ACTA ARITHMETICA
167.3 (2015)

Congruences of Ankeny–Artin–Chowla type and the p-adic class number formula revisited

by

František Marko (Hazleton, PA)

1. Introduction. A simple form of the celebrated Ankeny–Artin–Chowla congruence states the following. Let K be a real quadratic number field of prime discriminant $p \equiv 1 \pmod 4$, h be the class number of K, $\epsilon = (T + U\sqrt{p})/2 > 1$ be the fundamental unit of K, and $B_{(p-1)/2}$ be the $((p-1)/2)$th Bernoulli number. Denote $Q = U/T$. Then

$$Qh \equiv B_{(p-1)/2} \pmod p.$$

Jakubec and his collaborators generalized this result to congruences for cyclic totally real fields modulo p, p^2 and p^3 in [6–9, 12, 13, 16]. The method developed by Jakubec was purely elementary and algebraic; no analytic techniques were used. The purpose of this paper is to formulate these congruences in full generality and to prove them using the p-adic class number formula.

The p-adic class number formula states the following. Let K be a number field of degree n and discriminant $d(K)$, $h(K)$ be the class number of K, $R_p(K)$ be the p-adic regulator of K, χ_K be a character of K, and $L_p(s, \chi_K)$ be the corresponding p-adic L-function. Then

$$\frac{2^{n-1} h(K) R_p(K)}{\sqrt{d(K)}} = \prod_{\chi_K \neq 1} L_p(1, \chi_K).$$

As a consequence of our work, it turns out that the work of Jakubec et al. amounts to an elementary algebraic proof of the p-adic class number formula modulo p^3 and the method of Jakubec provides a framework for analogous proofs modulo higher powers of p.

To explain our main result, we need to introduce some notation and briefly outline the method of Jakubec. The reader is advised to consult

2010 *Mathematics Subject Classification*: Primary 11R29.
Key words and phrases: Bernoulli numbers, p-adic class number formula, Ankeny–Artin–Chowla congruences.

DOI: 10.4064/aa167-3-6

the references to fill in the missing details. Let p be an odd prime, $\zeta_p = \cos(2\pi/p) + i\sin(2\pi/p)$ be a primitive pth root of unity and $\eta = \zeta_p + \zeta_p^{-1}$, $L = \mathbb{Q}(\eta)$ be the maximal real subfield of $\mathbb{Q}(\zeta_p)$ of degree $m = (p-1)/2$ over $\mathbb{Q}$, and K be a cyclic subfield of $\mathbb{Q}(\zeta_p)$ of degree n over $\mathbb{Q}$. Write $k = (p-1)/n$ and denote by σ an automorphism that generates the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Denote by $\mathbb{Q}_p$ the p-adic completion of $\mathbb{Q}$, by K_p the p-adic completion of K, and by $\mathbb{Q}_p(\zeta_p)$ the p-adic completion of $\mathbb{Q}(\zeta_p)$.

Let π be the unique element of $\mathbb{Q}_p(\zeta_p)$ which satisfies $\pi^{p-1} = -p$ and $\zeta_p - 1 \equiv \pi \pmod{\pi^2}$, and let $\omega \in \mathbb{Q}_p$ be the $(p-1)$th root of unity given by $\sigma(\pi) = \omega\pi$. Then $\zeta_p = \sum_{i=0}^{p-2} a_i \pi^i$, where $a_i \in \mathbb{Q}_p$. Assign to η the polynomial

$$p_L(X) = \sum_{i=0}^{m-1} 2a_i X^{m-1-i}.$$

Fix a unit $\delta \in K$ of index f coprime to p and write $\delta = \sum_{i=0}^{n-1} x_i \beta_K^{\sigma^i}$, where $\beta_K = \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p)$ is the Gauss period of the field K. Assign to δ the polynomial

$$p_K(X) = \sum_{i=0}^{n-1} a_{ki}(x_0 + x_1\omega^{ki} + x_2\omega^{2ki} + \cdots + x_{n-1}\omega^{(n-1)ki})X^{n-1-i}.$$

The following statement is the main result of our paper.

THEOREM 1.1. *Let $p \equiv 1 \pmod 4$. Choose a unit δ in K of index f coprime to p and denote by S_r the sum of the rth powers of the roots of $p_K(X)$ and by T_r the sum of the $(rk/2)$th powers of the roots of $p_L(X)$. Then*

$$\frac{h(K)}{f}\prod_{r=1}^{n-1}\Big(\sum_{j=0}^{\infty}(-1)^j p^j \frac{S_{r+jn}}{r+jn}\Big) = \pm\prod_{r=1}^{n-1}\Big(\sum_{j=0}^{\infty}(-1)^j p^j \frac{T_{r+jn}}{r+jn}\Big) \tag{1}$$

$$= \pm\prod_{r=1}^{n-1}\Big(\sum_{s=0}^{\infty}\frac{r(r+n)\cdots(r+(s-1)n)}{s!n^s}C_{s,r}\Big), \tag{2}$$

where

$$C_{s,r} = -\sum_{l=0}^{s}(-1)^l\binom{s}{l}\frac{B_{rk+l(p-1)}}{rk+l(p-1)}(1-p^{rk+l(p-1)-1}) \equiv 0 \pmod{p^s},$$

$h(K)$ is the class number of the field K, and B_{2j} is the $(2j)$th Bernoulli number.

Next, we will explain the connection of this result to the work of Jakubec and describe the content of our paper. For a fixed positive integer t, the above result implies a congruence of Ankeny–Artin–Chowla type modulo p^t, analogous to congruences derived earlier by Jakubec et al.

Choose an integer a that is a primitive root modulo p^t such that the automorphism σ is given by $\sigma(\zeta_p) = \zeta_p^a$ and denote

$$g = a^{p^{t-1}}.$$

In [4], Jakubec introduced an element $\pi_{K,1} \in K$ such that $N_{K/\mathbb{Q}}(\pi_{K,1}) = (-1)^n p$ and $\sigma(\pi_{K,1}) \equiv g\pi_{K,1} \pmod{\pi_{K,1}^{n+1}}$ and determined the expansion of a Gauss period β_K modulo $\pi_{K,1}^{n+1}$. Later, in [5], he observed that for any fixed natural number t, it is possible to define $\pi_{K,t} \in K$ such that $N_{K/\mathbb{Q}}(\pi_{K,t}) = (-1)^n p$ and $\sigma(\pi_{K,t}) \equiv g\pi_{K,t} \pmod{\pi_{K,t}^{tn+1}}$. In Section 2, we will show that instead of various elements $\pi_{K,t}$ of K corresponding to different values t it is more natural to consider K embedded into its p-adic completion K_p, in which case all elements $\pi_{K,t}$ are restrictions of a single element $\pi_K \in K_p$ that satisfies $\pi_K^n = -p$. An explicit formula for π_K is also given.

