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).