COLLOQUIUM MATHEMATICUM

Online First version

PRODUCTS OF QUADRATIC RESIDUES AND RELATED IDENTITIES

BY

HAI-LIANG WU and LI-YUAN WANG (Nanjing)

Abstract. We study products of quadratic residues modulo odd primes and prove some identities involving quadratic residues. For instance, let p be an odd prime. We prove that if $p \equiv 5 \pmod 8$, then

$$\prod_{0<x<p/2,\,(\frac{x}{p})=1} x \equiv (-1)^{1+r} \pmod p,$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol and r is the number of 4th power residues modulo p in the interval $(0, p/2)$. Our work involves the class number formula, quartic Gauss sums, Stickelberger's congruence and values of Dirichlet L-series at negative integers.

1. Introduction. The study of quadratic residues modulo odd primes is one of the most classical topics in number theory, and it has deep relations with other areas in number theory such as Gauss sums and permutations over finite fields. For example, Gauss in 1811 determined the explicit value of quadratic Gauss sums (cf. [9, Chapter 5]), i.e.,

$$\tau_p := \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) e^{2\pi k\mathbf{i}/p} = \sqrt{(-1)^{(p-1)/2}p},$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol and $\mathbf{i}$ is the primitive 4th root of unity with $\mathrm{Arg}(\mathbf{i}) \equiv \pi/2 \pmod{2\pi\mathbb{Z}}$ (where $\mathrm{Arg}(z)$ denotes the argument of a complex number z). We know that Gauss sums have many applications in number theory and in the study of finite fields. As another application of quadratic residues, Sun [16] investigated many permutations over finite fields involving squares in finite fields, and in the same year he studied in [15] some determinants involving the Legendre symbol.

Let p be a prime with $p \equiv 1 \pmod 4$, and let $\zeta_p = e^{2\pi\mathbf{i}/p}$ be the primitive pth root of unity. Sun [16] proved that

2020 *Mathematics Subject Classification*: Primary 11A15; Secondary 11R11, 11R18.
Key words and phrases: quadratic residues, cyclotomic fields, Gauss sums.
Received 8 November 2020; revised 12 January 2021.
Published online 28 May 2021.

DOI: 10.4064/cm8437-2-2021

$$\prod_{k=1}^{(p-1)/2}(1-\zeta_p^{k^2})=\begin{cases}\sqrt{p}\,\varepsilon_p^{-h(p)} & \text{if } p\equiv 1 \pmod 4,\\ (-1)^{(h(-p)+1)/2}\mathbf{i}\sqrt{p} & \text{if } p\equiv 3 \pmod 4,\end{cases}$$

where $\varepsilon_p>1$ and $h(p)$ are the fundamental unit and the class number of the real quadratic field $\mathbb{Q}(\sqrt{p})$ respectively, and $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. In the same paper he also proved the following results:

- If $p\equiv 1 \pmod 4$, then
$$\prod_{0<j<k<p/2}(\zeta_p^{j^2}-\zeta_p^{k^2})^2=(-1)^{(p-1)/4}p^{(p-3)/4}\varepsilon_p^{h(p)}.$$
- If $p\equiv 3 \pmod 4$, then
$$\prod_{0<j<k<p/2}(\zeta_p^{j^2}-\zeta_p^{k^2})=\begin{cases}(-p)^{(p-3)/8} & \text{if } 8\,|\,p-3,\\ (-1)^{(p+1)/8+(h(-p)-1)/2}p^{(p-3)/8} & \text{if } 8\,|\,p-7.\end{cases}$$

Let $\#S$ denote the cardinality of a set S. Petrov and Sun [14] obtained the following further results:

- If $p\equiv 1 \pmod 8$, then
$$\prod_{0<j<k<p/2}(\zeta_p^{j^2}+\zeta_p^{k^2})=(-1)^{\#\{1\le k<p/4:(\frac{k}{p})=-1\}}.$$
- If $p\equiv 5 \pmod 8$, then
$$(-1)^{\#\{1\le k<p/4:(\frac{k}{p})=-1\}}\prod_{0<j<k<p/2}(\zeta_p^{j^2}+\zeta_p^{k^2})=\varepsilon_p^{-h(p)}.$$

