Bull. Aust. Math. Soc. **100** (2019), 362–371
doi:10.1017/S000497271900073X

APPLICATIONS OF LERCH'S THEOREM TO PERMUTATIONS OF QUADRATIC RESIDUES

LI-YUAN WANG and HAI-LIANG WU✉

(Received 8 February 2019; accepted 29 May 2019; first published online 10 July 2019)

Abstract

Let n be a positive integer and a an integer prime to n. Multiplication by a induces a permutation over $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Lerch's theorem gives the sign of this permutation. We explore some applications of Lerch's result to permutation problems involving quadratic residues modulo p and confirm some conjectures posed by Sun ['Quadratic residues and related permutations and identities', Preprint, 2018, arXiv:1809.07766]. We also study permutations involving arbitrary kth power residues modulo p and primitive roots modulo a power of p.

2010 *Mathematics subject classification*: primary 11A15; secondary 05A05, 11A07, 11B75, 11R11.

Keywords and phrases: Zolotarev's lemma, permutation, quadratic residue, Lerch's theorem, primitive root.

1. Introduction

For each integer a and any positive integer n, we let $\{a\}_n$ or $\overline{a}$ denote the least nonnegative residue of a modulo n. Let X be a finite ordered set. The parity of a permutation σ of X can be defined as the parity of the number of inversions for σ, that is, of pairs of elements x, y of X such that $x < y$ and $\sigma(x) > \sigma(y)$. The sign or signature of a permutation σ is denoted $\mathrm{sgn}(\sigma)$ and defined as $+1$ if σ is even and -1 if σ is odd.

Let p be an odd prime. For each integer a with $p \nmid a$, Zolotarev's lemma [9] states that the Legendre symbol (a/p) is equal to the sign of the permutation of $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ induced by multiplication by a. This result has many applications in modern number theory (see [1, 6]). Zolotarev's lemma can be generalised to all positive integers. Let n be a positive integer and a an integer prime to n. From elementary number theory, multiplication by a induces a permutation τ over $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Lerch [4] obtained the following theorem which determines the sign of τ.

This research was supported by the National Natural Science Foundation of China (grant no. 11571162).

THEOREM 1.1 (Lerch [4]). *Let $(\cdot/\cdot)$ denote the Jacobi symbol. With the notation as above,*

$$\operatorname{sgn}(\tau) = \begin{cases} \left(\dfrac{a}{n}\right) & \text{if } n \text{ is odd}, \\ 1 & \text{if } n \equiv 2 \pmod 4, \\ (-1)^{(a-1)/2} & \text{if } n \equiv 0 \pmod 4. \end{cases}$$

This result is discussed in [1]. Lerch's theorem is [1, Theorem 6.1] and it is generalised to any finite principal ring in [1, Theorem 2.6].

It turns out that the case of even n is very useful when we study permutation problems. We remark that the application of Lerch's theorem in this case is new and we believe that further applications can be found. We use the theorem here to determine the sign of a permutation induced by a kth power residue modulo an odd prime p.

Let p be an odd prime and k a positive integer with $\gcd(p-1,k)=1$. It is easy to see that

$$\{1,2,3,\dots,p-1\} = \{\{1^k\}_p, \{2^k\}_p, \{3^k\}_p, \dots, \{(p-1)^k\}_p\}.$$

Since $x^k \equiv 1 \pmod p$ implies $x \equiv 1 \pmod p$, we may therefore view

$$\{1^k\}_p, \{2^k\}_p, \{3^k\}_p, \dots, \{(p-1)^k\}_p$$

as a permutation of $1,2,3,\dots,p-1$. We denote this permutation by $\tau_{k,p}$. The condition $\gcd(p-1,k)=1$ implies that x^k is a permutation polynomial over $\mathbb{Z}/p\mathbb{Z} = \{\overline{0},\overline{1},\dots,\overline{p-1}\}$. The following theorem determines the sign of $\tau_{k,p}$.

