

A talk given at *Number Theory Workshop at Nanjing University* (Oct. 26-28, 2018) and *Zhejiang Normal Univ.* (Nov. 16, 2018) and the *5th Sichuan-Chongqing Workshop on Number Theory* (Dec. 15-17, 2018)

## On permutations and identities related to quadratic residues

Zhi-Wei Sun

Nanjing University, Nanjing 210093, P. R. China

[zwsun@nju.edu.cn](mailto:zwsun@nju.edu.cn)

<http://math.nju.edu.cn/~zwsun>

December 16, 2018

## Three new conjectures posed in 2018

**Conjecture** (Z.-W. Sun, April 28, 2018). Any integer  $n > 1$  can be written as  $a^2 + b^2 + 3^c + 5^d$  with  $a, b, c, d \in \{0, 1, 2, \dots\}$ .

*Remark.* I have verified this for  $n$  up to  $2 \times 10^{10}$ . **Prize for the solution:** 3500 US dollars.

**Conjecture** (Z.-W. Sun, May 1, 2018). For any integer  $n > 1$ , we can write  $2n$  as the sum of a prime, a power of 2 and a power of 5.

*Remark.* I have verified this for  $n$  up to  $10^{10}$ .

**Conjecture** (Z.-W. Sun, 2018-12-03) If a group  $G$  contains no element of order among  $2, \dots, n+1$ , then any  $A \subseteq G$  with  $|A| = n$  can be written as  $\{a_1, \dots, a_n\}$  with  $a_1, a_2^2, \dots, a_n^n$  pairwise distinct.

*Remark.* I have confirmed this for torsion-free abelian groups  $G$ . It is even open for cyclic groups of prime order.

## Quadratic residues modulo primes

Let  $p$  be an odd prime. For  $a \in \mathbb{Z}$  with  $p \nmid a$ , if  $x^2 \equiv a \pmod{p}$  for some  $x \in \mathbb{Z}$ , then  $a$  is called a *quadratic residue* modulo  $p$ , otherwise  $a$  is called a *quadratic nonresidue* modulo  $p$ .

For example, 1, 2, 4 are quadratic residues mod 7, and 3, 5, 6 are quadratic nonresidue mod 7. (Note that  $3^2 \equiv 2 \pmod{7}$ .)

If  $x = pq + r$  with  $q, r \in \mathbb{Z}$  and  $|r| \leq (p-1)/2$ , then

$$x^2 \equiv r^2 = |r|^2 \pmod{p}.$$

If  $0 \leq j < k \leq (p-1)/2$ , then

$$k^2 - j^2 = (k-j)(k+j) \not\equiv 0 \pmod{p}.$$

Therefore

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$$

give all the  $(p-1)/2$  quadratic residues modulo  $p$ .

## Legendre symbols

Let  $p$  be an odd prime and  $a \in \mathbb{Z}$ . The Legendre symbol  $\left(\frac{a}{p}\right)$  is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ for some } x \in \mathbb{Z}, \\ -1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ for no } x \in \mathbb{Z}. \end{cases}$$

It is well known that  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$  for any  $a, b \in \mathbb{Z}$ . Also,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv -1 \pmod{4}; \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

**The Law of Quadratic Reciprocity:** If  $p$  and  $q$  are distinct odd primes, then

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

## Gauss' Lemma

Gauss' Lemma plays important roles in many proofs of the Quadratic Reciprocity.

**Gauss' Lemma.** Let  $p$  be an odd prime and let  $a \in \mathbb{Z}$  with  $p \nmid a$ . Then

$$\left(\frac{a}{p}\right) = (-1)^{|\{1 \leq k < \frac{p}{2} : \{\frac{ak}{p}\} > \frac{1}{2}\}|},$$

where  $\{x\}$  denotes the fractional part of a real number  $x$ .

This lemma was extended to Jacobi symbols by M. Jenkins in 1867.

**Jenkins' Extension:** Let  $n$  be a positive odd integer and let  $a \in \mathbb{Z}$  with  $\gcd(a, n) = 1$ . Then

$$\left(\frac{a}{n}\right) = (-1)^{|\{1 \leq k < \frac{n}{2} : \{\frac{ak}{n}\} > \frac{1}{2}\}|}.$$

## Zolotarev's Lemma

Recall that for a permutation  $a_{\sigma(1)}, \dots, a_{\sigma(n)}$  of  $a_1, \dots, a_n$ , its *sign* (or *signature*) is given by

$$\text{sign}(\sigma) = (-1)^{|\{(i,j): 1 \leq i < j \leq n \ \& \ \sigma(i) > \sigma(j)\}|}.$$

For  $a \in \mathbb{Z}$  and  $n \in \mathbb{Z}^+ = \{1, 2, 3, \dots\}$ , let  $\{a\}_n$  denote the least nonnegative residue of  $a$  modulo  $n$ .

