NOTE ON A DETERMINANT

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

Received: 6/13/19, Accepted: 6/10/20, Published: 6/18/20

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 $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right)$ defined by $\zeta^\sigma = \zeta^{g^2}$. Recall that $\mathrm{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right) \simeq \mathbb{F}_p^\times$. In this paper, 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

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

In this paper, we prove the following theorem.

Theorem 1. *We have the following properties:*

1. *We have $\mathcal{D}_g\left(p,a,b\right) = 0$ if $p \equiv 1 \bmod 4$.*
2. *Suppose $p \equiv 3 \bmod 4$. The determinant $\mathcal{D}_g\left(p,a,b\right)$ does not depend on the choice of the value of g: consequently, it will be denoted in the following by $\mathcal{D}\left(p,a,b\right)$. There exists $d\left(p,a,b\right) \in \mathbb{Q}$ such that $\mathcal{D}\left(p,a,b\right) = d\left(p,a,b\right)\sqrt{-p}$. Furthermore,*

$$d\left(p,a,1\right) = (-1)^{\frac{p-3}{4}} \times 2^{\frac{p-3}{2}} \times p^{\frac{p-7}{4}} \times h_p^- \times \left(\frac{a}{p}\right),$$

where h_p^- is the p-th relative class number.

Remark 1. The case $b = -1$ is technically more involved and will be the aim of another paper.

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

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

By Theorem 1, this determinant is given by

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

Using Theorem 1, we deduce this beautiful corollary.

Corollary 1. *Suppose $p>3$ and $p\equiv 3 \bmod 4$. Let $\mathcal{C}(p,a)$ 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 $\mathbb{Q}(\sqrt{-p})$. We have the following result:

$$\mathcal{C}(p,a)=(-1)^{\frac{p-3}{4}}p^{\frac{p-7}{4}}h_p^-\left(\frac{p-1}{4h(-p)}+\left(\frac{a}{p}\right)\frac{\sqrt{-p}}{2}\right). \tag{1}$$

In 1851, Kummer (see [3], p.473) conjectured that $h_p^-\sim 2p\left(\frac{p}{4\pi^2}\right)^{\frac{p-1}{4}}=G(p)$ as $p\to+\infty$. For all rational integers ν such that $0\leq\nu\leq\frac{p-3}{2}$, denote by g_ν the rational integer such that $1\leq g_\nu<p$, $\quad g_\nu\equiv g^{2\nu} \bmod p$ (particularly, $g_0=1$). Denote by $\mathcal{T}_p$ the circulant determinant whose first line is given by

$$\frac{1}{\tan\left(\frac{\pi}{p}\right)}\quad\frac{1}{\tan\left(\frac{\pi}{p}g_1\right)}\cdots\frac{1}{\tan\left(\frac{\pi}{p}g_{\frac{p-3}{2}}\right)}.$$

From Theorem 1, we deduce the following result.

Corollary 2. *Denote by $(p_j)_{j\geq 1}$ the sequence of prime numbers p such that $p\equiv 3 \bmod 4$ (so that $p_1=3$, $p_2=7$ and so on). Kummer's conjecture is true for this set of prime numbers if and only if $\mathcal{T}_{p_j}\sim\left(\frac{p_j}{\pi}\right)^{\frac{p_j-1}{2}}$ as $j\to+\infty$.*

2. Two Useful Lemmas

Lemma 1. *Let $x\in\mathbb{F}_p^{\times}$. We have*

$$\sum_{j=1}^{p-1}j\zeta^{jx}=-\frac{p}{1-\zeta^x}.$$

Proof. Let Φ_p be the p-th cyclotomic polynomial. We have

$$\sum_{j=1}^{p-1} j\zeta^{jx} = \zeta^x \Phi_p'(\zeta^x) = \frac{p}{\zeta^x - 1}.$$

