NOTE ON A DETERMINANT (II)

Benjamin Dupuy
Laboratoire de mathématiques Mathmax de Libourne, Libourne, France
benjamin.dupuy1@ac-bordeaux.fr

Received: 11/1/20, Accepted: 5/30/21, Published: 6/3/21

Abstract

In this paper, we give the value of some determinants in terms of the p-relative class number where p is a prime number such that $p \equiv 3 \bmod 4$.

1. Introduction

Let p be an odd prime number, $\mathbb{F}_p$ be the field of p elements, $\zeta = \mathrm{e}^{\frac{2i\pi}{p}}$ and g be a primitive element of $\mathbb{F}_p^\times$. The extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension. Let $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right)$ be defined by $\zeta^\sigma = \zeta^{g^2}$. Recall that $\mathrm{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right) \simeq \mathbb{F}_p^\times$.

For $a \in \mathbb{F}_p^\times$ and $b \in \mathbb{Q}$, we denote by $\mathcal{D}_g\left(p,a,b\right)$ the circulant determinant whose first line is given by

$$\frac{1}{b-\zeta^a} - \frac{1}{b-\zeta^{-a}} \quad \frac{1}{b-\zeta^{a\sigma}} - \frac{1}{b-\zeta^{-a\sigma}} \cdots \frac{1}{b-\zeta^{a\sigma^{\frac{p-3}{2}}}} - \frac{1}{b-\zeta^{-a\sigma^{\frac{p-3}{2}}}}.$$

The determinant $\mathcal{D}_g\left(p,a,b\right)$ does not depend on the choice of the value of g (see [2]): consequently, it will be denoted in the following by $\mathcal{D}\left(p,a,b\right)$. It has been proved in [2] that there exists $d\left(p,a,b\right) \in \mathbb{Q}$ such that

$$\mathcal{D}(p,a,b) = d\left(p,a,b\right)\sqrt{-p}$$

with

$$d\left(p,a,b\right) = \begin{cases} 0 & \text{if } p \equiv 1 \bmod 4, \\ (-1)^{\frac{p-3}{4}} \times 2^{\frac{p-3}{2}} \times p^{\frac{p-7}{4}} \times h_p^- \times \left(\frac{a}{p}\right) & \text{if } p \equiv 3 \bmod 4 \text{ and } b = 1, \end{cases}$$

where h_p^- is the p-th relative class number. In this paper, we prove the following theorem.

Theorem 1. *Let p be a prime number such that $p \equiv 3 \bmod 4$. Let n be the order* *of* 2 *modulo* p*. We have:*

$$d\left(p,a,-1\right)=\begin{cases}(-1)^{\frac{p-3}{4}}\times\left(\frac{a}{p}\right)\times p^{\frac{p-7}{4}}\times 2^{\frac{p-3}{2}}\times h_p^-\times\left(1+2^{\frac{n}{2}}\right)^{\frac{p-1}{n}} & \textit{if } 2 \textit{ is not a square modulo } p,\\ (-1)^{\frac{p-3}{4}}\times\left(\frac{a}{p}\right)\times p^{\frac{p-7}{4}}\times 2^{\frac{p-3}{2}}\times h_p^-\times\left(1-2^{n}\right)^{\frac{p-1}{2n}} & \textit{otherwise.}\end{cases}$$

For example, for $p=7$, $a=1$ and $5 \bmod 7$ being a primitive element of $\mathbb{F}_7^{\times}$, $\mathcal{D}\left(7,1,-1\right)$ is defined by

$$\mathcal{D}\left(7,1,-1\right)=\begin{vmatrix}\frac{1}{-1-\zeta}-\frac{1}{-1-\overline{\zeta}} & \frac{1}{-1-\zeta^4}-\frac{1}{-1-\overline{\zeta^4}} & \frac{1}{-1-\zeta^2}-\frac{1}{-1-\overline{\zeta^2}}\\ \frac{1}{-1-\zeta^2}-\frac{1}{-1-\overline{\zeta^2}} & \frac{1}{-1-\zeta}-\frac{1}{-1-\overline{\zeta}} & \frac{1}{-1-\zeta^4}-\frac{1}{-1-\overline{\zeta^4}}\\ \frac{1}{-1-\zeta^4}-\frac{1}{-1-\overline{\zeta^4}} & \frac{1}{-1-\zeta^2}-\frac{1}{-1-\overline{\zeta^2}} & \frac{1}{-1-\zeta}-\frac{1}{-1-\overline{\zeta}}\end{vmatrix}.$$