**Zolotarev's Lemma (1872).** Let  $p$  be any odd prime, and let  $a \in \mathbb{Z}$  with  $p \nmid a$ . Then, the permutation  $\{aj\}_p$  ( $j = 1, \dots, p-1$ ) of  $1, \dots, p-1$  has the sign  $\left(\frac{a}{p}\right)$ .

**Frenbinus' Extension.** Let  $n$  be any positive odd integer relatively prime to  $a \in \mathbb{Z}$ . Then, the permutation  $\{aj\}_n$  ( $j = 0, \dots, n-1$ ) of  $0, 1, \dots, n-1$  has the sign  $\left(\frac{a}{n}\right)$ .

Recently, I noted that Zolotarev's Lemma is actually equivalent to Gauss' Lemma and Frenbinus' Extension is also equivalent to Jenkins' Extension of Gauss' Lemma.

## On the inverse of $k$ modulo $m$

Let  $m > 1$  be an odd integer, and let  $a_1 < \dots < a_{\varphi(m)}$  be all the numbers among  $1, \dots, m-1$  relatively prime to  $m$ . For each  $k \in \{1, \dots, m-1\}$  with  $\gcd(k, m) = 1$ , let  $\sigma_m(k) = \bar{k}$  be the inverse of  $k$  modulo  $m$ , that is,  $\bar{k} \in \{1, \dots, m-1\}$  and  $k\bar{k} \equiv 1 \pmod{m}$ . Then  $\sigma_m$  is a permutation of  $a_1, \dots, a_{\varphi(m)}$ .

Our following result determines  $\text{sign}(\sigma_m)$ .

**Theorem** (Z.-W. Sun, arXiv:1809.07766). For any odd integer  $m > 1$ , we have

$$\text{sign}(\sigma_m) = -1 \iff m \text{ is a power of a prime } p \equiv 1 \pmod{4}.$$

In particular,

$$\text{sign}(\sigma_p) = - \left( \frac{-1}{p} \right) \text{ for each odd prime } p.$$

## A mysterious discovery on Sept. 15, 2018

Let  $p = 2n + 1$  be an odd prime, and let  $a_1 < \dots < a_n$  be all the quadratic residues modulo  $p$  among  $1, \dots, p - 1$ . It is well known that  $\{1^2\}_p, \dots, \{n^2\}_p$  is a permutation of  $a_1, \dots, a_n$ . Let  $\pi_p$  denote this permutation. *What's the sign of the permutation  $\pi_p$ ?*

On Sept. 14, 2018, I made computation via Mathematica but could not see any pattern. Then I thought that perhaps  $\text{sign}(\pi_p)$  is distributed randomly.

After I waked up in the early morning of Sept. 15, 2018, I thought that it would be very interesting if  $\text{sign}(\pi_p)$  obeys certain pattern. Thus, I computed and analyzed  $\text{sign}(\pi_p)$  once again. This led to the following surprising discovery.

**Conjecture** (Z.-W. Sun, Sept. 15, 2018). Let  $p \equiv 3 \pmod{4}$  be a prime and let  $h(-p)$  be the class number of  $\mathbb{Q}(\sqrt{-p})$ . Then

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



## An example

For the prime  $p = 11$ ,

$$(\{1^2\}_{11}, \dots, \{5^2\}_{11}) = (1, 4, 9, 5, 3),$$

and

$$\begin{aligned} \{(j, k) : 1 \leq j < k \leq 5 \ \& \ \{j^2\}_{11} > \{k^2\}_{11}\} \\ &= \{(2, 5), (3, 4), (3, 5), (4, 5)\}. \end{aligned}$$

Thus

$$\text{sign}(\pi_{11}) = (-1)^4 = 1.$$

On  $\prod_{1 \leq i < j \leq (p-1)/2} (j^2 - i^2) \pmod p$

For an odd prime  $p$ , clearly  $\text{sign}(\pi_p)$  is the sign of the product

$$S_p := \prod_{1 \leq i < j \leq (p-1)/2} (\{j^2\}_p - \{i^2\}_p).$$

It is relatively easy to determine  $S_p$  modulo  $p$ .

**Theorem.** Let  $p = 2n + 1$  be an odd prime. Then

$$\prod_{1 \leq i < j \leq n} (j^2 - i^2) \equiv \begin{cases} -n! \pmod p & \text{if } p \equiv 1 \pmod 4, \\ 1 \pmod p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

*Sketch of My Proof.* This is because

$$\begin{aligned} & \prod_{1 \leq i < j \leq n} (j - i) \times \prod_{1 \leq i < j \leq n} (j + i) \\ &= \prod_{k=1}^n k^{n-k} \times \prod_{k=1}^n k^{\lfloor (k-1)/2 \rfloor} (p-k)^{\lfloor k/2 \rfloor} \\ &\equiv (-1)^{\sum_{k=0}^n \lfloor k/2 \rfloor} (n!)^{n-1} \pmod p \end{aligned}$$

and  $(n!)^2 \equiv (-1)^{n+1} \pmod p$  by Wilson's theorem.

