On the p-Part of the Ideal Class Group of $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ and Vandiver's Conjecture

F. THAINE

Dedicated to Paulo Ribenboim

Introduction

Let $p \geq 5$ be a prime number, ζ_p a primitive pth root of unity, $\mathbb{Z}_p$ the ring of p-adic integers, $\omega\colon \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ the Teichmüller character defined by $\omega(k) \equiv k \bmod p$, and e_k $(0 \leq k \leq p-2)$ the idempotents $(1/(p-1))\sum_{\sigma\in\Delta}\omega^k(\sigma)\sigma^{-1} \in \mathbb{Z}_p[\Delta]$. Denote by A the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$. In this article we study the orders of the ω^r-components $e_r(A)$ of A, with r even and $2 \leq r \leq p-3$. These components can be identified with the ω^r-components of the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$.

As is known by Mazur–Wiles theorems (see e.g. Rubin's appendix to [4], or [9, pp. 146, 299]), the orders $|e_r(A)|$ are equal to the orders $|e_r(W)|$ of the ω^r-components of the p-Sylow subgroup W of the group of units of $\mathbb{Z}[\zeta_p]$ modulo the subgroup of circular units, for r even $(2 \leq r \leq p-3)$, and the $|e_r(A)|$ are equal to the p-parts of the generalized Bernoulli numbers $B_{1,\omega^{-r}} = (1/p)\sum_{j=1}^{p-1}\omega^{-r}(j)j$, for r odd $(3 \leq r \leq p-2)$. The main motivation for this work is the belief that there exist p-adic integers, that can be defined in a relatively simple way, whose p-parts correspond to the numbers $|e_r(A)|$ for r even, as do the p-parts of generalized Bernoulli numbers for r odd.

Let r even $(2 \leq r \leq p-3)$ be fixed, and let n be a positive integer. Call l_n the largest integer $\leq n$ such that the number $\beta = \prod_{k=1}^{p-1}(1-\zeta_p^k)^{k^{(p-1-r)p^{n-1}}}$ is a p^{l_n}th power in $\mathbb{Q}(\zeta_p)$. We devote this article to the search of formulas for p^{l_n} because, as is known, if n is large enough then we have $|e_r(A)| = |e_r(W)| = p^{l_n}$.

In the first section we show, by using the Tchebotarev density theorem, that the global problem of determining p^{l_n} can be reduced to a set of similar problems in the completions $\mathbb{Q}(\zeta_p)_Q$ of $\mathbb{Q}(\zeta_p)$ with respect to some convenient prime ideals Q. For $m \geq 1$, call $\mathcal{P}_m$ the set of all prime ideals Q of $\mathbb{Z}[\zeta_p]$ that are above rational primes $q \equiv 1 \bmod p^m$ such that $p^{(q-1)/p} \equiv \zeta_p \bmod Q$. We prove that, given $m \geq 1$ and $k \geq 1$, if for each prime ideal $Q \in \mathcal{P}_m$ there is $\gamma_Q \in \mathbb{Z}[\zeta_p]$ such that $\beta \equiv \gamma_Q^{p^k} \bmod Q$, then $\beta = \gamma^{p^k}$ for some $\gamma \in \mathbb{Z}[\zeta_p]$ (Corollary of Proposition 1 and Hensel's lemma).

Received June 14, 1994. Revision received January 24, 1995.
This work was supported in part by grants from NSERC and FCAR.
Michigan Math. J. 42 (1995).

We also show that, given a prime ideal $Q \neq (\zeta_p - 1)$ of $\mathbb{Z}[\zeta_p]$, the problem of finding the largest integer $l_Q \leq n$ such that $\beta \equiv \gamma_Q^{p^{l_Q}} \bmod Q$, for some $\gamma_Q \in \mathbb{Z}[\zeta_p]$, can be solved by using Kummer's complementary reciprocity laws stated in [3]. More precisely, we use an extension of Kummer's results, obtained in [7], to express p^{l_Q} in terms of Gaussian periods of $\mathbb{Q}(\zeta_q)$, where q is the rational prime below Q (we choose a primitive qth root ζ_q of unity for each prime q). As a particular (and main) case we have the following result: Let $\mathcal{P}$ be the set of all prime ideals Q of $\mathbb{Z}[\zeta_p]$ above rational primes $q \equiv 1 \bmod p^n$. For each $Q \in \mathcal{P}$ let $s = s_Q$ be a primitive root modulo q such that $s^{(q-1)/p} \equiv \zeta_p \bmod Q$, and define the index $i(Q)$ of β with respect to Q and s as the least nonnegative integer such that

$$\beta \equiv s^{i(Q)} \bmod Q.$$

Clearly p^{l_n} divides $i(Q)$ for all $Q \in \mathcal{P}$. For $0 \leq j \leq p^n - 1$ and $Q \in \mathcal{P}$, denote by $\eta_j = \eta_j(Q)$ the Gaussian periods $\sum_{i=0}^{(q-1)/p^n - 1} \zeta_q^{s^{j+ip^n}}$, and, for $0 \leq j \leq p^n - 1$ and $l \in \mathbb{Z}$, define $\eta_{j+lp^n} = \eta_j$. Then, for all $Q \in \mathcal{P}$,

$$i(Q) \equiv \sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l)\eta_k\eta_{k-l} \bmod p^n. \qquad (*)$$

(Proposition 2.)

The foregoing results allow us to give a preliminary criterion to determine p^{l_n}, as follows.

THEOREM 1. *For all $Q \in \mathcal{P}$, above the rational prime q, define p^{l_Q} as the largest power of p, less than or equal to p^n, that divides the number $i(Q)$, where $i(Q) \equiv \sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l)\eta_k\eta_{k-l} \bmod p^n$. Let $m \geq n$. Then $p^{l_n} \leq p^{l_Q}$ for all $Q \in \mathcal{P}$, and p^{l_n} is the smallest of all p^{l_Q} such that $Q \in \mathcal{P}_m$. If n is large enough, then $p^{l_n} = |e_r(A)| = |e_r(W)|$.*

In the second section we improve this criterion using certain characterizations of Gaussian periods and cyclotomic numbers obtained in [8]. To simplify matters (in the article we actually work with a situation a bit more general), suppose that Q is a prime ideal in $\mathcal{P}_{2n}$ above the rational prime q. Then the primitive root $s = s_Q$ modulo q can be chosen so that $s \equiv pt^{p^n} \bmod q$ for some $t \in \mathbb{Z}$. With that choice, which we assume from now on, the periods η_i can be defined by $\eta_i = \sum_{x \in S} \zeta_q^{xp^i}$ with $S = \{x^{p^n} : x \in (\mathbb{Z}/q\mathbb{Z})^\times\}$, and they satisfy $\eta_i^p \equiv \eta_{i+1} \bmod p$ for all $i \in \mathbb{Z}$. Also, the minimal polynomial of η_0 over $\mathbb{Q}$ is irreducible modulo p, and p is inert in $\mathbb{Q}(\eta_0)$.

Let $Q \in \mathcal{P}_{2n}$. For $i \in \mathbb{Z}$, denote by $\bar{\eta}_i$ the congruence class of the period $\eta_i = \eta_i(Q)$ (defined as before) modulo p^n. The elements $\bar{\eta}_i \in \mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p^n-1}]/p^n\mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p^n-1}]$ have the following properties:

(i) $\bar{\eta}_0, \bar{\eta}_1, \ldots, \bar{\eta}_{p^n-1}$ are pairwise noncongruent modulo p;
(ii) $\sum_{k=0}^{p^n-1} \bar{\eta}_k = -1$;
(iii) $\sum_{k=0}^{p^n-1} \bar{\eta}_k\bar{\eta}_{k+i} = \delta_{0,i}$ for all $i \in \mathbb{Z}$;
(iv) $\bar{\eta}_i^p \equiv \bar{\eta}_{i+1} \bmod p$ for all $i \in \mathbb{Z}$; and

(v) $\sum_{k=0}^{p^n-1} \bar{\eta}_k \bar{\eta}_{k+i} \bar{\eta}_{k+j} = \bar{c}_{i,j}$ for some elements $\bar{c}_{i,j} \in \mathbb{Z}/p^n\mathbb{Z}$, $0 \le i, j \le p^n-1$, where we use the following version of Kronecker's delta:

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i \equiv j \bmod p^n, \\ 0 & \text{if } i \not\equiv j \bmod p^n. \end{cases}$$

For $0 \le i, j \le p^n-1$, define the integers $a_{i,j}$ by

$$\eta_0 \eta_i = \sum_{j=0}^{p^n-1} a_{i,j} \eta_j,$$

and define $a_{i+kp^n, j+lp^n} = a_{i,j}$ for $0 \le i, j \le p^n-1$ and $k, l \in \mathbb{Z}$. We are interested in the integers $a_{i,j}$ because

$$i(Q) \equiv \sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l) a_{k,l} \bmod p^n \qquad (**)$$

(formula 15, which extends a formula of Kummer given in [3, p. 100]). Denote by $\bar{a}_{i,j}$ the congruence class of $a_{i,j}$ modulo p^n and call M the matrix $[\bar{a}_{i,j}]_{0 \le i,j \le p^n-1}$. The elements $\bar{a}_{i,j} \in \mathbb{Z}/p^n\mathbb{Z}$ have the following properties: For all $i, j, l \in \mathbb{Z}$,

(a) $\bar{a}_{i,j} = \bar{a}_{j,i}$,
(b) $\sum_{k=0}^{p^n-1} \bar{a}_{k,j} = -\delta_{0,j}$,
(c) $\bar{a}_{i,j} = \bar{a}_{-i,j-i}$,
(d) $\sum_{k=0}^{p^n-1} \bar{a}_{i,k} \bar{a}_{k-j,l-j} = \sum_{k=0}^{p^n-1} \bar{a}_{j,k} \bar{a}_{k-i,l-i}$,
(e) the polynomial $\det(xI-M)$ is irreducible modulo p, and
(f) the elements $\bar{a}_{i,j}$ are labeled in such a way that, if $\bar{\eta}_0$ is a root of $\det(xI-M)$ modulo p, then $\bar{\eta}_0^{1+p^i} \equiv \sum_{k=0}^{p^n-1} \bar{a}_{i,k} \bar{\eta}_0^{p^k} \bmod p$ for $0 \le i \le p^n-1$.

There is only one Galois ring extension of $\mathbb{Z}/p^n\mathbb{Z}$ of degree p^n, up to isomorphism (see [5, Chaps. XV & XVI]); we call this extension $\mathfrak{R}_n$. It is isomorphic, for example, to $\mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p^n-1}]/p^n\mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p^n-1}] \cong \mathbb{Z}[\eta_0]/p^n\mathbb{Z}[\eta_0]$, with $Q \in \mathcal{P}_{2n}$, above q, and $\eta_i = \eta_i(Q)$ as before. We have $\mathfrak{R}_1 = \mathbb{F}_{p^p}$, the field with p^p elements.

Each of the following definitions will allow us to divide our problem of finding a formula for p^{l_n} in two parts.

DEFINITION I. Let $\bar{\eta}_0, \bar{\eta}_1, \ldots, \bar{\eta}_{p^n-1} \in \mathfrak{R}_n$. We say that $(\bar{\eta}_0, \bar{\eta}_1, \ldots, \bar{\eta}_{p^n-1})$ corresponds to a prime ideal $Q \in \mathcal{P}_{2n}$ above the rational prime q if, for the periods $\eta_i = \eta_i(Q)$ (defined as before), the element $\bar{\eta}_i$ can be identified with the congruence class of η_i modulo p^n for $0 \le i \le p^n-1$.

DEFINITION II. For $0 \le i, j \le p^n-1$ let $\bar{a}_{i,j} \in \mathbb{Z}/p^n\mathbb{Z}$. We say that the matrix $[\bar{a}_{i,j}]_{0 \le i,j \le p^n-1}$ corresponds to a prime ideal $Q \in \mathcal{P}_{2n}$ above the rational prime q if, for the periods $\eta_i = \eta_i(Q)$ and the integers $a_{i,j}$ (defined as before), the element $\bar{a}_{i,j}$ is the congruence class of $a_{i,j}$ modulo p^n for $0 \le i, j \le p^n-1$.

Our task can be divided as follows.

PROBLEM 1. Find, between the vectors $(\bar{\eta}_0, \bar{\eta}_1, \ldots, \bar{\eta}_{p^n-1}) \in \mathfrak{R}_n$ satisfying conditions (i)-(v) or the $p^n \times p^n$ matrices $M = [\bar{a}_{i,j}]$ with entries in $\mathbb{Z}/p^n\mathbb{Z}$ satisfying conditions (a)-(f), the vectors or matrices that correspond to prime ideals $Q \in \mathcal{P}_{2n}$.

PROBLEM 2. Find all elements $\bar{\Theta} = (\bar{\eta}_0, \bar{\eta}_1, \ldots, \bar{\eta}_{p^n-1}) \in \mathfrak{R}_n$ satisfying conditions (i)-(v) and all matrices

$$M = [\bar{a}_{i,j}]_{0 \le i,j \le p^n-1}$$

with entries in $\mathbb{Z}/p^n\mathbb{Z}$ satisfying conditions (a)-(f). Then calculate the values $\sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l)\bar{\eta}_k\bar{\eta}_{k-l}$ and $\sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l)\bar{a}_{k,l}$ that, by formulas (*) and (**), would be congruent to $i(Q)$ modulo p^n if $\bar{\Theta}$ and M corresponded to the prime ideal $Q \in \mathcal{P}_{2n}$.

Problem 1 is a question about p^n that can be treated without reference to $\mathbb{Q}(\zeta_p)$. In fact, we reduce this problem to a question of whether or not we can lift elements $\bar{\eta}_i$ satisfying properties (i)-(v) to elements in an extension of $\mathbb{Q}$ satisfying some simple properties (Proposition 8); or to a question on integral solutions of a system of linear and quadratic equations (Propositions 9 and 9′). This allows us to write some improved versions of Theorem 1 (Theorems 2 and 3).

We were not able, as yet, to give a complete solution of Problem 1. On the other hand, we believe that in Section 3 we give a very satisfactory solution of Problem 2 for $n = 1$, the case that is relevant to the study of Vandiver's conjecture. In this (and last) section we consider the question of whether or not, for a given even integer r $(2 \le r \le p-3)$, the ω^r-component of A is trivial. Vandiver's conjecture is the statement that all such components are trivial. Our aim is to answer this question with a criterion similar to that of regularity of a prime stated by Kummer.

So we assume now that $n = 1$. Call $\mathbb{F} = \mathbb{F}_{p^p}$ the field with p^p elements. We have $\mathfrak{R}_1 = \mathbb{F}$. We show that the field $\mathbb{F}$ has a canonical (up to a cyclic permutation) normal basis over $\mathbb{F}_p$ that has, from our viewpoint, very convenient properties. In fact, let $\epsilon \in \mathbb{F}$ be a fixed root of the polynomial $x^p + x^{p-1} - 1$. Define $\epsilon_i = \epsilon^{p^i}$ for $0 \le i \le p-1$ and define $\epsilon_{i+jp} = \epsilon_i$ for $0 \le i \le p-1$ and $j \in \mathbb{Z}$. Then the set $\{\epsilon_0, \epsilon_1, \ldots, \epsilon_{p-1}\}$ is a normal basis of $\mathbb{F}/\mathbb{F}_p$ that satisfies

$$\sum_{k=0}^{p-1} \epsilon_k = -1 \quad \text{and} \quad \sum_{k=0}^{p-1} \epsilon_{k+i}\epsilon_{k+j} = \delta_{i,j} \quad \text{for all } i, j \in \mathbb{Z}$$

(Proposition 12).

Let Q be a prime ideal in $\mathcal{P}_2$ above the rational prime q; *let* $\eta_i = \eta_i(Q)$ be the Gaussian periods defined by $\eta_i = \sum_{x \in S} \zeta_q^{xp^i}$, where $S = \{x^p : x \in (\mathbb{Z}/q\mathbb{Z})^\times\}$. There is a natural way to identify $\mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p-1}]/p\mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p-1}]$ with $\mathbb{F}$ (see formula (21)). Let $\bar{\eta}_i$ be the residue class of η_i in $\mathbb{F}$. Then the $\bar{\eta}_i$ satisfy properties (i)-(v) (with $n = 1$). Write $\bar{\eta}_0 = \sum_{k=0}^{p-1} u_k\epsilon_k$ with $u_k = u_k(Q) \in \mathbb{F}_p$. This makes a vector $(u_0, u_1, \ldots, u_{p-1}) = (u_0(Q), u_1(Q), \ldots, u_{p-1}(Q)) \in (\mathbb{F}_p)^p$

correspond to $Q\in\mathcal{P}_2$ in a unique way, which allows us to give the following definition.

DEFINITION III. Let $u_0, u_1, \ldots, u_{p-1}\in\mathbb{F}_p$. We say that $(u_0, u_1, \ldots, u_{p-1})$ corresponds to a prime ideal $Q\in\mathcal{P}_2$ above the rational prime q if $\bar{\eta}_0=\sum_{k=0}^{p-1}u_k\epsilon_k$, where the periods $\eta_i=\eta_i(Q)$ and their classes $\bar{\eta}_i\in\mathbb{F}$ are defined as before. If $(u_0, u_1, \ldots, u_{p-1})$ corresponds to a prime ideal $Q\in\mathcal{P}_m$, we define $u_{i+jp}=u_i$ for $0\le i\le p-1$ and $j\in\mathbb{Z}$.

If $(u_0, u_1, \ldots, u_{p-1})\in(\mathbb{F}_p)^p$ corresponds to a prime ideal $Q\in\mathcal{P}_2$ above the rational prime q, and if $\eta_i=\eta_i(Q)$ and $a_{i,j}$ are defined as above, then $\sum_{k=0}^{p-1}u_k=1$, $\sum_{k=0}^{p-1}u_{k+i}u_{k+j}=\delta_{i,j}$ for all $i, j\in\mathbb{Z}$, and $\epsilon_j=\sum_{k=0}^{p-1}u_{j-k}\bar{\eta}_k$ for $0\le j\le p-1$ (formula (23)). Furthermore (by using the nice multiplication table of the ϵ_i given in formula (27)), we prove that

$$a_{k,l}\equiv-\sum_{i=0}^{p-1}u_iu_{i-k}u_{i-l}+\sum_{j=1}^{p-1}\frac{1}{j}\sum_{i=0}^{p-1}(u_iu_{i-k}u_{i+j-l}+u_iu_{i+j-k}u_{i-l}-u_iu_{i+j-k}u_{i+j-l})$$

mod p for $0\le k, l\le p-1$, and that

$$\sum_{l=0}^{p-1}la_{l,k}\equiv-\sum_{i=0}^{p-1}iu_iu_{i-k}+\delta_{0,k}\sum_{l=0}^{p-1}lu_l-1 \bmod p \quad \text{for } 0\le k\le p-1$$

(formulas (30) and (31)). From this and (**) we get

$$i(Q)\equiv-\sum_{l=1}^{p-1}\left(\sum_{i=1}^{p-1}iu_iu_{i-l}\right)l^{p-1-r} \bmod p \qquad (***)$$

(see Theorem 4).

