An on-line talk (August 25-26, 2020)

On two products modulo primes

Zhi-Wei Sun

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

August 26, 2020

Abstract

Let p be an odd prime, and let $a, b, c \in \mathbb{Z}$. Define

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

and

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

In this talk we introduce the speaker's work on $S_p(a,b,c)$ and $T_p(a,b,c)$ modulo p. We determine $S_p(a,b,c)$ mod p completely, and determine $T_p(a,b,c)$ mod p in some special cases (such as $a=-c$). For example, we show that if $p\nmid ac(a+b+c)$ then

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

where $\Delta = b^2-4ac$. Our tools include the theory of quadratic residues and quartic residues modulo primes.

Part I. On the product $S_p(a, b, c)$

Wilson's Theorem

Wilson's Theorem. An integer $p > 1$ is a prime if and only if

$$(p-1)! = \prod_{k=1}^{p-1} k \equiv -1 \pmod{p}.$$

This was found by J. Wilson in 1770 and proved by J.L. Lagrange in 1771.

Corollary. For any odd prime p, we have

$$\left(\frac{p-1}{2}!\right)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

This is because

$$(p-1)! = \prod_{k=1}^{(p-1)/2} k(p-k) \equiv (-1)^{(p-1)/2} \prod_{k=1}^{(p-1)/2} k^2 \pmod{p}.$$

Mordell's result

By Wilson's theorem, for any prime $p \equiv 1 \pmod 4$ we have

$$\left(\frac{p-1}{2}!\right)^2 \equiv -1 \pmod p,$$

and for any prime $p \equiv 3 \pmod 4$ we have

$$\left(\frac{p-1}{2}!\right)^2 \equiv 1 \pmod p.$$

Theorem (L.J. Mordell [Amer. Math. Monthly 68(1961)]). For any prime $p > 3$ with $p \equiv 3 \pmod 4$, we have

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

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

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

In 2013 I encountered the product $\prod_{1\leqslant i<j\leqslant (p-1)/2}(j^2-i^2)^2$ modulo an odd prime p during my proof of the congruence

$$\left|\frac{1}{i^2+j^2}\right|_{1\leqslant i,j\leqslant (p-1)/2} \equiv \left(\frac{2}{p}\right) \pmod{p}$$

for any prime $p\equiv 3 \pmod 4$.

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

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

Sketch of My Proof. This is because

$$\prod_{1\leqslant i<j\leqslant n}(j-i) \times \prod_{1\leqslant i<j\leqslant n}(j+i)$$

$$=\prod_{k=1}^{n} k^{n-k} \times \prod_{k=1}^{n} k^{\lfloor (k-1)/2\rfloor}(p-k)^{\lfloor k/2\rfloor}$$

$$\equiv (-1)^{\sum_{k=0}^{n}\lfloor k/2\rfloor}(n!)^{n-1} \pmod p$$

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

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

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

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 [Finite Fields Appl. 59(2019)]). For any prime $p\equiv 1 \pmod 4$, we have the new congruence

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

The product $S_p(a, b, c)$

Let p be an odd prime, and let $a, b, c \in \mathbb{Z}$. Define

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

How to determine $S_p(a, b, c)$ modulo an odd prime p?

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

The case $p \nmid ac(a+b+c)$

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

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

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

Remark. I first found this result via a computer.

Lemma 1

We need a well known lemma.

Lemma 1. Let p be an odd prime, and let $a, b, c \in \mathbb{Z}$ with a or b not divisible by p. Then

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

Lemma 2

Lemma 2. Let p be an odd prime and let $a, b, c \in \mathbb{Z}$ with $ac(a+b+c) \not\equiv 0 \pmod{p}$. Write $\Delta = b^2 - 4ac$. Then

$$\begin{aligned}&|\{(j,k) : 1 \leqslant j < k \leqslant p-1 \text{ and } aj^2 + bjk + ck^2 \equiv 0 \pmod{p}\}| \\ =&\frac{p-1}{2}\left(1 + \left(\frac{\Delta}{p}\right)\right).\end{aligned}$$

