ACTA ARITHMETICA
LXXXV.4 (1998)

Note on the congruence of Ankeny–Artin–Chowla type modulo p^2

by

Stanislav Jakubec (Bratislava)

The results of [2] on the congruence of Ankeny–Artin–Chowla type modulo p^2 for real subfields of $\mathbb{Q}(\zeta_p)$ of a prime degree l is simplified. This is done on the basis of a congruence for the Gauss period (Theorem 1). The results are applied for the quadratic field $\mathbb{Q}(\sqrt{p})$, $p \equiv 5 \pmod 8$ (Corollary 1).

Notations

- B_n, E_n — Bernoulli and Euler numbers,
- $C_n = \dfrac{2^{n+1}(1-2^{n+1})B_{n+1}}{n+1}$,
- $Q_2 = \dfrac{2^{p-1}-1}{p}$ — Fermat quotient,
- $W_p = \dfrac{1+(p-1)!}{p}$ — Wilson quotient,
- $A_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n}$, $A_0 = 0$.

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

Let a be a fixed primitive root modulo p, let χ be the Dirichlet character of order n, $n \mid p-1$, $\chi(x) = \zeta_n^{\operatorname{ind}_a x}$. 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 $A_0(n), A_1(n), \ldots, A_{n-1}(n)$ by

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

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

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

1991 *Mathematics Subject Classification*: Primary 11R29.

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 δ be the unit

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

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 $S_j = S_j(d_1, \ldots, d_{l-1})$ = sum of jth 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

$$T_l = \frac{1-Q_2}{2}, \quad \text{where } Q_2 = \frac{2^{p-1}-1}{p},$$

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

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

Define

$$\alpha_i = c_0 + c_1 g^i + c_2 g^{2i} + \ldots + c_{l-2} g^{(l-2)i}$$

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:

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

THEOREM 1 OF [2]. *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 lth 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 $\alpha_i = c_0 + c_1 g^i + c_2 g^{2i} + \ldots + c_{l-2} g^{(l-2)i}$ 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 $\varepsilon = \pm 1$.

This theorem is applied to the real quadratic field.

The quadratic case: $K = \mathbb{Q}(\sqrt{p})$, $p \equiv 5 \pmod 8$ *and* $T + U\sqrt{p} > 1$ *is the fundamental unit*. By [2] 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

$$T_1 = -\frac{1}{((p-1)/2)!} 2^{(p-1)/2-1}(2^{(p-1)/2} - 1)B_{(p-1)/2} - \frac{p-1}{8} G_{(p-1)/4}(E^*),$$

$$T_2 = \tfrac{1}{2}(1 - Q_2),$$

$$T_3 = -\frac{1}{(3(p-1)/2)!} 2^{3(p-1)/2-1}(2^{3(p-1)/2} - 1)B_{3(p-1)/2} + \frac{3(p-1)}{4} F_{(p-1)/4}(E^*).$$

It is easy to see that

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

Hence

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

The greatest difficulty in applying Theorem 1 of [2] to fields of concrete degrees $l = 2, 3, \ldots$ is caused by the fact that the numbers $A_i(n)$, $G_j(E^*)$ and $F_j(E^*)$ are defined in a very complicated way. This constraint appears also in the case of a quadratic field, because of the unclear values $G_{(p-1)/4}(E^*)$ and $F_{(p-1)/4}(E^*)$ involved.

The aim of this paper is to eliminate the above mentioned constraints. This will be done on the basis of a congruence for the Gauss period (Theorem 1). The results will be applied to the real quadratic field $\mathbb{Q}(\sqrt{p})$, $p \equiv 5 \pmod 8$. In this case we get a simple congruence modulo p^2 (Corollary 1) involving: the fundamental unit $T + U\sqrt{p}$, the class number h, the Bernoulli numbers $B_{(p-1)/2}$, $B_{3(p-1)/2}$ and the Fermat quotient Q_2.

1. Congruence for the Gauss period. Let $p \equiv 1 \pmod n$ be prime and let K be a subfield of the field $\mathbb{Q}(\zeta_p)$ of the degree n over $\mathbb{Q}$. Let a be a primitive root modulo p. We consider the automorphism σ of the field $\mathbb{Q}(\zeta_p)$ such that $\sigma(\zeta_p) = \zeta_p^a$.