The preceding formulas motivate the study of the numbers $\sum_{i=0}^{p-1}iu_iu_{i-k}$, $0\le k\le p-1$, where $(u_0, u_1, \ldots, u_{p-1})\in(\mathbb{F}_p)^p$ corresponds to some prime ideal $Q\in\mathcal{P}_2$. It turns out that these numbers have interesting properties, some of which are shown in Proposition 14.

Now let us reconsider Problem 2 (for the case $n=1$) in light of our new formulas. It is easy to see that we can recast the problem as follows: Find all vectors $(u_0, u_1, \ldots, u_{p-1})\in(\mathbb{F}_p)^p$ such that

$$\sum_{k=0}^{p-1}u_k=1 \quad\text{and}\quad \sum_{k=0}^{p-1}u_ku_{k+i}=\delta_{0,i}; \qquad (****)$$

then, for each of these vectors, calculate the value of the right-hand side of congruence (***).

Before considering the general situation, we want to show a particular set of solutions we found after R. Kučera's observation that $u_0\equiv 1 \bmod p$ and $u_i\equiv i \bmod p$ for $1\le i\le p-1$ is a solution of (****).

PROPOSITION 15. *Let k be an odd number, $1\le k\le(p-3)/2$, and let $c\in\mathbb{Z}$. Then the system of congruences $\sum_{k=0}^{p-1}d_k\equiv 1$ mod p and $\sum_{k=0}^{p-1}d_kd_{k+i}\equiv\delta_{0,i}$*

mod p, for $0 \le i \le p-1$, *admits the solution* $d_0 = 1$ *and* $d_i = (ci)^k$ *for* $1 \le i \le p-1$.

This proposition allows us to prove the following theorem, which yields a means of verifying if the component $e_r(A)$ of the p-part of the ideal class group of $\mathbb{Q}(\zeta_p)$ is trivial for even integers r such that $2 \le r \le (p-1)/2$.

THEOREM 5. *Let k be an odd number,* $1 \le k \le (p-3)/2$, *and let c be an integer not divisible by p. Suppose that the vector* $(u_0, u_1, \ldots, u_{p-1}) \in (\mathbb{F}_p)^p$ *(or a cyclic permutation of it) corresponds to a prime ideal* $Q \in \mathcal{P}_2$, *where* $u_0 \equiv 1$ *and* $u_i \equiv (ci)^k$ *mod p, for* $1 \le i \le p-1$. *Then the component* $e_{k+1}(A)$ *of the p-part of the ideal class group of* $\mathbb{Q}(\zeta_p)$ *is trivial.*

Let us now consider the general situation. Call $\mathcal{G}_1$ the set of all $p \times p$ circulatory orthogonal matrices of determinant 1 with entries in $\mathbb{F}_p$. Solving the system of equations (****) is equivalent to finding all matrices in $\mathcal{G}_1$. We prove that $M \in \mathcal{G}_1$ if and only if $M = B^t B^{-1}$ for some invertible circulatory matrix B (Proposition 16) by using the idea of Hilbert's Theorem 90. The remaining task is to calculate the value of the right-hand side of equality (***) for all vectors $(u_0, u_1, \ldots, u_{p-1}) \in (\mathbb{F}_p)^p$ satisfying (****). Our solution takes the form of an explicit reciprocity law (that must be regarded as a version of Kummer's complementary reciprocity laws stated in [3]); this solution is the main result of Section 3:

THEOREM 7. *Let*

$$B(X) = b_0 + b_1 X + \cdots + b_{p-1} X^{p-1} \in \mathbb{Z}[X]$$

such that $B(1) \not\equiv 0$ *mod p. Write* $B(X^{-1})/B(X) \equiv \sum_{i=0}^{p-1} u_i X^i$ *mod* $(p, X^p - 1)$ *with* $u_i \in \mathbb{Z}$ *(hence the vector* $(u_0, u_1, \ldots, u_{p-1})$ *modulo p belongs to* $\mathcal{G}_1$*). Suppose that* $(u_0, u_1, \ldots, u_{p-1})$ *modulo p corresponds to a prime ideal* $Q \in \mathcal{P}_2$. *Then* $i(Q) \equiv 0$ *mod p (i.e.,* $\prod_{k=1}^{p-1} (1-\zeta_p^k)^{k^{p-1-r}} \equiv \gamma^p$ *mod Q for some* $\gamma \in \mathbb{Q}(\zeta_p)$*) if and only if* $\prod_{k=1}^{p-1} B(\zeta_p^k)^{k^{r-1}} \equiv \alpha^p$ *mod p for some* $\alpha \in \mathbb{Q}(\zeta_p)$. *This happens if and only if* $\sum_{k=1}^{p-1} k^r \zeta_p^k B'(\zeta_p^k)/B(\zeta_p^k) \equiv 0$ *mod p.*

The congruences $\sum_{k=1}^{p-1} k^r \zeta_p^k B'(\zeta_p^k)/B(\zeta_p^k) \equiv 0 \bmod p$ in Theorem 7 can be transformed in congruences between integers. A particular case is shown in Theorem 6, where, for the solution $u_0 = 1$ and $u_i = (a+1)a^{p-1-i}$ for $1 \le i \le p-1$ with $a \in \mathbb{F}_p - \{0, 1\}$ of (****), we show that

$$i(Q) \equiv \frac{2}{1-a} \sum_{l=1}^{p-1} l^{p-1-r} a^l \bmod p$$

if $(u_0, u_1, \ldots, u_{p-1})$ (or a cyclic permutation of it) corresponds to a prime ideal Q.

I am grateful to Professor Hershy Kisilevsky for his valuable comments, and to Professor Radan Kučera for showing me his calculations on cyclotomic polynomials and circulatory orthogonal matrices over $\mathbb{Z}/p\mathbb{Z}$ together with a nontrivial general example of such matrices.

1. The Orders of the Even ω^r-Components of the p-Part of the Ideal Class Group of $\mathbb{Q}(\zeta_p)$ in Terms of Gaussian Periods

Let $p \geq 5$ be a prime number, ζ_p a primitive pth root of unity, Δ the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, E the group of units of $\mathbb{Z}[\zeta_p]$, C the subgroup of circular units, W the p-Sylow subgroup of E/C, and A the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$. Let $\mathbb{Z}_p$ denote the ring of p-adic integers, ω: $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ the Teichmüller character defined by $\omega(k) \equiv k \bmod p$, and e_k $(0 \leq k \leq p-2)$ the idempotents $(1/(p-1))\sum_{\sigma\in\Delta}\omega^k(\sigma)\sigma^{-1} \in \mathbb{Z}_p[\Delta]$. We denote by B_i the ith Bernoulli number defined by $t/(e^t-1) = \sum_{i=0}^{\infty}(B_i/i!)t^i$. For every prime number $q \neq p$, choose a primitive root of unity ζ_q.

Let r and n be fixed integers such that r is even $(2 \leq r \leq p-3)$ and $n \geq 1$. Define

$$\beta = \beta_{r,n} = \prod_{k=1}^{p-1}(1-\zeta_p^k)^{k^{(p-1-r)p^{n-1}}}.$$

Let $l = l_n$ be the greatest integer, less than or equal to n, such that $\beta = \gamma^{p^l}$ with $\gamma \in \mathbb{Q}(\zeta_p)$. Clearly, by Euler's theorem, $l_n = \min(n, l_{n+1})$.

It is known that for n large enough the equality $|e_r(A)| = |e_r(W)| = p^l$ holds (see e.g. Rubin's appendix [4, p. 404]). Our objective in this article is to find convenient formulas for p^l. In this section we express p^l in terms of certain Gaussian periods of degree p^n. Now, β is a p^kth power in $\mathbb{Q}(\zeta_p)$ if and only if it is a p^kth power in each completion $\mathbb{Q}(\zeta_p)_Q$, where Q is a prime ideal of $\mathbb{Z}[\zeta_p]$ (see [1, Thm. 1, Chap. 9]). Therefore we have that p^l is the smallest of all integers $p^{l(Q)}$ such that $\beta = \gamma_Q^{p^{l_Q}}$ with $\gamma_Q \in \mathbb{Q}(\zeta_p)_Q$ and $l_Q \leq n$ maximal. A corollary to the following result (which is similar to [6, Prop. 4], whose proof is based on ideas of L. Washington and on a theorem of R. Schoof) shows that we need not consider all prime ideals Q (see also Thm. 3.1 in Rubin's appendix to [4]).

PROPOSITION 1. *Let $m \geq k \geq 1$ be integers, $\alpha \in \mathbb{Z}[\zeta_p] \cap \mathbb{R}$ (fix an embedding of $\mathbb{Q}(\zeta_p)$ into $\mathbb{C}$), and $\mathcal{C}$ an ideal class of $\mathbb{Q}(\zeta_p)$. Let $\mathcal{P}(\mathcal{C}, p^m)$ be the set of all prime ideals $Q \in \mathcal{C}$ that are above rational primes q satisfying $q \equiv 1 \bmod p^m$ and $p^{(q-1)/p} \equiv \zeta_p \bmod Q$. Denote by $\mathcal{C}_0$ the class of principal ideals and by H the Hilbert class field of $\mathbb{Q}(\zeta_p)$. Let $\phi_{\mathcal{C}} \in \mathrm{Gal}(H/\mathbb{Q}(\zeta_p))$ be the automorphism corresponding to $\mathcal{C}$ under the Artin map.*

(i) *Suppose that for all (except possibly finitely many) prime ideals Q in $\mathcal{P}(\mathcal{C}, p^m)$, we have that $\alpha = \gamma_Q^{p^k}$ with γ_Q in the completion $\mathbb{Q}(\zeta_p)_Q$. Then $\alpha = \delta^{p^{k-1}}$ for some $\delta \in \mathbb{Z}[\zeta_p] \cap \mathbb{R}$.*

(ii) *Suppose that for all (except possibly finitely many) prime ideals Q in $\mathcal{P}(\mathcal{C}, p^m) \cup \mathcal{P}(\mathcal{C}_0, p^m)$, we have that $\alpha = \gamma_Q^{p^k}$ with γ_Q in the completion $\mathbb{Q}(\zeta_p)_Q$. Let δ be as in* (i). *Then $\mathbb{Q}(\zeta_p, \delta^{1/p}) \subseteq H^{\langle\phi_{\mathcal{C}}\rangle}(\zeta_{p^m})$, where $H^{\langle\phi_{\mathcal{C}}\rangle}$ is the fixed field of the subgroup of* $\mathrm{Gal}(H/\mathbb{Q}(\zeta_p))$ *generated by $\phi_{\mathcal{C}}$.*

Proof. Let ζ_{p^m} be a primitive p^mth root of unity, and set $\phi = \phi_{\mathcal{C}}$.

We affirm that $\mathcal{P}(\mathcal{C}, p^m)$ is an infinite set. In fact, we have

$$\mathbb{Q}(\zeta_p, p^{1/p}) \cap \mathbb{Q}(\zeta_{p^m}) = \mathbb{Q}(\zeta_p)$$

(as follows, for example, from Kummer's theory on abelian extensions of exponent p) and

$$\mathbb{Q}(\zeta_{p^m}, p^{1/p}) \cap H = \mathbb{Q}(\zeta_p)$$

(otherwise $\mathbb{Q}_p(\zeta_{p^m}, p^{1/p})/\mathbb{Q}_p(\zeta_{p^m})$ would be unramified and hence by e.g. [9, Lemma 14.4(a)] $\mathbb{Q}_p(\zeta_{p^m}, p^{1/p})/\mathbb{Q}_p$ would be abelian). Therefore we can extend ϕ to an automorphism ϕ' of $H(\zeta_{p^m}, p^{1/p})$ such that $\phi'(\zeta_{p^m}) = \zeta_{p^m}$ and $\phi'(p^{1/p}) = \zeta_p p^{1/p}$. By the Tchebotarev density theorem there exist infinitely many prime ideals P of $H(\zeta_{p^m}, p^{1/p})$, unramified over $\mathbb{Q}$, such that the Frobenius map F_P for $H(\zeta_{p^m}, p^{1/p})/\mathbb{Q}(\zeta_{p^m})$ is ϕ' and such that the prime P' of $\mathbb{Q}(\zeta_{p^m})$ below P is of absolute degree 1. For each such P, the restriction $F_P|_H = \phi$ is the Frobenius map for $Q = P \cap \mathbb{Z}[\zeta_p]$, and so $Q \in \mathcal{C}$. Since P' is of absolute degree 1 and unramified over $\mathbb{Q}$, the rational prime q below Q is congruent to 1 modulo p^m. Finally, since the restriction $F_P|_{\mathbb{Q}(\zeta_p, p^{1/p})}$ is the corresponding Frobenius map for Q (i.e. $\zeta_p p^{1/p} \equiv (p^{1/p})^q \bmod Q\mathcal{O}_{\mathbb{Q}(\zeta_p, p^{1/p})}$), we have $p^{(q-1)/p} \equiv \zeta_p \bmod Q$. So $Q \in \mathcal{P}(\mathcal{C}, p^m)$. Therefore $\mathcal{P}(\mathcal{C}, p^m)$ contains infinitely many prime ideals Q below prime ideals P satisfying our conditions.

Let $\gamma = \alpha^{1/p^k}$ be the real p^kth root of α, and let L be the Galois closure of $\mathbb{Q}(\zeta_p, \gamma)$ over $\mathbb{Q}(\zeta_p)$. Then $L = \mathbb{Q}(\zeta_{p^e}, \gamma)$ for some e, $1 \le e \le k$. We will prove later that if the conditions in (i) are satisfied then $L \subseteq H(\zeta_{p^m}, p^{1/p})$. We assume this claim for the moment to see how it implies (i) and (ii). If the conditions in (i) are satisfied, we have that $L/\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_p, \gamma)/\mathbb{Q}(\zeta_p)$ are abelian extensions. Therefore $L = \mathbb{Q}(\zeta_p, \gamma)$. If we set $\delta = \gamma^p$ then the above equality implies that $\delta \in \mathbb{Z}[\zeta_p]$. (One way to prove this is as follows: Let a be the smallest positive integer such that $\gamma^{p^a} \in \mathbb{Q}(\zeta_p)$. If the affirmation is false then $a \ge 2$. Call $\nu = \gamma^{p^{a-2}}$. We have $\nu^p \notin \mathbb{Q}(\zeta_p)$, $\nu^{p^2} \in \mathbb{Q}(\zeta_p)$, and $\mathbb{Q}(\zeta_p, \nu) \subseteq \mathbb{Q}(\zeta_p, \gamma)$. So $\mathbb{Q}(\zeta_p, \nu)/\mathbb{Q}(\zeta_p)$ is abelian and $\zeta_{p^2} \in \mathbb{Q}(\zeta_p, \nu)$. Therefore

$$[\mathbb{Q}(\zeta_{p^2}, \nu) : \mathbb{Q}(\zeta_{p^2})] = p \quad \text{and} \quad \nu^p \in \mathbb{Q}(\zeta_{p^2}).$$

But then $\nu^{p^2} \in (\mathbb{Q}(\zeta_{p^2})^\times)^p \cap \mathbb{Q}(\zeta_p)^\times \cap \mathbb{R} = (\mathbb{Q}(\zeta_p)^\times \cap \mathbb{R})^p$, a contradiction. See Rubin's appendix to [4], step III of the proof of Thm. 3.1.) We have $\alpha = \delta^{p^{k-1}}$. On the other hand, for ϕ' as at the beginning of this proof, we have $\phi'(\gamma) = \gamma$. In fact, let $Q \in \mathcal{P}(\mathcal{C}, p^n)$, below the prime ideal P of $H(\zeta_{p^m}, p^{1/p})$ and above the rational prime q, be relatively prime with α, such that P is unramified over $\mathbb{Q}$ and the Frobenius map F_P for $H(\zeta_{p^m}, p^{1/p})/\mathbb{Q}(\zeta_{p^m})$ is ϕ' and such that $\alpha = \gamma_Q^{p^k}$ with $\gamma_Q \in \mathbb{Q}(\zeta_p)_Q$. Then, for some integer j, $\zeta_p^j \gamma = \phi'(\gamma) \equiv \gamma^q = \delta^{(q-1)/p}\gamma \bmod Q\mathcal{O}_L$. So $\zeta_p^j \equiv \delta^{(q-1)/p} \equiv \gamma_Q^{q-1} \equiv 1 \bmod Q$. Therefore $\zeta_p^j = 1$ and $\phi'(\gamma) = \gamma$. This shows that if the conditions in (i) are satisfied then $\alpha = \delta^{p^{k-1}}$ with $\delta \in \mathbb{Z}[\zeta_p] \cap \mathbb{R}$ and $\mathbb{Q}(\zeta_p, \delta^{1/p}) \subseteq H(\zeta_{p^m}, p^{1/p})^{\langle \phi' \rangle}$. If also the conditions in (ii) are satisfied, then

$$\mathbb{Q}(\zeta_p, \delta^{1/p}) \subseteq H(\zeta_{p^m}, p^{1/p})^{\langle \phi' \rangle} \cap H(\zeta_{p^m}) = H^{\langle \phi \rangle}(\zeta_{p^m}).$$

Suppose that the conditions in (i) are satisfied. In order to prove that $L \subseteq H(\zeta_{p^m}, p^{1/p})$, observe first that every $Q \in \mathcal{P}(\mathcal{C}, p^m)$, not dividing α and not belonging to the finite set of exceptions, splits completely in $\mathbb{Q}(\zeta_p, \gamma)$ and hence in L (because $X^{p^k}-\alpha \equiv X^{p^k}-\gamma_Q^{p^k} \bmod Q$ splits completely in $(\mathbb{Z}[\zeta_p]/Q)[X]$).

