Il y avait un jardin qu'on appelait la terre,
Avec un lit de mousse pour y faire l'amour.
Non ce n'était pas le Paradis ni l'Enfer,
Ni rien de déjà vu ni déjà entendu:
Un jour, mon enfant, pour toi il florira... [1]

To Seraina and Theres

REFLECTION, BERNOULLI NUMBERS AND THE PROOF OF CATALAN'S CONJECTURE

PREDA MIHĂILESCU

Abstract. Catalan's conjecture states that the equation $x^p - y^q = 1$ has no other integer solutions but $3^2 - 2^3 = 1$. We prove a theorem which simplifies the proof of this conjecture.

1. Introduction

Let p, q be distinct odd primes with $p \not\equiv 1 \mod q$, $\zeta \in \mathbb{C}$ be a primitive $p-$th root of unity, $E' = \mathbb{Z}[\zeta + \overline{\zeta}]^\times$ be the real units of $\mathbb{Q}(\zeta)$ and E'_q, the subgroup of those units which are q - adic $q-$th powers (also called q - primary units). Let $G =$ Gal $(\mathbb{Q}(\zeta + \overline{\zeta})/\mathbb{Q})$ and $\mathbb{F}_q[G]$ be the group ring over the prime finite field with characteristic q and $\mathbf{N} = \mathbf{N}_{\mathbb{Q}(\zeta+\overline{\zeta})/\mathbb{Q}} \in \mathbb{Z}[G]$. The main theorem of this paper states:

Theorem 1. *Let $p > q$ be odd primes with $p \not\equiv 1 \mod q$. If $\mathcal{C}$ is the ideal class group of $\mathbb{Q}(\zeta + \overline{\zeta})$, $E' = \mathbb{Z}[\zeta + \overline{\zeta}]^\times$ and $A_q = \{x \in \mathcal{C} : x^q = 1\}$ and the module $\mathbf{T}$ is defined by*

$$\mathbf{T} = \text{supp}(E_q/E^q) \bigcup \text{supp}(A_q),$$

then $\mathbf{T} \neq \mathbb{F}_q[G]/(\mathbf{N})$.

The notion of *support*: supp($\mathbf{T}$), will defined below and the signification of various modules over the group ring will be given in detail. The module $\mathbf{T}$ introduced above has the following connection to the Catalan conjecture, which is proved in [Mi]:

[1]Free after Georges Moustaki

Theorem 2. *If p, q are distinct odd primes with $p \not\equiv 1 \mod q$, such that Catalan's equation*

$$x^p - y^q = 1$$

has a non-trivial solution in the integers, then, with the notation introduced above, $\mathbf{T} = (\mathbf{N})$.

Remark 1. *In* [Mi]*, the Theorem of Thaine and the assumption $p > q$ are used for the proof of $\mathbf{T} \neq (\mathbf{N})$. The new Theorem allows herewith to bypass the use of Thaine's Theorem but not the condition $p > q$.*

2. Cyclotomic fields and their group rings

The $n-$th cyclotomic extension is denoted, following [Ono], by $\mathbf{C}_n$ and its maximal real subfield is $\mathbf{C}_n^+$; thus $\mathbf{C}_p = \mathbb{Q}(\zeta)$, etc. The $n-$th cyclotomic polynomial is $\Phi_n(X) \in \mathbb{Z}[X]$. The Galois groups are $G_n = \text{ Gal }(\mathbf{C}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\cdot\mathbb{Z})^*$ and $G_n^+ = \text{ Gal }(\mathbf{C}_n^+/\mathbb{Q})$. For $c \in (\mathbb{Z}/n\cdot\mathbb{Z})^*$, we let σ_c be the automorphism of $\mathbb{Q}(\zeta_n)$ with $\zeta_n \longrightarrow \zeta_n^c$. If n, n' are coprime odd integers, then the fields $\mathbf{C}_n, \mathbf{C}_{n'}$ are *linear independent* [Ono] and $G_{n\cdot n'} = G_n \times G_{n'}$. An automorphism $\sigma \in G_n$ lifts to $G_{nn'}$ by fixing $\zeta_{n'}$. Complex multiplication is an automorphism $\jmath \subset G_n$ for all $n \in \mathbb{N}$.

2.1. **Group rings.** If $\mathbf{R}$ is a ring and $G = \text{ Gal }(\mathbb{K}/\mathbb{Q})$ a Galois group, the module $\mathbf{R}[G]$ is a free $\mathbf{R}$ - module generated by the elements of G and is called the **group ring** of G. For $|G| \in \mathbf{R}^\times$, the group ring is **separable**, and we require that this condition holds. We shall write $\mathbf{R}[G]' = \mathbf{R}[G]/\left(\mathbf{N}_{\mathbb{K}/\mathbb{Q}}\right)$ for the submodule obtained by modding out the ideal generated by the norm. If n is an odd prime power, $G = G_n$ is generated by $\varsigma \in G$ and $\varphi(n) \in \mathbf{R}^\times$, then the polynomial $X^{\varphi(n)} - 1$ is separable over $\mathbf{R}$ and $\varsigma \mapsto X \mod X^{\varphi(n)} - 1$ induces an isomorphism

$$\begin{aligned} \iota_n \quad &: \quad \mathbf{R}[X]/(X^{\varphi(n)} - 1) \to \mathbf{R}[G_n] \quad \text{with} \\ \mathbf{R}[G]' \quad &= \quad \iota_n \left(\mathbf{R}[X] / \left(\frac{X^{\varphi(n)} - 1}{X - 1} \right) \right). \end{aligned} \tag{1}$$

For $(n.n') = 1$, the isomorphism ι extends by multiplicativity. It is thus defined for all cyclotomic fields and we shall write ι, irrespective of the value of n and the ring $\mathbf{R}$.

The real group ring embeds in $\mathbf{R}[G]$ by $\mathbf{R}[G^+] \cong \frac{1+\jmath}{2} \cdot \mathbf{R}[G]$ and if $\mathbf{R}$ is a finite field of odd characteristic, then $\mathbf{R}[G^+] \cong (1+\jmath)\mathbf{R}[G]$. In the latter case we shall think of the real group ring in terms of the module on the right hand side of the isomorphism. Let $G^- = G/G^+$, the *minus part* of G; then $\mathbf{R}[G^-] \cong \frac{1-\jmath}{2} \cdot \mathbf{R}[G]$, etc. In particular, since $\varphi(n)$ is even, under the isomorphism ι we have:

$$\begin{aligned} \mathbf{R}[G^+] \quad &= \quad \iota_n \left(\mathbf{R}[X] / \left(X^{\varphi(n)/2} - 1 \right) \right), \\ \mathbf{R}[G^+]' \quad &= \quad \iota_n \left(\mathbf{R}[X] / \left(\frac{X^{\varphi(n)/2} - 1}{X - 1} \right) \right), \quad \text{and} \\ \mathbf{R}[G^-] \quad &= \quad \iota_n \left(\mathbf{R}[X] / \left(X^{\varphi(n)/2} + 1 \right) \right). \end{aligned} \tag{2}$$

2.2. **Characters, idempotents and irreducible modules.** The topics we expand next belong to representation theory, essentially Maschke's Theorem. We expose it in some detail, in order to keep a consistent notation.

