Suppose for example that $Nq = \pm 4$. Since $2 = \pi \bar{\pi}$ where $\pi = 3 + \theta$, unique factorization implies that up to a unit factor, $q$ must equal $\pi^2$, $\pi \bar{\pi}$ or $\bar{\pi}^2$. Since $q > 0$ this unit factor is $w^4$ for some $n \in \mathbb{Z}$. Now $w = 27 + 100$ so that $w^4 \equiv 1 \pmod{4}$. Hence, $q \equiv \pi^2, \pi \bar{\pi}, \bar{\pi}^2, \pi \bar{\pi} \bar{\pi}, \pi \bar{\pi}^2 \pmod{4}$. Multiplying these out we find that none of them is compatible with the hypothesis $q \equiv 2 + 3\theta \pmod{4}$.

The rest of the cases in this proposition are settled by similar calculations.

References

c_1 \in \mathbb{Z}$ is a prime and if $(c_0 + c_1 x^{p-1}) \equiv 1 \pmod{p}$, then the $l$-class group of the pure field $\mathbb{Q}(\sqrt[p]{l})$ is not cyclic, i.e., rank $H(\mathbb{Q}(\sqrt[p]{l})) \geq 2$.

We conclude this introduction with some remarks about notations. In general we use multiplicative notations for groups and modules. Also the action of a group or a ring on a module is expressed by exponentiation, and $(x^n)^y = x^{ny}$.

1. Preliminaries. We use the notation of the introduction. For a finite extension $F/\mathbb{Q}$, let $H(l)$ denote the $l$-class group of $F$. If $A$ is a finite abelian group, rank $A$ is defined to be the number of invariants divisible by $l$. Also $\mathbb{Z}[l]$ is the group ring of $A$ over $\mathbb{Z}$. We denote by $\chi$ the group of $l$-adic characters of $T$, i.e., homomorphisms of $T$ into the group $\mathbb{Z}_l^*$ of units in $\mathbb{Z}_l$. Note that $\mathbb{Z}_l^*$ contains the $n$th roots of unity since $n | l - 1$. For a character $\chi$ in $X$, let $e_\chi$ be the idempotent of $\mathbb{Z}[l]$ attached to $\chi$; i.e.,

$$e_\chi = n^{-1} \sum_{\chi = \chi^{-1}} \chi(q^n - 1).$$

Then the $e_\chi$ are mutually orthogonal. For a $\mathbb{Z}[l]$-module $M$, let $M_{\langle \chi \rangle} = M_{\langle \chi \rangle} = \{ m \in M; \chi(m) = 1 \}$; then $M_{\langle \chi \rangle} = \{ m \in M; \chi(m) = 1 \}$ and $M = \bigoplus_{\chi \in X} M_{\langle \chi \rangle}$ (direct product). By $\theta$ we shall denote the element of $X$ such that $\theta = \chi^{-1}$ for all $\chi$ in $T$, then $\theta = 0$ is an order $n$, so generates $X$. Furthermore let $\Delta = 1 - 1 - 1$ and $\eta = \Gamma^{-1} - 1 - 1 - 1$. $\eta$ is known to be a unit of $\mathbb{Z}[l]$ (cf. [3], proof of Proposition 4.1 and [10], Lemma II.6).

For each integer $i \geq 0$, we define

$$I_i = H(K)^{\langle \chi \rangle} / H(K)^{\langle \chi \rangle} = H(K)^{\langle \chi \rangle},$$

Then each $I_i$ is a $\mathbb{Z}[l]$-module and $I_i = 1$. Also $I_i = 1$ for all $i \geq 1$ since $\chi \in \mathbb{Z}[l]$. As the degree $(K : L) = n$ is prime to $l$ by our assumption (a), the inclusion map: $H(L) \rightarrow H(K)$ is injective, so $H(L)$ may be considered to be a subgroup of $H(K)$, and then $H(L) = H(K)^{\langle \chi \rangle}$, where $\chi$ is the trivial character in $X$.

**Lemma 1.1.** rank $H(L) = \sum_{i = 0}^{l - 2} \left[ \frac{l}{l^2} \right] = \left[ \frac{l}{l^2} \right]$.

**Proof.** Since $\chi$ is invertible in $\mathbb{Z}[l]$ and $H(L)^{\langle \chi \rangle} = 1$, then $H(L)^{\langle \chi \rangle} = H(K)^{\langle \chi \rangle}$, which implies the assertion of the lemma.

**Lemma 1.2.** rank $I_i^{\langle \chi \rangle} = s$, where $s$ is the number of rational primes ramified fully in $L$ and decomposed completely in $k$.

**Proof.** This is immediate from [11], Theorem 3.

Let $U$ be the kernel of the $\Delta$-map from $I_0$ onto $I_1$. It is easily seen that $e_\chi \Delta = de_\chi (\mod \Delta^2 \mathbb{Z}[l][G])$ (cf. e.g. [10], Proposition II.5 (iii)); so that the $\Delta$-map gives rise to an exact sequence

$$1 \rightarrow U \rightarrow I_0 \rightarrow I_1 \rightarrow 1,$$

and therefore

$$\text{rank } I_1^{\langle \chi \rangle} = \text{rank } I_0^{\langle \chi \rangle} - \text{rank } U^{\langle \chi \rangle}.$$

The norm map, $N$, from $K$ to $k$ induces a homomorphism of the group of ideals of $K$ to the group of ideals of $k$ and so of $H(K)$ to $H(k)$ and we shall denote these homomorphisms by $N$. Let $\mathcal{H}(k)$ be the kernel of $N$: $H(K) \rightarrow H(k)$, and let $\mathcal{J} = H(K)/H(k)$; then $\mathcal{H}(K)$ and $J$ are $\mathbb{Z}[l]$-modules, and $J = 1$ since $l \mid \delta \mathbb{Z}_l + 1 - 1$. If $K/k$ is unramified, then $J = 1$ (cf. e.g. [6]). In the case that $K/k$ is ramified, the genus number formula obtained by Jaulent ([11], Theorem 3) provides rank $J^{\langle \chi \rangle}$. To describe it we introduce some notations. Let $s_0$ denote the number of rational primes which are ramified fully in $L$ and whose decomposition groups in $k/\mathbb{Q}$ are of order $\leq 2$. We define

$$a = \begin{cases} 1, & \text{if } K/k \text{ is ramified and } l = 3, \\ 0, & \text{otherwise.} \end{cases}$$