Now we present some earlier results on sums of quadratic residues. For any prime $p>3$, let

$$\mathcal{R}:=\left\{x\in\mathbb{Z}:\left(\frac{x}{p}\right)=1\right\}\quad\text{and}\quad\mathcal{N}:=\left\{x\in\mathbb{Z}:\left(\frac{x}{p}\right)=-1\right\}.$$

There are explicit formulas for the sums

$$A_p:=\sum_{0<x<p/2,\,x\in\mathcal{R}}x.$$

If we put

$$B_p:=\sum_{0<x<p/2,\,x\in\mathcal{N}}x,$$

then in view of

$$A_p+B_p=1+2+\cdots+\frac{p-1}{2}=\frac{p^2-1}{8}\tag{1.1}$$

it suffices to evaluate $A_p - B_p$. For $p \equiv 3 \pmod 4$ we have

$$A_p - B_p = \begin{cases} 0 & \text{if } p \equiv 7 \pmod 8, \\ ph(-p) & \text{if } p \equiv 3 \pmod 8, \end{cases} \tag{1.2}$$

which is a special case of the equation (23) in Lerch's paper [11].

To state the result for $p \equiv 1 \pmod 4$ we need to introduce Dirichlet L-series. Let

$$L\left(s, \left(\frac{\cdot}{p}\right)\right) = \sum_{n>0} \left(\frac{n}{p}\right) n^{-s}$$

be the Dirichlet L-series attached to the Legendre symbol $\left(\frac{\cdot}{p}\right)$, where s is any complex number with $\operatorname{Re} s > 1$. It is well known that $L(s, (\cdot/p))$ can be analytically continued to the whole complex plane. In the remaining part of this paper, we assume that $L(s, (\cdot/p))$ is defined on the whole complex plane. By Berndt's survey [1] we know that if χ denotes the Legendre symbol for p, then

$$A_p - B_p = -\frac{\tau(\chi)p}{\pi^2}(1 - \chi(2)/4)L(2, \chi), \tag{1.3}$$

where

$$L(2, \chi) = -\frac{\tau(\chi)\pi^2}{p^2} B_{2,\chi} \quad \text{and} \quad B_{2,\chi} = -2L(-1, \chi).$$

By (1.1)–(1.3) one can obtain the following results:

- If $p \equiv 3 \pmod 4$, then

$$A_p = \begin{cases} (p^2 - 1)/16 & \text{if } p \equiv 7 \pmod 8, \\ (p^2 - 1 + 8ph(-p))/16 & \text{if } p \equiv 3 \pmod 8, \end{cases} \tag{1.4}$$

  where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$.
- If $p \equiv 1 \pmod 4$, then

$$A_p = \begin{cases} \big(p^2 - 1 + 12 \cdot L(-1, (\cdot/p))\big)/16 & \text{if } p \equiv 1 \pmod 8, \\ \big(p^2 - 1 + 20 \cdot L(-1, (\cdot/p))\big)/16 & \text{if } p \equiv 5 \pmod 8. \end{cases} \tag{1.5}$$

Motivated by the above rich results on quadratic residues, in this paper we concentrate on the products concerning quadratic residues. Let p be an odd prime and set

$$M_p := \prod_{0<x<p/2,\, x\in\mathcal{R}} x.$$

We will determine $M_p \bmod p$. It turns out that these results involve quartic Gauss sums, Stickelberger's congruence and values of Dirichlet L-series at

negative integers. By Wilson's theorem one may easily verify that

$$M_p^2 \equiv \begin{cases} 1 \pmod p & \text{if } p \equiv 5 \pmod 8, \\ -1 \pmod p & \text{if } p \equiv 1 \pmod 8, \end{cases}$$

and hence we have

$$M_p \equiv \begin{cases} \pm 1 \pmod p & \text{if } p \equiv 5 \pmod 8, \\ \pm \frac{p-1}{2}! \pmod p & \text{if } p \equiv 1 \pmod 8. \end{cases}$$

We shall show that the value of M_p mod p behaves quite differently according as $p \equiv 5 \pmod 8$ or $p \equiv 1 \pmod 8$. So we discuss the two cases separately.