Let $M = LH(\zeta_{p^m}, p^{1/p})$. Since $\mathbb{Q}(\zeta_{p^m}) \cap \mathbb{Q}(\zeta_p, p^{1/p}) = \mathbb{Q}(\zeta_{p^m}, p^{1/p}) \cap H = \mathbb{Q}(\zeta_p)$, we can extend ϕ to an automorphism $\tilde{\phi}$ of M such that $\tilde{\phi}(\zeta_{p^m}) = \zeta_{p^m}$ and $\tilde{\phi}(p^{1/p}) = \zeta_p p^{1/p}$. Let $G = \mathrm{Gal}(M/H(\zeta_{p^m}, p^{1/p}))$ and let $f \in \tilde{\phi}G$. By the Tchebotarev density theorem there exist infinitely many prime ideals P of M, unramified over $\mathbb{Q}$, such that the prime P' of $\mathbb{Q}(\zeta_{p^m})$ below P is of absolute degree 1, and such that the Frobenius map F_P for $M/\mathbb{Q}(\zeta_{p^m})$ is f.

For P as above, the restriction $F_P|_H = f|_H = \phi$ is the Frobenius map for $Q = P \cap \mathbb{Z}[\zeta_p]$ with respect to $H/\mathbb{Q}(\zeta_p)$, so $Q \in \mathcal{C}$. Since P' is of absolute degree 1 and unramified over $\mathbb{Q}$, the rational prime q below Q is congruent to 1 modulo p^m. Since $f(p^{1/p}) = \zeta_p p^{1/p}$ we have, as before, that $p^{(q-1)/p} \equiv \zeta_p \bmod Q$. So $Q = P \cap \mathbb{Z}[\zeta_{p^m}] \in \mathcal{P}(\mathcal{C}, p^m)$ and we can choose P so as to avoid the finitely many exceptions and such that Q does not divide α. But then Q splits completely in L as we already showed. Therefore $f|_L = F_P|_L = \mathrm{id}$. That is, $f \in \mathrm{Gal}(M/L)$. This proves that $\tilde{\phi}G \subseteq \mathrm{Gal}(M/L)$. So $G \subseteq \mathrm{Gal}(M/L)$, which implies that $L \subseteq H(\zeta_{p^m}, p^{1/p})$ as desired. □

COROLLARY. *Let $m \geq 1$ and $1 \leq k \leq n$. If—for all (except possibly finitely many) prime ideals Q of $\mathbb{Q}(\zeta_p)$ that are above rational primes q such that $q \equiv 1 \bmod p^m$ and $p^{(q-1)/p} \equiv \zeta_p \bmod Q$—we have $\beta = \gamma_Q^{p^k}$ with $\gamma_Q \in \mathbb{Q}(\zeta_p)_Q$, then $\beta = \gamma^{p^k}$ for some $\gamma \in \mathbb{Q}(\zeta_p)$.*

Proof. Clearly we can assume that $m \geq k$. Let $\alpha \in \mathbb{Z}[\zeta_p] \cap \mathbb{R}$ be such that $\alpha = \beta\rho^{p^n}$ for some $\rho \in \mathbb{Q}(\zeta_p)$ (it follows from the definition of β that such an element α exists). Then the conditions on β in the corollary are also satisfied by α. By part (i) of the theorem we have that $\alpha = \delta^{p^{k-1}}$ for some $\delta \in \mathbb{Z}[\zeta_p] \cap \mathbb{R}$. By part (ii) and Galois theory, $\delta^{1/p} \in \mathbb{Q}(\zeta_{p^m})$. This implies that $\gamma_0 = \delta^{1/p} \in \mathbb{Q}(\zeta_p)$ (see Rubin's appendix to [4], step III of the proof of Thm. 3.1). Therefore $\beta = \alpha\rho^{-p^n} = \gamma_0^{p^k}\rho^{-p^n} = \gamma^{p^k}$ for some $\gamma \in \mathbb{Q}(\zeta_p)$. □

We return to our calculation of the numbers $p^l = p^{l_n}$. If $Q = (\zeta_p - 1)$ then, for n large enough, β is a p^kth power in $\mathbb{Q}(\zeta_p)_Q$ if and only if $L_p(1, \omega^r) \equiv 0 \bmod p^k$, where $L_p(s, \omega^r)$ is the p-adic L-function (see [9, Chap. 8]). We recall that $L_p(1, \omega^r) \equiv -B_{rp^{n-1}}/rp^{n-1} \bmod p^n$. Therefore, for n large enough, p^l divides $B_{rp^{n-1}}/rp^{n-1}$.

Let $Q \neq (\zeta_p - 1)$ be a prime ideal of $\mathbb{Z}[\zeta_p]$, q the rational prime below Q, f the inertia degree of Q/q, and F the field $\mathbb{Z}[\zeta_p]/Q$. Assume that $p^n \mid q^f - 1$. By Hensel's lemma, β is a p^kth power in $\mathbb{Q}(\zeta_p)_Q$ if and only if β is a p^kth power in F. We have $|F^\times| = q^f - 1$. Let $s = s_Q$ be a generator of $F^\times$ such that $s^{(q^f-1)/p} \equiv \zeta_p \bmod Q$. Define the index $i(Q) = i_r(Q)$ of β with respect to Q and s as the least nonnegative integer such that

$$\beta \equiv s^{i(Q)} \bmod Q. \tag{1}$$

Clearly p^l divides $i(Q)$. For $i \not\equiv 0 \bmod q^f-1$, define $\Phi(i)$ as the least positive integer such that $1-s^i = s^{\Phi(i)}$ in F. Denote by T the trace from F to $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ and by $G(X)$ the polynomial $\sum_{k=0}^{q^f-2} X^k \zeta_q^{T(s^k)}$ (note that $G(\zeta_p)$ is a Gauss sum, so $G(\zeta_p)\overline{G(\zeta_p)} = q^f$). It follows immediately from [7, formula (1)] that

$$\zeta_p G'(\zeta_p)/G(\zeta_p) \equiv -\sum_{k=1}^{q^f-2} k\zeta_q^{T(s^k)} + \sum_{k=1}^{(q^f-1)/p-1} \Phi(kp) + \sum_{k=1}^{p-1} \Phi\left(-k\frac{q^f-1}{p}\right)\zeta_p^k \tag{2}$$

mod p^n. On the other hand, it is clear that

$$i(Q) \equiv \sum_{k=1}^{p-1} \omega^{-r}(k)\Phi\left(k\frac{q^f-1}{p}\right) \bmod p^n \tag{3}$$

(see [7, proof of Thm. 1]).

Define the function $\tau\colon \mathbb{Z}_p[\zeta_q, \zeta_p] \to \mathbb{Z}_p[\zeta_q]$ by

$$\tau\left(\sum_{i=1}^{p-1} \alpha_i \zeta_p^i\right) = \sum_{i=1}^{p-1} \alpha_i \omega^{-r}(i),$$

where $\alpha_i \in \mathbb{Z}_p[\zeta_q]$. It can be easily proved that

$$\tau(\gamma(\zeta_p)) = \left(\sum_{i=1}^{p-1} \omega^r(i)\zeta_p^i\right)^{-1} \sum_{j=1}^{p-1} \omega^r(j)\gamma(\zeta_p^j) \tag{4}$$

for all $\gamma(X) \in \mathbb{Z}_p[\zeta_q][X]$.

From (2), (3), and (4) we obtain

$$i(Q) \equiv \tau(\zeta_p G'(\zeta_p)/G(\zeta_p)) = \left(\sum_{i=1}^{p-1} \omega^r(i)\zeta_p^i\right)^{-1} \sum_{j=1}^{p-1} \omega^r(j)\zeta_p^j G'(\zeta_p^j)/G(\zeta_p^j) \tag{5}$$

mod p^n (see also [7, Thm. 1]).

The following result extends Kummer's formulas [3, p. 100].

PROPOSITION 2. *Let $Q \neq (\zeta_p - 1)$ be a prime ideal of $\mathbb{Z}[\zeta_p]$, and let q, f, F, s, and T be as before. Let b be such that $p^n \mid b$ and $b \mid (q^f-1)/2$ if q is odd, or $b \mid q^f-1$ if $q=2$. For $0 \le j \le b-1$ denote by η_j the period $\sum_{i=0}^{(q^f-1)/b-1} \zeta_q^{T(s^{j+ib})}$ (so $\eta_j \in \mathbb{Q}(\zeta_q+\zeta_q^{-1})$), and for $0 \le j \le b-1$ and $l \in \mathbb{Z}$ define $\eta_{j+lb} = \eta_j$. Let $i(Q)$ be as in* (1). *Then*

$$i(Q) \equiv \sum_{k=1}^{b-1}\sum_{l=1}^{b-1} k\omega^{-r}(l)\eta_k\eta_{k-l} \bmod p^n.$$

Proof. Let $H(X) = \sum_{j=0}^{b-1} \eta_j X^j$. With $G(X)$ as above, we have $G(X) \equiv H(X) \bmod (X^{p^n}-1)$. Therefore

$$\begin{aligned}\frac{\zeta_p G'(\zeta_p)}{G(\zeta_p)} &\equiv \frac{\zeta_p H'(\zeta_p)}{H(\zeta_p)} = \frac{1}{q^f}\zeta_p H'(\zeta_p)\overline{H(\zeta_p)} \\ &\equiv \sum_{k=1}^{b-1} k\eta_k\zeta_p^k \sum_{i=0}^{b-1} \eta_i\zeta_p^{-i} = \sum_{k=1}^{b-1}\sum_{i=0}^{b-1} k\eta_k\eta_i\zeta_p^{k-i} \\ &= \sum_{k=1}^{b-1}\sum_{l=k-b+1}^{k} k\eta_k\eta_{k-l}\zeta_p^l \equiv \sum_{k=1}^{b-1}\sum_{l=0}^{b-1} k\eta_k\eta_{k-l}\zeta_p^l \bmod p^n.\end{aligned}$$

So, by (5) and a known property of Gauss sums, we have

$$\begin{aligned} i(Q) &\equiv \left(\sum_{i=1}^{p-1} \omega^r(i)\zeta_p^i\right)^{-1} \sum_{j=1}^{p-1} \omega^r(j) \sum_{k=1}^{b-1}\sum_{l=0}^{b-1} k\eta_k\eta_{k-l}\zeta_p^{lj} \\ &= \left(\sum_{i=1}^{p-1} \omega^r(i)\zeta_p^i\right)^{-1} \sum_{k=1}^{b-1}\sum_{l=0}^{b-1} k\eta_k\eta_{k-l} \sum_{j=1}^{p-1} \omega^r(j)\zeta_p^{lj} \\ &= \sum_{k=1}^{b-1}\sum_{l=1}^{b-1} k\eta_k\eta_{k-l}\omega^{-r}(l) \bmod p^n, \end{aligned}$$

as desired. □

The following criterion to determine p^{l_n} and $|e_r(A)|$ is an immediate consequence of formula (1), the corollary to Proposition 1, and Proposition 2.

THEOREM 1. *Let $\mathcal{P}$ be the set of all prime ideals Q of $\mathbb{Z}[\zeta_p]$ above rational primes $q \equiv 1 \bmod p^n$. For each $Q \in \mathcal{P}$ above q, choose a primitive root $s = s_Q$ modulo q such that $s^{(q-1)/p} \equiv \zeta_p \bmod Q$; define the Gaussian periods $\eta_j = \eta_j(Q)$ by $\eta_j = \sum_{i=0}^{(q-1)/p^n-1} \zeta_q^{s^{j+ip^n}}$ for $0 \le j \le p^n-1$, and by $\eta_{j+lp^n} = \eta_j$ for $0 \le j \le p^n-1$ and $l \in \mathbb{Z}$. Define p^{l_Q} as the largest power of p, less than or equal to p^n, that divides the number $i(Q)$, where*

$$i(Q) \equiv \sum_{k=1}^{p^n-1}\sum_{l=1}^{p^n-1} k\omega^{-r}(l)\eta_k\eta_{k-l} \bmod p^n.$$

Let $m \ge n$ and let $\mathcal{P}_m$ be the set of all prime ideals Q of $\mathbb{Z}[\zeta_p]$ that are above rational primes q such that $q \equiv 1 \bmod p^m$ and $s^{(q-1)/p} \equiv \zeta_p \bmod Q$. Then $p^l = p^{l_n} \le p^{l_Q}$ for all $Q \in \mathcal{P}$, and p^l is the smallest of all p^{l_Q} such that $Q \in \mathcal{P}_m$. If n is large enough, then $p^l = |e_r(A)| = |e_r(W)|$.

To derive more information about the numbers p^l from Theorem 1 we need some results, on the periods η_j and on the so-called cyclotomic numbers, that will be demonstrated in the next section.

2. Characterizations of Gaussian Periods and Cyclotomic Numbers and the Determination of $|e_r(A)|$.

We preserve the notation of the first section. Let $q \equiv 1 \bmod p^n$ be a prime number, s a primitive root modulo q, and $\eta_0, \eta_1, \ldots, \eta_{p^n-1}$ the Gaussian periods of degree p^n in $\mathbb{Q}(\zeta_q)$ defined by

$$\eta_i = \sum_{k=0}^{(q-1)/p^n-1} \zeta_q^{s^{i+kp^n}} \tag{6}$$

Define $\eta_{i+jp^n} = \eta_i$ for $0 \le i \le p^n-1$ and $j \in \mathbb{Z}$. For $i \in \mathbb{Z}$ write

$$\eta_0\eta_i = \sum_{j=0}^{p^n-1} a_{i,j}\eta_j, \tag{7}$$

with $a_{i,j} \in \mathbb{Z}$. Define $a_{i+kp^n, j+lp^n} = a_{i,j}$ for $0 \le i, j \le p^n-1$ and $k, l \in \mathbb{Z}$.

As is usual, for $0 \le i, j \le p^n - 1$ we define the cyclotomic numbers (i, j) of order p^n as the number of ordered pairs (k, l), $0 \le k, l \le (q-1)/p^n - 1$, such that $1 + s^{kp^n+i} = s^{lp^n+j} \bmod q$ (see e.g. [2]).

We use the following version of Kronecker's delta:

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i \equiv j \bmod p^n, \\ 0 & \text{if } i \not\equiv j \bmod p^n. \end{cases}$$

By [2, formula (6)] we have that

$$a_{i,j} = (i, j) - \frac{q-1}{p^n}\delta_{0,i}, \tag{8}$$

for $0 \le i, j \le p^n - 1$.

The following propositions—which are immediate consequences of [8], Propositions 1, 2, and 3, Theorem 1, and formulas (12), (15), and (30)—give characterizations of the periods η_i and of the numbers $a_{i,j}$ (or, equivalently, of the cyclotomic numbers (i, j)). We shall use Propositions 3 and 6, which have the simplest statements. Propositions 4 and 5 are included for a better understanding of periods and cyclotomic numbers, as well as the relations between them, and for future reference.

PROPOSITION 3. *Let $\theta_0, \theta_1, \ldots, \theta_{p^n-1}$ be elements of a field K containing $\mathbb{Q}$. Define $\theta_{j+kp^n} = \theta_j$ for $0 \le j \le p^n - 1$ and $k \in \mathbb{Z}$. Suppose that:*

(i) *$\theta_0, \theta_1, \ldots, \theta_{p^n-1}$ are linearly independent over $\mathbb{Q}$;*
(ii) *$\sum_{i=0}^{p^n-1} \theta_i = -1$;*
(iii) *$\sum_{i=0}^{p^n-1} \theta_i \theta_{i+j} = q\delta_{0,j} - (q-1)/p^n$ for $0 \le j \le p^n - 1$; and*
(iv) *the numbers*

$$b_{i,j} = \frac{1}{q}\left(\left(\frac{q-1}{p^n}\right)^2 + \sum_{k=0}^{p^n-1} \theta_k \theta_{k+i} \theta_{k+j}\right)$$

are rational integers for $0 \le i, j \le p^n - 1$.

Then $\theta_0, \theta_1, \ldots, \theta_{p^n-1}$ are (in a certain order) the periods $\eta_0, \eta_1, \ldots, \eta_{p^n-1}$ of degree p^n in $\mathbb{Q}(\zeta_q)$, where ζ_q is a primitive qth root of 1 in the algebraic closure of K.

Conversely, if $\theta_0, \theta_1, \ldots, \theta_{p^n-1}$ are the periods $\eta_0, \eta_1, \ldots, \eta_{p^n-1}$, then conditions (i)–(iv) *are satisfied and $b_{i,j} = (i, j) = a_{i,j} + ((q-1)/p^n)\delta_{0,i}$ for $0 \le i, j \le p^n - 1$.*

PROPOSITION 4. *Let $c_{i,j}$ $(i, j \in \mathbb{Z})$ be integers such that, for all i, j:*

(i) *$c_{i,j} = c_{i+p^n,j} = c_{i,j+p^n}$;*
(ii) *$\sum_{k=0}^{p^n-1} c_{i,k} = (q-1)/p^n - q\delta_{0,i}$; and*
(iii) *$\sum_{k=0}^{p^n-1} c_{k,j} = -\delta_{0,j}$.*

Let $\theta_0, \theta_1, \ldots, \theta_{p^n-1}$ be elements in a field K containing $\mathbb{Q}$ such that

(iv) *$\theta_0, \theta_1, \ldots, \theta_{p^n-1}$ are linearly independent over $\mathbb{Q}$, and*
(v) *$\theta_i \theta_j = \sum_{k=0}^{p^n-1} c_{j-i,k-i}\theta_k$ for $0 \le i, j \le p^n - 1$.*

Then $\theta_0, \theta_1, \ldots, \theta_{p^n-1}$ *are (in a certain order) the periods* $\eta_0, \eta_1, \ldots, \eta_{p^n-1}$, *and* $c_{i,j}$ *are the corresponding numbers* $a_{i,j} = (i,j) - ((q-1)/p^n)\delta_{0,i}$.

Conversely, if $\theta_i = \eta_i$ *and* $c_{i,j} = a_{i,j}$ *for* $i, j \in \mathbb{Z}$, *then conditions* (i)–(v) *are satisfied.*

PROPOSITION 5. *Let* $c_{i,j}$ $(i, j \in \mathbb{Z})$ *be integers such that, for all* i, j:

(i) $c_{i,j} = c_{i+p^n,j} = c_{i,j+p^n}$,
(ii) $\sum_{k=0}^{p^n-1} c_{i,k} = (q-1)/p^n - q\delta_{0,i}$; *and*
(iii) $\sum_{k=0}^{p^n-1} c_{k,j} = -\delta_{0,j}$.