Further we denote:

$$\beta_0 = \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p); \quad \beta_i = \sigma^i(\beta_0) \quad \text{for } i = 1, \ldots, n-1;$$
$$k = (p-1)/n; \quad a^k \equiv g \pmod p.$$

In [3] the following theorem is proved:

Theorem 1 of [3]. *There is a number $\pi \in K$ with $\pi \mid p$ such that*

(i) $N_{K/\mathbb{Q}}(\pi) = (-1)^n p$,
(ii) $\sigma(\pi) \equiv g\pi \pmod{\pi^{n+1}}$,
(iii) $\beta_0 \equiv k \sum_{i=0}^{n} \frac{1}{(ki)!}\pi^i \pmod{\pi^{n+1}}$.

In [4], it is proved that for any t there exists $\pi \in K$ such that

$$\sigma\pi \equiv g\pi \pmod{\pi^{tn+1}}, \quad \text{where } g^n \equiv 1 \pmod{p^t}.$$

Hence

$$\beta_0 \equiv \sum_{i=0}^{tn} a_i \pi^i \pmod{\pi^{tn+1}}, \quad 0 \le a_i < p. \tag{1}$$

Because $\pi^n \equiv -p \pmod{\pi^{tn+1}}$, the congruence (1) can be rewritten as

$$\beta_0 \equiv \sum_{i=0}^{n-1} a_i^* \pi^i \pmod{\pi^{tn+1}},$$

where $a_i^* = a_i - pa_{i+n} + p^2 a_{i+2n} + \ldots$

Hence for any divisor n of $p-1$, $n \neq 1$, there are numbers $a_0^*, a_1^*, \ldots, a_{n-1}^*$ such that

(i) $a_i^* \equiv \dfrac{k}{(ki)!} \pmod{p}$,

(ii) $\beta_0 \equiv \sum_{i=0}^{n-1} a_i^* \pi^i \pmod{\pi^{Sn+1}}$ for any exponent S.

LEMMA 1. *Let p be a prime and let n be a divisor of $p-1$, $n \neq 1$. There exists a prime divisor $\mathfrak{p}$ of the field $\mathbb{Q}(\zeta_n)$ with $\mathfrak{p} \mid p$ such that for any exponent S the following holds*:

(i) $a_i^* \equiv \dfrac{k}{(ki)!} \pmod{p}$ *for* $i = 1, \ldots, n-1$,

(ii) $\tau(\chi^i) \equiv n a_i^* \pi^i \pmod{\mathfrak{p}^S}$.

Proof. Take S and π such that

$$\sigma\pi \equiv g\pi \pmod{\pi^{(S+1)n+1}}, \qquad g^n \equiv 1 \pmod{p^{S+1}}.$$

Then

$$\beta_0 \equiv \sum_{i=0}^{n-1} a_i^* \pi^i \pmod{\pi^{(S+1)n+1}},$$

hence

$$\frac{1}{\pi^i}(\beta_0 - (a_0^* + a_1^*\pi + \ldots + a_{i-1}^*\pi^{i-1})) \equiv a_i^* + a_{i+1}^*\pi + \ldots + a_{n-1}^*\pi^{n-1-i} \pmod{\pi^{(S+1)n+1-i}}.$$

Now take the trace $\mathrm{Tr}_{K/\mathbb{Q}}$ of the right and left sides. For $0 < i < n$ we have

$$\mathrm{Tr}_{K/\mathbb{Q}}(A\pi^i) \equiv 0 \pmod{\pi^{(S+1)n+1}}.$$

It follows that

$$\frac{1}{\pi^i}\left(\beta_0 + \frac{1}{g^i}\sigma\beta_0 + \frac{1}{g^{2i}}\sigma^2\beta_0 + \ldots + \frac{1}{g^{(n-1)i}}\sigma^{n-1}\beta_0\right) \equiv n a_i^* \pmod{\pi^{(S+1)n+1-i}}.$$