Let $E(k)$ be the tensor product over $\mathbb{Z}$ of $E$, and of the group of units in $k$, and let $E = E(k)/E(k) \cap N K$; $E(k)$ and so $E$ are $\mathbb{Z}[l][G]$-modules. Then by the genus number formula,

$$\text{rank } J^{\langle \chi \rangle} = s_0 + a - \text{rank } E.$$
In particular if $K/k$ is unramified, $\psi$ is the trivial map since then $J = 1$.  

**Lemma 1.3.** We have 

$$\text{rank } I_0^{(0)} = \text{rank } H(k)^{(0)} + \text{rank } J^{(0)} - \text{rank } \psi(iH(k)^{(0)}).$$

**Proof.** Let $B = H(K)/H(K)^d$; then rank $I_0^{(0)} = \text{rank } (B^{(0)}/B^{(0)})$. The norm map $N$ gives rise to exact sequences:

$$1 \to J^{(0)} \to B^{(0)} \xrightarrow{N} H(k)^{(0)} \to 1,$$

and $D = \psi((H(K)^d/H(K)^{d})^0 \cap \overline{H}(K))$. As $$(H(K)^d/H(K)^{d})^0 = (H(K)^d)^0 \cap \overline{H}(K),$$ the kernel $D$ is the same as $\psi(iH(k)^{(0)} \cap \overline{H}(K))$. But by definition, $iH(k)^{(0)} \cap \overline{H}(K) = iH(k)^{(0)}$, so $D = \psi(iH(k)^{(0)})$. The above exact sequences now give the required result.

We conclude this section with the following

**Lemma 1.4.** Let $H$ be a $Z_1[T]$-submodule of $H(K)$. Then 

$$\text{rank } \psi(H^{(0)}) = \text{rank } \xi(NH^{(0)}) + \text{rank } \psi(H^{(0)}; H(k)^{(0)} \cap \overline{H}(K)) - \text{rank } \psi(iH(k)^{(0)}).$$

**Proof.** Since $(H(K)^d/H(K)^{d})^0 = (H(K)^d)^0 \cap \overline{H}(K)$, the module $\psi(H^{(0)})$ is isomorphic to $

\psi((H^{(0)}; H(k)^{(0)} \cap \overline{H}(K))$ where $\psi$ denotes the canonical homomorphism of $H(K)$ onto $H(K)/H(K)^d$. The norm map $N$ induces the following exact sequences:

$$1 \to \psi(iH(k)^{(0)} \cap \overline{H}(K)) \to \psi(iH(k)^{(0)} \cap \overline{H}(K)) \xrightarrow{N} N H^{(0)} H(k)^{(0)} \to 1,$$

and

$$1 \to \psi(iH(k)^{(0)} \cap \overline{H}(K)) \to \psi(iH(k)^{(0)} \cap \overline{H}(K)) \xrightarrow{N} H(k)^{(0)} \to 1.$$

Since $N H^{(0)} H(k)^{(0)}$ is isomorphic to $\xi(N H^{(0)})$, the lemma follows at once from these sequences.

2. **Lower bounds.** We use the foregoing notations. Let $H_1$ (resp. $H_1$) denote the set of elements $h$ in $H(K)$ with $h^d = 1$ (resp. $h^d H(K)^d$); they are $Z_1[G]$-modules. Since $H_1 H_1 = 1$ and $e_2 \delta \equiv \delta e_2 \mod{2} Z_1[G]$, it follows that $H_1^{(0)} = H_1^{(0)}$. For an ideal $a$ of $K$, we denote by $c(a)$ the ideal class of $K$ containing $a$. Let $H_1^a$ be the subgroup of $H(K)$ generated by the classes $c(a)$ with $a^d = a$; $H_1^a$ is also a $Z_1[G]$-module. Then, by [14], Theorem 1.8, $H_1^{(0)} = H_1^{(0)}$, and therefore $H_1^{(0)} = H_1^{(0)}$.

**Lemma 2.1.** Let as before $U$ be the kernel of the $\Delta$-map: 

$$I_0 = H(K)/H(K)^d H(K)^{d} \to I_1 = H(K)^d H(K)^{d} H(K)^{d} H(K)^{d}.$$ 

Then 

$$U^{(0)} = \phi(H_1^{(0)}).$$

**Proof.** Let $\overline{H}_1$ be the set of elements $h$ in $H(K)$ with $h^d H(K)^d$; then $U = \psi(\overline{H}_1^i)$, and so we want to show that $\phi(\overline{H}_1) = \phi(\overline{H}_1)$. First assume $h \in H_1$; then $(h^d - 1, h^{d-2}) - c = -c - 1$ for some $c \in H(K)$ since $l = \eta^{-1} d - 1 - \eta^{-1} d$. Putting $h_1 = h \eta^{-1} d - 1$ and $h_2 = c - 1$, we have $h_1^d = h_2^d$ and $h = h_1 h_2^d$; so that $h_1 \in H_1$ and $\phi(h) = \phi(h_1)$. Conversely assume $h_1 \in H_1$; then $h_1^d = h_2^d$ for some $h_2 \in H(K)$, and it is easy to see that $h \in H(K)$ where $h = h_1 h_2^d$; therefore $h_1 \in H_1$ and $\phi(h_1) = \phi(h)$. This completes the proof.

