A talk given at *the Int. Chengdu Number Theory Confer.*
(December 10-12, 2022)

New Results on Power Residues modulo Primes

Zhi-Wei Sun

Nanjing University, Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

December 12, 2022

Abstract

In this talk we introduce some new results on power residues modulo primes.

Let p be an odd prime, and let a be an integer not divisible by p. When m is a positive integer with $p \equiv 1 \pmod{2m}$ and 2 is an mth power residue modulo p, the speaker determines the value of the product $\prod_{k\in R_m(p)}(1+\tan\pi\frac{ak}{p})$, where

$R_m(p) = \{0 < k < p:\ k \in \mathbb{Z} \text{ is an } m\text{th power residue modulo } p\}$.

Let $p > 3$ be a prime. Let $b \in \mathbb{Z}$ and $\varepsilon \in \{\pm 1\}$. Joint with Q.-.H. Hou and H. Pan, we prove that

$$\left|\left\{N_p(a,b):\ 1 < a < p \text{ and } \left(\frac{a}{p}\right) = \varepsilon\right\}\right| = \frac{3-(\frac{-1}{p})}{2},$$

where $N_p(a,b)$ is the number of positive integers $x < p/2$ with $\{x^2+b\}_p > \{ax^2+b\}_p$, and $\{m\}_p$ with $m \in \mathbb{Z}$ is the least nonnegative residue of m modulo p.

We will also mention some open conjectures.

Part A. Two Products related to Quadratic and Quartic Residues

The product $S_p(a,b,c)$ in the case $p \nmid ac(a+b+c)$

For $a,b,c \in \mathbb{Z}$, how to determine

$$S_p(a,b,c) := \prod_{\substack{1 \leqslant i < j \leqslant p-1 \\ p \nmid ai^2+bij+cj^2}} (ai^2+bij+cj^2)$$

modulo an odd prime p. This may be viewed as an analogue problem of Wilson's theorem for binary quadratic forms.

Theorem 1 (Z.-W. Sun [Finite Fields Appl. 59(2019)]). Let $a,b,c \in \mathbb{Z}$ with $ac(a+b+c) \not\equiv 0 \pmod p$, and set $\Delta = b^2 - 4ac$. Then

$$S_p(a,b,c) \equiv \begin{cases} \left(\frac{a(a+b+c)}{p}\right) \pmod p & \text{if } p \mid \Delta, \\ -\left(\frac{ac(a+b+c)\Delta}{p}\right) \pmod p & \text{if } p \nmid \Delta, \end{cases}$$

where $(\frac{\cdot}{p})$ is the Legendre symbol.

Remark. I first found this result via a computer.

$S_p(a,b,c)$ mod p in the case $p \mid ac(a+b+c)$

Theorem 2 (Z.-W. Sun [Int. J. Number Theory 16(2020), 1833-1858]). Let p be an odd prime. In the case $p \mid ac(a+b+c)$, we have

$$S_p(a,b,c) \equiv \begin{cases} 0 \pmod p & \text{if } p \mid a,\ p \mid b\ \&\ p \mid c, \\ -(\frac{-a}{p}) \pmod p & \text{if } p \nmid a,\ p \mid b\ \&\ p \mid c, \\ -(\frac{b}{p}) \pmod p & \text{if } p \mid a,\ p \nmid b\ \&\ p \mid c, \\ -(\frac{-c}{p}) \pmod p & \text{if } p \mid a,\ p \mid b\ \&\ p \nmid c, \\ -(\frac{c}{p}) \pmod p & \text{if } p \mid a,\ p \nmid bc\ \&\ p \mid b+c, \\ -(\frac{a}{p}) \pmod p & \text{if } p \nmid ab,\ p \mid a+b\ \&\ p \mid c, \\ -(\frac{-a}{p}) \pmod p & \text{if } p \nmid ac,\ p \mid a-c,\ p \mid a+b+c, \\ (\frac{-ac}{p}) \pmod p & \text{if } p \nmid ac(a-c)\ \&\ p \mid a+b+c, \\ (\frac{-a(a+b)}{p}) \pmod p & \text{if } p \nmid ab(a+b)\ \&\ p \mid c, \\ (\frac{-c(b+c)}{p}) \pmod p & \text{if } p \mid a\ \&\ p \nmid bc(b+c). \end{cases}$$

Gauss' Lemma and Jenkins' extension

Gauss' Lemma. For any odd prime p and integer $x \not\equiv 0 \pmod{p}$, we have

$$\left(\frac{x}{p}\right) = (-1)^{|\{1 \leqslant k < p/2:\ \{kx\}_p > p/2\}|},$$

where $\{x\}_n$ denotes the least nonnegative integer r with $x \equiv r \pmod{n}$.

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

Jenkins (1867): For any positive odd integer n and integer x with $\gcd(x, n) = 1$, we have

$$\left(\frac{x}{n}\right) = (-1)^{|\{1 \leqslant k < n/2:\ \{kx\}_n > n/2\}|},$$

where $(\frac{\cdot}{n})$ is the Jacobi symbol.