Because $g^n \equiv 1 \pmod{p^{S+1}}$, there exists a prime divisor $\mathfrak{p}$ of the field $\mathbb{Q}(\zeta_n)$ with $\mathfrak{p} \mid p$ such that

$$1/g \equiv \zeta_n \pmod{\mathfrak{p}^{S+1}}.$$

Hence

$$\beta_0 + \frac{1}{g^i}\sigma\beta_0 + \frac{1}{g^{2i}}\sigma^2\beta_0 + \ldots + \frac{1}{g^{(n-1)i}}\sigma^{n-1}\beta_0 \equiv \tau(\chi^i) \pmod{\mathfrak{p}^{S+1}}.$$

Because $\pi^n \approx p$, we have $\tau(\chi^i) \equiv n a_i^* \pi^i \pmod{\mathfrak{p}^S}$. ∎

The following theorem gives a congruence for the Gauss period modulo π^{2n+1}. For simplicity, the coefficients are denoted by a_i (instead of a_i^*).

THEOREM 1. *Let p be an odd prime and let π be the above defined element of the field $\mathbb{Q}(\zeta_p)$. Then*

$$\zeta_p \equiv \frac{-1}{p-1} + a_1\pi + a_2\pi^2 + \ldots + a_{p-2}\pi^{p-2} \pmod{\pi^{2(p-1)+1}},$$

where

(i) $a_i \equiv \dfrac{1}{i!} + p\dfrac{1}{(i-1)!}(W_p - A_{i-1}) \pmod{p^2}$ *for* $i = 1, \ldots, (p-3)/2$,

(ii) $a_i a_{p-1-i} \equiv (-1)^{i+1}(1+2p) \pmod{p^2}$.

REMARK. On the basis of this theorem a congruence modulo $\pi^{2(p-1)+1}$ for any Gauss period β, $\beta \in K$, can be given. This follows from the fact that $\beta = \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p)$.

Proof (of Theorem 1). Clearly

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = -1 \equiv (p-1)a_0 \pmod{\pi^{2(p-1)+1}},$$

hence $a_0 \equiv \frac{-1}{p-1} \pmod{\pi^{2(p-1)+1}}$.

The congruence (ii) is proved as follows. By Lemma 1,

$$\tau(\chi^i) \equiv (p-1)a_i\pi^i \pmod{\pi^{2(p-1)+1}},$$
$$\tau(\chi^{p-1-i}) \equiv (p-1)a_{p-1-i}\pi^{p-1-i} \pmod{\pi^{2(p-1)+1}}.$$

Hence

$$\tau(\chi^i)\tau(\chi^{p-1-i}) = (-1)^i p \equiv (p-1)^2 a_i a_{p-1-i}(-p) \pmod{\pi^{2(p-1)+1}},$$

and we have (ii).

Now we prove (i). Since $\zeta_p^2 = \sigma_2(\zeta_p)$ we have

$$(1+p+p^2+a_1\pi+a_2\pi^2+\ldots+a_{p-2}\pi^{p-2})^2$$
$$\equiv 1+p+p^2+a_1 2^p\pi + a_2 2^{2p}\pi^2 + \ldots + a_{p-2}2^{p(p-2)}\pi^{p-2} \pmod{\pi^{2(p-1)+1}}.$$

Let us write the numbers a_i in the form

$$a_i = \frac{1}{i!} + x_i p \quad \text{for } i = 1, \ldots, (p-3)/2.$$

Squaring the left-hand side we get

$$(1+p+p^2)^2 + c_1\pi + c_2\pi^2 + \ldots + c_{p-2}\pi^{p-2},$$

where

$$c_1 = 2(1+p+p^2)(1+x_1p),$$
$$c_2 = 2(1+p+p^2)\left(\frac{1}{2!}+x_2p\right) + (1+x_1p)^2,$$

$$c_3 = 2(1+p+p^2)\left(\frac{1}{3!}+x_3p\right) + 2(1+x_1p)\left(\frac{1}{2!}+x_2p\right), \ \ldots$$

The coefficient of π^{p-1} (after squaring the left-hand side) is

$$\sum_{i=1}^{p-2} a_i a_{p-1-i} \equiv 1+2p \pmod{p^2},$$

which follows from the congruence (ii).

It is easy to see that it is sufficient to consider the coefficients of π^p, $\pi^{p+1}, \pi^{p+2}, \ldots$ modulo p.