For $n = 1 \ldots, p-1$, we have

$$\begin{aligned}&|\{(j,k) : 1 \leqslant j < k \leqslant p-1 \text{ and } aj^2 + bjk + ck^2 \equiv n \pmod{p}\}| \\ =&\frac{1}{2}\left(p - 3 - \left(\frac{\Delta}{p}\right)\right) \\ &- \frac{1}{2}\left(\frac{n}{p}\right)\left(\left(1 - p + p\left(\frac{\Delta}{p}\right)^2\right)\left(\frac{a}{p}\right) + \left(\frac{c}{p}\right) + \left(\frac{a+b+c}{p}\right)\right).\end{aligned}$$

Let

$$L = |\{(j,k) :\ 1 \leqslant j < k \leqslant p-1 \text{ and } aj^2+bjk+ck^2 \equiv n \pmod{p}\}|.$$

Then

$$\begin{aligned} L = &\left|\left\{(j,k) :\ 1 \leqslant j < k \leqslant \frac{p-1}{2} \text{ and } aj^2+bjk+ck^2 \equiv n \pmod{p}\right\}\right| \\ &+ \left|\left\{(p-j,p-k) :\ 1 \leqslant k \leqslant \frac{p-1}{2},\ k < j \leqslant p-1,\right.\right. \\ &\qquad \left.\left. \text{and } a(p-j)^2+b(p-j)(p-k)+c(p-k)^2 \equiv n \pmod{p}\right\}\right| \\ = &\left|\left\{(j,k) :\ 1 \leqslant k \leqslant \frac{p-1}{2},\ 0 \leqslant j \leqslant p-1,\ j \neq 0, k,\right.\right. \\ &\qquad \left.\left. \text{and } (2aj+bk)^2 - \Delta k^2 \equiv 4an \pmod{p}\right\}\right|. \end{aligned}$$

Hence

$$L = \sum_{k=1}^{(p-1)/2} \left(1 + \left(\frac{4an + \Delta k^2}{p}\right)\right)$$
$$- \left|\left\{1 \leqslant k \leqslant \frac{p-1}{2} : \ (bk)^2 - \Delta k^2 \equiv 4an \pmod{p}\right\}\right|$$
$$- \left|\left\{1 \leqslant k \leqslant \frac{p-1}{2} : \ ((2a+b)k)^2 - \Delta k^2 \equiv 4an \pmod{p}\right\}\right|.$$

In the case $n = 0$, this yields

$$L = \frac{p-1}{2}\left(1 + \left(\frac{\Delta}{p}\right)\right).$$

When $1 \leqslant n \leqslant p-1$, by the above we have

$$
\begin{aligned}
L =& \sum_{x=1}^{p-1} \frac{1+\left(\frac{x}{p}\right)}{2}\left(1+\left(\frac{\Delta x+4an}{p}\right)\right)-\frac{1+\left(\frac{cn}{p}\right)}{2}-\frac{1+\left(\frac{(a+b+c)n}{p}\right)}{2} \\
=& \frac{p-1}{2}+\frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)+\frac{1}{2}\left(\sum_{x=0}^{p-1}\left(\frac{\Delta x+4an}{p}\right)-\left(\frac{4an}{p}\right)\right) \\
&+\frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{\Delta x^2+4anx}{p}\right)-1-\frac{1}{2}\left(\frac{n}{p}\right)\left(\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)\right) \\
=& \frac{p-3}{2}-\frac{1}{2}\left(\frac{\Delta}{p}\right)-\frac{1}{2}\left(\frac{n}{p}\right)\left(1-p\delta_{\left(\frac{\Delta}{p}\right),0}\right)\left(\frac{a}{p}\right) \\
&-\frac{1}{2}\left(\frac{n}{p}\right)\left(\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)\right).
\end{aligned}
$$

