Int. J. Number Theory 16 (2020), no. 8, 1833–1858.

QUADRATIC RESIDUES AND QUARTIC RESIDUES MODULO PRIMES

ZHI-WEI SUN

Abstract. In this paper we study some products related to quadratic residues and quartic residues modulo primes. Let p be an odd prime and let A be any integer. We determine completely the product

$$f_p(A) := \prod_{\substack{1\leqslant i,j\leqslant (p-1)/2\\ p\nmid i^2-Aij-j^2}} (i^2-Aij-j^2)$$

modulo p; for example, if $p\equiv 1 \pmod 4$ then

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

where $(\frac{\cdot}{p})$ denotes the Legendre symbol. We also determine

$$\prod_{\substack{i,j=1\\ p\nmid 2i^2+5ij+2j^2}}^{(p-1)/2}\left(2i^2+5ij+2j^2\right) \text{ and } \prod_{\substack{i,j=1\\ p\nmid 2i^2-5ij+2j^2}}^{(p-1)/2}\left(2i^2-5ij+2j^2\right)$$

modulo p.

1. Introduction

For $n\in\mathbb{Z}^+=\{1,2,3,\ldots\}$ and $x=a/b$ with $a,b\in\mathbb{Z}$, $b\neq 0$ and $\gcd(b,n)=1$, we let $\{x\}_n$ denote the unique integer $r\in\{0,\ldots,n-1\}$ with $r\equiv x \pmod n$ (i.e., $a\equiv br \pmod n$). The well-known Gauss Lemma (see, e.g., [6, p. 52]) states that for any odd prime p and integer $x\not\equiv 0 \pmod p$ we have

$$\left(\frac{x}{p}\right)=(-1)^{|\{1\leqslant k<p/2:\ \{kx\}_p>p/2\}|},\tag{1.1}$$

where $(\frac{\cdot}{p})$ is the Legendre symbol. This was extended to Jacobi symbols by M. Jenkins [7] in 1867, who showed (by an elementary method) that for any positive odd integer n and integer x with $\gcd(x,n)=1$ we have

$$\left(\frac{x}{n}\right)=(-1)^{|\{1\leqslant k<n/2:\ \{kx\}_n>n/2\}|},\tag{1.2}$$

where $(\frac{\cdot}{n})$ is the Jacobi symbol. In the textbook [9, Chapters 11-12], H. Rademacher supplied a proof of Jenkins' result by using subtle properties of quadratic Gauss sums.

Now we present our first new theorem.

Theorem 1.1. *Let n be a positive odd integer, and let $x\in\mathbb{Z}$ with* $\gcd(x(1-x),n)=1$. *Then*

$$(-1)^{|\{1\leqslant k<n/2:\ \{kx\}_n>k\}|}=\left(\frac{2x(1-x)}{n}\right).\tag{1.3}$$

Key words and phrases. Quadratic residues, quartic residues, congruences, Lucas sequences.
2020 *Mathematics Subject Classification.* Primary 11A15; Secondary 11A07, 11B39.

Also,

$$(-1)^{|\{1\leqslant k<n/2:\ \{kx\}_n>n/2\ \&\ \{k(1-x)\}_n>n/2\}|}=\left(\frac{2}{n}\right), \tag{1.4}$$

$$(-1)^{|\{1\leqslant k<n/2:\ \{kx\}_n<n/2\ \&\ \{k(1-x)\}_n<n/2\}|}=\left(\frac{2x(x-1)}{n}\right), \tag{1.5}$$

and

$$(-1)^{|\{1\leqslant k<n/2:\ \{kx\}_n>n/2>\{k(1-x)\}_n\}|}=\left(\frac{2x}{n}\right). \tag{1.6}$$

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

$$S_p(a,b,c):=\prod_{\substack{1\leqslant i<j\leqslant p-1\\ p\nmid ai^2+bij+cj^2}}(ai^2+bij+cj^2). \tag{1.7}$$

Using Theorem 1.1, together with [15, Theorem 1.2], we completely determine $S_p(a,b,c)$ mod p in terms of Legendre symbols.

Theorem 1.2. *Let p be an odd prime, and let $a,b,c\in\mathbb{Z}$ and $\Delta=b^2-4ac$. When $p\nmid ac(a+b+c)$, we have*

$$S_p(a,b,c)\equiv\begin{cases}(\frac{a(a+b+c)}{p})\pmod p & \text{if } p\mid\Delta,\\ -(\frac{ac(a+b+c)\Delta}{p})\pmod p & \text{if } p\nmid\Delta.\end{cases} \tag{1.8}$$

In the case $p\mid ac(a+b+c)$, we have

$$S_p(a,b,c)\equiv\begin{cases}0\pmod p & \text{if } p\mid a,\ p\mid b \text{ and } p\mid c,\\ -(\frac{-a}{p})\pmod p & \text{if } p\nmid a,\ p\mid b \text{ and } p\mid c,\\ -(\frac{b}{p})\pmod p & \text{if } p\mid a,\ p\nmid b \text{ and } p\mid c,\\ -(\frac{-c}{p})\pmod p & \text{if } p\mid a,\ p\mid b \text{ and } p\nmid c,\\ -(\frac{c}{p})\pmod p & \text{if } p\mid a,\ p\nmid bc \text{ and } p\mid b+c,\\ -(\frac{a}{p})\pmod p & \text{if } p\nmid ab,\ p\mid a+b \text{ and } p\mid c,\\ -(\frac{-a}{p})\pmod p & \text{if } p\nmid ac,\ p\mid a-c \text{ and } p\mid a+b+c,\\ (\frac{-ac}{p})\pmod p & \text{if } p\nmid ac(a-c) \text{ and } p\mid a+b+c,\\ (\frac{-a(a+b)}{p})\pmod p & \text{if } p\nmid ab(a+b) \text{ and } p\mid c,\\ (\frac{-c(b+c)}{p})\pmod p & \text{if } p\mid a \text{ and } p\nmid bc(b+c),\end{cases} \tag{1.9}$$

We will prove Theorem 1.1 and those parts of Theorem 1.2 not covered by [15, Theorem 1.2] in Section 2.

Let p be an odd prime. For $a,b,c\in\mathbb{Z}$ we introduce

$$T_p(a,b,c):=\prod_{\substack{i,j=1\\ p\nmid ai^2+bij+cj^2}}^{(p-1)/2}(ai^2+bij+cj^2). \tag{1.10}$$

Our following theorem determines $T_p(1,-(a+b),-1)$ modulo p for all $a,b\in\mathbb{Z}$ with $ab\equiv-1\pmod p$.

Theorem 1.3. *Let p be any odd prime, and let $a,b\in\mathbb{Z}$ with $ab\equiv -1 \pmod p$. Set*

$$\{a,b\}_p := \prod_{\substack{i,j=1\\ i\not\equiv aj,bj \pmod p}}^{(p-1)/2} (i-aj)(i-bj), \tag{1.11}$$

which is congruent to $T_p(1,-(a+b),-1)$ modulo p.