Let C *be the matrix* $[c_{i,j}]_{0\le i,j\le p^n-1}$, θ_0 *an eigenvalue of* C, *and* r *a fixed integer* $(0 \le r \le p^n-1)$. *Call* $\gamma_{r,0}, \gamma_{r,1}, \ldots, \gamma_{r,p^n-1}$ *the co-factors of* $C-\theta_0 I$ *corresponding to the* rth *row. That is,*

$$\gamma_{r,m} = (-1)^{r+m} \det[c_{i,j} - \delta_{i,j}\theta_0]_{0\le i,j\le p^n-1,\, i\ne r,\, j\ne m}.$$

Suppose that

(iv) *the characteristic polynomial of* C *is irreducible over* $\mathbb{Q}$, *and*
(v) $\theta_0\gamma_{r,k}\gamma_{r,l} = \sum_{j=0}^{p^n-1} c_{l-k,j-k}\gamma_{r,0}\gamma_{r,j}$ *for* $0 \le k, l \le p^n-1$.

Then, after some reordering of the columns of C, *the numbers* $c_{i,j}$ *are the integers* $a_{i,j} = (i,j) - ((q-1)/p^n)\delta_{0,i}$.

Conversely, if $c_{i,j} = a_{i,j}$ *for* $i, j \in \mathbb{Z}$ *and* $\theta_0 = \eta_0$, *then these conditions* (i)–(v) *are satisfied,* $\gamma_{r,0} \ne 0$, *and* $\eta_k = (\eta_0/\gamma_{r,0})\gamma_{r,k}$ *for* $0 \le k \le p^n-1$.

PROPOSITION 6. *Let* $C = [c_{i,j}]_{0\le i,j\le p^n-1}$ *be a matrix with entries in* $\mathbb{Z}$. *Define* $c_{i+kp^n,j+lp^n} = c_{i,j}$ *for* $0 \le i, j \le p^n-1$ *and* $k, l \in \mathbb{Z}$. *Suppose that, for all integers* i, j, l *we have:*

(i) $\sum_{k=0}^{p^n-1} c_{i,k} = (q-1)/p^n - q\delta_{0,i}$;
(ii) $\sum_{k=0}^{p^n-1} c_{k,j} = -\delta_{0,j}$;
(iii) $c_{i,j} = c_{-i,j-i}$;
(iv) $\sum_{k=0}^{p^n-1} c_{i,k}c_{k-j,l-j} = \sum_{k=0}^{p^n-1} c_{j,k}c_{k-i,l-i}$; *and*
(v) *the polynomial* $\det(xI-C)$ *is irreducible over* $\mathbb{Q}$.

Then (after some relabeling of the periods $\eta_0, \eta_1, \ldots, \eta_{p^n-1}$) $c_{i,j} = a_{i,j} = (i,j) - ((q-1)/p^n)\delta_{0,i}$ *for* $0 \le i, j \le p^n-1$.

Conversely, if $c_{i,j} = a_{i,j}$ *for* $0 \le i, j \le p^n-1$, *then these conditions* (i)–(v) *are satisfied.*

We can restate Proposition 6 as follows.

PROPOSITION 6′. *Let* $C = [c_{i,j}]_{0\le i,j\le p^n-1}$ *be a matrix with entries in* $\mathbb{Z}$, *and let* R *be the* $p^n \times p^n$ *matrix* $[\delta_{i+1,j}]_{i,j}$; *that is,*

$$R = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}.$$

Denote the ith *row of a matrix* B *by* $[B]_i$. *Suppose that:*

(i) *the sum of the elements of the* ith *row of* C *is* $(q-1)/p^n - q\delta_{0,i}$;
(ii) *the sum of the elements of the* jth *column of* C *is* $-\delta_{0,j}$;
(iii) $[R^{-j}CR^j]_i = [R^{-i}CR^i]_j$;
(iv) $[CR^{-j}CR^j]_i = [CR^{-i}CR^i]_j$; *and*
(v) *the polynomial* $\det(xI-C)$ *is irreducible over* $\mathbb{Q}$.

Then (after some relabeling of the periods $\eta_0, \eta_1, \ldots, \eta_{p^n-1}$)

$$c_{i,j} = a_{i,j} = (i,j) - \frac{q-1}{p^n}\delta_{0,i} \quad \text{for } 0 \le i, j \le p^n - 1.$$

Conversely, if $c_{i,j} = a_{i,j}$ *for* $0 \le i, j \le p^n - 1$, *then conditions* (i)–(v) *are satisfied.*

Assume now that p is not a pth power modulo q. Then there is a primitive root s modulo q such that

$$s \equiv pt^{p^n} \bmod q \quad \text{for some } t \in \mathbb{Z}. \tag{9}$$

In fact, let s_1 be any primitive root modulo q. Write $p \equiv s_1^j \bmod q$, with $j \in \mathbb{Z}$. Since $p \nmid j$, by the Chinese remainder theorem there exists $j_1 \in \mathbb{Z}$, relatively prime with $q-1$ and such that $j \equiv j_1 \bmod p^n$. So $p \equiv s_1^{j_1 + p^n k} \bmod q$ for some $k \in \mathbb{Z}$. Therefore $s = s_1^{j_1}$ is a primitive root modulo q satisfying (9). Choose s as in (9) and let

$$S = \{x^{p^n} : x \in (\mathbb{Z}/q\mathbb{Z})^\times\}. \tag{10}$$

If the periods η_i are defined as in (6) then, for $i \ge 0$,

$$\eta_i = \sum_{x \in S} \zeta_q^{xp^i}. \tag{11}$$

This implies that

$$\eta_i^p \equiv \eta_{i+1} \bmod p \tag{12}$$

for all $i \in \mathbb{Z}$. Since $\{\eta_0, \eta_1, \ldots, \eta_{p^n-1}\}$ is an integral basis of $\mathbb{Q}(\eta_0)$ and its discriminant is a power of q, for any prime ideal P of $\mathbb{Q}(\eta_0)$ above p we have $\eta_i \not\equiv \eta_j \bmod P$ if $i \not\equiv j \bmod p^n$. Moreover, by (12), all the roots of the minimal polynomial of η_0 over $\mathbb{Q}$ with coefficients reduced modulo p (roots lying in the splitting field of the polynomial over $\mathbb{Z}/p\mathbb{Z}$) are conjugate of any given one by powers of the Frobenius automorphism. Therefore the minimal polynomial of η_0 over $\mathbb{Q}$ is irreducible modulo p, and p is inert in $\mathbb{Q}(\eta_0)$. In particular, $p \nmid \eta_0\eta_1 \cdots \eta_{p^n-1}$.

Conversely, let s be a primitive root modulo q and let the periods η_i be defined as in (6). Suppose that $\eta_0, \eta_1, \ldots, \eta_{p^n-1}$ are pairwise noncongruent modulo p and that $\eta_i^p \equiv \eta_{i+1} \bmod p$; then formula (9) holds. In fact, let u be an integer such that $p \equiv s^u \bmod q$. Then we must have that $\eta_{i+1} = \eta_{i+u}$. Therefore $u \equiv 1 \bmod p^n$ and (9) follows.

As in Theorem 1, define $\mathcal{P}$ as the set of all prime ideals Q of $\mathbb{Z}[\zeta_p]$ above rational primes $q \equiv 1 \bmod p^n$ and, for $m \ge 1$, define $\mathcal{P}_m$ as the set of all prime

ideals Q of $\mathbb{Z}[\zeta_p]$ above rational primes q such that $q \equiv 1 \bmod p^m$ and $p^{(q-1)/p} \equiv \zeta_p \bmod Q$. Note that if $Q \in \mathcal{P}_m$ is above the rational prime q and if s satisfies (9) then $s^{(q-1)/p} \equiv \zeta_p \bmod Q$.

These observations are summarized in the following lemma, which allows us to label the Gaussian periods in a way suitable for their use in formulas for $i(Q)$ (as in Proposition 2 and Theorem 1), where $Q \in \mathcal{P}_n$ is a prime ideal above q.

LEMMA 1. *Let $q \equiv 1 \bmod p^n$ be a prime number, s a primitive root modulo q, and η_i the Gaussian periods defined in* (6). *Then $s \equiv pt^{p^n} \bmod q$ for some $t \in \mathbb{Z}$ if and only if $\eta_0, \eta_1, \ldots, \eta_{p^n-1}$ are pairwise noncongruent modulo p and $\eta_i^p \equiv \eta_{i+1} \bmod p$ for all $i \in \mathbb{Z}$. In that case the periods η_i can be defined by* (10) *and* (11), *the minimal polynomial of η_0 is irreducible modulo p, and p is inert in $\mathbb{Q}(\eta_0)$.*

There is only one Galois ring extension of $\mathbb{Z}/p^n\mathbb{Z}$ of degree p^n, up to isomorphism (see [5, Chap. XV & XVI]); we call this extension $\mathcal{R}_n$. It is isomorphic, for example, to $\mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p^n-1}]/p^n\mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p^n-1}] \cong \mathbb{Z}[\eta_0]/p^n\mathbb{Z}[\eta_0]$, where $q \equiv 1 \bmod p^n$ is a prime such that p is not a pth power modulo q and the η_i are as in (11). (All properties of $\mathcal{R}_n$ that we shall use can be easily deduced from this representation.) Note that $\mathcal{R}_1 = \mathbb{F}_{p^p}$, the field with p^p elements.

The next proposition shows implications between certain properties satisfied by the residue classes modulo p^n of the periods η_i defined in (11) when $q \equiv 1 \bmod p^{2n}$.

PROPOSITION 7. *Let $\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1}$ be elements of $\mathcal{R}_n$. For $0 \le i \le p^n-1$ and $k \in \mathbb{Z}$, define $\bar{\theta}_{i+kp^n} = \bar{\theta}_i$. Suppose that:*

(i) $\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1}$ *are pairwise noncongruent modulo p;*
(ii) $\sum_{k=0}^{p^n-1} \bar{\theta}_k = -1$;
(iii) $\sum_{k=0}^{p^n-1} \bar{\theta}_k \bar{\theta}_{k+i} = \delta_{0,i}$ *for all $i \in \mathbb{Z}$;*
(iv) $\bar{\theta}_i^p \equiv \bar{\theta}_{i+1}$ *mod p for all $i \in \mathbb{Z}$; and*
(v) $\sum_{k=0}^{p^n-1} \bar{\theta}_k \bar{\theta}_{k+i} \bar{\theta}_{k+j} = \bar{c}_{i,j}$ *for some elements $\bar{c}_{i,j} \in \mathbb{Z}/p^n\mathbb{Z}$, $0 \le i, j \le p^n-1$.*

Write $\bar{c}_{i+kp^n, j+lp^n} = \bar{c}_{i,j}$ for $0 \le i, j \le p^n-1$ and $k, l \in \mathbb{Z}$, and call $\bar{C}$ the matrix $[\bar{c}_{i,j}]_{0 \le i,j \le p^n-1}$. Then, for all integers i, j and l:

(vi) $\bar{\theta}_i \bar{\theta}_j = \sum_{k=0}^{p^n-1} \bar{c}_{j-i,k-i} \bar{\theta}_k$;
(vii) $\det(xI - \bar{C}) = (x-\bar{\theta}_0)(x-\bar{\theta}_1)\cdots(x-\bar{\theta}_{p^n-1})$;
(viii) $\bar{c}_{i,j} = \bar{c}_{j,i}$;
(ix) $\bar{c}_{i,j} = \bar{c}_{-i,j-i}$;
(x) $\sum_{k=0}^{p^n-1} \bar{c}_{i,k} = -\delta_{0,i}$;
(xi) $\sum_{k=0}^{p^n-1} \bar{c}_{k,j} = -\delta_{0,j}$;
(xii) $\sum_{k=0}^{p^n-1} \bar{c}_{i,k} \bar{c}_{k-j,l-j} = \sum_{k=0}^{p^n-1} \bar{c}_{j,k} \bar{c}_{k-i,l-i}$; *and*
(xiii) *the polynomial* $\det(xI - \bar{C})$ *is irreducible modulo p.*

(xiv) *Define*

$$\bar{\gamma}_{i,j} = (-1)^{i+j} \det[\bar{c}_{u,v} - \delta_{u,v}\bar{\theta}_0]_{0 \le u,v \le p^n-1, u \ne i, v \ne j}.$$

Then $\bar{\gamma}_{l,0} \not\equiv 0 \bmod p$ *and* $\bar{\theta}_i = (\bar{\theta}_0/\bar{\gamma}_{l,0})\bar{\gamma}_{l,i}$.

Let $Q \in \mathcal{P}_{2n}$ *above* $q \in \mathbb{Z}$, *and let* η_i *be as in* (11). *Define the integers* $a_{i,j}$ *as in* (7). *Put* $\mathcal{R}_n = \mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p^n-1}]/p^n\mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p^n-1}]$. *If* $\bar{\theta}_i$ *and* $\bar{c}_{i,j}$ *are respectively the images of* η_i *in* $\mathcal{R}_n$ *and of* $a_{i,j}$ *in* $\mathbb{Z}/p^n\mathbb{Z}$, *then all conditions* (i)–(xiv) *are satisfied.* (*Note also that, since* $q \equiv 1 \bmod p^{2n}$, *by formula* (8) *we have* $a_{i,j} \equiv (i,j) \bmod p^n$.)

Proof. (For more details on this proof see [8], where we show similar results over $\mathbb{Z}$.) The last affirmation follows directly from Lemma 1, from [2, formula (14)], and from Propositions 3–6 (see also [2]).

Suppose that $\bar{\theta}_i \in \mathcal{R}_n$ and $\bar{c}_{i,k} \in \mathbb{Z}/p^n\mathbb{Z}$ satisfy conditions (i)–(v). Then

$$\sum_{k=0}^{p^n-1} \bar{c}_{j-i,k-i}\bar{\theta}_k = \sum_{k=0}^{p^n-1}\sum_{l=0}^{p^n-1} \bar{\theta}_l\bar{\theta}_{l+j-i}\bar{\theta}_{l+k-i}\bar{\theta}_k$$

$$= \sum_{l=0}^{p^n-1} \bar{\theta}_l\bar{\theta}_{l+j-i} \sum_{k=0}^{p^n-1} \bar{\theta}_{l+k-i}\bar{\theta}_k = \sum_{l=0}^{p^n-1} \bar{\theta}_l\bar{\theta}_{l+j-i}\delta_{l,i} = \bar{\theta}_i\bar{\theta}_j.$$

This proves (vi). From (vi) and the commutative and associative laws of multiplication in $\mathcal{R}_n$, we obtain (ix) and (xii) (for the last one expand the equality $(\bar{\theta}_0\bar{\theta}_i)\bar{\theta}_j = (\bar{\theta}_0\bar{\theta}_j)\bar{\theta}_i$). From (v) we get (viii). From (ii), (iii), and (v) we get (x). From (viii) and (x) we get (xi).

Let $T = (\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1})^t$ and let R be as in Proposition 6′. We can write (vi) as

$$(\bar{C} - \bar{\theta}_k I)R^k T = 0 \tag{13}$$

for all $k \in \mathbb{Z}$. In particular, $\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1}$ are eigenvalues of $\bar{C}$ and by (i) they are distinct modulo p; so we have (vii) (use Hensel's lemma). From (i), (iv), and (vii) we get (xiii). In fact, by (iv), all the $\bar{\theta}_i$ modulo p are conjugate of $\bar{\theta}_0$ over $\mathbb{Z}/p\mathbb{Z}$; by (i) there are p^n distinct such conjugates and by (vii) they are the roots of $\det(xI - \bar{C})$ modulo p.

To prove (xiv) fix l and observe first that, by (xiii), $\bar{\gamma}_{l,0} \not\equiv 0 \bmod p$. Call $\Gamma = (\gamma_{l,0}, \gamma_{l,1}, \ldots, \gamma_{l,p^n-1})^t$. We have $(\bar{C} - \bar{\theta}_0 I)\Gamma = 0$. Also, by (13), $(\bar{C} - \bar{\theta}_0 I)T = 0$. Since, by (xiii), $\bar{C} - \bar{\theta}_0 I$ modulo p has rank $p^n - 1$, for some $\lambda \in \mathbb{Z}/p^n\mathbb{Z}$ we must have that $(\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1}) = \lambda(\gamma_{l,0}, \gamma_{l,1}, \ldots, \gamma_{l,p^n-1})$. Therefore $\lambda = \bar{\theta}_0/\gamma_{l,0}$ and $\bar{\theta}_i = (\bar{\theta}_0/\gamma_{l,0})\gamma_{l,i}$. □

We will need the following lemma, similar to Lemma 1, to label the cyclotomic numbers in a way suitable for their use in formulas for $i(Q)$, where $Q \in \mathcal{P}_n$.

LEMMA 2. *Let* $q \equiv 1 \bmod p^n$ *be a prime number,* s *a primitive root modulo* q, η_i *the Gaussian periods defined in* (6), $a_{i,j}$ *the integers defined in* (7), *and* $\mathfrak{A}$ *the matrix* $[a_{i,j}]_{0 \le i,j \le p^n-1}$. *Then* $s \equiv pt^{p^n} \bmod q$ *for some* $t \in \mathbb{Z}$ *if and only if* $\det(xI - \mathfrak{A})$ *is irreducible mod* p *and for one* (*for each*) *of its roots* θ_0 *we have*

$$\theta_0^{1+p^i} \equiv \sum_{k=0}^{p^n-1} a_{i,k}\theta_0^{p^k} \bmod p \tag{14}$$

for $0 \le i \le p^n - 1$.

Proof. By Lemma 1, if $s \equiv pt^{p^n} \bmod q$ for some $t \in \mathbb{Z}$ then $\det(xI-\mathfrak{A})$ is irreducible modulo p and $\eta_i^p \equiv \eta_{i+1} \bmod p$. So (14) holds for any root θ_0 of $\det(xI-\mathfrak{A})$ (these roots are just the periods η_i). Conversely, suppose that $\det(xI-\mathfrak{A})$ is irreducible modulo p and that (14) holds for one of its roots θ_0. From formulas (7) and (14) and from the fact that $\theta_0 I-\mathfrak{A}$ modulo p has rank p^n-1, we can deduce that there is some $l \in \mathbb{Z}$ such that $\eta_i \equiv \theta_{i+l} \bmod p$ for all $i \in \mathbb{Z}$. Therefore $\eta_i^p \equiv \eta_{i+1} \bmod p$ and, by Lemma 1, $s \equiv pt^{p^n} \bmod q$ for some $t \in \mathbb{Z}$. □

The following definitions will each allow us to divide the problem of finding formulas for the numbers $i(Q)$, $Q \in \mathcal{P}_n$, and for the numbers p^l defined in Section 1, into two problems. Problem 1 consists of the search, between vectors in $\mathcal{R}_n^{p^n}$ or $p^n \times p^n$ matrices with entries in $\mathbb{Z}/p^n\mathbb{Z}$ satisfying certain congruence conditions, of the vectors and matrices that "correspond" to prime ideals $Q \in \mathcal{P}_n$. Problem 2 consists of the search of all vectors or matrices satisfying those congruence conditions and of the values obtained by formally substituting the coordinates of the vectors (or the entries of the matrices) into the formulas for $i(Q)$—that is, the values that will yield $i(Q)$ when the vectors or matrices actually correspond to prime ideals Q.