Proof of Theorem 1 in the case $p \mid \Delta$

If $p \mid \Delta$, then by Lemma 2 we have

$$\prod_{\substack{1 \leqslant i < j \leqslant p-1 \\ p \nmid ai^2+bij+cj^2}} (ai^2 + bij + cj^2)$$

$$\equiv \prod_{n=1}^{p-1} n^{\frac{p-3}{2}+\frac{1-p}{2}\left(\frac{a}{p}\right)+\frac{1}{2}\left(\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)\right)-\frac{1}{2}\left(1+\left(\frac{n}{p}\right)\right)\left((1-p)\left(\frac{a}{p}\right)+\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)\right)}$$

$$\equiv (-1)^{\frac{p-3}{2}+\frac{1-p}{2}\left(\frac{a}{p}\right)+\frac{1}{2}\left(\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)\right)} \prod_{k=1}^{(p-1)/2} (k^2)^{-\left((1-p)\left(\frac{a}{p}\right)+\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)\right)}$$

$$\equiv (-1)^{\frac{1}{2}\left(\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)\right)-1} \left((-1)^{(p+1)/2}\right)^{(1-p)\left(\frac{a}{p}\right)+\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)}$$

$$= (-1)^{\frac{1}{2}\left(\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)\right)-1} = \left(\frac{c(a+b+c)}{p}\right) = \left(\frac{a(a+b+c)}{p}\right) \pmod{p}$$

since $4ac \equiv b^2 \pmod{p}$.

Proof of Theorem 1 in the case $p \nmid \Delta$

Similarly, when $p \nmid \Delta$, by Lemma 2 we have

$$\prod_{\substack{1\leqslant i<j\leqslant (p-1)/2\\ p\nmid ai^2+bij+cj^2}} (ai^2+bij+cj^2)$$

$$\equiv \prod_{n=1}^{p-1} n^{\frac{p-3}{2}+\frac{1}{2}((\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p})-(\frac{\Delta}{p}))-\frac{1}{2}(1+(\frac{n}{p}))((\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))}$$

$$\equiv (-1)^{\frac{p-3}{2}+\frac{1}{2}((\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p})-(\frac{\Delta}{p}))} \prod_{k=1}^{(p-1)/2} (k^2)^{-((\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))}$$

$$\equiv (-1)^{\frac{p-3}{2}+\frac{1}{2}((\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p})-(\frac{\Delta}{p}))} \left((-1)^{(p+1)/2}\right)^{(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p})} \pmod p$$

and hence

$$\prod_{\substack{1\leqslant i<j\leqslant (p-1)\\ p\nmid ai^2+bij+cj^2}} (ai^2+bij+cj^2) \equiv (-1)^{\frac{1}{2}((\frac{a}{p})+(\frac{c}{p}))}(-1)^{\frac{1}{2}((\frac{a+b+c}{p})-(\frac{\Delta}{p}))}$$

$$= -\left(\frac{ac}{p}\right)\left(\frac{(a+b+c)\Delta}{p}\right) \pmod p.$$

Lemma 3

Lemma 3. For any odd prime p, we have

$$\prod_{1\leqslant i<j\leqslant p-1}(j-i)\equiv-\left(\frac{2}{p}\right)\frac{p-1}{2}!\pmod{p}.$$

Proof. Clearly $\binom{p-1}{k}\equiv(-1)^k \pmod{p}$ for all $k=0,\ldots,p-1$. Also, $(p-1)!\equiv-1 \pmod{p}$ by Wilson's theorem. Thus

$$\begin{aligned}\prod_{1\leqslant i<j\leqslant p-1}(j-i)&=\prod_{j=2}^{p-1}(j-1)!=\prod_{k=1}^{p-2}k!\\&=\frac{p-1}{2}!\prod_{0<k<(p-1)/2}\frac{(p-1)!}{\binom{p-1}{k}}\\&\equiv\frac{p-1}{2}!\prod_{0<k<(p-1)/2}(-1)^{k-1}\\&\equiv\frac{p-1}{2}!(-1)^{(p-3)(p-5)/8}=-\left(\frac{2}{p}\right)\frac{p-1}{2}!\pmod{p}.\end{aligned}$$

Lemma 4

For a positive integer n and a rational number x with denominator relatively prime to n, we let $\{x\}_n$ denote the unique integer $r \in \{0, \ldots, n-1\}$ with $x \equiv r \pmod{n}$.