Let $f \in \mathbb{N}_{>1}$ be a positive integer. A **Dirichlet character** ([Wa], Chapter 3) of conductor n is a multiplicative map $\psi : \mathbb{Z} \to \mathbb{C}$, such that $\psi(x) = \psi(y)$ if $x \equiv y \mod n$ and $\psi(x) = 0$ iff $(x, n) > 1$. The Dirichlet character is thus a multiplicative map $\chi : (\mathbb{Z}/f \cdot \mathbb{Z})^* \to \mathbb{C}$; if $n|n'$, one can regard the same character as a map $(\mathbb{Z}/n' \cdot \mathbb{Z})^* \to \mathbb{C}$ by composition with the natural projection $(\mathbb{Z}/n' \cdot \mathbb{Z})^* \to (\mathbb{Z}/n \cdot \mathbb{Z})^*$. The set of integers n' for which the same map is defined builds an ideal and it is convenient to choose the generator of this ideal as conductor. A character defined with respect to its minimal conductor - which is sometimes denoted [Wa] by n_χ is called **primitive**. We will only consider primitive characters. A character is **odd** if $\psi(-1) = -1$ and **even** if $\psi(-1) = 1$. Odd and even characters multiply like signs: odd times odd is even, etc. The *trivial* character is unique for all conductors and will be denoted by $\mathbf{1}$, so $\mathbf{1}(x) = 1$ for all $x \in \mathbb{Z}$. The isomorphism $G_n \cong (\mathbb{Z}/n \cdot \mathbb{Z})^*$ allows one to consider Dirichlet characters as characters of the Galois group $G_n = \text{Gal}\ (\mathbf{C}_n/\mathbb{Q})$. More precisely, let $H = (\mathbb{Z}/n \cdot \mathbb{Z})^* / \ker \psi \subset (\mathbb{Z}/n \cdot \mathbb{Z})^*$. Then there is a field $\mathbb{K}' \subset \mathbf{C}_n$ with Galois group isomorphic to H and ψ may be regarded as character of this field.

Let $G = \text{Gal}\ (\mathbb{K}/\mathbb{Q})$ as before and $\mathbf{R} = \mathbf{k}$ be a field and $\overline{\mathbf{k}}$ an algebraic closure. If $\mathbb{K} = \mathbf{C}_n$ is a cyclotomic field - the case we are interested in - then, due to the linear independence above mentioned, we may restrict ourselves to the case when n is a prime power; we shall also assume that n is odd. Furthermore, the polynomial $F(X) = X^{\varphi(n)} - 1$ should be separable over $\mathbf{k}$, so we require $(\text{char}(\mathbf{k}), \varphi(n)) = 1$. Let $\mathcal{F} \subset \mathbf{k}[X]$ be the set of irreducible factors of $X^{\varphi(n)} - 1$ over $\mathbf{k}$ and, naturally, $\mathcal{F}' = \mathbf{F} \setminus \{X - 1\}$; since $F(X)$ is separable, $F(X) = \prod_{f \in \mathcal{F}} f(X)$. We have the disjoint union $\mathcal{F} = \mathcal{F}^+ \cup \mathcal{F}^-$ induced by the rational polynomial factorization:

$$X^{\varphi(n)} - 1 = \left(X^{\varphi(n)/2} - 1\right) \cdot \left(X^{\varphi(n)/2} + 1\right).$$

The **primitive (Galois) characters** $\chi : G \to \overline{\mathbf{k}}$ are multiplicative maps which form a group G'. We shall make the dependence on $\mathbf{k}$ explicit by writing $G'(\mathbf{k})$, whenever the context requires it. The Galois characters $\chi \in G'(\mathbb{Q})$ can be identified to Dirichlet characters of conductor n via the convention

$$\chi(c) = \chi(\sigma_c) \quad \text{for } c \in (\mathbb{Z}/n \cdot \mathbb{Z})^*.$$

A simple and important property of sums of characters is the following:

Lemma 1. *Let G be an abelian Galois group and $H' \subset G'(\mathbf{k})$ a subgroup of the Galois characters. Then*

$$\sum_{\chi \in H'} \chi(x) = \begin{cases} 0 & \forall\ x \in \mathbb{Z} \ \setminus\ \ker(H'), \quad \textit{and} \\ |H'| & \forall\ x \in \ker(H'). \end{cases} \tag{3}$$

$$\sum_{x \in G} \chi(x) = \begin{cases} 0 & \forall\ \chi \in G',\ \chi \neq \mathbf{1}, \quad \textit{and} \\ |G| & \textit{if } \chi = \mathbf{1}. \end{cases} \tag{4}$$

Proof. Let $x \in \mathbb{Z}$ with $H'(x) \neq \{1\}$; then there is a $\chi' \in H'$ such that $\chi'(x) \neq 1$. Let $s(x) = \sum_{\chi \in K} \chi(x)$. Then

$$\begin{aligned}(\chi'(x)-1)\cdot s(x) &= \sum_{\chi \in H'} \chi(x) - \sum_{\chi \in H'} \chi'(x)\cdot\chi(x) \\ &= \sum_{\chi \in H'} \chi(x) - \sum_{\chi'' \in H'} \chi''(x) = 0.\end{aligned}$$

Since $(\chi'(x)-1) \neq 0$, it follows that $s(x) = 0$. For $x \in \ker(H')$ we have $\chi(x) = 1$ for all $\chi \in H'$ and obviously $s(x) = |H|$. The proof of (4) is similar. $\square$

Let $\mu \in \overline{\mathbf{k}}$ be a primitive $\varphi(n)-$th root of unity. Since G_n is cyclic, $\varsigma \in G$ is a generator, then $\chi(\varsigma) \in \overline{\mathbf{k}}$ determines all the values of χ by multiplicativity. Furthermore $\varsigma^{\varphi(n)} = 1$, so $(\chi(\varsigma))^{\varphi(n)} = 1$ and $\chi(\varsigma) \in <\mu>$ is an $\varphi(n)-$th root of unity.

The **orthogonal idempotents** [Lo] of G' over this field are:

$$1_\chi = \frac{1}{|G|}\cdot\sum_{\sigma\in G}\chi(\sigma)\cdot\sigma^{-1} \in \mathbf{k}(\mu)[G], \quad \forall\, \chi \in G'. \tag{5}$$

An easy computation shows that the idempotents verify:

$$\begin{array}{rcll} 1_{\chi_1}\times 1_{\chi_2} &=& \delta(\chi_1,\chi_2) & \forall \chi_1,\chi_2 \in G', \\ \sum_{\chi\in G'} 1_\chi &=& 1, & \\ \sigma\cdot 1_\chi &=& \chi(\sigma)\cdot 1_\chi, & \forall \sigma \in G, \chi \in G', \\ 1_\chi \times (\chi(\sigma_0)-\sigma_0) &=& 0 & \forall\, \sigma_0 \in G. \end{array} \tag{6}$$

Here $\delta(\chi_1,\chi_2) = 1$ if $\chi_1 = \chi_2$ and 0 otherwise. In general $1_\chi \notin \mathbf{k}[G]$, so they have merely an abstract meaning, but their actions may not be well defined. We need idempotents in $\mathbf{k}[G]$; let $S(\chi) = \text{ Gal } (\mathbf{k}(\chi(G))/\mathbf{k})$, where $\mathbf{k}(\chi(G))$ is the field obtained by adjoining all the values $\chi(x), x \in G$ to the base field $\mathbf{k}$. The action of $S(\chi)$ induces an equivalence relation on G' given by

$$\chi \sim \chi' \Leftrightarrow \exists\ s \in S(\chi)\ : \chi' = s(\chi).$$

We let $\mathfrak{X} \subset G'$ be a set of representants for the classes of $G'/\sim$. The $\mathbf{k}$ - *rational idempotents* are defined by taking traces:

$$\varepsilon_\chi = \frac{1}{|S(\chi)|}\cdot\sum_{s\in S(\chi)} 1_\chi \in \mathbf{k}[G], \quad \chi \in G'.$$