THEOREM 1.2. *With the notation as above,*

$$\operatorname{sgn}(\tau_{k,p}) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 4, \\ (-1)^{(k-1)/2} & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

REMARK 1.3. Let $p \equiv 2 \pmod 3$ be an odd prime. Sun [7] noticed that in this case $\sigma_3(\overline{k}) = \overline{k^3}$ with $0 \le k \le p-1$ is a permutation on the set $\mathbb{Z}/p\mathbb{Z} = \{\overline{0},\overline{1},\dots,\overline{p-1}\}$. He conjectured that $\operatorname{sgn}(\sigma_3) = (-1)^{(p+1)/2}$. This conjecture follows immediately from Theorem 1.2.

We now study permutations involving quadratic residues modulo an odd prime. Given an odd prime p, let $1 = a_1 < a_2 < \cdots < a_{(p-1)/2} \le p-1$ be all the quadratic residues modulo p in ascending order. It is easy to see that $a_1, a_2, \dots, a_{(p-1)/2}$ is a permutation of $\{1^2\}_p, \{2^2\}_p, \dots, \{((p-1)/2)^2\}_p$. Let π be this permutation. Sun [7] discussed the sign of this permutation. When $p \equiv 3 \pmod 4$, he evaluated the product

$$\prod_{1 \le j < k \le (p-1)/2} (\zeta_p^{j^2} - \zeta_p^{k^2})$$

by Galois theory, where $\zeta_p = e^{2\pi i/p}$ is a pth root of unity, and determined the sign of π in the case $p \equiv 3 \pmod 4$:

$$\operatorname{sgn}(\pi) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(h(-p)+1)/2} & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

https://doi.org/10.1017/S000497271900073X Published online by Cambridge University Press

where $h(-p)$ denotes the class number of $\mathbb{Q}(\sqrt{-p})$. In addition, he studied some other permutations on quadratic residues and posed some conjectures involving permutations of special forms.

Inspired by Sun's work, we now consider the following sequences:

$$\begin{aligned}
&A_0 : a_1, a_2, \ldots, a_{(p-1)/2},\\
&A_1 : \{1^2\}_p, \{2^2\}_p, \ldots, \left\{\left(\frac{p-1}{2}\right)^2\right\}_p,\\
&A_2 : \{2^2\}_p, \{4^2\}_p, \ldots, \{(p-1)^2\}_p,\\
&A_3 : \{1^2\}_p, \{3^2\}_p, \ldots, \{(p-2)^2\}_p,\\
&A_4 : \left\{1\left(\frac{1}{p}\right)\right\}_p, \left\{2\left(\frac{2}{p}\right)\right\}_p, \ldots, \left\{\frac{p-1}{2}\left(\frac{(p-1)/2}{p}\right)\right\}_p,
\end{aligned}$$

where $(\cdot/p)$ denotes the Legendre symbol. It is easy to see that A_i $(i = 0, 1, 2, 3)$ contains exactly all the quadratic residues modulo p and A_4 does so only when $p \equiv 3 \pmod 4$. If A_i is a permutation of A_j, then we call this permutation $\sigma_{i,j}$. The following theorem gives the sign of $\sigma_{2,1}$ and $\sigma_{3,1}$.

Theorem 1.4. *Let p be an odd prime. Then*

$$\operatorname{sgn}(\sigma_{2,1}) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 4,\\ \left(\frac{2}{p}\right) & \text{if } p \equiv 1 \pmod 4, \end{cases}$$

and

$$\operatorname{sgn}(\sigma_{3,1}) = \begin{cases} -\left(\frac{2}{p}\right) & \text{if } p \equiv 3 \pmod 4,\\ -1 & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

Remark 1.5. By Theorem 1.4, it is easy to see that $\operatorname{sgn}(\sigma_{2,3}) = -(2/p)$.

