Bull. Aust. Math. Soc. **105** (2022), 188–196
doi:10.1017/S000497272100054X

CUBES IN FINITE FIELDS AND RELATED PERMUTATIONS

HAI-LIANG WU and YUE-FENG SHE

(Received 25 May 2021; accepted 3 June 2021; first published online 15 July 2021)

Abstract

Let $p = 3n + 1$ be a prime with $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$ and let $g \in \mathbb{Z}$ be a primitive root modulo p. Let $0 < a_1 < \cdots < a_n < p$ be all the cubic residues modulo p in the interval $(0, p)$. Then clearly the sequence $a_1 \bmod p, a_2 \bmod p, \ldots, a_n \bmod p$ is a permutation of the sequence $g^3 \bmod p, g^6 \bmod p, \ldots, g^{3n} \bmod p$. We determine the sign of this permutation.

2020 *Mathematics subject classification*: primary 11A15; secondary 05A05, 11R18.

Keywords and phrases: permutations, primitive roots, cubes in finite fields.

1. Introduction

Investigating permutations over finite fields is an active topic in both number theory and finite fields. The Lagrange interpolation formula shows that each permutation over a finite field is in fact induced by a permutation polynomial. For example, let p be an odd prime and let a be an integer with $p \nmid a$. Then $x \bmod p \mapsto ax \bmod p$ (for $x = 0, 1, \ldots, p-1$) is a permutation over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Zolotarev [12] showed that the sign of this permutation is precisely the Legendre symbol (a/p). Later, Lerch [6] extended this result to the ring of residue classes modulo an arbitrary positive integer. In 2015, Brunyate and Clark [3] made a further extension to higher dimensional vector spaces over finite fields.

Recently, Sun [8, 9] studied permutations involving squares in finite fields. In fact, let $p = 2m + 1$ be an odd prime. Let $0 < b_1 < \cdots < b_m < p$ be all the quadratic residues modulo p in the interval $(0, p)$. Then clearly the sequence

$$1^2 \bmod p,\ 2^2 \bmod p, \ldots, m^2 \bmod p$$

is a permutation σ_p of the sequence

$$b_1 \bmod p,\ b_2 \bmod p, \ldots, b_m \bmod p.$$

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

Let $\mathrm{sign}(\sigma_p)$ denote the sign of σ_p. Sun [8, Theorem 1.4] obtained

$$\mathrm{sign}(\sigma_p) = \begin{cases} 1 & \text{if } p \equiv 3 \bmod 8, \\ (-1)^{(h(-p)+1)/2} & \text{if } p \equiv 7 \bmod 8, \end{cases}$$

where $h(-p)$ denotes the class number of $\mathbb{Q}(\sqrt{-p})$. Later, Petrov and Sun [7] determined the sign of σ_p in the case $p \equiv 1 \pmod 4$.

With this motivation, we consider permutations involving cubes in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (where p is an odd prime). The case $p \equiv 2 \bmod 3$ is trivial. Clearly in this case

$$\{x^3 \bmod p : x = 0, 1, \ldots, p-1\} = \mathbb{Z}/p\mathbb{Z}$$

and hence $x \bmod p \mapsto x^3 \bmod p$ $(x = 0, 1, \ldots, p-1)$ is a permutation τ_p over $\mathbb{Z}/p\mathbb{Z}$. The sign of τ_p is a direct consequence of Lerch's result [6] and we have $\mathrm{sign}(\tau_p) = (-1)^{(p+1)/2}$ (see [10, Theorem 1.2] for details).