The isomorphism ι defined by (1) extends to the field $\mathbf{k}[\mu]$, by fixing this extension. Then $\iota(\chi(\varsigma)) = \chi(\varsigma) = \nu$ is a root of unity whose order is equal to the order of the character $\chi \in G'$. The annihilator $\chi(\varsigma) - \varsigma$ of 1_χ maps under the isomorphism defined in (1) to $\iota\,(\chi(\varsigma)-\varsigma) = X - \nu$. The group $S(\chi)$ acts on χ and on ν but not on ς, and thus

$$\iota\left(\prod_{s\in S(\chi)} (\varsigma - s(\chi(\varsigma)))\right) \equiv \prod_{s\in S(\chi)} (X - s(\nu)) \equiv f_\chi(X) \mod X^{\varphi(n)-1}.$$

Note that the polynomial $f_\chi \in \mathbf{k}[X]$ since it is invariant under the group $S(\chi)$ acting on ν. Furthermore it is an irreducible factor of $X^{\varphi(n)} - 1$, so $f_\chi \in \mathcal{F}$. We have thus a one-to-one map $\phi : \mathfrak{X} \to \mathcal{F}, \chi \mapsto f_\chi$. Since $f_{\chi(\varsigma)}$ annihilates $1_{\chi'}$ for all conjugate characters of χ, it follows that it annihilates ε_χ. Furthermore, since

$(\varsigma - \chi(\varsigma))|(\sigma_0 - \chi(\sigma_0))$ for any $\sigma_0 \in G$, it is also the minimal annihilator. We have thus the following properties for the $\mathbf{k}$ - rational idempotents:

$$\begin{array}{rcll} \varepsilon_{\chi_1} \times \varepsilon_{\chi_2} & = & \delta(\chi_1, \chi_2) & \forall \chi_1, \chi_2 \in G', \\ \sum_{\chi \in \mathfrak{X}} \varepsilon_\chi & = & 1, & \\ \sigma \cdot \varepsilon_\chi & = & \chi(\sigma) \cdot \varepsilon_\chi, & \forall \sigma \in G, \chi \in G', \\ \varepsilon_\chi \times f_\chi(\sigma_0) & = & 0 & \forall\ \sigma_0 \in G. \end{array} \tag{7}$$

Here, unlike (6), $\delta(\chi_1, \chi_2) = 1$ if $\chi_1 \sim \chi_2$ and 0 otherwise.

We define the **irreducible submodules of** $\mathbf{k}[G]$ by $M_\chi = \varepsilon_\chi \cdot \mathbf{k}[G],\ \chi \in \mathfrak{X}$. By the previous remarks, they have $f_\chi(\varsigma)$ as minimal annihilator and thus $M_\chi \cong \mathbf{k}[G]/\left(f_\chi(\varsigma)\mathbf{k}[G]\right)$ and they are in fact *fields* and:

$$\mathbf{k}[G] = \bigoplus_{\chi \in \mathfrak{X}} \varepsilon_\chi \cdot \mathbf{k}[G] = \bigoplus_{\chi \in \mathfrak{X}} M_\chi. \tag{8}$$

Let H be a finite multiplicative abelian group on which G acts. The action of G makes H into a $\mathbf{k}[G]$ - module and (8) induces a direct sum representation of the module $\mathbf{H} = \mathbf{k}[G] \cdot H$:

$$\mathbf{k}[G] \cdot H = \bigoplus_{\chi \in \mathfrak{X}} (\varepsilon_\chi \cdot \mathbf{k}[G]) \cdot H = \bigoplus_{\chi \in \mathfrak{X}} M_\chi \cdot H. \tag{9}$$

The subgroups $M_\chi \cdot H \subset H$ are called **irreducible components** of H; a **component** is the direct sum of one or more irreducible components. Note that the $\mathbb{Q}$ - rational idempotents correspond to the factorization of $X^{\varphi(n)} - 1$ over the rationals. The induced $\mathbb{Q}$ - irreducible components are thus always unions of one of more $\mathbb{F}_r$ - irreducible components, for some prime r.

We define the **support and annihilator** of H as the direct sum of irreducible modules which act non-trivially, resp. trivially on H:

$$\begin{array}{rcl} \mathrm{supp}(H) & = & \bigoplus_{\chi \in \mathfrak{X}_0;\ M_\chi \cdot H \neq \{1\}} M_\chi \\ \mathrm{ann}(H) & = & \bigoplus_{\chi \in \mathfrak{X}_0;\ M_\chi \cdot H = \{1\}} M_\chi. \end{array} \tag{10}$$

Note that $\mathrm{supp}(H), \mathrm{ann}(H) \subset \mathbf{k}[G]$; they are components of $\mathbf{k}[G]$ and not of H. In particular, various unrelated abelian groups may share the same support and annihilator. Furthermore, an irreducible component needs not be a cyclic module. Since H is finite, there are a finite number of cyclic modules in $M_\chi \cdot H$:

$$\exists\ m_{\chi,1}, m_{\chi,2}, \ldots, m_{\chi,k} \in H : \quad M_\chi \cdot H = \bigoplus_{i=1}^{k} M_\chi \cdot m_{\chi,i}.$$

The number k of cyclic modules $M_\chi \cdot m_{\chi,i}$ in $M_\chi \cdot H$ is called the **cycle-rank** of $M_\chi \cdot H$ and will be denoted by $\mathrm{cyc.rk.}(M_\chi)$.

Let now n_1, n_2 be powers of coprime integers. Then $G = G_{n_1 \cdot n_2} = G_{n_1} \times G_{n_2}$, as noted in the previous section. A character $\chi \in G_{n_1 n_2}$ splits then in $\chi = \chi_1 \cdot \chi_2$, with $\chi_i \in G'_{n_i},\ i = 1, 2$. If $\mu \in \overline{\mathbf{k}}$ is a primitive $\varphi(n_1 n_2)-$th root of unity, we define the orthogonal idempotents by the same formula (5) used in the case of prime powers. Let $\chi \in G$ with $\chi = \chi_1 \cdot \chi_2$ as above. An easy computation shows that, using the representation $\tau \in G_{nn'}$ with $\tau = \sigma_1 \cdot \sigma_2$, where $\sigma_i \in G_{n_i},\ i = 1, 2$ we have:

$$
\begin{aligned}
1_\chi &= \frac{1}{|G|} \cdot \sum_{\tau \in G} \chi(\tau) \cdot \tau^{-1} = \frac{1}{|G_{n_1}| \cdot |G_{n_2}|} \cdot \sum_{\sigma_i \in G_{n_i}} \chi_1(\sigma_1) \cdot \chi_2(\sigma_2) \cdot \sigma_1^{-1} \cdot \sigma_2^{-1} \\
&= \left(\frac{1}{G_{n_1}} \cdot \sum_{\sigma_1 \in G_{n_1}} \chi_1(\sigma_1) \cdot \sigma_1^{-1} \right) \times \left(\frac{1}{G_{n_2}} \cdot \sum_{\sigma_2 \in G_{n_2}} \chi_2(\sigma_2) \cdot \sigma_2^{-1} \right) \qquad (11) \\
&= 1_{\chi_1} \times 1_{\chi_2}.
\end{aligned}
$$

Herewith all the properties of idempotents and further definitions which build up upon these properties, extend by multiplicativity to general cyclotomic fields.