An auxiliary theorem

Auxiliary Theorem (Z.-W. Sun [Int. J. Number Theory 16(2020), 1833-1858]). Let n be a positive odd integer, and let $x \in \mathbb{Z}$ with $\gcd(x(1-x), n) = 1$. Then

$$(-1)^{|\{1\leqslant k<n/2:\ \{kx\}_n>k\}|} = \left(\frac{2x(1-x)}{n}\right).$$

Also,

$$(-1)^{|\{1\leqslant k<n/2:\ \{kx\}_n>n/2\ \&\ \{k(1-x)\}_n>n/2\}|} = \left(\frac{2}{n}\right),$$

$$(-1)^{|\{1\leqslant k<n/2:\ \{kx\}_n<n/2\ \&\ \{k(1-x)\}_n<n/2\}|} = \left(\frac{2x(x-1)}{n}\right),$$

and

$$(-1)^{|\{1\leqslant k<n/2:\ \{kx\}_n>n/2>\{k(1-x)\}_n\}|} = \left(\frac{2x}{n}\right).$$

Lucas sequences

For any $A \in \mathbb{Z}$, we define the Lucas sequences $\{u_n(A)\}_{n\geqslant 0}$ and $\{v_n(A)\}_{n\geqslant 0}$ by

$$u_0(A) = 0,\ u_1(A) = 1, \text{ and } u_{n+1}(A) = Au_n(A) + u_{n-1}(A) \text{ for } n \in \mathbb{Z}^+,$$

and

$$v_0(A) = 2,\ v_1(A) = A, \text{ and } v_{n+1}(A) = Av_n(A) + v_{n-1}(A) \text{ for } n \in \mathbb{Z}^+.$$

It is well known that

$$u_n(A) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n(A) = \alpha^n + \beta^n$$

for all $n \in \mathbb{N} = \{0, 1, 2, \dots\}$, where

$$\alpha = \frac{A + \sqrt{A^2 + 4}}{2} \quad \text{and} \quad \beta = \frac{A - \sqrt{A^2 + 4}}{2}.$$

$T_p(a, b, c)$

Let p be an odd prime. The speaker introduced for $a, b, c \in \mathbb{Z}$ the product

$$T_p(a, b, c) := \prod_{\substack{i,j=1 \\ p \nmid ai^2+bij+cj^2}}^{(p-1)/2} (ai^2 + bij + cj^2),$$

and determined $T_p(a, b, c) \bmod p$ in the case $a + c = 0$.

On $T_p(1,-A,-1) \bmod p$

Theorem 3 (Z.-W. Sun [Int. J. Number Theory 16(2020)]). Let p be an odd prime and let $A \in \mathbb{Z}$.

(i) Suppose that $p \mid (A^2+4)$. Then $4 \mid p-1$, $\frac{A}{2} \equiv (-1)^k \frac{p-1}{2}! \pmod p$ for some $k \in \{0,1\}$, and

$$T_p(1,-A,-1) \equiv \begin{cases} (-1)^{(p+7)/8} \frac{p-1}{2}! \pmod p & \text{if } 8 \mid p-1, \\ (-1)^{k+(p-5)/8} \pmod p & \text{if } 8 \mid p-5. \end{cases}$$

(ii) When $(\frac{A^2+4}{p}) = 1$, we have

$$T_p(1,-A,-1) \equiv \begin{cases} -(A^2+4)^{\frac{p-1}{4}} \pmod p & \text{if } 4 \mid p-1, \\ -(A^2+4)^{\frac{p+1}{4}} u_{(p-1)/2}(A)/2 \pmod p & \text{if } 4 \mid p-3. \end{cases}$$

(iii) When $(\frac{A^2+4}{p}) = -1$, we have

$$T_p(1,-A,-1) \equiv \begin{cases} (-A^2-4)^{\frac{p-1}{4}} \pmod p & \text{if } 4 \mid p-1, \\ (-A^2-4)^{\frac{p+1}{4}} u_{(p+1)/2}(A)/2 \pmod p & \text{if } 4 \mid p-3. \end{cases}$$

A corollary

Corollary 1. Let p be an odd prime.

(i) We have

$$T_p(1,-1,-1) \equiv \begin{cases} -5^{(p-1)/4} \pmod p & \text{if } p \equiv 1,9 \pmod{20}, \\ (-5)^{(p-1)/4} \pmod p & \text{if } p \equiv 13,17 \pmod{20}, \\ (-1)^{\lfloor (p-10)/20 \rfloor} \pmod p & \text{if } p \equiv 3,7 \pmod{20}, \\ (-1)^{\lfloor (p-5)/10 \rfloor} \pmod p & \text{if } p \equiv 11,19 \pmod{20}. \end{cases}$$

(ii) We have

$$T_p(1,-2,-1) \equiv \begin{cases} -2^{(p-1)/4} \pmod p & \text{if } p \equiv 1 \pmod 8, \\ 2^{(p-1)/4} \pmod p & \text{if } p \equiv 5 \pmod 8, \\ (-1)^{(p-3)/8} \pmod p & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(p-7)/8} \pmod p & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

