leq j(a) < l$ and that $j(b) = 0$ or l for every $b \in I \setminus \{a\}$. Given any integer m, we then let

$$\mathcal{P}_a(m) = \left\{ (j_1, j_2) \in \mathfrak{G}_a \times \mathfrak{F} \;\middle|\; \sum_{b\in I} (tj_1(b) + j_2(b))b \equiv m \pmod{p^{n+1}} \right\},$$

$$\mathcal{Q}_a(m) = \left\{ (j_1, j_2) \in \mathfrak{F} \times \mathfrak{G}_a \;\middle|\; \sum_{b\in I} (tj_1(b) + j_2(b))b \equiv m \pmod{p^{n+1}} \right\}.$$

Moreover, in the case $l > 2$, we put

$$s_1(m) = \sum_{a\in I} \sum_{(j_1,j_2)\in\mathcal{P}_a(m)} \frac{(-1)^{j_1(a)+\sum_{b\in I}(j_1(b)+j_2(b))}}{j_1(a)},$$

$$s_2(m) = \sum_{a\in I} \sum_{(j_1,j_2)\in\mathcal{Q}_a(m)} \frac{(-1)^{j_2(a)+\sum_{b\in I}(j_1(b)+j_2(b))}}{j_2(a)};$$

in the case $l = 2$, we put

$$s_1(m) = \sum_{a\in I} |\mathcal{P}_a(m)|, \quad s_2(m) = \sum_{a\in I} |\mathcal{Q}_a(m)|.$$

Note that the rational numbers $s_1(m)$, $s_2(m)$ are l-adic integers.

Lemma 3. *Assume l to be a primitive root modulo p^n. If there exist integers c and d satisfying*

$$c \equiv d \pmod{p^n},$$
$$s_2(c) - s_1(c) \not\equiv s_2(d) - s_1(d) \pmod{l},$$

then l does not divide h_n/h_{n-1}.

Proof. Let x be an indeterminate. We denote by $J(x)$ the polynomial in $\mathbf{Z}[x]$ such that $(x-1)^l = x^l - 1 + lJ(x)$. Namely,

$$J(x) = \sum_{u=1}^{l-1} \frac{(-1)^{u-1}}{l}\binom{l}{u} x^u \quad \text{or} \quad J(x) = -x + 1$$

according as $l > 2$ or $l = 2$. We also define in $\mathbf{Z}[x]$

$$L(x) = \sum_{a\in I} \left(\prod_{b\in I\setminus\{a\}} (x^{lb} - 1)(x^{ltb} - 1) \right) \left((x^{la} - 1)J(x^{ta}) - (x^{lta} - 1)J(x^a) \right).$$

For any $m \in \mathbf{Z}$, the sum of the coefficients of x^u in $L(x)$ for all non-negative integers u with $u \equiv m \pmod{p^{n+1}}$ is congruent to $s_2(m) - s_1(m)$ modulo l; because

$$\frac{(-1)^{u-1}}{l}\binom{l}{u} \equiv \frac{1}{u} \pmod{l}$$

for every positive integer $u < l$ and, in the case $l = 2$,

$$\sum_{a\in I} \left(\prod_{b\in I\setminus\{a\}} (x^{2b} + 1)(x^{2tb} + 1) \right) \left((x^{2a} + 1)(x^{ta} + 1) + (x^{2ta} + 1)(x^a + 1) \right) - L(x) \in 2\mathbf{Z}[x].$$

Hence, in view of the relation $\sum_{r=0}^{p-1} \zeta^{rp^n} = 0$, we know that $L(\zeta) \not\equiv 0 \pmod{l}$ if and only if there exist integers c, d satisfying

$$c \equiv d \pmod{p^n},$$
$$s_2(c) - s_1(c) \not\equiv s_2(d) - s_1(d) \pmod{l}$$

(cf. Lemma 6 of [1]). Furthermore, the proof of Lemma 8 of [1] shows that, if $L(\zeta) \not\equiv 0 \pmod{l}$, then

