

CONGRUENCE OF ANKENY–ARTIN–CHOWLA TYPE MODULO p^2

STANISLAV JAKUBEC AND MIROSLAV LAŠŠÁK

Abstract. In this paper the results of [4] and [5] on the congruence of Ankeny–Artin–Chowla type modulo p^2 for real subfields of the $\mathbf{Q}(\zeta_p)$ of a prime degree $l > 2$ are simplified to explicit forms (2) and (3) of the Theorem 1. The congruence is then used to calculations of class numbers in special quintic fields and to some calculations in cubic fields.

Notation

B_n, E_n – Bernoulli and Euler numbers,

$$C_n = \frac{2^{n+1}(1-2^{n+1})B_{n+1}}{n+1},$$

$$Q_2 = \frac{2^{p-1}-1}{p} - \text{Fermat quotient},$$

$$W_p = \frac{1+(p-1)!}{p} - \text{Wilson quotient},$$

$$A_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}, \quad A_0 = 0,$$

U_K – the group of units of the field K ,

$\langle \delta \rangle$ – the group generated by all conjugates of a unit δ .

Introduction

Let p be a prime $p \equiv 1 \pmod{4}$ and let $T + U\sqrt{p} > 1$ be the fundamental unit of the quadratic field $\mathbf{Q}(\sqrt{p})$ and let h be its class number. Then the Ankeny–Artin–Chowla congruence is

$$h \frac{U}{T} \equiv B_{\frac{p-1}{2}} \pmod{p}.$$

Received on August 31, 1998.

1991 Mathematics Subject Classification. 11R29.

Key words and phrases: Class number, subfields of cyclotomic fields.

Since $h < p$, the class number h is uniquely determined by this congruence if $B_{\frac{p-1}{2}} \not\equiv 0 \pmod{p}$. Note that no prime p is known with $B_{\frac{p-1}{2}} \equiv 0 \pmod{p}$.

Let $p \equiv 1 \pmod{l}$ and let K be a subfield of the field $\mathbf{Q}(\zeta_p)$ of prime degree $l > 2$ and let δ be a unit of K such that $[U_K : \langle \delta \rangle] = f$, $(f, p) = 1$. Then by [3]

$$(1) \quad \frac{h_K}{f} S_1 \cdots S_{l-1} \equiv \left(\frac{-1}{l} \right) \frac{l}{2^{l-1}} B_{\frac{p-1}{l}} \cdots B_{\frac{(l-1)(p-1)}{l}} \pmod{p},$$

where h_K is the class number of K and S_1, \dots, S_{l-1} are rational functions dependent on the unit δ . If $f = 1$ then the unit δ is called a strong Minkowski unit, and then $(f, p) = 1$ is trivially satisfied. But the existence of a strong Minkowski unit is not known in general. According to the Theorem 3.10 of [7] such a unit exists in any cyclic field of prime degree $l < 23$. Note that the existence of a unit δ such that $(f, p) = 1$ is proved in the paper [2].

The aim of this paper is to prove the congruence of Ankeny–Artin–Chowla type modulo p^2 . The following examples demonstrate the usefulness of such a congruence.

Let $p \equiv 1 \pmod{3}$, K be a cubic subfield of the field $\mathbf{Q}(\zeta_p)$ and let $\delta, \sigma(\delta)$ be fundamental units of the field K , i. e. $f = 1$. If

$$B_{\frac{p-1}{3}} B_{\frac{2(p-1)}{3}} \not\equiv 0 \pmod{p},$$

then the class number h_K is uniquely determined by (1) because $h_K < p$. By [1] there is just one prime $p < 1000000$ with the property that $B_{\frac{p-1}{3}} B_{\frac{2(p-1)}{3}} \equiv 0 \pmod{p}$, namely $p = 5479$.

Let $p \equiv 1 \pmod{5}$ and let K be the quintic subfield of the field $\mathbf{Q}(\zeta_p)$ and let $\delta, \sigma(\delta), \sigma^2(\delta), \sigma^3(\delta)$ be fundamental units ($f = 1$). Since the inequality $h_K < p$ is not satisfied for all such fields so the congruence (1) is not sufficient to determine h_K .

The main result of the paper is the Theorem 1 which gives the congruence of Ankeny–Artin–Chowla type modulo p^2 in explicit form. This congruence is an essential simplification of [5]. If we take the congruence only modulo p we get directly (1).

The last section gives two applications of this congruence. In the first application, quintic fields of prime conductor $p = n^4 + 5n^3 + 15n^2 + 25n + 25$ are taken. In the paper [8] Schoof and Washington proved that the conjugates of a unit γ_0 (defined later) are fundamental units of K . So by means of the congruence (2) we calculated the class numbers h_K modulo p^2 for those fields for all prime conductors less than 10^9 . Schoof and Washington calculated

class number h_K for the first 26 fields of this type. For calculations they used Dirichlet's class number formula

$$h_K R_K = \frac{1}{16} \prod_{\chi \neq 1} \sqrt{p} L(1, \chi),$$

where $L(1, \chi)$ denotes Dirichlet's L -series and R_K is the regulator of K . Since the unit group of the ring of integers of K is generated by the zeros of Emma Lehmer's polynomial (proved in [8]), then $R_K = R$, where R is the regulator of Emma Lehmer's units. Both the right hand side and R are calculated with accurate approximation and using the fact that class number is an integer they obtained h_K .

In the second application we will make calculations in cubic fields of prime conductor p , $p \neq a^2 + 27b^2$. Let δ be a unit of the field K . The question whether $\delta, \sigma(\delta)$ are fundamental units of the field K is the question whether $f = 1$. By means of Theorem 1 the value $e \equiv \frac{h_K}{f} \pmod{p^2}$, $0 \leq e < p^2$, can be calculated. In the case $e > p$ we have $f \neq 1$ because in a cubic field $h_K < p$. So it means in such a case $\delta, \sigma(\delta)$ are not fundamental units.