Now let $s$ be the number defined in Lemma 1.2, let $p_1, \ldots, p_s$ be the rational primes ramified fully in $L$ and decomposed completely in $k$, let $\pi_1$ be a prime ideal of $k$ above $p_1$, and let $\Phi_1$ be the unique prime ideal of $K$ above $p_1$. Let $\xi$ denote the order of the factor group $C/k(H)/H(K)$; $C/k$ being the full ideal class group of $k$. Let $\Gamma$ denote the subgroup of $H_1^{(0)}$, generated by the classes $c(\Phi_1^i)$, $1 \leq i \leq s$. Then $\Gamma$ is a $Z_1[T]$-module, and it is easily seen that $H_1^{(0)} = \Gamma H_1^{(0)}$.

Since $(H_1^{(0)}; H(K)^{d})^{(0)} = (H_1^{(0)} H(K)^{d})^{(0)}$, it follows from Lemma 2.1 that 

$$U^{(0)} = \phi(\Gamma).$$

So it is clear that

$$\text{rank } U^{(0)} = \text{rank } \phi(\Gamma) \leq s.$$

**Proposition 2.2.** With the foregoing notations, we have

$$\text{rank } I_0^{(0)} = s_0 - a - \text{rank } E^{(0)} + \text{rank } H(k)^{d}$$

$$- \text{rank } \psi(I_1 H(K)^{d} \cap H(K)) - \text{rank } \xi(N \Gamma)$$

$$\geq s_0 - s - a - \text{rank } E^{(0)} - \text{rank } H(k)^{d} - \text{rank } \psi(iH(k)^{(0)}).$$

**Proof.** By equation (1.1),

$$\text{rank } I_0^{(0)} = \text{rank } I_0^{(0)} - \text{rank } U^{(0)}.$$

By Lemma 1.3 and equation (1.2),

$$\text{rank } I_0^{(0)} = \text{rank } H(k)^{(0)} + s_0 - a - \text{rank } E^{(0)} - \text{rank } \psi(iH(k)^{(0)}).$$
Since rank \( U(\Theta) \leq s \) by equation (2.1), then rank \( l_1^{(2s)} \geq \text{rank} \, I^{(s)}_1 - s \). So the desired inequality in the proposition follows at once. Also by equation (2.1), rank \( U(\Theta) = \text{rank} \, \varphi(I) \). But if we apply Lemma 1.4 to the \( \mathbb{Z} \Gamma \)-module \( I \), then

\[
\text{rank} \, \varphi(\Gamma) = \text{rank} \, \psi(\Gamma; H(k)^{(0)} \cap H(K)) - \text{rank} \, \psi(I; H(k)^{(0)}) + \text{rank} \, \xi(N \Gamma),
\]

which together with equation (2.2) provides the desired equality in the proposition.

Combining Lemmas 1.1, 1.2 and 2.2 yields the following

**Theorem 2.3.** We have

\[
\text{rank} \, H(L) \geq s + s_0 - a - \text{rank} \, E^{(s)} + \text{rank} \, H(k)^{(s)} - \text{rank} \, \psi(\Gamma; H(k)^{(0)} \cap H(K)) - \text{rank} \, \xi(N \Gamma)
\]

\[
\geq s + s_0 - a - \text{rank} \, E^{(s)} + \text{rank} \, H(k)^{(s)} - \text{rank} \, \psi(\Gamma; H(k)^{(0)}) - \text{rank} \, \xi(N \Gamma).
\]

Of special interest is the pure field case, \( L = \mathbb{Q}(\sqrt[\delta]{m}) \) where \( m \) is an \( \delta \)-th power-free rational integer. In this case the number \( s \) (resp. \( s_0 \)) is precisely the number of prime factors \( \equiv 1 \pmod{l} \) (resp. \( \equiv 1 \pmod{l} \)) of \( m \). Also \( E(k)^{(0)} = 1 \) or \( \Theta \) according as \( l \neq 3 \) or \( l = 3 \), where \( \Theta \) is a primitive cube root of unity (cf. [14], §1); in the cubic case it is known that rank \( E(k)^{(0)} = 0 \) or 1 according to whether or not every prime factor \( \neq 3 \) of \( m \) is congruent to \( \pm 1 \pmod{9} \) (cf. [7]). Furthermore the extension \( K/k \) in which \( k \) is the \( \delta \)-th cyclotomic field and \( K = k(\sqrt[\delta]{m}) \) is of course ramified. Therefore Theorem 2.3 then provides

**Corollary.** Let \( L = \mathbb{Q}(\sqrt[\delta]{m}) \) be a pure field of degree \( \delta \) where \( m \) is an \( \delta \)-th power-free rational integer. Then

\[
\text{rank} \, H(L) \geq s + s_0 - \text{rank} \, H(k)^{(s)} - \text{rank} \, \psi(\Gamma; H(k)^{(0)} \cap H(K)) - \text{rank} \, \xi(N \Gamma)
\]

\[
\geq s + s_0 - \text{rank} \, H(k)^{(s)} - \text{rank} \, \psi(I; H(k)^{(0)})
\]

\[
\geq s + s_0 - a - \text{rank} \, \psi(\Gamma) \quad \text{if} \quad l \neq 3.
\]

Here \( s \) (resp. \( s_0 \)) is the number of primes \( \equiv 1 \pmod{l} \) (resp. \( \equiv 1 \pmod{l} \)) dividing \( m \), and \( a \neq 0 \) or 1 according to whether or not every prime factor \( \neq 3 \) of \( m \) is congruent to \( \pm 1 \pmod{9} \).

**Remark.** The rank formula in the cubic case \( l = 3 \) in the corollary has been already obtained, independently of each other, by Gerth [2], Gras [4], and Kobayashi [12]. The corollary applies to the pure quintic case \( l = 5 \) to show that if at least one prime \( \equiv -1 \pmod{5} \) divides \( m \), then the class number of the pure quintic field \( L = \mathbb{Q}(\sqrt[\delta]{m}) \) is a multiple of 5; but this follows also from Theorems 1, 2 and 3 in [11], and gives an answer to one of the question raised in [8].