□

Lemma 2. *Let $\chi \in \widehat{\mathbb{F}_p^\times}$ be a non trivial character and $\mathcal{S}(\chi)$ be the sum defined by*

$$\mathcal{S}(\chi) = \sum_{x=1}^{p-1} \frac{\chi(x)}{1-\zeta^x}.$$

We have

$$\mathcal{S}(\chi) = -B_{1,\overline{\chi}} \times \tau(\chi),$$

where $B_{1,\overline{\chi}}$ is a generalized Bernoulli number (see [5]) and $\tau(\chi)$ is a Gauss sum defined by

$$\tau(\chi) = \sum_{x=1}^{p-1} \chi(x)\zeta^x.$$

Proof. Using Lemma 1, we obtain

$$\begin{aligned} -p\mathcal{S}(\chi) &= \sum_{x=1}^{p-1} \chi(x) \frac{-p}{1-\zeta^x} = \sum_{x=1}^{p-1} \chi(x) \sum_{j=1}^{p-1} j\zeta^{jx} \\ &= \sum_{j=1}^{p-1} j \sum_{x=1}^{p-1} \chi(x)\zeta^{jx} = \sum_{j=1}^{p-1} j\overline{\chi(j)} \sum_{x=1}^{p-1} \chi(jx)\zeta^{jx} \\ &= p\left(\frac{1}{p}\sum_{j=1}^{p-1} j\overline{\chi(j)}\right) \times \sum_{x=1}^{p-1} \chi(x)\zeta^x = pB_{1,\overline{\chi}} \times \tau(\chi). \end{aligned}$$

□

3. Proof of the First Part of the Theorem

Suppose $p \equiv 1 \bmod 4$. Let ξ be a $\frac{p-1}{2}$-th root of unity and $Z_{b,a} = \frac{1}{b-\zeta^a} - \frac{1}{b-\zeta^{-a}}$. Consider the polynomial

$$P_{b,a}(X) = \sum_{l=0}^{\frac{p-3}{2}} Z_{b,a}^{\sigma^l} X^l \in \mathbb{Q}(\zeta)[X].$$

$\mathcal{D}_g(p,a,b)$ being a circulant determinant, by a well known result, we have

$$\mathcal{D}_g(p,a,b)=\prod_{k=0}^{\frac{p-3}{2}}P_{b,a}\left(\xi^k\right). \tag{2}$$

Let $\mathcal{C}$ be the set of squares modulo p. Since $p\equiv 1 \bmod 4$, we have $-1\in\mathcal{C}$ so that

$$\begin{aligned}P_{b,a}(1)&=\sum_{c\in\mathcal{C}}\frac{1}{b-\zeta^{ac}}-\sum_{c\in\mathcal{C}}\frac{1}{b-\zeta^{-ac}}=\sum_{c\in\mathcal{C}}\frac{1}{b-\zeta^{ac}}-\sum_{c\in\mathcal{C}}\frac{1}{b-\zeta^{ac}}\\&=0.\end{aligned}$$

This proves that $\mathcal{D}_g(p,a,b)=0$ for $p\equiv 1 \bmod 4$. □

4. Proof of the Second Part of the Theorem

Suppose $p\equiv 3 \bmod 4$. Denote by $\widehat{\mathbb{F}_p^\times}^-$ (respectively $\widehat{\mathbb{F}_p^\times}^+$) the set of odd characters (respectively even characters) of $\mathbb{F}_p^\times$. From equality (2)

$$\mathcal{D}_g(p,a,b)=\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-}\sum_{x=1}^{p-1}\frac{\chi(x)}{b-\zeta^{ax}},$$

which proves that $\mathcal{D}_g(p,a,b)$ does not depend on the choice of the value of g.

Recall that $\sigma\in G$ is defined by $\zeta^\sigma=\zeta^{g^2}$. Let j be the complex conjugation. It is not difficult to see that $\mathcal{D}(p,a,b)^\sigma=\mathcal{D}(p,a,b)$ and $\mathcal{D}(p,a,b)^j=-\mathcal{D}(p,a,b)$. By a well known fact, as $p\equiv 3 \bmod 4$, the field $\mathbb{Q}(\sqrt{-p})$ is a subfield of $\mathbb{Q}(\zeta)$ and the extension $\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{-p})$ is a cyclic extension whose Galois group is generated by σ. As $\mathcal{D}(p,a,b)^\sigma=\mathcal{D}(p,a,b)$, $\mathcal{D}(p,a,b)$ is fixed by every automorphism in $\mathrm{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{-p})\right)$. By Galois theory, $\mathcal{D}(p,a,b)$ is an element of $\mathbb{Q}(\sqrt{-p})$. In other words, there exists $d(p,a,b)\in\mathbb{Q}$ and $e(p,a,b)\in\mathbb{Q}$ such that