On  $\prod_{1 \leq i < j \leq (p-1)/2} (i^2 + j^2) \pmod p$

On Sept. 16, 2018, I considered  $\prod_{1 \leq i < j \leq (p-1)/2} (i^2 + j^2) \pmod p$  and found that for any prime  $p > 3$  with  $p \equiv 3 \pmod 4$  we have

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

On Sept. 25, I obtained a proof, but soon Dr. Quanhui Yang told me that this is not new. The congruence appeared in the book G. J. Szekely (ed.), *Contests in Higher Mathematics*, Springer, New York, 1996.

**Theorem** (Z.-W. Sun, arXiv:1809.07766). For any prime  $p \equiv 1 \pmod 4$ , we have the new congruence

$$\prod_{\substack{1 \leq i < j \leq (p-1)/2 \\ p \nmid i^2 + j^2}} (i^2 + j^2) \equiv (-1)^{\lfloor (p-5)/8 \rfloor} \pmod p.$$

## A general congruence

**Theorem** (Z.-W. Sun, arXiv:1809.07766). Let  $p$  be an odd prime, and let  $a, b, c \in \mathbb{Z}$  with  $ac(a+b+c) \not\equiv 0 \pmod{p}$ . Set  $\Delta = b^2 - 4ac$ . Then

$$\prod_{\substack{1 \leq i < j \leq p-1 \\ p \nmid ai^2 + bij + cj^2}} (ai^2 + bij + cj^2) \equiv \begin{cases} \left(\frac{a(a+b+c)}{p}\right) \pmod{p} & \text{if } p \mid \Delta, \\ -\left(\frac{ac(a+b+c)\Delta}{p}\right) \pmod{p} & \text{if } p \nmid \Delta. \end{cases}$$

Consequently, if  $a + c = 0$  then

$$\begin{aligned} & \prod_{\substack{i, j=1 \\ p \nmid ai^2 + bij + cj^2}}^{(p-1)/2} (ai^2 + bij + cj^2) \\ & \equiv \begin{cases} \pm \frac{p-1}{2}! \pmod{p} & \text{if } \left(\frac{\Delta}{p}\right) = -1 \text{ or } (p \mid \Delta \ \& \ \left(\frac{2b}{p}\right) = 1), \\ \pm 1 \pmod{p} & \text{if } \left(\frac{\Delta}{p}\right) = 1 \text{ or } (p \mid \Delta \ \& \ \left(\frac{2b}{p}\right) = -1). \end{cases} \end{aligned}$$

## An auxiliary result

To prove such congruences, we need a known result on character sums.

**Lemma.** Let  $p$  be an odd prime, and let  $a, b, c \in \mathbb{Z}$  with  $a$  or  $b$  not divisible by  $p$ . Then

$$\sum_{x=0}^{p-1} \left( \frac{ax^2 + bx + c}{p} \right) = \begin{cases} -\left(\frac{a}{p}\right) & \text{if } p \nmid b^2 - 4ac, \\ (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2 - 4ac. \end{cases}$$

On  $\prod_{\substack{1 \leq i, j \leq (p-1)/2 \\ p \nmid i^2 - Aij - j^2}} (i^2 - Aij - j^2)$  modulo  $p$

**Theorem** (Sun, arXiv:1810.12102) Let  $p$  be an odd prime and let  $A \in \mathbb{Z}$ . Let  $u_0 = 0$ ,  $u_1 = 1$ , and  $u_{n+1} = Au_n + u_{n-1}$  for  $n \in \mathbb{Z}^+$ . If  $(\frac{A^2+4}{p}) = 1$ , then

$$\prod_{\substack{i, j=1 \\ p \nmid i^2 - Aij - j^2}}^{(p-1)/2} (i^2 - Aij - j^2) \equiv \begin{cases} -(A^2 + 4)^{(p-1)/4} \pmod{p} & \text{if } p \equiv 1 \pmod{4}, \\ -(A^2 + 4)^{(p+1)/4} u_{(p-1)/2} / 2 \pmod{p} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

If  $(\frac{A^2+4}{p}) = -1$ , then

$$\prod_{i, j=1}^{(p-1)/2} (i^2 - Aij - j^2) \equiv \begin{cases} (-A^2 - 4)^{(p-1)/4} \pmod{p} & \text{if } p \equiv 1 \pmod{4}, \\ (-A^2 - 4)^{(p+1)/4} u_{(p+1)/2} / 2 \pmod{p} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