$h_n/h_{n-1} \not\equiv 0 \pmod{l}$. We thus obtain the lemma. □

For each integer m, we let

$$\mathcal{P}(m) = \bigcup_{a\in I} \mathcal{P}_a(m), \quad \mathcal{Q}(m) = \bigcup_{a\in I} \mathcal{Q}_a(m).$$

Lemma 4. *Assume that l is a primitive root modulo p^n, and that there exist integers c and d satisfying*

$$c \equiv d \pmod{p^n},$$
$$|\mathcal{P}(c) \cup \mathcal{Q}(c)| = 1, \quad \mathcal{P}(d) \cup \mathcal{Q}(d) = \emptyset.$$

If $l = 2$, assume as well that $g_1(I) \cup g_2(I)$ contains 1 for the element (g_1, g_2) of $\mathcal{P}(c) \cup \mathcal{Q}(c)$. Then l does not divide h_n/h_{n-1}.

Proof. The hypothesis implies not only that $s_1(d) = s_2(d) = 0$ but that, for some $a \in I$ and every $b \in I \setminus \{a\}$,

$$|\mathcal{P}_a(c)| + |\mathcal{Q}_a(c)| = 1, \quad \mathcal{P}_b(c) = \mathcal{Q}_b(c) = \emptyset,$$

and hence $s_2(c) - s_1(c) \not\equiv 0 \pmod{l}$. The lemma therefore follows from Lemma 3. □

2. Given any pair $\kappa = (j_1, j_2)$ of maps $I \to \mathbf{Z}$, we naturally identify κ with a map $I \to \mathbf{Z} \times \mathbf{Z}$, i.e., we put

$$\kappa(a) = (j_1(a), j_2(a)) \quad \text{for each} \quad a \in I.$$

We also put

$$D = l(t+1)\sum_{a\in I} a - 1 = l(p^n + 2)\sum_{a\in I} a - 1.$$

Let us consider the case where $p = 5$ or 7.

Proposition 1. *Assume that $p = 5$ and that l is a primitive root modulo 25, i.e., $l \equiv 2, 3, 8, 12, 13, 17, 22, 23 \pmod{25}$. Then the l-class group of $\mathbf{Q}_\infty$ is trivial.*

Proof. Clearly, we have $V = \{1, i\}$. It follows that

$$\mathfrak{N}\left(\sum_{\xi\in V} z(\xi)\xi - 1\right) = (z(1) - 1)^2 + z(i)^2$$

for every map z in Φ. Therefore,

$$M = 8l^2 - 8l + 4 \quad \text{or} \quad M = 25$$

according as $l > 2$ or $l = 2$. We let, in $\mathbf{Z} \times \mathbf{Z}$,

$$S = \{(1,2), (1,3), (2,2), (2,3), (3,13), (4,13), (4,17), (5,23)\}.$$

Since the inequality $5^n \le M$ is equivalent to the condition that

$$\sqrt{\frac{5^n - 2}{8}} + \frac{1}{2} \le l \quad \text{or} \quad (n.l) = (2,2),$$

(n, l) belongs to S if and only if

$$5^n \le M \quad \text{and} \quad l < \frac{2}{\log 2}\log\left(\frac{5^{n+1}}{\pi}\sin\frac{\pi}{5}\right).$$

On the other hand, Lemma 4 of [1] implies

$$\|\eta\| < \left(\frac{5^{n+1}}{\pi}\sin\frac{\pi}{5}\right)^2.$$

We therefore know form Lemma 2 that l does not divide h_n/h_{n-1} unless (n, l) belongs to S.