(i) *We have*

$$-\{a,b\}_p \equiv \begin{cases} (\frac{a-b}{p}) \pmod p & \text{if } p\equiv 1 \pmod 4 \ \&\ p\nmid (a-b),\\ (\frac{a(a-b)}{p}) = (\frac{a^2+1}{p}) \pmod p & \text{if } p\equiv 3 \pmod 4.\end{cases} \tag{1.12}$$

(ii) *If $a\equiv b \pmod p$ and $p\equiv 1 \pmod 8$, then*

$$\{a,b\}_p \equiv (-1)^{(p+7)/8}\frac{p-1}{2}! \pmod p.$$

If $p\equiv 5 \pmod 8$ and $a\equiv b\equiv (-1)^k((p-1)/2)! \pmod p$ with $k\in\{0,1\}$, then

$$\{a,b\}_p \equiv (-1)^{k+(p-5)/8} \pmod p.$$

Our proof of Theorem 1.3 will be given in Section 3.

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

$$u_0(A)=0,\ u_1(A)=1,\ \text{and } u_{n+1}(A)=Au_n(A)+u_{n-1}(A) \text{ for } n=1,2,3,\ldots,$$

and

$$v_0(A)=2,\ v_1(A)=A,\ \text{and } v_{n+1}(A)=Av_n(A)+v_{n-1}(A) \text{ for } n=1,2,3,\ldots.$$

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

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

Thus

$$\left(\frac{A\pm\sqrt{A^2+4}}{2}\right)^n = \frac{v_n(A)\pm u_n(A)\sqrt{A^2+4}}{2} \quad \text{for all } n\in\mathbb{N}. \tag{1.13}$$

Now we state our fourth theorem which determines $T_p(1,-A,-1)$ for any odd prime p and integer A.

Theorem 1.4. *Let p be an odd prime and let $A\in\mathbb{Z}$.*

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

$$T_p(1,-A,-1)\equiv \begin{cases} (-1)^{(p+7)/8}((p-1)/2)! \pmod p & \text{if } p\equiv 1 \pmod 8,\\ (-1)^{k+(p-5)/8} \pmod p & \text{if } p\equiv 5 \pmod 8.\end{cases} \tag{1.14}$$

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

$$T_p(1,-A,-1)\equiv \begin{cases} -(A^2+4)^{(p-1)/4} \pmod p & \text{if } p\equiv 1 \pmod 4,\\ -(A^2+4)^{(p+1)/4}u_{(p-1)/2}(A)/2 \pmod p & \text{if } p\equiv 3 \pmod 4.\end{cases} \tag{1.15}$$

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

$$T_p(1,-A,-1)\equiv\begin{cases}(-A^2-4)^{(p-1)/4}\pmod p&\text{if } p\equiv 1\pmod 4,\\(-A^2-4)^{(p+1)/4}u_{(p+1)/2}(A)/2\pmod p&\text{if } p\equiv 3\pmod 4.\end{cases}\tag{1.16}$$

We will prove Theorem 1.4 in Section 4.

Let p be a prime with $p\equiv 1\pmod 4$. Then $(\frac{p-1}{2}!)^2\equiv -1\pmod p$ by Wilson's theorem. We may write $p=x^2+y^2$ with $x,y\in\mathbb{Z}$, $x\equiv 1\pmod 4$ and $y\equiv\frac{p-1}{2}!x\pmod p$. Recall that an integer a not divisible by p is a quartic residue modulo p (i.e., $z^4\equiv a\pmod p$ for some $z\in\mathbb{Z}$) if and only if $a^{(p-1)/4}\equiv 1\pmod p$. Dirichlet proved that 2 is a quartic residue modulo p if and only if $8\mid y$ (see, e.g., [6, p. 64, Exer. 28]). On the other hand, we have

$$\left|\left\{1\leqslant k<\frac p4:\ \left(\frac kp\right)=1\right\}\right|\equiv 0\pmod 2\iff y\equiv(-1)^{(p-1)/4}-1\pmod 8$$

as discovered by K. Burde [2] and re-proved by K. S. Williams [16]. In view of Williams and J. D. Currie [17, (1.4)], we have

$$2^{(p-1)/4}\equiv(-1)^{|\{1\leqslant k<\frac p4:\ (\frac kp)=-1\}|}\times\begin{cases}1\pmod p&\text{if } p\equiv 1\pmod 8,\\\frac{p-1}{2}!\pmod p&\text{if } p\equiv 5\pmod 8.\end{cases}$$

By Dirichlet's class number formula (see, e.g., L.E. Dickson [4, p. 101]),

$$\frac{p-1}{2}-4\left|\left\{1\leqslant k<\frac p4:\ \left(\frac kp\right)=-1\right\}\right|=h(-4p),$$

where $h(d)$ with $d\equiv 0,1\pmod 4$ not a square denotes the class number of the quadratic field with discriminant d. In 1905, Lerch (see, e.g., [5]) proved that

$$h(-3p)=2\sum_{1\leqslant k<p/3}\left(\frac kp\right).$$

By [17, Lemma 14],

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

Thus, if $p\equiv 1\pmod{12}$ then

$$(-3)^{(p-1)/4}\equiv(-1)^{\frac12\sum_{k=1}^{(p-1)/3}((\frac kp)-1)+\frac{p-1}{6}}=(-1)^{|\{1\leqslant k<\frac p3:\ (\frac kp)=-1\}|}\pmod p;$$

similarly, if $p\equiv 5\pmod{12}$ then

$$(-3)^{(p-1)/4}\equiv(-1)^{|\{1\leqslant k<\frac p3:\ (\frac kp)=-1\}|}\,\frac{p-1}{2}!\pmod p.$$

From Theorem 1.4, we deduce the following result which will be proved in Section 5.

Theorem 1.5. *Let p be an odd prime.*

(i) *We have*

$$T_p(1,-1,-1)\equiv\begin{cases}-5^{(p-1)/4}\pmod p & \text{if } p\equiv 1,9\pmod{20},\\ (-5)^{(p-1)/4}\pmod p & \text{if } p\equiv 13,17\pmod{20},\\ (-1)^{\lfloor (p-10)/20\rfloor}\pmod p & \text{if } p\equiv 3,7\pmod{20},\\ (-1)^{\lfloor (p-5)/10\rfloor}\pmod p & \text{if } p\equiv 11,19\pmod{20}.\end{cases}\tag{1.17}$$

(ii) *We have*

$$T_p(1,-2,-1)\equiv\begin{cases}-2^{(p-1)/4}\pmod p & \text{if } p\equiv 1\pmod{8},\\ 2^{(p-1)/4}\pmod p & \text{if } p\equiv 5\pmod{8},\\ (-1)^{(p-3)/8}\pmod p & \text{if } p\equiv 3\pmod{8},\\ (-1)^{(p-7)/8}\pmod p & \text{if } p\equiv 7\pmod{8}.\end{cases}\tag{1.18}$$

Now we state our sixth theorem.

Theorem 1.6. *Let $p>3$ be a prime and let $\delta\in\{\pm1\}$. If $p\equiv 1\pmod 4$, then*

$$T_p(2,5\delta,2)\equiv(-1)^{\lfloor (p+11)/12\rfloor}\pmod p.\tag{1.19}$$

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

$$T_p(2,5\delta,2)\equiv\left(\frac{6}{p}\right)\frac{\delta 2^{\delta}}{3^{\delta}}\binom{(p-3)/2}{(p-3)/4}^{-2\delta}\pmod p.\tag{1.20}$$

Note that there is no simple closed form for $\binom{(p-3)/2}{(p-3)/4}$ modulo a prime $p\equiv 3\pmod 4$. For a prime $p\equiv 1\pmod 4$ with $p=x^2+y^2$ ($x,y\in\mathbb{Z}$ and $x\equiv 1\pmod 4$), Gauss showed the congruence $\binom{(p-1)/2}{(p-1)/4}\equiv 2x\pmod p$, and S. Chowla, B. Dwork and R. J. Evans [3] used Gauss and Jacobi sums to prove further that

$$\binom{(p-1)/2}{(p-1)/4}\equiv\frac{2^{p-1}+1}{2}\left(2x-\frac{p}{2x}\right)\pmod{p^2},$$

which was first conjectured by F. Beukers. (See also [1, Chapter 9] for further related results.)