Now we consider the nontrivial case $p \equiv 1 \bmod 3$. Let $p = 3n + 1$ be a prime with $n \in \mathbb{N}$ and let $g \in \mathbb{Z}$ be a primitive root modulo p. Let $0 < a_1 < \cdots < a_n < p$ be all the cubic residues modulo p in the interval $(0, p)$. Then clearly the sequence

$$a_1 \bmod p, a_2 \bmod p, \ldots, a_n \bmod p$$

is a permutation $s_p(g)$ of the sequence

$$g^3 \bmod p, g^6 \bmod p, \ldots, g^{3n} \bmod p.$$

In order to state our result, we first introduce some notation. Let

$$\mathcal{P} := \{0 < x < p : x \text{ is a primitive root modulo } p\}.$$

It is known (see [4]) that $4p$ can be uniquely written as

$$4p = r^2 + 3s^2 \quad (r, s \in \mathbb{Z}) \tag{1.1}$$

with $r \equiv 1 \bmod 3$, $s \equiv 0 \bmod 3$ and $3s \equiv (2g^n + 1)r \bmod p$. Let $\omega = e^{2\pi i/3}$ be a primitive cubic root of unity. As p splits in $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\omega]$ is a principal ideal domain, we can write $p = \pi\bar{\pi}$ for some primary prime $\pi \in \mathbb{Z}[\omega]$ with $(g/\pi)_3 = \omega$, where $\bar{\pi}$ denotes the conjugate of π and the symbol $(\cdot/\pi)_3$ is the cubic residue symbol modulo π. For convenience, we briefly recall the definition of the cubic residue symbol (see [5, Ch. 9] for details). For any $x \in \mathbb{Z}[\omega]$ with $\pi \nmid x$, there is a unique $i \in \{0, 1, 2\}$ such that $x^n \equiv \omega^i \bmod \pi\mathbb{Z}[\omega]$. Hence, for any $x \in \mathbb{Z}[\omega]$ with $\pi \nmid x$, we define the cubic residue symbol $(x/\pi)_3$ by

$$\left(\frac{x}{\pi}\right)_3 = \begin{cases} 1 & \text{if } x^n \equiv \omega^0 \bmod \pi\mathbb{Z}[\omega], \\ \omega & \text{if } x^n \equiv \omega^1 \bmod \pi\mathbb{Z}[\omega], \\ \omega^2 & \text{if } x^n \equiv \omega^2 \bmod \pi\mathbb{Z}[\omega]. \end{cases}$$

https://doi.org/10.1017/S000497272100054X Published online by Cambridge University Press

We also define

$$\delta_p := |\{0 < x < p/4 : x \text{ is a cubic residue modulo } p\}|, \tag{1.2}$$

$$\alpha_p := |\{0 < x < p/2 : x \text{ is a sixth power residue modulo } p\}|, \tag{1.3}$$

$$\gamma_p := \left|\left\{0 < x < p/2 : \left(\frac{x}{p}\right) = 1 \text{ and } \left(\frac{x}{\pi}\right)_3 = \omega^2\right\}\right|, \tag{1.4}$$

where $|S|$ denotes the cardinality of a set S.

With this notation, we now state our main result.

Theorem 1.1. *Let $p = 3n + 1$ be a prime with $n \in \mathbb{N}$.*

(i) *If $p \equiv 1 \bmod 12$, then*

$$|\{g \in \mathcal{P} : sign(s_p(g)) = 1\}| = |\{g \in \mathcal{P} : sign(s_p(g)) = -1\}|.$$

(ii) *If $p \equiv 7 \pmod{12}$, then $sign(s_p(g))$ is independent of the choice of g and*

$$sign(s_p(g)) = (-1)^{\delta_p+(1+\alpha_p)(1+r)+(h(-p)+1-2\alpha_p)(2-r+3s)/4+s(1+\gamma_p)+(n-2)/4},$$

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

Remark 1.2. For any primitive roots g, g' modulo p, the product of $\text{sign}(s_p(g))$ and $\text{sign}(s_p(g'))$ is indeed equal to the sign of the permutation which sends the sequence

$$g^3 \bmod p,\ g^6 \bmod p, \ldots, g^{3n} \bmod p$$

to the sequence

$$g'^3 \bmod p,\ g'^6 \bmod p, \ldots, g'^{3n} \bmod p.$$

The signs of the permutations of this type are direct consequences of Lerch's theorem [6] and were investigated by Wang and the first author in [10, Theorem 3.2].

We will prove Theorem 1.1 in the next section.