The coefficient of π^p is

$$\sum_{i=2}^{p-2} a_i a_{p-i} \equiv \sum_{i=2}^{p-2} \frac{1}{i!}\cdot\frac{1}{(p-i)!} \equiv \frac{1}{p!}\sum_{i=2}^{p-2}\binom{p}{i} \equiv -\frac{1}{p}(2^p-2-2p) \pmod{p}.$$

Let d_{p+k} be the coefficient of π^{p+k} for $k>0$. Then

$$d_{p+k} \equiv \frac{-1}{p}\cdot\frac{1}{k!}\left(2^{p+k} - 2\sum_{i=0}^{k+1}\binom{p+k}{i}\right) \pmod{p}.$$

Since $\pi^{p-1} \equiv -p \pmod{\pi^{2(p-1)+1}}$, we have

$$\begin{aligned}
1+2p+3p^2 &+ c_1\pi + c_2\pi^2 + \ldots + c_{p-2}\pi^{p-2} \\
&\quad - p(1+2p-2(Q_2-1)\pi + d_{p+1}\pi^2 + \ldots + d_{p+p-3}\pi^{p-2}) \\
&\equiv 1+p+p^2+2^p(1+x_1p)\pi + 2^{2p}\left(\frac{1}{2!}+x_2p\right)\pi^2 \\
&\quad + \ldots + 2^{(p-2)p}\left(\frac{1}{(p-2)!}+x_{p-2}\right)\pi^{p-2} \pmod{\pi^{2(p-1)+1}}.
\end{aligned}$$

It follows that

$$\left(c_2 - pd_{p+1} - 2^{2p}\left(\frac{1}{2!}+x_2p\right)\right)\pi^2 + \left(c_3 - pd_{p+2} - 2^{3p}\left(\frac{1}{3!}+x_3p\right)\right)\pi^3 + \ldots \equiv 0 \pmod{\pi^{2(p-1)+1}}.$$

Hence the coefficients of $\pi^2, \pi^3, \ldots$ must be divisible by p. After reducing by p we get

$$\frac{c_2 - pd_{p+1} - 2^{2p}\left(\frac{1}{2!}+x_2p\right)}{p}\pi^2 + \frac{c_3 - pd_{p+2} - 2^{3p}\left(\frac{1}{3!}+x_3\right)}{p}\pi^3 + \ldots \equiv 0 \pmod{\pi^{p-1+1}},$$

hence

$$\frac{c_2 - pd_{p+1} - 2^{2p}\left(\frac{1}{2!}+x_2p\right)}{p} \equiv 0 \pmod{p},$$

$$\frac{c_3 - pd_{p+2} - 2^{3p}\left(\frac{1}{3!} + x_3 p\right)}{p} \equiv 0 \pmod{p},$$

etc.

Substituting for c_2 and reducing we have

$$\frac{2^2}{2!} \cdot \frac{1 - 2^{2(p-1)}}{p} + \frac{2}{2!} + 2x_1 + (2 - 2^2)x_2 - d_{p+1} \equiv 0 \pmod{p}.$$

Continuing, we find that $x_1, x_2, \ldots, x_{(p-3)/2}$ satisfy the system of linear equations modulo p with matrix

$$\begin{pmatrix} 1 & 1-2 & 0 & & \ldots & & 0 \\ \frac{1}{2!} & \frac{1}{1!} & 1-2^2 & 0 & 0 & \ldots & 0 \\ \frac{1}{3!} & \frac{1}{2!} & \frac{1}{1!} & 1-2^3 & 0 & \ldots & 0 \\ \vdots & & & & & & \\ \frac{1}{((p-3)/2)!} & \frac{1}{((p-5)/2)!} & \ldots & \frac{1}{3!} & \frac{1}{2!} & 1 & 1-2^{(p-3)/2} \end{pmatrix},$$

and right-hand side consisting of the numbers r_k satisfying

$$2r_k = d_{p+k} + \frac{1}{(k+1)!} 2^{k+1} \frac{2^{(k+1)(p-1)} - 1}{p} - \frac{2}{(k+1)!},$$

where

$$d_{p+k} \equiv \frac{-1}{p} \cdot \frac{1}{k!}\left(2^{p+k} - 2\sum_{i=0}^{k+1}\binom{p+k}{i}\right) \pmod{p}.$$