Suppose now that (n, l) belongs to S. In view of $1068^2 \equiv -1 \pmod{5^6}$, let a_0 be the integer such that

$$0 < a_0 < 5^{n+1}, \quad a_0 \equiv 1068 \pmod{5^{n+1}},$$

and take as $\mathfrak{p}$ the prime ideal of $\mathbf{Q}(i)$ generated by 5 and $a_0 - i$. We then have

$$I = \{1, a_0\}, \quad D = l(a_0 + 1)(5^n + 2) - 1.$$

In the case $n \ge 2$,

$$\mathcal{P}(D) = \mathcal{P}(D + 2\cdot 5^n) = \mathcal{Q}(D + 2\cdot 5^n) = \emptyset,$$

and $\mathcal{Q}(D)$ consists only of the map $\theta : I \to \mathbf{Z} \times \mathbf{Z}$ for which

$$\theta(1) = (l, l-1), \quad \theta(a_0) = (l, l).$$

In the case $(n, l) = (1, 3)$,

$$\mathcal{P}(23) = \{\psi\}, \quad \mathcal{Q}(23) = \{\theta_1, \theta_2\}, \quad \mathcal{P}(28) = \emptyset,$$
$$\mathcal{Q}(28) = \{\theta_3\},$$

with the maps ψ, θ_1, θ_2, θ_3 of I into $\mathbf{Z} \times \mathbf{Z}$ defined by

$$\psi(1) = (0,3), \quad \psi(a_0) = (2,3), \quad \theta_1(1) = (3,2),$$
$$\theta_1(a_0) = (3,3), \quad \theta_2(1) = (3,1), \quad \theta_2(a_0) = (0,3),$$
$$\theta_3(1) = (3,0), \quad \theta_3(a_0) = (3,2);$$

hence one sees that

$$s_2(23) - s_1(23) = 0, \quad s_2(28) - s_1(28) = \frac{1}{2}.$$

In the case $(n, l) = (1, 2)$,

$$\mathcal{P}(15) = \mathcal{Q}(10) = \emptyset, \quad \mathcal{Q}(15) = \{\theta\},$$
$$\mathcal{P}(10) = \{\psi_1, \psi_2\},$$

with the maps θ, ψ_1, ψ_2 of I into $\mathbf{Z} \times \mathbf{Z}$ defined by

$$\theta(1) = (2,1), \quad \theta(a_0) = (2,2), \quad \psi_1(1) = (1,2),$$
$$\psi_1(a_0) = (2,2), \quad \psi_2(1) = (0,2), \quad \psi_2(a_0) = (1,0),$$

so that

$$s_2(15) - s_1(15) = 1, \quad s_2(10) - s_1(10) = -2.$$

Hence the proof is completed by Lemmas 1, 3 and 4. □

Proposition 2. *Assume that $p = 7$ and that l is a primitive root modulo 49, namely, $l \equiv 3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47 \pmod{49}$. Then the l-class group of $\mathbf{Q}_\infty$ is trivial.*

Proof. Let us set $\rho = e^{\pi i/3}$ for simplicity. As $V = \{1, \rho, \rho^2\}$, we find that

$$\begin{aligned}\mathfrak{N}\left(\sum_{\xi\in V} z(\xi)\xi - 1\right) &= (z(1) + z(\rho) - 1)^2 - (z(\rho) + z(\rho^2))(z(1) \\ &\quad + z(\rho) - 1) + (z(\rho) + z(\rho^2))^2\end{aligned}$$

for every z in Φ. When the right hand side of the above takes its maximum, one of $z(1)$, $z(\rho)$, $z(\rho^2)$ belongs to $\{1, 2l-1\}$ and the others belong to $\{0, 2l\}$. Thus we obtain

$$M = (4l-2)^2 - 4l(4l-2) + (4l)^2 = 16l^2 - 8l + 4.$$

We now let

$$S = \{(1,3), (2,3), (2,5), (3,5), (3,17), (4,17)\}.$$

It follows that (n, l) belongs to $S \cup \{(1,5)\}$ if and only if

$$7^n \le M, \quad l < \frac{3}{\log 2} \log\left(\frac{7^{n+1}}{\pi} \sin\frac{\pi}{7}\right).$$

In the case $n = 1$, we also have

$$\|\eta\| = \frac{\sin(12\pi/49)\sin(17\pi/49)\sin(20\pi/49)}{\sin(2\pi/49)\sin(11\pi/49)\sin(13\pi/49)} < 2^4.$$

Hence Lemma 2, together with Lemma 4 of [1], shows that l does not divide h_n/h_{n-1} unless (n, l) belongs to S.