## A corollary

**Theorem** (Sun, arXiv:1810.12102) Let  $p$  be an odd prime.

(i) We have

$$\prod_{\substack{i,j=1 \\ p \nmid i^2 - (i+j)j}}^{(p-1)/2} (i^2 - (i+j)j) \equiv \begin{cases} -5^{(p-1)/4} \pmod{p} & \text{if } p \equiv 1, 9 \pmod{20}, \\ (-1)^{\lfloor \frac{p-5}{10} \rfloor} \pmod{p} & \text{if } p \equiv 11, 19 \pmod{20}, \end{cases}$$

$$\prod_{i,j=1}^{(p-1)/2} (i^2 - (i+j)j) \equiv \begin{cases} (-1)^{\lfloor (p-10)/20 \rfloor} \pmod{p} & \text{if } p \equiv 3, 7 \pmod{20}, \\ (-5)^{(p-1)/4} \pmod{p} & \text{if } p \equiv 13, 17 \pmod{20}. \end{cases}$$

(ii) We have

$$\prod_{\substack{i,j=1 \\ p \nmid i^2 - (2i+j)j}}^{(p-1)/2} (i^2 - (2i+j)j) \equiv \begin{cases} -2^{(p-1)/4} \pmod{p} & \text{if } p \equiv 1 \pmod{8}, \\ (-1)^{(p-7)/8} \pmod{p} & \text{if } p \equiv 7 \pmod{8}, \end{cases}$$

$$\prod_{i,j=1}^{(p-1)/2} (i^2 - (2i+j)j) \equiv \begin{cases} (-1)^{(p-3)/8} \pmod{p} & \text{if } p \equiv 3 \pmod{8}, \\ 2^{(p-1)/4} \pmod{p} & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

## Known results involving $\zeta = e^{2\pi i/p}$

**Lemma** Let  $p$  be an odd prime, and let  $\zeta = e^{2\pi i/p}$ .

(i) For any  $a \in \mathbb{Z}$  with  $p \nmid a$ , we have

$$\prod_{n=1}^{p-1} (1 - \zeta^{an}) = p,$$

$$\sum_{x=0}^{p-1} \zeta^{ax^2} = \left(\frac{a}{p}\right) \sqrt{(-1)^{(p-1)/2} p} \quad (\text{Gauss}).$$

(ii) (Dirichlet's class number formula) If  $p \equiv 1 \pmod{4}$ , then

$$\prod_{n=1}^{p-1} (1 - \zeta^n)^{\binom{n}{p}} = \varepsilon_p^{-2h(p)},$$

where  $\varepsilon_p$  and  $h(p)$  are the fundamental unit and the class number of the quadratic field  $\mathbb{Q}(\sqrt{p})$  respectively. When  $p \equiv 3 \pmod{4}$ , we have

$$ph(-p) = - \sum_{k=1}^{p-1} k \left(\frac{k}{p}\right).$$



$$\text{On } \prod_{k=1}^{(p-1)/2} (1 - \zeta^{ak^2})$$

**Theorem** (Z.-W. Sun, arXiv:1809.07766). Let  $p > 3$  be a prime and let  $\zeta = e^{2\pi i/p}$ . Let  $a$  be any integer not divisible by  $p$ .

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

$$\prod_{k=1}^{(p-1)/2} (1 - \zeta^{ak^2}) = \sqrt{p} \varepsilon_p^{-\left(\frac{a}{p}\right)h(p)}.$$

(ii) If  $p \equiv 3 \pmod{4}$ , then

$$\prod_{k=1}^{(p-1)/2} (1 - \zeta^{ak^2}) = (-1)^{(h(-p)+1)/2} \left(\frac{a}{p}\right) \sqrt{p} i.$$

On  $\prod_{k=1}^{(p-1)/2} \sin \pi \frac{ak^2}{p}$  and  $\prod_{k=1}^{(p-1)/2} \cos \pi \frac{ak^2}{p}$

**Corollary.** Let  $p > 3$  be a prime and let  $a \in \mathbb{Z}$  with  $p \nmid a$ . Then

$$2^{(p-1)/2} \prod_{k=1}^{(p-1)/2} \sin \pi \frac{ak^2}{p} = (-1)^{(a+1)\lfloor (p+1)/4 \rfloor} \sqrt{p} \times \begin{cases} \varepsilon_p^{-\left(\frac{a}{p}\right)h(p)} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{(h(-p)+1)/2} \left(\frac{a}{p}\right) & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

and

$$2^{(p-1)/2} \prod_{k=1}^{(p-1)/2} \cos \pi \frac{ak^2}{p} = \begin{cases} \varepsilon_p^{(1-\left(\frac{2}{p}\right))\left(\frac{a}{p}\right)h(p)} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{(p+1)/4} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