An open conjecture

Recall that

$$T_p(a,b,c) := \prod_{\substack{i,j=1\\ p\nmid ai^2+bij+cj^2}}^{(p-1)/2} (ai^2+bij+cj^2).$$

Conjecture 1 (Z.-W. Sun [Int. J. Number Theory 16(2020)]). For any prime $p \equiv 1 \pmod{12}$, we have

$$T_p(1,\pm 4,1) \equiv -3^{(p-1)/4} \pmod{p}.$$

Remark. K.S. Williams and J.D. Currie [Canad. J. Math. 34(1982)] showed that for any prime $p \equiv 1 \pmod 4$ we have

$$(-3)^{(p-1)/4} \equiv \begin{cases} (-1)^{h(-3p)/4} \pmod{p} & \text{if } p \equiv 1 \pmod{12}, \\ (-1)^{(h(-3p)-2)/4}\frac{p-1}{2}! \pmod{p} & \text{if } p \equiv 5 \pmod{12}, \end{cases}$$

where $h(-d)$ denotes the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$.

Two more conjectures

Conjecture 2 (Z.-W. Sun, May 2022). For any prime $p \equiv 1 \pmod 8$, we have

$$\prod_{\substack{1\le i,j\le (p-1)/2\\ p\nmid i^2+6ij+j^2}} (i^2+6ij+j^2) \equiv -2^{(p-1)/4} \pmod p$$

and

$$\prod_{\substack{1\le i,j\le (p-1)/2\\ p\nmid i^2-6ij+j^2}} (i^2-6ij+j^2) \equiv -2^{(p-1)/4} \pmod p.$$

Conjecture 3 (Z.-W. Sun, May 2022). Let p be a prime with $p \equiv 1 \pmod 8$, and write $p = x^2 + 2y^2$ with $x, y \in \mathbb{Z}$ and $x \equiv 1 \pmod 4$. Then

$$\prod_{\substack{1\le i,j\le (p-1)/2\\ p\nmid i^2+4ij+2j^2}} (i^2+4ij+2j^2) \equiv (-1)^{(x+3)/4} 2^{(p-1)/4} \pmod p,$$

$$\prod_{\substack{1\le i,j\le (p-1)/2\\ p\nmid i^2-4ij+2j^2}} (i^2-4ij+2j^2) \equiv (-1)^{(x+3)/4} 2^{(p-1)/4} \pmod p.$$

Part B. New Results on Quadratic Residues

A mysterious discovery on Sept. 15, 2018

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

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

After I waked up in the early morning of Sept. 15, 2018, I thought that it would be very interesting if $\mathrm{sign}(\pi_p)$ obeys certain pattern. Thus, I computed and analyzed $\mathrm{sign}(\pi_p)$ 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

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

An example

For the prime $p = 11$,

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

and

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

Thus

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

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

Theorem 4 (Z.-W. Sun [Finite Fields Appl. 59(2019), 246-283]).
Let p be a prime with $p \equiv 3 \pmod 4$. Then

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

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

$$\prod_{1 \leqslant j < k \leqslant (p-1)/2} \csc \pi \frac{a(k^2-j^2)}{p} = \prod_{1 \leqslant j < k \leqslant (p-1)/2} \left(\cot \pi \frac{aj^2}{p} - \cot \pi \frac{ak^2}{p} \right)$$

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

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

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

Our proof of the theorem involves Galois theory.

The function $N_p(a, b)$

Motivated by the above work of Sun, for an odd prime p and integers a and b, Q.-H. Hou and Z.-W. Sun introduced in 2018 the notation

$$N_p(a, b) := \left| \left\{ 1 \leqslant x \leqslant \frac{p-1}{2} : \ \{x^2 + b\}_p > \{ax^2 + b\}_p \right\} \right|.$$

Example. We have $N_7(4, 0) = 2$ since

$$\{1^2\}_7 < \{4 \times 1^2\}_7, \ \{2^2\}_7 > \{4 \times 2^2\}_7 \text{ and } \{3^2\}_7 > \{4 \times 3^2\}_7.$$

Let p be a prime with $p \equiv 1 \pmod 4$. Then $q^2 \equiv -1 \pmod p$ for some integer q, hence for $a, x \in \mathbb{Z}$ we have $\{(qx)^2\}_p > \{a(qx)^2\}_p$ if and only if $\{x^2\}_p < \{ax^2\}_p$. Thus, for each $a = 2, \ldots, p-1$ there are exactly $(p-1)/4$ positive integers $x < p/2$ such that $\{x^2\}_p > \{ax^2\}_p$. Therefore $N_p(a, 0) = (p-1)/4$ for all $a = 2, \ldots, p-1$.

A joint work with Q.-H. Hou and H. Pan

The following result was originally conjectured by Q.-H. Hou and Z.-W. Sun in 2018.

