VANISHING OF EIGENSPACES AND CYCLOTOMIC FIELDS

ROBERT OSBURN

Abstract. We use a result of Thaine to give an alternative proof of the fact that, for a prime $p > 3$ congruent to 3 modulo 4, the component $e_{(p+1)/2}$ of the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$ is trivial.

1. Introduction

Let $p > 3$ be a prime, ζ_p a pth primitive root of 1, and Δ the Galois group of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$. Let $q \neq p$ be a prime and n the order of q modulo p. Assume $q \not\equiv 1 \bmod p$ and so $n \geq 2$, $p(q-1)|q^n-1$, and $n|p-1$. Set $f = (q^n-1)/p$ and $e = (p-1)/n$. Let Q be a prime ideal of $\mathbb{Z}[\zeta_p]$ above q and let $\mathbb{F} = \mathbb{Z}[\zeta_p]/Q$. Thus $\mathbb{F} \cong \mathbb{F}_{q^n}$, the finite field with q^n elements. Let $\alpha \in \mathbb{Z}[\zeta_p]$ be a generator of $\mathbb{F}^\times$ such that

$$\alpha^f \equiv \zeta_p \bmod Q.$$

Now let A be the p-Sylow subgroup of the ideal class group $\mathbb{Q}(\zeta_p)$, $\mathbb{Z}_p$ the ring of p-adic integers, $\omega : \Delta \to \mathbb{Z}_p^\times$ is the Teichmüller character defined by

$$\omega(k) \equiv k \bmod p,$$

and e_r, $0 \leq r \leq p-2$, the idempotents

$$\frac{1}{p-1}\sum_{\lambda \in \Delta} \omega^r(\lambda)\lambda^{-1} \in \mathbb{Z}_p[\Delta].$$

As A is a $\mathbb{Z}_p[\Delta]$-module, we have the decomposition (see Section 6.3 in [9])

$$A = \bigoplus_{r=0}^{p-2} e_r(A).$$

It is well-known that for r even, $2 \leq r \leq p-3$, $e_r(A)$ can be identified with the components of the p-part of the ideal class group of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Vandiver's conjecture says that all even components $e_r(A)$ vanish. Via K-theory, Kurihara [5] proved that the "top" even eigenspace $e_{p-3}(A)$ always vanishes. Kurihara's proof uses the surjectivity of the Chern map

$$K_4(\mathbb{Z}) \otimes \mathbb{Z}/p \to e_{p-3}(A).$$

Soulé [6] extended Kurihara's result and showed the following: Let $n > 1$ odd. If $\log p > n^{224n^4}$, then $e_{p-n}(A)$ is trivial. Our main result is the following.

Theorem 1.1. *If $p > 3$ is a prime congruent to 3 modulo 4, then $e_{(p+1)/2}(A)$ is trivial.*

One can use the reflection theorem (see Theorem 10.9 in [9]) and the class number formula for the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ to prove Theorem 1.1. Precisely, if $e_{(p+1)/2}(A)$ is non-trivial, then $e_{(p-1)/2}(A)$ is non-trivial and so (see Section 2 for the definition of v) $p \mid n-2v$; but $n-2v < p$, a contradiction. Recently, Thaine [8] investigated properties of certain numbers (see d_i and a_k in Section 2) related to Gaussian periods

2000 *Mathematics Subject Classification.* Primary: 11R18; Secondary: 11T22.

and showed that they are useful in the study of certain components of the ideal class group of $\mathbb{Q}(\zeta_p)$. In particular, Thaine states: "We believe that the theorem [Theorem 1 in [8] or Theorem 2.2 below] can be used to show that, with l odd ($1 \leq l \leq e-1$), some of the components $e_{p-ln}(A)$ of A are trivial. The idea is to show that if $e_{p-ln}(A)$ is non-trivial, then *all* prime numbers q of order n modulo p must have a certain form; we hope this will contradict some version of Dirichlet's theorem on primes in arthimetic progressions."