3. **Computation of the ranks of** \( \psi(\Gamma; H(k)^{(0)} \cap H(K)) \) **and** \( \psi(I; H(k)^{(0)}) \).

In this section we interpret the ranks in terms of the ranks of certain matrices whose elements are in the finite field \( F_l \) of \( l \) elements. We put \( V = \Gamma; H(k)^{(0)} \cap H(K) \) and \( W = I; H(k)^{(0)} \). By virtue of [5], Theorem 1, rank \( \psi(V) \) and rank \( \psi(W) \) appearing in our lower bounds can be expressed as follows. Let \( \alpha_1, \ldots, \alpha_l \) be the prime ideals of \( k \) ramified fully in \( K \), \( \alpha \), \( \beta \), \( \Gamma \), \( \Delta \), \( \Theta \) be the norm residue symbol at a prime \( q \) of \( k \) in the cyclic extension \( K/k \) (as to its definition and properties see [5], Part II, §6), and let \( \lambda_q : k^* \to S = G(K/k) \) be the homomorphism defined by \( \lambda_q(\gamma) = (\gamma, K/k) = \gamma \pmod{\Gamma} \), \( \gamma \in k^* \). Let \( s_1, \ldots, s_\delta \) (resp. \( \beta_1, \beta_2 \) ) be elements of \( k^* \) such that the classes \( c(N_\delta^{-1}(s_\delta)) \) and \( c(N^{-1}(\beta_1, \beta_2)) \) generate \( V \) and \( W \), respectively, for \( N \delta \), \( N \) denotes the inverse for \( N \) and \( \delta \) denotes the principal ideal of \( k \) generated by \( \delta \). Then \( \{s_1, \ldots, s_\delta \} \) is a set of generators for \( \Delta \).

For these \( \alpha_1 \)'s (resp. \( \beta_1 \)'s; \( \gamma_1 \)'s), we denote by \( M \) (resp. \( M_\delta \); \( M \delta \)) the \( n \times t \) (resp. \( \infty \times t \); \( \infty \times \infty \)) matrix with \( i \), \( j \) component \( \lambda_q(2) \) (resp. \( \lambda_q(1) \); \( \lambda_q(2) \)) and let

\[
\psi(V) = \left( M \right), \quad \psi(W) = \left( M_\delta \right).
\]

Then it follows easily from [5], Theorem 1, that

\[
\text{rank} \, \psi(V) = \gamma \text{rank} \, \psi(M), \quad \text{rank} \, \psi(W) = \gamma \text{rank} \, \psi(M_\delta),
\]

where \( M \), \( M_\delta \) and \( M \delta \) all may be viewed in the obvious manner as matrices over the field \( F_l \). Their ranks, of course, are independent of the choice of the \( \alpha \)'s, \( \beta \)'s and \( \gamma \)'s.

Now we let \( \overline{\alpha} \) be an element of \( Z \) such that \( \overline{\alpha} \equiv \overline{e}(mod \mathbb{Z} \Gamma \mathbb{Z}[T]) \), and let \( \overline{\alpha} \) : \( T \to \mathbb{Z} \) be the map given by \( \overline{\alpha}(\delta) : \overline{\alpha}(\gamma) = \overline{\delta}(\gamma) \). Now \( \overline{\alpha} \) is defined for all \( q \in T \) and for all \( \alpha \in k^* \) and for all \( \alpha \in T \), we have

\[
\overline{\alpha} : \overline{\alpha}(\gamma) = \overline{\gamma}(\delta) = (\gamma, \delta) \text{ for all } \gamma \in k^*.
\]

As is easily seen, the \( \alpha \)'s (resp. \( \beta \)'s; \( \gamma \)'s), we may write \( \alpha_1 \) (resp. \( \beta_1 \); \( \gamma_1 \)) instead of \( \alpha_1 \) (resp. \( \beta_1 \); \( \gamma_1 \)) and then each one of them, say \( \gamma \), satisfies \( \gamma \equiv \overline{\gamma}(\delta) \text{ for all } \gamma \in k^* \). From this and the basic properties of the norm residue symbol it follows that for all \( \gamma \in T \) and all \( q \in k^* \), the \( \lambda_q : k^* \to S = G(k/q) \) has an order other than 1 or 2, then \( \lambda_q(1) = 1 \). Let \( p_1, \ldots, p_\delta \) be defined as in Section 2, let \( p_\delta + 1, \ldots, p_\delta \) be the rational primes which are ramified fully in \( L \) and whose decomposition groups in \( G(k/Q) \) are of order 2, and let \( \psi(s) \leq s \leq s_\delta \), then be a prime ideal of \( k \) above \( p_1 \).

\[
\psi(\overline{\alpha}) = \left( M_\delta \right), \quad \psi(V) = \left( M \right), \quad \psi(W) = \left( M_\delta \right).
\]

\[
\psi(V) = \left( M \right), \quad \psi(W) = \left( M_\delta \right).
\]
matrix with $i, j$ component $\lambda_{ij}(a_i)$ (resp. $\lambda_{ij}(b_i)$), and let $\tilde{M}_v = \left( \begin{array}{c} \tilde{m}_v \\ \tilde{M}_w \end{array} \right)$. Then it follows from the above that

\[ \text{rank } \psi(V) = \text{rank } \tilde{M}_v - \text{rank } \tilde{M}, \]
\[ \text{rank } \psi(W) = \text{rank } \tilde{M}_w - \text{rank } \tilde{M}. \]

So our next task is to consider each $\lambda_{ij}$, $1 \leq j \leq s_0$. Call $p$ one of these primes $p_1$'s, let $p$ be the rational prime below $p$, and let $k_p$ (resp. $Q_p$) denote the completion of $k$ (resp. $Q$) at $p$ (resp. $p$). Then the compositum $K/k$ is a cyclic extension of $k_p$ of degree $l$. Let $J_p$ denote the subgroup of $k_p^\times$ corresponding to the cyclic extension $K/k$. In the natural manner, we may regard $J_p$ as a homomorphism of $k^\times$ to $k_p^\times$. So we are now interested only in the group $J_p$. To examine it, we use some facts which may be found in [13]. Let $f$ be the conductor of the cyclic extension $K/k$; then $f = f$. We distinguish the following five cases.