When $p \equiv 3 \pmod 4$, we determine the sign of $\sigma_{4,0}$ in the next theorem.

Theorem 1.6. *Let p be an odd prime with $p \equiv 3 \pmod 4$. Let $h(-p)$ denote the class number of $\mathbb{Q}(\sqrt{-p})$ and let $\lfloor\cdot\rfloor$ denote the floor function. Then*

$$\operatorname{sgn}(\sigma_{4,0}) = \begin{cases} (-1)^{\lfloor (p+1)/8 \rfloor} & \text{if } p \equiv 3 \pmod 8,\\ (-1)^{\lfloor (p+1)/8 \rfloor + (h(-p)+1)/2} & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Remark 1.7. Combining Sun's result and Theorem 1.6 gives

$$\operatorname{sgn}(\sigma_{4,1}) = (-1)^{\lfloor (p+1)/8 \rfloor}.$$

Sun posed several conjectures, one of which is as follows. For an odd prime p and an integer k, define $R(k, p)$ to be the unique $r \in \{0, 1, \ldots, (p-1)/2\}$ with k congruent to r or $-r$ modulo p and set

$$N_p := \#\{(i, j) : 1 \le i < j \le (p-1)/2 \text{ and } R(i^2, p) > R(j^2, p)\},$$

https://doi.org/10.1017/S000497271900073X Published online by Cambridge University Press

where $\#S$ denotes the cardinality of a finite set S. With this notation, Sun conjectured that $N_p \equiv \lfloor (p+1)/8 \rfloor \pmod 2$ for every odd prime p. Although we cannot prove this conjecture completely, we are able to obtain the following result.

THEOREM 1.8. *With the notation as above, for any prime* $p \equiv 3 \pmod 4$,

$$N_p \equiv \left\lfloor \frac{p+1}{8} \right\rfloor \pmod 2.$$

Let p be an odd prime and $A = \{1, 2, \ldots, (p-1)/2\}$. Sun [7] defined a permutation τ_p as follows: for each $k \in A$, $\tau_p(k)$ is the unique integer $k^* \in A$ with $kk^* \equiv \pm 1 \pmod p$. Sun [7] proved that $\operatorname{sgn}(\tau_p) = -(2/p)$. We give a simpler proof of this result using Lerch's theorem.

THEOREM 1.9. *With the notation as above,* $\operatorname{sgn}(\tau_p) = -(2/p)$.

The proofs of Theorems 1.2, 1.4, 1.6, 1.8, 1.9 will be given in the next section. In Section 3, we turn to another kind of permutation which involves primitive roots.

2. Proofs of the theorems

PROOF OF THEOREM 1.2. Let g be a primitive root modulo p. Then

$$\{1, 2, 3, \ldots, p-1\} = \{\{g^0\}_p, \{g^1\}_p, \{g^2\}_p, \ldots, \{g^{p-2}\}_p\}.$$

Since

$$\tau_{k,p}(g^i) = g^{ki} \pmod p,$$

we see that $\tau_{k,p}$ induces a permutation

$$\hat{\tau}(\bar{i}) = \overline{ki} \pmod{p-1}$$

on the set $\mathbb{Z}/(p-1)\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{p-2}\}$. It is easy to see that $\hat{\tau}$ and $\tau_{k,p}$ have the same factorisation. Hence

$$\operatorname{sgn}(\tau_{k,p}) = \operatorname{sgn}(\hat{\tau}) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 4, \\ (-1)^{(k-1)/2} & \text{if } p \equiv 1 \pmod 4, \end{cases}$$

by Lerch's theorem. □

We need the following lemma which originally appeared in [8, pages 364–365].