Theorem 5 (Q.-H. Hou, H. Pan and Z.-W. Sun [C. R. Math. Acad. Sci. Paris, 360(2022)]) Let $p > 3$ be a prime, and let b be any integer. Set

$$S = \left\{ N_p(a, b) :\ 1 < a < p \text{ and } \left(\frac{a}{p}\right) = 1 \right\}$$

and

$$T = \left\{ N_p(a, b) :\ 1 < a < p \text{ and } \left(\frac{a}{p}\right) = -1 \right\}.$$

Then $|S| = |T| = 1$ if $p \equiv 1 \pmod 4$, and $|S| = |T| = 2$ if $p \equiv 3 \pmod 4$. Moreover, the set S does not depend on the value of b.

Examples

Let's adopt the notation in the theorem.

For $p = 5$, we have $S = \{1\}$ for any $b \in \mathbb{Z}$, and the set T depends on b as illustrated by the following table:

b	0	1	2	3	4
T	$\{1\}$	$\{0\}$	$\{1\}$	$\{2\}$	$\{1\}$

.

For $p = 7$, we have $S = \{1, 2\}$ for any $b \in \mathbb{Z}$, and the set T depends on b as illustrated by the following table:

b	0	1	2	3	4	5	6
T	$\{0,1\}$	$\{1,2\}$	$\{2,3\}$	$\{1,2\}$	$\{2,3\}$	$\{1,2\}$	$\{0,1\}$

.

Two lemmas

Lemma 1 (Dirichlet). For any prime $p \equiv 3 \pmod 4$, we have

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

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

Lemma 2. For any prime $p \equiv 3 \pmod 4$ with $p > 3$, there are $x, y, z \in \{1, \ldots, p-1\}$ such that

$$\begin{aligned} \left(\frac{x}{p}\right) &= \left(\frac{x+1}{p}\right) = 1, \\ -\left(\frac{y}{p}\right) &= \left(\frac{y+1}{p}\right) = 1, \\ \left(\frac{z}{p}\right) &= -\left(\frac{z+1}{p}\right) = 1. \end{aligned}$$

Proof of the theorem

Let $a \in \{2, \ldots, p-1\}$. For any $x \in \mathbb{Z}$, it is easy to see that

$$\left\{\frac{ax^2+b}{p}\right\} + \left\{\frac{(1-a)x^2}{p}\right\} - \left\{\frac{x^2+b}{p}\right\}$$
$$= \begin{cases} 0 & \text{if } \{x^2+b\}_p > \{ax^2+b\}_p, \\ 1 & \text{if } \{x^2+b\}_p < \{ax^2+b\}_p, \end{cases}$$

where $\{\alpha\}$ denotes the fractional part of a real number α. Thus

$$\begin{aligned} N_p(a,b) &= \sum_{x=1}^{(p-1)/2} \left(1 + \left\{\frac{x^2+b}{p}\right\} - \left\{\frac{ax^2+b}{p}\right\} - \left\{\frac{(1-a)x^2}{p}\right\}\right) \\ &= \frac{p-1}{2} + \sum_{x=1}^{\frac{p-1}{2}} \left\{\frac{x^2+b}{p}\right\} - \sum_{x=1}^{\frac{p-1}{2}} \left\{\frac{ax^2+b}{p}\right\} - \sum_{x=1}^{\frac{p-1}{2}} \left\{\frac{(1-a)x^2}{p}\right\} \\ &= \frac{p-1}{2} + \sum_{\substack{x=1 \\ (\frac{x}{p})=1}}^{p-1} \left\{\frac{x+b}{p}\right\} - \sum_{\substack{y=1 \\ (\frac{y}{p})=(\frac{a}{p})}}^{p-1} \left\{\frac{y+b}{p}\right\} - \sum_{\substack{z=1 \\ (\frac{z}{p})=(\frac{1-a}{p})}}^{p-1} \frac{z}{p}. \end{aligned}$$

Proof of the theorem (continued)

Suppose that $(\frac{a}{p}) = \varepsilon$ with $\varepsilon \in \{\pm 1\}$. Then

$$N_p(a,b) = \frac{p-1}{2} + \sum_{\substack{x=1 \\ (\frac{x}{p})=1}}^{p-1} \left\{ \frac{x+b}{p} \right\} - \sum_{\substack{y=1 \\ (\frac{y}{p})=\varepsilon}}^{p-1} \left\{ \frac{y+b}{p} \right\} - \sum_{\substack{z=1 \\ (\frac{z}{p})=\delta\varepsilon}}^{p-1} \frac{z}{p},$$

where $\delta = (\frac{a(1-a)}{p})$.

If $\varepsilon = 1$, then

$$N_p(a,b) = \frac{p-1}{2} - \frac{1}{p} \sum_{\substack{z=1 \\ (\frac{z}{p})=\delta}}^{p-1} z$$

does not depend on b.

