ACTA ARITHMETICA
LXXIV.4 (1996)

Congruence of Ankeny–Artin–Chowla type modulo p^2 for cyclic fields of prime degree l

by

Stanislav Jakubec (Bratislava)

Introduction. Let $p \equiv 1 \pmod 4$, let $T+U\sqrt{p} > 1$ be the fundamental unit, and let h be the class number of $\mathbb{Q}(\sqrt{p})$. The following congruence (Ankeny–Artin–Chowla congruence) holds:

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

For a cubic field $K \subset \mathbb{Q}(\zeta_p+\zeta_p^{-1})$, $p \equiv 1 \pmod 3$ the analogous congruence was proved by Feng Ke Qin in [1]. In general, for fields of the lth degree, the analogous congruence is proved in [5].

The aim of this paper is to prove a congruence of Ankeny–Artin–Chowla type modulo p^2 for real Abelian fields of a prime degree l and a prime conductor p. The importance of such a congruence can be demonstrated by the following example. Let K be a cubic field. In [5], the following congruence is proved:

$$h_K S_1 S_2 \equiv -\tfrac{3}{4} B_{(p-1)/3} B_{2(p-1)/3} \pmod p. \tag{1}$$

As is well known, $h_K < p$ for a cubic field. If $B_{(p-1)/3}B_{2(p-1)/3} \equiv 0 \pmod p$, then $S_1S_2 \equiv 0 \pmod p$, hence the congruence (1) does not provide any information about h_K. Note that such a prime exists, e.g. $p = 5479$. We have

$$B_{(p-1)/3} = B_{1826} \equiv 0 \pmod{5479}.$$

In this paper two applications of the main theorem (Theorem 1), for a quadratic and for a cubic field, will be given.

Let l and p be primes such that $p \equiv 1 \pmod l$ and let $K \subset \mathbb{Q}(\zeta_p+\zeta_p^{-1})$ with $[K:\mathbb{Q}] = l$. Let a be a primitive root modulo p. As is well known, the conjugates of the unit

1991 *Mathematics Subject Classification*: Primary 11R29.

$$\eta_a = N_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})/K}\left(\zeta_p^{(1-a)/2}\frac{1-\zeta_p^a}{1-\zeta_p}\right),$$

generate the group of cyclotomic units $C(K)$ of K. Consider the unit

$$\eta_2 = N_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})/K}(\zeta_p+\zeta_p^{-1}).$$

It is easy to prove that if 2 is not an lth power modulo p, then the conjugates of the unit η_2 generate the group $C(K)$. Let $\langle\varepsilon\rangle$ be the group generated by all conjugates of the unit ε.

According to ([3], Lemma 1, p. 69) for a cyclic field K with $[K:\mathbb{Q}]=l$, there is a unit δ such that $[U_K:\langle\delta\rangle]=f$, where $(p,f)=1$.

The following is taken from [5]. According to [8] and [9] (see also [10], p. 284), we have $h_K=[U_K:C(K)]$, where $C(K)=\langle\eta_2\rangle$ is the group of cyclotomic units of K. From $[U_K:\langle\delta\rangle]=f$ we have $\eta_2^f\in\langle\delta\rangle$. Let $[\langle\delta\rangle:\langle\eta_2^f\rangle]=e$. Clearly $[\langle\eta_2\rangle:\langle\eta_2^f\rangle]=f^{l-1}$.

Consider two towers of groups

$$\langle\eta_2^f\rangle\subset\langle\delta\rangle\subset U_K,\qquad \langle\eta_2^f\rangle\subset\langle\eta_2\rangle\subset U_K.$$

This implies $ef=h_Kf^{l-1}$ and hence $e=h_Kf^{l-2}$. Let

$$\eta_2^f=\delta^{c_0}\sigma(\delta)^{c_1}\ldots\sigma^{l-2}(\delta)^{c_{l-2}}.$$

It is easy to prove that

$$e=N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(c_0+c_1\zeta_l+\ldots+c_{l-2}\zeta_l^{l-2}).$$

Note that a unit δ for which $f=1$ is called a *strong Minkowski unit*. As is well known, a strong Minkowski unit exists for a cyclic fields K with $l<23$. The problem of existence of a strong Minkowski unit for cyclic fields of small non-prime degree is solved in [7].

Let a be a fixed primitive root modulo p, let χ be the Dirichlet character of order n, $n\mid p-1$, $\chi(x)=\zeta_n^{\mathrm{ind}_a x}$. Let g be such that $g\equiv a^{(p-1)/n} \pmod p$ and $g^n\equiv 1 \pmod{p^p}$. Denote by $\mathfrak{p}$ a prime divisor of $\mathbb{Q}(\zeta_n)$ such that $\mathfrak{p}\mid p$ and $1/g\equiv\zeta_n \pmod{\mathfrak{p}^p}$.

Define the rational numbers $A_0(n),A_1(n),\ldots,A_{n-1}(n)$ in the following way:

$$A_0(n)=-1/n,$$

$$\tau(\chi^i)^n\equiv n^nA_i(n)^n(-p)^i \pmod{\mathfrak{p}^{2+i}},\quad A_i(n)\equiv\frac{(p-1)/n}{(i(p-1)/n)!} \pmod p, \tag{2}$$

where $\tau(\chi)$ is the Gauss sum.

Put $m=(p-1)/2$, and

$$G_j(X)=A_0(m)X^j+A_1(m)X^{j-1}+\ldots+A_j(m),$$

$$F_j(X)=\frac{1}{(p-1)!}X^j+\frac{1}{(p+1)!}X^{j-1}+\frac{1}{(p+3)!}X^{j-2}+\ldots+\frac{1}{(p+2j-1)!}.$$

Define

$$E_n^* = \frac{E_{2n}}{(2n)!} \quad \text{for } n = 1, 2, 3, \ldots,$$

where E_{2n} are the Euler numbers, i.e. $E_0 = 1$, $E_2 = -1$, $E_4 = 5$, $E_6 = -61$, $E_8 = 1385$, $E_{10} = -50521$, $E_{12} = 2702765$, $E_{14} = -199360981, \ldots$

Consider the formal expressions $G_j(E^*)$ and $F_j(E^*)$, where

$$(E^*)^k = E_k^*.$$

Let $\beta_0, \beta_1, \ldots, \beta_{l-1}$ be the integral basis of the field K formed by the Gauss periods. Let