Though we have made some numerical tests via a computer, we are unable to find general patterns for $T_p(a,b,c)$ modulo p, where p is an arbitrary odd prime and a,b,c are arbitrary integers.

Let p be an odd prime. It is known (cf. [15, (1.6) and (1.7)]) that

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

From this we immediately get

$$\prod_{\substack{1\leqslant i<j\leqslant (p-1)/2\\ p\nmid i^2+j^2}}\left(\frac{i^2+j^2}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1\pmod 4,\\ (-1)^{\lfloor (p+1)/8\rfloor} & \text{if } p\equiv 3\pmod 4.\end{cases}$$

As the product $\prod_{1\leqslant i<j\leqslant (p-1)/2}(i^2-j^2)$ modulo p was determined via [15, (1.5)], we also know the value of the product

$$\prod_{1\leqslant i<j\leqslant (p-1)/2}\left(\frac{i^2-j^2}{p}\right)=\prod_{1\leqslant i<j\leqslant (p-1)/2}\left(\frac{i-j}{p}\right)\left(\frac{i+j}{p}\right)$$

Motivated by this, we obtain the following result.

Theorem 1.7. *Let $p>3$ be a prime and let $\delta\in\{\pm1\}$. Then*

$$\prod_{1\leqslant i<j\leqslant(p-1)/2}\left(\frac{j+\delta i}{p}\right)=\begin{cases}(-1)^{|\{0<k<\frac p4:\ (\frac kp)=\delta\}|}&\text{if } p\equiv1\pmod 4,\\(-1)^{(p-3)/8}&\text{if } p\equiv3\pmod 8,\\(-1)^{(p+1)/8+(h(-p)+1)/2}&\text{if } p\equiv7\pmod 8.\end{cases}\tag{1.21}$$

We will prove Theorems 1.6 and 1.7 in Section 6, and pose ten conjectures in Section 7.

2. Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1. 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

$$\left|\left\{1\leqslant k<\frac n2:\ \{kx\}_n>k\right\}\right|=\frac{n-1}{2}-\sum_{k=1}^{(n-1)/2}\left(\left\lfloor\frac{kx}{n}\right\rfloor-\left\lfloor\frac{k(x-1)}{n}\right\rfloor\right)$$

and hence

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

As $\{kx\}_n\equiv1+n-\{kx\}_n\pmod 2$ for all $k=1,\ldots,(n-1)/2$, we have

$$\begin{aligned}\sum_{k=1}^{(n-1)/2}\{kx\}_n&\equiv\sum_{\substack{k=1\\ \{kx\}_n<n/2}}^{(n-1)/2}\{kx\}_n+\sum_{\substack{k=1\\ \{kx\}_n>n/2}}^{(n-1)/2}(1+(n-\{kx\}_n))\\&=\sum_{\substack{k=1\\ \{kx\}_n>n/2}}^{(n-1)/2}1+\sum_{r=1}^{(n-1)/2}r\\&=\left|\left\{1\leqslant k<\frac n2:\ \{kx\}_n>\frac n2\right\}\right|+\frac{n^2-1}{8}\pmod 2.\end{aligned}$$

and hence

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

with the help of (1.2). Similarly,

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

In view of the above, we obtain

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

This proves (1.3).

When $1\leqslant k<n/2$ and $\{kx\}_n<n/2$, we clearly have

$$\{kx\}_n>k\iff\{k(1-x)\}_n>\frac{n}{2}.$$

Thus

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

and hence by (1.2) and (1.3) we get

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

This proves (1.4).

In view of (1.2) and (1.4), we also have

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

This proves (1.6).

By (1.4) and (1.6), we have

$$\begin{aligned}&\left(\frac{2}{n}\right)(-1)^{|\{1\leqslant k<n/2:\ \{kx\}_n<n/2\ \&\ \{k(1-x)\}_n<n/2\}|}\\=&(-1)^{|\{1\leqslant k<n/2:\ (\{kx\}_n-n/2)(\{k(1-x)\}_n-n/2)>0\}|}\\=&(-1)^{(n-1)/2-|\{1\leqslant k<n/2:\ \{kx\}_n>n/2>\{k(1-x)\}_n\text{ or }\{k(1-x)\}_n>n/2>\{kx\}_n\}|}\\=&\left(\frac{-1}{n}\right)\left(\frac{2x}{n}\right)\left(\frac{2(1-x)}{n}\right)=\left(\frac{x(x-1)}{n}\right).\end{aligned}$$

So (1.5) also holds.

The proof of Theorem 1.1 is now complete. □

For any odd prime p and rational p-adic integer x, we define

$$N_p(x):=|\{1\leqslant k<p/2:\ \{kx\}_p>k\}|. \tag{2.1}$$

Proof of Theorem 1.2. By parts (ii)-(iv) of Sun [15, Theorem 1.2], the desired result holds except for the cases

$$\text{I. } p\nmid ac(a-c) \text{ and } p\mid a+b+c,$$
$$\text{II. } p\nmid ab(a+b) \text{ and } p\mid c,$$
$$\text{III. } p\mid a \text{ and } p\nmid bc(b+c).$$

In case I, by [15, Theorem 1.2(iii)] we have

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

As

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

by Theorem 1.1, we obtain

$$S_p(a,b,c)\equiv\left(\frac{2a(c-a)}{p}\right)\left(\frac{2c(a-c)}{p}\right)=\left(\frac{-ac}{p}\right)\pmod p.$$

In case II, by [15, Theorem 1.2(iv)] we have

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

As

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

by Theorem 1.1, we get

$$S_p(a,b,c)\equiv\left(\frac{-2a(a+b)}{p}\right)\left(\frac{2}{p}\right)=\left(\frac{-a(a+b)}{p}\right)\pmod p.$$

In case III, by [15, Theorem 1.2(iv)] we have

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

Since $(-1)^{N_p(-c/b)}=(\frac{-2c(b+c)}{p})$ by Theorem 1.1, we deduce that

$$S_p(a,b,c)\equiv\left(\frac{-2c(b+c)}{p}\right)\left(\frac{2}{p}\right)=\left(\frac{-c(b+c)}{p}\right)\pmod p.$$

In view of the above, we have completed the proof of Theorem 1.2. □

3. Proof of Theorem 1.3

Lemma 3.1. *Let p be any odd prime. Then*

$$\left(\frac{p-1}{2}!\right)^2\equiv(-1)^{(p+1)/2}\pmod p,\tag{3.1}$$

and

$$\prod_{1\leqslant i<j\leqslant(p-1)/2}(j^2-i^2)\equiv\begin{cases}-((p-1)/2)!\pmod p & \text{if } p\equiv1\pmod 4,\\ 1\pmod p & \text{if } p\equiv3\pmod 4.\end{cases}\tag{3.2}$$

Remark 3.2. (3.1) is an easy consequence of Wilson's theorem. (3.2) is also known, see [15, (1.5)] and its few-line proof there.