$$\mathcal{D}(p,a,b)=e(p,a,b)+d(p,a,b)\sqrt{-p}.$$

But $\mathcal{D}(p,a,b)^j=-\mathcal{D}(p,a,b)$ so that $e(p,a,b)=0$. Finally,

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

Show that

$$d(p,1,1)=(-1)^{\frac{p-3}{4}}\times 2^{\frac{p-3}{2}}\times p^{\frac{p-7}{4}}\times h_p^-.$$

From equality (2) and Lemma 2, we deduce that

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

By Corollary 4.6 of [5] or Theorem 11.7.16 of [1],

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

so that

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

By Theorem 4.17 of [5],

$$\prod_{\chi\in\widehat{\mathbb{F}_p^\times}^-} -\frac{1}{2}B_{1,\chi} = \frac{h_p^-}{2p}. \tag{4}$$

From (3) and (4), we deduce that

$$\begin{aligned}\mathcal{D}(p,1,1) &= 2^{\frac{p-1}{2}}(-1)^{\frac{p-3}{4}}\sqrt{-1}p^{\frac{p-1}{4}}\frac{h_p^-}{2p}\\ &= (-1)^{\frac{p-3}{4}}2^{\frac{p-3}{2}}p^{\frac{p-7}{4}}h_p^-\sqrt{-p}.\end{aligned}$$

Let $a\in\mathbb{F}_p^\times$ be a square modulo p. As $p\equiv 3 \bmod 4$, 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 $\tau\in\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ defined by $\zeta^\tau = \zeta^a$. 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 $\mathcal{D}(p,-a,1) = \mathcal{D}(p,-1,1)^\tau$ with $\mathcal{D}(p,-1,1)\in\mathbb{Q}(\sqrt{-p})$ so that

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

We obtain, j being the complex conjugation

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

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

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

The theorem is proved. □

5. Proof of Corollary 1

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

$$\mathcal{C}(p,1) = (-1)^{\frac{p-3}{4}} p^{\frac{p-7}{4}} h_p^- \left(\frac{p-1}{4h(-p)} + \frac{\sqrt{-p}}{2} \right).$$

Consider the polynomial

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

Since $\mathcal{C}(p,1)$ is a circulant determinant

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

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 $Q\left(\xi^k\right) = \frac{1}{2} P_{1,1}\left(\xi^k\right)$, so that

$$\begin{aligned}
\mathcal{C}(p,1) &= \frac{Q(1)}{2^{\frac{p-3}{2}} P_{1,1}(1)} \prod_{k=0}^{\frac{p-3}{2}} P_{1,1}\left(\xi^k\right) = \frac{Q(1)}{2^{\frac{p-3}{2}} P_{1,1}(1)} \mathcal{D}(p,1,1) \\
&= \frac{Q(1)}{2^{\frac{p-3}{2}} P_{1,1}(1)} \times (-1)^{\frac{p-3}{4}} 2^{\frac{p-3}{2}} p^{\frac{p-7}{4}} h_p^- \sqrt{-p} \\
&= (-1)^{\frac{p-3}{4}} p^{\frac{p-7}{4}} h_p^- \frac{Q(1)}{P_{1,1}(1)} \sqrt{-p}.
\end{aligned}$$