For $1 \le i$ the following congruence holds:

$$\binom{p+k}{i} \equiv \binom{k}{i}\left(1 + p\left(\frac{1}{k} + \frac{1}{k+1} + \ldots + \frac{1}{k-i+1}\right)\right) \pmod{p^2}.$$

From this we get

$$\begin{aligned}\sum_{i=0}^{k+1}\binom{p+k}{i} \equiv 2^k + \frac{1}{k+1} \\ &+ p\left(A_k + \binom{k}{k-1}(A_k - A_1) + \binom{k}{k-2}(A_k - A_2) + \ldots\right. \\ &\left. + \binom{k}{1}(A_k - A_{k-1})\right) \pmod{p^2}.\end{aligned}$$

After rearrangements we have

$$r_k \equiv \frac{1}{k!}\left(2^k A_k - \sum_{i=1}^{k}\binom{k}{i} A_i\right) \pmod{p}.$$

Put

$$x_i = \frac{x_1}{(i-1)!} - \frac{A_{i-1}}{(i-1)!} \qquad \text{for } i = 1, \ldots, (p-3)/2.$$

For each $n = 1, \ldots, (p-3)/2$ we obtain

$$\begin{aligned}
&\frac{1}{n!}x_1 + \frac{1}{(n-1)!}\left(\frac{x_1}{1!} - \frac{A_1}{1!}\right) + \frac{1}{(n-2)!}\left(\frac{x_1}{2!} - \frac{A_2}{2!}\right) \\
&\qquad + \ldots + \frac{1}{1!}\left(\frac{x_1}{(n-1)!} - \frac{A_{n-1}}{(n-1)!}\right) + (1-2^n)\left(\frac{x_1}{n!} - \frac{A_n}{n!}\right) \\
&= \frac{1}{n!}x_1\left(\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}\right) - \frac{2^n}{n!}x_1 - \frac{1}{n!}\sum_{i=1}^{n}\binom{n}{i}A_i + \frac{2^n}{n!}A_n \\
&= r_n.
\end{aligned}$$

Hence the numbers $x_1, x_2, \ldots, x_{(p-3)/2}$, where

$$x_i = \frac{x_1}{(i-1)!} - \frac{A_{i-1}}{(i-1)!} \qquad \text{for } i = 1, \ldots, (p-3)/2,$$

are the solution of the system of equations considered. It remains to determine x_1. Consider the coefficient a_2,

$$a_2 = \frac{1}{2!} + x_2 p = \frac{1}{2!} + p(x_1 - 1).$$

By Theorem 5 of [4],

$$\begin{aligned}
&\zeta_p + \zeta_p^{-1} \\
&\quad \equiv 2(1+p+p^2) + \left(\frac{2}{2!} - 2p\frac{p-1-p(p+1)B_{p-1}}{p}\right)\pi_1 + \ldots \pmod{\pi_1^{2m+1}},
\end{aligned}$$

where $m = (p-1)/2$ and $\pi_1 = \pi^2$. It follows that

$$2a_2 = 1 + 2p(x_1 - 1) \equiv 1 - 2p\frac{p-1-p(p+1)B_{p-1}}{p} \pmod{p^2},$$

hence

$$x_1 \equiv \frac{1 + p(p+1)B_{p-1}}{p} \equiv W_p \pmod{p}. \ \blacksquare$$

2. Applications. Define $N = (p-1) + i\frac{p-1}{l}$, $n = i\frac{p-1}{l} - 1$.

THEOREM 2. *For the number T_i the following congruences hold*:

(i) $$T_{l+i} \equiv \frac{N}{2n!}\left(-\frac{C_{N-1} - C_n}{p} + A_n C_n + \sum_{i=0}^{n-1}\binom{n}{i}\frac{C_i}{n-i} - \frac{E_{n+1}}{n+1}\right) \pmod{p},$$

(ii) $$T_i \equiv \frac{C_n}{2n!} - i\frac{p(p-1)}{2ln!}\left(\frac{E_{n+1}}{n+1} - W_pC_n - \sum_{i=0}^{n-1}\binom{n}{i}\frac{C_i}{n-i}\right) \pmod{p^2}$$

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

P r o o f. To determine T_{l+i} it is necessary to determine the sum

$$F_j(E^*) = \frac{1}{(p-1)!}\cdot\frac{E_{2j}}{(2j)!} + \frac{1}{(p+1)!}\cdot\frac{E_{2j-2}}{(2j-2)!} + \ldots + \frac{1}{(p+2j-1)!},$$

where $j = (n+1)/2$.