3. Explicit reflection

We let now ℓ be an odd prime and $n \in \mathbb{N}$ be divisible by ℓ and such that $\ell \not| \varphi(n)$. The fields will be $\mathbb{K} = \mathbf{C}_n$, so Gal $(\mathbb{K}/\mathbb{Q}) = G_n$, and $\mathbf{k} = \mathbb{F}_\ell$. Remember that the group ring $\mathbf{k}[G_n]$ is defined by multiplicativity and it is *semisimple*, since $\ell = \mathrm{char}(\mathbf{k}) \not| \, |G_n|$.

There is a unique character $\omega = \omega_\ell \in G_n^{'}$ such that

$$\sigma(\zeta_\ell) = \zeta_\ell^{\omega(\sigma)}, \quad \forall\ \sigma \in G_n.$$

This character is called the **cyclotomic character** for ℓ and it is an odd character. If $\chi \in G'$ we define the **reflected character** $\chi^* \in G'$ by

$$\chi^*(\sigma) = \omega(\sigma) \cdot \chi(\sigma^{-1}). \qquad (12)$$

Since $\omega(\sigma) \in \mathbb{F}_\ell = \mathbf{k}$ it follows that χ^* is irreducible iff χ is so; also, ω being odd, reflection changes the parity of a character. The definition of *reflected irreducible modules* and *reflected idempotents* follows naturally. We shall write $1_\chi^* = 1_{\chi^*}$, etc. One also remarks that reflection is an *involutive* operation, since $(\chi^*)^* = \omega \cdot \left(\omega\chi^{-1}\right)^{-1} = \chi$.

If $n = \ell$, the polynomial $\Phi_{\varphi(\ell)} = \Phi_{\ell-1}(X) = \prod_{j=1}^{\ell-1} (X - j)$ splits in linear factors over $\mathbf{k}$. The orthogonal idempotents are thus annihilated by linear polynomials $\varsigma - j$ and can be indexed by these polynomials. They have in this case the representation ([Wa], Chapter 6.2):

$$\varepsilon_j = \varepsilon_{\chi_j} = -\sum_{\sigma \in G_\ell} \omega^j(\sigma) \cdot \sigma^{-1}. \qquad (13)$$

Reflection of idempotents follows here the simple law: $\varepsilon_j^* = \varepsilon_{p-j}$.

We now expose Leopoldt's *Reflection Theorem*, which will establish relations between various ℓ - groups which are all $\mathbf{k}[G_n]$ modules. Leopoldt's original paper [Le] (see also [Lo]), treats the general case in which $\mathbb{K}$ is a normal field containing ζ_ℓ and such that $([\mathbb{K}/\mathbb{Q}], \ell) = 1$. Furthermore, the groups are ℓ - Sylow groups, while we are only interested in their elementary ℓ - subgroups, i.e. the subgroups of exponent ℓ. This second modification is only marginal, but it allows to bypass a step in which the base field for the group rings has to be $\mathbf{k} = \mathbb{Q}_\ell$, the ℓ - adic rational field.

Let $\mathcal{C}$ be the ideal class group of $\mathbb{K}$ and $E = \mathcal{O}(\mathbb{K}^+)^\times$ be the real units. Let $\alpha \in \mathbb{K}$ have valuation zero at each prime $\mathcal{L} \supset (\ell)$; we say that α is ℓ - **primary** iff

$$\alpha \equiv \nu^\ell \mod \ell \cdot (1 - \zeta_\ell)^2, \quad \text{for some} \quad \nu \in \mathbb{K}.$$

We then write $\mathbb{K}_\ell = \{x \in \mathbb{K}^\times : x \text{ is } \ell \text{ - primary}\}$ and let $E_\ell = E \cap \mathbb{K}_\ell$. Note that if $\mathbb{K}' \subset \mathbb{K}$ is a field in which ℓ is inert, then the necessary condition for ℓ - primary numbers in $\mathbb{K}'$ is $\alpha \equiv \nu^\ell \mod \ell^2$.

The first *actors* of reflection are then:

$$\begin{aligned} A_\ell &= \{x \in \mathcal{C} : x^\ell = 1\}, \quad \text{and} \\ U_\ell &= E_\ell / E^\ell. \end{aligned}$$

If $A_\ell \neq \{1\}$, there is a *maximal abelian unramified elementary ℓ - extension* $\mathbb{L} \supset \mathbb{K}$ - i.e. an extension with ℓ - elementary Galois group $H = \text{Gal}(\mathbb{L}/\mathbb{K})$. This is a subfield of the Hilbert class field of $\mathbb{K}$ and the Artin map yields an isomorphism between the groups $H \cong A_\ell$. The module $\mathbf{k}[G]$ acts on H by conjugation: $\sigma h = h^\sigma = \sigma^{-1} \circ h \circ \sigma$, for all $h \in H, \sigma \in G$. Finally, a number $\alpha \in \mathbb{K}$ is called ℓ - **singular** if there is a non-principal ideal $\mathfrak{a} \subset x \in A_\ell$ such that $\mathfrak{a}^\ell = (\alpha)$. Note that by definition $\alpha \notin \mathbb{K}^\ell$. We let $B = \{\alpha \in \mathbb{K} : \alpha \text{ is } \ell \text{ - singular}\} \cap (\mathbb{K}_\ell \setminus E_\ell)$ and $B_\ell = B/(K^\times)^\ell$.

Theorem 3 (Leopoldt's Reflection Theorem)**.** *Notations being like above, let $M = M_\chi \subset \mathbf{k}[G]'$ be an irreducible submodule, with $\chi \in \mathfrak{X}$ an even character. Then the $\mathbf{k}[G]'$ - modules A_ℓ, U_ℓ and B_ℓ are related by:*

$$\begin{aligned} \text{cyc.rk.}(M_\chi B_\ell) + \text{cyc.rk.}(M_\chi U_\ell) &= \text{cyc.rk.}(M^*_\chi A_\ell), \\ \text{cyc.rk.}(M^*_\chi B_\ell) &= \text{cyc.rk.}(M_\chi A_\ell), \quad \textit{and} \\ \text{cyc.rk.}(M_\chi B_\ell) \leq \text{cyc.rk.}(M_\chi A_\ell), \quad & \text{cyc.rk.}(M^*_\chi B_\ell) \leq \text{cyc.rk.}(M^*_\chi A_\ell). \end{aligned} \tag{14}$$

Moreover, the following inequality holds:

$$\begin{aligned} \text{cyc.rk.}(M_\chi \cdot A_\ell) &\leq \text{cyc.rk.}(M^*_\chi \cdot A_\ell) \\ &\leq \text{cyc.rk.}(M_\chi \cdot A_\ell) + \text{cyc.rk.}(M_\chi \cdot U_\ell). \end{aligned} \tag{15}$$

Proof. Note that the norm $\mathbf{N}_{\mathbb{K}/\mathbb{Q}}$ annihilates all the groups under consideration, which explains why we concentrate on $\mathbf{k}[G]'$. The numbers in B are primary singular non-units and the union $F_\ell = B_\ell \cup U_\ell$ is disjoint, so $\text{cyc.rk.}(MF_\ell) = \text{cyc.rk.}(MB_\ell) + \text{cyc.rk.}(MU_\ell)$ for each simple submodule $M \subset \mathbf{k}[G]'$. If $x \in F_\ell$ and $y \in \mathbb{K}^\times,\ y \equiv x \mod (K^\times)^\ell$, then $\mathbb{K}(y^{1/\ell})$ is an unramified abelian extension (e.g. [Wa], Chapter 9, Exercises). These are exactly all possibilities for generating the extension $\mathbb{L}$. The last line in (14) is obvious, since it takes an ideal in $\mathfrak{a} \in x \in A_\ell$ in order to define a singular number in B, and not all singular numbers are also primary, so the inequalities may be strict.