We first consider the case $p \equiv 5 \pmod 8$. To state our result we need to introduce the rational 4th power residue symbol. For any prime $p \equiv 1 \pmod 4$ and integer a we define the rational 4th power residue symbol as follows:

$$\left(\frac{a}{p}\right)_4 = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a 4th power residue modulo } p, \\ -1 & \text{otherwise.} \end{cases}$$

THEOREM 1.1. *Let $p \equiv 5 \pmod 8$ be a prime. Then*

$$\prod_{0<x<p/2,\, x\in\mathcal{R}} x \equiv (-1)^{1+\#\{0<x<p/2:\,(\frac{x}{p})_4=1\}} \pmod p.$$

We now consider the case $p \equiv 1 \pmod 8$. This case is related to quartic Gauss sums and Stickelberger's congruence. Here we give a brief review of these (for more details the readers may refer to [7, Chapter 3]). Let $p \equiv 1 \pmod 8$ be a prime, and let $\zeta_{p-1} = e^{2\pi \mathbf{i}/(p-1)}$. Let $K = \mathbb{Q}(\zeta_{p-1}, \zeta_p)$, and let $\mathcal{O}_K$ be the ring of algebraic integers of K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying above the prime ideal $(1-\zeta_p)\mathbb{Z}[\zeta_p]$ of $\mathbb{Z}[\zeta_p]$. Clearly we have

$$\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p,$$

where $\mathbb{F}_p$ denotes the finite field with p elements. It is known that the map

$$u_{\mathfrak{p}} : \zeta_p^k \mapsto \zeta_p^k \pmod{\mathfrak{p}}$$

is a bijection from $\{\zeta_{p-1}^k : k = 0, 1, \ldots, p-2\}$ onto $(\mathcal{O}_K/\mathfrak{p})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$, where $R^\times$ denotes the group of invertible elements of the ring R. We now let $\omega_{\mathfrak{p}} = u_{\mathfrak{p}}^{-1}$ be the mulplicative character of $\mathbb{F}_p$. Clearly $\omega_{\mathfrak{p}}$ generates the character group $\chi(\mathbb{F}_p)$. We let $\chi_\pi = \omega_{\mathfrak{p}}^{-(p-1)/4}$ be the character of order 4. We consider the Jacobi sum $J(\chi_\pi, \chi_\pi)$. By [7, Proposition 3.6.4] we have

$$J(\chi_\pi, \chi_\pi) \equiv -\frac{\frac{p-1}{2}!}{\left(\frac{p-1}{4}!\right)^2} \pmod{\mathfrak{p}}. \tag{1.6}$$

Moreover, it is known (cf. [2, Theorem 3.9]) that

$$J(\chi_\pi,\chi_\pi)=a+4b\mathbf{i} \tag{1.7}$$

with $a\equiv -1 \pmod 4$ and $p=a^2+16b^2$.

Now we consider the Gauss sum $G(\chi_\pi)$. In 1977, Loxton [12] posed the following conjecture concerning the explicit value of $G(\chi_\pi)$ (in a slightly different form):

$$G(\chi_\pi)=C_p\left(\frac{|b|}{|a|}\right)(-1)^b p^{1/4}J(\chi_\pi,\chi_\pi)^{1/2}, \tag{1.8}$$

where $\left(\frac{\cdot}{|a|}\right)$ is the Jacobi symbol, $p^{1/4}$, $\operatorname{Re} J(\chi_\pi,\chi_\pi)^{1/2}>0$ and C_p is defined by

$$C_p=\pm 1 \quad\text{and}\quad C_p\equiv \frac{4|b|}{a}\left(\frac{p-1}{2}\right)! \pmod p. \tag{1.9}$$

Later Matthews [13] confirmed Loxton's elegant conjecture. Hence almost 175 years after Gauss's determination of quadratic Gauss sums, an elegant formula for quartic Gauss sum has been found. The readers may refer to [3] for the history and details on Gauss sums.