We have

$$\begin{aligned} pF_j(E^*) = {} & \frac{p}{(p-1)!}\cdot\frac{E_{2j}}{(2j)!} \\ & + \frac{1}{(p-1)!}\left(\frac{E_{2j-2}}{(p+1)(2j-2)!} + \frac{E_{2j-4}}{(p+1)(p+2)(p+3)(2j-4)!}\right. \\ & \left. + \ldots + \frac{1}{(p+1)(p+2)\ldots(p+2j-1)}\right) \pmod{p^2}. \end{aligned}$$

Expressing the product $(p+1)(p+2)\ldots(p+i)$ modulo p^2 we get

$$\begin{aligned} pF_j(E^*) = {} & \frac{p}{(p-1)!}\cdot\frac{E_{2j}}{(2j)!} \\ & + \frac{1}{(p-1)!}\left(\frac{E_{2j-2}}{(p+1)(2j-2)!} + \frac{E_{2j-4}}{3!(1+pA_3)(2j-4)!}\right. \\ & \left. + \ldots + \frac{1}{(2j-1)!(1+pA_{2j-1})}\right) \pmod{p^2}. \end{aligned}$$

From $1/(1+pk) \equiv 1 - pk \pmod{p^2}$ we get

$$\begin{aligned} pF_j(E^*) \equiv {} & \frac{p}{(p-1)!}\cdot\frac{E_{2j}}{(2j)!} \\ & + \frac{1}{(p-1)!(2j-1)!} \\ & \times\left(\binom{2j-1}{1}E_{2j-2} + \binom{2j-1}{3}E_{2j-4} + \ldots + 1\right) \\ & - \frac{p}{(p-1)!(2j-1)!}\left(\binom{2j-1}{1}E_{2j-2}A_1 + \binom{2j-1}{3}E_{2j-4}A_3\right. \\ & \left. + \ldots + A_{2j-1}\right) \pmod{p^2}. \end{aligned}$$

According to formula (51.1.2) of [1],

$$\sum_{k=1}^{n}(\pm 1)^k\frac{(-n)_k}{k!}E_k = \frac{1}{n+1}(-2)^{n+1}(2^{n+1}-1)B_{n+1},$$

we have

$$\binom{2j-1}{1}E_{2j-2}+\binom{2j-1}{3}E_{2j-4}+\ldots+1=\frac{1}{2j}2^{2j}(2^{2j}-1)B_{2j}=-C_{2j-1}.$$

Now summing up we get

$$\binom{2j-1}{1}E_{2j-2}A_1+\binom{2j-1}{3}E_{2j-4}A_3+\ldots+A_{2j-1}.$$

Since

$$\sum_{k=1}^{\infty}\frac{(\pm1)^k A_k}{k!}x^k=e^{\pm x}(C+\ln x-\mathrm{Ei}(\mp x)),$$

$$\sum_{k=1}^{\infty}\frac{(\pm1)^k}{kk!}x^k=-C-\ln x+\mathrm{Ei}(\pm x),$$

it follows that

$$\sum_{k=1}^{\infty}\frac{(-1)^k A_k}{k!}x^k=-e^{-x}\sum_{k=1}^{\infty}\frac{1}{kk!}x^k.$$

Moreover,

$$\frac{2}{e^x+e^{-x}}=1+\frac{E_2}{2!}x^2+\frac{E_4}{4!}x^4+\ldots,$$

hence the generating function for the sum we looked for is

$$\frac{2}{e^{2x}+1}\sum_{k=1}^{\infty}\frac{1}{kk!}x^k,\quad\text{where}\quad\frac{2}{e^x+1}=\sum_{k=0}^{\infty}\frac{C_k}{k!}\cdot\frac{x^k}{2^k}.$$