Case 1. $p \neq l$ and $p \notin \{p_1, \ldots, p_l\}$; in this case $k_p = Q_p$ and $p \equiv 1 \pmod{f}$. Also $p||f$.

Case 2. $p = l \in \{p_1, \ldots, p_l\}$. Write $p = 1$; then $k_p = Q_p$ and $p || f$.

Case 3. $p \neq l$ and $p \notin \{p_1, \ldots, p_q\}$, in which case $k_p/Q_p$ is a quadratic unramified extension and $p \equiv -1 \pmod{f}$. Also $p||f$.

Case 4. $p = l \in \{p_1, \ldots, p_q\}$ and $k_p/Q_p$ is a quadratic unramified extension. In this case $l|f$.

Case 5. $p \neq l \in \{p_1, \ldots, p_q\}$, and $k_p/Q_p$ is a quadratic ramified extension. If $l > 3$, then $l|f$. If $l = 3$, then either $l || f$ or $l || f$; but in this case the Hasse's product formula for the norm residue symbol enables us to delete the column of the matrices $M, \tilde{M}_v$, and $\tilde{M}_w$ that involves the prime $l$, and so we may leave out this cubic case.

Now we let, for each integer $i \geq 1$,

\[ U_{i}^{(0)} = \{ x \in k_p^\times : x \equiv 1 \pmod{p^i} \}, \]

let $U_p = \{ x \in k^\times : x \equiv 1 \pmod{p} \}$ be the $p$-units, and let $\zeta_m$ be a primitive $m$th root of unity contained in $k^\times$.

Case 3. In this case it is seen that

\[ J_p = \langle \xi \rangle \times \xi^{-1} \times U_p^{(0)}. \]

In fact $p || f$ means that $U_p^{(0)} = J_p$. Since the extension $L/k$ is nonabelian of degree $l$, local class field theory shows that $Q_p^\times = J_p$. Also this extension is tamely ramified, so we have $L \cdot Q_p = P_{p^i} = \xi \langle \xi \rangle \times \xi^{-1} \times U_p^{(0)}$ for some $d \in Q_p^\times$, which implies that $d \in J_p$. As the index of the group $\langle \xi \rangle \times \xi^{-1} \times U_p^{(0)}$ is exactly $l$, it must coincide with $J_p$.

Case 4. An argument similar to the above shows that

\[ J_p = \langle \pi \rangle \times \langle \pi^{-1} \rangle \times U_p^{(0)} \]

Case 5. In this case there is an element $\pi$ of $k^\times$ such that $\pi^2 \in \mathbb{Z}$, and $k_i = Q_i(\pi)$. Then we have

\[ J_p = \langle \pi \rangle \times \langle \pi^{-1} \rangle \times U_p^{(0)} \]

Case 6. $k_i$ is an extension of $k$ such that $\pi^2 \in \mathbb{Z}$, and $k_i = Q_i(\pi)$. Then we have

\[ J_p = \langle \pi \rangle \times \langle \pi^{-1} \rangle \times U_p^{(0)} \]

Let $I(f)$ be the group of ideals of $k$ prime to $f$, and let $J$ denote the congruence subgroup of $I(f)$ corresponding to the cyclic extension $K/k$ in the sense of global class field theory. We shall show that the complete determination of the number $\mu_i$ may be done when the congruence group $J$ is given. Let $f' = |f|$, and let $I(f')$ be the group of ideals of $k$ prime to $f'$. As $|p|f'$ is prime to $p$, and so $I(f') \subseteq I(f)$. Let $P(f') = \{ \alpha \}; \alpha \equiv k \times, \alpha \equiv 1 \pmod{f'}$. And $P(f) = \{ \alpha \}; \alpha \equiv k \times, \alpha \equiv 1 \pmod{f'}$. Since the conductor of $J$ is $f$, then $I(f^t) \subseteq J$, and so $J(f^t) \supseteq P(f)$. This implies that $I(f) = J(f^t)$ since $f$ is of index 1 in $f$. Also the canonical homomorphism of $I(f)$ to $P(f)$ is surjective. Hence it follows that

\[ I(f) = I(f) \cap P(f) \]

and therefore there is an element $\omega_i$ of $k^\times$ such that $\omega_i \equiv 1 \pmod{f}$, and $\omega_i \equiv 1 \pmod{f'}$. Since $f_i$ is $n$, put $\omega_i = (\omega_i)^{n-1}$; then $\omega_i \equiv 1 \pmod{f}$. By the definition of the norm residue symbol in [2], Part III, § 6, we have

\[ u_i, K/k = \left( \frac{K/k}{\omega_i} \right) \]

where $\left( \frac{K/k}{\omega_i} \right)$ denotes the Artin symbol of $K/k$. From this it follows that

\[ u_i \equiv \omega_i \equiv 1 \pmod{f} \]

But it is clear that $\omega_i \equiv 1 \pmod{f}$. Also we have $u_i \equiv 1 \pmod{f'}$, since $u_i \equiv 1 \pmod{f}$ and $u_i \equiv 1 \pmod{f'}$. Thus we conclude that $u_i$ satisfies $(\omega_i, u_i) \equiv 1 \pmod{f}$, and accordingly we may set $u_i = \omega_i$. As was shown in [13], the congruence group $J$ can be defined by a linear
functional on the $F_l$-space $(\mathcal{O}/f)^* / (\mathcal{O}/f)^*$ where $\mathcal{O}$ is the ring of integers in $k$ and $(\mathcal{O}/f)^*$ is the group of units in the factor ring $\mathcal{O}/f$. Hence in Case 1 the linear functional attached to the congruence group $J$ enables one to determine completely the group $J_f$.