LEMMA 2.1 [8]. *Let p be a prime with $p \equiv 3 \pmod 4$. Then*

$$\prod_{1 \le i < j \le (p-1)/2} (i^2 + j^2) \equiv (-1)^{\lfloor (p+1)/8 \rfloor} \pmod p.$$

For convenience, we let $m = (p-1)/2$ throughout the remainder of this section.

https://doi.org/10.1017/S000497271900073X Published online by Cambridge University Press

Proof of Theorem 1.4. If σ is a permutation of a finite set $S = \{x_1, \dots, x_n\}$, which may be viewed as a subset of a field $\mathbb{F}$, then

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} (\sigma(j) - \sigma(i))/(j - i)$$

by definition. In the present situation, all elements can be viewed as in $\mathbb{F}_p$. Thus

$$\begin{aligned}
\operatorname{sgn}(\sigma_{2,1}) &= \prod_{1 \le i < j \le (p-1)/2} \frac{(2j)^2 - (2i)^2}{j^2 - i^2} \pmod p \\
&= \prod_{1 \le i < j \le (p-1)/2} 4 = 4^{1/2 \cdot (p-1)/2 \cdot (p-3)/2} = \left(\frac{2}{p}\right)^{(p-3)/2} \pmod p \\
&= \begin{cases} 1 & \text{if } p \equiv 3 \pmod 4, \\ \left(\dfrac{2}{p}\right) & \text{if } p \equiv 1 \pmod 4. \end{cases}
\end{aligned}$$

Similarily,

$$\begin{aligned}
\operatorname{sgn}(\sigma_{3,1}) &= \prod_{1 \le i < j \le m} \frac{(2j-1)^2 - (2i-1)^2}{j^2 - i^2} \pmod p \\
&= \prod_{1 \le i < j \le m} 4 \cdot \frac{j + i - 1}{j + i} \pmod p \\
&= 2^{m \cdot (m-1)} \cdot \frac{2}{m+1} \cdot \frac{4}{m+2} \cdot \cdots \cdot \frac{2m-2}{2m-1} \pmod p \\
&= 2^{m \cdot (m-1)} \cdot 2^{m-1} \cdot \frac{(m-1)! \cdot m!}{(2m-1)!} \pmod p \\
&= 2^{m^2 - 1} \cdot \frac{2}{p-1} \cdot (m!)^2 \pmod p \\
&= -\left(\frac{2}{p}\right)^{(p-1)/2} \cdot \left(\frac{p-1}{2}!\right)^2 \pmod p.
\end{aligned}$$

This gives

$$\operatorname{sgn}(\sigma_{3,1}) = \begin{cases} -1 & \text{if } p \equiv 1 \pmod 4, \\ -\left(\dfrac{2}{p}\right) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

□

Proof of Theorem 1.6. Assume $p \equiv 3 \pmod 4$. Since $a_1, a_2, \dots, a_m$ is the list of all $(p-1)/2$ quadratic residues among $1, \dots, p-1$ in ascending order, we only need to count the number of ordered pairs (i, j) with $1 \le i < j \le m$ and $\{i(i/p)\}_p > \{j(j/p)\}_p$. Denote this number by $s(p)$. Given any i with $1 \le i < m$, it is easy to check that if $(i/p) = 1$ then the number of j with $1 \le i < j \le m$ and $\{i(i/p)\}_p > \{j(j/p)\}_p$ is zero and

https://doi.org/10.1017/S000497271900073X Published online by Cambridge University Press

if $(i/p) = -1$ then this number is $(p-1)/2 - i$. Thus

$$\begin{aligned} s(p) &= \sum_{1\le i\le (p-1)/2} \left(\frac{p-1}{2} - i\right)\cdot \frac{1}{2}\left(1 - \left(\frac{i}{p}\right)\right) \\ &= \frac{(p-1)(p-3)}{16} - \frac{p-1}{4} \sum_{1\le i\le (p-1)/2} \left(\frac{i}{p}\right) + \frac{1}{2} \sum_{1\le i\le (p-1)/2} i\left(\frac{i}{p}\right). \end{aligned}$$