Definition 1. Let $\bar{\eta}_0, \bar{\eta}_1, \ldots, \bar{\eta}_{p^n-1} \in \mathcal{R}_n$ and let $m \geq n$. We say that $(\bar{\eta}_0, \bar{\eta}_1, \ldots, \bar{\eta}_{p^n-1})$ corresponds to a prime ideal $Q \in \mathcal{P}_m$ above a rational prime q if, for the periods η_i defined by (10) and (11), the element $\bar{\eta}_i$ can be identified with the congruence class of η_i modulo p^n for $0 \leq i \leq p^n-1$.

Definition 2. For $0 \leq i, j \leq p^n-1$, let $\bar{a}_{i,j} \in \mathbb{Z}/p^n\mathbb{Z}$ and $m \geq n$. We say that the matrix $[\bar{a}_{i,j}]_{0 \leq i,j \leq p^n-1}$ corresponds to a prime ideal $Q \in \mathcal{P}_m$ above a rational prime q if for the periods η_i defined by (10) and (11), and for the integers $a_{i,j}$ as in (7), the element $\bar{a}_{i,j}$ is the congruence class of $a_{i,j}$ modulo p^n for $0 \leq i, j \leq p^n-1$.

From Propositions 3, 6, and 7, and from Lemmas 1 and 2, we derive the following criteria for recognizing when a vector $(\bar{\eta}_i)_{0 \leq i \leq p^n-1}$ with $\bar{\eta}_i \in \mathcal{R}_n$, and a matrix $[\bar{a}_{i,j}]_{0 \leq i,j \leq p^n-1}$ with $\bar{a}_{i,j} \in \mathbb{Z}/p^n\mathbb{Z}$, correspond to a prime ideal $Q \in \mathcal{P}_{2n}$.

Proposition 8. *Let* $\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1}$ *be elements of* $\mathcal{R}_n$. *If* $(\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1})$ *corresponds to a prime ideal* $Q \in \mathcal{P}_{2n}$, *then the* $\bar{\theta}_i$ *satisfy:*

(a) $\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1}$ *are pairwise noncongruent modulo* p;
(b) $\sum_{k=0}^{p^n-1} \bar{\theta}_k = -1$;
(c) $\sum_{k=0}^{p^n-1} \bar{\theta}_k \bar{\theta}_{k+i} = \delta_{0,i}$ *for all* $i \in \mathbb{Z}$;
(d) $\bar{\theta}_i^p \equiv \bar{\theta}_{i+1}$ *mod* p *for all* $i \in \mathbb{Z}$; *and*
(e) $\sum_{k=0}^{p^n-1} \bar{\theta}_k \bar{\theta}_{k+i} \bar{\theta}_{k+j} = \bar{c}_{i,j}$ *for some elements* $\bar{c}_{i,j} \in \mathbb{Z}/p^n\mathbb{Z}$, $0 \leq i, j \leq p^n-1$,

where we define $\bar{\theta}_{i+jp^n} = \bar{\theta}_i$ *for* $0 \leq i \leq p^n-1$ *and* $j \in \mathbb{Z}$.

Conversely, suppose that the $\bar{\theta}_i$ *satisfy conditions* (a)–(e) (*so these elements satisfy, together with the* $\bar{c}_{i,j} \in \mathbb{Z}/p^n\mathbb{Z}$, *all conditions of Proposition 7*).

Then $(\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1})$ *corresponds to a prime ideal* $Q \in \mathcal{P}_{2n}$ *above a rational prime* q *if, for some prime* $q \equiv 1 \bmod p^{2n}$ *and for* $0 \le i \le p^n - 1$, *the elements* $\bar{\theta}_i$ *are the congruence classes modulo* p^n *of elements* θ_i *in some field extension of* $\mathbb{Q}$ *(i.e.* $\bar{\theta}_i$ *is the image of* θ_i *in* $\mathbb{Z}[\theta_0, \theta_1, \ldots, \theta_{p^n-1}]/p^n\mathbb{Z}[\theta_0, \theta_1, \ldots, \theta_{p^n-1}]$*) that satisfy:*

(i) $\sum_{k=0}^{p^n-1} \theta_k = -1$;
(ii) $\sum_{k=0}^{p^n-1} \theta_k \theta_{k+i} = q\delta_{0,i} - (q-1)/p^n$ *for* $0 \le i \le p^n - 1$; *and*
(iii) *the numbers*

$$b_{i,j} = \frac{1}{q}\left(\left(\frac{q-1}{p^n}\right)^2 + \sum_{k=0}^{p^n-1} \theta_k \theta_{k+i} \theta_{k+j}\right)$$

are rational integers for $0 \le i, j \le p^n - 1$,

where we define $\theta_{i+jp^n} = \theta_i$ *for* $0 \le i \le p^n - 1$ *and* $j \in \mathbb{Z}$. *(Observe that by Proposition 3 the* θ_i *are the periods of degree* p^n *of* $\mathbb{Q}(\zeta_q)$.)

Proof. If $(\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1})$ corresponds to a prime ideal $Q \in \mathcal{P}_{2n}$, then the $\bar{\theta}_i$ satisfy conditions (b), (c), and (e) by Proposition 3, and conditions (a) and (d) by Lemma 1.

Now suppose that the $\bar{\theta}_i$ satisfy conditions (a)–(e) and that they are the congruence classes modulo p^n of elements θ_i in some field extension of $\mathbb{Q}$ that, for some prime $q \equiv 1 \bmod p^{2n}$, satisfy conditions (i)–(iii). Conditions (a)–(e) imply, by Proposition 7, that $\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1}$ are linearly independent modulo p; hence $\theta_0, \theta_1, \ldots, \theta_{p^n-1}$ are linearly independent over $\mathbb{Q}$. Therefore, by Proposition 3, Lemma 1, and Definition 1, we have that $(\theta_0, \theta_1, \ldots, \theta_{p^n-1})$ corresponds to a prime ideal $Q \in \mathcal{P}_{2n}$ above q. □

PROPOSITION 9. *Let* $\bar{c}_{i,j}$, $0 \le i, j \le p^n - 1$, *be elements in* $\mathbb{Z}/p^n\mathbb{Z}$. *If the matrix* $\bar{C} = [\bar{c}_{i,j}]_{0 \le i,j \le p^n-1}$ *corresponds to a prime ideal* $Q \in \mathcal{P}_{2n}$, *then the* $\bar{c}_{i,j}$ *satisfy:*

(a) $\bar{c}_{i,j} = \bar{c}_{j,i}$;
(b) $\sum_{k=0}^{p^n-1} \bar{c}_{k,j} = -\delta_{0,j}$;
(c) $\bar{c}_{i,j} = \bar{c}_{-i,j-i}$;
(d) $\sum_{k=0}^{p^n-1} \bar{c}_{i,k}\bar{c}_{k-j,l-j} = \sum_{k=0}^{p^n-1} \bar{c}_{j,k}\bar{c}_{k-i,l-i}$ *for all* $i, j, l \in \mathbb{Z}$;
(e) $\det(xI - \bar{C})$ *is irreducible modulo* p,

where we define $\bar{c}_{i+kp^n, j+lp^n} = \bar{c}_{i,j}$ *for* $0 \le i, j \le p^n - 1$ *and* $k, l \in \mathbb{Z}$; *and*

(f) *the elements* $\bar{c}_{i,j}$ *are labeled in such a way that, if* $\bar{\theta}_0$ *is a root of* $\det(xI - \bar{C})$, *then* $\bar{\theta}_0^{1+p^i} \equiv \sum_{k=0}^{p^n-1} \bar{c}_{i,k}\bar{\theta}_0^{p^k} \bmod p$ *for* $0 \le i \le p^n - 1$.

Conversely, suppose that the $\bar{c}_{i,j}$ *satisfy conditions* (a)–(f). *Then the matrix* $\bar{C}$ *corresponds to a prime ideal* $Q \in \mathcal{P}_{2n}$ *above a rational prime* q *if, for some prime* $q \equiv 1 \bmod p^{2n}$ *and for* $0 \le i, j \le p^n - 1$, *the elements* $\bar{c}_{i,j}$ *are the congruence classes modulo* p^n *of integers* $c_{i,j}$ *satisfying:*

(i) $\sum_{k=0}^{p^n-1} c_{i,k} = (q-1)/p^n - q\delta_{0,i}$;
(ii) $\sum_{k=0}^{p^n-1} c_{k,j} = -\delta_{0,j}$;

(iii) $c_{i,j}=c_{-i,j-i}$; *and*
(iv) $\sum_{k=0}^{p^n-1} c_{i,k}c_{k-j,l-j}=\sum_{k=0}^{p^n-1} c_{j,k}c_{k-i,l-i}$ *for all* $i,j,l\in\mathbb{Z}$,
where we define $c_{i+kp^n,j+lp^n}=c_{i,j}$ *for* $0\le i,j\le p^n-1$ *and* $k,l\in\mathbb{Z}$.

Proof. If the matrix $\bar{C}=[\bar{c}_{i,j}]_{0\le i,j\le p^n-1}$ corresponds to a prime ideal $Q\in\mathcal{P}_{2n}$, then the $\bar{c}_{i,j}$ satisfy condition (a) by formula (8), conditions (b), (c), and (d) by Proposition 6, and conditions (e) and (f) by Lemma 2.

Now suppose that, for some prime $q\equiv 1 \bmod p^{2n}$ and for $0\le i,j\le p^n-1$, elements $\bar{c}_{i,j}$ satisfying conditions (a)–(f) are the congruence classes modulo p^n of integers $c_{i,j}$ satisfying conditions (i)–(iv). Note that, by condition (e), $\det(xI-C)$ is irreducible over $\mathbb{Q}$. Then, by Proposition 6, Lemma 2, and Definition 2, we have that the matrix $\bar{C}$ corresponds to a prime ideal $Q\in\mathcal{P}_{2n}$ above q. □

We can restate Proposition 9 in a more suggestive way as follows.

PROPOSITION 9′. *Let* $\bar{c}_{i,j}$, $0\le i,j\le p^n-1$, *be integers such that* $0\le\bar{c}_{i,j}\le p^n-1$. *If the matrix* $\bar{C}=[\bar{c}_{i,j}]_{0\le i,j\le p^n-1}$ *modulo* p^n *corresponds to a prime ideal* $Q\in\mathcal{P}_{2n}$, *then the* $\bar{c}_{i,j}$ *satisfy:*

(a) $\bar{c}_{i,j}\equiv\bar{c}_{j,i} \bmod p^n$;
(b) $\sum_{k=0}^{p^n-1}\bar{c}_{k,j}\equiv-\delta_{0,j} \bmod p^n$;
(c) $\bar{c}_{i,j}\equiv\bar{c}_{-i,j-i} \bmod p^n$;
(d) $\sum_{k=0}^{p^n-1}\bar{c}_{i,k}\bar{c}_{k-j,l-j}\equiv\sum_{k=0}^{p^n-1}\bar{c}_{j,k}\bar{c}_{k-i,l-i} \bmod p^n$ *for all* $i,j,l\in\mathbb{Z}$;
(e) $\det(xI-\bar{C})$ *is irreducible modulo* p,

where we define $\bar{c}_{i+kp^n,j+lp^n}=\bar{c}_{i,j}$ *for* $0\le i,j\le p^n-1$ *and* $k,l\in\mathbb{Z}$; *and*

(f) *the elements* $\bar{c}_{i,j}$ *are labeled in such a way that, if* $\bar{\theta}_0$ *is a root of* $\det(xI-\bar{C})$, *then* $\bar{\theta}_0^{1+p^i}\equiv\sum_{k=0}^{p^n-1}\bar{c}_{i,k}\bar{\theta}_0^{p^k} \bmod p$ *for* $0\le i\le p^n-1$.

Conversely, suppose that the integers $\bar{c}_{i,j}$ (*such that* $0\le\bar{c}_{i,j}\le p^n-1$) *satisfy conditions* (a)–(f). *Then the matrix* $\bar{C}$ *modulo* p^n *corresponds to a prime ideal* $Q\in\mathcal{P}_{2n}$ *above a rational prime* q *if there exist integers* $t_{i,j}$, $0\le i,j\le p^n-1$, *such that:*

(i) $\sum_{k=0}^{p^n-1}t_{k,j}=-(1/p^n)(\sum_{k=0}^{p^n-1}\bar{c}_{k,j}+\delta_{0,j})$;
(ii) $t_{j,i}=t_{i,j}+((q-1)/p^{2n})(\delta_{0,i}-\delta_{0,j})$;
(iii) $t_{i,j}=t_{-i,j-i}$; *and*
(iv)
$$\begin{aligned}&\sum_{k=0}^{p^n-1}\bar{c}_{i,k}\bar{c}_{k-j,l-j}+p^n\sum_{k=0}^{p^n-1}\bar{c}_{i,k}t_{k-j,l-j}\\&\quad+p^n\sum_{k=0}^{p^n-1}t_{i,k}\bar{c}_{k-j,l-j}+p^{2n}\sum_{k=0}^{p^n-1}t_{i,k}t_{k-j,l-j}\\&=\sum_{k=0}^{p^n-1}\bar{c}_{j,k}\bar{c}_{k-i,l-i}+p^n\sum_{k=0}^{p^n-1}\bar{c}_{j,k}t_{k-i,l-i}\\&\quad+p^n\sum_{k=0}^{p^n-1}t_{j,k}\bar{c}_{k-i,l-i}+p^{2n}\sum_{k=0}^{p^n-1}t_{j,k}t_{k-i,l-i}\end{aligned}$$
for all $i,j,l\in\mathbb{Z}$,

where we define $t_{i+kp^n,j+lp^n}=t_{i,j}$ *for* $0\le i,j\le p^n-1$ *and* $k,l\in\mathbb{Z}$.

Proof. The first statement is clear by Proposition 9. For the converse, with integers $\bar{c}_{i,j}$ and $t_{i,j}$ satisfying the above conditions write $c_{i,j} = \bar{c}_{i,j} + p^n t_{i,j}$. Then the integers $c_{i,j}$ satisfy all conditions of Proposition 9 (to better understand condition (ii), see formula (8)). Therefore the matrix $\bar{C}$ modulo p^n corresponds to a prime $Q \in \mathcal{P}_n$. □

The next result is an improved version of Theorem 1. More precise information for the case $n = 1$ is given in Section 3 where we study Vandiver's conjecture.

THEOREM 2. *Let V_n be the set of all p^n-tuples $(\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1})$ of elements in $\mathfrak{R}_n$ that satisfy:*

(a) *$\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1}$ are pairwise noncongruent modulo p;*
(b) *$\sum_{k=0}^{p^n-1} \bar{\theta}_k = -1$;*
(c) *$\sum_{k=0}^{p^n-1} \bar{\theta}_k \bar{\theta}_{k+i} = \delta_{0,i}$ for all $i \in \mathbb{Z}$;*
(d) *$\bar{\theta}_i^p \equiv \bar{\theta}_{i+1} \bmod p$ for all $i \in \mathbb{Z}$; and*
(e) *$\sum_{k=0}^{p^n-1} \bar{\theta}_k \bar{\theta}_{k+i} \bar{\theta}_{k+j} = \bar{c}_{i,j}$ for some elements $\bar{c}_{i,j} \in \mathbb{Z}/p^n\mathbb{Z}$, $0 \le i, j \le p^n - 1$,*

where we define $\bar{\theta}_{i+jp^n} = \bar{\theta}_i$ for $0 \le i \le p^n - 1$ and $j \in \mathbb{Z}$ (therefore these elements satisfy, together with the $\bar{c}_{i,j} \in \mathbb{Z}/p^n\mathbb{Z}$, all conditions of Proposition 7). Let U_n be the set of all p^n-tuples $(\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1})$ of elements in $\mathfrak{R}_n$ that correspond to prime ideals $Q \in \mathcal{P}_{2n}$ (see Definition 1 and Proposition 8). For all $\bar{\Theta} = (\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p^n-1}) \in (\mathfrak{R}_n)^{p^n}$ call $\nu(\bar{\Theta})$ the greatest power of p, less than or equal to p^n, that divides $\sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l) \bar{\theta}_k \bar{\theta}_{k-l}$. Then $U_n \subseteq V_n$ and $p^{l_n} = \min\{\nu(\bar{\Theta}) : \bar{\Theta} \in U_n\}$.

Proof. The proof is immediate from Theorem 1, Definition 1, and Proposition 8. □

Let Q be a prime ideal of $\mathbb{Z}[\zeta_p]$ above a rational prime $q \equiv 1 \bmod p^n$, and let s be a primitive root modulo q such that $s^{(q-1)/p} \equiv \zeta_p \bmod Q$. Define the periods η_i and the integers $a_{i,j}$ as in (6) and (7). Let $i(Q)$ be as in (1). By Proposition 2, we have $i(Q) \equiv \sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l) \eta_k \eta_{k-l} \bmod p^n$. Therefore $i(Q)\eta_0 \equiv \sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l) \eta_0 \eta_k \eta_{k-l} \bmod p^n$. Taking traces (from $\mathbb{Q}(\eta_0)$ to $\mathbb{Q}$) and applying Propositions 3 and 6, we get

$$\begin{aligned} i(Q) &\equiv -\sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l) \left(q a_{k,k-l} + q\left(\frac{q-1}{p^n}\right) - \left(\frac{q-1}{p^n}\right)^2 \right) \\ &= -q \sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l) a_{k,k-l} \equiv -\sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l) a_{-k,-l} \bmod p^n. \end{aligned}$$

Therefore

$$i(Q) \equiv \sum_{k=1}^{p^n-1} \sum_{l=1}^{p^n-1} k\omega^{-r}(l) a_{k,l} \bmod p^n \tag{15}$$

(see also the Kummer formulas in [3, p. 100]). This result can be used to express p^{l_n} in terms of rational integers as follows.