In [6] and [8], the elements $\pi_{K,1}$ together with the existence of a certain morphism were used to derive congruences of Ankeny–Artin–Chowla type for cyclic totally real fields K modulo p. In [7], these congruences were extended modulo p^2 with the help of an obscure map Φ. The clarification of the role of Φ for congruences modulo p^2 was given in [12], modulo p^3 in [16], and the general case was settled in [17]. In [9], a connection of this approach with expansion of ζ_p modulo π^{2p-1} was revealed. Motivated by this, the expansion of ζ_p modulo π^{3p-2} was found in [10]. In our p-adic setting, this expansion of ζ_p is given as $\zeta_p = \sum_{i=0}^{p-2} a_i \pi^i$ for $a_i \in \mathbb{Q}_p$. Expansions of ζ_p modulo p^t can be derived explicitly by truncating the Dwork series $E_\pi(X) = \exp(\pi X - \pi X^p)$. In Section 3, we show how the expansion of ζ_p modulo p^t follows from the Gross–Koblitz formula and illustrate it explicitly modulo p^4.

In Section 4, we derive generalized Kummer congruences using p-adic interpolation, and in Section 5 we identify one side of the congruences of Ankeny–Artin–Chowla type derived by Jakubec as a product of the p-adic L-functions corresponding to nontrivial characters χ of the field K considered modulo appropriate powers of p. The other side of these congruences is identified in Section 6 with the p-adic regulator of K. This explains how the p-adic class number formula is related to the method of Jakubec.

Under some simplifying assumptions, the method of Jakubec provides a simple and purely elementary proof of (1). An elementary proof of (2) modulo p^2 was established in [9] and [12], and modulo p^3 in [16] and [13]. Undoubtedly, an analogous elementary proof of (2) exists modulo higher powers of p.

Finally, to illustrate the above results, an explicit formula for a quadratic field K and an explicit congruence modulo p^4 for a cubic field K are given in Section 8.

2. Elements π_K. In this section only, assume that K is an arbitrary subfield of $\mathbb{Q}(\zeta_p)$. Recall that $n = [K : \mathbb{Q}]$ and $kn = p-1$. The prime p is totally ramified in $\mathbb{Q}(\zeta_p)$ and factors as $p = \mathfrak{p}^{p-1}$, where $\mathfrak{p} = (1-\zeta_p)$. Thus p is totally ramified in K and $p = \mathfrak{p}_K^n$ for a unique divisor $\mathfrak{p}_K$ of K.

Recall the previous definition of g and denote $g_n = g^k$ so that $g_n^n \equiv 1 \pmod{p^t}$ for each n dividing $p-1$.

[4, Theorem] and [5, p. 106] show the existence of elements $\pi_{K,t} \in K$, unique modulo $\mathfrak{p}_K^{nt+1}$, satisfying

(i) $\mathrm{N}_{K/\mathbb{Q}}(\pi_{K,t}) = (-1)^n p$,
(ii) $\sigma(\pi_{K,t}) \equiv g_n \pi_{K,t} \pmod{\pi_{K,t}^{tn+1}}$, and
(iii) $\beta_K \equiv \sum_{i=0}^{n} \frac{k}{(ki)!} \pi_{K,t}^i \pmod{\pi_{K,t}^{n+1}}$.

[16, Lemma 1.1] asserts that additionally, if K_1 and K_2 are two subfields of $\mathbb{Q}(\zeta_p)$ of degrees n_1 and n_2 respectively such that $K_1 \subset K_2$ and $\pi_{K_1,t}$ and $\pi_{K_2,t}$ satisfy (i)–(iii), then

$$\pi_{K_1,t} \equiv \pi_{K_2,t}^{n_2/n_1} \pmod{\pi_{K_2,t}^{tn_2+1}}.$$

Observe that $\mathbb{Q}_p$ contains all roots of unity of order n because n divides $p-1$.

Lemma 2.1. *There is a unique element $\pi_K \in K_p$ satisfying $\pi_K^n = -p$ and $\beta_K \equiv \sum_{i=0}^{n-1} \frac{k}{(ki)!} \pi_K^i \pmod{p}$. Moreover, $N_{K_p/\mathbb{Q}_p}(\pi_K) = (-1)^n p$, $\sigma(\pi_K) = \omega^k \pi_K$ and $\pi_{K_1} = \pi_{K_2}^{n_2/n_1}$ for subfields $K_2 \subset K_1 \subset \mathbb{Q}(\zeta_p)$ of degrees n_2 and n_1, respectively.*

Proof. First we show the existence of a unique $\pi \in \mathbb{Q}_p(\zeta_p)$ that satisfies $\pi^{p-1} = -p$ and $\zeta_p - 1 \equiv \pi \pmod{\pi^2}$. By [1, p. 158], we have $\frac{p}{(1-\zeta_p)^{p-1}} \equiv -1 \pmod{\mathfrak{p}}$. Applying [18, Lemma 5.30] with $m = p-1$, $a = p$, $b = 1-\zeta_p$, $\eta = -1$ and $c = -p$ we obtain the existence of $\Pi \in \mathbb{Q}_p(\zeta_p)$ satisfying $\Pi^{p-1} = -p$. There are $p-1$ elements Π satisfying $\Pi^{p-1} = -p$; they differ by scalar factors that are $(p-1)$th roots of unity (belonging to $\mathbb{Q}_p$), and they are permuted by the automorphism σ. The element π is then uniquely determined by the requirements that $\pi^{p-1} = -p$ and $\zeta_p - 1 \equiv \pi \pmod{\pi^2}$.

Set $\pi_K = \pi^k$. Then π_K is a root of the polynomial $X^n + p$ that splits completely over $\mathbb{Q}_p(\pi_K)$ because $\mathbb{Q}_p$ contains all roots of unity of order n (since n divides $p-1$). Since $[\mathbb{Q}_p(\pi_K) : \mathbb{Q}_p] = n$, we obtain $K_p = \mathbb{Q}_p(\pi_K)$ and $\pi_K \in K_p$. Moreover, π_K generates the local ideal $\mathfrak{p}_{K_p}$ of K_p.

Define a character θ by $\theta(g) = \sigma(\pi)/\pi = \omega$, $\omega^{p-1} = 1$, and the corresponding Gauss sums by $\tau(\theta^i) = \sum_{j=0}^{p-2} \theta^i(j)\zeta_p^j$. Write $\zeta_p = \sum_{i=0}^{p-2} a_i\pi^i$ and compute the trace of the expression

$$\frac{1}{\pi^i}(\zeta_p - a_0 - a_1\pi - \cdots - a_{i-1}\pi^{i-1}) = a_i + a_{i+1}\pi + \cdots + a_{p-2}\pi^{p-2}.$$

Using $\mathrm{Tr}_{\mathbb{Q}_p(\zeta_p)/Q_p}(\pi^i) = 0$ for $i = 1, \ldots, p-2$ we find that $(p-1)a_i = \tau(\theta^{-i})/\pi^i$. Then [2, Theorem 11.2.10] (a p-adic version of Stickelberger's congruence) implies $\zeta_p \equiv \sum_{i=0}^{p-2} \frac{1}{i!}\pi^i \pmod p$. Finally, taking the trace of the last expression we conclude that $\beta_K \equiv \sum_{i=0}^{n-1} \frac{k}{(ki)!}\pi_K^i \pmod p$. The remaining assertions are immediate. ∎

The previous lemma shows that the main result of [4] is essentially a "disguised" Stickelberger's congruence. It also implies that $\mathrm{N}_{\mathbb{Q}(\zeta_p)/K}(\pi) = (-1)^{k+1}\pi^k$.