We have the following one-to-one maps:

$$F_\ell \leftrightarrow H \leftrightarrow A_\ell.$$

The first map is a consequence of the above remark, the second is the Artin map. The last line of (14) follows now from

$$|M^* A_\ell| = |MF_\ell| = |MB_\ell| + |MU_\ell|.$$

For odd characters χ, $M_\chi \cdot U_\ell = \{1\}$, since in this case M_χ annihilates the real units. This explains the asymmetry between the first two lines of (14). The symmetry is regained if we write, with F_ℓ defined above,

$$\text{cyc.rk.}(M_\chi F_\ell) = \text{cyc.rk.}(M^*_\chi A_\ell). \tag{16}$$

This relation holds for *any* character χ, and we shall prove it below. The extension $\mathbb{L}/\mathbb{K}$ is an abelian Kummer extension [La]; for $b \in \mathbf{b} \in F_\ell$, the extension $\mathbb{K}(b^{1/\ell})$

depends only upon the class $\mathbf{b} \in F_\ell$ of the algebraic number b. There is thus a (Kummer-) pairing $H \times F_\ell \rightarrow < \zeta_\ell >$ given by

$$< h, \mathbf{b} > = \frac{hb^{1/\ell}}{b^{1/\ell}}, \quad \text{for any} \quad b \in \mathbf{b}.$$

The pairing [La] does not depend upon the choice of the $\ell-$th root of b, is bilinear and non-degenerate. Furthermore, it is G - covariant in the sense that

$$< h^\sigma, b^\sigma > = < h, b >^\sigma, \quad \forall \ \sigma \in G. \tag{17}$$

Let now $\chi \in G'$. We claim that the Kummer pairing verifies the reflection property:

$$< \varepsilon_\chi^* h, \mathbf{b} > = < h, \varepsilon_\chi \mathbf{b} > . \tag{18}$$

Indeed $< h, \mathbf{b} >^\sigma = \zeta_\ell^{n\sigma} = < h, \mathbf{b} >^{\omega(\sigma)}$ so (17) implies $\sigma < h, \mathbf{b} > = < h, \mathbf{b} >^{\omega(\sigma)} = < h, \omega(\sigma)\mathbf{b} >$. The statement now follows by directly inserting the definition of ε_χ and using the fact that $|S(\chi)| = |S(\chi^*)|$. Let now $\mathbf{b} \in M_\chi F_\ell$, so $\varepsilon_\chi \mathbf{b} = \mathbf{b}$. Then (18) implies that

$$< h, \mathbf{b} > = < \varepsilon_\chi^* h, \mathbf{b} >,$$

so if $< h, \mathbf{b} > \neq 1$ then $\varepsilon_\chi^* h \neq 1$. But this means that $h \in M_\chi^* H$; however, if $b \in \mathbf{b} \in F_\ell$ and $1 \neq h \in$ Gal $(\mathbb{K}(b^{1/\ell})/\mathbb{K})$, then the pairing is necessarily $< h, \mathbf{b} > \neq 1$. This shows that the correspondence $F_\ell \leftrightarrow H$ acts componentwise by reflection, implies (16) and completes the proof. □

The main application of reflection is, for our purpose, the following:

Proposition 1. *Let $n = \ell \cdot n'$ with $\ell \not| \varphi(n)$, ℓ an odd prime and $n \in \mathbb{N}$. Let A_ℓ, U_ℓ be like above and $\chi \in G'_{n'}$, an even character belonging to the field $\mathbb{K}' = \mathbf{C}_{n'} \subset \mathbb{K}$. If $M_\chi U_\ell$ or $M_\chi A_\ell$ are not trivial, then $M_\chi^* A_\ell \neq \{1\}$*

Proof. If $M_\chi U_\ell \neq \{1\}$, then by the first line in (14), $M_\chi^* A_\ell \neq \{1\}$. Otherwise, if $M_\chi A_\ell$ is non trivial, then $M_\chi^* B_\ell$ is non trivial as a consequence of the second and third lines in (14). In both cases, $M_\chi^* A_\ell \neq \{1\}$, which completes the proof. □

Let ε_1 be the orthogonal idempotent in (13), defined with respect to $\ell = q$. The Proposition implies:

Corollary 1. *Let $\mathbf{T}$ and A_q be as in the statement of Theorem 1. Then $\mathbf{T}^* \supset$ $\mathrm{supp}(\varepsilon_1 \cdot A_q)$.*

Proof. If $\chi \in G_p$ then $\chi^* = \omega \cdot \chi^{-1}$ and $M^*\chi \subset \varepsilon_1 \mathbf{k}[G_{pq}]$. The statement follows now from Proposition 1. □

4. Bernoulli numbers

If $\chi \neq 1$ is a Dirichlet character of conductor f, then the **generalized Bernoulli numbers** are defined ([Wa], Chapter 4), by:

$$B_{1,\chi} = \frac{1}{f} \cdot \sum_{a=1}^{f} a \cdot \chi(a). \tag{19}$$

A major distinction between Galois characters and Dirichlet characters becomes clear in the definition (19): although it is formally identical to the definition of the idempotent $1_{\chi^{-1}}$, no factorization like (11) is possible. The reason is that in the definition of idempotents, $\chi(\sigma)$ is multiplied by an automorphism - thus, under the identification of Galois and Dirichlet characters, there is an implicit reduction modulo the conductor of χ. In (19) however, the factors a are considered as complex numbers, so the factorization is true only modulo f.

The next lemma gathers some computational facts on various characters:

Lemma 2. *Let ℓ, n be like in the previous section and $\mu \in \mathbb{C}$ a primitive $\varphi(n)-$th root of unity, $\mathbb{L} = \mathbb{Q}(\mu)$ and $(\ell) \subset \mathfrak{L} \subset \mathcal{O}(\mathbb{L})$ a prime ideal above ℓ. Let $\mathbb{F}_r = \mathcal{O}(\mathbb{L})/\mathfrak{L}$ be a field of characteristic ℓ so that the group $G'_n(\mathbb{F}_\ell)$ has images in $\mathbb{F}_r$; finally, let $\mathbb{L}' \supset \mathbb{Q}_\ell$ the extension of the ℓ-adic field for which $\mathcal{O}(\mathbb{L}')/(\ell \cdot \mathcal{O}(\mathbb{L}')) = \mathbb{F}_r$* [Go].

If $\nu \equiv \mu \mod \mathfrak{L} \in \mathbb{F}_r$, then μ is the unique root of unity in $\mathbb{C}$ with this property. Furthermore, there is a unique $\varphi(n)-$th root of unity $\mu' \in \mathbb{L}'$ such that $\mu' \mod (\ell \cdot \mathcal{O}(\mathbb{L}')) = \nu$. If $\chi \in G'_n(\mathbb{F}_\ell)$ there are unique characters $\psi_\chi \in D'_n = G'_n(\mathbb{Q})$ and $\lambda_\chi \in G'_n(\mathbb{Q}_\ell)$ - thus a Dirichlet and a ℓ - adic character - such that

$$\begin{array}{lcll} \psi_\chi(x) & \equiv & \chi(x) \mod \mathfrak{L}, & \forall\, x \in \mathbb{Z}, \\ \lambda_\chi(x) & \equiv & \chi(x) \mod (\ell \cdot \mathcal{O}(\mathbb{L}')), & \forall\, x \in \mathbb{Z}, \\ \psi_\chi(x) & \equiv & \lambda_\chi(x) \mod \mathfrak{L}^N, & \forall\, x \in \mathbb{Z}, N \in \mathbb{N}. \end{array} \tag{20}$$