The main theorem

In the papers [4], [5] the congruence of Ankeny–Artin–Chowla type modulo p^2 for real subfields of the field $\mathbf{Q}(\zeta_p)$ of prime degree l is proved. The following notation is taken from [4] and [5].

Let $\beta_0, \beta_1, \dots, \beta_{l-1}$ be the integral basis of the field K formed by the Gauss periods, where $\beta_{i+1} = \sigma(\beta_i)$, $i = 0, \dots, l-2$ and σ is the automorphism $\sigma(\zeta_p) = \zeta_p^r$, r is a primitive root modulo p . Let δ be a unit of K ,

$$\delta = x_0\beta_0 + x_1\beta_1 + \dots + x_{l-1}\beta_{l-1}.$$

Associate to the unit δ the polynomial $f(X) = X^{l-1} + d_1X^{l-2} + \dots + d_{l-1}$, where for $i = 1, \dots, \frac{l-1}{2}$

$$d_i = \frac{1}{\left(i\frac{p-1}{l}\right)!} (1 - \nu_i) \frac{x_0 + x_1g^i + \dots + x_{l-1}g^{i(l-1)}}{x_0 + x_1 + \dots + x_{l-1}},$$

$$d_{l-i} = - \left(i\frac{p-1}{l}\right)! (1 + \nu_i) \frac{x_0 + x_1g^{-i} + \dots + x_{l-1}g^{-i(l-1)}}{x_0 + x_1 + \dots + x_{l-1}},$$

$$g \equiv r^{\frac{p-1}{l}} \pmod{p^2} \quad \text{and} \quad \nu_i = \frac{ip}{l} \left(W_p - A_{i\frac{p-1}{l}} \right).$$

Write $S_j = S_j(d_1, d_2, \dots, d_{l-1})$ for the sum of j -th powers of the roots of the polynomial $f(X)$, for $j = 1, 2, \dots, 2l - 1$. Hence

$$S_1 = -d_1, \quad S_2 = d_1^2 - 2d_2, \quad S_3 = -d_1^3 + 3d_1d_2 - 3d_3, \dots$$

THEOREM 1. *Let l, p be primes, $p \equiv 1 \pmod{l}$ and let $K \subset \mathbf{Q}(\zeta_p + \zeta_p^{-1})$ with $[K : \mathbf{Q}] = l > 2$. Suppose that 2 is not the l -th power modulo p . Let δ be a unit of K such that $[U_K : \langle \delta \rangle] = f$, $(f, p) = 1$. Denote $k = \frac{p-1}{l}$.*

(i) *Let $B_{ik} \not\equiv 0 \pmod{p}$ for all $i = 1, \dots, l-1$. Then*

$$(2) \quad \frac{h_K}{f} S_1 \cdots S_{l-1} \left(1 - p \sum_{i=1}^{l-1} \frac{i S_{l+i}}{(l+i) S_i} \right) \\ \equiv \left(\frac{-1}{l} \right) \frac{l}{2^{l-1}} B_k \cdots B_{(l-1)k} \left(\frac{l+1}{2} + p(l-1) - \sum_{i=1}^{l-1} \frac{i^2 B_{(l+i)k}}{l(l+i) B_{ik}} \right) \pmod{p^2}.$$

(ii) *Let $I \subseteq \{1, \dots, l-1\}$ be such that $i \in I$ if and only if $B_{ik} \equiv 0 \pmod{p}$. Let $S_i \equiv 0 \pmod{p}$ and $\frac{(l+i)B_{ik}}{lp} - \frac{i^2 B_{(l+i)k}}{l(l+i)p} \not\equiv 0 \pmod{p}$ for all $i \in I$. Then the following congruence holds*

$$(3) \quad \frac{h_K}{f} \prod_{i \notin I} S_i \cdot \prod_{i \in I} \left(\frac{S_i}{p} - \frac{i S_{l+i}}{l+i} \right) \\ \equiv \left(\frac{-1}{l} \right) \frac{l}{2^{l-1}} \prod_{i \notin I} B_{ik} \cdot \prod_{i \in I} \left(\frac{(l+i)B_{ik}}{lp} - \frac{i^2 B_{(l+i)k}}{l(l+i)p} \right) \pmod{p}.$$

REMARK. In the case (ii) the assumption $S_i \equiv 0 \pmod{p}$ for all $i \in I$ is in accordance with Vandiver's conjecture. The statement $S_i \not\equiv 0 \pmod{p}$ for some $i \in I$ leads to $p|h_K$.

Let now $\frac{(l+i)B_{ik}}{lp} - \frac{i^2 B_{(l+i)k}}{l(l+i)p} \equiv 0 \pmod{p}$ for some $i \in \{1, \dots, l-1\}$. Then, similarly, the statement $\frac{S_i}{p} - \frac{i S_{l+i}}{l+i} \not\equiv 0 \pmod{p}$ leads to $p|h_K$.

First we shall prove two lemmas necessary for the proof of the Theorem 1.

Define the mapping $\Phi : \mathbf{Q}^{2l-1} \rightarrow \mathbf{Q}^l$ as follows

$$\Phi(X_1, X_2, \dots, X_{2l-1}) = (1 - pY_l, Y_1 - pY_{l+1}, \dots, Y_{l-1} - pY_{2l-1}),$$

where $Y_0 = 1$ and for $m > 0$

$$Y_m = Y_m(X_1, \dots, X_m) = (-1)^m \frac{1}{m!} \begin{vmatrix} X_1 & 1 & 0 & \dots & 0 \\ X_2 & X_1 & 2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ X_{m-1} & X_{m-2} & X_{m-3} & \dots & m-1 \\ X_m & X_{m-1} & X_{m-2} & \dots & X_1 \end{vmatrix}.$$

LEMMA 1. *The following properties hold*

$$(i) \quad Y_m(X_1, \dots, X_m) = -\frac{1}{m} \sum_{i=0}^{m-1} X_{m-i} Y_i(X_1, \dots, X_i).$$