The connection between the elements $\pi_{K,t}$, [16, Lemma 1.1] and Lemma 2.1, which is the p-adic version of [16, Lemma 1.1], is explained in the next lemma.

The number $E = (\zeta_p - 1)^{p-1}/p$ is a unit of the field $\mathbb{Q}(\zeta_p)$ such that $E \equiv 1 \pmod{(\zeta_p - 1)}$ and $E^{p^i} \equiv 1 \pmod{p^i}$ for each natural number i.

LEMMA 2.2. *We have* $\pi_{K,t} = (-1)^{k+1} N_{\mathbb{Q}(\zeta_p)/K}((\zeta_p - 1)E^{p^{t-1}+\cdots+p+1})$ *and* $\lim_{t\to\infty} \pi_{K,t} = \pi_K$ *with respect to the p-adic metric.*

Proof. Using [11, Lemma 1] we verify that $\pi_t = (\zeta_p - 1)E^{p^{t-1}+\cdots+p+1}$ satisfies conditions (i)–(iii) for the field $\mathbb{Q}(\zeta_p)$ and $\pi_t^{p-1} \equiv -p \pmod{p^t}$. Moreover, the congruences $E^{p^i} \equiv 1 \pmod{p^i}$ imply that $\pi_{t_1} \equiv \pi_{t_2} \pmod{p^{t_1}}$ for $t_2 > t_1$, showing the existence of the p-adic limit $\lim_{t\to\infty} \pi_t = \Pi \in \mathbb{Q}_p(\zeta_p)$ for which $\Pi^{p-1} = -p$ and $\zeta_p \equiv 1 + \Pi \pmod{\Pi^2}$; this proves the claim in the case $K = \mathbb{Q}(\zeta_p)$. In the general case, $\pi_{K,t} = (-1)^{k+1}\mathrm{N}_{\mathbb{Q}(\zeta_p)/K}(\pi_t)$ and $\pi_{K,t} \equiv \pi_t^k \pmod{p^t}$ by [16, proof of Lemma 1.1]. This implies $\lim_{t\to\infty} \pi_{K,t} = \pi^k = \pi_K$. ∎

For this reason, it is more natural to work in the p-adic completions K_p rather than in K itself.

3. Expansions of ζ_p modulo powers of π. Define

$$W = \frac{(p-1)! + 1}{p}, \qquad A_j = \sum_{i=1}^{j} \frac{1}{i}, \qquad A_0 = 0,$$

$$H_j = \sum_{i=1}^{j} \frac{1}{i^2}, \qquad H_0 = 0, \qquad L_j = \sum_{i=1}^{j} \frac{1}{i^3}, \qquad L_0 = 0.$$

In the proof of Lemma 2.1, it was established that $\zeta_p \equiv \sum_{i=0}^{p-2} \frac{1}{i!}\pi^i \pmod{\pi^{p-1}}$. Papers [9] and [10] give explicit congruences for ζ_p modulo π^{2p-1} and π^{3p-2}, respectively.

Recall the definition of the Dwork series $E_\pi(X) = \exp(\pi X - \pi X^p)$. By [14, Theorem 14.3.2], we have $E_\pi(1) = \zeta_p$. To obtain a representation for ζ_p modulo a power of p, it is possible to appropriately truncate the above Dwork series. For example, according to [14, Lemma 14.2.2], to obtain a congruence modulo p^2 it suffices to truncate $E_\pi(X)$ modulo $X^{2(p+1)+1}$.

A more explicit approach is to use the representation

$$\zeta_p = \sum_{i=0}^{p-2} \left(\frac{1}{p-1} \frac{\tau(\theta^{-i})}{\pi^i} \right) \pi^i$$

derived earlier and the Gross–Koblitz formula. According to [2, (11.2.12)], this formula states that $\tau(\theta^{-i})/\pi^i = -\Gamma_p\left(\frac{i}{p-1}\right)$, where $\Gamma_p(x)$ is the p-adic Gamma function.

To explain this approach, we now derive an explicit congruence for ζ_p modulo p^4. For simplicity assume that $p \equiv 1 \pmod 4$. Then $L_{p-1} \equiv 0 \pmod p$ and also $H_{p-1} \equiv 0 \pmod p$. Furthermore, since

$$2A_{p-1} = \sum_{i=1}^{p-1} \left(\frac{1}{i} + \frac{1}{p-i} \right) = p \sum_{i=1}^{p-1} \frac{1}{i(p-i)} \equiv -pH_{p-1} \equiv 0 \pmod{p^2},$$

we also have $A_{p-1} \equiv 0 \pmod{p^2}$.

PROPOSITION 3.1. *Let $p \equiv 1 \pmod 4$ be a prime. Then*

$$\zeta_p \equiv \sum_{i=0}^{p-2} c_{p-1-i}\pi^i \pmod{p^4},$$

where

$$\begin{aligned} c_i = i!(-1)^i \Bigg(& 1 - ipW + p^2\left(-iW + \frac{i(i-1)}{2}W^2\right) \\ & + p^3\left(\frac{i(2i-1)}{2}W^2 - \frac{i(i-1)(i-2)}{6}W^3\right)\Bigg) \\ & \cdot \Bigg(1 + p\left(iA_{i-1} + \frac{(i-1)i}{2}A_{p-1}\right) \\ & + p^2\left(iA_{i-1} + i^2\left(\frac{A_{i-1}^2}{2} - \frac{H_{i-1}}{2}\right) - \frac{(i-1)i(2i-1)}{12}H_{p-1}\right) \\ & + p^3\left(iA_{i-1} + i^2\left(\frac{A_{i-1}^2}{2} - \frac{H_{i-1}}{2}\right) + i^3\left(\frac{A_{i-1}^3}{6} - \frac{A_{i-1}H_{i-1}}{2} + \frac{L_{i-1}}{3}\right)\right)\Bigg). \end{aligned}$$

Proof. It is enough to find certain values of p-adic Gamma functions modulo p^4. We have

$$\Gamma_p\Big(1-\frac{i}{p-1}\Big) \equiv \Gamma_p\Big(1+\frac{(p^4-1)i}{p-1}\Big) = \Gamma_p\big(1+i(1+p+p^2+p^3)\big) = -\prod_{\substack{j=1\\(p,j)=1}}^{i(1+p+p^2+p^3)} j \pmod{p^4}.$$

We write

$$\begin{aligned}\frac{1}{p-1}\prod_{d=1}^{i}(ip^3+ip^2+ip+d) &\equiv i!\Big(1+ipA_{i-1}+ip^2A_{i-1}+i^2p^2\big(\tfrac12A_{i-1}^2-\tfrac12H_{i-1}\big)+ip^3A_{i-1}\\ &\quad+i^2p^3\big(\tfrac12A_{i-1}^2-\tfrac12H_{i-1}\big)+i^3p^3\big(\tfrac16A_{i-1}^3-\tfrac12A_{i-1}H_{i-1}+\tfrac13L_{i-1}\big)\Big) \pmod{p^4}\end{aligned}$$

and

$$\begin{aligned}\prod_{d=1}^{p-1}(ap^3+bp^2+cp+d) &= (p-1)!\Big(1+cpA_{p-1}+bp^2A_{p-1}+c^2p^2\big(\tfrac12A_{p-1}^2-\tfrac12H_{p-1}\big)+ap^3A_{p-1}\\ &\quad+bcp^3\big(\tfrac12A_{p-1}^2-\tfrac12H_{p-1}\big)+c^3p^3\big(\tfrac16A_{p-1}^3-\tfrac12A_{p-1}H_{p-1}+\tfrac13L_{p-1}\big)\Big)\\ &\equiv(-1+pW)\big(1+cpA_{p-1}-c^2p^2\tfrac12H_{p-1}\big) \pmod{p^4}.\end{aligned}$$