If ω is the cyclotomic character for ℓ, then

$$\widehat{\omega} := \psi_\omega(x) \equiv x^{\ell^{N-1}} \mod \mathfrak{L}^N, \quad \forall\, x \in \mathbb{Z}, N \in \mathbb{N}. \tag{21}$$

Proof. There is exactly one $\mu \in \mathbb{C}$ with $\mu \equiv \nu \mod \mathfrak{L}$. If this was not the case and $\mu_1 \equiv \mu_2 \equiv \nu \mod \mathfrak{L}$, then $\mu_1 - \mu_2 \equiv 0 \mod \mathfrak{L}$ and $\mathbf{N}(\mu_1 - \mu_2) \equiv 0 \mod \ell$. But the norm on the right hand side is only divisible by primes dividing the order of μ, thus dividing $\varphi(n)$, which is coprime to ℓ, so $\mu_1 = \mu_2$. The unicity of the root μ' is proved similarly. It is an elementary fact on ℓ - adic extensions [Go], that $\mathcal{O}(\mathbb{L})/(\mathfrak{L}^N) \cong \mathcal{O}(\mathbb{L}')/\left(\ell^N \cdot \mathcal{O}(\mathbb{L}')\right)$ for all $N \in \mathbb{N}$. Let $\chi \in G'_n(\mathbb{F}_\ell)$ and $e_\chi(x) : \mathbb{Z} \to \mathbb{Z}/(\varphi(n) \cdot \mathbb{Z})$ be the exponent with $\chi(x) = \nu^{e_\chi(x)}$; then the characters in (20) are given by $\psi_\chi(x) = \mu^{e_\chi(x)}$ and $\lambda_\chi(x) = (\mu')^{e_\chi(x)}$. The properties in (20) are immediate consequences.

Finally, the character ω has order $\ell - 1$ and is defined by its values for $a = 1, 2, \ldots, \ell - 1$ for which $\omega(a) \equiv a \mod \ell$. One verifies that the character $\psi_\omega \mod \mathfrak{L}^N$ given by (21) has exactly these properties and the claim (21) follows from the unicity of ψ_ω and λ_ω. □

For even characters, $B_{1,\chi} = 0$ and the odd characters are connected to the field $\mathbb{K}$ by the class number formula [Wa], Theorem 4.17:

$$h_n^- = 2^k \cdot n \cdot \prod_{\chi \text{ odd}} B_{1,\chi}, \quad k \in \mathbb{Z}$$

Since we are interested in divisibility of h_n^- by the odd prime ℓ, the power of 2 is of less concern in our case. The factor n cancels with the denominator of $B_{1,\widehat{\omega_t}}$, for all the cyclotomic characters defined with respect to prime divisors of $t|n$; all the other Bernoulli numbers are algebraic integers. The class number formula indicates that if $\ell | h_n^-$, then some Bernoulli numbers will be divisible by prime ideals above ℓ. The next step is to follow this indication and gather a finer, component dependent information about divisibility of $B_{1,\chi}$ by primes above ℓ.

Let

$$\theta = \frac{1}{n} \cdot \sum_{0<c<n;(c,n)=1} a \cdot \sigma_c^{-1}$$

be the Stickelberger element of $\mathbb{K}$ ([Wa], Theorem 15.1). Then $\theta_c = (c - \sigma_c)\theta \in \mathbb{Z}[G_n]$, for $(c, n) = 1$ and it annihilates the class group $\mathcal{C}$ of $\mathbb{K}$. Idempotents, Bernoulli numbers and Stickelberger element are related by the following formula, which is a consequence of (6). We assume here that the characters $\chi \in G'$ are defined with respect to the field $\mathbf{k} = \mathbb{Q}$ and they are identified to Dirichlet characters as shown before.

$$\begin{array}{rcll} \theta \cdot 1_\chi & = & B_{1,\chi^{-1}} \cdot 1_\chi, & \forall\ \chi \in G'(\mathbb{Q}), \\ (c - \sigma_c)\theta \cdot 1_\chi & = & (c - \chi(c)) \cdot B_{1,\chi^{-1}} \cdot 1_\chi, & \forall\ \chi \in G'(\mathbb{Q}). \end{array} \tag{22}$$

By reducing the above relations modulo primes lying above ℓ, we obtain important information about Bernoulli numbers, when an ℓ - component of the class group is non trivial.

Proposition 2. *Let ℓ be an odd prime and $n = \ell \cdot n' \in \mathbb{N}$ with $(\ell, \varphi(n)) = 1$, $\mathbb{K} = \mathbf{C}_n$; for $m | \varphi(n)$, $m > 1$, let $\mu \in \mathbb{C}$ be a primitive $m-$*th *root of unity and $G = G_n(\mathbb{F}_\ell)$. We fix a prime ideal $(\ell) \subset \mathfrak{L} \subset \mathcal{O}(\mathbb{Q}(\mu))$ and consider $\chi \in G'$, a non - trivial primitive group character of exact order m, other then the cyclotomic character ω_ℓ.*

Let $\mathcal{C}$ be the class group of $\mathbb{K}$, $A_\ell = \{x \in \mathcal{C} : x^\ell = 1\}$ and suppose that $M_\chi \cdot A_\ell \neq \{1\}$. If $\psi = \psi_\chi$ is the Dirichlet character defined in (20), then:

$$B_{1,\psi^{-1}} \equiv 0 \mod \mathfrak{L}. \tag{23}$$

Furthermore, if $M_\chi \cdot A_\ell \neq \{1\}$ for all characters of exact order m, then

$$B_{1,\psi^{-1}} \equiv 0 \mod \ell \cdot \mathcal{O}(\mathbb{Q}(\mu)). \tag{24}$$

Proof. Let $c \in \mathbb{Z}$ with $\chi(c) \not\equiv c \mod \ell$ - this is possible, since $\chi \neq \omega_\ell$ - so $\theta_c = (c - \sigma_c)\theta \in \mathbb{Z}[G]$ and it annihilates the class group. Thus $\theta_c \cdot 1_\kappa A_\ell = \{1\}$ for all $\kappa \in G'$ and in particular for κ belonging to $S(\chi)\chi$. But since $M_\chi A_\ell \neq \{1\}$, it follows that the last annihilation is non trivial. We insert c in the second relation of (22) and use $c - \chi(c) \not\equiv 0 \mod \mathfrak{L}$, thus finding

$$\theta_c \varepsilon_\chi \quad \equiv \quad (c - \chi(c)) \cdot B_{1,\psi^{-1}} \cdot \varepsilon_\chi \mod \mathfrak{L}.$$

Since ε_χ does by definition not annihilate $M_\chi A_\ell$ and $c - \chi(c) \mod \mathfrak{L} \in \mathbb{F}_r^\times$, it follows that $B_{1,\psi^{-1}}$ must vanish modulo $\mathfrak{L}$, which is the statement of (23).