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

Associate with the unit δ the polynomial $f(X)$ as follows:

$$f(X) = X^{l-1} + d_1X^{l-2} + d_2X^{l-3} + \ldots + d_{l-1},$$

where

$$d_i = -lA_i(l)\frac{x_0 + x_1g^i + x_2g^{2i} + \ldots + x_{l-1}g^{i(l-1)}}{x_0 + x_1 + \ldots + x_{l-1}}$$

for $i = 1, \ldots, l-1$. Put

$$S_j = S_j(d_1, \ldots, d_{l-1}) = \text{sum of the } j\text{th powers of the roots of } f(X)$$

for $j = 1, \ldots, 2l-1$. Hence

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

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

$$T_i = -\frac{1}{(i(p-1)/l)!}2^{i(p-1)/l-1}(2^{i(p-1)/l}-1)B_{i(p-1)/l} - i\frac{p-1}{4l}G_{i(p-1)/(2l)}(E^*)$$

for $i = 1, \ldots, l-1$, and

$$T_l = \frac{1-q_2}{2}, \quad \text{where} \quad q_2 = \frac{2^{p-1}-1}{p},$$

$$\begin{aligned} T_{l+i} = {} & -\frac{1}{(p-1+i(p-1)/l)!}2^{p-1+i(p-1)/l-1}(2^{p-1+i(p-1)/l}-1) \\ & \times B_{(p-1+i(p-1)/l)} \\ & + \left(\frac{p-1}{2} + i\frac{p-1}{2l}\right)F_{i(p-1)/(2l)}(E^*) \end{aligned}$$

for $i = 1, \ldots, l-1$.

Define

$$\alpha_i = c_0 + c_1g^i + c_2g^{2i} + \ldots + c_{l-2}g^{(l-2)i}$$

for $i = 1, \ldots, 2l-1$.

Let $X_1, \ldots, X_{2l-1} \in \mathbb{Q}$ and let

$$g(X) = X^{2l-1} + Y_1 X^{2l-2} + \ldots + Y_{2l-1}$$

be a polynomial such that

$$X_j = \text{sum of the } j\text{th powers of the roots of } g(X).$$

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

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

Now the main theorem of this paper be formulated.

THEOREM 1. *Let l and p be primes with $p \equiv 1 \pmod{l}$ and let $K \subset \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ with $[K : \mathbb{Q}] = l$. Suppose that 2 is not an l-th power modulo p. Let δ be a unit of K such that $[U_K : \langle\delta\rangle] = f$, $(f,p) = 1$. Let $\eta_2^f = \delta^{c_0}\sigma(\delta)^{c_1}\ldots\sigma^{l-2}(\delta)^{c_{l-2}}$ and $\alpha_i = c_0 + c_1 g^i + \ldots + c_{l-2}g^{(l-2)i}$ for $i = 1, \ldots, 2l-1$. The following congruence holds*:

$$\varepsilon\left(\frac{x_0 + x_1 + \ldots + x_{l-1}}{-l}\right)^{\alpha_l}\Phi(\alpha_1 S_1, \ldots, \alpha_{2l-1}S_{2l-1}) \equiv (2+2p)^{f(p-1)/(2l)}\Phi(fT_1, \ldots, fT_{2l-1}) \pmod{p^2}, \tag{3}$$

where $\varepsilon = \pm 1$.

Remark. The class number h_K appears in the preceding congruence implicitly, via the congruence

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

This congruence can be proved in the following way:

We have the congruence $1/g \equiv \zeta_l \pmod{\mathfrak{p}^p}$ and hence

$$\sigma_{-1}(c_0 + c_1\zeta_l^i + \ldots + c_{l-2}\zeta_l^{(l-2)i}) \equiv \alpha_i \pmod{\mathfrak{p}^p};$$

this yields

$$h_K f^{l-2} = e = N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(c_0 + c_1\zeta_l + \ldots + c_{l-2}\zeta_l^{l-2}) \equiv \alpha_1 \ldots \alpha_{l-1} \pmod{p^2}.$$

The congruence (3) gives l congruences (one in each component). If

$$B_{(p-1)/l}B_{2(p-1)/l}\ldots B_{(l-1)(p-1)/l} \not\equiv 0 \pmod{p},$$

then from the congruence (3), the numbers $\alpha_1, \ldots, \alpha_{l-1}$ modulo p^2 can be calculated. Using the congruence

$$h_K f^{l-2} \equiv \alpha_1 \ldots \alpha_{l-1} \pmod{p^2},$$

also h_K can be calculated modulo p^2. If

$$B_{(p-1)/l}B_{2(p-1)/l}\ldots B_{(l-1)(p-1)/l} \equiv 0 \pmod{p},$$

then the numbers $\alpha_1, \ldots, \alpha_{l-1}$ and hence also h_K can be calculated at most modulo p.

Before proving Theorem 1, we show its applications to quadratic and cubic fields.

The quadratic case $K=\mathbb{Q}(\sqrt{p})$, $p\equiv 5 \pmod 8$. Let

$$\delta = x_0\beta_0 + x_1\beta_1 = x_0\frac{-1+\sqrt{p}}{2} + x_1\frac{-1-\sqrt{p}}{2} > 1$$

be a fundamental unit of $\mathbb{Q}(\sqrt{p})$. Then

$$d_1 = -2A_1(2)\frac{x_0-x_1}{x_0+x_1}.$$

Hence

$$S_1 = 2A_1(2)\frac{x_0-x_1}{x_0+x_1}, \quad S_2 = 4A_1(2)^2\frac{(x_0-x_1)^2}{(x_0+x_1)^2}, \quad S_3 = 8A_1(2)^3\frac{(x_0-x_1)^3}{(x_0+x_1)^3}.$$

For $A_1(2)$ we have

$$\tau(\chi)^2 \equiv 4A_1(2)^2(-p) \pmod{\mathfrak{p}^3}, \qquad A_1(2) \equiv \frac{(p-1)/2}{((p-1)/2)!} \pmod p.$$

Hence

$$A_1(2)^2 \equiv -\frac{1}{4} \pmod{p^2}, \qquad A_1(2) \equiv \frac{(p-1)/2}{((p-1)/2)!} \pmod p.$$

Therefore

$$S_1 = 2A_1(2)\frac{x_0-x_1}{x_0+x_1}, \quad S_2 = -\frac{(x_0-x_1)^2}{(x_0+x_1)^2}, \quad S_3 = -2A_1(2)\frac{(x_0-x_1)^3}{(x_0+x_1)^3}.$$

Let

$$\frac{x_0+x_1}{-2} + \frac{x_0-x_1}{2}\sqrt{p} = T + U\sqrt{p} > 1.$$

It can be proved that $|\eta_2| = |N_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})/\mathbb{Q}(\sqrt{p})}(\zeta_p+\zeta_p^{-1})| < 1$, hence it is necessary to start from the unit $T-U\sqrt{p}$. We have

$$S_1 = 2A_1(2)\frac{U}{T}, \quad S_2 = -\frac{U^2}{T^2}, \quad S_3 = -2A_1(2)\frac{U^3}{T^3}.$$