By Dirichlet's class number formula [2, Corollary 5.3.13],

$$\begin{aligned} -ph(-p) &= \sum_{1\le i\le p-1} i\left(\frac{i}{p}\right) = \sum_{1\le i\le (p-1)/2} \left(i\left(\frac{i}{p}\right) + (p-i)\left(\frac{p-i}{p}\right)\right) \\ &= \sum_{1\le i\le (p-1)/2} \left(2i\left(\frac{i}{p}\right) - p\left(\frac{i}{p}\right)\right). \end{aligned}$$

This implies

$$\sum_{1\le i\le (p-1)/2} i\left(\frac{i}{p}\right) = \frac{1}{2}\left(-ph(-p) + p \sum_{1\le i\le (p-1)/2} \left(\frac{i}{p}\right)\right).$$

Thus,

$$\begin{aligned} s(p) &= \frac{(p-1)(p-3)}{16} - \frac{1}{4}ph(-p) + \frac{1}{4} \sum_{1\le i\le (p-1)/2} \left(\frac{i}{p}\right) \\ &= \frac{(p-1)(p-3)}{16} - \frac{1}{4}ph(-p) + \frac{1}{4}\left(h(-p) - \left(\frac{2}{p}\right)\right). \end{aligned}$$

The last equality follows from Dirichlet's class number formula in another form [2, Corollary 5.3.13]:

$$h(-p) = \frac{1}{2 - \left(\frac{2}{p}\right)} \sum_{1\le i\le (p-1)/2} \left(\frac{i}{p}\right).$$

When $p \equiv 3 \pmod 8$, letting $p = 8k+3$ yields

$$s(p) \equiv k \pmod 2.$$

When $p \equiv 7 \pmod 8$, letting $p = 8k+7$ yields

$$s(p) \equiv k + 1 + \frac{h(-p)+1}{2} \pmod 2.$$

This gives

$$s(p) \equiv \begin{cases} \lfloor (p+1)/8 \rfloor + (h(-p)+1)/2 \pmod 2 & \text{if } p \equiv 3 \pmod 8, \\ \lfloor (p+1)/8 \rfloor \pmod 2 & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

which completes the proof. □

https://doi.org/10.1017/S000497271900073X Published online by Cambridge University Press

Proof of Theorem 1.8. Let S be the set $\{1, 2, \ldots, (p-1)/2\}$ and $\tau : i \mapsto R(i^2, p)$ be a map from S to itself. Since $p \equiv 3 \pmod 4$, it is obvious that τ is a bijection, thus also a permutation on S. Clearly, $A_1 = \{\{1^2\}_p, \{2^2\}_p, \ldots, \{((p-1)/2)^2\}_p\}$ contains exactly all quadratic residues modulo p. We define a map f from S to A_1 as follows. For each $k \in S$, set $f(k) = \{k^2\}_p$. Then

$$\begin{aligned}\operatorname{sgn}(\sigma_{4,1}) = \operatorname{sgn}(f \circ \sigma_{4,1} \circ f^{-1}) &= \prod_{1 \le i < j \le (p-1)/2} \frac{j^4 - i^4}{j^2 - i^2} \pmod p \\ &= \prod_{1 \le i < j \le (p-1)/2} (j^2 + i^2) \pmod p \\ &= (-1)^{\lfloor (p+1)/8 \rfloor} \pmod p.\end{aligned}$$

The last equality follows from Lemma 2.1. □

Proof of Theorem 1.9. For each integer k, recall that $\{k\}_p$ is the least nonnegative residue of k modulo p. Let $k \in A = \{1, 2, \ldots, (p-1)/2\}$. For each $k \in A$, we can write $\tau_p(k) = \{\varepsilon_k k^{-1}\}_p$, where

$$\varepsilon_k = \begin{cases} 1 & \text{if } 1 \le \{k^{-1}\}_p \le (p-1)/2, \\ -1 & \text{otherwise.} \end{cases}$$