Lemma 4. Let p be an odd prime, and let $a, b \in \mathbb{Z}$ with $a \not\equiv 0, 1 \pmod{p}$. Then

$$|\{x \in \{0, 1 \ldots, p-1\} : \ \{ax+b\}_p > x\}| = \frac{p-1}{2}.$$

Proof. For $x \in \{0, \ldots, p-1\}$, obviously

$$\{ax+b+1\}_p > x \iff p-1 > \{ax+b\}_p \geqslant x.$$

As $a \not\equiv 0, 1 \pmod{p}$, we have

$$|\{x \in [0,p) : \ \{ax+b\}_p = x\}| = 1 = |\{x \in [0,p) : \ \{ax+b\}_p = p-1\}|.$$

Thus

$$|\{x \in [0,p-1] : \ \{ax+b+1\}_p > x\}| = |\{x \in [0,p-1] : \ \{ax+b\}_p > x\}|.$$

Continue the proof

In view of the above, it suffices to prove the desired result for $b = 0$. For $x = 1, \ldots, p-1$, clearly $\{ax\}_p \neq x$ (since $a \not\equiv 1 \pmod{p}$), and also

$$\begin{aligned} \{ax\}_p > x &\iff p - \{ax\}_p < p - x \\ &\iff \{a(p-x)\}_p < p - x. \end{aligned}$$

So

$$|\{x \in \{0, 1 \ldots, p-1\} : \ \{ax\}_p > x\}| = \frac{p-1}{2}.$$

The case $p \nmid ac$ and $p \mid a+b+c$

Theorem 2 (Z.-W. Sun [Finite Fields Appl. 59(2019)]). Let $a, b, c \in \mathbb{Z}$ with $p \nmid ac$ and $p \mid a+b+c$. Then

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

$$\equiv \begin{cases} (-1)^{N_p(a/c)}\left(\frac{2c(a-c)}{p}\right) \pmod p & \text{if } p\nmid a-c,\\ (-1)^{(p+1)/2}\left(\frac{a}{p}\right) \pmod p & \text{if } p\mid a-c,\end{cases}$$

where

$$N_p(x) := |\{1\leqslant k\leqslant (p-1)/2 :\ \{kx\}_p > k\}|$$

for any p-adic integer x.

Proof of Theorem 2 in the case $p \mid a - c$

If $a \equiv c \pmod{p}$, then $b \equiv -a - c \equiv -2a \pmod{p}$ and hence

$$\begin{aligned}
&\prod_{\substack{1 \leqslant i < j \leqslant p-1 \\ p \nmid ai^2 + bij + cj^2}} (ai^2 + bij + cj^2) \\
&\equiv \prod_{1 \leqslant i < j \leqslant p-1} a(j-i)^2 = a^{\frac{p-1}{2}(p-2)} \prod_{1 \leqslant i < j \leqslant p-1} (j-i)^2 \\
&\equiv \left(\frac{a}{p}\right) \left(\frac{p-1}{2}!\right)^2 \equiv (-1)^{(p+1)/2} \left(\frac{a}{p}\right) \pmod{p}
\end{aligned}$$

with the help of Lemma 3.

Proof of Theorem 2 in the case $p \nmid a - c$

Now assume that $a \not\equiv c \pmod{p}$. For $1 \leqslant i < j \leqslant p-1$, clearly

$$ai^2 + bij + cj^2 \equiv (i-j)(ai-cj) \equiv c(j-i)\left(j - \frac{a}{c}i\right) \pmod{p}.$$

Note that

$$\prod_{\substack{1 \leqslant i < j \leqslant p-1 \\ p \nmid ai - cj}} \left(j - \frac{a}{c}i\right) \equiv \prod_{r=1}^{p-1} r^{|\{(i,j):\ 1 \leqslant i < j \leqslant p-1 \ \&\ j - \frac{a}{c}i \equiv r \pmod{p}\}|}$$

$$\equiv \prod_{r=1}^{p-1} r^{|\{1 \leqslant i \leqslant p-1:\ \{r + \frac{a}{c}i\}_p > i\}|}$$

$$\equiv (p-1)!^{(p-1)/2-1} \equiv (-1)^{(p+1)/2} \pmod{p}.$$

with the help of Lemma 4 and Wilson's theorem.