2. Proof of Theorem 1.1

We first introduce some notation. Let $p = 3n + 1$ be a prime with $n \in \mathbb{N}$ and let $g \in \mathbb{Z}$ be a primitive root modulo p. Let $\omega = e^{2\pi i/3}$ be a primitive cubic root of unity.

As p splits in $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\omega]$ is a principal ideal domain, we can write $p = \pi\bar{\pi}$ for some primary prime element $\pi \in \mathbb{Z}[\omega]$ with $(g/\pi)_3 = \omega$, where $\bar{\pi}$ denotes the conjugate of π and the symbol $(\cdot/\pi)_3$ is the cubic residue symbol modulo π. For convenience, we use the symbol $\mathfrak{p}$ to denote the prime ideal $\pi\mathbb{Z}[\omega]$. Recall that from (1.1), $4p$ can be uniquely written as

$$4p = r^2 + 3s^2 \quad (r, s \in \mathbb{Z})$$

with $r \equiv 1 \bmod 3$, $s \equiv 0 \bmod 3$ and $3s \equiv (2g^n + 1)r \bmod p$.

Lemma 2.1 [1, Corollary 10.6.2(c)]. *For any k with $0 < k < p$, let*

$$N(k) := |\{(x, y) : 0 < x, y < p,\ y^3 - x^3 \equiv k \bmod p\}|.$$

https://doi.org/10.1017/S000497272100054X Published online by Cambridge University Press

Then, with the above notation,

$$N(k) = \begin{cases} p + r - 8 & \textit{if} \left(\frac{k}{\pi}\right)_3 = 1, \\ (2p - r + 3s - 4)/2 & \textit{if} \left(\frac{k}{\pi}\right)_3 = \omega, \\ (2p - r - 3s - 4)/2 & \textit{if} \left(\frac{k}{\pi}\right)_3 = \omega^2. \end{cases}$$

For any k with $0 < k < p$, define

$$r_k := \left|\left\{(x, y) : 0 < x < y < p, y - x \equiv k \bmod p, \left(\frac{x}{\pi}\right)_3 = \left(\frac{y}{\pi}\right)_3 = 1\right\}\right|. \tag{2.1}$$

We need the following result.

LEMMA 2.2. *We have*

$$\sum_{0<k<p/2} r_{p-k} \equiv \left|\left\{0 < x < p/4 : \left(\frac{x}{\pi}\right)_3 = 1\right\}\right| \bmod 2.$$

PROOF. From the definition,

$$\sum_{0<k<p/2} r_{p-k} = \left|\left\{(x, y) : 0 < x < y < p,\ y - x > p/2, \left(\frac{x}{\pi}\right)_3 = \left(\frac{y}{\pi}\right)_3 = 1\right\}\right|. \tag{2.2}$$

Replacing y by $p - y$ in the right-hand side of (2.2),

$$\sum_{0<k<p/2} r_{p-k} = \left|\left\{(x, y) : 0 < x, y < p,\ x + y < p/2, \left(\frac{x}{\pi}\right)_3 = \left(\frac{y}{\pi}\right)_3 = 1\right\}\right|.$$

By symmetry,

$$\sum_{0<k<p/2} r_{p-k} \equiv \left|\left\{0 < x < p/4 : \left(\frac{x}{\pi}\right)_3 = 1\right\}\right| \bmod 2.$$

This completes the proof. □

Now we define the following sets:

$$A_1 := \left\{0 < x < p/2 : \left(\frac{x}{\pi}\right)_3 = 1\right\},$$

$$A_\omega := \left\{0 < x < p/2 : \left(\frac{x}{\pi}\right)_3 = \omega\right\},$$

$$A_{\omega^2} := \left\{0 < x < p/2 : \left(\frac{x}{\pi}\right)_3 = \omega^2\right\}.$$

For the following result, recall that $\mathfrak{p} = \pi\mathbb{Z}[\omega])$ and α_p and γ_p were defined in (1.3) and (1.4).

https://doi.org/10.1017/S000497272100054X Published online by Cambridge University Press