Suppose now that (23) holds for all characters of order m and let ψ_χ be the Dirichlet character induced by one of the $\chi \in G_n'(\mathbb{F}_\ell)$. Let $\sigma \in$ Gal $(\mathbb{Q}(\mu)/\mathbb{Q})$; then $\sigma(\psi)$ is also a character of exact order m for which (23) holds. Thus

$$B_{1,\sigma^{-1}(\psi^{-1})} = \sigma^{-1}\left(B_{1,\psi^{-1}}\right) \equiv 0 \mod \mathfrak{L},$$

and, by applying σ to the above congruence, we find that $B_{1,\psi^{-1}} \equiv 0 \mod \sigma\mathfrak{L}$. This is the case for all $\sigma \in$ Gal $(\mathbb{Q}(\mu)/\mathbb{Q})$ and (24) follows. □

In particular, when the situation described in the Proposition happens for the reflected of *all* even characters in $\mathbb{F}_\ell[G_{n'}]'$, then we have:

Corollary 2. *Let the notations be the same as in Lemma 2, $n' \geq 7$ or $n' = 5$ and suppose that $M_\chi^* \cdot A_\ell \neq \{1\}$ for all even characters $\chi \in \mathbb{F}_\ell[G_{n'}]'$. If $\mu \in \mathbb{C}$ is a primitive $\varphi(n')-$*th *root of unity and $(\ell) \subset \mathfrak{L} \subset \mathcal{O}(\mathbb{Q}(\mu))$ is a prime ideal above ℓ, then for all even Dirichlet characters ψ of conductor n' the following holds:*

$$B_{1,\widetilde{\omega}^{-1}\cdot\psi} \equiv 0 \mod \ell \cdot \mathcal{O}(\mathbb{Q}(\mu)). \tag{25}$$

Proof. Note that for $n' < 7,\ n' \neq 5$, we have $\varphi(n') \leq 2$ and there are no non-trivial even characters in $G'_{n'}$. The Corollary is a consequence of (24) and the fact that the ideal (ℓ) in the $m-$th cyclotomic extension lifts to the ideal (ℓ) in $\mathbb{Q}(\mu)$, for any $1 < m | \varphi(n')$. □

5. Proof of the Theorem

The proof of Theorem 1 is an application of Corollaries 1 and 2 combined with some involved computations with congruences and integer parts. Let p, q be the primes in Theorem 1 and let $\ell = q, n = pq$ and $n' = p$. Since $p \not\equiv 1 \mod q$ and $p > q, p \geq 5$, we are in the situation of the previous results. Assume that $\mathbf{T} = (\mathbf{N})$ in Theorem 1. Then Corollary 1 implies that $M^*_\chi A_q$ is non trivial for all even, non-trivial $\chi \in G'_p$ with images in $\overline{\mathbb{F}}_q$. Let $\mu \in \mathbb{C}$ be a primitive $(p-1)/2-$th root of unity - since we consider only even characters of G_p, their order divides $(p-1)/2$; let $\mathcal{E}_p$ be the set of all even, non-trivial Dirichlet characters of conductor p. Then Corollary 2 implies that (25) holds for all $\psi \in \mathcal{E}_p$. for such ψ, we write $\beta_{1,\psi} = pqB_{1,\psi}$, so that

$$B_{1,\psi} \equiv 0 \mod q \Leftrightarrow \beta_{1,\psi} \equiv 0 \mod q^2.$$

The characters $\psi \in \mathcal{E}_p$ are even, $\psi(a) = \psi(p-a)$.

We need some facts on computations modulo pq. Let $0 < u < q,\ 0 < v < p$ be the unique integers given by the extended Euclid algorithm, such that $up + vq \equiv 1 \mod pq$. The following easy consequence of the definition of u, v will be used below:

$$v \equiv \pm 1 \mod p \quad \Leftrightarrow \quad q \equiv \mp 1 \mod p. \tag{26}$$

Let $0 < x(a,b) < pq$ and $0 \leq n(a,b) < p$ be the unique integers with

$$x(a,b) = b + q \cdot n(a,b) \quad \equiv \quad \begin{cases} a \mod p, & a = 1, 2, \ldots, p-1, \\ b \mod q, & b = 1, 2, \ldots, q-1. \end{cases}$$

Then $x(a,b) \equiv upb + vqa \mod pq$ and

$$\begin{aligned} q \cdot n(a,b) &\equiv avq + bq\frac{up-1}{q} \equiv q(av - bv) \mod pq, \quad \text{so} \\ n(a,b) &\equiv (a-b)v \mod p. \end{aligned} \tag{27}$$

Note the identity $n(a,b) + n(p-q, q-b) = p-1$. Indeed, since $x(p-a, q-b) = pq - x(a,b)$, we have

$$pq = b + qn(a,b) + (q-b) + qn(p-a, q-b) = q \cdot (1 + n(a,b) + n(p-a, q-b)),$$

which confirms the claim. For $a = 1, 2, \ldots, p-1$ we let $f(a) \in \mathbb{F}_q$ be defined by:

$$f(a) \equiv \sum_{b=1}^{q-1} b^{-1} \cdot n(a,b) \mod q. \tag{28}$$

Then

$$f(p-a) \equiv \sum_{b=q-1}^{1} (q-b)^{-1} \cdot n(p-a, q-b) \equiv \sum_{b=q-1}^{1} -b^{-1} \cdot (p-1-n(a,b)) \equiv f(a) \mod q.$$

With this, (25) implies for all non trivial $\psi \in \mathcal{E}_p$:

$$\begin{aligned}\beta_{1,\widetilde{\omega}^{-1}\psi} &= \sum_{a=1;\ b=1}^{(p-1)/2,q-1} \psi(a)\widetilde{\omega}^{-1}(b) \cdot (x(a,b) + x(p-a,b)) \\ &\equiv \sum_{a=1;b=1}^{(p-1)/2;\ q-1} 2\psi(a)b^{1-q} + qb^{-1} \cdot (n(a,b) + n(p-a,b)) \mod q^2.\end{aligned}$$

From (4), since $\psi \neq \mathbf{1}$, we have $2 \cdot \sum_{a=1}^{(p-1)/2} \psi(a) = \sum_{a=1}^{p-1} \psi(a) = 0$. The sum vanishes in $\mathbb{C}$ and a fortiori modulo q^2, and with the definition (28), the previous congruence becomes

$$\sum_{a=1}^{(p-1)/2} \psi(a) \cdot f(a) \equiv 0 \mod q, \quad \psi \in \mathcal{E}_p. \tag{29}$$

We can regard the above as an homogeneous linear system of equations over $\mathbb{F}_q$, with $(p-1)/2$ unknowns and $(p-3)/2$ equations. One recognizes that the system matrix has a submatrix of rank $(p-3)/2$, which is in fact a Vandermonde matrix. An easy verification shows that the constant vector is a solution of (29), so

$$\exists\ c_0 \in \mathbb{F}_q \quad \text{such that} \quad f(a) = c_0, \quad \text{for} \quad a = 1, 2, \ldots, p-1.$$

Since $x - p \cdot \left[\frac{x}{p}\right] \in \{0, 1, \ldots, p-1\}$ for all $x \in \mathbb{Z}$, it follows that $n(a,b) = (a-b) - p \cdot \left[\frac{a-b}{p}\right]$. We can compute the constant c_0 directly, using (27):

$$c_0 \equiv \sum_{b=1}^{q-1} b^{-1} \left((a-b)v - p\left[\frac{(a-b)v}{p}\right] \right) \equiv v - p \cdot \sum_{b=1}^{q-1} b^{-1} \left[\frac{(a-b)v}{p}\right] \mod q.$$

With a new constant $c_1 \equiv \frac{v-c_0}{p} \equiv uv - uc_0 \mod q$, we have the linear system of equations:

$$\sum_{b=1}^{q-1} b^{-1} \cdot \left[\frac{(a-b)v}{p}\right] - c_1 \equiv 0 \mod q, \quad a = 1, 2, \ldots, p-1. \tag{30}$$

For a heuristic investigation of (30), let us define

$$\theta_{a,b} = \sum_{b=1}^{q-1} \left(\left[\frac{(a-b)v}{p}\right] \cdot \sigma_b^{-1} \right) - c_1 \in \mathbb{F}_q[G_q].$$

Then (30) says that $\varepsilon_1 \theta_{a,b} = 0$ for $a = 1, 2, \ldots, p-1$ and ε_1 the idempotent in (13), with respect to $\ell = q$. We assume that the vectors $(n(a,b))_{b=1}^{q-1}$ are random distributed for $a = 1, 2, \ldots, (p-1)/2$. By fixing c_1 such that $\theta_{1,b}\varepsilon_1 = 0$, the probability that the same component vanishes for the further $(p-3)/2$ independent elements in $\mathbb{F}_q[G]_q$ is $q^{-(p-3)/2}$. For fixed p and $q < N \to \infty$, the probability that (30) is verified for at least one q is thus $P(p) < \zeta\left(\frac{p-3}{2}\right) - 1 < 1$, with ζ, the Riemann function. The heuristic suggests thus that (30) has no solutions, irrespective of the size of p and q.