Let

$$B = \left\{\{1^2\}_p, \{2^2\}_p, \ldots, \left\{\left(\frac{p-1}{2}\right)^2\right\}_p\right\}.$$

We define a map f_1 from A to B by $f_1(k) = \{k^2\}_p$ for each $k \in A$. Clearly, f_1 is a bijection. On the other hand, let

$$\begin{aligned} A' &= \left\{\{\varepsilon_1 1^{-1}\}_p, \ldots, \left\{\varepsilon_{(p-1)/2}\left(\frac{p-1}{2}\right)^{-1}\right\}_p\right\}, \\ B' &= \left\{\{1^{-2}\}_p, \ldots, \left\{\left(\frac{p-1}{2}\right)^{-2}\right\}_p\right\}. \end{aligned}$$

We define a map f_2 from A' to B' by $f_2(\{\varepsilon_k k^{-1}\}_p) = \{k^{-2}\}_p$ for each $\{\varepsilon_k k^{-1}\}_p$. Clearly, f_2 is a bijection. Moreover, $f_2 \circ \tau_p \circ f_1^{-1}$ is a permutation on B with

$$f_2 \circ \tau_p \circ f_1^{-1}(k^2) = \{k^{-2}\}_p.$$

It is easy to see that

$$\operatorname{sgn}(\tau_p) = \operatorname{sgn}(f_2 \circ \tau_p \circ f_1^{-1}).$$

On the other hand, if we let g be a primitive root of p, then

$$f_2 \circ \tau_p \circ f_1^{-1}(g^{2l}) = g^{-2l}.$$

Hence, $f_2 \circ \tau_p \circ f_1^{-1}$ induces a permutation π_{-1} on $\mathbb{Z}/(p-1)/2\mathbb{Z} = \{\overline{1}, \overline{2}, \ldots, \overline{(p-1)/2}\}$. Moreover, $\pi_{-1}(\overline{s}) = \overline{-s}$ for each $\overline{s} \in \mathbb{Z}/(p-1)/2\mathbb{Z}$. Thus our theorem follows from Lerch's theorem. □

https://doi.org/10.1017/S000497271900073X Published online by Cambridge University Press

3. Permutations involving primitive roots

In 2018, Kohl [3] posed a permutation problem involving primitive roots of an odd prime on Mathoverflow. Let p be an odd prime, $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ and g a primitive root modulo p. Define

$$\sigma_g(b) := g^b$$

for each $b \in \{1, \ldots, p-1\}$ and $\sigma_g(0) = 0$. If we identify $\mathbb{Z}/p\mathbb{Z}$ with $\{0, 1, \ldots, p-1\}$, we can view σ_g as a permutation over $\mathbb{Z}/p\mathbb{Z}$. Let $\mathcal{R}_p$ denote the set of all primitive roots of p. Kohl considered the sign of the permutation σ_g and posed the following conjecture which was proved by Ladisch and Petrov (see [3]).

Conjecture 3.1 [3]. *Assume the notation defined above.*

(i) *If* $p \equiv 1 \pmod 4$, *then* $\#\{g \in \mathcal{R}_p : \operatorname{sgn}(\sigma_g) = 1\} = \#\{g \in \mathcal{R}_p : \operatorname{sgn}(\sigma_g) = -1\}$.

(ii) *If* $p \equiv 3 \pmod 4$ *and* $g \in \mathcal{R}_p$, *then*

$$\operatorname{sgn}(\sigma_g) \equiv (-1)^{(h(-p)-1)/2} \pmod p,$$

where $h(-p)$ *denotes the class number of* $\mathbb{Q}(\sqrt{-p})$.