Next,

$$\begin{aligned}\prod_{c=0}^{i-1}\prod_{d=1}^{p-1}(ip^3+ip^2+cp+d) &\equiv(-1+pW)^i\prod_{c=0}^{i-1}\big(1+cpA_{p-1}-c^2p^2\tfrac12H_{p-1}\big)\\ &\equiv(-1+pW)^i\Big(1+\frac{(i-1)i}{2}pA_{p-1}-\frac{(i-1)i(2i-1)}{6}p^2\tfrac12H_{p-1}\Big) \pmod{p^4}\end{aligned}$$

and

$$\begin{aligned}\prod_{c=0}^{p-1}\prod_{d=1}^{p-1}(ap^3+bp^2+cp+d) &\equiv(-1+pW)^p\prod_{c=0}^{p-1}\big(1+cpA_{p-1}-c^2p^2\tfrac12H_{p-1}\big)\\ &\equiv(-1+pW)^p \pmod{p^4}.\end{aligned}$$

Consequently,

$$\prod_{b=0}^{i-1}\prod_{c=0}^{p-1}\prod_{d=1}^{p-1}(ip^3+bp^2+cp+d) \equiv (-1+pW)^{ip} \pmod{p^4}$$

and

$$\prod_{a=0}^{i-1}\prod_{b=0}^{p-1}\prod_{c=0}^{p-1}\prod_{d=1}^{p-1}(ap^3+bp^2+cp+d)\equiv(-1+pW)^{ip^2}\pmod{p^4}.$$

Combining all together we get

$$\begin{aligned}&\Gamma_p\Big(1-\frac{i}{p-1}\Big)\\&\quad\equiv-(-1+pW)^{i(1+p+p^2)}i!\Big(1+\frac{(i-1)i}{2}pA_{p-1}-\frac{(i-1)i(2i-1)}{6}p^2\tfrac{1}{2}H_{p-1}\Big)\\&\qquad\cdot\Big(1+ipA_{i-1}+ip^2A_{i-1}+i^2p^2\big(\tfrac{1}{2}A_{i-1}^2-\tfrac{1}{2}H_{i-1}\big)+ip^3A_{i-1}\\&\qquad+i^2p^3\big(\tfrac{1}{2}A_{i-1}^2-\tfrac{1}{2}H_{i-1}\big)+i^3p^3\big(\tfrac{1}{6}A_{i-1}^3-\tfrac{1}{2}A_{i-1}H_{i-1}+\tfrac{1}{3}L_{i-1}\big)\Big)\pmod{p^4},\end{aligned}$$

and the statement follows. ∎

Using [14, Theorem 14.1.3], which implies $\Gamma_p\big(\frac{i}{p-1}\big)\Gamma_p\big(1-\frac{i}{p-1}\big)=(-1)^i$, we see immediately that the above proposition extends the expansions of ζ_p obtained in [9] and [10]. Hence the representation of ζ_p modulo p^t follows from the Gross–Koblitz formula.

4. Generalized Kummer congruences and p-adic L-functions. In this section we derive a formula relating values of p-adic L-functions at 1 to generalized Kummer congruences.

Proposition 4.1. *Let $\chi=\theta^{kj}$ be a nontrivial character corresponding to a field K (that is, $1\le j\le n-1$). Then*

$$L_p(1,\chi)=\sum_{s=0}^{\infty}(-1)^s\frac{j(j+n)\cdots(j+(s-1)n)}{s!n^s}C_s,$$

where

$$C_s=-\sum_{l=0}^{s}(-1)^{s-l}\binom{s}{l}\frac{B_{jk+l(p-1)}}{jk+l(p-1)}(1-p^{jk+l(p-1)-1})\equiv0\pmod{p^s}.$$

Proof. From the construction of the p-adic L-function (see [19, Theorem 5.11]) corresponding to χ we have

$$L_p(1-(ns+j)k,\chi)=-\frac{B_{(ns+j)k}}{(ns+j)k}(1-p^{(ns+j)k-1}).$$

The sequence of negative integers $\{-u_s=1-(ns+j)k=1-jk-(p-1)s\}_{s=0}^{\infty}$ is dense in the set $\mathbb{Z}_p$ of p-adic integers. Therefore $L_p(X,\chi)$ is the unique continuous function $f(X)$ on $\mathbb{Z}_p$ that satisfies

$$f(1-jk-(p-1)s)=-\frac{B_{jk+(p-1)s}}{jk+(p-1)s}(1-p^{jk+(p-1)s-1}).$$

Using p-adic interpolation as in [3, pp. 322 and 333], we obtain

$$f(X) = \sum_{s=0}^{\infty} K_s Q_s(X),$$

where

$$P_s(X) = (X-1+jk)(X-1+jk+(p-1))\cdots(X-1+jk+(s-1)(p-1)),$$

$$P_s(1-jk-s(p-1)) = (-1)^s s!(p-1)^s,$$

$$P'_{s+1}(1-jk-l(p-1)) = (-1)^l l!(s-l)!(p-1)^s,$$

$$Q_s(X) = \frac{P_s(X)}{P_s(1-jk-s(p-1))}$$

and

$$\begin{aligned} C_s &= \sum_{l=0}^{s} \frac{P_s(1-jk-s(p-1))}{P'_{s+1}(1-jk-l(p-1))} f(1-jk-l(p-1)) \\ &= -\sum_{l=0}^{s} \frac{(-1)^s s!(p-1)^s}{(-1)^l l!(s-l)!(p-1)^s} \frac{B_{jk+l(p-1)}}{jk+l(p-1)} (1-p^{jk+l(p-1)-1}) \\ &= -\sum_{l=0}^{s} (-1)^{s-l} \binom{s}{l} \frac{B_{jk+l(p-1)}}{jk+l(p-1)} (1-p^{jk+l(p-1)-1}). \end{aligned}$$

In particular,

$$Q_s(1) = \frac{(jk)(jk+kn)\cdots(jk+(s-1)kn)}{(-1)^s s!(kn)^s} = (-1)^s \frac{j(j+n)\cdots(j+(s-1)n)}{s!n^s}$$

and

$$L_p(1,\chi) = f(1) = \sum_{s=0}^{\infty} (-1)^s \frac{j(j+n)\cdots(j+(s-1)n)}{s!n^s} C_s.$$

The generalized Kummer congruence (see [3, Corollary 6 of Theorem 7])

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} \frac{B_{l+s(p-1)}}{l+s(p-1)} (1-p^{l-1+s(p-1)}) \equiv 0 \pmod{p^r}$$

which is valid for l not divisible by $p-1$ concludes the proof. ∎

5. p-adic logarithms. In [7], [9] and [13], explicit formulas for specific sums of roots of polynomials corresponding to expansions of ζ_p were obtained. We will show how these expressions correspond to p-adic logarithms of units.