For a proof, we shall need to restrict generality to the case $p > q$, as in the statement of Theorem 1, and since p and q are primes, then $p - 2 \geq q$. We let $s_v(z) = \left[\frac{(z+1)v}{p}\right] - \left[\frac{zv}{p}\right]$ for $z \in \mathbb{Z}$. Since $0 < v < p$, if follows that $0 \leq s_v(z) \leq 1$ for all $z \in \mathbb{Z}$.

We extend the summation range to $b = 0$ and replace b^{-1} by $\omega^{-1}(b)$ which is also defined at $b = 0$. By subtracting the identities above for two successive values $a, a+1$ with $0 < a < p-2$, if follows that

$$\begin{aligned} c_1 - c_1 &\equiv \sum_{b=0}^{q-1} \omega^{-1}(b) \cdot \left(\left[\frac{(a+1-b)v}{p} \right] - \left[\frac{(a-b)v}{p} \right] \right) \\ &\equiv \sum_{b=0}^{q-1} \omega^{-1}(b) \cdot s_v(a-b) \equiv 0 \mod q. \end{aligned}$$

or, equivalently

$$\sum_{t=a+1-q}^{a} \omega^{-1}(a-t) \cdot s_v(t) \equiv 0 \mod q. \tag{31}$$

Since $p > q$, relation (26) implies that $v \not\equiv \pm 1 \mod p$ and a simple computation shows that $s_v(z) = s_v(z+q)$ for $1 - q < z \leq 0$. This allows to keep the argument of $s_v(t)$ in the range $0 \leq t < q$, when $a < q$:

$$\sum_{t=0}^{q-1} \omega^{-1}(a-t) \cdot s_v(t) \equiv 0 \mod q, \quad a = 1, 2, \ldots, p-2. \tag{32}$$

The first q equations in (32) then lead to a quadratic homogeneous system modulo q. Let the matrices $\Omega_i \in M(\mathbb{F}_q, q-i)$, $i = 0, 1$, be defined by:

$$\Omega_i = \left(\omega^{-1}(a-t) \right)_{a,t=0}^{q-1-i}, \quad i = 0, 1.$$

Then Ω_1 is a submatrix of Ω_0, which is the system matrix of the first q equations in the system (32). Note that Ω_1 is a Toeplitz matrix and it has the characteristic polynomial $X^{q-1}+1$ - as results by applying an usual method of numerical analysts for such matrices. The method consists in completing the matrix into a $2(q-1) \times 2(q-1)$ circulant matrix, whose eigenvalues are then $\xi_{2(q-1)}^k$, where $\xi_{2(q-1)}$ is a primitive $2(q-1)-$th root of unity over $\mathbb{F}_q$ (i.e. the quadratic root of a generator of $\mathbb{F}_q$) and $k = 0, 1, \ldots, 2(q-1)-1$. One verifies that the odd powers are eigenvalues of Ω_1, which leads to the claimed characteristic polynomial. In particular, Ω_1 is a regular matrix and since $\Omega_0 \mathbf{x} = \mathbf{0}$ allows the constant vector as solution, it follows that this is also the only solution. But then $s_v(t)$ is the constant vector, for $t = 0, \ldots, q-1$; since $s_v(0) = 0$ and

$$\sum_{t=0}^{q-1} s_v(t) = \sum_{t=0}^{q-1} \left(\left[\frac{(t+1)v}{p} \right] - \left[\frac{tv}{p} \right] \right) = \left[\frac{qv}{p} \right] = \left[\frac{1+(q-u)p}{p} \right] = q - u > 0.$$

We reached a contradiction, which completes the proof of the Theorem.

Remark 2. *The careful reader may have noted that we started from a redundant system of equations, which allowed for the substitution $a \to p-a$ and we obtained a non redundant system of rank $q-1$. This may seem surprising, especially if $q - 1 > \frac{p-1}{2}$. However tracing back the use of $s_v(t) = s_v(t+q)$, one notes that (31) is invariant under the above substitution, while (32) is not.*

The Theorem 1 is tailored for the needs of the proof of Catalan's equation. The Proposition 2 allows for more general results and raises more general questions then the Theorem, questions and results which shall be presented separately.

The general question is the following: given $\ell, n = \ell \cdot n'$ *like in the previous section and if* $\mathbf{T} \subset \mathbb{F}_\ell[G_n]$ *is one of the supports* $\mathrm{supp}(A_\ell), \mathrm{supp}(F_\ell)$*, is it possible that* $\mathbf{T}$ *a full* $\mathbb{Q}$ *- rational component of* $\mathbb{F}_\ell[G]$ *? Further manipulation of the fundamental system (29) together with heuristics similar to the one above (and the one used by Washington in* [Wa] *for analysing the likeliness of Vandiver's conjecture), suggest that this fact should never happen, independently of the size of* ℓ, n'*, as long as the degree of the rational components is at least* 3*. In lack of a proof, we* ***conject*** *it is impossible and will investigate this conjecture in future works.*

Conjecture 1. *Let* ℓ, n *be like in the previous section and* $\mathbf{T} \subset \mathbb{F}_\ell[G]$ *be one of* $\mathrm{supp}(A_\ell), \mathrm{supp}(F_\ell)$*. Let*

$$g(X) \in \mathbb{Z}[X] \quad \text{with} \quad g(X) | \frac{X^{\varphi(n)} - 1}{X^2 - 1},$$

be an irreducible factor of degree at least 3 *and let*

$$\mathfrak{X}_g = \{ \ \chi \in G : g(X) \equiv 0 \mod (\ell, f_\chi(X)) \ \}.$$

Then $\cup_{\chi \in \mathfrak{X}_g} M_\chi \not\subset \mathbf{T}$.

Acknowledgments: I thank Francisco Thaine for his suggestions and encouragement shown during the development of this paper.

References

[Go] Fernando Q. Gouvêa: *p – adic Numbers, An Introduction*, Second Edition, Springer Universitext (1991).

[La] Lang, S.: *Algebra*, Third Edition, Springer 2002, Graduate Texts in Mathematics **211**

[Le] Leopoldt, H. W.: *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abhandlungen der Deutschen Akademie der Wissenschaftern, Berlin, Kl. Math. Nat. 1953, no. 2 (1954).

[Lo] Long, R. : *Algebraic number theory*, Marcel Dekker, Series in Pure and Applied Mathematics (1977).

[Mi] P. Mihăilescu: *Primary Cyclotomic Units and a Proof of Catalan's Conjecture*, J. reine angew. Math. **572** (2004), pp. 167-195.

[Ono] Takashi Ono: *Algebraic Number Theory*, Academic Press.

[Wa] L. Washington: *Introduction to Cyclotomic Fields*, Second Edition, Springer (1996), Graduate Texts in Mathematics **83**.

(P. Mihăilescu) Gesamthochschule Paderborn
E-mail address, P. Mihăilescu: `preda@upb.de`