THEOREM 3. *Let* Y_n *be the set of all matrices* $\bar{C}=[\bar{c}_{i,j}]_{0\le i,j\le p^n-1}$ *over* $\mathbb{Z}/p^n\mathbb{Z}$ *such that:*

(a) $\bar{c}_{i,j}=\bar{c}_{j,i}$;
(b) $\sum_{k=0}^{p^n-1}\bar{c}_{k,j}=-\delta_{0,j}$;
(c) $\bar{c}_{i,j}=\bar{c}_{-i,j-i}$;
(d) $\sum_{k=0}^{p^n-1}\bar{c}_{i,k}\bar{c}_{k-j,l-j}=\sum_{k=0}^{p^n-1}\bar{c}_{j,k}\bar{c}_{k-i,l-i}$ *for all* $i,j,l\in\mathbb{Z}$;
(e) $\det(xI-\bar{C})$ *is irreducible modulo* p,

where we define $\bar{c}_{i+kp^n,j+lp^n}=\bar{c}_{i,j}$ *for* $0\le i,j\le p^n-1$ *and* $k,l\in\mathbb{Z}$; *and*

(f) *the elements* $\bar{c}_{i,j}$ *are labeled in such a way that, if* $\bar{\theta}_0$ *is a root of* $\det(xI-\bar{C})$, *then* $\bar{\theta}_0^{1+p^i}\equiv\sum_{k=0}^{p^n-1}\bar{c}_{i,k}\bar{\theta}_0^{p^k}$ *mod* p *for* $0\le i\le p^n-1$.

Let X_n *be the set of all matrices* $[\bar{c}_{i,j}]_{0\le i,j\le p^n-1}$ *over* $\mathbb{Z}/p^n\mathbb{Z}$ *that correspond to prime ideals* $Q\in\mathcal{P}_{2n}$ (*see Definition 2 and Propositions 9 and 9'*). *For each matrix* $\bar{\alpha}=[\bar{c}_{i,j}]_{0\le i,j\le p^n-1}$ *over* $\mathbb{Z}/p^n\mathbb{Z}$, *define* $\mu(\bar{\alpha})$ *as the greatest power of* p, *less than or equal to* p^n, *that divides* $\sum_{k=1}^{p^n-1}\sum_{l=1}^{p^n-1}k\omega^{-r}(l)\bar{c}_{k,l}$. *Then* $X_n\subseteq Y_n$ *and* $p^{l_n}=\min\{\mu(\bar{\alpha}):\bar{\alpha}\in X_n\}$.

Proof. The proof is immediate from formula (15), Definition 2, and Proposition 9. □

3. On Vandiver's Conjecture

As before, let r be an even integer such that $2\le r\le p-3$. In this section we investigate whether or not $|e_r(A)|=|e_r(W)|$ is trivial. We preserve the notation of the previous sections but now we need only consider the case $n=1$. In fact, if $\beta=\beta_r=\prod_{k=1}^{p-1}(1-\zeta_p^k)^{k^{p-1-r}}$ then, by the results mentioned at the beginning of Section 1, we have that p divides $|e_r(A)|$ if and only if β_r is a pth power in $\mathbb{Z}[\zeta_p]$; that is, if and only if $p^l=p^{l_1}>1$. So take $n=1$ and let m be an integer ≥ 1.

Recall that (for $n=1$) $\mathcal{P}$ is the set of all prime ideals of $\mathbb{Z}[\zeta_p]$ above rational primes $q\equiv 1 \bmod p$, and $\mathcal{P}_m$ is the set of all prime ideals Q of $\mathbb{Z}[\zeta_p]$ that are above rational primes $q\equiv 1 \bmod p^m$ such that $p^{(q-1)/p}\equiv\zeta_p \bmod Q$. For every $Q\in\mathcal{P}$ above the rational prime q, choose a primitive root $s=s_Q$ modulo q such that $s^{(q-1)/p}\equiv\zeta_p \bmod Q$ and define $i(Q)$ as in (1). Define also the Gaussian periods of degree p of $\mathbb{Q}(\zeta_q)$ and the integers $a_{i,j}$ by

$$\eta_i=\sum_{j=0}^{(q-1)/p-1}\zeta_q^{s^{i+jp}} \tag{16}$$

for $0\le i\le p-1$; $\eta_{i+jp}=\eta_i$ for $0\le i\le p-1$ and $j\in\mathbb{Z}$;

$$\eta_0\eta_i=\sum_{j=0}^{p-1}a_{i,j}\eta_j \tag{17}$$

for $0\le i\le p-1$; and $a_{i+kp,j+lp}=a_{i,j}$ for $0\le i,j\le p-1$ and $k,l\in\mathbb{Z}$. By Proposition 2 and formula (15), we have

$$i(Q)\equiv\sum_{k=1}^{p-1}\sum_{l=1}^{p-1}kl^{p-1-r}\eta_k\eta_{k-l}\equiv\sum_{k=1}^{p-1}\sum_{l=1}^{p-1}kl^{p-1-r}a_{k,l} \bmod p. \tag{18}$$

These are Kummer's formulas (see [3, p. 100]).

The following propositions give important information about the indices $i(Q)$ modulo p. Proposition 11 is a particular case of [7, Cor. 3 of Thm. 2]. Recall that if $p^l > 1$ then p divides the Bernoulli number B_r.

PROPOSITION 10. *Let $Q \in \mathcal{P}$, and let a be an integer not divisible by p. Let $\sigma_a \in \Delta$ be the automorphism such that $\sigma_a(\zeta_p) = \zeta_p^a$. Then $i(\sigma_a(Q)) \equiv a^{p-r} i(Q)$ mod p.*

Proof. Call $\sigma = \sigma_a$. Let q be the rational prime below Q. Let s_Q and $s_{\sigma(Q)}$ be primitive roots modulo q such that $s_Q^{(q-1)/p} \equiv \zeta_p \bmod Q$ and $s_{\sigma(Q)}^{(q-1)/p} \equiv \zeta_p \bmod \sigma(Q)$. Since $s_Q^{(q-1)/p} \equiv \zeta_p^a \bmod \sigma(Q)$ we have $s_{\sigma(Q)}^a \equiv s_Q t_1^p \bmod q$ for some $t_1 \in \mathbb{Z}$. On the other hand, $\beta_r \equiv s_Q^{i(Q)} \bmod Q$ and $\beta_r \equiv s_{\sigma(Q)}^{i(\sigma(Q))} \bmod \sigma(Q)$. So $\sigma(\beta_r) \equiv s_Q^{i(Q)} \bmod \sigma(Q)$ and, since $\sigma(\beta_r) = \beta_r^{a^r} \alpha^p$ for some $\alpha \in \mathbb{Z}[\zeta_p]$, we have $s_Q^{a^{r-1} i(\sigma(Q)) + t_2 p} \equiv s_{\sigma(Q)}^{a^r i(\sigma(Q))} \equiv s_Q^{i(Q) + t_3 p} \bmod q$ for some $t_2, t_3 \in \mathbb{Z}$. Therefore $a^{r-1} i(\sigma(Q)) \equiv i(Q) \bmod p$. □

PROPOSITION 11. *Let Q_1, Q_2, and Q_3 be prime ideals in $\mathcal{P}$. Suppose that $p \mid B_r$. Then: If Q_1 is a principal ideal, $i(Q_1) \equiv 0$ mod p. If Q_1 and Q_2 are in the same ideal class, $i(Q_1) \equiv i(Q_2)$ mod p. If Q_3 is in the ideal class of $Q_1 Q_2$, $i(Q_3) \equiv i(Q_1) + i(Q_2)$ mod p.*

We intend to use Theorems 2 and 3 to obtain information about p^l. One pleasant fact about working with $n = 1$ is that now $\mathcal{R}_n = \mathbb{F}_{p^p}$, the field with p^p elements, that we call $\mathbb{F}$ from now on. The field $\mathbb{F}$ has a canonical (up to a cyclic permutation) normal basis with nice properties, as we shall show.

Let $\epsilon \in \mathbb{F}$ be a fixed root of the polynomial $x^p + x^{p-1} - 1$ and let $\alpha = \epsilon^{-1}$. For $0 \le i \le p-1$ define $\epsilon_i = \epsilon^{p^i}$, and for $0 \le i \le p-1$ and $j \in \mathbb{Z}$ define $\epsilon_{i+jp} = \epsilon_i$. By the Artin–Schreier theorem we have that $\mathbb{F} = \mathbb{F}_p(\alpha) = \mathbb{F}_p(\epsilon)$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Recall that now we use the following version of Kronecker's delta:

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i \equiv j \bmod p, \\ 0 & \text{if } i \not\equiv j \bmod p. \end{cases}$$

PROPOSITION 12. *The set $\{\epsilon_0, \epsilon_1, \ldots, \epsilon_{p-1}\}$ is a normal basis of $\mathbb{F}/\mathbb{F}_p$. Moreover, we have*

(i) $\sum_{k=0}^{p-1} \epsilon_k = -1$ *and*
(ii) $\sum_{k=0}^{p-1} \epsilon_{k+i} \epsilon_{k+j} = \delta_{i,j}$ *for all $i, j \in \mathbb{Z}$.*

Proof. Clearly the first affirmation is a consequence of (ii). Since $\epsilon_0, \epsilon_1, \ldots, \epsilon_{p-1}$ are the roots of $x^p + x^{p-1} - 1$ we have (i). To prove (ii), observe first that $\alpha^p - \alpha - 1 = 0$, so

$$\alpha^{2p} + \alpha^2 + 1 - 2\alpha^{p+1} - 2\alpha^p + 2\alpha = 0 \quad \text{and} \quad (\alpha^2)^p - 2(\alpha^2)^{(p+1)/2} + \alpha^2 - 1 = 0.$$

Therefore, since the conjugates of α^2 are $\alpha^2, (\alpha+1)^2, \ldots, (\alpha+p-1)^2$, and since these are distinct elements, we have

$$x^p - 2x^{(p+1)/2} + x - 1 = (x - \alpha^2)(x - (\alpha+1)^2) \cdots (x - (\alpha+p-1)^2).$$

Hence, for all $i\in\mathbb{Z}$,

$$(x+i^2)^p-2(x+i^2)^{(p+1)/2}+x+i^2-1$$
$$=(x-(\alpha^2-i^2))(x-((\alpha+1)^2-i^2))\cdots(x-((\alpha+p-1)^2-i^2)).$$

Taking logarithmic derivatives of both sides of the preceding equality and substituting $x=0$, we get

$$\frac{i^{p-1}-1}{i^{2p}-2i^{p+1}+i^2-1}=\sum_{k=0}^{p-1}\frac{1}{(\alpha+k-i)(\alpha+k+i)}=\sum_{k=0}^{p-1}\epsilon_{k-i}\epsilon_{k+i}.$$

Property (ii) follows from this equality. □

Now we show properties of the coordinates of certain special elements of $\mathbb{F}$ with respect to the basis $\{\epsilon_0,\epsilon_1,\ldots,\epsilon_{p-1}\}$ (see Proposition 8).

PROPOSITION 13. *Let* $\bar\theta_i$, $i\in\mathbb{Z}$, *be elements of* $\mathbb{F}$ *such that:*

(a) $\bar\theta_i^p=\bar\theta_{i+1}$ (*so, in particular,* $\bar\theta_{i+p}=\bar\theta_i$);
(b) $\sum_{k=0}^{p-1}\bar\theta_k=-1$; *and*
(c) $\sum_{k=0}^{p-1}\bar\theta_k\bar\theta_{k+i}=\delta_{0,i}$ *for all* $i\in\mathbb{Z}$.

Write

(d) $\bar\theta_0=\sum_{k=0}^{p-1}d_k\epsilon_k$ *with* $d_k\in\mathbb{F}_p$,

and define $d_{i+jp}=d_i$ *for* $0\le i\le p-1$ *and* $j\in\mathbb{Z}$. *Then:*

(i) $\sum_{k=0}^{p-1}d_k=1$;
(ii) $\sum_{k=0}^{p-1}d_{k+i}d_{k+j}=\delta_{i,j}$ *for all* $i,j\in\mathbb{Z}$; *and*
(iii) $\epsilon_j=\sum_{k=0}^{p-1}d_{j-k}\bar\theta_k$ *for* $0\le j\le p-1$.

Proof. (i) Take traces (from $\mathbb{F}$ to $\mathbb{F}_p$) of both sides of equality (d).

(ii) By (a) and (d) we have $\bar\theta_{-i}=\sum_{k=0}^{p-1}d_{k+i}\epsilon_k$, so

$$\bar\theta_{-i}\bar\theta_{-j}=\sum_{k=0}^{p-1}\sum_{l=0}^{p-1}d_{k+i}d_{l+j}\epsilon_k\epsilon_l.$$

Taking traces, we get $\delta_{i,j}=\sum_{k=0}^{p-1}\sum_{l=0}^{p-1}d_{k+i}d_{l+j}\delta_{k,l}=\sum_{k=0}^{p-1}d_{k+i}d_{k+j}$.

(iii) By (ii), the circulatory matrix $D=[d_{j-i}]_{i,j}$, $0\le i,j\le p-1$, is such that $DD^t=I$; that is, $D^{-1}=[d_{i-j}]_{i,j}$. Equality (iii) follows immediately. □

Given $Q\in\mathcal{P}_m$ above the rational prime q, we have $s^{(q-1)/p}\equiv\zeta_q\equiv p^{(q-1)/p}$ mod Q. So $s\equiv pt^p$ mod q for some $t\in\mathbb{Z}$, and we can write formula (16) in the form

$$\eta_i=\sum_{x\in S}\zeta_q^{xp^i},\quad\text{where } S=\{x^p: x\in(\mathbb{Z}/q\mathbb{Z})^\times\},\tag{19}$$

for $i\ge 0$. Therefore

$$\eta_i^p\equiv\eta_{i+1}\bmod p\tag{20}$$

for $i\in\mathbb{Z}$. This implies that p is inert in $\mathbb{Q}(\eta_0)$. It is easy to verify that the number $\eta_0+2\eta_1+\cdots+(p-1)\eta_{p-2}$ is a root modulo p of the polynomial

$x^p - x - 1$. We identify $\mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p-1}]/p\mathbb{Z}[\eta_0, \eta_1, \ldots, \eta_{p-1}]$ with $\mathbb{F}$ by identifying $\eta_0 + 2\eta_1 + \cdots + (p-1)\eta_{p-2}$ modulo p with α. Call $\bar{\eta}_i$ the congruence class of η_i in $\mathbb{F}$. Since $\epsilon = \alpha^{-1} = \alpha^{p-1} - 1$, we have

$$\epsilon = \frac{1}{\bar{\eta}_0 + 2\bar{\eta}_1 + \cdots + (p-1)\bar{\eta}_{p-2}} = (\bar{\eta}_0 + 2\bar{\eta}_1 + \cdots + (p-1)\bar{\eta}_{p-2})^{p-1} - 1. \quad (21)$$

With this identification, we can associate with each $Q \in \mathcal{P}_m$, in a unique way, a vector $(u_0, u_1, \ldots, u_{p-1}) = (u_0(Q), u_1(Q), \ldots, u_{p-1}(Q)) \in (\mathbb{F}_p)^p$, the coordinate vector of $\bar{\eta}_0$ with respect to the basis $\{\epsilon_0, \epsilon_1, \ldots, \epsilon_{p-1}\}$ of $\mathbb{F}/\mathbb{F}_p$. That is,

$$\bar{\eta}_0 = \sum_{i=0}^{p-1} u_i \epsilon_i. \quad (22)$$

DEFINITION 3. Let $u_0, u_1, \ldots, u_{p-1} \in \mathbb{F}_p$. We say that $(u_0, u_1, \ldots, u_{p-1})$ corresponds to a prime ideal $Q \in \mathcal{P}_m$ above the rational prime q if equality (22) holds, where the periods η_i are defined by (19) and $\bar{\eta}_i$ is the congruence class of η_i in $\mathbb{F}$. If $(u_0, u_1, \ldots, u_{p-1})$ corresponds to a prime ideal $Q \in \mathcal{P}_m$, we define $u_{i+jp} = u_i$ for $0 \le i \le p-1$ and $j \in \mathbb{Z}$.