Let $X_m = M_m + mpZ_m$, $X_l = M_l$, $X_{l+m} = (l+m)Z_m$ (M_m, Z_m are independent variables) for $m = 1, \dots, l-1$. Then

(ii)

$$Y_m(X_1, \dots, X_m) \equiv$$

$$\equiv Y_m(M_1, \dots, M_m) - p \sum_{i=0}^{m-1} Z_{m-i} Y_i(M_1, \dots, M_i) \pmod{p^2},$$

(iii)

$$Y_l(X_1, \dots, X_l) \equiv Y_l(M_1, \dots, M_l) \pmod{p},$$

(iv)

$$Y_{l+m}(X_1, \dots, X_{l+m}) \equiv$$

$$\equiv Y_{l+m}(M_1, \dots, M_l, 0, \dots, 0) - \sum_{i=0}^{m-1} Z_{m-i} Y_i(M_1, \dots, M_i) \pmod{p}$$

for $m = 1, \dots, l-1$.

$$(v) \quad \Phi(X_1, \dots, X_{2l-1}) \equiv \Phi(M_1, \dots, M_l, 0, \dots, 0) \pmod{p^2}.$$

PROOF. The formula (i) can be proved directly from the definition of Y_m . We prove (ii) by induction. For $m = 1$ we have $Y_1(X_1) = -M_1 - pZ_1 = Y_1(M_1) - pZ_1$. Let now $m < l$ and (ii) holds for all $i = 1, \dots, m-1$. Using formula (i) we have

$$Y_m(X_1, \dots, X_m) \equiv$$

$$\equiv -\frac{1}{m} \sum_{i=0}^{m-1} M_{m-i} Y_i(X_1, \dots, X_i) - \frac{1}{m} p \sum_{i=0}^{m-1} (m-i) Z_{m-i} Y_i(M_1, \dots, M_i)$$

$$\equiv -\frac{1}{m} M_m - \frac{1}{m} \sum_{i=1}^{m-1} M_{m-i} Y_i(X_1, \dots, X_i) - pZ_m$$

$$- \frac{1}{m} p \sum_{i=1}^{m-1} (m-i) Z_{m-i} Y_i(M_1, \dots, M_i) \pmod{p^2}.$$

Now we can apply induction to the second term

$$\begin{aligned}
 & \sum_{i=1}^{m-1} M_{m-i} Y_i(X_1, \dots, X_i) \\
 & \equiv \sum_{i=1}^{m-1} M_{m-i} \left(Y_i(M_1, \dots, M_i) - p \sum_{j=0}^{i-1} Z_{i-j} Y_j(M_1, \dots, M_j) \right) \\
 & \equiv \sum_{i=1}^{m-1} M_{m-i} Y_i(M_1, \dots, M_i) - p \sum_{i=1}^{m-1} \sum_{j=0}^{i-1} M_{m-i} Z_{i-j} Y_j(M_1, \dots, M_j) \\
 & \equiv \sum_{i=1}^{m-1} M_{m-i} Y_i(M_1, \dots, M_i) - p \sum_{i=1}^{m-1} Z_{m-i} \sum_{j=0}^{i-1} M_{i-j} Y_j(M_1, \dots, M_j) \\
 & \equiv \sum_{i=1}^{m-1} M_{m-i} Y_i(M_1, \dots, M_i) + p \sum_{i=1}^{m-1} i Z_{m-i} Y_i(M_1, \dots, M_i) \pmod{p^2}
 \end{aligned}$$

and together it gives

$$\begin{aligned}
 & Y_m(X_1, \dots, X_m) \\
 & \equiv Y_m(M_1, \dots, M_m) - \frac{1}{m} p \sum_{i=1}^{m-1} (i + m - i) Z_{m-i} Y_i(M_1, \dots, M_i) - p Z_m \\
 & \equiv Y_m(M_1, \dots, M_m) - p \sum_{i=0}^{m-1} Z_{m-i} Y_i(M_1, \dots, M_i) \pmod{p^2}
 \end{aligned}$$

and (ii) is proved. Using formula (i) and the fact that $X_m \equiv M_m \pmod{p}$ and $Y_m(X_1, \dots, X_m) \equiv Y_m(M_1, \dots, M_m) \pmod{p}$ for all $m = 1, \dots, l-1$ we obtain (iii).

Similarly by induction we can prove also (iv). Then (v) follows directly from (ii), (iii) and (iv). \square

LEMMA 2. *Let $P_1, \dots, P_{2l-1}, R_1, \dots, R_{2l-1}$ be p -integral rational numbers and*

$$\Phi(P_1, \dots, P_{2l-1}) \equiv \frac{1 - pY_l(P_1, \dots, P_l)}{1 - pY_l(R_1, \dots, R_l)} \Phi(R_1, \dots, R_{2l-1}) \pmod{p^2}.$$

Then for $m = 1, \dots, l-1$

$$(4) \quad P_m \equiv R_m \pmod{p},$$

$$(5) \quad P_m \equiv R_m + p \frac{m}{l+m} (P_{l+m} - R_{l+m}) \pmod{p^2}.$$

PROOF. The components of the congruence modulo p can be written in the following form

$$Y_m(P_1, \dots, P_m) \equiv Y_m(R_1, \dots, R_m) \pmod{p}$$

($m = 1, \dots, l - 1$) and using (i) of the Lemma 1 we can prove by induction the congruence (4).