The purpose of this note is to give an alternative proof of Theorem 1.1 using Thaine's result. The proof will show that non-trivial eigenspaces lead to representations of certain integers by binary quadratic forms with restrictive divisibility properties on the parameters. A density calculation will show that that this divisibility property doesn't occur for all primes q of order $(p-1)/2$ modulo p and thus the eigenspace must vanish. It might be of some interest to see if similar vanishing results can be obtained for other even indexed eigenspaces $e_r(A)$ by considering an appropriate quadratic form (see (2) of Remark 4.1).

2. Indices of Cyclotomic Units

We discuss a result of Thaine on congruences involving indices of cyclotomic units. Let us consider the components $e_{p-ln}(A)$ for l odd, $1 \leq l \leq e-1$. For r even, $2 \leq r \leq p-3$, let

$$\beta_r = \prod_{i=1}^{p-1} (1-\zeta_p^i)^{i^{p-1-r}}$$

and let $i_r(Q)$ be the least nonnegative integer such that

$$\beta_r \equiv \alpha^{i_r(Q)} \bmod Q.$$

It is well-known that $e_r(A)$ is trivial if and only if β_r is not the pth power of an element of $\mathbb{Z}[\zeta_p]$ (see Theorem 15.7 and the discussion preceding Theorem 8.14 in [9]). In particular, we have the following.

Proposition 2.1. *For r even, $2 \leq r \leq p-3$, if $i_r(Q) \not\equiv 0 \bmod p$, then $e_r(A)$ is trivial.*

In order to study the indices $i_r(Q)$, we need to introduce certain numbers. Let g be a primitive root modulo p. For $k \in \mathbb{Z}$, we define

$$a_k = nq^v \sum_{i=0}^{e-1} g^{nki} d_i,$$

where d_i is defined (see (14) in [8]) as

$$d_i = \frac{\eta_{g^i} - \eta_0}{q^v}$$

for $0 \leq i \leq e-1$ where the η_i's are the Gaussian periods ($0 \leq i \leq p-1$)

$$\eta_i = \sum_{j=0}^{f-1} \zeta_q^{T(\alpha^{i+pj})}.$$

Here T is the trace from $\mathbb{F}$ to $\mathbb{F}_q$. Given an integer a, denote by $|a|_p$ the smallest nonnegative residue of a modulo p. Then v is given by (13) [8], namely

$$v = \min_{0 \leq k \leq e-1} \frac{1}{p} \sum_{l=0}^{n-1} |g^{k+el}|_p.$$

Note that $v \geq 1$. The following theorem (see Theorem 1 in [8]) summarizes some properties of the numbers a_k and d_i and will be useful when considering $e_{p-ln}(A)$.

Theorem 2.2. *(i) We have*

$$e^2q^{n-2v} = \left(\sum_{i=0}^{e-1} d_i\right)^2 + p\left(e\sum_{i=0}^{e-1} d_i^2 - \Big(\sum_{i=0}^{e-1} d_i\Big)^2\right).$$

(ii) The numbers a_k satisfy the following congruences: $a_0 \equiv -1 \bmod p$, and for l odd $(1 \le l \le e-1)$,

$$\sum_{m=1}^{l} (-1)^m \binom{ln}{mn} a_{l-m}a_m \equiv -l \cdot i_{p-ln}(Q) \bmod p.$$

3. Quadratic Forms

Let $p > 3$ be a prime congruent to 3 modulo 4. In this section, we study the representation of primes and a multiple of a certain power of a prime by the quadratic form $x^2 + py^2$.

Proposition 3.1. *Let $p > 3$ be a prime with $p \equiv 3 \bmod 4$ and h be the class number of $\mathbb{Q}(\sqrt{-p})$. Then there exists a prime $q \neq p$ with $\left(\frac{-p}{q}\right) = 1$ such that if (u, v) is an integer solution to the equation*

$$x^2 + py^2 = q,$$

then $p \nmid v$.