Proof of the theorem (continued)

If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$ and hence

$$\sum_{\substack{z=1 \\ (\frac{z}{p})=1}}^{p-1} z = \sum_{\substack{z=1 \\ (\frac{p-z}{p})=1}}^{p-1} (p-z) = p\frac{p-1}{2} - \sum_{\substack{z=1 \\ (\frac{z}{p})=1}}^{p-1} z,$$

thus

$$\sum_{\substack{z=1 \\ (\frac{z}{p})=1}}^{p-1} z = p\frac{p-1}{4}$$

and

$$\sum_{\substack{z=1 \\ (\frac{z}{p})=-1}}^{p-1} z = \sum_{z=1}^{p-1} z - p\frac{p-1}{4} = p\frac{p-1}{4}.$$

So, if $p \equiv 1 \pmod 4$, then $|S| = |T| = 1$, and moreover

$$S = \left\{\frac{p-1}{2} - \frac{p-1}{4}\right\} = \left\{\frac{p-1}{4}\right\}.$$

Proof of the theorem (continued)

Now assume that $p \equiv 3 \pmod 4$. We want to show that $|S| = |T| = 2$.

By Lemma 1,

$$\sum_{z=1}^{p-1} z \left(\frac{z}{p}\right) = -ph(-p) \neq 0.$$

Thus

$$\sum_{\substack{z=1 \\ (\frac{z}{p})=1}}^{p-1} z = \sum_{z=1}^{p-1} z \frac{1+(\frac{z}{p})}{2} = p\frac{p-1}{4} - \frac{p}{2}h(-p)$$

and hence

$$\sum_{\substack{z=1 \\ (\frac{z}{p})=-1}}^{p-1} z = \sum_{z=1}^{p-1} z - \sum_{\substack{z=1 \\ (\frac{z}{p})=1}}^{p-1} z = p\frac{p-1}{4} + \frac{p}{2}h(-p).$$

Proof of the theorem (continued)

By Lemma 2, for some $a \in \{2, \ldots, p-2\}$ we have $(\frac{a-1}{p}) = (\frac{a}{p}) = 1$ and hence $(\frac{a(1-a)}{p}) = -1$. For $a' = p + 1 - a$, we have

$$\left(\frac{a'}{p}\right) = -1 \text{ and } \left(\frac{a'(1-a')}{p}\right) = \left(\frac{(1-a)a}{p}\right) = -1.$$

By Lemma 2, for some $a_*, b_* \in \{2, \ldots, p-2\}$ we have

$$-\left(\frac{a_*-1}{p}\right) = \left(\frac{a_*}{p}\right) = 1 \quad \text{and} \quad \left(\frac{b_*-1}{p}\right) = -\left(\frac{b_*}{p}\right) = 1.$$

Note that

$$\left(\frac{a_*(1-a_*)}{p}\right) = 1 = \left(\frac{b_*(1-b_*)}{p}\right).$$

Now we clearly have $|S| = |T| = 2$. Moreover,

$$S = \left\{\frac{p-1}{2} - \left(\frac{p-1}{4} \pm \frac{h(-p)}{2}\right)\right\} = \left\{\frac{p-1 \pm 2h(-p)}{4}\right\}.$$

Part C. Power Residues related to the Tangent Function

New product formulas for tangent and cotangent functions

Theorem 5. (Z.-W. Sun, arXiv:1908.02155, Publ. Math. Debrecen.) Let n be any positive odd integer. Then

$$\prod_{r=0}^{n-1}\left(1+\cot\pi\frac{x+r}{n}\right)=\left(\frac{2}{n}\right)2^{(n-1)/2}\left(1+\left(\frac{-1}{n}\right)\cot\pi x\right)$$

for all $x\in\mathbb{C}\setminus\mathbb{Z}$, and

$$\prod_{r=0}^{n-1}\left(1+\tan\pi\frac{x+r}{n}\right)=\left(\frac{2}{n}\right)2^{(n-1)/2}\left(1+\left(\frac{-1}{n}\right)\tan\pi x\right)$$

for all $x\in\mathbb{C}$ with $x-1/2\notin\mathbb{Z}$, where $(\frac{-1}{n})$ and $(\frac{2}{n})$ are Jacobi symbols.

A new class number formula

Theorem 6. (Z.-W. Sun, arXiv:1908.02155, Publ. Math. Debrecen.) Let $p>3$ be a prime and let $a\in\mathbb{Z}$ with $p\nmid a$. Then

$$\sum_{k=1}^{(p-1)/2}\frac{1}{\cot\pi\frac{ak^2}{p}-1}=\sum_{k=1}^{(p-1)/2}\frac{1}{1-\tan\pi\frac{ak^2}{p}}-\frac{p-1}{2}$$

$$=\frac{p}{4}\left(\left(\frac{-1}{p}\right)-1\right)+\left(\frac{-2a}{p}\right)\frac{\sqrt{p}}{2}\sum_{k=1}^{(p-1)/2}(-1)^k\left(\frac{k}{p}\right).$$