Lemma 3.3. *Let p be a prime with $p \equiv 1 \pmod 4$. Then*

$$\left|\left\{1 \leqslant k \leqslant \frac{p-1}{2} : \left\{k \times \frac{p-1}{2}!\right\}_p > \frac{p}{2}\right\}\right| = \frac{p-1}{4}. \tag{3.3}$$

Proof. Let $a = ((p-1)/2)!$. Then $a^2 \equiv -1 \pmod p$ by (3.1). For any $k = 1, \ldots, (p-1)/2$, there is a unique integer $k^* \in \{1, \ldots, (p-1)/2\}$ congruent to ak or $-ak$ modulo p. Note that $k^* \neq k$ since $a \not\equiv \pm 1 \pmod p$. If $\{ak\}_p > p/2$ then $\{ak^*\}_p = \{a(-ak)\}_p = k < p/2$; if $\{ak\}_p < p/2$ then $\{ak^*\}_p = \{a(ak)\}_p = p - k > p/2$. So, exactly one of $\{ak\}_p$ and $\{ak^*\}_p$ is greater than $p/2$. Therefore (3.3) holds. $\square$

Remark 3.4. In view of Gauss' Lemma, Lemma 3.3 is stronger than the fact that $(\frac{((p-1)/2)!}{p}) = (\frac{2}{p})$ for any prime $p \equiv 1 \pmod 4$ (cf. [14, Lemma 2.3]).

Proof of Theorem 1.3. Observe that

$$\begin{aligned}\prod_{\substack{i,j=1\\ p\nmid i^2-j^2}}^{(p-1)/2}(i^2-j^2) =& \prod_{1\leqslant i<j\leqslant (p-1)/2}(i^2-j^2)(j^2-i^2)\\ =&(-1)^{\binom{(p-1)/2}{2}}\prod_{1\leqslant i<j\leqslant (p-1)/2}(j^2-i^2)^2\end{aligned}$$

and hence

$$\prod_{\substack{i,j=1\\ p\nmid i^2-j^2}}^{(p-1)/2}(i^2-j^2) \equiv -\left(\frac{2}{p}\right) \pmod p \tag{3.4}$$

with the help of Lemma 3.1.

When $a \equiv \pm 1 \pmod p$, we have $b \equiv \mp 1 \not\equiv a \pmod p$ and hence

$$\{a,b\}_p \equiv -\left(\frac{2}{p}\right) = \begin{cases}-(\frac{a-b}{p}) \pmod p & \text{if } p \equiv 1 \pmod 4,\\ -(\frac{a^2+1}{p}) \pmod p & \text{if } p \equiv 3 \pmod 4.\end{cases}$$

So (1.12) holds in the case $a \equiv \pm 1 \pmod p$.

Below we assume that $a \not\equiv \pm 1 \pmod p$. As $ab \equiv -1 \pmod p$, we have

$$\begin{aligned}\{a,b\}_p =& \prod_{\substack{i,j=1\\ i\not\equiv aj,bj \pmod p}}^{(p-1)/2}(i-aj) \times \prod_{\substack{i,j=1\\ j\not\equiv ai,bi \pmod p}}^{(p-1)/2}(j-bi)\\ \equiv& \prod_{\substack{i,j=1\\ p\nmid (i-aj)(j+ai)}}^{(p-1)/2}(i-aj) \times \prod_{\substack{i,j=1\\ p\nmid (i+aj)(j-ai)}}^{(p-1)/2}\frac{i+aj}{a} \pmod p.\end{aligned} \tag{3.5}$$

(i) If $p \equiv 3 \pmod 4$, then $(\frac{-1}{p}) = -1$ and hence $a \not\equiv b \pmod p$. Now we prove (1.12) under the assumption $a \not\equiv b \pmod p$. Note that $a^2 \not\equiv \pm 1 \pmod p$.

For $1\leqslant i,j\leqslant (p-1)/2$, we cannot have $i^2-a^2j^2\equiv j^2-a^2i^2\equiv 0 \pmod p$. Thus

$$\begin{aligned}&\left|\left\{(i,j):\ 1\leqslant i,j\leqslant \frac{p-1}{2}\ \&\ p\nmid (i+aj)(j-ai)\right\}\right|\\
=&\left(\frac{p-1}{2}\right)^2-\left|\left\{(i,j):\ 1\leqslant i,j\leqslant \frac{p-1}{2}\ \&\ p\mid i+aj\right\}\right|\\
&-\left|\left\{(i,j):\ 1\leqslant i,j\leqslant \frac{p-1}{2}\ \&\ p\mid j-ai\right\}\right|\\
=&\left(\frac{p-1}{2}\right)^2-\left|\left\{1\leqslant j\leqslant \frac{p-1}{2}:\ \{aj\}_p>\frac p2\right\}\right|\\
&-\left|\left\{1\leqslant i\leqslant \frac{p-1}{2}:\ \{ai\}_p<\frac p2\right\}\right|\\
=&(p-1)\frac{p-1}{4}-\frac{p-1}{2}=\frac{p-1}{2}\cdot\frac{p+1}{2}-(p-1)\end{aligned}$$

and hence

$$a^{|\{(i,j):\ 1\leqslant i,j\leqslant (p-1)/2\ \&\ p\nmid (i+aj)(j-ai)\}|}\equiv (a^{(p-1)/2})^{(p+1)/2}\equiv\left(\frac ap\right)^{(p+1)/2}\pmod p.$$

Combining this with (3.5), we obtain

$$\begin{aligned}&\left(\frac ap\right)^{(p+1)/2}\{a,b\}_p\\
\equiv&\prod_{\substack{i,j=1\\ p\nmid (i^2-a^2j^2)(j^2-a^2i^2)}}^{(p-1)/2}(i^2-a^2j^2)\times\prod_{\substack{i,j=1\\ i\equiv aj\ (\mathrm{mod}\ p)}}^{(p-1)/2}(i+aj)\times\prod_{\substack{i,j=1\\ i\equiv -aj\ (\mathrm{mod}\ p)}}^{(p-1)/2}(i-aj)\\
&\times\prod_{\substack{i,j=1\\ j-ai\equiv -a(i+bj)\equiv 0\ (\mathrm{mod}\ p)}}^{(p-1)/2}(i-aj)\times\prod_{\substack{i,j=1\\ j+ai\equiv a(i-bj)\equiv 0\ (\mathrm{mod}\ p)}}^{(p-1)/2}(i+aj)\\
\equiv&\prod_{\substack{i,j=1\\ p\nmid i^2-a^2j^2}}^{(p-1)/2}(i^2-a^2j^2)\Big/\prod_{\substack{i,j=1\\ p\mid j^2-a^2i^2}}^{(p-1)/2}(i^2-a^2j^2)\\
&\times(-1)^{|\{1\leqslant j\leqslant (p-1)/2:\ \{aj\}_p>p/2\}|}\prod_{j=1}^{(p-1)/2}(2aj)\\
&\times(-1)^{|\{1\leqslant j\leqslant (p-1)/2:\ \{bj\}_p>p/2\}|}\prod_{j=1}^{(p-1)/2}(bj+aj)\pmod p\end{aligned}$$

Thus, by using (3.4) and Gauss' Lemma, we see that

$$\begin{aligned}\left(\frac{a}{p}\right)^{(p+1)/2}\{a,b\}_p \equiv& \prod_{\substack{i,k=1\\ p\nmid i^2-k^2}}^{(p-1)/2}(i^2-k^2)\Big/\prod_{i=1}^{(p-1)/2}(i^2-a^2(a^2i^2))\\ &\times\left(\frac{ab}{p}\right)(2a(a+b))^{(p-1)/2}\left(\frac{p-1}{2}!\right)^2\\ \equiv& -\left(\frac{2}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{2(a^2-1)(1-a^4)}{p}\right)\\ =& -\left(\frac{a^2+1}{p}\right)=-\left(\frac{a^2-ab}{p}\right) \pmod p.\end{aligned}$$

This proves (1.12).