Modulo p^2 we can write

$$\begin{aligned} Y_m(P_1, \dots, P_m) - Y_m(R_1, \dots, R_m) &\equiv \\ &\equiv p(Y_{l+m}(P_1, \dots, P_{l+m}) - Y_{l+m}(R_1, \dots, R_{l+m})) - \\ &\quad - pY_m(R_1, \dots, R_m)(Y_l(P_1, \dots, P_l) - Y_l(R_1, \dots, R_l)) \pmod{p^2}. \end{aligned}$$

At first we shall prove by induction the following congruence

$$\begin{aligned} Y_{l+m}(P_1, \dots, P_{l+m}) - Y_{l+m}(R_1, \dots, R_{l+m}) &\equiv \\ &\equiv - \sum_{i=0}^m \frac{1}{l+i} Y_{m-i}(R_1, \dots, R_{m-i})(P_{l+i} - R_{l+i}) \pmod{p} \end{aligned}$$

for $m = 0, \dots, l - 1$. For $m = 0$

$$\begin{aligned} Y_l(P_1, \dots, P_l) - Y_l(R_1, \dots, R_l) &= -\frac{1}{l}(P_l - R_l) - \\ &\quad - \frac{1}{l} \sum_{i=1}^{l-1} (P_{l-i} Y_i(P_1, \dots, P_i) - R_{l-i} Y_i(R_1, \dots, R_i)) \end{aligned}$$

and the sum vanishes modulo p by (4). Let the congruence hold for all $i = 1, \dots, m - 1$. Then for m

$$\begin{aligned} Y_{l+m}(P_1, \dots, P_{l+m}) - Y_{l+m}(R_1, \dots, R_{l+m}) &= \\ &= -\frac{1}{l+m} \sum_{i=0}^{m+l-1} (P_{l+m-i} Y_i(P_1, \dots, P_i) - R_{l+m-i} Y_i(R_1, \dots, R_i)) \\ &\equiv -\frac{1}{l+m} \sum_{i=0}^m Y_i(R_1, \dots, R_i)(P_{l+m-i} - R_{l+m-i}) \\ &\quad - \frac{1}{l+m} \sum_{i=m+1}^{l-1} (P_{l+m-i} Y_i(P_1, \dots, P_i) - R_{l+m-i} Y_i(R_1, \dots, R_i)) \\ &\quad - \frac{1}{l+m} \sum_{i=0}^{m-1} R_{m-i} (Y_{l+i}(P_1, \dots, P_{l+i}) - Y_{l+i}(R_1, \dots, R_{l+i})) \pmod{p}. \end{aligned}$$

The second sum vanishes modulo p and, applying induction, the third sum can be rewritten in the following form

$$\begin{aligned} \sum_{i=0}^{m-1} R_{m-i} \sum_{j=0}^i \left(-\frac{1}{l+j} \right) Y_{i-j}(R_1, \dots, R_{i-j})(P_{l+j} - R_{l+j}) &\equiv \\ &\equiv - \sum_{i=0}^{m-1} \frac{1}{l+i} (P_{l+i} - R_{l+i}) \sum_{j=0}^{m-i-1} R_{m-i-j} Y_j(R_1, \dots, R_j) \equiv \\ &\equiv \sum_{i=0}^{m-1} \frac{m-i}{l+i} Y_{m-i}(R_1, \dots, R_{m-i})(P_{l+i} - R_{l+i}) \pmod{p}. \end{aligned}$$

And together with the first sum this gives the congruence we promised to prove

$$\begin{aligned} Y_{l+m}(P_1, \dots, P_{l+m}) - Y_{l+m}(R_1, \dots, R_{l+m}) &\equiv -\frac{1}{l+m} (P_{l+m} - R_{l+m}) - \\ &- \frac{1}{l+m} \sum_{i=0}^{m-1} Y_{m-i}(R_1, \dots, R_{m-i})(P_{l+i} - R_{l+i}) \left(1 + \frac{m-i}{l+i} \right) \equiv \\ &\equiv - \sum_{i=0}^m \frac{1}{l+i} Y_{m-i}(R_1, \dots, R_{m-i})(P_{l+i} - R_{l+i}) \pmod{p}. \end{aligned}$$

Then we have

$$\begin{aligned} (6) \\ Y_m(P_1, \dots, P_m) - Y_m(R_1, \dots, R_m) &\equiv \\ &\equiv -p \sum_{i=1}^m \frac{1}{l+i} Y_{m-i}(R_1, \dots, R_{m-i})(P_{l+i} - R_{l+i}) \pmod{p^2} \end{aligned}$$

for $m = 1, \dots, l-1$.

Similarly we shall prove (5) by induction. For $m = 1$ by (6)

$$P_1 - R_1 = -(Y_1(P_1) - Y_1(R_1)) \equiv p \frac{1}{l+1} (P_{l+1} - R_{l+1}) \pmod{p^2}.$$

Using (i) of Lemma 1, we have for any $m = 1, \dots, l-1$

$$\begin{aligned} (7) \quad Y_m(P_1, \dots, P_m) - Y_m(R_1, \dots, R_m) &= \\ &= -\frac{1}{m} (P_m - R_m) - \frac{1}{m} \sum_{i=1}^{m-1} (P_{m-i} Y_i(P_1, \dots, P_i) - R_{m-i} Y_i(R_1, \dots, R_i)). \end{aligned}$$

By means of the induction hypothesis and (6), each element in the sum can be written in the following form

$$\begin{aligned} & P_{m-i}Y_i(P_1, \dots, P_i) - R_{m-i}Y_i(R_1, \dots, R_i) \\ &= Y_i(P_1, \dots, P_i)(P_{m-i} - R_{m-i}) + R_{m-i}(Y_i(P_1, \dots, P_i) - Y_i(R_1, \dots, R_i)) \\ &\equiv Y_i(P_1, \dots, P_i)p \frac{m-i}{l+m-i} (P_{l+m-i} - R_{l+m-i}) \\ &\quad - pR_{m-i} \sum_{j=1}^i \frac{1}{l+j} Y_{i-j}(R_1, \dots, R_{i-j})(P_{l+j} - R_{l+j}) \pmod{p^2}. \end{aligned}$$

We can now sum the previous congruence

$$\begin{aligned} & p \sum_{i=1}^{m-1} \frac{i}{l+i} Y_{m-i}(P_1, \dots, P_{m-i})(P_{l+i} - R_{l+i}) \\ &\quad - p \sum_{i=1}^{m-1} R_{m-i} \sum_{j=1}^i \frac{1}{l+j} Y_{i-j}(R_1, \dots, R_{i-j})(P_{l+j} - R_{l+j}) \\ &\equiv p \sum_{i=1}^{m-1} Y_{m-i}(R_1, \dots, R_{m-i})(P_{l+i} - R_{l+i}) \left(\frac{i}{l+i} + \frac{m-i}{l+i} \right) \\ &\equiv pm \sum_{i=1}^{m-1} \frac{1}{l+i} Y_{m-i}(R_1, \dots, R_{m-i})(P_{l+i} - R_{l+i}) \pmod{p^2}. \end{aligned}$$

Now substituting to (7) and using (6) we get the congruence (5). \square

PROOF OF THE THEOREM 1. We start with the notation introduced in [5] and the Theorem 1 of [5].