The integer 2 is a square modulo 7 and 3 is the order of 2 modulo 7. By Theorem 1, this determinant is given by

$$\mathcal{D}\left(7,1,-1\right)=(-1)^{\frac{7-3}{4}}\times\left(\frac{1}{7}\right)\times 7^{\frac{7-7}{4}}\times 2^{\frac{7-3}{2}}\times h_7^-\times\left(1-2^3\right)^{\frac{7-1}{2\times 3}}\sqrt{-7}=28\sqrt{-7}.$$

Using Theorem 1, we deduce this beautiful corollary.

Corollary 1. *Suppose* $p>3$ *and* $p\equiv 3 \bmod 4$*. Let* $\mathcal{C}\left(p,a\right)$ *be the circulant determinant whose first line is given by*

$$\frac{1}{1+\zeta^a}\quad\frac{1}{1+\zeta^{a\sigma}}\cdots\frac{1}{1+\zeta^{a\sigma^{\frac{p-3}{2}}}}$$

and $h(-p)$ *be the class number of* $\mathbb{Q}\left(\sqrt{-p}\right)$*. We have the following result:*

$$\mathcal{C}\left(p,a\right)=\left(\frac{p-1}{4h(-p)\left(1-2\left(\frac{2}{p}\right)\right)}-\left(\frac{a}{p}\right)\frac{\sqrt{-p}}{2}\right)\frac{d\left(p,1,-1\right)}{2^{\frac{p-3}{2}}}.\qquad(1)$$

2. Five Useful Lemmas

Lemma 1 ([3])**.** *Let* χ *be an odd character of conductor* $f_\chi\neq 2 \bmod 4$*. Let* S_χ *be the sum defined by*

$$\mathcal{S}_\chi=\sum_{1\leq x\leq\frac{f_\chi}{2}}\chi(x).$$

We have

$$\mathcal{B}_{1,\chi}=-\frac{1}{2-\overline{\chi}(2)}\mathcal{S}_\chi,$$

where $\mathcal{B}_{1,\chi}$ *is a generalized Bernoulli number (see [5]).*

Lemma 2 ([4, Lemma 1]). *Let* $\tau_n = \boldsymbol{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{\zeta^n}{1+\zeta}\right)$ *be the relative trace of* $\frac{\zeta^n}{1+\zeta}$ *for* $n = 1, ..., p-1$. *Then*

$$\tau_n = \begin{cases} \frac{p-1}{2} & \text{if } n \equiv 1 \bmod 2, \\ -\frac{p+1}{2} & \text{if } n \equiv 0 \bmod 2. \end{cases}$$

Lemma 3. *Let* G *be a finite abelian group and* $\widehat{G}$ *its group of characters. Let* g *be an element of* G *and* n *its order. Then*

$$for\ all\ Z \in \mathbb{C}, \quad \prod_{\chi \in \widehat{G}} (1 - \chi(g)Z) = (1 - Z^n)^{\frac{|G|}{n}}.$$

Proof. Let μ_n be the group of n-th roots of unity. We have

$$for\ all\ Z \in \mathbb{C}, \quad \prod_{w \in \mu_n} (1 - wZ) = 1 - Z^n.$$

Let $w \in \mu_n$. There exist exactly $\frac{|G|}{n}$ characters χ of $\widehat{G}$ such that $\chi(g) = w$, so that

$$for\ all\ Z \in \mathbb{C}, \quad \prod_{\chi \in \widehat{G}} (1 - \chi(g)Z) = \left(\prod_{w \in \mu_n} (1 - wZ)\right)^{\frac{|G|}{n}} = (1 - Z^n)^{\frac{|G|}{n}}.$$

□

Lemma 4. *Let* p *be a prime number,* $p \equiv 3 \bmod 4$. *Let* n *be the order of* 2 *modulo* p. *Denote by* $\widehat{\mathbb{F}_p^\times}^-$ *the set of odd characters of* $\mathbb{F}_p^\times$. *Then*

$$\prod_{\chi \in \widehat{\mathbb{F}_p^\times}^-} (1 - 2\chi(2)) = \begin{cases} (1 - 2^n)^{\frac{p-1}{2n}} & \text{if } 2 \text{ is a square modulo } p, \\ \left(1 + 2^{\frac{n}{2}}\right)^{\frac{p-1}{n}} & \text{otherwise.} \end{cases}$$