LEMMA 2.3. *Let $p \equiv 7 \bmod 12$ be a prime.*

(i) *We have*

$$\prod_{x \in A_1} x \equiv (-1)^{1+\alpha_p} \bmod p.$$

(ii) *If*

$$\beta_p := \left|\left\{0 < x < p/2 : \left(\frac{x}{p}\right) = 1 \text{ and } \left(\frac{x}{\pi}\right)_3 = \omega\right\}\right|,$$

then

$$\prod_{x \in A_\omega} x \equiv (-1)^{1+\beta_p} \omega^2 \bmod \mathfrak{p}.$$

(iii) *We have*

$$\prod_{x \in A_{\omega^2}} x \equiv (-1)^{1+\gamma_p} \omega \bmod \mathfrak{p}.$$

PROOF. (i) One can verify the following polynomial congruence:

$$\prod_{0<x<p,\,(x/\pi)_3=1} (T - x) \equiv T^n - 1 \bmod p.$$

Hence,

$$(-1)^{n/2}\Big(\prod_{x \in A_1} x\Big)^2 \equiv -1 \bmod p.$$

Since $p \equiv 3 \bmod 4$,

$$\Big(\prod_{x \in A_1} x\Big)^2 \equiv 1 \bmod p.$$

Thus,

$$\prod_{x \in A_1} x \equiv (-1)^{n/2-\alpha_p} \equiv (-1)^{1+\alpha_p} \bmod p.$$

(ii) As in (i),

$$\prod_{0<x<p,\,(x/\pi)_3=\omega} (T - x) \equiv T^n - \omega \bmod \mathfrak{p}.$$

Hence,

$$\Big(\prod_{x \in A_\omega} x\Big)^2 \equiv \omega \bmod \mathfrak{p}.$$

https://doi.org/10.1017/S000497272100054X Published online by Cambridge University Press

Noting that $\omega = (\omega^2)^2$ is a quadratic residue modulo $\mathfrak{p}$, by the definition of β_p,

$$\prod_{x \in A_\omega} x \equiv (-1)^{1+\beta_p} \omega^2 \bmod \mathfrak{p}.$$

(iii) With essentially the same method as in (ii), one can verify (iii). □

Let $\Phi_{p-1}(T)$ be the $(p-1)$th cyclotomic polynomial and let

$$P(T) := \prod_{1 \le i < j \le n} (T^{3^j} - T^{3^i}).$$

LEMMA 2.4 [11, Lemma 2.5]. *Let $G(T)$ be an integral polynomial defined by*

$$G(T) = \begin{cases} (-1)^{(n-2)/4} \cdot n^{n/2} & \text{if } p \equiv 3 \bmod 4, \\ (-1)^{(n-4)/4} \cdot n^{n/2} \cdot T^{(p-1)/4} & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

Then $\Phi_{p-1}(T) \mid (P(T) - G(T))$.

Now we are in a position to prove our main result.

PROOF OF THEOREM 1.1. From the definition,

$$\operatorname{sign}(s_p) \equiv \prod_{1 \le i < j \le n} \frac{g^{3^j} - g^{3^i}}{a_j - a_i} \bmod \mathfrak{p}.$$

We first consider the numerator. Since p splits completely in the cyclotomic field $\mathbb{Q}(e^{2\pi i/(p-1)})$, it follows that $\Phi_{p-1}(T) \bmod p\mathbb{Z}[T]$ splits completely in $\mathbb{Z}/p\mathbb{Z}[T]$. Also, the set of all primitive $(p-1)$th roots of unity maps bijectively onto the set of all primitive $(p-1)$th roots of unity in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Hence,

$$\Phi_{p-1}(T) \equiv \prod_{x \in \mathcal{P}} (T - x) \bmod p, \tag{2.3}$$

where

$$\mathcal{P} := \{0 < x < p : x \text{ is a primitive root modulo } p\}.$$

By Lemma 2.4 and (2.3),

$$\prod_{1 \le i < j \le n} (g^{3^j} - g^{3^i}) = P(g) \equiv G(g) \bmod p,$$

that is,

$$\prod_{1 \le i < j \le n} (g^{3^j} - g^{3^i}) \equiv \begin{cases} (-1)^{(n-2)/4} \cdot n^{n/2} \bmod p & \text{if } 4 \mid p-3, \\ (-1)^{(n-4)/4} \cdot n^{n/2} \cdot g^{(p-1)/4} \bmod p & \text{if } 4 \mid p-1. \end{cases} \tag{2.4}$$