By Lemma 2, $P_{1,1}(1) = -B_{1,\left(\frac{\cdot}{p}\right)} \times \tau\left(\left(\frac{\cdot}{p}\right)\right)$ which implies that $P_{1,1}(1) = h(-p)\sqrt{-p}$ by Theorem 4.17 of [5] and Theorem 11.7.16 of [1]. Furthermore, we have

$$\begin{aligned}
2Q(1) &= P_{1,1}(1) + \sum_{k=1}^{p-1} \frac{1}{1-\zeta^k} = P_{1,1}(1) + \frac{\Phi_p'(1)}{\Phi_p(1)} \\
&= P_{1,1}(1) + \frac{p(p-1)}{2p} = \frac{p-1}{2} + h(-p)\sqrt{-p},
\end{aligned}$$

so that $Q(1) = \frac{p-1}{4} + \frac{h(-p)\sqrt{-p}}{2}$. Finally,

$$\begin{aligned}\mathcal{C}(p,1) &= (-1)^{\frac{p-3}{4}} p^{\frac{p-7}{4}} h_p^- \frac{\frac{p-1}{4} + \frac{h(-p)\sqrt{-p}}{2}}{h(-p)\sqrt{-p}} \sqrt{-p} \\ &= (-1)^{\frac{p-3}{4}} p^{\frac{p-7}{4}} h_p^- \left(\frac{p-1}{4h(-p)} + \frac{\sqrt{-p}}{2} \right).\end{aligned}$$

which concludes the proof. □

6. Proof of Corollary 2

We can easily see that $\mathcal{D}(p_j, 1, 1) = (-1)^{\frac{p_j-3}{4}} \sqrt{-1} \mathcal{T}_{p_j}$, so that, by Theorem 1,

$$\mathcal{T}_{p_j} = 2^{\frac{p_j-3}{2}} p_j^{\frac{p_j-7}{4}} h_{p_j}^- \sqrt{p_j} = \frac{h_{p_j}^-}{G(p_j)} \left(\frac{p_j}{\pi} \right)^{\frac{p_j-1}{2}},$$

which concludes the proof. □

Remark 2. Let $p \equiv 3 \bmod 4$ be a prime number. By Hadamard's inequality,

$$\mathcal{T}_p \leq \left(\sum_{\nu=0}^{\frac{p-3}{2}} \frac{1}{\tan^2\left(\frac{\pi}{p} g_\nu\right)} \right)^{\frac{p-1}{4}}, \tag{5}$$

with

$$\begin{aligned}\sum_{\nu=0}^{\frac{p-3}{2}} \frac{1}{\tan^2\left(\frac{\pi}{p} g_\nu\right)} &= \sum_{g_\nu < \frac{p}{2}} \frac{1}{\tan^2\left(\frac{\pi}{p} g_\nu\right)} + \sum_{g_\nu > \frac{p}{2}} \frac{1}{\tan^2\left(\frac{\pi}{p} g_\nu\right)} \\ &= \sum_{g_\nu < \frac{p}{2}} \frac{1}{\tan^2\left(\frac{\pi}{p} g_\nu\right)} + \sum_{g_\nu > \frac{p}{2}} \frac{1}{\tan^2\left(\frac{\pi}{p}(p - g_\nu)\right)} \\ &= \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{\tan^2\left(\frac{k\pi}{p}\right)} = \frac{(p-1)(p-2)}{6} \quad (see \quad [4]).\end{aligned}$$

Using (5) and Corollary 2, we obtain $2^{\frac{p-3}{2}} p^{\frac{p-7}{4}} h_p^- \sqrt{p} < \left(\frac{p^2}{6}\right)^{\frac{p-1}{4}}$, so that $h_p^- < 2p \left(\frac{p}{24}\right)^{\frac{p-1}{4}}$. Using much more sophisticated methods from analytic number theory, it has been proved in [2], that $h_p^- \leq 2p \left(\frac{p}{39}\right)^{\frac{p-1}{4}}$ if $p > 9649$.

Acknowledgments I thank the referee for helpful suggestions.

References

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

[2] K. Debaene, The first factor of the class number of the p-th cyclotomic field, *Arch. Math. (Basel)* **102** (2014), 237-244.

[3] E. Kummer, Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers, *J. Math. Pures Appl. (1)* **16** (1851), 377-498.

[4] I. Papadimitriou, A simple proof of the formula $\sum_{k=1}^{+\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$, *Amer. Math. Monthly* **80**, no. 4 (1973) 424-425.

[5] L. Washington, *Introduction to Cyclotomic Fields*, second edition, Springer, New York, 1996.