**Case 2.** In this case $J_f$ is written in the form

$$J_f = \langle (1 + \mu_l f) \times (\mathbb{Z}_{\geq 1}) \times U(2) \rangle$$

where $\mu \in \mathbb{Z}$, $1 \leq \mu_l \leq l$. There are $l$ subgroups of $k^*$ of such form. As in Case 1, if we let $a_0$ be an element of $k^*$ such that $(a_0) \in J$ (such $a_0$ does exist) and if we let $a_l$, $1 \leq l \leq l$, be elements of $k^*$ such that $\forall l \geq 1$ (mod $l!$) then it is seen that $l (1 + i l)$ (mod $l^2$) then it is seen that $1 (1 + i l)$ (mod $l$) $\in J$. And so the linear functional attached to the congruence group $J$ enables one to determine completely the group $J_f$. Of course, it would not be hard to express the above numbers $\mu_l$ and $\mu_0$ by means of the coefficients of the linear functional, but we shall not explain it here.

Now we mention how to find the numbers $\alpha$'s and $\beta$'s defined above. For an ideal $\alpha$ of $k$, let $c'(\alpha)$ denote the ideal class of $k$ containing $\alpha$. Let $b_1, \ldots, b_s$ be ideals of $k$ whose classes $c'(b_i)$ generate the group $H(k)^{\infty} / \{ \epsilon \in H(k)^{\infty} : \epsilon = 1 \}$ for each $i$, we write $b_i = (b_i)$ with $b_i = k^*$. In view of the definition of $\beta$'s, we may choose $\beta$'s as the $b$'s. As is well known, the ideals $b$'s and hence $\beta$'s may be chosen to be prime to the ideal $1$; then the $\beta$'s are also prime to $\mathfrak{p}$ since $\mathfrak{p} = 1$. The restriction of the homomorphism $\lambda : k^* \to k^*$, to the group $k^* \cap U_f$ induces the homomorphism $\lambda^* : k^* \cap U_f / (\epsilon)$. Our result about $J_f$ described above shows that the group $J_f \cap U_f$ also depends only on a pair $(k, f)$ (though $J_f$ itself does not always). So by choosing these $\beta$'s prime to $\mathfrak{f}$, we conclude that rank $\psi(W)$ depends only on the pair $(k, f)$; namely if we denote by $K_i$, $i = 1, 2$, metacyclic extensions of $Q$ with the same maximal abelian subfield $k$ and with the same conductor $f$ over $k$, then with respect to these fields $K_1$ and $K_2$ both $\lambda(W)$ are the same, and therefore so are both of the second lower bounds in Theorem 2.3 that involve these ranks.

To find the numbers $\alpha$'s associated with the group $\Gamma = \Gamma (H(k)^{\infty} / \mathfrak{p} H(K))$, we must recall the definition of the group $\Gamma$ described in Section 2, where $\Gamma$ was defined to be $\langle \langle \alpha' \langle \alpha(1) \rangle, \ldots, \alpha'(a_0) \rangle = H(k)^{\infty} \rangle$, and let $P_k$ denote the group of principal ideals in $k$. If we let $(a_1), \ldots, (a_s)$ be generators for the factor group

$$\langle \langle \alpha' \langle \alpha(1) \rangle, \ldots, \alpha'(a_0) \rangle = H(k)^{\infty} \rangle \quad \text{for } 1 \leq i \leq s, \quad \text{and } 1 \leq l \leq r \rangle \cap P_k \rangle,$$

it follows from the above that these numbers $a_1, \ldots, a_s$ may be chosen as the $a$'s in question.

We conclude this section with a remark about the congruence subgroup $J_f$. A defining polynomial of $L$ over $Q$, if known, enables one to determine immediately $J_f$, in our Cases 1 and 2 (cf. [9]).

**4. Examples.** As our first example, we let $k/Q$ be a quadratic extension with class number 1. Let $p_1, p_2$ be distinct rational primes $\equiv 1$ (mod $l$) which are completely decomposed in $k$; we let $f = p_1 p_2$, and assume that every units of $k$ are $l$-th power residues mod $f$. Let $G$ be the ring of integers in $k$, and let $Y = (\mathcal{O}/f)^*/(\mathcal{O}/f)^*$, which may be viewed as a $F_l$-space. Then $Y$ is a $F_l[\gamma]$-module where $\gamma$ is the generator for the Galois group $G(k/Q)$, and $Y \cong F_l$. Before we let $t(f)$ denote the group of ideals of $l$ prime to $f$, we let $F(f) = \langle \gamma \rangle$, $\gamma \equiv 1$ (mod $f$), and set $C = t(f)/F(f)$. Then it follows from our assumption on the units of $k$ that $Y$ is $F_l[\gamma]$-isomorphic onto $C/C' \cong F_l$ through a map $\psi$ defined by $\psi(\gamma) = (y)$ for every $y \in Y$. Let $Y' = \langle \gamma \in Y, y' \equiv y \pmod{f} \rangle$; then $Y' \cong F_l'$. For $i = 1, 2$, we denote by $\gamma_i$ a generator for the group $(Z/p_i Z)$. Take $x_1 \in k^*$ such that $x_1 \equiv r_1 (\mod p_1)$ and $x_2 \equiv 1 (\mod p_2)$; take $x_2 \in k^*$ such that $x_2 \equiv 1 (\mod p_1)$ and $x_2 \equiv 1 (\mod f)$. Then $\langle x_1, x_2 \rangle$ is a $F_l$-basis for $Y'$. Furthermore, take $x_2 \in k^*$ such that $x_2 \equiv r_1 (\mod p_2)$, $x_1 \equiv r_2 (\mod p_1)$ and $x_2 \equiv 1 (\mod f)$; then $x_2 \equiv p_2 (\mod p_1)$, and for $i = 1, 2$, $p_i$ is a prime ideal of $k$ above $p_i$. Then $\langle x_1, x_2 \rangle$ is a $F_l$-basis for $Y'$. Let $J$ be the set of congruence subgroups of $J(f)$ with the following properties: $J$ contains $P(f)$, is of index $l$ in $J(f)$, and has a conductor $f$, and the abelian extension $K_f$ of $k$ that corresponds to $J$ is dihedral of degree $2l$ over $Q$. For $1 \leq j \leq l - 1$, let $Y_j$ be the subgroup of $Y$ generated by $Y$ and by $(x_j x_{l-j} \mod f)$. Then it is easily seen that $J = \{Y, Y_j, 1 \leq j \leq l - 1\}$, and so there are precisely $(l - 1)$ dihedral extensions of $Q$ with the given conductor $f$ over $k$. Now fixing $j$, put $J = Y_j$, and $x = x_{l-j}$. For $i = 1, 2$, write $\alpha_i = (x_i) \in J$, and put $\alpha_i = p_i (\mod p_1)$, $x_i \equiv p_2 (\mod f)$. Clearly we can pick for $i = 1, 2$, $x_i \equiv p_i (\mod f)$, and $x_i \equiv 1 (\mod f)$, and $x_i \equiv 1 (\mod f)$. However, from the Hasse's product formula for the norm residue symbol we have for $i = 1, 2$:

$$\alpha_i (\alpha_i^{-1}) \cdot \lambda_{l-i} (\alpha_i^{-1}) = 1.$$
(mod p_1^2)]; then \( u_0 \equiv p_1 b_1 \epsilon^{-1} r_1^{-1} z^{-1} \) (mod \( p_1^2 \)). On the other hand it follows from \( \alpha_{1,1}^x = p_1 a_1 \) that \( b \equiv a_1 r_1^{-1} \epsilon_1 x^{-1} \) (mod \( p_1^2 \)). Hence \( u_0 \equiv p_1 r_1^{-2} z^{-1} x^{-1} \) (mod \( p_1^2 \)), so that \( p_1 r_1^{-2} z^{-1} x^{-1} \in J_{p_1} \), which implies that \( J_{p_1} = \langle p_1 r_1^{-2} z^{-1} x^{-1} \rangle \times U_{p_1}^1 \). Considering the map \( \lambda_{\gamma_1} \) to be a homomorphism of \( k^* \) to the factor group \( k^*/J_{p_1} \), we have from the above that \( \lambda_{\gamma_1} (\alpha_{1,1}^x) = (r_1^{2} \epsilon_1 \mod J_{p_1}) \).

In view of the definition of \( e_2 \), it is clear that its vanishing is independent of the choice of \( J \) in \( \mathcal{J} \), and therefore so is rank \( \langle \lambda_{\gamma_1} (\alpha_{1,1}^x) \rangle \). But this follows also from the fact that \( \lambda_{\gamma_1} (\alpha_{1,1}^x) = \lambda_{\gamma_2} (\alpha_{1,1}^x)^{-1} \), which was a consequence of the Hasse's product formula. Thus rank \( \psi(V) \) and hence the first lower bound in Theorem 2.3 that involves this rank are independent of the choice of \( J \) in \( \mathcal{J} \). (Note that rank \( \psi(V) = \text{rank} \langle \lambda_{\gamma_1} (\alpha_{1,1}^x), \lambda_{\gamma_2} (\alpha_{1,1}^x) \rangle \) by means of the product formula.)

For our next example we let \( L = \mathbb{Q}(\sqrt[p]{p}) \) where \( p = (c_0 + c_1)^{(n+1)} \) is a prime, \( n \geq 5 \), and \( c_0, c_1 \in \mathbb{Z} \). Let \( \zeta \) be a primitive \( l \)th root of unity, \( k = \mathbb{Q}(\zeta) \), and \( P(X) = c_0 + c_1 X \). Then \( p \) is a norm of \( P(\zeta) \), and so \( p \equiv 1 \mod \ell \). Also \( p \equiv (P(\zeta)) \) is a prime ideal of \( k \) above \( p \). Let \( r \) be a generator for the group \( (\mathbb{Z}/l\mathbb{Z})^* \), and \( \tau \) be a generator for the Galois group \( G(k/\mathbb{Q}) \) defined by \( \zeta \equiv \zeta^p \).

As before we denote by \( e \) the idempotent of \( \mathbb{Z}_l[G(k/\mathbb{Q})] \) attached to the character \( \theta \); in this case \( e \) is defined by \( \theta^l = 1 \equiv (\mod \ell) \). So putting \( g(X) = \sum_{i=0}^{l-1} r_1 X^i \) where \( 0 \leq i \leq l-2 \), \( r_1 \in \mathbb{Z} \) are chosen such that \( 1 \leq r_1 \leq l-1 \) and \( r_1 \equiv r \) (mod \( \ell \)), we have \( e \equiv -g(r) \) (mod \( \ell \)). Put \( n(X) = \sum_{i=0}^{l-1} X^i \) and \( f(X) = g(X) - n(X) \). For elements \( \gamma_1, \gamma_2 \) of \( k^* \) both prime to \( p \), \( \gamma_1 \equiv \gamma_2 \) (mod \( p \)) means that \( \gamma_1 \gamma_2^{-1} \) is an \( l \)th power residue mod \( p \). Then it follows from the properties of the norm residue symbol that

\[
P(\zeta)^{l} = n^{l-1} \mod \ell \]