If $(u_0, u_1, \ldots, u_{p-1}) \in (\mathbb{F}_p)^p$ corresponds to a prime ideal $Q \in \mathcal{P}_2$, then by Propositions 8 and 13 (with $\bar{\eta}_i$ as in Definition 3 and $\bar{\theta}_i = \bar{\eta}_i$) we have that

$$\begin{aligned} &\sum_{k=0}^{p-1} u_k = 1, \\ &\sum_{k=0}^{p-1} u_{k+i} u_{k+j} = \delta_{i,j} \quad \text{for all } i, j \in \mathbb{Z}, \quad \text{and} \\ &\epsilon_j = \sum_{k=0}^{p-1} u_{j-k} \bar{\eta}_k \quad \text{for } 0 \le j \le p-1. \end{aligned} \quad (23)$$

From (21), (22), and Proposition 12, we obtain the following formula for the $u_i = u_i(Q)$, $0 \le i \le p-1$, when $Q \in \mathcal{P}_2$:

$$u_i = \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}\left(\frac{\bar{\eta}_{-i}}{\bar{\eta}_0 + 2\bar{\eta}_1 + \cdots + (p-1)\bar{\eta}_{p-2}}\right). \quad (24)$$

Now we study the multiplication table for the basis $\{\epsilon_0, \epsilon_1, \ldots, \epsilon_{p-1}\}$. Since $\alpha = \epsilon^{-1}$ satisfies $\alpha^p = \alpha + 1$, we have $\alpha^{p^k} = \alpha + k$ for $k \ge 0$ and therefore $k\epsilon^{p^{k+1}} = \epsilon - \epsilon^{p^k}$. This yields

$$\epsilon_0 \epsilon_k = \frac{1}{k}\epsilon_0 - \frac{1}{k}\epsilon_k \quad \text{for } 1 \le k \le p-1. \quad (25)$$

On the other hand, by Proposition 12 the trace $\epsilon + \epsilon^p + \cdots + \epsilon^{p^{p-1}} = -1$. Write $\epsilon^2 = x_0\epsilon_0 + x_1\epsilon_1 + \cdots + x_{p-1}\epsilon_{p-1}$ with $x_i \in \mathbb{F}_p$. Then by (25) we have

$$\begin{aligned} -\epsilon &= \epsilon(\epsilon + \epsilon^p + \cdots + \epsilon^{p^{p-1}}) \\ &= \left(x_0 + 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}\right)\epsilon + (x_1 - 1)\epsilon^p + \left(x_2 - \frac{1}{2}\right)\epsilon^{p^2} \\ &\quad + \cdots + \left(x_{p-1} - \frac{1}{p-1}\right)\epsilon^{p^{p-1}}; \end{aligned}$$

hence $x_0=-1$ and $x_i=1/i$ for $1\le i\le p-1$. Therefore

$$\epsilon_0^2=-\epsilon_0+\sum_{i=1}^{p-1}\frac{1}{i}\epsilon_i. \tag{26}$$

Formulas (25) and (26) give the multiplication table of $\epsilon_0,\epsilon_1,\ldots,\epsilon_{p-1}$. In matrix form, if

$$\mathfrak{M}=\begin{bmatrix} -1 & 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{p-1} \\ 1 & -1 & 0 & 0 & \cdots & 0 \\ \frac{1}{2} & 0 & -\frac{1}{2} & 0 & \cdots & 0 \\ \frac{1}{3} & 0 & 0 & -\frac{1}{3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{p-1} & 0 & 0 & 0 & \cdots & -\frac{1}{p-1} \end{bmatrix},$$

then

$$\epsilon_0\begin{bmatrix}\epsilon_0\\ \epsilon_1\\ \vdots\\ \epsilon_{p-1}\end{bmatrix}=\mathfrak{M}\begin{bmatrix}\epsilon_0\\ \epsilon_1\\ \vdots\\ \epsilon_{p-1}\end{bmatrix}. \tag{27}$$

Let $\bar\theta_i$ and d_i be as in Proposition 13. Then $\bar\theta_0=\sum_{i=0}^{p-1}d_i\epsilon_i$ and so

$$\bar\theta_k=\sum_{i=0}^{p-1}d_{i-k}\epsilon_i \quad \text{for } 0\le k\le p-1. \tag{28}$$

We want to find the multiplication table of the normal basis $\{\bar\theta_0,\bar\theta_1,\ldots,\bar\theta_{p-1}\}$ of $\mathbb{F}$ over $\mathbb{F}_p$. By (25), (26), and (28) we have

$$\begin{aligned}
\bar\theta_0\bar\theta_k&=\sum_{i=0}^{p-1}d_i\epsilon_i\sum_{j=0}^{p-1}d_{j-k}\epsilon_j\\
&=\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}d_id_{i+j-k}\epsilon_i\epsilon_{i+j}\\
&=\sum_{i=0}^{p-1}d_id_{i-k}(\epsilon_0^2)^{p^i}+\sum_{i=0}^{p-1}\sum_{j=1}^{p-1}d_id_{i+j-k}(\epsilon_0\epsilon_j)^{p^i}\\
&=\sum_{i=0}^{p-1}d_id_{i-k}\Big(-\epsilon_0+\sum_{l=1}^{p-1}\frac{1}{l}\epsilon_l\Big)^{p^i}+\sum_{i=0}^{p-1}\sum_{j=1}^{p-1}d_id_{i+j-k}\Big(\frac{1}{j}\epsilon_0-\frac{1}{j}\epsilon_j\Big)^{p^i}\\
&=-\sum_{i=0}^{p-1}d_id_{i-k}\epsilon_i+\sum_{i=0}^{p-1}\sum_{l=1}^{p-1}d_id_{i-k}\frac{1}{l}\epsilon_{i+l}\\
&\quad+\sum_{i=0}^{p-1}\sum_{j=1}^{p-1}d_id_{i+j-k}\frac{1}{j}\epsilon_i-\sum_{i=0}^{p-1}\sum_{j=1}^{p-1}d_id_{i+j-k}\frac{1}{j}\epsilon_{i+j}\\
&=\sum_{i=0}^{p-1}\Big[-d_id_{i-k}+\sum_{j=1}^{p-1}\frac{1}{j}(d_{i-j}d_{i-j-k}+d_id_{i+j-k}-d_{i-j}d_{i-k})\Big]\epsilon_i.
\end{aligned}$$

So, by Proposition 13 (iii) we have $\bar\theta_0\bar\theta_k=\sum_{l=0}^{p-1}c_{k,l}\bar\theta_l$, where

$$c_{k,l}=\sum_{i=0}^{p-1} d_{i-l}\left[-d_i d_{i-k}+\sum_{j=1}^{p-1}\frac{1}{j}(d_{i-j}d_{i-j-k}+d_i d_{i+j-k}-d_{i-j}d_{i-k})\right]$$
$$=-\sum_{i=0}^{p-1} d_i d_{i-k}d_{i-l}$$
$$+\sum_{j=1}^{p-1}\frac{1}{j}\sum_{i=0}^{p-1}(d_{i-j}d_{i-j-k}d_{i-l}+d_i d_{i+j-k}d_{i-l}-d_{i-j}d_{i-k}d_{i-l}).$$

Therefore $\bar\theta_0\bar\theta_k=\sum_{l=0}^{p-1}c_{k,l}\bar\theta_l$ for $0\le k\le p-1$, where

$$c_{k,l}=-\sum_{i=0}^{p-1} d_i d_{i-k}d_{i-l}$$
$$+\sum_{j=1}^{p-1}\frac{1}{j}\sum_{i=0}^{p-1}(d_i d_{i-k}d_{i+j-l}+d_i d_{i+j-k}d_{i-l}-d_i d_{i+j-k}d_{i+j-l}). \tag{29}$$

Call $D_{k,l}=\sum_{i=0}^{p-1} d_i d_{i-k}d_{i-l}$. By (29), we have

$$\sum_{l=0}^{p-1} lc_{k,l}=-\sum_{l=0}^{p-1} lD_{k,l}+\sum_{j=1}^{p-1}\frac{1}{j}\sum_{l=0}^{p-1} lD_{k,l-j}$$
$$+\sum_{j=1}^{p-1}\frac{1}{j}\sum_{l=0}^{p-1} lD_{k-j,l}-\sum_{j=1}^{p-1}\frac{1}{j}\sum_{l=0}^{p-1} lD_{k-j,l-j}$$
$$=-\sum_{l=0}^{p-1} lD_{k,l}+\sum_{j=1}^{p-1}\frac{1}{j}\sum_{l=0}^{p-1}(l+j)D_{k,l}$$
$$+\sum_{j=1}^{p-1}\frac{1}{j}\sum_{l=0}^{p-1} lD_{k-j,l}-\sum_{j=1}^{p-1}\frac{1}{j}\sum_{l=0}^{p-1}(l+j)D_{k-j,l}$$
$$=-\sum_{l=0}^{p-1} lD_{k,l}+\sum_{j=1}^{p-1}\frac{1}{j}\sum_{l=0}^{p-1} lD_{k,l}+\sum_{j=1}^{p-1}\sum_{l=0}^{p-1} D_{k,l}$$
$$+\sum_{j=1}^{p-1}\frac{1}{j}\sum_{l=0}^{p-1} lD_{k-j,l}-\sum_{j=1}^{p-1}\frac{1}{j}\sum_{l=0}^{p-1} lD_{k-j,l}-\sum_{j=1}^{p-1}\sum_{l=0}^{p-1} D_{k-j,l}$$
$$=-\sum_{l=0}^{p-1} lD_{k,l}-\delta_{k,0}-\sum_{j=1}^{p-1}\delta_{k,j}=-\sum_{l=0}^{p-1} lD_{k,l}-1$$
$$=-\sum_{i=0}^{p-1} d_i d_{i-k}\sum_{l=0}^{p-1} ld_{i-l}-1=\sum_{i=0}^{p-1} d_i d_{i-k}\sum_{l=0}^{p-1}(l-i)d_l-1$$
$$=-\sum_{i=0}^{p-1} id_i d_{i-k}+\delta_{0,k}\sum_{l=0}^{p-1} ld_l-1.$$

In particular, if $(u_0,u_1,\ldots,u_{p-1})\in(\mathbb{F}_p)^p$ corresponds to a prime ideal $Q\in\mathcal{P}_2$ above the rational prime q, and if η_i and $a_{i,j}$ are as in (19) and (17), then

$$a_{k,l}\equiv-\sum_{i=0}^{p-1} u_i u_{i-k}u_{i-l}$$
$$+\sum_{j=1}^{p-1}\frac{1}{j}\sum_{i=0}^{p-1}(u_i u_{i-k}u_{i+j-l}+u_i u_{i+j-k}u_{i-l}-u_i u_{i+j-k}u_{i+j-l}) \tag{30}$$

mod p for $0 \le k, l \le p-1$, and

$$\sum_{l=0}^{p-1} la_{l,k} \equiv -\sum_{i=0}^{p-1} iu_i u_{i-k} + \delta_{0,k} \sum_{l=0}^{p-1} lu_l - 1 \bmod p \quad \text{for } 0 \le k \le p-1. \tag{31}$$

From formulas (18) and (31) we obtain

$$i(Q) \equiv -\sum_{l=1}^{p-1} \left(\sum_{i=1}^{p-1} iu_i u_{i-l} \right) l^{p-1-r} \bmod p. \tag{32}$$

We summarize some of these results and their relation to our study of $|e_r(A)|$ in the next theorem.

THEOREM 4. *Suppose that* $(u_0, u_1, \ldots, u_{p-1}) \in (\mathbb{F}_p)^p$ *corresponds to a prime ideal* $Q \in \mathcal{P}_2$ *above the rational prime* q *(see Definition 3). Then the elements* u_i *satisfy* $\sum_{k=0}^{p-1} u_k = 1$ *and* $\sum_{k=0}^{p-1} u_k u_{k+i} = \delta_{0,i}$ *for* $0 \le i \le p-1$. *With the Gaussian periods* η_i *defined by* (19) *and the integers* $a_{i,j}$ *defined by* (17), *we have*

$$a_{k,l} \equiv -\sum_{i=0}^{p-1} u_i u_{i-k} u_{i-l} + \sum_{j=1}^{p-1} \frac{1}{j} \sum_{i=0}^{p-1} (u_i u_{i-k} u_{i+j-l} + u_i u_{i+j-k} u_{i-l} - u_i u_{i+j-k} u_{i+j-l})$$

mod p *for* $0 \le k, l \le p-1$, *and*

$$i(Q) \equiv \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} kl^{p-1-r} a_{k,l} \equiv -\sum_{l=1}^{p-1} \left(\sum_{i=1}^{p-1} iu_i u_{i-l} \right) l^{p-1-r} \bmod p,$$

where $i(Q) = i_r(Q)$ *is defined by* (1) *for a primitive root* s *modulo* q *such that* $p \equiv st^p \bmod q$ *for some* $t \in \mathbb{Z}$.

Let $m \ge 2$. *If* $p \mid i(Q)$ *for all* $Q \in \mathcal{P}_m$ *then the component* $e_r(A)$ *of the* p*-Sylow subgroup* A *of the ideal class group of* $\mathbb{Q}(\zeta_p)$ *is nontrivial. Furthermore (by Proposition 11), if* p *divides the Bernoulli number* B_r *and* $p \mid i(Q)$ *for an arbitrarily chosen prime ideal* $Q \in \mathcal{P}_m$ *in each ideal class of* A, *then* $e_r(A)$ *is nontrivial. If* $p \nmid B_r$ *or* $p \nmid i(Q)$ *for some* $Q \in \mathcal{P}_2$ *(or* $Q \in \mathcal{P}$*), then* $e_r(A)$ *is trivial.*

OBSERVATIONS. (1) The value of Theorem 4, and of the other theorems in this section, relies on our ability to recognize whether or not a given $(u_0, u_1, \ldots, u_{p-1}) \in (\mathbb{F}_p)^p$, with $\sum_{k=0}^{p-1} u_k = 1$ and $\sum_{k=0}^{p-1} u_k u_{k+i} = \delta_{0,i}$, corresponds to a prime ideal $Q \in \mathcal{P}_2$. To enable such recognition we can use Propositions 8, 9, and 9′, together with the following fact (a consequence of formulas (28) and (29), Proposition 7, and Definition 3): Let $\bar{\theta}_k = \sum_{i=0}^{p-1} u_{i-k} \epsilon_i$, $0 \le k \le p-1$, and let

$$\bar{c}_{k,l} = -\sum_{i=0}^{p-1} u_i u_{i-k} u_{i-l} + \sum_{j=1}^{p-1} \frac{1}{j} \sum_{i=0}^{p-1} (u_i u_{i-k} u_{i+j-l} + u_i u_{i+j-k} u_{i-l} - u_i u_{i+j-k} u_{i+j-l})$$

for $0 \le k, l \le p-1$. Then $(u_0, u_1, \ldots, u_{p-1})$ corresponds to a prime ideal $Q \in \mathcal{P}_2$ if and only if $(\bar{\theta}_0, \bar{\theta}_1, \ldots, \bar{\theta}_{p-1})$ corresponds to Q; that is, if and only if $[\bar{c}_{i,j}]_{0 \le i,j \le p-1}$ corresponds to Q. See Definitions 1 and 2.

(2) We can strengthen Theorem 4 as follows: If $p \mid B_r$ and $p \mid i(Q)$ for an arbitrarily chosen prime ideal $Q \in \mathcal{P}_m$ in each ideal class from a set of classes that generate $e_{p-r}(A)$, then $e_r(A)$ is nontrivial. In fact, by Proposition 11, the function $i: \mathcal{P} \to \mathbb{Z}/p\mathbb{Z}$, defined by $i: Q \mapsto i(Q) \bmod p$, is then a class function that induces a homomorphism I: {ideal class group of $\mathbb{Q}(\zeta_p)$} $\to \mathbb{Z}/p\mathbb{Z}$. This homomorphism is trivial on ideal classes of order nondivisible by p and on ideal classes in $e_k(A)$ for $1 \le k \le p-1$, $k \ne p-r$, as follows easily from Proposition 10. If I is also trivial on a set of generators of $e_{p-r}(A)$, then I is the zero function; that is, $i(Q) \equiv 0 \bmod p$ for all $Q \in \mathcal{P}$. Therefore $e_r(A)$ is nontrivial.

Theorem 4 and formula (31) motivate the study of the numbers $\sum_{i=0}^{p-1} i u_i u_{i-k}$, $0 \le k \le p-1$, where $(u_0, u_1, \ldots, u_{p-1}) \in (\mathbb{F}_p)^p$ corresponds to some prime ideal $Q \in \mathcal{P}_2$. It turns out that these numbers have interesting properties based on the relations $\sum_{k=0}^{p-1} u_k = 1$ and $\sum_{k=0}^{p-1} u_k u_{k+i} = \delta_{0,i}$ for $0 \le i \le p-1$. In particular we obtained the following result, which will prove to be useful in our study of $|e_r(A)|$.

PROPOSITION 14. *Let $\mathcal{G}$ be the group of all $p \times p$ circulatory orthogonal matrices (i.e., matrices $M = [d_{j-i}]_{i,j}$ such that $MM^t = I$), with entries in $\mathbb{F}_p$, that we represent by their first rows $(d_0, d_1, \ldots, d_{p-1})$. Equivalently, let $\mathcal{G}$ be the group of all vectors $(d_0, d_1, \ldots, d_{p-1}) \in (\mathbb{F}_p)^p$ such that $\sum_{k=0}^{p-1} d_k d_{k+i} = \delta_{0,i}$ for $0 \le i \le p-1$, where we define $d_{i+jp} = d_i$ (for $0 \le i \le p-1$ and $j \in \mathbb{Z}$), with the operation $(d_0, d_1, \ldots, d_{p-1}) * (d'_0, d'_1, \ldots, d'_{p-1}) = (d''_0, d''_1, \ldots, d''_{p-1})$, where $d''_l = \sum_{i=0}^{p-1} d_i d'_{l-i}$. Then the map $f: \mathcal{G} \to (\mathbb{F}_p)^p$ defined by $f(d_0, d_1, \ldots, d_{p-1}) = (d'_0, d'_1, \ldots, d'_{p-1})$, where $d'_l = \sum_{i=0}^{p-1} i d_i d_{i-l} - \delta_{0,l} \sum_{j=0}^{p-1} j d_j$ for $0 \le l \le p-1$, is a homomorphism.*

The elements $\sum_{i=0}^{p-1} i d_i d_{i-k} - \delta_{0,k} \sum_{j=0}^{p-1} j d_j \in \mathbb{F}_p$, $0 \le k \le p-1$, are invariant by cyclic permutations of $d_0, d_1, \ldots, d_{p-1}$, and we have $\sum_{i=0}^{p-1} i d_i d_{i-k} = \sum_{i=0}^{p-1} i d_i d_{i+k}$ for $0 \le k \le p-1$.

Let $\mathcal{G}_1$ be the subgroup of $\mathcal{G}$ of matrices of determinant 1. Equivalently, let $\mathcal{G}_1$ be the subgroup of $\mathcal{G}$ formed by the elements $(d_0, d_1, \ldots, d_{p-1})$ such that $\sum_{k=0}^{p-1} d_k = 1$. Then $\mathcal{G} \cong \mathcal{G}_1 \oplus (-I)\mathcal{G}_1$.

Proof. Let $(d_0, d_1, \ldots, d_{p-1}), (d'_0, d'_1, \ldots, d'_{p-1}) \in \mathcal{G}$ and let $d''_l = \sum_{i=0}^{p-1} d_i d'_{l-i}$ for $0 \le l \le p-1$. Then

$$\sum_{k=0}^{p-1} k d''_k d''_{k-l} = \sum_{i=0}^{p-1} d_i \sum_{j=0}^{p-1} d_j \sum_{k=0}^{p-1} k d'_{k-i} d'_{k-l-j}$$

$$= \sum_{i=0}^{p-1} d_i \sum_{j=0}^{p-1} d_j \sum_{k=0}^{p-1} (i+k) d'_k d'_{k+i-l-j}$$

$$= \sum_{i=0}^{p-1} d_i \sum_{j=0}^{p-1} d_j \left[i\left(\sum_{k=0}^{p-1} d'_k d'_{k+i-l-j} \right) + \left(\sum_{k=0}^{p-1} k d'_k d'_{k+i-l-j} \right) \right]$$

$$= \sum_{i=0}^{p-1} i d_i \sum_{j=0}^{p-1} d_j \delta_{i-l,j} + \sum_{j=0}^{p-1} \left(\sum_{i=0}^{p-1} d_i d_{i+j} \right) \sum_{k=0}^{p-1} k d'_k d'_{k-l-j}$$

$$= \sum_{i=0}^{p-1} i d_i d_{i-l} + \sum_{j=0}^{p-1} \delta_{0,j} \sum_{k=0}^{p-1} k d'_k d'_{k-l-j}$$

$$= \sum_{k=0}^{p-1} k d_k d_{k-l} + \sum_{k=0}^{p-1} k d'_k d'_{k-l}.$$

This proves that f is a homomorphism.