For any prime $p\equiv 1\pmod 4$, $\sum_{k=1}^{(p-1)/2}(\frac{k}{p})=0$ and hence

$$\sum_{k=1}^{(p-1)/2}(-1)^k\left(\frac{k}{p}\right)=\sum_{k=1}^{(p-1)/2}(1+(-1)^k)\left(\frac{k}{p}\right)=\left(\frac{2}{p}\right)h(-p)$$

since $\frac{h(-p)}{2}=\sum_{0<k<p/4}(\frac{k}{p})$, therefore we have

$$h(-p)=\frac{2}{\sqrt{p}}\sum_{k=1}^{(p-1)/2}\frac{1}{\cot\pi\frac{k^2}{p}-1}.$$

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

Theorem 7. (Z.-W. Sun, arXiv:1908.02155) Let p be an odd prime and let $a\in\mathbb{Z}$ with $p\nmid a$. Let ε_p and $h(p)$ be the fundamental unit and the class number of the field $\mathbb{Q}(\sqrt{d})$ respectively.
(i) If $p\equiv 1\pmod 8$, then

$$\prod_{k=1}^{(p-1)/2}\left(1+\tan\pi\frac{ak^2}{p}\right)=(-1)^{|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}2^{(p-1)/4},$$

$$\prod_{k=1}^{(p-1)/2}\left(1+\cot\pi\frac{ak^2}{p}\right)=(-1)^{|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}\frac{2^{(p-1)/4}}{\sqrt{p}}\varepsilon_p^{(\frac{a}{p})h(p)}.$$

If $p\equiv 5\pmod 8$, then

$$\prod_{k=1}^{(p-1)/2}\left(1+\tan\pi\frac{ak^2}{p}\right)=(-1)^{|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}2^{(p-1)/4}\left(\frac{a}{p}\right)\varepsilon_p^{-3(\frac{a}{p})h(p)},$$

$$\prod_{k=1}^{(p-1)/2}\left(1+\cot\pi\frac{ak^2}{p}\right)=(-1)^{|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}\left(\frac{a}{p}\right)\frac{2^{(p-1)/4}}{\sqrt{p}}.$$

Part (ii) of Theorem 7

(ii) Suppose that $p \equiv 3 \pmod 4$ and write $\varepsilon_p^{h(p)} = a_p + b_p\sqrt{p}$ with a_p and b_p positive integers. Set

$$s_p = \sqrt{a_p + (-1)^{(p+1)/4}} \quad \text{and} \quad t_p = \frac{b_p}{s_p}.$$

Then

$$\prod_{k=1}^{(p-1)/2}\left(1+\tan\pi\frac{ak^2}{p}\right) = (-1)^{\delta_{p,3}+\lfloor\frac{p+1}{8}\rfloor+\frac{h(-p)+1}{2}\cdot\frac{p+1}{4}}2^{\frac{p-3}{4}}\left(s_p+\left(\frac{a}{p}\right)t_p\sqrt{p}\right),$$

where the Kronecker symbol $\delta_{p,3}$ takes 1 or 0 according as $p=3$ or not. Also,

$$\prod_{k=1}^{(p-1)/2}\left(1+\cot\pi\frac{ak^2}{p}\right) = (-1)^{\lfloor\frac{p-3}{8}\rfloor+\frac{h(-p)-1}{2}\cdot\frac{p-3}{4}}2^{\frac{p-3}{4}}\left(t_p+\left(\frac{a}{p}\right)\frac{s_p}{\sqrt{p}}\right).$$

On $\prod_{k=1}^{(p-1)/2}(i - e^{2\pi i k^2/p})$

For an odd prime p, we define

$$G_p(x) := \prod_{k=1}^{(p-1)/2}(x - e^{2\pi i k^2/p}).$$

In the case $p \equiv 3 \pmod 4$, Dirichlet realized that $(i - (\frac{2}{p}))G_p(i) \in \mathbb{Z}[\sqrt{p}]$, and K. S. Williams [J. Number Theory 15 (1982)] determined the exact value of $G_p(\pm i)$. To prove Theorem 5, we also need to determine $G_p(\pm i)$ in the case $p \equiv 1 \pmod 4$.

Theorem 8 (Z.-W. Sun, arXiv:1908.02155, Publ. Math. Debrecen) Let $p \equiv 1 \pmod 4$ be a prime. If $p \equiv 1 \pmod 8$, then

$$G_p(i) = (-1)^{\frac{p-1}{8}+|\{1\le k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}.$$

If $p \equiv 5 \pmod 8$, then

$$G_p(i) = i(-1)^{\frac{p-5}{8}+|\{1\le k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}\varepsilon_p^{-h(p)}.$$

On $G_p(\pm\omega)$ with $p \equiv 1 \pmod 4$

Let $\omega := e^{2\pi i/3} = (-1+\sqrt{-3})/2$.