Recall that $\varepsilon_p=\frac{u_p+v_p\sqrt{p}}{2}>1$ ($u_p,v_p\in\mathbb{Z}$) and $h(p)$ are the fundamental unit and the class number of $\mathbb{Q}(\sqrt{p})$ respectively. Now we consider the number field $L=K(\varepsilon_p^{1/2},J(\chi_\pi,\chi_\pi)^{1/2})$. Let $\mathcal{O}_L$ be the ring of algebraic integers of L. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$. By [15, Corollary 1.1], if we write $\varepsilon_p^{h(p)}=a_p+b_p\sqrt{p}$ with $2a_p, 2b_p$ integers, then we have

$$a_p\equiv -\frac{p-1}{2}! \pmod p. \tag{1.10}$$

For more results on the congruences involving fundamental units, the readers may refer to [6, 17]. Combining (1.6) with (1.10), we obtain

$$\frac{\varepsilon_p^{h(p)}}{(((p-1)/4)!)^2\cdot J(\chi_\pi,\chi_\pi)}\equiv 1 \pmod{\mathfrak{p}}.$$

We therefore define β_p by

$$\beta_p=0,1 \quad\text{and}\quad (-1)^{\beta_p}\equiv \frac{\varepsilon_p^{h(p)/2}}{((p-1)/4)!\cdot J(\chi_\pi,\chi_\pi)^{1/2}} \pmod{\mathfrak{P}}, \tag{1.11}$$

where $\varepsilon_p^{1/2}$ and $\operatorname{Re} J(\chi_\pi,\chi_\pi)^{1/2}>0$.

THEOREM 1.2. *Let $p\equiv 1 \pmod 8$ be a prime. If we write $p=a^2+16b^2$ with $a,b\in\mathbb{Z}$, then*

$$\prod_{0<x<p/2,\, x\in\mathcal{R}} x\equiv C_p(-1)^{1+\beta_p+\lfloor p/8\rfloor}\left(\frac{|b|}{|a|}\right)\frac{p-1}{2}! \pmod p,$$

where $C_p=\pm 1$ is defined in (1.9)*, and $\left(\frac{\cdot}{|a|}\right)$ is the Jacobi symbol.*

We will prove our main results in Section 2. In Section 3 we pose some problems for further research.

2. Proofs of the main results. We keep the notations from Section 1.

Proof of Theorem 1.1. Let $p \equiv 5 \pmod 8$ be a prime. Clearly

$$-1 \cdot \prod_{0<x<p/2,\, x\in\mathcal{R}} x^2 \equiv \prod_{0<x<p/2,\, x\in\mathcal{R}} x(p-x) \equiv \prod_{0<x<p,\, x\in\mathcal{R}} x \equiv -1 \pmod p.$$

Hence $\prod_{0<x<p/2,\, x\in\mathcal{R}} x \equiv \pm 1 \pmod p$. If we set

$$r = \#\Big\{0 < x < p/2 : \Big(\frac{x}{p}\Big)_4 = 1\Big\},$$

then

$$\prod_{0<x<p/2,\, x\in\mathcal{R}} \Big(\frac{x}{p}\Big)_4 = \Big(\frac{\prod_{0<x<p/2,\, x\in\mathcal{R}} x}{p}\Big)_4 = (-1)^{(p-1)/4-r}.$$

Noting that -1 is a 4th non-residue modulo p, we therefore have

$$\prod_{0<x<p/2,\, x\in\mathcal{R}} x \equiv (-1)^{(p-1)/4-r} = (-1)^{r+1} \pmod p. \ \blacksquare$$

To prove Theorem 1.2 we need to know the explicit value of the product

$$W_p := \prod_{0<x<p/2,\, x\in\mathcal{R}} (1-\zeta_p^{2x}).$$

Let $\zeta_p = e^{2\pi \mathbf{i}/p}$. It is clear that for any integer k with $p \nmid k$ we have

$$(1-\zeta_p^k)/(1-\zeta_p) \equiv k \pmod{(1-\zeta_p)\mathbb{Z}[\zeta_p]}.$$

One deduces that

$$2^{(p-1)/4} \times \prod_{0<x<p/2,\, x\in\mathcal{R}} x \equiv \prod_{0<x<p/2,\, x\in\mathcal{R}} \frac{1-\zeta_p^{2x}}{1-\zeta_p} \pmod{(1-\zeta_p)\mathbb{Z}[\zeta_p]}.$$