## More identities involving the sine and cosine functions

**Theorem** (Z.-W. Sun, arXiv:1809.07766). Let  $p$  be an odd prime and let  $a \in \mathbb{Z}$  with  $p \nmid a$ . Then

$$\prod_{\substack{1 \leq j < k \leq (p-1)/2 \\ p \nmid j^2+k^2}} \sin \pi \frac{a(j^2 + k^2)}{p}$$

$$= \left( \frac{p}{2^{p-1}} \right)^{(p - (\frac{-1}{p}) - 4)/8} \times \begin{cases} \varepsilon_p^{(\frac{a}{p})h(p)(1+(\frac{2}{p}))/2} & \text{if } 4 \mid p-1, \\ (-1)^{(p-3)/8} & \text{if } 8 \mid p-3, \\ (-1)^{(p+1)/8+(h(-p)+1)/2} \left(\frac{a}{p}\right) & \text{if } 8 \mid p-7, \end{cases}$$

and

$$\prod_{1 \leq j < k \leq (p-1)/2} \cos \pi \frac{a(j^2 + k^2)}{p} = (-1)^{a \frac{p+1}{2} \lfloor \frac{p-1}{4} \rfloor} 2^{-\frac{p-1}{2} \lfloor \frac{p-3}{4} \rfloor}.$$

## More identities involving the sine and cosine functions

**Theorem** (Z.-W. Sun, arXiv:1809.07766). Let  $p$  be an odd prime, and let  $a, b, c \in \mathbb{Z}$  with  $ac(a+b+c) \not\equiv 0 \pmod{p}$ . Set  $\Delta = b^2 - 4ac$  and

$$m = \sum_{\substack{1 \leq j < k \leq p-1 \\ p \nmid aj^2 + bjk + ck^2}} (aj^2 + bjk + ck^2).$$

Then

$$\begin{aligned} & (-1)^m (2^{p-1} p^{-1})^{(p-3 - (\frac{\Delta}{p}))/2} \prod_{\substack{1 \leq j < k \leq p-1 \\ p \nmid aj^2 + bjk + ck^2}} \sin \pi \frac{aj^2 + bjk + ck^2}{p} \\ &= \begin{cases} (-1)^{(b + (\frac{\Delta}{p})) \frac{p-1}{4}} \varepsilon_p^{h(p)((1-p + p(\frac{\Delta}{p})^2)(\frac{a}{p}) + (\frac{c}{p}) + (\frac{a+b+c}{p}))} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{a+b} \frac{p-3}{4} \left( \frac{a(a+b+c)}{p} \right) & \text{if } 4 \mid p-3 \text{ \& } p \mid \Delta, \\ (-1)^{a+(b-1) \frac{p-3}{4} + \frac{h(-p)+1}{2}} \left( \frac{ac(a+b+c)\Delta}{p} \right) & \text{if } 4 \mid p-3 \text{ \& } p \nmid \Delta. \end{cases} \end{aligned}$$

## More identities involving the sine and cosine functions

Consequently,

$$\begin{aligned}
 & 2^{(p-1)(p-3-\frac{\Delta}{p})/2} \prod_{1 \leq j < k \leq p-1} \cos \pi \frac{aj^2 + bjk + ck^2}{p} \\
 = & \begin{cases} (-1)^{b(p-1)/4} \varepsilon_p^{h(p)((\frac{2}{p})-1)((1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))} & \text{if } 4 \mid p-1, \\
 (-1)^{a+b(p-3)/4+(\frac{\Delta}{p})(p+1)/4} & \text{if } 4 \mid p-3. \end{cases}
 \end{aligned}$$

## Determination of $\text{sign}(\pi_p)$ for $p \equiv 3 \pmod{4}$

**Theorem** (Z.-W. Sun, arXiv:1809.07766). Let  $p$  be a prime with  $p \equiv 3 \pmod{4}$ . Then

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

Moreover, for any  $a \in \mathbb{Z}$  with  $p \nmid a$ , we have

$$\begin{aligned} \prod_{1 \leq j < k \leq (p-1)/2} \csc \pi \frac{a(k^2 - j^2)}{p} &= \prod_{1 \leq j < k \leq (p-1)/2} \left( \cot \pi \frac{aj^2}{p} - \cot \pi \frac{ak^2}{p} \right) \\ &= \begin{cases} (2^{p-1}/p)^{(p-3)/8} & \text{if } p \equiv 3 \pmod{8}, \\ (-1)^{(h(-p)+1)/2} \left(\frac{a}{p}\right) (2^{p-1}/p)^{(p-3)/8} & \text{if } p \equiv 7 \pmod{8}, \end{cases} \end{aligned}$$