(ii) Now we come to prove part (ii) of Theorem 1.3. Assume that $a\equiv b \pmod p$. Then $a^2\equiv ab\equiv -1 \pmod p$ and hence $p\equiv 1 \pmod 4$. As $j\pm ai\equiv \pm a(i\mp aj) \pmod p$, by (3.5) we have

$$\begin{aligned}\{a,b\}_p \equiv& a^{-|\{(i,j):\ 1\leqslant i,j\leqslant (p-1)/2\ \&\ p\nmid i+aj\}|}\prod_{\substack{i,j=1\\ p\nmid i-aj}}^{(p-1)/2}(i-aj)\times\prod_{\substack{i,j=1\\ p\nmid i+aj}}^{(p-1)/2}(i+aj)\\ \equiv& a^{-(p-1)^2/4+|\{(i,j):\ 1\leqslant i,j\leqslant (p-1)/2\ \&\ p\mid i+aj\}|}\prod_{\substack{i,j=1\\ p\nmid i^2-(aj)^2}}^{(p-1)/2}(i^2-(aj)^2)\\ &\times\prod_{\substack{i,j=1\\ p\mid i-aj}}^{(p-1)/2}(i+aj)\times\prod_{\substack{i,j=1\\ p\mid i+aj}}^{(p-1)/2}(i-aj)\\ \equiv& a^{|\{(i,j):\ 1\leqslant i,j\leqslant (p-1)/2\ \&\ p\mid i+aj\}|}\prod_{\substack{i,k=1\\ p\nmid i^2-k^2}}^{(p-1)/2}(i^2-k^2)\\ &\times(-1)^{|\{1\leqslant j\leqslant (p-1)/2:\ \{aj\}_p>p/2\}|}\prod_{j=1}^{(p-1)/2}(2aj). \pmod p\end{aligned}$$

Applying (3.4) and Gauss' Lemma, from the above we get

$$\begin{aligned}\{a,b\}_p \equiv& a^{|\{1\leqslant j\leqslant (p-1)/2:\ \{aj\}_p>p/2\}|}\times\left(-\left(\frac{2}{p}\right)\right)\left(\frac{a}{p}\right)(2a)^{(p-1)/2}\frac{p-1}{2}!\\ \equiv& -\frac{p-1}{2}!\times a^{|\{1\leqslant j\leqslant (p-1)/2:\ \{aj\}_p>p/2\}|} \pmod p.\end{aligned}\tag{3.6}$$

As $a^2\equiv -1\equiv ((p-1)/2)!)^2$, we have $a\equiv (-1)^k((p-1)/2)! \pmod p$ for some $k\in\{0,1\}$. In view of Lemma 3.3,

$$\begin{aligned}&\left|\left\{1\leqslant j\leqslant \frac{p-1}{2}:\ \left\{-\frac{p-1}{2}!\,j\right\}_p>\frac{p}{2}\right\}\right|\\ =&\left|\left\{1\leqslant j\leqslant \frac{p-1}{2}:\ \left\{\frac{p-1}{2}!\,j\right\}_p<\frac{p}{2}\right\}\right|=\frac{p-1}{4}.\end{aligned}$$

Hence

$$\begin{aligned}&a^{|\{1\leqslant j\leqslant (p-1)/2:\ \{aj\}_p>p/2\}|}\\=&a^{(p-1)/4}=(-1)^{k(p-1)/4}\left(\frac{p-1}{2}!\right)^{(p-1)/4}\\\equiv&\begin{cases}(\frac{p-1}{2}!)^{2(p-1)/8}\equiv(-1)^{(p-1)/8}\pmod p&\text{if }p\equiv1\pmod 8,\\(-1)^k\frac{p-1}{2}!(\frac{p-1}{2}!)^{2(p-5)/8}\equiv(-1)^{k+(p-5)/8}\frac{p-1}{2}!\pmod p&\text{if }p\equiv5\pmod 8.\end{cases}\end{aligned}$$

Combining this with (3.6) we immediately obtain the desired results in Theorem 1.3(ii).

In view of the above, we have completed the proof of Theorem 1.3. □

4. Proof of Theorem 1.4

Proof of Theorem 1.4(i). As $A^2\equiv-4\pmod p$, we have $(\frac{-1}{p})=1$ and hence $p\equiv 1\pmod 4$. Since $((p-1)/2)^2\equiv-1\equiv(A/2)^2\pmod p$, for some $k\in\{0,1\}$ we have $A/2\equiv(-1)^k((p-1)/2)!\pmod p$. Choose $a,b\in\mathbb{Z}$ with $a\equiv b\equiv A/2\pmod p$. Note that $\{a,b\}_p\equiv T_p(1,-A,-1)\pmod p$. Applying Theorem 1.3(ii) we immediately get the desired (1.14). □

For any odd prime p and integer A with $\Delta=A^2+4\not\equiv0\pmod p$, it is known (cf. [13, Lemma 2.3]) that

$$u_{(p-(\frac{\Delta}{p})/2}(A)v_{(p-(\frac{\Delta}{p}))/2}(A)=u_{p-(\frac{\Delta}{p})}(A)\equiv0\pmod p.$$

Lemma 4.1. *Let $A\in\mathbb{Z}$ and let p be an odd prime not dividing $\Delta=A^2+4$. Then*

$$p\mid v_{(p-(\frac{\Delta}{p}))/2}(A)\iff\left(\frac{-1}{p}\right)=-1.\tag{4.1}$$

Remark 4.2. This is a known result, see, e.g., [10, Chapter 2, (IV.23)].

Proof of Theorem 1.4(ii). Let $\Delta=A^2+4$. As $(\frac{\Delta}{p})=1$, we have $d^2\equiv\Delta$ for some $d\in\mathbb{Z}$ with $p\nmid d$. Choose integers a and b such that

$$a\equiv\frac{A+d}{2}\pmod p\ \text{and}\ b\equiv\frac{A-d}{2}\pmod p.$$

Then $a+b\equiv A\pmod p$ and $ab\equiv(A^2-d^2)/4\equiv-1\pmod p$. Thus, for any $i,j\in\mathbb{Z}$ we have

$$i^2-Aij-j^2\equiv(i-aj)(i-bj)\pmod p.$$

If $p\equiv1\pmod 4$, then

$$(A^2+4)^{(p-1)/4}\equiv d^{(p-1)/2}\equiv(a-b)^{(p-1)/2}\equiv\left(\frac{a-b}{p}\right)\pmod p.$$

If $p\equiv3\pmod 4$, then

$$\left(\frac{2d(A+d)}{p}\right)=\left(\frac{ad}{p}\right)=\left(\frac{a(a-b)}{p}\right).$$