Proof of Theorem 2 in the case $p \nmid a - c$

Also,

$$\prod_{\substack{1 \leqslant i < j \leqslant p-1 \\ p \mid ai - cj}} c(j-i) \equiv \prod_{\substack{i=1 \\ \{\frac{a}{c} i\}_p > i}}^{p-1} c\left(\frac{a}{c} i - i\right)$$

$$\equiv \prod_{\substack{i=1 \\ \{\frac{a}{c} i\}_p > i}}^{(p-1)/2} (a-c)i \times \prod_{\substack{i=1 \\ \{\frac{a}{c}(p-i)\}_p > p-i}}^{(p-1)/2} (a-c)(p-i)$$

$$\equiv \prod_{i=1}^{(p-1)/2} (a-c)i \times (-1)^{|\{1 \leqslant i \leqslant \frac{p-1}{2} :\ \{\frac{a}{c} i\}_p < i\}|}$$

$$\equiv \left(\frac{a-c}{p}\right) \frac{p-1}{2}! (-1)^{(p-1)/2 - N_p(a/c)} \pmod{p}.$$

Continue the proof

Hence

$$\prod_{\substack{1\leqslant i<j\leqslant p-1\\ p\nmid ai-cj}} c(j-i) \equiv \frac{\prod_{1\leqslant i<j\leqslant p-1} c(j-i)}{\left(\frac{a-c}{p}\right)^{\frac{p-1}{2}}!(-1)^{(p-1)/2-N_p(a/c)}}$$

$$\equiv \frac{-c^{(p-1)(p-2)/2}\left(\frac{2}{p}\right)^{\frac{p-1}{2}}!}{\left(\frac{a-c}{p}\right)^{\frac{p-1}{2}}!(-1)^{(p-1)/2-N_p(a/c)}}$$

$$\equiv \left(\frac{2c(a-c)}{p}\right)(-1)^{(p+1)/2+N_p(a/c)} \pmod{p}.$$

Therefore

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

$$\equiv \prod_{\substack{1\leqslant i<j\leqslant p-1\\ p\nmid ai-cj}} c(j-i) \times \prod_{\substack{1\leqslant i<j\leqslant p-1\\ p\nmid ai-cj}} \left(j-\frac{a}{c}i\right)$$

$$\equiv \left(\frac{2c(a-c)}{p}\right)(-1)^{N_p(a/c)} \pmod{p}.$$

Theorem 3

Theorem 3 (Z.-W. Sun [Finite Fields Appl. 59(2019)]). Let $a, b, c \in \mathbb{Z}$ with $p \mid ac$. Then

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

$$\equiv \begin{cases} -\left(\frac{b}{p}\right) \pmod p & \text{if } p\mid a,\ p\nmid b \text{ and } p\mid c,\\ -\left(\frac{c}{p}\right) \pmod p & \text{if } p\mid a,\ p\nmid bc \text{ and } p\mid b+c,\\ (-1)^{N_p(-c/b)}\left(\frac{2}{p}\right) \pmod p & \text{if } p\mid a \text{ and } p\nmid bc(b+c),\\ (-1)^{(p+1)/2}\left(\frac{c}{p}\right) \pmod p & \text{if } p\mid a,\ p\mid b \text{ and } p\nmid c,\\ (-1)^{(p+1)/2}\left(\frac{a}{p}\right) \pmod p & \text{if } p\nmid a,\ p\mid b \text{ and } p\mid c,\\ (-1)^{(p+1)/2}\left(\frac{b}{p}\right) \pmod p & \text{if } p\nmid ab,\ p\mid a+b \text{ and } p\mid c,\\ (-1)^{N_p(-a/b)}\left(\frac{2}{p}\right) \pmod p & \text{if } p\nmid ab(a+b) \text{ and } p\mid c, \end{cases}$$

where $N_p(x) := |\{1 \leqslant k \leqslant (p-1)/2 :\ \{kx\}_p > k\}|$ for any p-adic integer x.

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

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

A new theorem

Recall that $N_p(x) := |\{1 \leqslant k \leqslant (p-1)/2 : \ \{kx\}_p > k\}|$ for any p-adic integer x.