Therefore

$$2^{(p-1)/4} \cdot \prod_{0<x<p/2,\, x\in\mathcal{R}} x \equiv \frac{W_p}{(1-\zeta_p)^{(p-1)/4}} \pmod{(1-\zeta_p)\mathbb{Z}[\zeta_p]}.$$

The following lemma gives the explicit value of W_p.

LEMMA 2.1. *Let $p \equiv 1 \pmod 4$ be a prime. Then*

$$\prod_{0<x<p/2,\, x\in\mathcal{R}} (1-\zeta_p^{2x}) = \begin{cases} (-1)^{\lfloor p/8\rfloor} \zeta_p^{\frac{p^2-1+12L(-1,(\cdot/p))}{16}} p^{1/4} \varepsilon_p^{-h(p)/2} & \text{if } 8 \mid p-1, \\ (-1)^{1+\lfloor p/8\rfloor} \zeta_p^{\frac{p^2-1+20L(-1,(\cdot/p))}{16}} \mathbf{i} \cdot p^{1/4} \varepsilon_p^{h(p)/2} & \text{if } 8 \mid p-5, \end{cases}$$

where $\lfloor\cdot\rfloor$ is the floor function and $p^{1/4}, \varepsilon_p^{1/2} > 0$.

Proof. We first compute the absolute value of W_p. By definition,

$$W_p \cdot \overline{W_p} = \prod_{k=1}^{(p-1)/2} (1-\zeta_p^{2k^2}) = \sqrt{p} \cdot \varepsilon_p^{-(\frac{2}{p})h(p)}. \tag{2.1}$$

The last equality is a known result (cf. [16, Theorem 1.3]), and $\overline{W_p}$ denotes the conjugate of W_p. Now we determine the argument $\mathrm{Arg}(W_p)$ of the complex number W_p. We have the following equalities:

$$\begin{aligned} W_p &= \prod_{0<x<p/2,\, x\in\mathcal{R}} -\zeta_p^x(\zeta_p^x - \zeta_p^{-x}) \\ &= (-1)^{(p-1)/4} \cdot \zeta_p^{A_p} \prod_{0<x<p/2,\, x\in\mathcal{R}} 2\mathbf{i}\sin\frac{2\pi x}{p}, \end{aligned} \tag{2.2}$$

where A_p is defined as in the introduction. From this we obtain

$$\mathrm{Arg}(W_p) \equiv \begin{cases} \lfloor p/8\rfloor\pi + 2\pi A_p/p \pmod{2\pi\mathbb{Z}} & \text{if } p\equiv 1 \pmod 8, \\ -\pi/2 + \lfloor p/8\rfloor\pi + 2\pi A_p/p \pmod{2\pi\mathbb{Z}} & \text{if } p\equiv 5 \pmod 8. \end{cases}$$

By the explicit formula for A_p in the introduction,

$$W_p = \begin{cases} (-1)^{\lfloor p/8\rfloor}\zeta_p^{(p^2-1+12L(-1,(\cdot/p)))/16} p^{1/4}\varepsilon_p^{-h(p)/2} & \text{if } p\equiv 1 \pmod 8, \\ (-1)^{1+\lfloor p/8\rfloor}\zeta_p^{(p^2-1+20L(-1,(\cdot/p)))/16}\mathbf{i}\cdot p^{1/4}\varepsilon_p^{h(p)/2} & \text{if } p\equiv 5 \pmod 8. \end{cases}$$ ∎

To prove Theorem 1.2 we also need the following lemma, which is known as Stickelberger's congruence (cf. [7, Theorem 3.6.6]).