For the numbers T_1, T_2, T_3 we have

$$\begin{aligned}
T_1 &= -\frac{1}{((p-1)/2)!}2^{(p-1)/2-1}(2^{(p-1)/2}-1)B_{(p-1)/2} - \frac{p-1}{8}G_{(p-1)/4}(E^*),\\
T_2 &= \tfrac{1}{2}(1-q_2),\\
T_3 &= -\frac{1}{(3(p-1)/2)!}2^{3(p-1)/2-1}(2^{3(p-1)/2}-1)B_{3(p-1)/2}\\
&\quad + (3(p-1)/4)F_{(p-1)/4}(E^*).
\end{aligned}$$

It is easy to see that

$$\Phi(X_1,X_2,X_3)=\Big(1-p\frac{X_1^2-X_2}{2},-X_1-p\Big(-\frac{1}{6}X_1^3+\frac{1}{2}X_1X_2-\frac{1}{3}X_3\Big)\Big).$$

Hence

$$\varepsilon\Big(\frac{x_0+x_1}{-2}\Big)^{\alpha_2}\Phi(\alpha_1S_1,\alpha_2S_2,\alpha_3S_3)\equiv(2+2p)^{(p-1)/4}\Phi(T_1,T_2,T_3)\pmod{p^2}.$$

Since $(x_0+x_1)/(-2)=T$ and $\alpha_1=\alpha_2=\alpha_3=h$, we get

$$\varepsilon T^h\Phi(hS_1,hS_2,hS_3)\equiv(2+2p)^{(p-1)/4}\Phi(T_1,T_2,T_3)\pmod{p^2},$$

where $\varepsilon=\pm1$. It can be proved that $\varepsilon=(-1)^{1+r}$, where r is the number of quadratic residues modulo p in the interval $(p/4,p/2)$.

The cubic case. Let p be a prime such that $p\equiv1\pmod 3$, $p\neq a^2+27b^2$ and let

$$\delta=x_0\beta_0+x_1\beta_1+x_2\beta_2.$$

Then

$$d_1=-3A_1(3)\frac{x_0+x_1g+x_2g^2}{x_0+x_1+x_2},\qquad d_2=-3A_2(3)\frac{x_0+x_1g^2+x_2g}{x_0+x_1+x_2}.$$

For the numbers $A_1(3),A_2(3)$ we have

$$\tau(\chi)^3\equiv27A_1(3)^3(-p)\pmod{\mathfrak{p}^3},\qquad A_1(3)\equiv\frac{(p-1)/3}{((p-1)/3)!}\pmod p,$$

$$\tau(\chi^2)^3\equiv27A_2(3)^3(-p)^2\pmod{\mathfrak{p}^4},\qquad A_2(3)\equiv\frac{(p-1)/3}{(2(p-1)/3)!}\pmod p.$$

As is well known, $\tau(\chi)^3=pJ(\chi,\chi)$, where $J(\chi,\chi)$ is the Jacobi sum.

Let $J(\chi,\chi)=a+b\zeta_3$, $a\equiv-1,b\equiv0\pmod 3$ and $p=a^2-ab+b^2$. Hence

$$-\Big(a+b\frac{1}{g}\Big)\equiv27A_1(3)^3\pmod{p^2},\qquad A_1(3)\equiv\frac{(p-1)/3}{((p-1)/3)!}\pmod p.$$

The number $A_2(3)$ is determined by the congruence

$$-1\equiv27^2A_1(3)^3A_2(3)^3\pmod{p^2},\qquad A_2(3)\equiv\frac{(p-1)/3}{(2(p-1)/3)!}\pmod p.$$

For the numbers $T_1,\dots,T_5$ we have

$$T_i=-\frac{1}{(i(p-1)/3)!}2^{i(p-1)/3-1}(2^{i(p-1)/3}-1)B_{i(p-1)/3}-i\frac{p-1}{12}G_{i(p-1)/6}(E^*)$$

for $i=1,2$, and

$$T_3=\tfrac12(1-q_2),$$

$$
\begin{aligned}
T_{3+i} = & -\frac{1}{(p-1+i(p-1)/3)!}2^{p-1+i(p-1)/3-1}(2^{p-1+i(p-1)/3}-1) \\
& \times B_{(p-1+i(p-1)/3)} \\
& + \left(\frac{p-1}{2}+i\frac{p-1}{6}\right)F_{i(p-1)/6}(E^*)
\end{aligned}
$$

for $i = 1, 2$.

It is easy to prove that for $\Phi(X_1, \ldots, X_5)$ we have

$$
\begin{aligned}
&\Phi(X_1, \ldots, X_5) \\
&\quad = \bigg(1 - p\bigg(-\frac{1}{6}X_1^3 + \frac{1}{2}X_1X_2 - \frac{1}{3}X_3\bigg), \\
&\qquad - X_1 - p\bigg(\frac{1}{24}X_1^4 + \frac{1}{3}X_1X_3 + \frac{1}{8}X_2^2 - \frac{1}{4}X_1^2X_2 - \frac{1}{4}X_4\bigg), \\
&\qquad \frac{1}{2}(X_1^2 - X_2) - p\bigg(-\frac{1}{120}X_1^5 + \frac{1}{4}X_1X_4 + \frac{1}{6}X_2X_3 \\
&\qquad + \frac{1}{12}X_1^3X_2 - \frac{1}{6}X_1^2X_3 - \frac{1}{8}X_1X_2^2 - \frac{1}{5}X_5\bigg)\bigg).
\end{aligned}
$$

Hence

$$
\begin{aligned}
&\pm\left(\frac{-1}{3}\right)^{\alpha_3}(x_0+x_1+x_2)^{\alpha_3}\Phi(\alpha_1S_1, \ldots, \alpha_5S_5) \\
&\qquad\qquad \equiv (2+2p)^{(p-1)/6}\Phi(T_1, \ldots, T_5) \pmod{p^2}.
\end{aligned}
$$

Proof of Theorem 1. Let $g_1(X), \ldots, g_r(X)$ be polynomials such that $g_i(X) \not\equiv 0 \pmod{X}$. Let

$$g(X) \equiv g_1(X)^{b_1} \ldots g_r(X)^{b_r} \pmod{X^M}.$$

Let s_j be the homomorphism defined in [4]. We have

$$s_j(g(X)) = b_1s_j(g_1(X)) + b_2s_j(g_2(X)) + \ldots + b_rs_j(g_r(X)),$$

for $j = 1, \ldots, M-1$. Define

$$X_j = b_1s_j(g_1(X)) + b_2s_j(g_2(X)) + \ldots + b_rs_j(g_r(X))$$

for $j = 1, \ldots, M-1$. Let

$$g(X) \equiv C_0 + C_1X + C_2X^2 + \ldots + C_{M-1}X^{M-1} \pmod{X^M}.$$

Consider the reciprocal polynomial

$$F(X) = X^{M-1} + \frac{C_1}{C_0}X^{M-2} + \ldots + \frac{C_{M-1}}{C_0}.$$

By the definition of the homomorphism s_j (see [4]) we have

$$X_j = \text{sum of the } j\text{th powers of the roots of } F(X).$$

The numbers $C_1/C_0, C_2/C_0, \ldots, C_{M-1}/C_0$ can be calculated by the Newton recurrence formula.