*Remark.* Note that for  $1 \leq j < k \leq (p-1)/2$  we have

$$\{j^2\}_p > \{k^2\}_p \iff \cot \pi \frac{j^2}{p} < \cot \pi \frac{k^2}{p}.$$

## Reduction to $\prod_{1 \leq j < k \leq (p-1)/2} \sin \pi \frac{a(k^2 - j^2)}{p}$

For real numbers  $\theta_1$  and  $\theta_2$ , clearly

$$\cot \pi \theta_1 - \cot \pi \theta_2 = \frac{\cos \pi \theta_1}{\sin \pi \theta_1} - \frac{\cos \pi \theta_2}{\sin \pi \theta_2} = \frac{\sin \pi(\theta_2 - \theta_1)}{\sin \pi \theta_1 \sin \pi \theta_2}.$$

Thus

$$\begin{aligned} & \prod_{1 \leq j < k \leq (p-1)/2} \frac{\sin \pi a(k^2 - j^2)/p}{\cot \pi a j^2/p - \cot \pi a k^2/p} \\ &= \prod_{1 \leq j < k \leq (p-1)/2} \sin \pi \frac{a j^2}{p} \sin \pi \frac{a k^2}{p} \\ &= \prod_{k=1}^{(p-1)/2} \left( \sin \pi \frac{a k^2}{p} \right)^{|\{1 \leq j \leq (p-1)/2: j \neq k\}|}. \end{aligned}$$

Recall that we have determined the value of  $\prod_{k=1}^{(p-1)/2} \sin \pi \frac{a k^2}{p}$ .

Reduction to  $\prod_{1 \leq j < k \leq (p-1)/2} (e^{2\pi i a j^2/p} - e^{2\pi i a k^2/p})$

For  $1 \leq j < k \leq (p-1)/2$ , clearly

$$\begin{aligned} \sin \pi \frac{a(k^2 - j^2)}{p} &= \frac{e^{i\pi a(k^2 - j^2)/p} - e^{-i\pi a(k^2 - j^2)/p}}{2i} \\ &= \frac{i}{2} e^{-i\pi a(k^2 + j^2)/p} (e^{2\pi i a j^2/p} - e^{2\pi i a k^2/p}). \end{aligned}$$

It is easy to show that

$$\sum_{1 \leq j < k \leq (p-1)/2} (j^2 + k^2) = \frac{p-3}{2} \sum_{k=1}^{(p-1)/2} k^2 = \frac{p-3}{2} \cdot \frac{p^2-1}{24} p.$$



Determine  $\prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{aj^2} - \zeta^{ak^2})^2$  with  $\zeta = e^{2\pi i/p}$

$$\begin{aligned}
 & \prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{aj^2} - \zeta^{ak^2})^2 \\
 = & (-1)^{\binom{(p-1)/2}{2}} \prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{aj^2} - \zeta^{ak^2})(\zeta^{ak^2} - \zeta^{aj^2}) \\
 = & (-1)^{\binom{(p-1)/2}{2}} \prod_{k=1}^{(p-1)/2} \prod_{\substack{j=1 \\ j \neq k}}^{(p-1)/2} (\zeta^{ak^2} - \zeta^{aj^2}) \\
 = & (-1)^{(p-1)(p-3)/8} \prod_{n=1}^{p-1} (1 - \zeta^{an})^{r(n)},
 \end{aligned}$$

where

$$\begin{aligned}
 r(n) &= |\{(j, k) : 1 \leq j, k < p/2 \text{ \& } j^2 - k^2 \equiv n \pmod{p}\}| \\
 &= \sum_{\substack{0 < x < p \\ p \nmid n+x}} \frac{\binom{x}{p} + 1}{2} \cdot \frac{\binom{n+x}{p} + 1}{2} = \left\lfloor \frac{p-1}{4} \right\rfloor - \frac{1 + \binom{-1}{p}}{2} \cdot \frac{1 + \binom{n}{p}}{2}.
 \end{aligned}$$

The value of  $\prod_{1 \leq j < k \leq (p-1)/2} (e^{2\pi i a j^2 / p} - e^{2\pi i a k^2 / p})^2$

When  $p \equiv 1 \pmod{4}$ , we get

$$\prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{aj^2} - \zeta^{ak^2})^2 = (-1)^{(p-1)/4} p^{(p-3)/4} \varepsilon_p^{(\frac{a}{p})h(p)}.$$

If  $p \equiv 3 \pmod{4}$ , then

$$\prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{aj^2} - \zeta^{ak^2})^2 = (-p)^{(p-3)/4}.$$

*How to determine the value of  $\prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{aj^2} - \zeta^{ak^2})$  in the case  $p \equiv 3 \pmod{4}$ ?*

**We need Galois theory!**

## The cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$

Let  $n > 1$  be an integer and let  $\zeta_n = e^{2\pi i/n}$ . The minimal polynomial of  $\zeta_n$  over  $\mathbb{Q}$  is the cyclotomic polynomial

$$\Phi_n(x) = \prod_{\substack{a=1 \\ (a,n)=1}}^n (x - \zeta_n^a) \in \mathbb{Z}[x].$$