For any positive integer n, clearly

$$\begin{aligned}u_n(A) =&\frac{1}{\sqrt{\Delta}}\bigg(\bigg(\frac{A+\sqrt{\Delta}}{2}\bigg)^n - \bigg(\frac{A-\sqrt{\Delta}}{2}\bigg)^n\bigg)\\ =&\frac{1}{2^{n-1}}\sum_{k=0}^{\lfloor (n-1)/2\rfloor}\binom{n}{2k+1}A^{n-1-2k}\Delta^k\\ \equiv&\frac{1}{2^{n-1}}\sum_{k=0}^{\lfloor (n-1)/2\rfloor}\binom{n}{2k+1}A^{n-1-2k}d^{2k}\\ =&\frac{1}{d}\bigg(\bigg(\frac{A+d}{2}\bigg)^n - \bigg(\frac{A-d}{2}\bigg)^n\bigg) \pmod p\end{aligned}$$

and

$$\begin{aligned}v_n(A) = \bigg(\frac{A+\sqrt{\Delta}}{2}\bigg)^n + \bigg(\frac{A-\sqrt{\Delta}}{2}\bigg)^n = \frac{1}{2^{n-1}}\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n}{2k}A^{n-2k}\Delta^k\\ \equiv\frac{1}{2^{n-1}}\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n}{2k}A^{n-2k}d^{2k} = \bigg(\frac{A+d}{2}\bigg)^n + \bigg(\frac{A-d}{2}\bigg)^n \pmod p.\end{aligned}$$

In the case $p\equiv 3 \pmod 4$, we have $p \mid v_{(p-1)/2}(A)$ by Lemma 4.1, and hence

$$\begin{aligned}\bigg(\frac{2\delta(A+d)}{p}\bigg) \equiv& d^{(p-1)/2}\bigg(\frac{A+d}{2}\bigg)^{(p-1)/2} \equiv d^{(p-1)/2}\frac{v_{(p-1)/2}(A)+du_{(p-1)/2}(A)}{2}\\ \equiv& \left(d^2\right)^{(p+1)/4}\frac{u_{(p-1)/2}(A)}{2} \equiv \Delta^{(p+1)/4}\frac{u_{(p-1)/2}(A)}{2} \pmod p.\end{aligned}$$

In view of the above, we obtain (1.15) from Theorem 1.3(i). □

Lemma 4.3. *Let p be an odd prime, and let $A\in\mathbb{Z}$ with $\Delta = A^2+4\not\equiv 0 \pmod p$. If $p\equiv 1 \pmod 4$, then*

$$u_{(p+(\frac{\Delta}{p}))/2}(A) \equiv \pm\Delta^{(p-1)/4} \pmod p. \tag{4.2}$$

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

$$u_{(p-(\frac{\Delta}{p}))/2}(A) \equiv \pm 2\Delta^{(p-3)/4} \pmod p. \tag{4.3}$$

Remark 4.4. This is a known result, see, e.g., [11, Theorem 4.1].

Proof of Theorem 1.4(iii). Let

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

As $x^2-Ax-1=(x-\alpha)(x-\beta)$, both α and β are algebraic integers. Observe that

$$\begin{aligned}&\prod_{i,j=1}^{(p-1)/2}(i^2-Aij-j^2)\\ =&\prod_{i,j=1}^{(p-1)/2}(i-\alpha j)(i-\beta j)=\prod_{i,j=1}^{(p-1)/2}(i-\alpha j)\times\prod_{i,j=1}^{(p-1)/2}(j-\beta i)\\ =&\prod_{i,j=1}^{(p-1)/2}(i-\alpha j)\times\prod_{i,j=1}^{(p-1)/2}\frac{\alpha j+i}{\alpha}=\alpha^{-((p-1)/2)^2}\prod_{i,j=1}^{(p-1)/2}(i^2-\alpha^2j^2)\\ =&\alpha^{-((p-1)/2)^2}\prod_{i,j=1}^{(p-1)/2}(-j^2)\left(\alpha^2-\frac{i^2}{j^2}\right)\\ =&(-\alpha)^{-((p-1)/2)^2}\left(\frac{p-1}{2}!\right)^{2\frac{p-1}{2}}\prod_{j=1}^{(p-1)/2}\prod_{i=1}^{(p-1)/2}\left(\alpha^2-\frac{i^2}{j^2}\right)\end{aligned}$$

and hence

$$\prod_{i,j=1}^{(p-1)/2}(i^2-Aij-j^2)\equiv\beta^{((p-1)/2)^2}\prod_{k=1}^{(p-1)/2}(\alpha^2-k^2)^{(p-1)/2}\pmod p$$

(in the ring of all algebraic integers) since for any $j,k=1,\dots,(p-1)/2$ there is a unique $i\in\{1,\dots,(p-1)/2\}$ congruent to jk or $-jk$ modulo p. Note that

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

Thus

$$\begin{aligned}\prod_{i,j=1}^{(p-1)/2}(i^2-Aij-j^2)\equiv&\beta^{((p-1)/2)^2}((\alpha^2)^{(p-1)/2}-1)^{(p-1)/2}\\ =&\beta^{((p-1)/2)^2}\left(\alpha^{p-1}-1\right)^{(p-1)/2}\\ =&\left((-\alpha)^{(p-1)/2}-\beta^{(p-1)/2}\right)^{(p-1)/2}\pmod p.\end{aligned}$$

Case 1. $p\equiv 1\pmod 4$.

In this case,

$$\begin{aligned}\prod_{i,j=1}^{(p-1)/2}(i^2-Aij-j^2)\equiv&\left(\frac{\alpha^{(p-1)/2}-\beta^{(p-1)/2}}{\alpha-\beta}\right)^{(p-1)/2}(\alpha-\beta)^{(p-1)/2}\\ =&u_{(p-1)/2}(A)^{(p-1)/2}\Delta^{(p-1)/4}\pmod p.\end{aligned}$$

As $(\frac{\Delta}{p})=-1$, by Lemma 4.3 we have $u_{(p-1)/2}(A)\equiv\pm\Delta^{(p-1)/4}\pmod p$ and hence

$$u_{(p-1)/2}(A)^{(p-1)/2}\equiv\Delta^{\frac{p-1}{2}\cdot\frac{p-1}{4}}\equiv(-1)^{(p-1)/4}\pmod p.$$

Therefore

$$\prod_{i,j=1}^{(p-1)/2}(i^2-Aij-j^2)\equiv(-\Delta)^{(p-1)/4}\pmod p.$$

Case 2. $p \equiv 3 \pmod 4$.

In this case,

$$\prod_{i,j=1}^{(p-1)/2}(i^2-Aij-j^2) \equiv -\left(\alpha^{(p-1)/2}+\beta^{(p-1)/2}\right)^{(p-1)/2} = -\,v_{(p-1)/2}(A)^{(p-1)/2} \pmod p.$$

It is easy to see that $2v_{n-1}(A)=\Delta u_n(A)-Av_n(A)$ for all $n=1,2,3,\ldots$. Hence

$$2v_{(p-1)/2}(A)=\Delta u_{(p+1)/2}(A)-Av_{(p+1)/2}(A)\equiv \Delta u_{(p+1)/2}(A) \pmod p$$

since $v_{(p+1)/2}(A)=v_{(p-(\frac{\Delta}{p}))/2}(A)\equiv 0 \pmod p$ by Lemma 4.1. Thus

$$\prod_{i,j=1}^{(p-1)/2}(i^2-Aij-j^2) \equiv -\left(\frac{\Delta}{2}u_{(p+1)/2}(A)\right)^{(p-1)/2} \equiv \frac{u_{(p+1)/2}(A)}{2}\left(\frac{u_{(p+1)/2}(A)}{2}\right)^{(p-3)/2} \pmod p.$$