Theorem 9 (Z.-W. Sun, arXiv:1908.02155, Publ. Math. Debrecen) Let $p \equiv 1 \pmod 4$ be a prime. Then

$$(-1)^{|\{1\leqslant k\leqslant\lfloor\frac{p+1}{3}\rfloor:\ (\frac{k}{p})=-1\}|}G_p(\omega) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{12}, \\ \omega\varepsilon_p^{h(p)} & \text{if } p \equiv 5 \pmod{12}; \end{cases}$$

$$G_p(-\omega) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{12}, \\ -\omega\varepsilon_p^{-2h(p)} & \text{if } p \equiv 5 \pmod{24}, \\ \omega & \text{if } p \equiv 17 \pmod{24}. \end{cases}$$

A Key Lemma. Let $p \equiv 1 \pmod 4$ be a prime. Then

$$(-1)^{|\{1\leqslant k<\frac{p}{3}:\ (\frac{k}{p})=-1\}|}(-3)^{(p-1)/4} \equiv \begin{cases} 1 \pmod p & \text{if } 12 \mid p-1, \\ \frac{p-1}{2}! \pmod p & \text{if } 12 \mid p-5, \end{cases}$$

where $h(-3p)$ is the class number of the field $\mathbb{Q}(\sqrt{-3p})$.

On $G_p(\omega)$ with $p \equiv 3 \pmod 4$

Conjecture 4 (Z.-W. Sun, arXiv:1908.02155, Publ. Math. Debrecen). Let $p > 3$ be a prime with $p \equiv 3 \pmod 4$. Then

$$G_p(\omega^{\pm 1}) = (-1)^{(h(-p)+1)/2}\left(\frac{p}{3}\right)\frac{x_p\sqrt{3} \mp y_p\sqrt{p}}{2} \times \begin{cases} i^{\pm 1} & \text{if } p \equiv 7 \pmod{12}, \\ (-1)^{|\{1 \le k < \frac{p}{3}:\ (\frac{k}{p})=1\}|}(i\omega)^{\pm 1} & \text{if } p \equiv 11 \pmod{12}, \end{cases}$$

where (x_p, y_p) is the least positive integer solution to the diophantine equation $3x^2 + 4(\frac{p}{3}) = py^2$.

Example. For the primes $p = 79,\ 227$, Conjecture 4 predicts that

$$G_{79}(\omega) = i\frac{\sqrt{79} - 5\sqrt{3}}{2} \text{ and } G_{227}(\omega) = i\omega(1338106\sqrt{3} - 153829\sqrt{227}).$$

On $G_p(\zeta)$ with $\zeta^{10} = 1$

Conjecture 5 (Z.-W. Sun, arXiv:1908.02155, Publ. Math. Debrecen). Let ζ be any primitive tenth root of unity. Then

$$\prod_{k=1}^{(p-1)/2} (\zeta - e^{2\pi i k^2/p}) = (-1)^{|\{1\le k\le \frac{p+9}{10}:\ (\frac{k}{p})=-1\}|}$$

for each prime $p \equiv 21 \pmod{40}$, and

$$\prod_{k=1}^{(p-1)/2} (\zeta - e^{2\pi i k^2/p}) = (-1)^{|\{1\le k\le \frac{p+1}{10}:\ (\frac{k}{p})=-1\}|}\zeta^2$$

for any prime $p \equiv 29 \pmod{40}$.

mth power residues modulo primes

Let $m \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, and let p be a prime with $p \equiv 1 \pmod{m}$. If $a \in \mathbb{Z}$ is not divisible by p, and $x^m \equiv a \pmod{p}$ for some integer x, then a is called an mth power residue modulo p. The set

$$R_m(p) = \{k \in \{1, \ldots, p-1\} :\ k \text{ is an } m\text{th power residue modulo } p\}$$

has cardinality $(p-1)/m$.

For an integer $a \not\equiv 0 \pmod{p}$, the mth power residue symbol $(\frac{a}{p})_m$ is a unique mth root ζ of unity such that

$$a^{(p-1)/m} \equiv \zeta \pmod{p}$$

in the ring of all algebraic integers. (Note that a primitive root g modulo p has order $p-1$ which is a multiple of m.) In particular,

$$\left(\frac{-1}{p}\right)_m = (-1)^{(p-1)/m}.$$

Our main result

Theorem 10 (Z.-W. Sun, arXiv:2208.05928, Czechslovak Math. J.) Let $m \in \mathbb{Z}^+$, and let p be a prime with $p \equiv 1 \pmod{2m}$. Suppose that 2 is an mth power residue modulo p. For any integer a not divisible by p, we have

$$\prod_{k \in R_m(p)} \left(1 + \tan \pi \frac{ak}{p}\right) = \left(\frac{-2}{p}\right)_{2m} (-2)^{(p-1)/(2m)} = \left(\frac{2}{p}\right)_{2m} 2^{(p-1)/(2m)}.$$

Corollary 2. Let $p = x^2 + 27y^2$ be a prime with $x, y \in \mathbb{Z}^+$. For any integer $a \not\equiv 0 \pmod{p}$, we have

$$\prod_{k \in R_3(p)} \left(1 + \tan \pi \frac{ak}{p}\right) = (-1)^{xy/2}(-2)^{(p-1)/6}.$$

Corollary 3. Let $p = x^2 + 64y^2$ be a prime with $x, y \in \mathbb{Z}^+$. For any integer $a \not\equiv 0 \pmod{p}$, we have

$$\prod_{k \in R_4(p)} \left(1 + \tan \pi \frac{ak}{p}\right) = (-1)^{y}(-2)^{(p-1)/8}.$$