Let $p(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_d$ be a polynomial of degree d that has roots $\lambda_1, \ldots, \lambda_d$. For each j, define $s_j = \lambda_1^j + \cdots + \lambda_d^j$ to be the sum of

the jth powers of the roots of $p(X)$. Recall that in the Introduction we have assigned to a unit $\delta \in K$ the polynomial $p_K(X)$ and have denoted by S_r the sum of the rth powers of the roots of $p_K(X)$.

LEMMA 5.1. *Let $\delta \in K$ be a unit such that $\delta = d_0 + d_1\pi_K + \cdots + d_{n-1}\pi_K^{n-1}$, where $d_i \in K_p$, and $p(X) = d_0X^{n-1} + d_1X^{n-2} + \cdots + d_{n-1}$ be the corresponding polynomial of degree $n-1$. Then*

$$S_r = \sum_{j=0}^{\infty}(-1)^j p^j \frac{s_{r+jn}}{r+jn} = \frac{1}{n\pi_K^r}\sum_{i=0}^{n-1}\omega^{-rki}\log(\delta^{\sigma^i})$$

for $r = 1, \ldots, n-1$.

Proof. For $i = 0, \ldots, n-1$ let $\lambda_{1,i}, \ldots, \lambda_{n-1,i}$ be the roots of

$$p_i(X) = d_0X^{n-1} + d_1\omega^{ki}X^{n-2} + \cdots + d_{n-1}\omega^{(n-1)ki}$$

and $s_{j,i}$ be the sum of the jth powers of these roots. Using Newton's formulas and induction we verify that $s_{r+jn,i} = s_{r+jn,0}\omega^{kri}$ for $i, r = 1, \ldots, n-1$ and each j. Lemma 2.1 implies $\delta^{\sigma^i} = d_0(1-\lambda_{1,i}\pi_K)\cdots(1-\lambda_{n-1,i}\pi_K)$. Then

$$\begin{aligned}\log_p(\delta^{\sigma^i}) &= \log_p(d_0) + \sum_{l=1}^{n-1}\sum_{j=1}^{\infty}\lambda_{l,i}^j\frac{\pi_K^j}{j} = \log_p(d_0) + \sum_{j=1}^{\infty}s_{j,i}\frac{\pi_K^j}{j}\\ &= \log_p(d_0) + \left(-p\frac{s_{n,0}}{n} + p^2\frac{s_{2n,0}}{2n} + \cdots + (-1)^j p^j\frac{s_{jn,0}}{jn} + \cdots\right)\\ &\quad + \sum_{l=1}^{n-1}\sum_{j=0}^{\infty}(-1)^j p^j\frac{s_{l+jn,0}}{l+jn}\omega^{lki}\pi_K^l.\end{aligned}$$

Since $\sum_{i=0}^{n-1}\omega^{ki} = 0$ and δ is a unit, we obtain

$$\begin{aligned}0 = \log_p(1) &= \sum_{i=0}^{n-1}\log_p(\delta^{\sigma^i})\\ &= n\log_p(d_0) + n\left(-p\frac{s_{n,0}}{n} + p^2\frac{s_{2n,0}}{2n} + \cdots + (-1)^j p^j\frac{s_{jn,0}}{jn} + \cdots\right).\end{aligned}$$

Therefore we can write simply

$$\log_p(\delta^{\sigma^i}) = \sum_{l=1}^{n-1}\sum_{j=0}^{\infty}(-1)^j p^j\frac{s_{l+jn,0}}{l+jn}\omega^{lki}\pi_K^l$$

and

$$\sum_{i=0}^{n-1}\omega^{-rki}\log_p(\delta^{\sigma^i}) = n\sum_{j=0}^{\infty}(-1)^j p^j\frac{s_{r+jn,0}}{r+jn}\pi_K^r. \quad \blacksquare$$

We will apply the previous lemma to the case when $K = L$ and $\delta = \zeta_p + \zeta_p^{-1}$. Since $\delta = \eta_2^{\sigma}$, where $\eta_2 = \zeta_p^{(p-1)/2} + \zeta_p^{(p+1)/2}$, we have

$$\sum_{i=0}^{m-1} \omega^{-2ri} \log_p(\delta^{\sigma^i}) = \sum_{i=0}^{m-1} \omega^{-2ri} \log_p(\eta_2^{\sigma^{i+1}}) = \frac{\omega^{2r}}{2} \sum_{i=1}^{p-1} \omega^{-2ri} \log_p(\eta_2^{\sigma^i})$$
$$= \frac{\chi(2)}{2} \sum_{j=1}^{p-1} \overline{\chi}(j) \log_p(\zeta_p^{-j/2} + \zeta_p^{j/2}),$$

where $\omega^{2ri} = \chi(2^i)$ for a nontrivial even character $\chi = \theta^{2r}$ belonging to L.

Rewrite the expression

$$\frac{\chi(2)}{2} \sum_{j=1}^{p-1} \overline{\chi}(j) \log_p(\zeta_p^{-j/2} + \zeta_p^{j/2})$$
$$= \frac{\chi(2)}{2} \sum_{j=1}^{p-1} \overline{\chi}(j) \big(\log_p(1 - \zeta_p^{2j}) - \log_p(1 - \zeta_p^j)\big)$$
$$= \frac{\chi(2)}{2}(\chi(2) - 1) \sum_{j=1}^{p-1} \overline{\chi}(j) \log_p(1 - \zeta_p^j) = \frac{\chi(4) - \chi(2)}{2} \frac{-p}{\tau(\chi)} L_p(1, \chi)$$

according to [19, Theorem 5.18].

Assume now that $\zeta_p = \sum_{i=0}^{p-2} a_i \pi^i$. Then $\zeta_p + \zeta_p^{-1} = \sum_{i=0}^{m-1} a_{2i} \pi_L^i$ and $p(X) = a_0 X^{m-1} + a_2 X^{m-2} + \cdots + a_{2m-2}$ is the polynomial corresponding to δ. According to Lemma 5.1 applied to L and δ, the corresponding S_r equals

$$\frac{1}{m\pi_L^r} \sum_{i=0}^{m-1} \omega^{-2ri} \log_p(\delta^{\sigma^i}) = \frac{\chi(4) - \chi(2)}{(p-1)\pi^{2r}} \frac{-p}{\tau(\chi)} L_p(1, \chi)$$
$$= \frac{\chi(4) - \chi(2)}{p-1} \frac{-\tau(\overline{\chi})}{\pi^{2r}} L_p(1, \theta^{2r}) = \frac{\theta^{2r}(4) - \theta^{2r}(2)}{p-1} \Gamma_p\left(\frac{2r}{p-1}\right) L_p(1, \theta^{2r})$$

by [19, Lemmas 4.7 and 4.8] and the Gross–Koblitz formula.

We have proved the following proposition.