According to [2] and [4] we have:

Proposition 1. *There is a number* $\pi \in \mathbb{Q}(\zeta_p + \zeta_p^{-1}), \pi \mid p$ *such that*

(i) $N_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})/\mathbb{Q}}(\pi) = (-1)^m p$,

(ii) $\sigma(\pi) \equiv g\pi \pmod{\pi^{2m+1}}$, $g \equiv a^{2p} \pmod{p^2}$,

(iii) $\zeta_p + \zeta_p^{-1} \equiv \sum_{i=0}^{2m} a_i \pi^i \pmod{\pi^{2m+1}}$, *where* $0 \le a_i < p$ *and* $a_i \equiv (2/(2i)!) \pmod{p}$ *for* $i = 1, \ldots, m$.

The numbers a_{m+i} *for* $i = 1, \ldots, m$, *are defined by*

$$a_{m+1} = 2\frac{p-1-p(p+1)B_{p-1}}{p}.$$

If 2 *is a primitive root modulo* p *then the coefficients* $a_{m+2}, a_{m+3}, \ldots, a_{2m}$ *are given by the recurrence formula*

$$a_{m+1+s} \equiv \frac{1}{4^{s+1}-4}\left(\frac{4^{p(s+1)}a_{s+1} - b_{s+1}}{p} + b_{m+s+1}\right) \pmod{p},$$

where b_{s+1} *and* b_{m+1+s} *are the coefficients of* X^{s+1} *and* X^{m+1+s}, *respectively*, *in the polynomial*

$$\left(2 + \frac{2}{2!}X + \ldots + \frac{2}{(p-1)!}X^m + a_{m+1}X^{m+1} + \ldots + a_{m+s}X^{m+s}\right)^2. \ \blacksquare$$

Proposition 2. *Let* $K \subset \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ *with* $[K : \mathbb{Q}] = n$. *There is a number* $\pi \in K$ *with* $\pi \mid p$ *such that*

(i) $N_{K/\mathbb{Q}}(\pi) = (-1)^n p$,

(ii) $\sigma(\pi) \equiv g\pi \pmod{\pi^{n+1}}$, $g \equiv a^{p(p-1)/n} \pmod{p^2}$,

(iii) $\beta_0 \equiv \sum_{i=0}^{2n} a_i^* \pi^i \pmod{\pi^{2n+1}}$, *where* $0 \le a_i^* < p$ *and where* $a_i^* \equiv ((p-1)/n)/(i(p-1)/n)! \pmod{p}$ *for* $i = 1, \ldots, n$. $\blacksquare$

From now on we will use the following transformation. Let

$$\gamma \equiv c_0 + c_1\pi + c_2\pi^2 + \ldots + c_{2l-1}\pi^{2l-1} \pmod{\pi^{2l}}.$$

From $\pi^l \equiv -p \pmod{\pi^{2l}}$ we have

$$\gamma \equiv (c_0 - pc_l) + (c_1 - pc_{l+1})\pi + \ldots + (c_{l-1} - pc_{2l-1})\pi^{l-1} \pmod{\pi^{2l}}.$$

Lemma 1. *Let* $\alpha, \beta \in K$ *with* $\alpha\beta \not\equiv 0 \pmod{\pi}$. *Let*

$$\alpha \equiv e_0 + e_1\pi + \ldots + e_{l-1}\pi^{l-1} \pmod{\pi^{2l}},$$
$$\beta \equiv b_0 + b_1\pi + \ldots + b_{l-1}\pi^{l-1} \pmod{\pi^{2l}}.$$

Relate to the conjugation $\sigma^i(\alpha)$ *the polynomial*

$$f_i(X) = e_0 + e_1 g^i X + e_2 g^{2i} X^2 + \ldots + e_{l-1} g^{i(l-1)} X^{l-1}.$$

Let

$$F(X) \equiv f_0(X)^{c_0} f_1(X)^{c_1} \ldots f_{l-2}(X)^{c_{l-2}}$$
$$\equiv d_0 + d_1 X + \ldots + d_{2l-1} X^{2l-1} \pmod{X^{2l}}.$$

Define $X_i = s_i(F(X))$. *Then*

$$\alpha^{c_0} \sigma(\alpha)^{c_1} \ldots \sigma^{l-2}(\alpha)^{c_{l-2}} \equiv \beta \pmod{p^2}$$

if and only if

$$d_0 \Phi(X_1, \ldots, X_{2l-2}) \equiv (b_0, b_1, \ldots, b_{l-1}) \pmod{p^2}.$$

P r o o f. Clearly

$$\alpha^{c_0} \sigma(\alpha)^{c_1} \ldots \sigma^{l-2}(\alpha)^{c_{l-2}} \equiv d_0 + d_1 \pi + \ldots + d_{2l-1} \pi^{2l-1} \pmod{\pi^{2l}}.$$

The coefficients $d_1/d_0, d_2/d_0, \ldots, d_{2l-1}/d_0$ can be expressed using the numbers $X_1, \ldots, X_{2l-1}$ by the Newton recurrence formula. Clearly

$$d_0 + d_1 \pi + \ldots + d_{2l-1} \pi^{2l-1}$$
$$\equiv (d_0 - p d_l) + (d_1 - p d_{l+1}) \pi + \ldots + (d_{l-1} - p d_{2l-1}) \pi^{l-1} \pmod{\pi^{2l}}.$$

From the definition of the mapping Φ it follows that

$$(d_0 - p d_l, d_1 - p d_{l+1}, \ldots, d_{l-1} - p d_{2l-1}) \equiv d_0 \Phi(X_1, X_2, \ldots, X_{2l-1}) \pmod{p^2}.$$