Theorem 4 (Z.-W. Sun, Int. J. Number Theory, in press). 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

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

Proof of the first equality in Theorem 4

For each $k = 1, \ldots, (n-1)/2$, we have

$$\left\lfloor \frac{kx}{n} \right\rfloor - \left\lfloor \frac{k(x-1)}{n} \right\rfloor = \begin{cases} 0 & \text{if } \{kx\}_n > k, \\ 1 & \text{if } \{kx\}_n < k. \end{cases}$$

Thus

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

and hence

$$\begin{aligned} & (-1)^{|\{1 \leqslant k < n/2 : \ \{kx\}_n > k\}|} \left(\frac{-1}{n} \right) \\ =& (-1)^{\sum_{k=1}^{(n-1)/2} \lfloor kx/n \rfloor + \sum_{k=1}^{(n-1)/2} \lfloor k(x-1)/n \rfloor} \\ =& (-1)^{(\sum_{k=1}^{(n-1)/2} (2x-1)k - \sum_{k=1}^{(n-1)/2} \{kx\}_n - \sum_{k=1}^{(n-1)/2} \{k(x-1)\}_n)/n} \\ =& (-1)^{(n^2-1)/8} (-1)^{\sum_{k=1}^{(n-1)/2} \{kx\}_n + \sum_{k=1}^{(n-1)/2} \{k(x-1)\}_n}. \end{aligned}$$

Continue the proof

As $\{kx\}_n \equiv 1 + n - \{kx\}_n \pmod 2$ for all $k = 1, \ldots, (n-1)/2$, we have

$$\begin{aligned}\sum_{k=1}^{(n-1)/2} \{kx\}_n &\equiv \sum_{\substack{k=1 \\ \{kx\}_n < n/2}}^{(n-1)/2} \{kx\}_n + \sum_{\substack{k=1 \\ \{kx\}_n > n/2}}^{(n-1)/2} (1 + (n - \{kx\}_n)) \\ &= \sum_{\substack{k=1 \\ \{kx\}_n > n/2}}^{(n-1)/2} 1 + \sum_{r=1}^{(n-1)/2} r \\ &= \left|\left\{1 \leqslant k < \frac{n}{2} : \ \{kx\}_n > \frac{n}{2}\right\}\right| + \frac{n^2-1}{8} \pmod 2.\end{aligned}$$

and hence

$$(-1)^{\sum_{k=1}^{(n-1)/2} \{kx\}_n} = \left(\frac{x}{n}\right)\left(\frac{2}{n}\right) = \left(\frac{2x}{n}\right).$$

Similarly,

$$(-1)^{\sum_{k=1}^{(n-1)/2} \{k(x-1)\}_n} = \left(\frac{x}{n}\right)\left(\frac{2}{n}\right) = \left(\frac{2(x-1)}{n}\right).$$

Continue the proof

In view of the above, we obtain

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

as desired.

Combining Theorems 1-4, we have completely determine $S_p(a,b,c)$ modulo p in all cases.

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

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

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

Part II. On the product $T_p(a, b, c)$

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 $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$, 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. For $a,b,c \in \mathbb{Z}$ we introduce the product

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

We are able to determine $T_p(a,b,c)$ mod p in the case $a+c=0$.

On $T_p(1,-A,-1)$ mod p

Theorem (Z.-W. Sun, Int. J. Number Theory, in press). 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

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

Some Lemmas

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

$$\left| \left\{ 1 \leqslant k \leqslant \frac{p-1}{2} : \left\{ k \times \frac{p-1}{2}! \right\}_p > \frac{p}{2} \right\} \right| = \frac{p-1}{4}.$$

For any odd prime p and integer A with $\Delta = A^2 + 4 \not\equiv 0 \pmod p$, it is known that

$$u_{(p-(\frac{\Delta}{p})/2}(A) v_{(p-(\frac{\Delta}{p}))/2}(A) = u_{p-(\frac{\Delta}{p})}(A) \equiv 0 \pmod p.$$

Lemma. Let $A \in \mathbb{Z}$ and let p be an odd prime not dividing $\Delta = A^2 + 4$. Then

$$p \mid v_{(p-(\frac{\Delta}{p}))/2}(A) \iff \left(\frac{-1}{p} \right) = -1.$$

This is a known result, see, e.g., Ribenboim's book *The Book of Prime Number Records* (Springer, 1980).