Proof. By Theorem 9.12 in [3], there are infinitely many primes q with $\left(\frac{-p}{q}\right) = 1$ such that $x^2 + py^2 = q$ has an integer solution. Let $\mathcal{S}_1$ denote the set of primes represented by $x^2 + py^2$ and $\mathcal{S}_2$ denote the set of primes represented by $x^2 + p^3y^2$. Suppose for every prime $q \neq p$, we have $p \mid v$. Then the quadratic forms $x^2 + py^2$ and $x^2 + p^3y^2$ represent the same infinite set of primes and thus $\mathcal{S}_1$ and $\mathcal{S}_2$ have the same Dirichlet density. By Theorems 7.24 and 9.12 in [3], we have the following: for $p \equiv 7 \bmod 8$,

$$\mathcal{S}_1 \text{ has density } \frac{1}{2h}$$

and

$$\mathcal{S}_2 \text{ has density } \frac{1}{2ph},$$

which is a contradiction. For $p \equiv 3 \bmod 8$,

$$\mathcal{S}_1 \text{ has density } \frac{1}{6h}$$

and

$$\mathcal{S}_2 \text{ has density } \frac{1}{6ph},$$

a contradiction. Therefore, there exists a prime q such that $p \nmid v$. □

We now need the following result from [1] (see Theorem 2, page 224).

Theorem 3.2. *Let p and q be distinct odd primes and assume that $u^2 + pv^2 = q$ for some relatively prime integers u and v. Let*

$$\beta = u + v\sqrt{-p}.$$

If s is an odd positive integer, define polynomials $x(u, v)$ and $y(u, v)$ by

$$x(u,v)+y(u,v)\sqrt{-p}=\beta^s.$$

Then

$$y(u,v)=v\sum_{j=0}^{(s-1)/2}\binom{s}{2j}(-pv^2)^{(s-2j-1)/2}(u^2)^j \tag{1}$$

and $(x(u,v),\ y(u,v))$ *is a solution to* $x^2+py^2=q^s$.

Corollary 3.3. *Let* $p>3$ *be a prime with* $p\equiv 3 \bmod 4$ *and* h *be the class number of* $\mathbb{Q}(\sqrt{-p})$. *Then there a prime* $q\neq p$ *with* $\left(\frac{-p}{q}\right)=1$ *such that if* (C,D) *is a solution of the equation*

$$x^2+py^2=4q^h,$$

then $p\nmid D$.

Proof. By Proposition 3.1, there exists a prime $q\neq p$ such that for the integer solution (u,v) to the equation $x^2+py^2=q$, we have $p\nmid v$. We also have that $p\nmid u$ since otherwise p would divide q. Now take $s=h$ in Theorem 3.2. By (1) and the fact that h is odd (see Corollary 18.4 in [2]), we see that for the solution $(x(u,v),\ y(u,v))$ to the equation

$$x^2+py^2=q^h, \tag{2}$$

$p\nmid y(u,v)$. Multiplying (2) by 4, we have $p\nmid D$. □

4. Proof of Theorem 1.1

Proof. Let $p>3$ be a prime with $p\equiv 3 \bmod 4$, $q\neq p$ be a prime of order $(p-1)/2$ modulo p, and g a primitive root modulo p. Thus $\left(\frac{-p}{q}\right)=1$. Suppose $e_{(p+1)/2}(A)$ is nontrivial. Then by Proposition 2.1, $i_{(p+1)/2}(Q)\equiv 0 \bmod p$. By Theorem 2.2, (ii), we have that

$$a_1\equiv 0 \bmod p$$

and so by the definition of a_1,

$$d_1\equiv d_0 \bmod p.$$

By Theorem 2.2, (i),

$$\begin{aligned}4q^{(p-1)/2-2v}&=(d_0+d_1)^2+p(2(d_0^2+d_1^2)-(d_0-d_1)^2)\\&=(d_0+d_1)^2+p(d_0-d_1)^2,\end{aligned}$$

where $p\mid(d_0-d_1)$. We now claim that $(p-1)/2-2v=h$ where h is the class number of $\mathbb{Q}(\sqrt{-p})$. To see this, note that $n=(p-1)/2$ and so $e=2$ and $l=1$. Thus

$$v=\min\left\{\frac{1}{p}\sum_{l=0}^{\frac{p-3}{2}}|g^{2l}|_p,\frac{1}{p}\sum_{l=0}^{\frac{p-3}{2}}|g^{1+2l}|_p\right\}.$$

As g is a primitive root modulo p, the first sum, say R, appearing in v is

$$\frac{1}{p}\sum_{\substack{s=0\\ \left(\frac{s}{p}\right)=1}}^{\frac{p-1}{2}} s.$$