Lemma 1 is proved. ∎

Proposition 2 gives

$$\beta_0 \equiv -1/l + (a_1^* - p a_{l+1}^*) \pi + \ldots + (a_{l-1}^* - p a_{2l-1}^*) \pi^{l-1} \pmod{\pi^{2l}},$$

where $0 \le a_i^* < p$ and $a_i^* \equiv ((p-1)/n)/(i(p-1)/n)! \pmod p$ for $i = 1, \ldots, l-1$. According to [4] we have

$$a_i^* - p a_{l+i}^* \equiv A_i(l) \pmod{p^2}.$$

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

$$\delta \equiv -\frac{1}{l}(x_0 + x_1 + \ldots + x_{l-1})$$
$$+ \sum_{i=1}^{l-1} A_i(l)(x_0 + x_1 g^i + x_2 g^{2i} + \ldots + x_{l-1} g^{i(l-1)}) \pi^i \pmod{\pi^{2l}}.$$

Let

$$\delta^{c_0} \sigma(\delta)^{c_1} \ldots \sigma^{l-2}(\delta)^{c_{l-2}} = \eta_2^f.$$

Then X_j corresponding to the product on the left-hand side is equal to

$$c_0 s_j(\delta) + c_1 g^j s_j(\delta) + \ldots + c_{l-2} g^{j(l-2)} s_j(\delta) = \alpha_j S_j$$

for $j = 1, \ldots, 2l-1$. Hence the number corresponding to the left-hand side is

$$\left(\frac{x_0 + x_1 + \ldots + x_{l-1}}{-l}\right)^{\alpha_l} \Phi(\alpha_1 S_1, \ldots, \alpha_{2l-1} S_{2l-1}).$$

Now we prove that the right-hand side is equal to

$$(2+2p)^{f(p-1)/l} \Phi(fT_1, \ldots, fT_{2l-1}).$$

By Proposition 1 we have

$$\zeta_p + \zeta_p^{-1} \equiv \sum_{i=0}^{2m} a_i \pi^i \pmod{\pi^{2m+1}},$$

where $0 \le a_i < p$ and $a_i \equiv (2/(2i)!) \pmod{p}$ for $i = 1, \ldots, m$, and hence

$$\zeta_p + \zeta_p^{-1} \equiv A_0(m) + A_1(m)\pi + \ldots + A_{m-1}(m)\pi^{m-1} \pmod{\pi^{2m}}.$$

Consider the polynomial

$$g(X) = A_0(m)X^{m-1} + A_1(m)X^{m-2} + \ldots + A_{m-1}(m).$$

Now we shall calculate the numbers

$$s_i = \text{sum of the } i\text{th powers of the roots of } g(X)$$

for $i = 1, \ldots, 2m-1$ modulo p^2. It is easy to see that for $i > m-1$ it is enough to determine s_i modulo p. Let $W_1, W_2, \ldots$ be a linearly recurrent sequence modulo p of order $m-1$ defined by

$$W_i = \frac{-1}{(2i)!} 2^{2i-1}(2^{2i}-1)B_{2i} \quad \text{for } i = 1, \ldots, m-1.$$

For $i > m-1$ we have

$$W_i = -\left(\frac{1}{2!}W_{i-1} + \frac{1}{4!}W_{i-2} + \ldots + \frac{1}{(2m-2)!}W_{i-m+1}\right).$$

Lemma 2. *The following congruence holds*:

$$s_{n+1} \equiv \frac{-1}{(2n+2)!} 2^{2n+1}(2^{2n+2}-1)B_{2n+2} - \frac{n+1}{2} G_{n+1}(E^*) \pmod{p^2}$$

for $n+1 < m$.

Proof. It is easy to see that $A_0(m) \equiv 2 + 2p \pmod{p^2}$. Clearly

$$(2+2p)\frac{1-p}{2} \equiv 1 \pmod{p^2}.$$

Consider the polynomial

$$g^*(X) = X^{m-1} + C_1 X^{m-2} + \ldots + C_{m-1},$$

where

$$C_i \equiv \frac{1-p}{2} A_i(m) \pmod{p^2}.$$

Obviously s_n is equal to the sum of the nth powers of the roots of $g^*(X)$. Write

$$C_1 = c_1 + b_1 p, \quad C_2 = c_2 + b_2 p, \ \dots, \ C_{m-1} = c_{m-1} + b_{m-1} p.$$

It is known that there exists a polynomial $f_n(x_1, \dots, x_n)$ such that

$$s_n = f_n(c_1 + b_1 p, \dots, c_n + b_n p).$$

Write $s_n = r_n + t_n p$. Clearly $r_1 + t_1 p = -(c_1 + b_1 p)$. Put $t_1 = -b_1$.

According to the Newton recurrent formula we have

$$r_2 + t_2 p + (c_1 + b_1 p)(r_1 + t_1 p) + 2(c_2 + p b_2) = 0.$$

The last equation can be rewritten in the form

$$r_2 + c_1 r_1 + 2c_2 + p(t_2 + c_1 t_1 + r_1 b_1 + 2b_2) = 0.$$

Define $F_2 = r_1 b_1 + 2b_2$. Hence $r_2 + c_1 r_1 + 2c_2 + p(t_2 + c_1 t_1 + F_2) = 0$. Put $t_2 = -(c_1 t_1 + F_2)$.

Further we have

$$r_3 + t_3 p + (c_1 + b_1 p)(r_2 + t_2 p) + (c_2 + b_2 p)(r_1 + t_1 p) + 3(c_3 + b_3 p) = 0,$$

hence

$$r_3 + c_1 r_2 + c_2 r_1 + 3c_3 + p(t_3 + c_1 t_2 + c_2 t_1 + b_1 r_2 + b_2 r_1 + 3b_3) = 0.$$

Define $F_3 = b_1 r_2 + b_2 r_1 + 3b_3$. Then we put

$$\begin{aligned}
t_3 &= t_1(c_1^2 - c_2) + c_1 F_2 - F_3,\\
t_4 &= t_1(-c_1^3 + 2c_1 c_2 - c_3) - (c_1^2 - c_2)F_2 + c_1 F_3 - F_4,\\
t_5 &= t_1(c_1^4 - 3c_1^2 c_2 + 2c_1 c_3 + c_2^2 - c_4) - (-c_1^3 + 2c_1 c_2 - c_3)F_2\\
&\qquad - (c_1^2 - c_2)F_3 + c_1 F_4 - F_5.
\end{aligned}$$

Consider the numbers

$$K_2 = -c_1, \quad K_4 = c_1^2 - c_2, \quad K_6 = -c_1^3 + 2c_1 c_2 - c_3, \ \dots$$