It is known that the Galois group

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma \in \text{Aut}(\mathbb{Q}(\zeta_n)) : \sigma(r) = r \text{ for all } r \in \mathbb{Q}\}$$

has exactly  $\varphi(n)$  elements, and they are

$$\varphi_a \quad (1 \leq a \leq n \text{ \& } (a, n) = 1) \text{ with } \varphi_a(\zeta_n) = \zeta_n^a.$$

The value of  $\prod_{1 \leq j < k \leq (p-1)/2} (e^{2\pi i a j^2/p} - e^{2\pi i a k^2/p})^2$

Let  $p$  be an odd prime let  $\zeta = e^{2\pi i/p}$ . Let  $a \in \mathbb{Z}$  with  $p \nmid a$ , and let  $\varphi_a \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  with  $\varphi_a(\zeta) = \zeta^a$ . Then

$$\begin{aligned} \varphi_a \left( \sqrt{(-1)^{(p-1)/2} p} \right) &= \varphi_a \left( \sum_{x=0}^{p-1} \zeta^{x^2} \right) \\ &= \sum_{x=0}^{p-1} \zeta^{ax^2} = \left( \frac{a}{p} \right) \sqrt{(-1)^{(p-1)/2} p}. \end{aligned}$$

Now assume that  $p \equiv 3 \pmod{4}$ . Recall that

$$\prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{j^2} - \zeta^{k^2})^2 = (-p)^{(p-3)/4}.$$

So, for some  $\varepsilon \in \{\pm 1\}$ , we have

$$\prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{j^2} - \zeta^{k^2}) = \varepsilon (\sqrt{p} i)^{(p-3)/4}.$$

On  $\prod_{1 \leq j < k \leq (p-1)/2} (e^{2\pi i a j^2/p} - e^{2\pi i a k^2/p})$

Applying the automorphism  $\varphi_a$  of the cyclotomic field  $\mathbb{Q}(\zeta)$ , we get

$$\prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{a j^2} - \zeta^{a k^2}) = \varepsilon \varphi_a(\sqrt{p} i)^{(p-3)/4} = \varepsilon \left( \left( \frac{a}{p} \right) \sqrt{p} i \right)^{(p-3)/4}.$$

Thus, for any  $r = 1, \dots, (p-1)/2$  we have

$$\prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{r^2 j^2} - \zeta^{r^2 k^2}) = \varepsilon (\sqrt{p} i)^{(p-3)/4};$$

on the other hand,

$$\prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{r^2 j^2} - \zeta^{r^2 k^2}) = \prod_{1 \leq j < k \leq (p-1)/2} (1 - \zeta^{r^2(k^2-j^2)}).$$

## Determine $\varepsilon$

Therefore

$$\begin{aligned} & \left( \varepsilon (\sqrt{p} i)^{(p-3)/4} \right)^{(p-1)/2} \\ &= \prod_{1 \leq j < k \leq (p-1)/2} \prod_{r=1}^{(p-1)/2} (1 - \zeta^{(k^2-j^2)r^2}) \\ &= \prod_{1 \leq j < k \leq (p-1)/2} \left( (-1)^{h(-p)+1/2} \left( \frac{k^2-j^2}{p} \right) \sqrt{p} i \right). \end{aligned}$$

and hence

$$\begin{aligned} \varepsilon = \varepsilon^{(p-1)/2} &= (-1)^{\frac{h(-p)+1}{2} \cdot \frac{(p-1)(p-3)}{8}} \prod_{1 \leq j < k \leq (p-1)/2} \left( \frac{k^2-j^2}{p} \right) \\ &= (-1)^{\frac{h(-p)+1}{2} \cdot \frac{p-3}{4}}. \end{aligned}$$

## Another theorem and a related conjecture

**Theorem** (Sun, arXiv:1809.07766). Let  $p$  be an odd prime and let  $\zeta = e^{2\pi i/p}$ . Let  $a \in \mathbb{Z}$  with  $p \nmid a$ . Then

$$\begin{aligned} & (-1)^{a \frac{p+1}{2} \lfloor \frac{p-1}{4} \rfloor} 2^{(p-1)(p-3)/8} \prod_{1 \leq j < k \leq (p-1)/2} \cos \pi \frac{a(k^2 - j^2)}{p} \\ &= \prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{aj^2} + \zeta^{ak^2}) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod{4}, \\ \pm \varepsilon_p^{\left(\frac{a}{p}\right) h(p) \left(\left(\frac{2}{p}\right) - 1\right)/2} & \text{if } p \equiv 1 \pmod{4}. \end{cases} \end{aligned}$$