Hence

$$\sum_{k=0}^{\infty}\frac{C_k}{k!}x^k\sum_{k=1}^{\infty}\frac{1}{kk!}x^k,$$

and it follows that

$$\binom{2j-1}{1}E_{2j-2}A_1+\binom{2j-1}{3}E_{2j-4}A_3+\ldots+A_{2j-1}=\sum_{i=0}^{n-1}\binom{n}{i}\frac{C_i}{n-i},$$

where $n=2j-1$. Therefore

$$pF_j(E^*)\equiv\frac{-C_n}{n!(p-1)!}+\frac{p}{n!}\left(\sum_{i=0}^{n-1}\binom{n}{i}\frac{C_i}{n-i}-\frac{E_{n+1}}{n+1}\right)\pmod{p^2}.$$

Hence

$$\begin{aligned}pT_{l+i}=&-\frac{p}{\left(p-1+i\frac{p-1}{l}\right)!}2^{p-1+i(p-1)/l-1}(2^{p-1+i(p-1)/l}-1)B_{(p-1+i(p-1)/l)}\\&+\left(\frac{p-1}{2}+i\frac{p-1}{2l}\right)\left(\frac{-C_n}{n!(p-1)!}+\frac{p}{n!}\left(\sum_{i=0}^{n-1}\binom{n}{i}\frac{C_i}{n-i}-\frac{E_{n+1}}{n+1}\right)\right)\end{aligned}$$

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

Rearranging this congruence we get the congruence (i). The congruence (ii) is obtained using Theorem 1 by substituting $2+2p, 2a_2, 2a_4, \ldots$ for $A_0(m), A_1(m), \ldots$, in the formula for $G_j(E^*)$, $j = i(p-1)/(2l)$. ∎

Corollary 1. *Let p be a prime, $p \equiv 5 \pmod 8$. Let $T + U\sqrt{p} > 1$ be a fundamental unit and h be the class number. Then*:

$$\frac{1}{p}(2^{(p-9)/4}(C_{N-1} - 3C_n) \pm 2Uh)$$
$$\equiv 2^{(p-1)/4} B_{(p-1)/2}\left(-U^2h + \frac{2}{3}U^2 - \frac{Q_2}{2}\right) \pm h(h-1)U^3 \pmod p,$$

where the sign $\pm$ is chosen in such a way that the left-hand side is a p-integer, and $N = 3(p-1)/2$, $n = (p-1)/2 - 1$.

Proof. We get this congruence using Theorem 2, by substitution into the congruence for a quadratic field from [2] and by rearranging modulo p^2. Note that the sums $\sum_{i=0}^{n-1}\binom{n}{i}\frac{C_i}{n-i}$ and the numbers $E_{n+1}/(n+1)$, W_p cancel each other by these rearrangements. ∎

Remark. The congruence in Corollary 1 can be rewritten in the form

$$\frac{1}{p}\left(2^{(p-1)/4}\left(\frac{1}{3}B_{3(p-1)/2} - 3B_{(p-1)/2}\right) \pm 2Uh\right)$$
$$\equiv 2^{(p-1)/4} B_{(p-1)/2}\left(-U^2h + \frac{2}{3}U^2 + 2 - \frac{Q_2}{2}\right) \pm h(h-1)U^3 \pmod p.$$

Example. (i) If $p = 29$ then $h = 1$, $U = 1/2$, $C_{41} \equiv 82 \pmod{841}$, $C_{13} \equiv 662 \pmod{841}$, $Q_2 \equiv 2 \pmod{29}$.

(ii) If $p = 229$ then $h = 3$, $U = 1/2$, $C_{341} \equiv 32702 \pmod{52441}$, $C_{113} \equiv 27206 \pmod{52441}$, $Q_2 \equiv 68 \pmod{229}$.

References

[1] E. R. Hansen, *A Table of Series and Products*, Prentice-Hall, 1973.
[2] S. Jakubec, *Congruence of Ankeny–Artin–Chowla type modulo p^2 for cyclic fields of prime degree l*, Acta Arith. 74 (1996), 293–310.
[3] —, *The congruence for Gauss's period*, J. Number Theory 48 (1994), 36–45.
[4] —, *On Vandiver's conjecture*, Abh. Math. Sem. Univ. Hamburg 64 (1994), 105–124.

Matematický ústav SAV
Štefánikova 49
814 73 Bratislava, Slovakia
E-mail: jakubec@mau.savba.sk

Received on 14.11.1997 (3297)