The numbers $c_1, c_2, c_3, \dots$ are equal to $1/2!, 1/4!, 1/6!, \dots$ modulo p. Define

$$K_{2n} = K_{2n}^*/(2n)!.$$

Then

$$\frac{K_{2n}^*}{(2n)!} + \frac{1}{(2)!} \cdot \frac{K_{2n-2}^*}{(2n-2)!} + \dots + \frac{1}{(2n-2)!} \cdot \frac{K_2^*}{2!} + \frac{1}{(2n)!} = 0,$$

hence

$$\frac{1}{(2n)!}\left(K_{2n}^* + \binom{2n}{2} K_{2n-2}^* + \dots + 1\right) = 0,$$

and therefore $K_{2n}^* = E_{2n}$, the Euler number. Using induction by n we put

$$t_{n+1} = t_1 \frac{E_{2n}}{(2n)!} - F_2 \frac{E_{2n-2}}{(2n-2)!} - \dots - F_{n+1}, \tag{4}$$

where

$F_2 = b_1 r_1 + 2b_2, \quad F_3 = b_1 r_2 + b_2 r_1 + 3b_3, \quad F_4 = b_1 r_3 + b_2 r_2 + b_3 r_1 + 4b_4, \ \ldots$

Since $t_1 = -b_1$, we have

$$\begin{aligned} t_{n+1} = & -b_1 \frac{E_{2n}}{(2n)!} - \frac{E_{2n-2}}{(2n-2)!}(b_1 r_1 + 2b_2) \\ & - \ldots - (b_1 r_n + b_2 r_{n-1} + \ldots + (n+1) b_{n+1}). \end{aligned}$$

In the last equation we first cancel the brackets by multiplication and then make new brackets by factoring out $b_1, \ldots, b_{n+1}$. The summand obtained by factoring out b_1 is

$$b_1 \left(\frac{E_{2n}}{(2n)!} + r_1 \frac{E_{2n-2}}{(2n-2)!} + \ldots + r_n \right). \tag{5}$$

According to [4, Lemma 3],

$$r_i \equiv -\frac{1}{(2i)!} 2^{2i-1}(2^{2i}-1) B_{2i} \pmod{p}.$$

By substitution into (5) we get the sum

$$\begin{aligned} \frac{E_{2n}}{(2n)!} - \frac{E_{2n-2}}{(2n-2)!} \cdot \frac{1}{2!} 2(2^2-1) B_2 - \frac{E_{2n-4}}{(2n-4)!} \cdot \frac{1}{4!} 2^3 (2^4-1) B_4 \\ - \ldots - \frac{1}{(2n)!} 2^{2n-1}(2^{2n}-1) B_{2n}. \end{aligned}$$

The following identity holds:

$$\begin{aligned} \frac{E_{2n}}{(2n)!} - \frac{E_{2n-2}}{(2n-2)!} \cdot \frac{1}{2!} 2(2^2-1) B_2 - \frac{E_{2n-4}}{(2n-4)!} \cdot \frac{1}{4!} 2^3 (2^4-1) B_4 \\ - \ldots - \frac{1}{(2n)!} 2^{2n-1}(2^{2n}-1) B_{2n} = (n+1) \frac{E_{2n}}{(2n)!}. \end{aligned} \tag{6}$$

This identity can be proved in the following way. For the functions $\sec x$ and $\tan x$, we have

$$\begin{aligned} \sec x &= 1 - \frac{E_2}{2!} x^2 + \frac{E_4}{4!} x^4 - \frac{E_6}{6!} x^6 + \ldots, \\ \tan x &= 2^2(2^2-1) B_2 \frac{x}{2!} - 2^4 (2^4-1) B_4 \frac{x^3}{4!} + \ldots \end{aligned}$$

Then

$$\tan x \cdot \sec x = \frac{2^2(2^2-1)}{2!} B_2 x - \left(\frac{E_2 B_2 2^2 (2^2-1)}{2!2!} + \frac{2^4(2^4-1) B_4}{4!} \right) x^3 + \ldots$$

The identity (6) follows from the equation

$$\frac{d(\sec x)}{dx} = \tan x \cdot \sec x.$$

Using the identity (6), by induction ($n+1 \to 1$) we have

$$t_{n+1} = -(n+1)\left(b_1 \frac{E_{2n}}{(2n)!} + b_2 \frac{E_{2n-2}}{(2n-2)!} + \ldots + b_{n+1}\right). \tag{7}$$

The numbers $a_1, \ldots, a_{m-1}$ from Proposition 1 are

$$a_i \equiv \frac{2}{(2i)!} \pmod{p}, \qquad 0 < a_i < p.$$

Define the numbers D_i as follows:

$$\frac{1-p}{2} a_i + pD_i \equiv \frac{1}{(2i)!} \pmod{p^2}, \qquad 0 \le D_i < p,$$

hence

$$D_i \equiv \frac{1}{p}\left(\frac{1}{(2i)!} - \frac{1-p}{2} a_i\right) \pmod{p}.$$

Let v_{n+1} be the sum of the $(n+1)$th powers of the roots of the polynomial

$$X^{m-1} + \frac{1-p}{2} a_1 X^{m-2} + \ldots + \frac{1-p}{2} a_{m-1}.$$

According to [4, Lemma 3], the sum of the $(n+1)$th powers of the roots of the polynomial

$$X^{m-1} + \frac{1}{2!} X^{m-2} + \frac{1}{4!} X^{m-3} + \ldots + \frac{1}{(2m-2)!},$$

is equal to

$$\frac{-1}{(2n+2)!} 2^{2n+1} (2^{2n+2} - 1) B_{2n+2}.$$

Hence

$$\begin{aligned} v_{n+1} &= \frac{-1}{(2n+2)!} 2^{2n+1} (2^{2n+2} - 1) B_{2n+2} \\ &\quad + p(n+1)\left(D_1 \frac{E_{2n}}{(2n)!} + D_2 \frac{E_{2n-2}}{(2n-2)!} + \ldots + D_{n+1}\right). \end{aligned}$$

Therefore

$$\begin{aligned} s_{n+1} &= \frac{-1}{(2n+2)!} 2^{2n+1} (2^{2n+2} - 1) B_{2n+2} \\ &\quad + p(n+1)\left(D_1 \frac{E_{2n}}{(2n)!} + D_2 \frac{E_{2n-2}}{(2n-2)!} + \ldots + D_{n+1}\right) \\ &\quad - p(n+1)\left(b_1 \frac{E_{2n}}{(2n)!} + b_2 \frac{E_{2n-2}}{(2n-2)!} + \ldots + b_{n+1}\right). \end{aligned} \tag{8}$$