As will be seen below, the latter condition is equivalent to saying that \( c_0 + c_1 \equiv 1 \mod \ell \), or, what amounts to the same, \( (c_0 + c_1)^{(n+1)l} \equiv 1 \mod \ell \). Put

\[
Q(X) = \prod_{i=1}^{l-2} (c_0 + c_1 X^i)^{n+1} \mod \ell \]

then \( Q(\zeta) = P(\zeta)^{n+1} \). Furthermore put

\[
c = \prod_{i=1}^{l-2} (c_0 + c_1 X^i)^{n+1} \mod \ell \]

and \( R(X) = cQ(X) \); 

since \( \zeta \equiv -c_0/c_1 \) (mod \( p \)), then \( R(\zeta) \equiv R(-c_0/c_1) \) (mod \( p \)). Let \( \mathcal{A} = \{ j \} \), \( 1 \leq j \leq l-2 \}, \mathcal{A} = \{ 2, 3, \ldots, l-1 \}, \mathcal{A} = \{ j \} \in \mathcal{A}, \mathcal{A} = \{ j \} \in \mathcal{A} \). In the following the product \( \prod \) and summation \( \sum \) are only taken over all \( j \in \mathcal{A} \), the product \( \prod \) over all \( \{ j \} \in \mathcal{A} \), and the summation \( \sum \) over all \( j \in \mathcal{A} \). Putting \( d = -c_0 \), we have

\[
R(-c_0/c_1) = d(d-c_1) \prod_{j \in \mathcal{A}} d^j \prod_{j \in \mathcal{A}} (d^j - c_1^j)^{l-1} \prod_{j \in \mathcal{A}} (d^j - c_1^j)^{l-1} \mod p \]

But, for each \( \{ j \} \in \mathcal{A} \),

\[
d^j d^j (d^j - c_1^j)^{l-1} \equiv d(d-c_1) \prod_{j \in \mathcal{A}} d^j \prod_{j \in \mathcal{A}} (d^j - c_1^j)^{l-1} \mod p \]

Therefore

\[
Q(\zeta) = d(d-c_1) \prod_{j \in \mathcal{A}} d^j \prod_{j \in \mathcal{A}} (d^j - c_1^j)^{l-1} \mod p \]

Since \( l \geq 5 \), then \( 1 + \sum d^j \equiv 0 \) (mod \( \ell \)), which implies that

\[
\prod d^j d^j \equiv \prod d^j \prod (d^j - c_1^j)^{l-1} \mod p \]

Also

\[
\prod j^2 \equiv (1 + \sum d^j)^2 \equiv \sum (d^j - c_1^j)^{l-1} \mod p \]

so that

\[
\nu \equiv \prod c_1^2 \mod p \]

Thus we conclude from the above that

\[
Q(\zeta) \equiv d - c_1 \equiv c_0 + c_1 \mod p \]

which was to be shown.

Now we assume that \( (c_0 + c_1)^{(n+1)l} \equiv 1 \mod p \). Let \( \Gamma \) be as defined in Section 2, and let \( \Psi \) be the unique prime ideal of \( k = \mathbb{Q}(\zeta) \) above \( p = (P(\zeta)) \); then \( \Gamma \) is generated by \( c(\Psi)^l \), and so \( N \Gamma = 1 \), which implies that \( V = \Gamma \cdot \mathbb{A}(k) = \Gamma \). Then \( (P(\zeta)^l, K/k) = 1 \) implies that \( \text{rank} \psi(V) \)
Therefore the first lower bound for rank \( H(Q(\sqrt[3]{p})) \) in the corollary to Theorem 2.3 becomes \( 2+\text{rank } H(k) - \text{rank } (W) \); in particular this says that the \( l \)-class group \( H(Q(\sqrt[3]{p})) \) is not cyclic.

References

[7] T. Honda, Pure cubic fields whose class numbers are multiples of \( 3 \), ibid. 3 (1971), pp. 7–12.

Received on 31. 1. 1985
and in revised form on 15. 5. 1985

LeVeque’s superelliptic equation over function fields

by

R. C. Mason (Cambridge) and B. Brindza (Debrecen)

I. Introduction. In a letter to Mordell written in 1925, later published, Siegel [9] proved that the hyperelliptic equation \( y^2 = g(x) \) has only finitely many solutions in integers \( x \) and \( y \): \( g \) denotes a polynomial with integer coefficients, possessing at least three simple zeros. Siegel’s later investigations revealed his celebrated theorem [10] concerning the solutions of any polynomial equation \( F(x, y) = 0 \); he proved that there are only finitely many integer solutions, unless the curve associated with \( F \) has genus zero and no more than two infinite valuations. Siegel’s proof was ineffective: he employed both the Mordell–Weil theorem and his own theorem on the approximation of algebraic numbers by rationals, which was a development of the pioneering work of Thue. In 1964 LeVeque [3] generalized Siegel’s result on the hyperelliptic equation to prove that the superelliptic equation \( y^n = f(x) \) has only finitely many solutions in any ring of algebraic integers, unless of course it falls into the exceptional cases predicted by Siegel’s general theorem. The conditions on \( f \) and \( m \) equivalent to the exceptional cases are given below (A). LeVeque’s result was ineffective. In 1968 Baker proved the first general effective result on Diophantine equations by employing his celebrated lower bound for linear forms in logarithms: he effectively solved first the Thue equation, and then the hyperelliptic and certain superelliptic equations [1]. Baker’s bounds were improved by Sprindžuk [11], [12]. LeVeque’s theorem of 1964 was recently made completely effective by Brindza [2].

This paper is devoted to establishing a bound on the solutions of LeVeque’s equation in the analogous case of function fields. Let \( k \) denote an algebraically closed field of characteristic zero, and \( k(z) \) the rational function field over \( k \). Let us consider the set of solutions \( X, Y \) in the ring of polynomials \( k[z] \) of the hyperelliptic equation \( Y^2 = G(X) \), where \( G \) is a polynomial with coefficients in \( k[z] \) and possessing at least three simple zeros. It is plainly possible for this equation to have infinitely many solutions, for example if the coefficients of \( G \) actually lie in \( k \). However, it is