By (2.4), for any $g' \in \mathcal{P}$,

$$\prod_{1 \le i < j \le n} \frac{g^{3^j} - g^{3^i}}{(g')^{3^j} - (g')^{3^i}} \equiv \begin{cases} (g/g')^{(p-1)/4} \bmod p & \text{if } 4 \mid p-1, \\ 1 \bmod p & \text{if } 4 \mid p-3. \end{cases}$$

https://doi.org/10.1017/S000497272100054X Published online by Cambridge University Press

If $p \equiv 1 \bmod 4$, this implies that $\mathrm{sign}(s_p(g)) \cdot \mathrm{sign}(s_p(g^{-1})) = -1$ and so

$$|\{g \in \mathcal{P} : \mathrm{sign}(s_p(g)) = 1\}| = |\{g \in \mathcal{P} : \mathrm{sign}(s_p(g)) = -1\}|.$$

If $p \equiv 3 \bmod 4$, it is clear that $\mathrm{sign}(s_p(g))$ is independent of the choice of g.

We now consider the denominator and assume that $p \equiv 3 \bmod 4$. From the definition of r_k in (2.1), it is clear that

$$\prod_{1\le i<j\le n}(a_j - a_i) \equiv \prod_{0<k<p} k^{r_k} \equiv (-1)^{\sum_{0<k<p/2} r_{p-k}} \cdot \prod_{0<k<p/2} k^{r_k+r_{p-k}}$$
$$\equiv (-1)^{\delta_p} \prod_{0<k<p/2} k^{r_k+r_{p-k}} \bmod \mathfrak{p},$$

where δ_p is defined in (1.2) and the last congruence follows from Lemma 2.2. From the definition of r_k, one can verify that for $0 < k < p$,

$$r_k + r_{p-k} = N(k)/9,$$

where $N(k)$ is defined in Lemma 2.1. Consequently,

$$\prod_{1\le i<j\le n}(a_j - a_i) \equiv (-1)^{\delta_p} \prod_{x\in A_1} x^{p+r-8/9} \prod_{y\in A_\omega} y^{2p-r+3s-4/18} \prod_{z\in A_{\omega^2}} z^{2p-r-3s-4/18} \bmod \mathfrak{p}.$$

By Lemma 2.3,

$$\prod_{x\in A_1} x^{p+r-8/9} \equiv (-1)^{(1+\alpha_p)(1+r)} \bmod \mathfrak{p},$$
$$\prod_{y\in A_\omega} y^{2p-r+3s-4/18} \prod_{z\in A_{\omega^2}} z^{2p-r-3s-4/18} \equiv (-1)^{(\beta_p+\gamma_p)(-r+3s)/2+(1+\gamma_p)s}\omega^{2s/3} \bmod \mathfrak{p}.$$

Note that

$$\alpha_p + \beta_p + \gamma_p = |\{0 < x < p/2 : x \text{ is a quadratic residue modulo } p\}|.$$

By the class number formula of $\mathbb{Q}(\sqrt{-p})$ (see [2, Theorem 4, page 346]),

$$|\{0 < x < p/2 : x \text{ is a quadratic residue modulo } p\}| \equiv \frac{h(-p)+1}{2} \bmod 2,$$

where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$. Thus,

$$\prod_{1\le i<j\le n}(a_j - a_i) \equiv (-1)^{\delta_p+(1+\alpha_p)(1+r)+(h(-p)+1-2\alpha_p)(2-r+3s)/4+s(1+\gamma_p)}\omega^{2s/3} \bmod \mathfrak{p}. \tag{2.5}$$