PROPOSITION 5.1. *Let $\zeta_p = \sum_{i=0}^{p-2} a_i \pi^i$, let $\lambda_1, \ldots, \lambda_{m-1}$ be the roots of $p(X) = 2a_0 X^{m-1} + 2a_2 X^{m-2} + \cdots + 2a_{2m-2}$ and let $s_r = \lambda_1^r + \cdots + \lambda_{m-1}^r$. Then for $r = 1, \ldots, m-1$ we have*

$$\sum_{j=0}^{\infty} (-1)^j p^j \frac{s_{r+jm}}{r+jm} = \frac{\theta^{2r}(4) - \theta^{2r}(2)}{p-1} \Gamma_p\left(\frac{2r}{p-1}\right) L_p(1, \theta^{2r})$$
$$= (\theta^{2r}(2) - \theta^{2r}(4)) a_{2r} L_p(1, \theta^{2r}).$$

6. p-adic regulator. In Proposition 5.1 we have applied Lemma 5.1 to the field L and explained the appearance of p-adic L-functions in the context of Jakubec's work. We now apply Lemma 5.1 to the field K and a suitable unit ϵ to obtain a relationship to the p-adic regulator of K.

Assume as before that $\zeta_p = \sum_{i=0}^{p-2} a_i \pi^i$. Using the properties of the element π, we see that $\beta_K = k \sum_{i=0}^{n-1} a_{ki} \pi_K^i$.

PROPOSITION 6.1. *Let $\epsilon = \sum_{i=0}^{n-1} x_i \beta_K^{\sigma^i}$ be a unit in K of index f,*

$$p(X) = k \sum_{i=0}^{n-1} a_{ki}(x_0 + x_1\omega^{ki} + x_2\omega^{2ki} + \cdots + x_{n-1}\omega^{(n-1)ki}) X^{n-1-i},$$

$d(K)$ be the discriminant and $R_p(K)$ be the p-adic regulator of the field K. If n is odd, then

$$(-1)^{(n-1)/2} \prod_{r=1}^{n-1} \sum_{j=0}^{\infty} (-1)^j p^j \frac{s_{r+jn}}{r+jn} = \frac{f^{n-1}}{n^{n-2}} \frac{R_p(K)}{\sqrt{d(K)}}.$$

If n is even, then

$$(-1)^{n/2} \Gamma_p\left(\frac{1}{2}\right) \prod_{r=1}^{n-1} \sum_{j=0}^{\infty} (-1)^j p^j \frac{s_{r+jn}}{r+jn} = \frac{f^{n-1}}{n^{n-2}} \frac{R_p(K)}{\sqrt{d(K)}}.$$

Proof. Since

$$\epsilon = k \sum_{i=0}^{n-1} a_{ki}(x_0 + x_1\omega^{ki} + x_2\omega^{2ki} + \cdots + x_{n-1}\omega^{(n-1)ki}) \pi_K^i,$$

the polynomial $p(X)$ corresponds to ϵ. By Lemma 5.1,

$$\begin{aligned} \sum_{j=0}^{\infty} (-1)^j p^j \frac{s_{r+jn}}{r+jn} &= \frac{1}{n\pi_K^r} \sum_{i=0}^{n-1} \theta^{-rk}(g^i) \log_p(\epsilon^{\sigma^i}) \\ &= \frac{1}{n\pi_K^r} \sum_{\rho \in \mathrm{Gal}(K/\mathbb{Q})} \chi(\rho) \log_p(\epsilon^\rho) \end{aligned}$$

for $r = 1, \ldots, n-1$, where $\chi(\sigma^i) = \theta^{-rk}(g^i)$ is a nontrivial character corresponding to the field K.

Therefore

$$\prod_{r=1}^{n-1} \sum_{j=0}^{\infty} (-1)^j p^j \frac{s_{r+jn}}{r+jn} = \prod_{r=1}^{n-1} \frac{1}{n\pi_K^r} \sum_{\rho \in \mathrm{Gal}(K/\mathbb{Q})} \chi(\rho) \log_p(\epsilon^\rho).$$

If n is odd, then the last expression equals

$$\frac{1}{n^{n-1}(-p)^{(n-1)/2}} \prod_{\chi_K \neq 1} \sum_{\rho \in \mathrm{Gal}(K/\mathbb{Q})} \chi(\rho) \log_p(\epsilon^\rho) = (-1)^{(n-1)/2} \frac{f^{n-1}}{n^{n-2}} \frac{R_p(K)}{\sqrt{d(K)}}$$

by [19, Theorem 3.11, Lemma 5.26 and p. 74]. As usual, since $R_p(K)$ is determined only up to a sign, we can choose it suitably and obtain the desired equality.

If n is even, then

$$\prod_{r=1}^{n-1} \frac{1}{\pi_K^r} = \frac{1}{(-p)^{n/2-1}} \frac{1}{\pi^m} = \frac{1}{(-p)^{n/2-1}} \frac{-\Gamma_p(1/2)}{\sqrt{p}}$$

by the Gross–Koblitz formula and [2, Theorem 1.3.4] because $\tau(\theta^m) = \sqrt{p}$. The second statement follows. ∎

We remark that $\Gamma_p(1/2)$ is a fourth root of unity which is a primitive root in the case $p \equiv 1 \pmod 4$.

7. p-adic class number formula

PROPOSITION 7.1. *Let $p \equiv 1 \pmod 4$ and $p(X)$ be a polynomial corresponding to $N_{L/K}(\zeta_1 + \zeta_p^{-1})$ and s_r be the sum of the rth powers of its roots. Then*

$$\sum_{j=0}^{\infty} (-1)^j p^j \frac{s_{r+jn}}{r+jn} = (\theta^{kr}(4) - \theta^{kr}(2)) \frac{1}{2n} \Gamma_p\left(\frac{r}{n}\right) L_p(1, \theta^{kr}).$$

If n is odd, then

$$(-1)^{(n-1)/2} \prod_{r=1}^{n-1} \sum_{j=0}^{\infty} (-1)^j p^j \frac{s_{r+jn}}{r+jn} = \frac{1}{2^{n-1} n^{n-2}} \prod_{\chi_K \neq 1} L_p(1, \chi_K).$$

If n is even, then

$$(-1)^{n/2} \Gamma_p\left(\frac{1}{2}\right) \prod_{r=1}^{n-1} \sum_{j=0}^{\infty} (-1)^j p^j \frac{s_{r+jn}}{r+jn} = \frac{1}{2^{n-1} n^{n-2}} \prod_{\chi_K \neq 1} L_p(1, \chi_K).$$

Proof. If $\zeta_p = \sum_{i=0}^{p-2} a_i \pi^i$, then the polynomial $p_L(X) = 2a_0 X^{m-1} + 2a_2 X^{m-2} + \cdots + 2a_{2m-2}$ corresponds to $\zeta_p + \zeta_p^{-1}$. Denote the sum of the ith powers of its roots by $s_{L,i}$. Using Newton's formulas and Lemma 2.1 we verify that $s_r = (k/2) s_{L,kr/2}$ for each $r = 1, \ldots, n-1$. Therefore the first statement follows from Proposition 5.1.