We have $f(0,1,0,\ldots,0) = (0,0,\ldots,0)$. Since f is a homomorphism, this proves that the elements $\sum_{i=0}^{p-1} i d_i d_{i-k}$, $0 \le k \le p-1$, are invariant by cyclic permutations of the d_i. Also

$$\sum_{i=0}^{p-1} i d_i d_{i-k} = \sum_{i=0}^{p-1} (i+k) d_i d_{i+k} = \sum_{i=0}^{p-1} i d_i d_{i+k} + k \sum_{i=0}^{p-1} d_i d_{i+k} = \sum_{i=0}^{p-1} i d_i d_{i+k}$$

for $0 \le k \le p-1$.

Finally, note that if $M \in \mathcal{G}$ then $\det(M) = \pm 1$. Hence $\mathcal{G} \cong \mathcal{G}_1 \oplus (-I)\mathcal{G}_1$. Also, the determinant of a circulatory $p \times p$ matrix $M = [d_{j-i}]_{i,j}$ (subindices modulo p) over $\mathbb{F}_p$ is $\sum_{k=0}^{p-1} d_k$. So $M \in \mathcal{G}_1$ if and only if $M \in \mathcal{G}$ and $\sum_{k=0}^{p-1} d_k = 1$. □

The following nontrivial solution for the congruences $\sum_{k=0}^{p-1} d_k \equiv 1$ and $\sum_{k=0}^{p-1} d_k d_{k+i} \equiv \delta_{0,i} \bmod p$ $(0 \le i \le p-1)$ was shown to me by R. Kučera: $d_0 = 1$ and $d_i = i$ for $1 \le i \le p-1$. Kučera also calculated all the solutions for this system of congruences for $p = 5$ and $p = 7$, and a few solutions for $p = 11$. A study of the reason why Kučera's solution works leads to the following generalization.

PROPOSITION 15. *Let k be an odd number, $1 \le k \le (p-3)/2$ and $c \in \mathbb{Z}$. Then the system of congruences $\sum_{k=0}^{p-1} d_k \equiv 1$ mod p and $\sum_{k=0}^{p-1} d_k d_{k+i} \equiv \delta_{0,i}$ mod p (for $0 \le i \le p-1$) admits the solution $d_0 = 1$ and $d_i = (ci)^k$ for $1 \le i \le p-1$.*

Proof. With the values above we have $\sum_{i=0}^{p-1} d_i^2 = 1 + c^{2k} \sum_{i=1}^{p-1} i^{2k} \equiv 1 \bmod p$ and

$$\sum_{i=0}^{p-1} d_i d_{i+l} = (cl)^k - (cl)^k + \sum_{i=0}^{p-1} (ci)^k (c(i+l))^k$$

$$= c^{2k} \sum_{i=0}^{p-1} i^k (i+l)^k \equiv -\binom{k}{p-1-k} (cl)^{2k} = 0 \bmod p. \qquad \square$$

We now show a way to verify if the component $e_r(A)$ of the p-part of the ideal class group of $\mathbb{Q}(\zeta_p)$ is trivial for r even and $2 \le r \le (p-1)/2$.

THEOREM 5. *Let k be an odd number, $1 \le k \le (p-3)/2$, and let c be an integer nondivisible by p. Suppose that the vector $(u_0, u_1, \ldots, u_{p-1}) \in (\mathbb{F}_p)^p$, where $u_0 \equiv 1$ and $u_i \equiv (ci)^k \bmod p$ for $1 \le i \le p-1$ (or a cyclic permutation of this vector), corresponds to a prime ideal $Q \in \mathcal{P}_2$ (see Definition 3 and Proposition 15). Then the component $e_{k+1}(A)$ of the p-part of the ideal class group of $\mathbb{Q}(\zeta_p)$ is trivial.*

Proof. For $0 \le l \le p-1$ we have

$$\begin{aligned}\sum_{i=0}^{p-1} iu_i u_{i+l} &\equiv -lu_{-l} + c^{2k} \sum_{i=0}^{p-1} ii^k (i+l)^k \\ &= c^k l^{k+1} + c^{2k} \sum_{i=0}^{p-1} i^{k+1} \sum_{j=0}^{k} \binom{k}{j} i^j l^{k-j} \\ &\equiv c^k l^{k+1} - c^{2k} \binom{k}{p-2-k} l^{2k+1} = c^k l^{k+1} \bmod p.\end{aligned}$$

Therefore, by Theorem 4,

$$i(Q) = i_r(Q) \equiv -c^k \sum_{l=0}^{p-1} l^{k+1} l^{p-1-r} = -c^k \sum_{l=0}^{p-1} l^{p+k-r} \bmod p.$$

Hence $i_r(Q) \equiv c^k \not\equiv 0 \bmod p$ if $r = k+1$, and $i_r(Q) \equiv 0 \bmod p$ if $r \ne k+1$. In particular, by Theorem 4, $e_{k+1}(A)$ is trivial. □

We can use the idea of Hilbert's Theorem 90 to characterize the $p \times p$ circulatory orthogonal matrices of determinant 1 with entries in $\mathbb{F}_p$. Denote by $\mathcal{G}_1$ the group of all such matrices, as in Proposition 14.

PROPOSITION 16. *$M \in \mathcal{G}_1$ if and only if $M = B^t B^{-1}$ for some invertible circulatory matrix B.*

Proof. Let $M \in \mathcal{G}_1$. Then $B = I + M^t$ is invertible and circulatory, and $MB = B^t$. Conversely, if B is invertible and circulatory and $M = B^t B^{-1}$, then M is circulatory, $MM^t = I$, and $\det(M) = 1$. □

Let R be the $p \times p$ matrix $[\delta_{i+1,j}]_{i,j}$; that is,

$$R = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}. \tag{33}$$

The $p \times p$ circulatory matrices with entries in $\mathbb{F}_p$ are precisely the matrices $B = \sum_{k=0}^{p-1} b_k R^k$ with $b_k \in \mathbb{F}_p$. Note that for such a matrix B we have that $B^p = (b_0 + b_1 + \cdots + b_{p-1})I$, and so $B^{-1} = (b_0 + b_1 + \cdots + b_{p-1})^{-1} B^{p-1}$ if $b_0 + b_1 + \cdots + b_{p-1} \ne 0$.

If $B=R-aI$ where $a\in\mathbb{F}_p-\{0,1\}$, then

$$\begin{aligned}B^tB^{-1}&=(1-a)^{-1}(R^{p-1}-aI)(R-aI)^{p-1}\\&=(1+a)a^{p-2}I+(1+a)a^{p-3}R+\cdots\\&\quad+(1+a)aR^{p-3}+(1+a)R^{p-2}+R^{p-1}.\end{aligned}$$

Therefore, if

$$M_a=I+(1+a)a^{p-2}R+(1+a)a^{p-3}R^2+\cdots+(1+a)R^{p-1} \tag{34}$$

then $M_a\in\mathcal{G}_1$ for $a\in\mathbb{F}_p-\{0,1\}$.

PROPOSITION 17. *Let* $a\in\mathbb{F}-\{0,1,-1\}$, *let* M_a *be as in* (34), *and let* f: $\mathcal{G}\to(\mathbb{F}_p)^p$ *be the homomorphism defined in Proposition 14. Then*

$$f(M_a)=\left(\frac{1}{a-1}(a^{p-l}+a^l-\delta_{0,l}(a+1))\right)_{0\le l\le p-1}$$

Proof. Call $d_0=1$ and $d_i=(1+a)a^{p-1-i}$ for $1\le i\le p-1$. Then $f(M_a)=(d_0',\ldots,d_{p-1}')$ where, for $0\le l\le p-1$,

$$\begin{aligned}d_l'&=\sum_{i=0}^{p-1}id_id_{i-l}-\delta_{0,l}\sum_{j=0}^{p-1}jd_j\\&=\sum_{j=1}^{l-1}j(a+1)a^{p-1-j}(a+1)a^{l-1-j}+l(a+1)a^{p-1-l}\\&\quad+\sum_{j=1}^{p-1-l}(l+j)(a+1)a^{p-1-l-j}(a+1)a^{p-1-j}-\delta_{0,l}\frac{a+1}{a-1}\\&=(a+1)\left[(a+1)a^{l-1}\sum_{j=1}^{l-1}ja^{-2j}+la^{-l}+(a+1)a^l\sum_{j=l+1}^{p-1}ja^{-2j}\right]-\delta_{0,l}\frac{a+1}{a-1}\\&=(a+1)\left[(1-a^2)a^{l-1}\sum_{j=1}^{l-1}ja^{-2j}-la^{1-l}+(a+1)a^l\sum_{j=1}^{p-1}ja^{-2j}\right]-\delta_{0,l}\frac{a+1}{a-1}\\&=\frac{1}{a-1}(a^{1-l}+a^l)-\delta_{0,l}\frac{a+1}{a-1}.\end{aligned}$$

Here we have used the identity

$$X+2X^2+\cdots+(l-1)X^{l-1}=\frac{(X-1)lX^l-(X^{l+1}-X)}{(X-1)^2}.$$ □

If, in particular, the matrix M_a defined in (34) (or, better, if its first row) corresponds to a prime ideal $Q\in\mathcal{P}_2$, then the index $i(Q)$ is essentially a Mirimanoff polynomial in a, as is shown in the next theorem.

THEOREM 6. *Suppose that the vector* $(u_0,u_1,\ldots,u_{p-1})\in(\mathbb{F}_p)^p$ (*or a cyclic permutation of it*) *corresponds to a prime ideal* $Q\in\mathcal{P}_2$ (*see Definition 3*), *where, for some* $a\in\mathbb{F}_p-\{0,1\}$, $u_0=1$ *and* $u_i=(a+1)a^{p-1-i}$ *for* $1\le i\le p-1$. *Then*

$$i(Q) \equiv \frac{2}{1-a} \sum_{l=1}^{p-1} l^{p-1-r} a^l \bmod p.$$

Proof. By (32) and Proposition 17, if $a \in \mathbb{F}_p - \{0, 1, -1\}$ we have

$$\begin{aligned} i(Q) &\equiv -\sum_{l=1}^{p-1} l^{p-1-r} \sum_{i=1}^{p-1} i u_i u_{i-l} \\ &= -\sum_{l=1}^{p-1} l^{p-1-r} \frac{1}{a-1}(a^{p-l} + a^l) = \\ &= \frac{1}{1-a}\left(\sum_{l=1}^{p-1} l^{p-1-r} a^{p-l} + \sum_{l=1}^{p-1} l^{p-1-r} a^l\right) \\ &= \frac{2}{1-a} \sum_{l=1}^{p-1} l^{p-1-r} a^l \bmod p. \end{aligned}$$

The result is trivial if $a = -1$. □

By using the logarithmic derivative it can be shown that, for $a \in \mathbb{Z}$,

$$\sum_{l=1}^{p-1} l^{p-1-r} a^l \equiv 0 \bmod p$$

if and only if $\prod_{k=1}^{p-1} (\zeta_p^k - a)^{k^{r-1}} \equiv \alpha^p \bmod p$ for some $\alpha \in \mathbb{Q}(\zeta_p)$. This suggests that Theorem 6 can be generalized to give a criterion for the divisibility by p of the indices $i(Q)$, for all $Q \in \mathcal{P}_2$, in the form of an explicit reciprocity law. In order to obtain such a criterion we need the following proposition.

PROPOSITION 18. *Let R be as in* (33), *and let $d_0 I + d_1 R + \cdots + d_{p-1} R^{p-1}$ be in $\mathcal{G}_1$ (with $d_i \in \mathbb{F}_p$). Call $D(X) = \sum_{i=0}^{p-1} d_i X^i$. Then $XD'(X)/D(X) \equiv \sum_{l=0}^{p-1} (\sum_{i=0}^{p-1} i d_i d_{i-l}) X^l$ mod $X^p - 1$. That is,*

$$RD'(R)(D(R))^{-1} = \sum_{l=0}^{p-1} \left(\sum_{i=0}^{p-1} i d_i d_{i-l}\right) R^l.$$

Proof. Since $(D(R))^{-1} = D(R)^t = \sum_{j=0}^{p-1} d_{p-j} R^j$ (subindices modulo p), and since $X^p - 1$ is the minimal polynomial of R, we have that $(D(X))^{-1} \equiv \sum_{i=0}^{p-1} d_{p-i} X^i \bmod X^p - 1$. Therefore

$$\begin{aligned} \frac{XD'(X)}{D(X)} &\equiv \sum_{i=0}^{p-1} i d_i X^i \sum_{j=0}^{p-1} d_{p-j} X^j \\ &\equiv \sum_{l=0}^{p-1} \left(\sum_{i=0}^{p-1} i d_i d_{i-l}\right) X^l \bmod X^p - 1. \end{aligned}$$

□

Now we can prove the main result of this section, which must be combined with Theorem 4, Observation 1 (following Theorem 4), and Proposition 16.

THEOREM 7. *Let $B(X) = b_0 + b_1 X + \cdots + b_{p-1} X^{p-1} \in \mathbb{Z}[X]$ such that $B(1) \not\equiv 0$ mod p. Write $B(X^{-1})/B(X) \equiv \sum_{i=0}^{p-1} u_i X^i$ mod $(p, X^p - 1)$ with $u_i \in \mathbb{Z}$ (hence $\sum_{i=0}^{p-1} u_i R^i$ modulo p belongs to $\mathcal{G}_1$). Suppose that the vector*

$(u_0, u_1, \ldots, u_{p-1})$ modulo p corresponds to a prime ideal $Q \in \mathfrak{P}_2$ (see Definition 3). Then $i(Q) \equiv 0 \bmod p$ (i.e. $\prod_{k=1}^{p-1}(1-\zeta_p^k)^{k^{p-1-r}} \equiv \gamma^p \bmod Q$ for some $\gamma \in \mathbb{Q}(\zeta_p)$) if and only if $\prod_{k=1}^{p-1} B(\zeta_p^k)^{k^{r-1}} \equiv \alpha^p \bmod p$ for some $\alpha \in \mathbb{Q}(\zeta_p)$. This happens if and only if $\sum_{k=1}^{p-1} k^r \zeta_p^k B'(\zeta_p^k)/B(\zeta_p^k) \equiv 0 \bmod p$.

Proof. (We identify the integers u_i with their congruence classes modulo p.) Call $U(X) = \sum_{i=0}^{p-1} u_i X^i$. Since $R^{-1} = R^t$ we have, by Proposition 16, that $U(R) = B(R)^t/B(R) \in \mathfrak{S}_1$. So, by Proposition 18, we have $XU'(X)/U(X) \equiv \sum_{l=0}^{p-1}(\sum_{i=0}^{p-1} iu_i u_{i-l})X^l \bmod X^p-1$. On the other hand,

$$\begin{aligned}\frac{XU'(X)}{U(X)} &= \frac{X\frac{d}{dX}(B(X^{-1})/B(X))}{B(X^{-1})/B(X)} \\ &= \frac{X\frac{d}{dX}(B(X^{-1}))}{B(X^{-1})} - \frac{X\frac{d}{dX}(B(X))}{B(X)} \\ &= -X^{-1}\frac{B'(X^{-1})}{B(X^{-1})} - X\frac{B'(X)}{B(X)}.\end{aligned}$$

Therefore

$$\begin{aligned}-2\sum_{k=1}^{p-1} k^r X^k \frac{B'(X^k)}{B(X^k)} &\equiv -\sum_{k=1}^{p-1} k^r X^{-k}\frac{B'(X^{-k})}{B(X^{-k})} - \sum_{k=1}^{p-1} k^r X^k \frac{B'(X^k)}{B(X^k)} \\ &\equiv \sum_{k=1}^{p-1} k^r \frac{U'(X^k)}{U(X^k)} \equiv \sum_{k=1}^{p-1} k_r \sum_{l=0}^{p-1}\left(\sum_{i=0}^{p-1} iu_i u_{i-l}\right)X^{kl} \\ &\equiv \sum_{k=1}^{p-1} k^r X^k \sum_{l=0}^{p-1} l^{p-1-r} \sum_{i=0}^{p-1} iu_i u_{i-l} \bmod X^p-1.\end{aligned}$$

Hence, by (32),

$$2\sum_{k=1}^{p-1} k^r X^k \frac{B'(X^k)}{B(X^k)} \equiv i(Q)\sum_{k=1}^{p-1} k^r X^k \bmod (p, X^p-1). \tag{35}$$

Since $(\zeta_p-1)^{p-1-r} \| \sum_{k=1}^{p-1} k^r \zeta_p^k$, it follows from formula (35) that $i(Q) \equiv 0 \bmod p$ if and only if $\sum_{k=1}^{p-1} k^r \zeta_p^k (B'(\zeta_p^k)/B(\zeta_p^k)) \equiv 0 \bmod (\zeta_p-1)^{p-r}$, if and only if $\sum_{k=1}^{p-1} k^r \zeta_p^k (B'(\zeta_p^k)/B(\zeta_p^k)) \equiv 0 \bmod p$.

The fact that $\prod_{k=1}^{p-1} B(\zeta_p^k)^{k^{r-1}} \equiv \alpha^p \bmod p$ for some $\alpha \in \mathbb{Q}(\zeta_p)$ if and only if $\sum_{k=1}^{p-1} k^r \zeta_p^k (B'(\zeta_p^k)/B(\zeta_p^k)) \equiv 0 \bmod p$ can be easily proved by using the logarithmic derivative.

References

[1] E. Artin and J. Tate, *Class field theory,* Benjamin, New York, 1967.

[2] L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem. I,* Amer. J. Math. 57 (1935), 391–424.

[3] E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen,* J. Reine Angew. Math. 44 (1852), 93–146.

[4] S. Lang, *Cyclotomic fields I and II,* combined 2nd ed., Springer, New York, 1990.

[5] B. R. McDonald, *Finite rings with identity,* Dekker, New York, 1974.
[6] F. Thaine, *On the ideal class groups of real abelian number fields,* Ann. of Math (2) 128 (1988), 1–18.
[7] ———, *On the relation between units and Jacobi sums in prime cyclotomic fields,* Manuscripta Math. 73 (1991), 127–151.
[8] ———, *Properties that characterize Gaussian periods and cyclotomic numbers,* Proc. Amer. Math. Soc. (to appear).
[9] L. C. Washington, *Introduction to cyclotomic fields,* Graduate Texts in Math., Springer, New York, 1982.

Department of Mathematics
and Statistics - CICMA
Concordia University
Montreal, Quebec H3G 1M8
Canada