By (2.4),

$$\prod_{1\le i<j\le n}(g^{3j} - g^{3i}) \equiv (-1)^{(n-2)/4} \cdot n^{n/2} \bmod p. \tag{2.6}$$

By the result in [4, Exercise 4.15]), 3 is a cubic residue modulo p if and only if the equation $4p = X^2 + 243Y^2$ has integral solutions. With our notation in (1.1), this is equivalent to $s \equiv 0 \bmod 9$. We now divide the remaining proof into two cases.

https://doi.org/10.1017/S000497272100054X Published online by Cambridge University Press

Case I: 3 is not a cubic residue modulo p. Since

$$\mathrm{sign}(s_p) \equiv \prod_{1\le i<j\le n} \frac{g^{3j}-g^{3i}}{a_j-a_i} \equiv \pm 1 \bmod \mathfrak{p},$$

we must have $n^{n/2} \equiv \varepsilon\omega^{2s/3}$ for some $\varepsilon \in \{\pm 1\}$. Hence,

$$\varepsilon \equiv n^{3n/2} \equiv \left(\frac{-3}{p}\right) \equiv 1 \bmod \mathfrak{p}.$$

Combining this with (2.5) and (2.6),

$$\mathrm{sign}(s_p(g)) = (-1)^{\delta_p+(1+\alpha_p)(1+r)+(h(-p)+1-2\alpha_p)(2-r+3s)/4+s(1+\gamma_p)+(n-2)/4}.$$

Case II: 3 is a cubic residue modulo p. In this case, $n^{n/2} = \pm 1$ and hence

$$n^{n/2} = n^{3n/2} \equiv \left(\frac{-3}{p}\right) = 1 \bmod \mathfrak{p}.$$

Combining this with (2.5) and (2.6),

$$\mathrm{sign}(s_p(g)) = (-1)^{\delta_p+(1+\alpha_p)(1+r)+(h(-p)+1-2\alpha_p)(2-r+3s)/4+s(1+\gamma_p)+(n-2)/4}.$$

This completes the proof. □

Acknowledgements

We thank the referee for helpful comments. The first author would like to thank Professor Hao Pan for his encouragement.

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums* (Wiley, New York, 1998).
[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory* (Academic Press, New York, 1966).
[3] A. Brunyate and P. L. Clark, 'Extending the Zolotarev–Frobenius approach to quadratic reciprocity', *Ramanujan J.* **37** (2015), 25–50.
[4] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication* (Wiley, New York, 1989).
[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edn, Graduate Texts in Mathematics, 84 (Springer, New York, 1990).
[6] M. Lerch, 'Sur un théorème de Zolotarev', *Bull. Internat. Acad. François Joseph* **3** (1896), 34–37.
[7] F. Petrov and Z.-W. Sun, 'Proof of some conjectures involving quadratic residues', *Electron. Res. Arch.* **28** (2020), 589–597.
[8] Z.-W. Sun, 'Quadratic residues and related permutations and identities', *Finite Fields Appl.* **59** (2019), 246–283.
[9] Z.-W. Sun, 'On quadratic residues and quartic residues modulo primes', *Int. J. Number Theory* **16**(8) (2020), 1833–1858.
[10] L.-Y. Wang and H.-L. Wu, 'Applications of Lerch's theorem to permutations of quadratic residues', *Bull. Aust. Math. Soc.* **100** (2019), 362–371.
[11] H.-L. Wu and Y.-F. She, 'Jacobsthal sums and permutations of biquadratic residues', *Finite Fields Appl.* **70** (2021), Article no. 101789.
[12] G. Zolotarev, 'Nouvelle démonstration de la loi de réciprocité de Legendre,' *Nouv. Ann. Math.* **11** (1872), 354–362.

https://doi.org/10.1017/S000497272100054X Published online by Cambridge University Press

HAI-LIANG WU, School of Science,
Nanjing University of Posts and Telecommunications,
Nanjing 210023, PR China
e-mail: whl.math@smail.nju.edu.cn

YUE-FENG SHE, Department of Mathematics,
Nanjing University, Nanjing 210093, PR China
e-mail: she.math@smail.nju.edu.cn