According to [14, Theorem 14.1.3], the condition $p \equiv 1 \pmod 4$ implies that $\prod_{r=1}^{n-1} \Gamma_p(r/n)$ equals $(-1)^{(n-1)/2}$ if n is odd, and it equals $(-1)^{n/2-1} \Gamma_p(1/2)$ if n is even. Since $\prod_{\chi_K \neq 1} (\chi_K(4) - \chi_K(2)) = \prod_{r=1}^{n} (\omega^{2kr} - \omega^{kr}) = n$ and $1/\Gamma_p(1/2) = -\Gamma_p(1/2)$, the claims follow. ∎

7.1. Proof of Theorem 1.1. According to [15, Theorem 1], it is possible to choose a unit $\epsilon \in K$ of index f coprime to p. (If $n = l$ is an odd prime, then K has a Minkowski unit of index 1, that is, its conjugations generate

the group of units of the field K modulo ± 1.) Therefore the existence of a unit δ from the statement of Theorem 1.1 is guaranteed.

For equation (1) use Propositions 6.1 and 7.1, and the p-adic class number formula

$$\frac{2^{n-1}h(K)R_p(K)}{\sqrt{d(K)}} = \prod_{\chi_K \neq 1} L_p(1, \chi_K)$$

(see [19, Theorem 5.24]). Equation (2) follows from Proposition 4.1. ∎

7.2. Elementary proof of equation (1) of Theorem 1.1. We will give an elementary proof of (1) following an idea of Jakubec. For this part, for simplicity, we will also assume that every nontrivial nth power residue is congruent to a power of 2 modulo p. This guarantees that $\eta_K = \mathrm{N}_{L/K}(\zeta_p + \zeta_p^{-1})$ generates the group of cyclotomic units of K. In particular, if $g = 2$ is a primitive root modulo p, then by [19, Proposition 8.11], the unit

$$\eta_2 = \zeta_p^{-1/2}\frac{1-\zeta_p^2}{1-\zeta_p} = \zeta_p^{p-1/2}(1+\zeta_p) = \zeta_p^{(p-1)/2} + \zeta_p^{(p+1)/2}$$

generates the group $C(L)$ of cyclotomic units of L.

Proof of (1). The unit $\eta_K = \mathrm{N}_{L/K}(\zeta_1 + \zeta_p^{-1})$ generates the group of cyclotomic units of K and the group $\langle \eta_K^f \rangle$ generated by conjugations of η_K^f is contained in the group $\langle \delta \rangle$ generated by conjugation of δ. Moreover, the index e equals $[\langle \delta \rangle : \langle \epsilon \rangle] = f^{n-2}h(K)$ and if we write

$$\eta_K^f = \delta^{c_0}\sigma(\delta)^{c_1}\cdots\sigma^{n-2}(\delta)^{c_{n-2}},$$

then [15, Lemma 1] implies $e = \left|\prod_{i=1}^{n-1}\alpha_i\right|$, where

$$\alpha_i = c_0 + c_1\omega^{ki} + \cdots + c_{n-2}\omega^{(n-2)ki}.$$

For the polynomial $p(X)$ assigned to η_K^f, we compute the quantity

$$\prod_{r=1}^{n-1}\left(\sum_{j=0}^{\infty}(-1)^j p^j \frac{s_{r+jn}}{r+jn}\right).$$

On the one hand, it is equal to

$$f^{n-1}\prod_{r=1}^{n-1}\left(\sum_{j=0}^{\infty}(-1)^j p^j \frac{T_{r+jn}}{r+jn}\right).$$

On the other hand, since each s_i equals $\alpha_i S_i$, it also equals

$$\prod_{r=1}^{n-1}\alpha_r\left(\sum_{j=0}^{\infty}(-1)^j p^j \frac{S_{r+jn}}{r+jn}\right) = \pm e\prod_{r=1}^{n-1}\left(\sum_{j=0}^{\infty}(-1)^j p^j \frac{S_{r+jn}}{r+jn}\right). \blacksquare$$

If n is a prime, it is possible to remove the ambiguity of the sign in Theorem 1.1 (see e.g. [6]). Also, if n is a prime, then K contains a Minkowski unit δ (for which $f = 1$) and Theorem 1.1 is equivalent to the p-adic class number formula. The advantage of this refomulation is that it is possible to find its elementary and explicit form modulo powers of p, in particular [9] contains its explicit form modulo p^2 and [13] modulo p^3.

In [9], Jakubec formulated the basic idea of his elementary approach to Theorem 1.1 modulo p^2 with the help of some obscure map Φ. An explicit formula in the case modulo p^2 was subsequently obtained in [12]. Extension of this result to the case modulo p^3 was prepared by [16] and carried out in [13]. The reference to the map Φ was removed in the general case modulo p^t under some natural integrality conditions in [17].

8. Explicit formulas

8.1. Quadratic field

PROPOSITION 8.1. *Let $p \equiv 1 \pmod 4$, K be a quadratic field and $\epsilon = T + U\sqrt{p} > 1$ be its fundamental unit, and let $Q = U/T$. Then*

$$h(K)\sum_{j=0}^{\infty}\frac{Q^{2j+1}}{2j+1}p^j = \sum_{j=0}^{\infty}\frac{\binom{2j}{j}}{4^j}K_j,$$

where

$$K_j = \sum_{l=0}^{j}(-1)^l\binom{j}{l}\frac{B_{(j+2l)m}}{j+2l}(1-p^{(j+2l)m-1}) \equiv 0 \pmod{p^j}.$$

Proof. Following [7, p. 297], use Propositions 6.1 and 7.1, Theorem 1.1 and Proposition 4.1. ∎

If we consider the above proposition modulo p, we obtain the classical Ankeny–Artin–Chowla congruence (see the introduction above or [19, Theorem 5.37]). Explicit versions of the above congruence modulo p^2 was obtained in [12] and modulo p^3 in [13].

8.2. Cubic field. As an illustration, we give an explicit congruence for a cubic field K modulo p^4.

PROPOSITION 8.2. *Let $p \equiv 1 \pmod 4$, $n = 3$ and $\delta = \sum_{i=0}^{n-1} x_i\beta_K^{\sigma^i}$ be a unit of K of index f coprime to p. Set*

$$e_1 = \frac{x_0 + x_1\omega^{(p-1)/3} + x_2\omega^{2(p-1)/3}}{x_0 + x_1 + x_2}, \qquad e_2 = \frac{x_0 + x_1\omega^{2(p-1)/3} + x_2\omega^{(p-1)/3}}{x_0 + x_1 + x_2},$$

and denote by J a Jacobi sum $J(\theta^{-(p-1)/3}, \theta^{-(p-1)/3})$ corresponding to a