Similarly, the second sum, say V, appearing in v is

$$\frac{1}{p}\sum_{\substack{t=0\\ \left(\frac{t}{p}\right)=-1}}^{\frac{p-1}{2}} t.$$

By [4], $V + R = (p-1)/2$ and $h = V - R$. This implies that $v = R$. Thus $R = (p-1)/4 - h/2$ and so

$$(p-1)/2 - 2v = (p-1)/2 - 2R = h.$$

So for every prime q of order $(p-1)/2 \bmod p$, if C and D are integers such that

$$4q^h = C^2 + pD^2,$$

then we have that $p \mid D$. By Corollary 3.3, this is a contradiction. Thus $e_{(p+1)/2}(A)$ is trivial. □

Remark 4.1. (1) The quadratic form which appears in the proof of Theorem 1.1 has been studied by Stickelberger [7]. His elegant result is as follows: Let $-k$ be a negative fundamental discriminant so that $\mathbb{Q}(\sqrt{-k})$ is an imaginary quadratic field of discriminant $-k$ and class number h. Assume $k \neq 3$, 4, or 8. Let q be a prime such that $\left(\frac{-k}{q}\right) = 1$. Then there are integers C and D, unique up to sign, for which

$$4q^h = C^2 + kD^2$$

where $k \nmid C$. Moreover, for prime $k \geq 7$, $C \equiv 2(-q)^{-R} \bmod k$ where R is as above.

(2) It might be possible to prove similar vanishing results for $e_{(3p+1)/4}(A)$ where $p \equiv 5 \bmod 8$ and for $e_{(5p+1)/6}(A)$ where $p \equiv 7 \bmod 12$. The difficulty is that the resulting quadratic forms are more involved. Namely, the first case corresponds to $e = 4$ and so by Theorem 2.2, (i), we have

$$16q^{(p-1)/4-2v} = \left(\sum_{i=0}^{3} d_i\right)^2 + p\left(4\sum_{i=0}^{3} d_i^2 - \Big(\sum_{i=0}^{3} d_i\Big)^2\right).$$

The second case corresponds to $e = 6$ and thus by Theorem 2.2, (i), we have

$$36q^{(p-1)/6-2v} = \left(\sum_{i=0}^{5} d_i\right)^2 + p\left(6\sum_{i=0}^{5} d_i^2 - \Big(\sum_{i=0}^{5} d_i\Big)^2\right).$$

Acknowledgments

The author would like to thank Francisco Thaine and Pieter Moree for their comments and encouragement. The author would also like to thank the Max-Planck-Institut für Mathematik for their hospitality and support during the preparation of this paper.

References

[1] E. Bender, N. Herzberg, *Some Diophantine equations related to the quadratic form* ax^2+by^2, Studies in algebra and number theory, 219–272, edited by Gian-Carlo Rota, Advances in Mathematics, Supp. Studies, **6**, Academic Press, New York-London, 1979.

[2] P.E. Conner, J. Hurrelbrink, *Class Number Parity*, Ser. Pure Math. **8**, World Sci., Singapore, 1988.

[3] D. Cox, *Primes of Form* $x^2 + ny^2$, John Wiley & Sons, Inc, New York, 1989.

[4] G.L. Dirichlet, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres (Première Partie)*, J. reine angew. Math. **19** (1839), 324–369.

[5] M. Kurihara, *Some remarks on conjectures about cyclotomic fields and K-groups of* $\mathbb{Z}$, Compositio Math. **81** (1992), 223–236.

[6] C. Soulé, *Perfect forms and Vandiver's conjecture*, J. Reine Angew. Math. **517** (1999), 209–221.

[7] L. Stickelberger, *Über eine Verallgemeinerung der Kreistheilung*, Math. Ann. **37** (1890), 321–367.

[8] F. Thaine, *On Gaussian periods that are rational integers*, Michigan Math. J. **50** (2002), 313–337.

[9] L. Washington, *Introduction to cyclotomic fields*, 2nd ed., Grad. Texts in Math., **83**, Springer-Verlag, New York, 1997.

Max-Planck Institut für Mathematik, Vivatsgasse 7, 53111 Bonn, Germany
E-mail address: osburn@mpim-bonn.mpg.de