Proof. By Lemma 3,

$$\prod_{\chi \in \widehat{\mathbb{F}_p^\times}} (1 - 2\chi(2)) = (1 - 2^n)^{\frac{p-1}{n}}.$$

• Let C be the group of nonzero squares modulo p. Suppose that $2 \in C$. Denote by $\widehat{\mathbb{F}_p^\times}^+$ the group of even characters of $\mathbb{F}_p^\times$ and by $\widehat{C}$ the group of characters of C. By Lemma 3

$$\prod_{\chi \in \widehat{\mathbb{F}_p^\times}^+} (1 - 2\chi(2)) = \prod_{\chi \in \widehat{C}} (1 - 2\chi(2)) = (1 - 2^n)^{\frac{p-1}{2n}}$$

so that

$$\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}(1-2\chi(2))=\frac{\prod_{\chi\in\widehat{\mathbb{F}_p^\times}}(1-2\chi(2))}{\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^+}(1-2\chi(2))}$$
$$=\frac{(1-2^n)^{\frac{p-1}{n}}}{(1-2^n)^{\frac{p-1}{2n}}}$$
$$=(1-2^n)^{\frac{p-1}{2n}}.$$

• Suppose that $2\notin C$. In this case, $-2\in C$. Let n' be the order of -2 modulo p. From the equality $2=(-1)\times(-2)$ and from the fact that $\frac{p-1}{2}$ and 2 are coprime integers (since $p\equiv 3 \bmod 4$), we deduce that $n=2n'$. Then, by Lemma 3

$$\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^+}(1-2\chi(2))=\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^+}(1-2\chi(-2))=\prod_{\chi\in\widehat{C}}(1-2\chi(-2))$$
$$=\left(1-2^{\frac{n}{2}}\right)^{\frac{p-1}{2\times\frac{n}{2}}}=\left(1-2^{\frac{n}{2}}\right)^{\frac{p-1}{n}},$$

so that

$$\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}(1-2\chi(2))=\frac{\prod_{\chi\in\widehat{\mathbb{F}_p^\times}}(1-2\chi(2))}{\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^+}(1-2\chi(2))}=\frac{(1-2^n)^{\frac{p-1}{n}}}{\left(1-2^{\frac{n}{2}}\right)^{\frac{p-1}{n}}}=\left(1+2^{\frac{n}{2}}\right)^{\frac{p-1}{n}}.$$

The lemma is proved. □

Lemma 5. *Let $p>2$ be a prime number. Let $\chi\in\widehat{\mathbb{F}_p^\times}$ be a nontrivial character. Then*

$$\tau\left(\overline{\chi}\right)\sum_{x=1}^{p-1}\frac{\chi(x)}{1+\zeta^x}=p\left(2\overline{\chi}(2)-1\right)\mathcal{B}_{1,\overline{\chi}},$$

where $\tau\left(\overline{\chi}\right)$ is a Gauss sum defined by

$$\tau\left(\overline{\chi}\right)=\sum_{y=1}^{p-1}\overline{\chi}(y)\zeta^y.$$

Proof. In this proof, for an integer y coprime with p, we denote by y^{-1} the inverse of y modulo p. We have

$$\begin{aligned}\tau\left(\overline{\chi}\right)\sum_{x=1}^{p-1}\frac{\chi(x)}{1+\zeta^x} &= \sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\frac{\chi(x)\overline{\chi}(y)\zeta^y}{1+\zeta^x} = \sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\frac{\chi(xy^{-1})\zeta^y}{1+\zeta^x} = \sum_{z=1}^{p-1}\sum_{y=1}^{p-1}\frac{\chi(z)\zeta^y}{1+\zeta^{yz}}\\ &= \sum_{z=1}^{p-1}\chi(z)\mathbf{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{\zeta^{z^{-1}}}{1+\zeta}\right) = \sum_{z=1}^{p-1}\overline{\chi}(z)\mathbf{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{\zeta^z}{1+\zeta}\right)\\ &= \sum_{1\leq z<p, z\equiv 0 \bmod 2}\overline{\chi}(z)\mathbf{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{\zeta^z}{1+\zeta}\right)\\ &+ \sum_{1\leq z<p, z\equiv 1 \bmod 2}\overline{\chi}(z)\mathbf{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{\zeta^z}{1+\zeta}\right).\end{aligned}$$