LEMMA 2.2. *Let notations be as in Section* 1, *and let* $p\equiv 1 \pmod 8$ *be a prime. Then for all* $0\le r\le p-2$,

$$\frac{G(\omega_{\mathfrak{p}}^{-r})}{(\zeta_p-1)^r} \equiv \frac{-1}{r!} \pmod{\mathfrak{p}},$$

where $G(\omega_{\mathfrak{p}}^{-r})$ *is the Gauss sum associated to the character* $\omega_{\mathfrak{p}}^{-r}$.

Proof of Theorem 1.2. By Lemma 2.2,

$$\frac{G(\chi_\pi)}{(1-\zeta_p)^{(p-1)/4}} \equiv \frac{-1}{((p-1)/4)!} \pmod{\mathfrak{P}}.$$

By (1.8) we obtain

$$\frac{C_p(\frac{|b|}{|a|})(-1)^b p^{1/4} J(\chi_\pi,\chi_\pi)^{1/2}}{(1-\zeta_p)^{(p-1)/4}} \equiv \frac{-1}{((p-1)/4)!} \pmod{\mathfrak{P}}.$$

If we write $p=a^2+16b^2$ with $a,b\in\mathbb{Z}$, then it is known that 2 is a 4th residue modulo p if and only if $2\mid b$. Hence

$$\frac{p^{1/4}}{(1-\zeta_p)^{(p-1)/4}} \equiv \frac{-C_p(\frac{|b|}{|a|})(\frac{2}{p})_4}{((p-1)/4)!\cdot J(\chi_\pi,\chi_\pi)^{1/2}} \pmod{\mathfrak{P}}.$$

Combining this with Lemma 2.1, we obtain

$$\prod_{0<x<p/2,\, x\in\mathcal{R}} x \equiv \frac{(-1)^{1+\lfloor p/8\rfloor}\varepsilon_p^{-h(p)/2}C_p\big(\frac{|b|}{|a|}\big)}{((p-1)/4)!\cdot J(\chi_\pi,\chi_\pi)^{1/2}} \pmod{\mathfrak{P}}.$$

By (1.10), we have $\varepsilon_p^{h(p)} \equiv -\frac{p-1}{2}! \pmod{\mathfrak{P}}$. From this, we finally deduce that

$$\begin{aligned}\prod_{0<x<p/2,\, x\in\mathcal{R}} x &\equiv \frac{(-1)^{1+\lfloor p/8\rfloor}\varepsilon_p^{h(p)/2}C_p\big(\frac{|b|}{|a|}\big)}{((p-1)/4)!\cdot J(\chi_\pi,\chi_\pi)^{1/2}}\cdot\left(\frac{p-1}{2}!\right)\\ &\equiv C_p(-1)^{1+\beta_p+\lfloor p/8\rfloor}\left(\frac{|b|}{|a|}\right)\left(\frac{p-1}{2}!\right) \pmod{\mathfrak{P}}.\end{aligned}$$

This implies our desired result. ∎

3. Some open problems. In this section, we pose some open problems for further research. For any $k, n \in \mathbb{Z}^+$, we define

$$H_k^{(n)} := \sum_{1\le x\le k} \frac{1}{x^n}.$$

These numbers are known as *harmonic numbers*. Let $p > 3$ be a prime. In 1862 Wolstenholme showed that

$$H_{p-1}^{(1)} \equiv 0 \pmod{p^2}.$$

Later Lehmer [10] determined $H_{(p-1)/2}^{(1)} \bmod p^2$ completely. Motivated by the above work, we define

$$H_{\mathcal{R},(p-1)/2}^{(n)} := \sum_{0<x<p/2,\, x\in\mathcal{R}} \frac{1}{x^n}.$$

It is easy to see that if $p \equiv 3 \pmod 4$, then

$$H_{\mathcal{R},(p-1)/2}^{(1)} \equiv \tfrac{1}{2}H_{(p-1)/2}^{(1)} \pmod p,$$

and that if $p \equiv 1 \pmod 4$, then

$$H_{\mathcal{R},(p-1)/2}^{(2)} \equiv 0 \pmod p.$$

In view of the above, we now pose our first problem:

Problem 3.1.