As $(\frac{\Delta}{p})=-1$, by Lemma 4.3 we have $u_{(p+1)/2}(A)\equiv \pm 2\Delta^{(p-3)/4} \pmod p$, and hence

$$\prod_{i,j=1}^{(p-1)/2}(i^2-Aij-j^2) \equiv \frac{u_{(p+1)/2}(A)}{2}\Delta^{\frac{p-3}{4}\cdot\frac{p-3}{2}} = \frac{u_{(p+1)/2}(A)}{2}\Delta^{\frac{p+1}{2}\cdot\frac{p+1}{4}-(p-1)} \equiv \frac{u_{(p+1)/2}(A)}{2}(-\Delta)^{(p+1)/4} \pmod p.$$

In view of the above, we have completed the proof of Theorem 1.4(iii). □

5. Proof of Theorem 1.5

Proof Theorem 1.5. Note that $\{u_n(1)\}_{n\geqslant 0}$ is just the Fibonacci sequence $\{F_n\}_{n\geqslant 0}$. By [12, Corollary 2(iii)], if $p\equiv 3 \pmod 4$ and $(\frac{5}{p})=1$, then

$$u_{(p-1)/2}(1)=F_{(p-1)/2}\equiv -2(-1)^{\lfloor (p-5)/10\rfloor}5^{(p-3)/4} \pmod p$$

and hence

$$-5^{(p+1)/4}\frac{u_{(p-1)/2}(1)}{2}\equiv(-1)^{\lfloor (p-5)/10\rfloor}5^{(p+1)/4+(p-3)/4}\equiv(-1)^{\lfloor (p-5)/10\rfloor} \pmod p.$$

Similarly, if $p\equiv 3 \pmod 4$ and $(\frac{5}{p})=-1$, then

$$u_{(p+1)/2}(1)=F_{(p+1)/2}\equiv 2(-1)^{\lfloor (p-5)/10\rfloor}5^{(p-3)/4} \pmod p$$

and hence

$$5^{(p+1)/4}\frac{u_{(p+1)/2}(1)}{2}\equiv(-1)^{\lfloor (p-5)/10\rfloor}5^{(p+1)/4+(p-3)/4}\equiv(-1)^{\lfloor (p+5)/10\rfloor} \pmod p.$$

Therefore Theorem 1.4 with $A=1$ yields (1.17).

When $p\equiv 1 \pmod 4$, we obviously have

$$8^{(p-1)/4}=2^{(p-1)/2+(p-1)/4}\equiv\left(\frac{2}{p}\right)2^{(p-1)/4}=(-2)^{(p-1)/4} \pmod p.$$

If $p\equiv 7\ (\mathrm{mod}\ 8)$, then

$$u_{(p-1)/2}(2)\equiv(-1)^{(p+1)/8}2^{(p-3)/4}\ (\mathrm{mod}\ p)$$

by [11, (1.7)], and hence

$$-8^{(p+1)/4}\frac{u_{(p-1)/2}(2)}{2}\equiv-\,2^{(3p+3)/4}(-1)^{(p+1)/8}2^{(p-7)/4}\equiv(-1)^{(p-7)/8}\ (\mathrm{mod}\ p).$$

Similarly, if $p\equiv 3\ (\mathrm{mod}\ 8)$, then

$$u_{(p+1)/2}(2)\equiv(-1)^{(p+5)/8}2^{(p-3)/4}\ (\mathrm{mod}\ p)$$

by [11, (1.7)], and hence

$$(-8)^{(p+1)/4}\frac{u_{(p+1)/2}(2)}{2}\equiv-\,2^{(3p+3)/4}(-1)^{(p+5)/8}2^{(p-7)/4}\equiv(-1)^{(p-3)/8}\ (\mathrm{mod}\ p).$$

So Theorem 1.4 with $A=2$ yields (1.18). This ends the proof. □

6. Proofs of Theorems 1.6 and 1.7

For $n=1,2,3,\ldots$, we adopt the notation

$$n!!:=\prod_{k=0}^{\lfloor (n-1)/2\rfloor}(n-2k).$$

Lemma 6.1. *Let $p>3$ be a prime. Then*

$$\frac{p-1}{2}!!\prod_{\substack{i,j=1\\ p\nmid 2i+j}}^{(p-1)/2}(2i+j)\equiv\left(\frac{-2}{p}\right)\frac{p-3}{2}!!\prod_{\substack{i,j=1\\ p\nmid 2i-j}}^{(p-1)/2}(2i-j)\equiv\pm1\ (\mathrm{mod}\ p).\tag{6.1}$$

Proof. Set

$$A_p:=\frac{p-1}{2}!!\prod_{\substack{i,j=1\\ p\nmid 2i+j}}^{(p-1)/2}(2i+j)\quad\text{and}\quad B_p:=\frac{p-3}{2}!!\prod_{\substack{i,j=1\\ p\nmid 2i-j}}^{(p-1)/2}(2i-j).$$

Then

$$\begin{aligned}\frac{A_pB_p}{((p-1)/2)!}&\equiv\prod_{\substack{i,j=1\\ p\nmid 2i+j}}^{(p-1)/2}(2i+j)\times\prod_{\substack{i,j=1\\ p\nmid 2i+p-j}}^{(p-1)/2}(2i+p-j)=\prod_{i=1}^{(p-1)/2}\Bigg(\frac{1}{2i}\prod_{\substack{j=0\\ p\nmid 2i+j}}^{p-1}(2i+j)\Bigg)\\&\equiv\prod_{i=1}^{(p-1)/2}\frac{(p-1)!}{2i}\equiv\frac{(\frac{-2}{p})}{((p-1)/2)!}\ (\mathrm{mod}\ p)\end{aligned}$$

and hence

$$A_pB_p\equiv\left(\frac{-2}{p}\right)\ (\mathrm{mod}\ p).\tag{6.2}$$

On the other hand,

$$\begin{aligned}\frac{B_p}{((p-3)/2)!!} =& \prod_{\substack{i,j=1\\ p\nmid 2(\frac{p+1}{2}-i)-j}}^{(p-1)/2} \left(2\left(\frac{p+1}{2}-i\right)-j\right)\\ \equiv& \prod_{\substack{i,j=1\\ p\nmid 2i+j-1}}^{(p-1)/2}(1-j-2i) = \prod_{i=1}^{(p-1)/2}\frac{-2i}{(-(p-1)/2-2i)^*}\prod_{\substack{j=1\\ p\nmid j+2i}}^{(p-1)/2}(-j-2i)\\ \equiv& \frac{(-2)^{(p-1)/2}((p-1)/2)!}{\prod_{\substack{1\leqslant i<p/2\\ 4i\neq p+1}}((p+1)/2-2i)}\prod_{\substack{i,j=1\\ p\nmid 2i+j}}^{(p-1)/2}(2i+j)\\ &\times(-1)^{\sum_{i=1}^{(p-1)/2}((p-1)/2-|\{1\leqslant j\leqslant (p-1)/2:\ p\mid 2i+j\}|)} \pmod p,\end{aligned}$$

where k^* is 1 or k according as $p\mid k$ or not. Note that

$$\prod_{1\leqslant i<p/4}\left(\frac{p+1}{2}-2i\right)=\frac{p-3}{2}!!.$$

Therefore

$$\begin{aligned}\left(\frac{-2}{p}\right)\frac{B_p}{A_p} \equiv& \frac{((p-1)/2)!}{((p-1)/2)!!}\times\prod_{(p+1)/4<i<p/2}\frac{1}{((p+1)/2-2i)}\\ &\times(-1)^{((p-1)/2)^2-|\{1\leqslant i\leqslant (p-1)/2:\ 2i>p/2\}|}\\ \equiv& \frac{((p-3)/2)!!(-1)^{((p-1)/2)^2-((p-1)/2-\lfloor (p-1)/4\rfloor)}}{(-1)^{\lfloor (p-1)/4\rfloor}\prod_{(p+1)/4<i<p/2}(2i-(p+1)/2)} = 1 \pmod p,\end{aligned}$$

and hence

$$A_p\equiv\left(\frac{-2}{p}\right)B_p \pmod p \tag{6.3}$$

which gives the first congruence in (6.1).