Define the numbers $T_1, T_2, \dots, T_{2l-1}$ as follows

$$\begin{aligned} T_i &\equiv \frac{C_{n_i}}{2n_i!} - i \frac{p(p-1)}{2ln_i!} \left(\frac{E_{n_i+1}}{n_i+1} - W_p C_{n_i} - \mu_i \right) \pmod{p^2}, \\ T_l &\equiv \frac{1}{2}(1 - Q_2) \pmod{p}, \\ T_{l+i} &\equiv \frac{N_i}{2n_i!} \left(-\frac{C_{N_i-1} - C_{n_i}}{p} + A_n C_{n_i} + \mu_i - \frac{E_{n_i+1}}{n_i+1} \right) \pmod{p}, \end{aligned}$$

where $N_i = (p-1) + i \frac{p-1}{l}$, $n_i = i \frac{p-1}{l} - 1$ and $\mu_i = \sum_{j=0}^{n_i-1} \binom{n_i}{j} \frac{C_j}{n_i-j}$ for $i = 1, \dots, l-1$.

THEOREM 1 OF [5]. Let l, p be primes, $p \equiv 1 \pmod{l}$ and let $K \subset \mathbf{Q}(\zeta_p + \zeta_p^{-1})$, $[K : \mathbf{Q}] = l > 2$. Suppose that 2 is not the l -th power modulo p . Let δ be a unit of K such that $[U_K : \langle \delta \rangle] = f$, $(f, p) = 1$. Let

$$\delta = x_0\beta_0 + x_1\beta_1 + \cdots + x_{l-1}\beta_{l-1}.$$

Let the integers $\alpha_1, \alpha_2, \dots, \alpha_{l-1}$ form a solution of the congruence

$$\begin{aligned} \varepsilon \left(\frac{x_0 + x_1 + \cdots + x_{l-1}}{-l} \right)^{\alpha_l} \Phi(\alpha_1 S_1, \dots, \alpha_l S_l, \alpha_1 S_{l+1}, \dots, \alpha_{l-1} S_{2l-1}) &\equiv \\ &\equiv (2 + 2p)^{f \frac{2l-1}{2}} \Phi(fT_1, fT_2, \dots, fT_{2l-1}) \pmod{p^2}, \end{aligned}$$

where $\alpha_l = g\alpha_1 + g^2\alpha_2 + \cdots + g^{l-1}\alpha_{l-1}$ and $\varepsilon = \pm 1$.

Then

$$\alpha_1 \alpha_2 \cdots \alpha_{l-1} \equiv h_K f^{l-2} \pmod{p^2}.$$

Based on the definition of the mapping Φ we can rewrite the congruence of the Theorem 1 of [5] to l congruences. Assuming the congruence in the first component we get

$$\begin{aligned} \varepsilon \left(\frac{x_0 + x_1 + \cdots + x_{l-1}}{-l} \right)^{\alpha_l} \\ \equiv (2 + 2p)^{f \frac{2l-1}{2}} \frac{1 - pY_l(fT_1, \dots, fT_l)}{1 - pY_l(\alpha_1 S_1, \dots, \alpha_l S_l)} \pmod{p^2}, \end{aligned}$$

hence

$$\begin{aligned} \Phi(\alpha_1 S_1, \dots, \alpha_{l-1} S_{2l-1}) \\ \equiv \frac{1 - pY_l(\alpha_1 S_1, \dots, \alpha_l S_l)}{1 - pY_l(fT_1, \dots, fT_l)} \Phi(fT_1, \dots, fT_{2l-1}) \pmod{p^2}. \end{aligned}$$

Define the numbers V_1, V_2, \dots, V_{l-1} as follows

$$(8) \quad V_i \equiv \frac{C_{n_i}}{2n_i!} + i \frac{p}{2ln_i!} \left(-\frac{C_{N_i-1} - C_{n_i}}{p} + A_{n_i} C_{n_i} - W_p C_{n_i} \right) \pmod{p^2},$$

where $N_i = (p-1) + i \frac{p-1}{l}$, $n_i = i \frac{p-1}{l} - 1$ for $i = 1, 2, \dots, l-1$.

By the Lemma 1 we have

$$Y_i(fT_1, \dots, fT_l) \equiv Y_i(fV_1, \dots, fV_{l-1}, fT_l) \pmod{p}$$

and

$$\Phi(fT_1, \dots, fT_{2l-1}) \equiv \Phi(fV_1, \dots, fV_{l-1}, fT_l, 0, \dots, 0) \pmod{p^2}.$$

Now we can apply the Lemma 2 and get for $m = 1, \dots, l - 1$

$$(9) \quad \alpha_m S_m \equiv fV_m \pmod{p},$$

$$(10) \quad \alpha_m S_m \equiv fV_m + p \frac{m}{l+m} \alpha_m S_{l+m} \pmod{p^2}.$$