Since

$$D_i \equiv \frac{1}{p}\left(\frac{1}{(2i)!} - \frac{1-p}{2} a_i\right),$$

from (8) we get

$$(9)\quad s_{n+1} = \frac{-1}{(2n+2)!}2^{2n+1}(2^{2n+2}-1)B_{2n+2} - \frac{(n+1)E_{2n+2}}{(2n+2)!} + (n+1)\frac{p-1}{2}\left(a_1\frac{E_{2n}}{(2n)!} + a_2\frac{E_{2n-2}}{(2n-2)!} + \ldots + a_{n+1}\right) + p\frac{n+1}{2}\left(a_{m+1}\frac{E_{2n}}{(2n)!} + a_{m+2}\frac{E_{2n-2}}{(2n-2)!} + \ldots + a_{m+n+1}\right),$$

where $a_1, \ldots, a_m, a_{m+1}, a_{m+2}, \ldots$ are the numbers from Proposition 1. Since $A_i(m) = a_i - pa_{m+i}$, from the equality (9) we get

$$s_{n+1} = \frac{-1}{(2n+2)!}2^{2n+1}(2^{2n+2}-1)B_{2n+2} - \frac{n+1}{2}G_{n+1}(E^*). \ \blacksquare$$

LEMMA 3. *The following congruence holds*:

$$W_{m+j} \equiv -\frac{1}{(p-1+2j)!}2^{p-1+2j-1}(2^{p-1+2j}-1)B_{p-1+2j} + (m+j)F_j(E^*) \pmod p$$

for $j = 1, \ldots, m-1$.

Proof. Let $n > 2p-3$. Consider the polynomial

$$h(X) = X^n + \frac{1}{2!}X^{n-1} + \frac{1}{4!}X^{n-2} + \ldots + \frac{1}{(2n)!}.$$

Let W_i^* be the sum of the ith powers of the roots of $h(X)$. By [4, Lemma 3],

$$W_i^* = -\frac{1}{(2i)!}2^{2i-1}(2^{2i}-1)B_{2i}.$$

The characteristic polynomial of the sequence W_i is

$$X^{m-1} + \frac{1}{2!}X^{m-2} + \frac{1}{4!}X^{m-3} + \ldots + \frac{1}{(2m-2)!}.$$

Hence W_i is the sum of the ith powers of the roots of this polynomial.

Let

$$c_1 = \frac{1}{2!}, \quad c_2 = \frac{1}{4!}, \ \ldots$$

Obviously

$$W_m = W_m^* + mc_m,$$
$$W_{m+1} = W_{m+1}^* + c_mW_1 + (m+1)c_{m+1} - c_1mc_m.$$

We can write

$$G_m = mc_m, \qquad G_{m+1} = (m+1)c_{m+1} - c_1G_m.$$

By induction we can prove that

$$(10)\quad \begin{aligned} W_{m+j} = W^*_{m+j} &+ c_m W_j + (c_{m+1} + c_m E^*_1) W_{j-1} \\ &+ (c_{m+2} + c_{m+1} E^*_1 + c_m E^*_2) W_{j-2} + \dots \\ &+ (c_{m+j-1} + c_{m+j-2} E^*_1 + \dots + c_m E^*_{j-1}) W_1 + G_{m+j}. \end{aligned}$$

Now we rewrite the right side of (10). We cancel the brackets by multiplication and make new brackets by factoring out $c_m, c_{m+1}, \dots$

E.g., the summand obtained by factoring out c_m is

$$c_m (W_j + E^*_1 W_{j-1} + E^*_2 W_{j-2} + \dots + E^*_{j-1} W_1).$$

From (6) we get

$$c_m (W_j + E^*_1 W_{j-1} + E^*_2 W_{j-2} + \dots + E^*_{j-1} W_1) = c_m j E^*_j.$$

By repeating this procedure with each summand we have

$$(11)\quad \begin{aligned} &W_{m+j} \\ &= W^*_{m+j} + j c_m E^*_j + (j-1) c_{m+1} E^*_{j-1} + \dots + c_{m+j-1} E^*_1 + G_{m+j}. \end{aligned}$$

By induction it is easy to prove

$$(12)\qquad G_{m+j} = (m+1) c_{m+j} + (m+j-1) c_{m+j-1} E^*_1 + \dots + m c_m E^*_j.$$

Substituting (12) into (11) we get

$$W_{m+j} = W^*_{m+j} + (m+j)(c_{m+j} + c_{m+j-1} E^*_1 + \dots + c_m E^*_j). \ \blacksquare$$

Since $\eta_2 = N_{\mathbb{Q}(\zeta_p + \zeta_p^{-1})/K}(\zeta_p + \zeta_p^{-1})$ we have

$$\eta_2^f \equiv r_0 + \sum_{i=1}^{l-1} r_{i(p-1)/(2l)} \pi^{i(p-1)/(2l)} \pmod{\pi^{2m}},$$

where $r_0 = (2+2p)^{f(p-1)/(2l)}$. From Lemmas 1–3 we deduce that the right-hand side is equal to

$$(2+2p)^{f(p-1)/(2l)} \Phi(fT_1, \dots, fT_{2l-1}).$$

It remains to prove that $T_l = (1-q_2)/2$. From the proof of Lemma 3 we have

$$T_l \equiv \frac{-1}{(p-1)!} 2^{p-2} (2^{p-1} - 1) B_{p-1} + \frac{p-1}{2} \cdot \frac{1}{(p-1)!},$$

hence

$$T_l \equiv \frac{-1}{(p-1)!} 2^{p-2} \frac{2^{p-1} - 1}{p} p B_{p-1} + \frac{p-1}{2} \cdot \frac{1}{(p-1)!}.$$

From $pB_{p-1} \equiv -1 \pmod{p}$ the required congruence follows. Theorem 1 is proved. $\blacksquare$

Example 1 ($p = 13, l = 3$, $K \subset \mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$, $[K : \mathbb{Q}] = 3$). By Proposition 1 we have

$$\zeta_{13} + \zeta_{13}^{-1} \equiv 2 + \pi + 12\pi^2 + 3\pi^3 + 4\pi^4 + 9\pi^5 + 11\pi^6 + 2\pi^7 + 12\pi^8 + 8\pi^9 + 10\pi^{10} + 4\pi^{11} \pmod{\pi^{12}},$$

hence

$$\begin{aligned}\zeta_{13} + \zeta_{13}^{-1} &\equiv A_0(m) + A_1(m)\pi + \ldots + A_5(m)\pi^5\\ &\equiv 28 + 144\pi + 25\pi^2 + 68\pi^3 + 43\pi^4 + 126\pi^5 \pmod{\pi^{12}}.\end{aligned}$$