By Lemma 2, if z is an integer such that $1 \leq z < p$, we have

$$\mathbf{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{\zeta^z}{1+\zeta}\right) = \begin{cases} \frac{p-1}{2} & \text{if } z \equiv 1 \bmod 2,\\ \frac{p-1}{2} - p & \text{if } z \equiv 0 \bmod 2,\end{cases}$$

so that

$$\begin{aligned}\tau\left(\overline{\chi}\right)\sum_{x=1}^{p-1}\frac{\chi(x)}{1+\zeta^x} &= \sum_{1\leq z<p, z\equiv 0 \bmod 2}\overline{\chi}(z)\left(\frac{p-1}{2}-p\right) + \sum_{1\leq z<p, z\equiv 1 \bmod 2}\overline{\chi}(z)\frac{p-1}{2}\\ &= \frac{p-1}{2}\sum_{z=1}^{p-1}\overline{\chi}(z) - p\sum_{1\leq z<p, z\equiv 0 \bmod 2}\overline{\chi}(z).\end{aligned}$$

The character χ being a nontrivial character, we have

$$\sum_{z=1}^{p-1}\overline{\chi}(z) = 0,$$

so that

$$\tau\left(\overline{\chi}\right)\sum_{x=1}^{p-1}\frac{\chi(x)}{1+\zeta^x} = -p\sum_{1\leq z<p, z\equiv 0 \bmod 2}\overline{\chi}(z) = -p\overline{\chi}(2)\sum_{1\leq x<\frac{p}{2}}\overline{\chi}(x).$$

By Lemma 1

$$-p\overline{\chi}(2)\sum_{1\leq x<\frac{p}{2}}\overline{\chi}(x) = p\overline{\chi}(2)(2-\chi(2))\mathcal{B}_{1,\overline{\chi}} = p(2\overline{\chi}(2)-1)\mathcal{B}_{1,\overline{\chi}}.$$

The lemma is proved. □

3. Proof of the Theorem

We first show that

$$d\left(p,1,-1\right)=\begin{cases}(-1)^{\frac{p-3}{4}}\times p^{\frac{p-7}{4}}\times 2^{\frac{p-3}{2}}\times h_p^-\times\left(1+2^{\frac{n}{2}}\right)^{\frac{p-1}{n}} & \text{if 2 is not a square modulo } p,\\ (-1)^{\frac{p-3}{4}}\times p^{\frac{p-7}{4}}\times 2^{\frac{p-3}{2}}\times h_p^-\times\left(1-2^{n}\right)^{\frac{p-1}{2n}} & \text{otherwise.}\end{cases}$$

Let ξ be a primitive $\frac{p-1}{2}$-th root of unity. Let $P\in\mathbb{Q}\left(\zeta\right)[X]$ defined by

$$P(X)=\sum_{k=0}^{\frac{p-3}{2}}\left(\frac{1}{1+\zeta^{\sigma^k}}-\frac{1}{1+\zeta^{-\sigma^k}}\right)X^k.$$

By a well known result,

$$\mathcal{D}\left(p,1,-1\right)=\prod_{l=0}^{\frac{p-3}{2}}-P\left(\xi^l\right)=\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}-\sum_{x=1}^{p-1}\frac{\chi(x)}{1+\zeta^x},$$

so that

$$\begin{aligned}\mathcal{D}\left(p,1,-1\right)\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}\tau(\chi)&=\mathcal{D}\left(p,1,-1\right)\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}\tau(\overline{\chi})\\&=\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}-\tau(\overline{\chi})\sum_{x=1}^{p-1}\frac{\chi(x)}{1+\zeta^x}.\end{aligned}$$

By Lemma 5

$$\begin{aligned}\mathcal{D}\left(p,1,-1\right)\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}\tau(\chi)&=\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}-p\left(2\overline{\chi}(2)-1\right)\mathcal{B}_{1,\overline{\chi}}\\&=p^{\frac{p-1}{2}}\times\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}(1-2\overline{\chi}(2))\times\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}\mathcal{B}_{1,\overline{\chi}}\\&=p^{\frac{p-1}{2}}\times\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}(1-2\chi(2))\times\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}\mathcal{B}_{1,\chi}.\end{aligned}$$