Throughout this section, we set $n = \phi(p^r) = p^{r-1}(p-1)$. We investigate the sign of the permutation induced by the primitive roots of a power of an odd prime. Given an odd prime p and a positive integer r, let $\mathcal{R}_{p^r}$ denote the set of all primitive roots of p^r and let $1 = b_1 < b_2 < \cdots < b_n < p^r$ be the least nonnegative reduced residue system modulo p^r in ascending order. For each $g \in \mathcal{R}_{p^r}$, we define a permutation σ_g on $\{b_1, \ldots, b_n\}$ by

$$\sigma_g : \ b_i \mapsto g^i \pmod{p^r}.$$

Theorem 3.2. *Assume the notation defined above.*

(i) *If* $p \equiv 1 \pmod 4$, *then*

$$\#\{g \in \mathcal{R}_{p^r} : \operatorname{sgn}(\sigma_g) = 1\} = \#\{g \in \mathcal{R}_{p^r} : \operatorname{sgn}(\sigma_g) = -1\} = n/2.$$

(ii) *If* $p \equiv 3 \pmod 4$ *and* $g \in \mathcal{R}_{p^r}$, *then*

$$\operatorname{sgn}(\sigma_g) = (-1)^{(h(-p)-1)/2},$$

where $h(-p)$ *denotes the class number of* $\mathbb{Q}(\sqrt{-p})$.

Proof of Theorem 3.2(i). When $p \equiv 1 \pmod 4$,

$$\sigma_{g^{-1}} \circ \sigma_g^{-1}(g^i) = g^{-i}.$$

Thus $\sigma_{g^{-1}} \circ \sigma_g^{-1}$ induces a permutation π_{-1} on $\mathbb{Z}/n\mathbb{Z} = \{\overline{1}, \overline{2}, \ldots, \overline{n}\}$, where $\pi_{-1}(\overline{k}) = \overline{-k}$. Since n is even, the fixed points are $n/2$ and n and so there remain $((n-2)/2)$ 2-cycles. Note that $(n-2)/2$ is odd when $p \equiv 1 \pmod 4$. It follows that π_{-1} is an odd permutation, which implies (i) of Theorem 3.2. □

https://doi.org/10.1017/S000497271900073X Published online by Cambridge University Press

Proof of Theorem 3.2(ii). Suppose $p \equiv 3 \pmod 4$. From the definition,

$$\operatorname{sgn}(\sigma_g) = \prod_{1\le k<j\le n} \frac{\{g^j\}_{p^r} - \{g^k\}_{p^r}}{b_j - b_k}.$$

Thus we only need to determine this quantity modulo p.

First we consider the numerator. Let

$$f(z) = \prod_{1\le k<j\le n} (z^j - z^k).$$

Set $\zeta_n = e^{2\pi i/n}$. Then

$$f(\zeta_n)^2 = (-1)^{n(n-1)/2} \prod_{1\le k\ne j\le n} (\zeta_n^j - \zeta_n^k) = -1 \cdot \prod_{1\le j\le n} \frac{z^n - 1}{z - \zeta_n^j}\bigg|_{z=\zeta_n^j} = -1 \cdot \prod_{1\le j\le n} n\zeta_n^{j(n-1)} = n^n.$$

On the other hand, for each pair (k, j) with $1 \le k < j \le n$, it is easy to see that

$$\operatorname{Arg}(\zeta_n^j - \zeta_n^k) = \operatorname{Arg}(\zeta_n^{(j+k)/2}(\zeta_n^{(j-k)/2} - \zeta_n^{-(j-k)/2})) \equiv \frac{j+k}{n}\pi + \frac{\pi}{2} \pmod{2\pi},$$

where $\operatorname{Arg}(z)$ denotes the argument of the complex number z. Thus

$$\operatorname{Arg}(f(\zeta_n)) \equiv \sum_{1\le k<j\le n} \left(\frac{j+k}{n}\pi + \frac{\pi}{2}\right) \equiv \frac{(3n+2)(n-1)}{4}\pi \pmod{2\pi}.$$

Hence,

$$f(\zeta_n) = (-1)^{(3n+2)/4} n^{n/2} = p^{n(r-1)/2}(-1)^{(3n+2)/4}(p-1)^{n/2}.$$