In the case (i), the congruences (9) and (10) imply

$$\alpha_m S_m \equiv fV_m \left(1 + p \frac{m S_{l+m}}{(l+m) S_m} \right) \pmod{p^2}$$

and multiplying these congruences for $m = 1, \dots, l - 1$ we obtain

$$\alpha_1 \cdots \alpha_{l-1} S_1 \cdots S_{l-1} \equiv f^{l-1} V_1 \cdots V_{l-1} \left(1 + p \sum_{i=1}^{l-1} \frac{i S_{l+i}}{(l+i) S_i} \right) \pmod{p^2}$$

and using the congruence from the Theorem 1 of [5] we get

$$(11) \quad \frac{h_K}{f} S_1 \cdots S_{l-1} \left(1 - p \sum_{i=1}^{l-1} \frac{i S_{l+i}}{(l+i) S_i} \right) \equiv V_1 \cdots V_{l-1} \pmod{p^2}.$$

Let $B_{ik} \not\equiv 0 \pmod{p}$ for $i = 1, \dots, l - 1$. We can substitute V_1, \dots, V_{l-1} from (8) and simplify the right hand side of (11) modulo p^2 . We have

$$(12) \quad V_1 \cdots V_{l-1} \equiv \frac{1}{2^{l-1}} \frac{2^k(1-2^k)2^{2k}(1-2^{2k}) \cdots 2^{(l-1)k}(1-2^{(l-1)k})}{k!(2k)! \cdots ((l-1)k)!} \times \\ \times B_k \cdots B_{(l-1)k} \left(1 + \frac{p}{l} \left(- \sum_{i=1}^{l-1} i \frac{C_{N_i-1}}{C_{N_i}} - \frac{1}{p} + \sum_{i=1}^{l-1} i A_{N_i} - \frac{l(l-1)}{2} W_p \right) \right).$$

Let $a \in \mathbf{Z}$, $a \equiv 2^k \pmod{p}$, $a^l \equiv 1 \pmod{p^2}$. Let $2^k \equiv a + xp \pmod{p^2}$, $x \in \mathbf{Z}$. Hence

$$2^{kl} = 2^{p-1} \equiv 1 + pQ_2 \equiv 1 + la^{l-1}xp \pmod{p^2}.$$

It gives $x \equiv \frac{aQ_2}{l} \pmod{p}$ and consequently $2^k \equiv a \left(1 + \frac{Q_2}{l} p \right) \pmod{p^2}$, $2^{ki} \equiv a^i \left(1 + \frac{i}{l} p Q_2 \right) \pmod{p^2}$. And now we have

$$2^{ik}(1-2^{ik}) \equiv a^i \left(1 + \frac{i}{l} p Q_2 \right) (1-a^i) \left(1 - \frac{i}{l} \frac{a^i}{1-a^i} p Q_2 \right) \equiv \\ \equiv a^i(1-a^i) \left(1 + \frac{i}{l} p Q_2 \frac{1-2a^i}{1-a^i} \right) \pmod{p^2}.$$

Since $a^l \equiv 1 \pmod{p^2}$, the following congruence holds

$$a \cdot a^2 \cdots a^{l-1} (1-a)(1-a^2) \cdots (1-a^{l-1}) \equiv l \pmod{p^2}.$$

We obtain

$$2^k (1-2^k) \cdots 2^{(l-1)k} (1-2^{(l-1)k}) \equiv l \left(1 + \frac{1}{l} Q_2 p \sum_{i=1}^{l-1} i \frac{1-2a^i}{1-a^i} \right) \pmod{p^2}.$$

Now we express product $k!(2k)! \cdots ((l-1)k)!$ modulo p^2 . For each $i = 1, \dots, \frac{l-1}{2}$ we have

$$(ik)!((l-i)k)! \equiv (p-1)!(1+pA_{ik}) \equiv -(1-pW_p)(1+pA_{ik}) \pmod{p^2}$$

and together

$$k! \cdots ((l-1)k)! \equiv (-1)^{\frac{l-1}{2}} \left(1 - \frac{l-1}{2} pW_p \right) \left(1 + p \sum_{i=1}^{\frac{l-1}{2}} A_{ik} \right) \pmod{p^2}.$$

Substituting to (12) we have

$$\begin{aligned} V_1 \cdots V_{l-1} &\equiv \left(\frac{-1}{l} \right) \frac{l}{2^{l-1}} \left(1 + \frac{1}{l} Q_2 p \sum_{i=1}^{l-1} i \frac{1-2a^i}{1-a^i} \right) \left(1 - p \sum_{i=1}^{\frac{l-1}{2}} A_{ik} \right) \times \\ &\times B_k \cdots B_{(l-1)k} \left(1 + \frac{p}{l} \left(- \sum_{i=1}^{l-1} i \frac{C_{N_i-1}}{C_{N_i}} - 1 + \sum_{i=1}^{l-1} i A_{N_i} \right) \right) \pmod{p^2}. \end{aligned}$$

Furthermore

$$\begin{aligned} \frac{C_{N_i-1}}{C_{N_i}} - 1 &= \frac{1}{p} \left(\frac{2^{p-1}(1-2^{(l+i)k})}{1-2^{ik}} \frac{ikB_{(l+i)k}}{(l+i)kB_{ik}} - 1 \right) \equiv \\ &\equiv \frac{1}{p} \left(\frac{iB_{(l+i)k}}{(l+i)B_{ik}} - 1 \right) + Q_2 \frac{1-2a^i}{1-a^i} \pmod{p}, \end{aligned}$$

because

$$\begin{aligned} \frac{2^{p-1}(1-2^{(l+i)k})}{1-2^{ik}} &\equiv \frac{(1+pQ_2)(1-(1+pQ_2)a^i(1+\frac{i}{l}pQ_2))}{(1-a^i)(1-\frac{i}{l}\frac{a^i}{1-a^i}pQ_2)} \equiv \\ &\equiv 1 + pQ_2 \frac{1-2a^i}{1-a^i} \pmod{p^2}. \end{aligned}$$

This gives

$$V_1 \cdots V_{l-1} \equiv \left(\frac{-1}{l}\right) \frac{l}{2^{l-1}} \left(1 - p \sum_{i=1}^{\frac{l-1}{2}} A_{ik}\right) B_k \cdots B_{(l-1)k} \times \\ \times \left(1 + \frac{p}{l} \left(-\frac{1}{p} \sum_{i=1}^{l-1} \left(\frac{i^2 B_{(l+i)k}}{(l+i)B_{ik}} - i\right) + \sum_{i=1}^{l-1} iA_{ni}\right)\right) \pmod{p^2}.$$

Finally, using congruence

$$\sum_{i=1}^{l-1} iA_{ni} = \sum_{i=1}^{l-1} iA_{ki-1} \equiv \sum_{i=1}^{l-1} iA_{ik} + l(l-1) \equiv l \sum_{i=1}^{\frac{l-1}{2}} A_{ik} + l(l-1) \pmod{p}$$

we get congruence (2).