By Theorem 4.17 of [5],

$$\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}B_{1,\chi}=-\frac{2^{\frac{p-3}{2}}h_p^-}{p}.\tag{2}$$

By Corollary 4.6 of [5]

$$\prod_{\chi\in\widehat{\mathbb{F}_p^\times}}\tau(\chi)=(-1)^{\frac{p-3}{4}}p^{\frac{p-2}{2}}\sqrt{-1},\qquad \prod_{\chi\in\widehat{\mathbb{F}_p^\times}^+}\tau(\chi)=p^{\frac{p-3}{4}},$$

so that

$$\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}\tau(\chi)=\frac{(-1)^{\frac{p-3}{4}}p^{\frac{p-2}{2}}\sqrt{-1}}{p^{\frac{p-3}{4}}}=(-1)^{\frac{p-3}{4}}\sqrt{-1}p^{\frac{p-1}{4}}. \tag{3}$$

From (2) and (3), we deduce that

$$\begin{aligned}\mathcal{D}(p,1,-1)\times(-1)^{\frac{p-3}{4}}\sqrt{-1}p^{\frac{p-1}{4}}&=p^{\frac{p-1}{2}}\times\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}(1-2\chi(2))\times\left(-\frac{2^{\frac{p-3}{2}}h_p^-}{p}\right)\\&=-(2p)^{\frac{p-3}{2}}\times h_p^-\times\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}(1-2\chi(2)),\end{aligned}$$

so that

$$\mathcal{D}(p,1,-1)=(-1)^{\frac{p-3}{4}}\times2^{\frac{p-3}{2}}\times p^{\frac{p-7}{4}}\times h_p^-\times\sqrt{-p}\times\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}(1-2\chi(2)).$$

By Lemma 4,

$$\mathcal{D}(p,1,-1)=\begin{cases}(-1)^{\frac{p-3}{4}}\times2^{\frac{p-3}{2}}\times p^{\frac{p-7}{4}}\times h_p^-\times\left(1+2^{\frac{n}{2}}\right)^{\frac{p-1}{n}}\times\sqrt{-p} & \text{if 2 is not a square modulo } p,\\(-1)^{\frac{p-3}{4}}\times2^{\frac{p-3}{2}}\times p^{\frac{p-7}{4}}\times h_p^-\times(1-2^n)^{\frac{p-1}{2n}}\times\sqrt{-p} & \text{otherwise.}\end{cases}$$

Let $a\in\mathbb{F}_p^\times$ be a square modulo p. As $p\equiv3\bmod4$, to terminate the proof of the theorem, it suffices to prove that

$$\mathcal{D}(p,a,-1)=\mathcal{D}(p,1,-1),\quad \mathcal{D}(p,-a,-1)=-\mathcal{D}(p,1,-1).$$

Let $\tau\in\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ be defined by $\zeta^\tau=\zeta^a$. The automorphism τ is an element of $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{-p}))$ since $p\equiv3\bmod4$. We have $\mathcal{D}(p,a,-1)=\mathcal{D}(p,1,-1)^\tau$ with $\mathcal{D}(p,1,-1)\in\mathbb{Q}(\sqrt{-p})$ so that

$$\mathcal{D}(p,a,-1)=\mathcal{D}(p,1,-1).$$

We have $\mathcal{D}(p,-a,-1)=\mathcal{D}(p,-1,-1)^\tau$. By Theorem 1 of [2], $\mathcal{D}(p,-1,-1)$ is an element of $\mathbb{Q}(\sqrt{-p})$ so that

$$\mathcal{D}(p,-a,-1)=\mathcal{D}(p,-1,-1)^\tau=\mathcal{D}(p,-1,-1).$$

We obtain, j being the complex conjugation

$$\mathcal{D}\left(p,-a,-1\right)=\mathcal{D}\left(p,-1,-1\right)=\mathcal{D}\left(p,1,-1\right)^{j}=\left(-1\right)^{\frac{p-1}{2}}\mathcal{D}\left(p,1,-1\right).$$

As $p\equiv 3 \bmod 4$, $\frac{p-1}{2}$ is an odd integer, so that

$$\mathcal{D}\left(p,-a,-1\right)=-\mathcal{D}\left(p,1,-1\right).$$

The theorem is proved. □

4. Proof of the Corollary

To prove (1), it is sufficient to prove that

$$\mathcal{C}\left(p,1\right)=\left(\frac{p-1}{4h(-p)\left(1-2\left(\frac{2}{p}\right)\right)}-\frac{\sqrt{-p}}{2}\right)\frac{d\left(p,1,-1\right)}{2^{\frac{p-3}{2}}}.$$