Since $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is isomorphic to the group generated by ζ_n,

$$p^{-n(r-1)/2} \prod_{1\le k<j\le n} (\{g^j\}_{p^r} - \{g^k\}_{p^r}) \equiv (-1)^{(3n+2)/4+n/2} \pmod p. \tag{3.1}$$

Next we consider the denominator. Since

$$\prod_{1\le k<j\le n} \frac{\{g^j\}_{p^r} - \{g^k\}_{p^r}}{b_j - b_k} = \pm 1,$$

we only need to determine

$$p^{-n(r-1)/2} \prod_{1\le k<j\le n} (b_j - b_k) \pmod p.$$

Note that

$$p^{-n(r-1)/2} \prod_{1\le k<j\le n} (b_j - b_k) \equiv \prod_{1\le i<j\le p-1} (j-i)^{p^{r-1}} \prod_{1\le i\ne j\le p-1} (j-i)^{\binom{p^{r-1}}{2}} \pmod p. \tag{3.2}$$

It is known that

$$\prod_{1\le i<j\le p-1} (j-i) \equiv \left(\frac{p-1}{2}\right)! \cdot (-1)^{(p-3)/4} \pmod p \tag{3.3}$$

https://doi.org/10.1017/S000497271900073X Published online by Cambridge University Press

and, by [5],

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{(h(-p)+1)/2} \pmod{p}, \tag{3.4}$$

where $h(-p)$ denotes the class number of $\mathbb{Q}(\sqrt{-p})$. Observe that

$$\prod_{1\le i\ne j\le p-1}(j-i) = -1\cdot\prod_{1\le i<j\le p-1}(j-i)^2. \tag{3.5}$$

Combining (3.2)–(3.5), we obtain

$$p^{-n(r-1)/2}\prod_{1\le k<j\le n}(b_j-b_k) \equiv (-1)^{(h(-p)+1)/2+(p-3)/4+r+1} \pmod{p}. \tag{3.6}$$

Our desired result follows from (3.1) and (3.6). □

Acknowledgements

We are grateful to Professor Hao Pan for his helpful suggestions on the writting of this paper. We are exceedingly grateful for the careful reading and indispensable suggestions of the anonymous referee.

References

[1] A. Brunyate and P. L. Clark, 'Extending the Zolotarev–Frobenius approach to quadratic reciprocity', *Ramanujan J.* **37** (2015), 25–50.
[2] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, 138 (Springer, New York, 1993).
[3] S. Kohl, Question 302865 in MathOverflow, solved by F. Ladisch and F. Petrov, available at https://mathoverflow.net/questions/302865/.
[4] M. Lerch, 'Sur un théorème de Zolotarev', *Bull. Intern. Acad. François Joseph* **3** (1896), 34–37.
[5] L. J. Mordell, 'The congruence $((p-1)/2)! \equiv \pm 1 (\mathrm{mod}\ p)$', *Amer. Math. Monthly* **68** (1961), 145–146.
[6] H. Pan, 'A remark on Zolotarev's theorem', Preprint, 2006, arXiv:0601026.
[7] Z. W Sun, 'Quadratic residues and related permutations and identities', Preprint, 2018, arXiv:1809.07766.
[8] G. J. Szekely (ed), *Contests in Higher Mathematics* (Springer, New York, 1996).
[9] G. Zolotarev, 'Nouvelle démonstration de la loi de réciprocité de Legendre', *Nouvelles Ann. Math.* **11** (1872), 354–362.

LI-YUAN WANG, Department of Mathematics,
Nanjing University, Nanjing 210093, People's Republic of China
e-mail: wly@smail.nju.edu.cn

HAI-LIANG WU, Department of Mathematics,
Nanjing University, Nanjing 210093, People's Republic of China
e-mail: whl.math@smail.nju.edu.cn

https://doi.org/10.1017/S000497271900073X Published online by Cambridge University Press