In the case (ii), for any $m \in I$ the congruence (10) gives

$$\alpha_m \left(\frac{S_m}{p} - \frac{mS_{l+m}}{l+m}\right) \equiv f \frac{V_m}{p} \pmod{p}$$

and by multiplication of these congruences for $i \in I$ together with congruences (9) for $i \notin I$ we get

$$\alpha_1 \cdots \alpha_{l-1} \prod_{i \notin I} S_i \cdot \prod_{i \in I} \left(\frac{S_i}{p} - \frac{iS_{l+i}}{l+i}\right) \equiv f^{l-1} \prod_{i \notin I} V_i \cdot \prod_{i \in I} \frac{V_i}{p} \pmod{p},$$

and the substitution of V_i gives the required congruence. \square

Applications

THE QUINTIC CASE. In [6] Emma Lehmer exhibits a family of polynomials $F_n(X) \in \mathbf{Z}[X]$ for $n \in \mathbf{Z}$. The polynomials are given by

$$F_n(X) = X^5 + n^2 X^4 - (2n^3 + 6n^2 + 10n + 10)X^3 + \\ + (n^4 + 5n^3 + 11n^2 + 15n + 5)X^2 + (n^3 + 4n^2 + 10n + 10)X + 1.$$

Let $p = n^4 + 5n^3 + 15n^2 + 25n + 25$ be a prime number. It is proved in [6] that the following translation γ_0 of Gaussian period β_0 is a root of the polynomial $F_n(X)$

$$\gamma_0 = \left(\frac{n}{5}\right) \beta_0 + \frac{\left(\left(\frac{n}{5}\right) - n^2\right)}{5}.$$

Note that the polynomials $F_n(X)$ have no root modulo 2 and it implies that 2 is not a quintic residue modulo p . So we can use the Theorem 1.

Schoof and Washington in [8] proved that the conjugates of the unit γ_0 are fundamental units.

Set $\delta = \gamma_0$. Suppose that $\left(\frac{n}{5}\right) = 1$, hence $\delta = \beta_0 - \frac{n^2-1}{5} = \frac{n^2-1}{5}(\beta_0 + \beta_1 + \beta_2 + \beta_3 + \beta_4) + \beta_0 = \frac{n^2+4}{5}\beta_0 + \frac{n^2-1}{5}\beta_1 + \frac{n^2-1}{5}\beta_2 + \frac{n^2-1}{5}\beta_3 + \frac{n^2-1}{5}\beta_4$. Therefore $x_0 = \frac{n^2-1}{5} + 1$, $x_1 = x_2 = x_3 = x_4 = \frac{n^2-1}{5}$ which imply

$$\frac{x_0 + x_1g + x_2g^2 + x_3g^3 + x_4g^4}{x_0 + x_1 + x_2 + x_3 + x_4} \equiv \frac{1}{n^2} \pmod{p^2}.$$

Similarly if $\left(\frac{n}{5}\right) = -1$ then

$$\frac{x_0 + x_1g + x_2g^2 + x_3g^3 + x_4g^4}{x_0 + x_1 + x_2 + x_3 + x_4} \equiv -\frac{1}{n^2} \pmod{p^2}.$$

Thus we have determined numbers d_1, d_2, d_3, d_4 .

The class numbers h_K modulo p^2 for all prime conductors of given type less than 10^9 , computed by means of the congruence (2), are given in the following table. The first 26 values ($p < 10^7$) of the table correspond to calculations in [8].

n	p	$h_K \pmod{p^2}$	
-1,-2	11	1	
-3	31	1	
1	71	1	
-4	101	1	
2	191	11	
-6	631	11	
4	941	16	= 2^4
-9	3931	256	= 2^8
7	5051	1451	
8	7841	421	
-11	9551	541	
-18	80251	37631	= $11^2 \cdot 311$
16	90281	19301	
-21	154291	108691	= $11 \cdot 41 \cdot 241$
-22	187751	76901	= $11 \cdot 6991$
23	349211	186091	= $71 \cdot 2621$
26	555671	721151	= $661 \cdot 1091$
27	641491	1566401	
-31	788231	1217821	= $11 \cdot 110711$