**Conjecture** (Sun, arXiv:1809.07766). Let  $p$  be a prime with  $p \equiv 1 \pmod{4}$ , and let  $\zeta = e^{2\pi i/p}$ . Let  $a$  be an integer not divisible by  $p$ . Then

$$\begin{aligned} & (-1)^{|\{1 \leq k < p/4 : \left(\frac{k}{p}\right) = -1\}|} \prod_{1 \leq j < k \leq (p-1)/2} (\zeta^{aj^2} + \zeta^{ak^2}) \\ &= \begin{cases} 1 & \text{if } p \equiv 1 \pmod{8}, \\ \left(\frac{a}{p}\right) \varepsilon_p^{-\left(\frac{a}{p}\right) h(p)} & \text{if } p \equiv 5 \pmod{8}. \end{cases} \end{aligned}$$

On  $\left| \left\{ 1 \leq k \leq \frac{p-1}{2} : \{k^m\}_p > \frac{p}{2} \right\} \right|$

**Conjecture** (Sun, arXiv:1809.07766). (i) For any prime  $p \equiv 5 \pmod{6}$ , we have

$$\left| \left\{ 1 \leq k \leq \frac{p-1}{2} : \{k^3\}_p > \frac{p}{2} \right\} \right| - \frac{p+1}{6} \in \{2n : n = 0, 1, 2, \dots\},$$

$$|\{(j, k) : 1 \leq j < k \leq p-1 \text{ and } \{j^3\}_p > \{k^3\}_p\}| \equiv \frac{p+1}{6} \pmod{2}.$$

(ii) For any integer  $m > 1$ , we have

$$\left| \left\{ 1 \leq k \leq \frac{p-1}{2} : \{k^m\}_p > \frac{p}{2} \right\} \right| \sim \frac{p}{4} \quad (\text{as } p \rightarrow \infty)$$

*Remark.* The parity in part (i) was confirmed by my PhD students Li-Yuan Wang and Hai-Liang Wu, while part (ii) was confirmed by Zhe-Feng Xu who proved that

$$\left| \left\{ 1 \leq k \leq \frac{p-1}{2} : \{k^m\}_p > \frac{p}{2} \right\} \right| = \frac{p}{4} + O(\sqrt{p} \log^2 p).$$



## Conjecture on determinants involving the tangent function

**Conjecture** (Sun, arXiv:1809.07766). Let  $p > 3$  be a prime.

(i) Define the matrices  $T_p^+$  and  $T_p^-$  by

$$T_p^+ := \left[ \tan \pi \frac{i^2 + j^2}{p} \right]_{0 \leq i, j \leq (p-1)/2}, \quad T_p^- := \left[ \tan \pi \frac{i^2 - j^2}{p} \right]_{0 \leq i, j \leq (p-1)/2}.$$

If  $p \equiv 3 \pmod{4}$ , then

$$\det T_p^+ = 2^{(p-1)/2} p^{(p+1)/4}, \quad \det T_p^- = p^{(p+1)/4}.$$

(ii) Let  $(T_p^+)_*$  (resp.,  $(T_p^-)_*$ ) be the matrix obtaining from  $T_p^+$  (resp.,  $T_p^-$ ) via replacing all the entries in the first row by 1. Then

$$\det(T_p^+)_* = \begin{cases} (-p)^{(p-1)/4} & \text{if } p \equiv 1 \pmod{4}, \\ 2^{(p-1)/2} (-p)^{(p-3)/4} \sqrt{p} & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

$$\det(T_p^-)_* = \begin{cases} p^{(p-1)/4} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{(h(-p)-1)/2} (-p)^{(p-3)/4} \sqrt{p} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

*Remark.*  $\det T_p^+ = \det T_p^- = 0$  if  $p \equiv 1 \pmod{4}$ .

## A very challenging conjecture on quadratic residues

During Oct. 1-8, I visited the Center of Applied Math. at Tianjin Univ. Prof. Qing-Hu Hou and I wish to find a combinatorial proof of my result that  $\text{sign}(\pi_p) = 1$  for primes  $p \equiv 3 \pmod{8}$ . As a by-product, we formulate a **quite mysterious conjecture** on quadratic residues modulo primes which looks very challenging!

## A very challenging conjecture on quadratic residues

During Oct. 1-8, I visited the Center of Applied Math. at Tianjin Univ. Prof. Qing-Hu Hou and I wish to find a combinatorial proof of my result that  $\text{sign}(\pi_p) = 1$  for primes  $p \equiv 3 \pmod{8}$ . As a by-product, we formulate a **quite mysterious conjecture** on quadratic residues modulo primes which looks very challenging!

We will announce the conjecture at the beginning of 2019.

## Main references:

1. Z.-W. Sun, *Quadratic residues and related permutations and identities*, arXiv:1809.07766,  
<http://arxiv.org/abs/1809.07766>
2. Z.-W. Sun, *On quadratic residues and quartic residues modulo primes*, arXiv:1810.12102, <http://arxiv.org/abs/1810.12102>

Thank you!