A corollary

Corollary. 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

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

On $T_p(2, \pm 5, 2) \bmod p$

Theorem (Z.-W. Sun, Int. J. Number Theory, in press). Let $p > 3$ be a prime and let $\delta \in \{\pm 1\}$. If $p \equiv 1 \pmod 4$, then

$$T_p(2, 5\delta, 2) \equiv (-1)^{\lfloor (p+11)/12 \rfloor} \pmod p.$$

When $p \equiv 3 \pmod 4$, we have

$$T_p(2, 5\delta, 2) \equiv \left(\frac{6}{p}\right) \frac{\delta 2^\delta}{3^\delta} \binom{(p-3)/2}{(p-3)/4}^{-2\delta} \pmod p.$$

Lemma. Let $p > 3$ be a prime. Then

$$\frac{p-1}{2}!! \prod_{\substack{i,j=1 \\ p \nmid 2i+j}}^{(p-1)/2} (2i+j) \equiv \left(\frac{-2}{p}\right) \frac{p-3}{2}!! \prod_{\substack{i,j=1 \\ p \nmid 2i-j}}^{(p-1)/2} (2i-j) \equiv \pm 1 \pmod p.$$

Remark. The speaker conjectured that the sign is $(-1)^{(p-1)/4}$ if $p \equiv 1 \pmod 4$, and $(-1)^{(h(-p)+1)/2}$ if $p \equiv 3 \pmod 4$. This was confirmed by F. Petrov on MathOverflow.

On products of Legendre symbols

Theorem (Z.-W. Sun, Int. J. Number Theory, in press). Let $p > 3$ be a prime and let $\delta \in \{\pm 1\}$. Then

$$\prod_{1\leqslant i<j\leqslant (p-1)/2}\left(\frac{j+\delta i}{p}\right)=\begin{cases}(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=\delta\}|} & \text{if } 4\mid p-1,\\ (-1)^{(p-3)/8} & \text{if } 8\mid p-3,\\ (-1)^{(p+1)/8+(h(-p)+1)/2} & \text{if } 8\mid p-7,\end{cases}$$

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

A conjecture

Conjecture (Z.-W. Sun, Int. J. Number Theory, in press). For any prime $p>3$, we have

$$\prod_{\substack{i,j=1\\ p\nmid 6i+j}}^{(p-1)/2}\left(\frac{6i+j}{p}\right)$$

$$=\begin{cases}(-1)^{|\{1\leqslant k<p/12:\ (\frac{k}{p})=-1\}|} & \text{if } p\equiv 1 \pmod{24},\\ (-1)^{|\{\frac{p+3}{4}\leqslant k\leqslant \lfloor\frac{p+1}{3}\rfloor:\ (\frac{k}{p})=-1\}|} & \text{if } p\equiv 5,-7,-11 \pmod{24},\\ (-1)^{(h(-p)+1)/2+\lfloor (p+1)/24\rfloor} & \text{if } p\equiv -1,-5 \pmod{24},\\ (-1)^{\lfloor p/24\rfloor-1} & \text{if } p\equiv 7,11 \pmod{24},\end{cases}$$

and

$$\prod_{\substack{i,j=1\\ p\nmid 6i-j}}^{(p-1)/2}\left(\frac{6i-j}{p}\right)=(-1)^{|\{\frac{p+2}{4}<k<\frac{p}{3}:\ (\frac{k}{p})=1\}|}.$$

Remark. This and some other similar conjectures of mine have been proved by my PhD student Chao Huang.

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 (Z.-W. Sun, Int. J. Number Theory, in press). 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

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

Main References

Main References:

1. Zhi-Wei Sun, *Quadratic residues and related permutations and identities*, Finite Fields Appl. **59** (2019), 246-283.

2. Zhi-Wei Sun, *On quadratic residues and quartic residues modulo primes*, Int. J. Number Theory, in press.

Thank you!