-32	899321	798256	=	$2^4 \cdot 49891$
-36	1464901	4628591	=	$11 \cdot 420781$
-37	1640531	1636721		
-42	2766691	20599841	=	$31 \cdot 664511$
41	3196631	8088176	=	$2^4 \cdot 505511$
51	7468771	28850896	=	$2^4 \cdot 521 \cdot 3461$
-54	7758151	37142851	=	$101 \cdot 367751$
56	10761041	148819696	=	$2^4 \cdot 1151 \cdot 8081$
-61	12765251	66431941		
-62	13640831	70642451	=	$11 \cdot 6422041$
66	20479231	182277211	=	$61 \cdot 2988151$
67	21723971	1127756881	=	$181 \cdot 1091 \cdot 5711$
68	23024621	627986096	=	$2^4 \cdot 31 \cdot 1266101$
73	30425111	335434451	=	$11 \cdot 30494041$
77	37526591	3233114891		
78	39481051	644240861	=	$11 \cdot 1721 \cdot 34031$
-84	46927381	2068985771		
82	48071951	2210817521	=	$11 \cdot 881 \cdot 228131$
84	52858621	3141700201	=	$55931 \cdot 56171$
-88	56676161	5912208301		
89	66388151	1132538941	=	$41 \cdot 27622901$
-99	91352671	3144379001		
99	101060611	3041883856	=	$2^4 \cdot 11^2 \cdot 1571221$
-102	103090711	3626779141		
101	109367471	7522340051	=	$59^2 \cdot 2160971$
103	118176251	4099008881	=	$11 \cdot 3001 \cdot 124171$
-108	129922621	20060176081	=	$11 \cdot 10631 \cdot 171541$
106	132373991	7815148121	=	$11^2 \cdot 4721 \cdot 13681$
-109	134858531	6311175376	=	$2^4 \cdot 11 \cdot 35858951$
107	137379251	15085381091	=	$11^2 \cdot 2141 \cdot 58231$
-113	156021611	21628396061	=	$151 \cdot 281 \cdot 509731$
114	176501551	11080371781	=	$56311 \cdot 196771$
-119	192317591	32915044096	=	$2^8 \cdot 11 \cdot 31 \cdot 377051$
118	202304771	10025116211	=	$11 \cdot 2441 \cdot 373361$
-121	205717691	11420513591		
122	230839031	60390377311	=	$11 \cdot 5490034301$
128	279170201	24178878281		
129	287909191	32215474121		
137	365417111	125121548101	=	$11^3 \cdot 31 \cdot 3032441$
139	387022451	42590939281	=	$11 \cdot 3871903571$
-143	403843751	118398260816	=	$2^4 \cdot 11 \cdot 31 \cdot 21700561$
-147	451386751	155312785456	=	$2^4 \cdot 9707049091$

-157 588589571 152530304861	=	11 · 61 · 331 · 686761
158 643301291 92380627811	=	28351 · 3258461
159 659610571 150913029641	=	11 ² · 41 · 661 · 46021
-163 684652511 785372557471	=	41 · 19155428231
161 693157511 207156367681	=	66841 · 3099241
-164 701739461 124240930231	=	11 · 41 · 275478781
162 710402911 421336924016	=	2 ⁴ · 26333557751
-168 773305201 936192896591	=	131 · 1381 · 5174881
-172 850210301 170865966736	=	2 ⁴ · 11251 · 949171
176 987240521 362885296531	=	41 · 331 · 26739761

THE CUBIC CASE. The smallest positive residue of h_K/f modulo p^2 for several prime conductors p and for all units $\delta = x_0\beta_0 + x_1\beta_1 + x_2\beta_2$, where $-1000 \leq x_i \leq 1000$ ($i = 0, 1, 2$), is calculated in the following table. If this value is bigger than p then the corresponding unit is not strong Minkowski unit.

Prime $p = 163$.

unit	h_K/f	unit	h_K/f
(1, 2, 0)	17714	(515, 648, 307)	22633
(3, 4, 4)	4	(547, 693, 705)	22774
(4, 5, 5)	4	(587, 596, 461)	20438
(53, 54, 42)	1	(640, 651, 505)	14761
(53, 55, 44)	22774	(693, 705, 547)	22774
(57, 58, 45)	17714	(750, 763, 592)	22774
(62, 63, 49)	1	(812, 826, 641)	14761
(63, 65, 49)	22774	(875, 891, 690)	20438
(102, 118, 109)	17713	(993, 1000, 792)	18179
(352, 485, 478)	18179		

Prime $p = 607$.

unit	h_K/f	unit	h_K/f
(0, 2, 1)	332312	(185, 210, 209)	19343
(7, 8, 8)	4	(193, 219, 218)	34870
(8, 9, 9)	4	(193, 221, 219)	49147
(178, 202, 201)	201479	(401, 422, 394)	216134
(180, 203, 201)	162682		

Prime $p = 751$.

unit	h_K/f	unit	h_K/f
(-53, 38, 12)	483967	(407, 459, 420)	307785
(406, 458, 419)	381320		

Prime $p = 1879$.

unit	h_K/f
(-104, 85, 22)	2353762

Prime $p = 1951$.

unit	h_K/f	unit	h_K/f
(-5, 4, 4)	2537602	(77, 80, 74)	4
(76, 79, 73)	4		

REFERENCES

- [1] J. P. BUHLER, R. E. CRANDALL, R. W. SOMPOLSKI, *Irregular primes to one million*, Math. Comp. **59** (1992), 717–722.
- [2] S. JAKUBEC, *On divisibility of class number of real abelian fields of prime conductor*, Abh. Math. Sem. Univ. Hamburg, **63** (1993), 67–86.
- [3] S. JAKUBEC, *Congruence of Ankeny–Artin–Chowla type for cyclic fields of prime degree l* , Math. Proc. Camb. Phil. Soc., **119** (1996), 17.
- [4] S. JAKUBEC, *Congruence of Ankeny–Artin–Chowla type modulo p^2 for cyclic fields of prime degree l* , Acta Arithmetica, **LXXIV.4** (1996), 293–310.
- [5] S. JAKUBEC, *Note on the congruence of Ankeny–Artin–Chowla type modulo p^2* , Acta Arithmetica, **LXXXV.4** (1998), 377–388.
- [6] E. LEHMER, *Connection between Gaussian periods and cyclic units*, Math. Comp., **50** (1988), 535–541.
- [7] W. NARKIEWICZ, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd edition, Springer–Verlag (1990).
- [8] R. SCHOOF, L. C. WASHINGTON, *Quintic polynomials and real cyclotomic fields with large class number*, Math. Comp., **50** (1988), 543–556.
- [9] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, 2nd edition, Springer–Verlag (1997).

MATHEMATICAL INSTITUTE
 SLOVAK ACADEMY OF SCIENCES
 ŠTEFÁNIKOVA 49
 814-73 BRATISLAVA
 SLOVAKIA

e-mail:

`jakubec@savba.savba.sk`

`lassak@savba.savba.sk`