(i) *Let $p \equiv 1 \pmod 4$ be a prime. Can we determine the explicit value of $H_{\mathcal{R},(p-1)/2}^{(1)} \bmod p$?*

(ii) *Let $p \equiv 3 \pmod 4$ be a prime. Can we determine the explicit value of $H_{\mathcal{R},(p-1)/2}^{(2)} \bmod p$?*

The following table gives the values of $H^{(1)}_{\mathcal{R},(p-1)/2} \bmod p$ for primes less than 100 with $p \equiv 1 \pmod 4$:

p	5	13	17	29	37	41	53	61	73	89	97
$H^{(1)}_{\mathcal{R},(p-1)/2} \bmod p$	1	7	4	23	12	18	10	13	17	83	40

We also calculated the values of $H^{(2)}_{\mathcal{R},(p-1)/2} \bmod p$ for primes less than 100 with $p \equiv 3 \pmod 4$:

p	3	7	11	19	23	31	43	47	59	67	71	79	83
$H^{(2)}_{\mathcal{R},(p-1)/2} \bmod p$	1	3	8	5	19	13	29	17	14	18	56	40	14

Now we turn to a problem concerning products of quadratic residues.

PROBLEM 3.2. *Let $p \equiv 3 \pmod 4$ be a prime. Let $M_p = \prod_{0<x<p/2,\, x\in\mathcal{R}} x$. Is there any pattern for the values of $M_p \bmod p$?*

The following table gives the values of $M_p \bmod p$ for primes less than 100 with $p \equiv 3 \pmod 4$:

p	3	7	11	19	23	31	43	47	59	67	71	79	83
$M_p \bmod p$	1	2	5	17	18	5	41	4	29	10	58	38	51

Acknowledgements. We are grateful to the referee for a careful reading of the original manuscript and for helpful comments which improved the quality of our paper.

This research is supported by the National Natural Science Foundation of China (Grant No. 11971222). The first author is also supported by NUPTSF (Grant No. NY220159).

REFERENCES

[1] B. C. Berndt, *Classical theorems on quadratic residues*, Enseign. Math. 22 (1976), 261–304.
[2] B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory 11 (1979), 349–398.
[3] B. C. Berndt and R. J. Evans, *The determination of Gauss sums*, Bull. Amer. Math. Soc. 5 (1981), 107–129.
[4] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.
[5] R. Chapman, *Determinants of Legendre symbol matrices*, Acta Arith. 115 (2004), 231–244.
[6] S. Chowla, *On the class number of real quadratic fields*, Proc. Nat. Acad. Sci. USA 47 (1961), 878.
[7] H. Cohen, *Number Theory. Vol. I: Tools and Diophantine Equations*, Springer, 2007.
[8] H. Cohen, *Number Theory. Vol. II: Analytic and Modern Tools*, Springer, 2007.
[9] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, 1990.

[10] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. 39 (1938), 350–360.
[11] M. Lerch, *Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers*, Acta Math. 29 (1905), 333–424.
[12] J. H. Loxton, *Some conjectures concerning Gauss sums*, J. Reine Angew. Math. 297 (1978), 153–158.
[13] C. R. Matthews, *Gauss sums and elliptic functions. II. The quartic sum*, Invent. Math. 54 (1979), 23–52.
[14] F. Petrov and Z.-W. Sun, *Proof of some conjectures involving quadratic residues*, Electron. Res. Arch. 28 (2020), 589–597.
[15] Z.-W. Sun, *On some determinants with Legendre symbol entries*, Finite Fields Appl. 56 (2019), 285–307.
[16] Z.-W. Sun, *Quadratic residues and related permutations and identities*, Finite Fields Appl. 59 (2019), 246–283.
[17] H.-L. Wu and Y.-F. She, *On a polynomial involving roots of unity and its applications*, arXiv:2001.02860 (2020).

Hai-Liang Wu
School of Science
Nanjing University of Posts
and Telecommunications
Nanjing 210023
People's Republic of China
E-mail: whl.math@smail.nju.edu.cn

Li-Yuan Wang (corresponding author)
School of Physical
and Mathematical Sciences
Nanjing Tech University
Nanjing 211816
People's Republic of China
E-mail: wly@smail.nju.edu.cn