An auxiliary theorem

Theorem 11 (Z.-W. Sun, arXiv:2208.05928, Czechslovak Math. J.). Let m be a positive integer, and let p be a prime with $p \equiv 1 \pmod{2m}$. Suppose that 2 is an mth power residue modulo p. For any integer $a \not\equiv 0 \pmod{p}$, we have

$$\prod_{k \in R_m(p)} (i - e^{2\pi iak/p}) = \left(\frac{-2}{p}\right)_{2m} i^{(p-1)/(2m)}$$

and

$$\prod_{k \in R_m(p)} (i + e^{2\pi iak/p}) = \left(\frac{2}{p}\right)_{2m} i^{(p-1)/(2m)}.$$

Remark. The two identities in the theorem are equivalent.

Lemma. Let m be a positive integer, and let p be a prime with $p \equiv 1 \pmod{2m}$. Then we have

$$\sum_{k \in R_m(p)} k = \frac{p(p-1)}{2m}.$$

Proof of the first identity Theorem 11

Let $c := \prod_{k \in R_m(p)} \left(i - e^{2\pi iak/p}\right)$. As $k \in \mathbb{Z}$ is an mth power residue modulo p if and only if $-k$ is an mth power residue modulo p, we also have $c = \prod_{k \in R_m(p)} \left(i - e^{2\pi ia(-k)/p}\right)$. Thus

$$\begin{aligned}
c^2 &= \prod_{k \in R_m(p)} \left(i - e^{2\pi iak/p}\right)\left(i - e^{-2\pi iak/p}\right) \\
&= \prod_{k \in R_m(p)} \left(i^2 + 1 - i\left(e^{2\pi iak/p} + e^{-2\pi iak/p}\right)\right) \\
&= (-i)^{|R_m(p)|} \prod_{k \in R_m(p)} \left(e^{2\pi iak/p} + e^{-2\pi iak/p}\right) \\
&= (-i)^{(p-1)/m} \prod_{k \in R_m(p)} e^{-2\pi iak/p}\left(1 + e^{4\pi iak/p}\right) \\
&= (-1)^{(p-1)/(2m)} e^{-2\pi i \sum_{k \in R_m(p)} ak/p} \prod_{k \in R_m(p)} \frac{1 - e^{2\pi ia(4k)/p}}{1 - e^{2\pi ia(2k)/p}}.
\end{aligned}$$

Proof of the first identity in Theorem 11

Note that

$$e^{-2\pi i \sum_{k \in R_m(p)} ak/p} = e^{-2\pi i a(p-1)/(2m)} = 1$$

by the lemma. As 2 is an mth power residue modulo p, we also have

$$\begin{aligned}\prod_{k \in R_m(p)} \left(1 - e^{2\pi i ak/p}\right) &= \prod_{k \in R_m(p)} \left(1 - e^{2\pi i a(2k)/p}\right) \\ &= \prod_{k \in R_m(p)} \left(1 - e^{2\pi i a(4k)/p}\right).\end{aligned}$$

Combining the above, we see that

$$c^2 = (-1)^{(p-1)/(2m)} \times 1 \times 1 = (-1)^{(p-1)/(2m)}.$$

Proof of the first identity in Theorem 11

Write $c = \delta i^{(p-1)/(2m)}$ with $\delta \in \{\pm 1\}$. In the ring of all algebraic integers, we have

$$\begin{aligned} c^p &= \prod_{k \in R_m(p)} (i - e^{2\pi i a k/p})^p \\ &\equiv \prod_{k \in R_m(p)} (i^p - 1) = (i^p - 1)^{(p-1)/m} \\ &= ((i^p - 1)^2)^{(p-1)/(2m)} = (-2i^p)^{(p-1)/(2m)} \pmod{p}. \end{aligned}$$

Thus

$$\delta i^{p(p-1)/(2m)} = c^p \equiv (-2)^{(p-1)/(2m)} i^{p(p-1)/(2m)} \pmod{p}$$

and hence

$$\delta \equiv (-2)^{(p-1)/(2m)} \equiv \left(\frac{-2}{p}\right)_{2m} \pmod{p}.$$

Therefore $\delta = (\frac{-2}{p})_{2m}$ and hence $c = (\frac{-2}{p})_{2m} i^{(p-1)/(2m)}$ as desired.

Main references:

1. Q.-H. Hou, H. Pan and Z.-W. Sun, *A new theorem on quadratic residues modulo primes*, C. R. Math. Acad. Sci. Paris **360** (2022), 1065–1069.

2. Z.-W. Sun, *Quadratic residues and related permutations and identities*, Finite Fields Appl. **59** (2019), 246-283.

3. Z.-W. Sun, *Trigonometric identities and quadratic residues*, accepted by Publ. Math. Debrecen. See also arXiv:1908.02155.

4. Z.-W. Sun, *The tangent function and power residues modulo primes*, accepted by Czechslovak Math. J. (arXiv:2208.05928)

Thank you!