It is easy to see that

$$\begin{aligned}\eta_2 &= N_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})/K}(\zeta_p + \zeta_p^{-1})\\ &\equiv (28 + 144\pi + 25\pi^2 + 68\pi^3 + 43\pi^4 + 126\pi^5)\\ &\quad \times (28 - 144\pi + 25\pi^2 - 68\pi^3 + 43\pi^4 - 126\pi^5)\\ &\equiv 56 + 86\pi^2 + 50\pi^4 \pmod{\pi^{12}}.\end{aligned}$$

The number $\beta_0 = \zeta_{13} + \zeta_{13}^5 + \zeta_{13}^8 + \zeta_{13}^{12}$ is the Gauss period. By Proposition 2 we have

$$\beta_0 \equiv -\tfrac{1}{3} + A_1(3)\pi + A_2(3)\pi^2 \pmod{\pi^6}$$

(π is a prime divisor of the field K, $[K : \mathbb{Q}] = 3$, $\pi \mid p$). For $A_1(3), A_2(3)$ we have

$$\tau(\chi)^3 \equiv 27A_1(3)^3(-13) \pmod{\mathfrak{p}^3}, \quad A_1(3) \equiv \frac{4}{4!} \pmod{13},$$
$$-1 \equiv 27^2 A_1(3)^3 A_2(3)^3 \pmod{169}, \quad A_2(3) \equiv \frac{4}{8!} \pmod{13}.$$

The number g satisfies $g \equiv 2^{4\cdot 13} \equiv 146 \pmod{169}$, and

$$\tau(\chi)^3 = pJ(\chi,\chi), \qquad J(\chi,\chi) = -4 - 3\zeta_3.$$

Hence $A_1(3) \equiv 4/4! \equiv 11 \pmod{13}$. Thus

$$-\left(-4 - 3\frac{1}{146}\right) \equiv 27(11 + 13k)^3 \pmod{169}.$$

It follows that $A_1(3) = 50, A_2(3) = 86$.

The fundamental unit of the field K is $\delta = \beta_2$. Hence

$$d_1 = -3 \cdot 50 \cdot 146^2 \equiv 80 \pmod{169}, \qquad d_2 = -3 \cdot 86 \cdot 146 \equiv 19 \pmod{169}.$$

Therefore

$$S_1 = -80, \quad S_2 = 109, \quad S_3 = 2, \quad S_4 = 5, \quad S_5 = 4.$$

A calculation gives

$$T_1 = 154, \quad T_2 = 109, \quad T_3 = 12, \quad T_4 = 12, \quad T_5 = 4.$$

Clearly $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = \alpha_5 = 1$, hence the relevant congruence is

$$\pm\Big(-\frac{1}{3}\Big)^{\alpha_3} \Phi(-80, 109, 2, 5, 4) \equiv 28^2 \Phi(154, 109, 12, 12, 4)$$
$$\equiv (56, 86, 50) \pmod{169}. \ \blacksquare$$

Example 2. We have

$$\begin{aligned}\zeta_{37} + \zeta_{37}^{-1} \equiv{}& 2 + \pi + 34\pi^2 + 11\pi^3 + 22\pi^4 + 6\pi^5 + 32\pi^6 + 14\pi^7 \\ &+ 9\pi^8 + 12\pi^9 + 16\pi^{10} + 5\pi^{11} + 23\pi^{12} + 24\pi^{13} \\ &+ 20\pi^{14} + 3\pi^{15} + 26\pi^{16} + 33\pi^{17} + 35\pi^{18} + 25\pi^{19} \\ &+ 29\pi^{20} + 11\pi^{21} + 10\pi^{22} + 10\pi^{23} + 11\pi^{24} + 8\pi^{25} \\ &+ 8\pi^{26} + 19\pi^{27} + 20\pi^{28} + 19\pi^{29} + 8\pi^{30} + 36\pi^{31} \\ &+ 12\pi^{32} + 18\pi^{33} + 31\pi^{34} + 35\pi^{35} + 3\pi^{36} \pmod{\pi^{37}}.\end{aligned}$$

Therefore $A_0(m) = 76$, $A_1(m) = 445$, $A_2(m) = 330$, $A_3(m) = 973$, $A_4(m) = 1021$, $A_5(m) = 1005$, $A_6(m) = 994$, $A_7(m) = 1087$, $A_8(m) = 1082$, $A_9(m) = 678$, $A_{10}(m) = 645$, $A_{11}(m) = 671$, $A_{12}(m) = 1096$, $A_{13}(m) = 61$, $A_{14}(m) = 945$, $A_{15}(m) = 706$, $A_{16}(m) = 248$, $A_{17}(m) = 107$.

References

[1] K. Q. Feng, *The Ankeny–Artin–Chowla formula for cubic cyclic number fields*, J. China Univ. Sci. Tech. 12 (1982), 20–27.

[2] S. Jakubec, *The congruence for Gauss period*, J. Number Theory 48 (1994), 36–45.

[3] —, *On divisibility of class number of real Abelian fields of prime conductor*, Abh. Math. Sem. Univ. Hamburg 63 (1993), 67–86.

[4] —, *On Vandiver's conjecture*, ibid. 64 (1994), 105–124.

[5] —, *Congruence of Ankeny–Artin–Chowla type for cyclic fields of prime degree l*, Math. Proc. Cambridge Philos. Soc., to appear.

[6] A. A. Kiselev and I. Sh. Slavutskiĭ, *The transformation of Dirichlet's formulas and the arithmetical computation of the class number of quadratic fields*, in: Proc. Fourth All-Union Math. Congr. (Leningrad 1961), Vol. II, Nauka, Leningrad, 1964, 105–112 (in Russian).

[7] F. Marko, *On the existence of p-units and Minkowski units in totally real cyclic fields*, Abh. Math. Sem. Univ. Hamburg, to appear.

[8] R. Schertz, *Über die analytische Klassenzahlformel für reelle abelsche Zahlkörper*, J. Reine Angew. Math. 307/308 (1979), 424–430.

[9] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), 181–234.

[10] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, in: Séminaire de Théorie des Nombres, Paris 1979–80, M.-J. Bertin (ed.), Progr. Math. 12, Birkhäuser, 1981, 277–286.

Matematický ústav SAV
Štefánikova 49
814 73 Bratislava, Slovakia

Received on 16.11.1994
and in revised form on 12.7.1995 (2696)