Next, suppose (n, l) to be in S. Let a_0 be the positive integer $< 7^{n+1}$ such that $a_0 \equiv 1354 \pmod{7^{n+1}}$, hence, $a_0^2 - a_0 + 1 \equiv 0 \pmod{7^{n+1}}$. Take as $\mathfrak{p}$ the prime ideal of $\mathbf{Q}(\rho)$ generated by 7 and $a_0 - \rho$, so that

$$I = \{1, a_0, a_0 - 1\}, \quad D = 2la_0(7^n + 2) - 1.$$

If (n, l) equals $(4, 17)$, $(3, 5)$ or $(2, 3)$, then we have

$$|\mathcal{P}(D + 3\cdot 7^n)| = 1, \quad \mathcal{Q}(D + 3\cdot 7^n) = \emptyset,$$

$$\mathcal{P}(D + 5\cdot 7^n) = \mathcal{Q}(D + 5\cdot 7^n) = \emptyset.$$

In the case $(n, l) = (3, 17)$ and the case $(n, l) = (2, 5)$, we see respectively that

$$|\mathcal{P}(2548)| = 1, \quad \mathcal{Q}(2548) = \mathcal{P}(3920) = \mathcal{Q}(3920) = \emptyset$$

and that

$$|\mathcal{P}(129)| = 1, \quad \mathcal{Q}(129) = \mathcal{P}(227) = \mathcal{Q}(227) = \emptyset.$$

In the case $(n, l) = (1, 3)$, we obtain

$$\mathcal{P}(7) = \{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5\}, \quad \mathcal{Q}(7) = \{\theta_1, \theta_2, \theta_3\},$$
$$\mathcal{P}(21) = \{\psi_6\}, \quad \mathcal{Q}(21) = \{\theta_4, \theta_5\},$$

where $\psi_1, \ldots, \psi_6$, $\theta_1, \ldots, \theta_5$ are the maps $I \to \mathbf{Z} \times \mathbf{Z}$ such that

$$\begin{aligned}
&\psi_1(1) = (1,3),\ \psi_1(a_0) = (3,3),\ \psi_1(a_0-1) = (0,3),\\
&\psi_2(1) = (0,3),\ \psi_2(a_0) = (3,0),\ \psi_2(a_0-1) = (1,0),\\
&\psi_3(1) = (3,3),\ \psi_3(a_0) = (1,0),\ \psi_3(a_0-1) = (3,3),\\
&\psi_4(1) = (3,0),\ \psi_4(a_0) = (2,0),\ \psi_4(a_0-1) = (3,3),\\
&\psi_5(1) = (3,0),\ \psi_5(a_0) = (1,3),\ \psi_5(a_0-1) = (3,0),\\
&\theta_1(1) = (3,2),\ \theta_1(a_0) = (3,3),\ \theta_1(a_0-1) = (3,3),\\
&\theta_2(1) = (3,0),\ \theta_2(a_0) = (3,1),\ \theta_2(a_0-1) = (0,3),\\
&\theta_3(1) = (0,0),\ \theta_3(a_0) = (3,2),\ \theta_3(a_0-1) = (3,0),\\
&\psi_6(1) = (3,3),\ \psi_6(a_0) = (3,3),\ \psi_6(a_0-1) = (2,0),\\
&\theta_4(1) = (3,1),\ \theta_4(a_0) = (3,3),\ \theta_4(a_0-1) = (0,3),\\
&\theta_5(1) = (3,2),\ \theta_5(a_0) = (0,3),\ \theta_5(a_0-1) = (0,0).
\end{aligned}$$

Therefore, in this case,

$$s_2(7) - s_1(7) = -\frac{5}{2}, \quad s_2(21) - s_1(21) = 1.$$

Thus Lemmas 1, 3 and 4 complete the proof of the proposition. □

We would continue our discussion, not assuming $p \le 7$. It is possible to do so to some extent with the help of a computer.

Acknowledgement. The author thanks the referee who read the paper carefully and made several helpful comments.

Reference

[1] K. Horie, Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field, J. London Math. Soc. (2) **66** (2002), no. 2, 257–275.