Consider the polynomial

$$Q(X)=\sum_{l=0}^{\frac{p-3}{2}}\frac{1}{1+\zeta^{\sigma^{l}}}X^{l}\in\mathbb{Q}\left(\zeta\right)[X].$$

The determinant $\mathcal{C}\left(p,1\right)$ being a circulant determinant,

$$\mathcal{C}\left(p,1\right)=\prod_{k=0}^{\frac{p-3}{2}}Q\left(\xi^{k}\right).$$

Let k be a rational integer such that $0<k\leq\frac{p-3}{2}$. The equality $\sum_{l=0}^{\frac{p-3}{2}}\xi^{kl}=0$ implies that $Q\left(\xi^{k}\right)=\frac{1}{2}P\left(\xi^{k}\right)$, so that

$$\begin{aligned}\mathcal{C}\left(p,1\right)&=\frac{Q(1)}{2^{\frac{p-3}{2}}P(1)}\prod_{k=0}^{\frac{p-3}{2}}P\left(\xi^{k}\right)=\frac{(-1)^{\frac{p-1}{2}}Q(1)}{2^{\frac{p-3}{2}}P(1)}\prod_{k=0}^{\frac{p-3}{2}}-P\left(\xi^{k}\right)\\&=-\frac{Q(1)}{2^{\frac{p-3}{2}}P(1)}\mathcal{D}\left(p,1,-1\right)=-\frac{Q(1)}{2^{\frac{p-3}{2}}P(1)}d\left(p,1,-1\right)\sqrt{-p}.\end{aligned}$$

We have $P(1)=\sum_{x=1}^{p-1}\frac{\left(\frac{x}{p}\right)}{1+\zeta^{x}}$. By Lemma 5,

$$P(1)=-\sqrt{-p}\left(2\left(\frac{2}{p}\right)-1\right)\mathcal{B}_{1,\left(\frac{\cdot}{p}\right)}$$

so that

$$P(1) = h(-p)\left(2\left(\frac{2}{p}\right) - 1\right)\sqrt{-p}, \tag{4}$$

by Theorem 4.17 of [5]. Recall that C is the group of nonzero squares modulo p. We have

$$\begin{aligned} 2Q(1) &= 2\sum_{x\in C}\frac{1}{1+\zeta^x} = \sum_{x=1}^{p-1}\frac{1}{1+\zeta^x} + \sum_{x=1}^{p-1}\frac{\left(\frac{x}{p}\right)}{1+\zeta^x} = \mathbf{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{1}{1+\zeta}\right) + P(1) \\ &= \frac{p-1}{2} + h(-p)\left(2\left(\frac{2}{p}\right) - 1\right)\sqrt{-p}, \end{aligned}$$

using Lemma 1 of [4] and (4), so that

$$\begin{aligned} \mathcal{C}(p,1) &= -\frac{Q(1)}{2^{\frac{p-3}{2}}P(1)}d(p,1,-1)\sqrt{-p} = -\frac{\frac{p-1}{4} + h(-p)\left(2\left(\frac{2}{p}\right)-1\right)\frac{\sqrt{-p}}{2}}{2^{\frac{p-3}{2}}h(-p)\left(2\left(\frac{2}{p}\right)-1\right)}d(p,1,-1) \\ &= \left(\frac{p-1}{4h(-p)\left(1-2\left(\frac{2}{p}\right)\right)} - \frac{\sqrt{-p}}{2}\right)\frac{d(p,1,-1)}{2^{\frac{p-3}{2}}}. \end{aligned}$$

□

Acknowledgements. I thank the referee and the editor for many useful remarks.

References

[1] Cohen, H., *Number Theory*, Springer, New York, 2007.

[2] Dupuy, B., Note on a determinant, *Integers* **20** (2020), #A48.

[3] Long, R. L., *Algebraic Number Theory*, Monographs and textbooks in pure and applied mathematics **41**, M. Dekker, 1977.

[4] Mihailescu, P., New bounds and conditions for the equation of Nagell-Ljunggren, *J. Number Theory* **124** (2007), 380-395.

[5] Washington, L., *Introduction to Cyclotomic Fields*, Springer, Berlin, second edition, 1997.