cubic character $\theta^{-(p-1)/3}$. *Then*

$$\begin{aligned}
&\frac{h(K)}{f}\\
&\cdot\big[e_1+p(Je_1^4+4e_1^2e_2+2J^{-1}e_2^2)+p^2(J^2e_1^7+7Je_1^5e_2^2+14e_1^3e_2^2+7J^{-1}e_1e_2^3)\\
&\qquad+p^3(J^4e_1^{11}+11J^3e_1^9e_2+44J^2e_1^7e_2^2+77Je_1^5e_2^3+55e_1^3e_2^4+11J^{-1}e_1e_2^5)\big]\\
&\cdot\big[Je_1^2+2e_2+p(J^2e_1^5+5Je_1^3e_2+5e_1e_2^2)\\
&\qquad+p^2(J^3e_1^8+8J^2e_1^6e_2+20Je_1^4e_2^2+16e_1^2e_2^3+2J^{-1}e_2^4)\\
&\qquad+p^3(J^4e_1^{11}+11J^3e_1^9e_2+44J^2e_1^7e_2^2+77Je_1^5e_2^3+55e_1^3e_2^4+11J^{-1}e_1e_2^5)\big]\\
&\equiv\pm\bigg[\frac{B_k}{k}+\frac{1}{3}m\bigg(\frac{B_k}{k}-\frac{B_{4k}}{4k}\bigg)+\frac{2}{9}m\bigg(\frac{B_k}{k}-2\frac{B_{4k}}{4k}+\frac{B_{7k}}{7k}\bigg)\\
&\qquad\qquad+\frac{14}{81}\bigg(\frac{sB_k}{k}-3\frac{B_{4k}}{4k}+3\frac{B_{7k}}{7k}-\frac{B_{10k}}{10k}\bigg)\bigg]\\
&\quad\cdot\bigg[\frac{B_{2k}}{2k}+\frac{2}{3}\bigg(\frac{B_{2k}}{2k}-\frac{B_{5k}}{5k}\bigg)+\frac{5}{9}\bigg(\frac{B_{2k}}{2k}-2\frac{B_{5k}}{5k}+\frac{B_{8k}}{8k}\bigg)\\
&\qquad\qquad+\frac{40}{81}\bigg(\frac{B_{2k}}{2k}-3\frac{B_{5k}}{5k}+3\frac{B_{8k}}{8k}-\frac{B_{11k}}{11k}\bigg)\bigg]\pmod{p^4}.
\end{aligned}$$

Proof. Using Theorem 1.1, we can compute S_i from the quadratic polynomial

$$X^2+\Gamma_p(1/3)e_1X+\Gamma_p(2/3)e_2=X^2+\gamma e_1X-e_2\gamma^{-1},$$

where $\gamma=\Gamma_p(1/3)$. Since $\gamma^3=J$, Newton's formulas imply

$$\begin{aligned}
-S_1\gamma^{-1}&=e_1,\\
S_2\gamma&=Je_1^2+2e_2,\\
S_4\gamma^{-1}&=Je_1^4+4e_1^2e_2+2J^{-1}e_2^2,\\
-S_5\gamma&=J^2e_1^5+5Je_1^3e_2+5e_1e_2^2,\\
-S_7\gamma^{-1}&=J^2e_1^7+7Je_1^5e_2^2+14e_1^3e_2^2+7J^{-1}e_1e_2^3,\\
S_8\gamma&=J^3e_1^8+8J^2e_1^6e_2+20Je_1^4e_2^2+16e_1^2e_2^3+2J^{-1}e_2^4,\\
S_{10}\gamma^{-1}&=J^3e_1^{10}+10J^2e_1^8e_2+35Je_1^6e_2^2+50e_1^4e_2^3+25J^{-1}e_1^2e_2^4+2J^{-2}e_2^5,\\
-S_{11}\gamma&=J^4e_1^{11}+11J^3e_1^9e_2+44J^2e_1^7e_2^2+77Je_1^5e_2^3+55e_1^3e_2^4+11J^{-1}e_1e_2^5,
\end{aligned}$$

and the claim follows. ∎

There are similar formulas modulo higher powers of p that relate $h(K)$, f, Bernoulli numbers, e_1, e_2 and the cubic Jacobi sum J. The cubic Jacobi sum is determined explicitly in [2, Section 3.1] as $J=(r_3+is_3\sqrt{3})/2$, where $4p=r_3^2+27s_3^2$ and $r_3\equiv 1 \pmod 3$. Additionally, $J^{-1}=(r_3-is_3\sqrt{2})/(2p)$.

8.3. Other fields. To obtain explicit congruences for fields K of higher degrees n, we need to understand the fundamental units of K. This is known only for special types of fields of degree higher than 3, say for quintic fields of Lehmer's type. Congruences modulo p^2 for these types of fields were investigated in [12]. As in the case of the cubic field K above, the explicit congruences involve coefficients

$$\frac{x_0 + x_1\omega^{ki} + x_2\omega^{2ki} + \cdots + x_{n-1}\omega^{(n-1)ki}}{x_0 + \cdots + x_{n-1}}$$

and Jacobi sums of order n.

References

[1] E. Artin and J. Tate, *Class Field Theory*, W. A. Benjamin, New York, 1967.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[3] J. Fresnel, *Nombres de Bernoulli et fonctions L p-adiques*, Ann. Inst. Fourier (Grenoble) 17 (1967), no. 2, 281–333.

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

[5] S. Jakubec, *On Vandiver's conjecture*, Abh. Math. Sem. Univ. Hamburg 64 (1994), 105–124.

[6] S. Jakubec, *Congruence of Ankeny–Artin–Chowla type for cyclic fields of prime degree l*, Math. Proc. Cambridge Philos. Soc. 119 (1996), 17–22.

[7] S. Jakubec, *Congruence of Ankeny–Artin–Chowla type modulo p^2 for cyclic fields of prime degree l*, Acta Arith. 74 (1996), 293–310.

[8] S. Jakubec, *Congruence of Ankeny–Artin–Chowla type for cyclic fields*, Math. Slovaca 48 (1998), 323–326.

[9] S. Jakubec, *Note on the congruence of Ankeny–Artin–Chowla type modulo p^2*, Acta Arith. 85 (1998), 377–388.

[10] S. Jakubec, *Connection between Fermat quotients and Euler numbers*, Math. Slovaca 58 (2008), 19–30.

[11] S. Jakubec, *A connection between sums of binomial coefficients and Gross–Koblitz formula*, Math. Slovaca 62 (2012), 13–16.

[12] S. Jakubec and M. Laššák, *Congruence of Ankeny–Artin–Chowla type modulo p^2*, Ann. Math. Sil. 12 (1998), 75–92.

[13] S. Jakubec and F. Marko, *Ankeny–Artin–Chowla congruences modulo p^3*, Math. Slovaca 63 (2013), 1183–1208.

[14] S. Lang, *Cyclotomic Fields I and II*, Grad. Texts in Math. 121, Springer, New York, 1990.

[15] F. Marko, *On the existence of p-units and Minkowski units in totally real cyclic fields*, Abh. Math. Sem. Univ. Hamburg 66 (1996), 89–111.

[16] F. Marko, *Towards Ankeny–Artin–Chowla congruence modulo p^3*, Ann. Math. Sil. 20 (2006), 31–55.

[17] F. Marko, *Decomposition of congruences involving a map Φ*, Math. Slovaca 60 (2010), 793–800.

[18] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer Monogr. Math., Springer, Berlin, 2004.

[19] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.

František Marko
Pennsylvania State University
76 University Drive
Hazleton, PA 18202, U.S.A.
E-mail: fxm13@psu.edu

Received on 20.4.2014
and in revised form on 6.8.2014 (7779)