Combining (6.2) and (6.3), we see that $A_p^2\equiv B_p^2\equiv 1 \pmod p$. So (6.1) does hold. This ends the proof. □

Proof of Theorem 1.6. As $2i^2+\delta 5ij+2j^2=(i+\delta 2j)(2i+\delta j)$, we have

$$\begin{aligned}\prod_{\substack{i,j=1\\ p\nmid 2i^2+\delta 5ij+2j^2}}^{(p-1)/2}(2i^2+\delta 5ij+2j^2) =& \prod_{\substack{i,j=1\\ p\nmid (i+\delta 2j)(2i+\delta j)}}^{(p-1)/2}(i+\delta 2j)\times\prod_{\substack{i,j=1\\ p\nmid (i+\delta 2j)(2i+\delta j)}}^{(p-1)/2}(2i+\delta j)\\ =& \prod_{\substack{i,j=1\\ p\nmid (i+\delta 2j)(2i+\delta j)}}^{(p-1)/2}(i+\delta 2j)\times\prod_{\substack{i,j=1\\ p\nmid (i+\delta 2j)(2i+\delta j)}}^{(p-1)/2}(2j+\delta i)\\ =& \prod_{\substack{i,j=1\\ p\nmid i+\delta 2j}}^{(p-1)/2}\delta(i+\delta 2j)^2\times\prod_{\substack{i,j=1\\ p\mid j+\delta 2i}}^{(p-1)/2}\frac{1}{\delta(i+\delta 2j)^2}.\end{aligned}$$

(Note that $i+\delta 2j\equiv j+\delta 2i\equiv 0\pmod p$ for no $i,j=1,\ldots,(p-1)/2$.) Thus, applying Lemma 6.1 and (3.1) we get

$$\begin{aligned}&\prod_{\substack{i,j=1\\ p\nmid 2i^2+\delta 5ij+2j^2}}^{(p-1)/2}(2i^2+\delta 5ij+2j^2)\\ \equiv&\frac{\delta^{|(i,j):\ 1\leqslant i,j\leqslant(p-1)/2\ \&\ p\nmid i+\delta 2j\}|}}{((p-2+\delta)/2)!!^2}\times\prod_{\substack{i=1\\ \{\delta 2i\}_p>p/2}}^{(p-1)/2}\frac{1}{\delta(i+\delta 2(p-2\delta i))^2}\\ \equiv&\frac{\delta^{((p-1)/2)^2-|\{1\leqslant j\leqslant(p-1)/2:\ \{\delta 2j\}_p>p/2\}|}}{((p-2+\delta)/2)!!^2}\times\prod_{\substack{i=1\\ \{\delta 2i\}_p>p/2}}^{(p-1)/2}\frac{1}{\delta(i-4i)^2}\\ \equiv&\frac{\delta^{(p-1)^2/4}}{((p-2+\delta)/2)!!^2}\times\prod_{i=1}^{(p-1)/2}(3i)^{-1-\delta}\times\prod_{i=1}^{\lfloor p/4\rfloor}(3i)^{2\delta}\\ \equiv&\frac{\delta^{(p-1)^2/4}}{((p-2+\delta)/2)!!^2}\times\frac{3^{2\delta\lfloor p/4\rfloor}\lfloor p/4\rfloor!^{2\delta}}{((p-1)/2)!^{1+\delta}}\\ \equiv&\delta^{(p-1)^2/4}(-1)^{\frac{p+1}{2}\cdot\frac{1+\delta}{2}}3^{2\delta\lfloor p/4\rfloor}\left(\frac{\lfloor p/4\rfloor!^{\delta}}{((p-2+\delta)/2)!!}\right)^2\\ =&(-1)^{(p+\delta)/2}3^{2\delta\lfloor p/4\rfloor}\left(\frac{\lfloor p/4\rfloor!^{\delta}}{((p-2+\delta)/2)!!}\right)^2\pmod p.\end{aligned}$$

Case 1. $p\equiv 1\pmod 4$.

In this case,

$$\left(\frac{\lfloor p/4\rfloor!^{\delta}}{((p-2+\delta)/2)!!}\right)^2=\begin{cases}1/2^{(p-1)/2} & \text{if } \delta=1,\\ 2^{(p-1)/2}/((p-1)/2)!^2 & \text{if } \delta=-1.\end{cases}$$

Thus, with the help of (3.1) we have

$$\begin{aligned}&(-1)^{(p+\delta)/2}3^{2\delta\lfloor p/4\rfloor}\left(\frac{\lfloor p/4\rfloor!^{\delta}}{((p-2+\delta)/2)!!}\right)^2\\ \equiv&(-1)^{(1+\delta)/2}\left(\frac{3}{p}\right)^{\delta}\left(\frac{2}{p}\right)^{-\delta}\delta=-\left(\frac{6}{p}\right)=(-1)^{\lfloor(p+11)/12\rfloor}\pmod p,\end{aligned}$$

and hence (1.19) follows from the above.

Case 2. $p\equiv 3\pmod 4$.

In this case, with the aid of (3.1) we have

$$\begin{aligned}&(-1)^{(p+\delta)/2}3^{2\delta\lfloor p/4\rfloor}\left(\frac{\lfloor p/4\rfloor!^{\delta}}{((p-2+\delta)/2)!!}\right)^2\\ \equiv&(-1)^{(\delta-1)/2}3^{\delta((p-1)/2-1)}\left(\frac{2^{(p-3)/4}}{(p-1)/2\times\binom{(p-3)/2}{(p-3)/4}}\right)^{2\delta}\left(\frac{p-1}{2}!\right)^{\delta-1}\\ \equiv&\delta\left(\frac{3}{p}\right)3^{-\delta}2^{\delta(p+1)/2}\binom{(p-3)/2}{(p-3)/4}^{-2\delta}\equiv\left(\frac{6}{p}\right)\frac{\delta 2^{\delta}}{3^{\delta}}\binom{(p-3)/2}{(p-3)/4}^{-2\delta}\pmod p,\end{aligned}$$

and hence (1.20) holds.

In view of the above, we have completed the proof. □

Proof of Theorem 1.7. Let $n=(p-1)/2$. Clearly,

$$\prod_{1\leqslant i<j\leqslant n}(j-i)=\prod_{k=1}^{n}k^{|\{1\leqslant i\leqslant n:\ i+k\leqslant n\}|}=\prod_{k=1}^{n}k^{n-k}$$

and hence

$$\prod_{1\leqslant i<j\leqslant n}\left(\frac{j-i}{p}\right)=\left(\frac{n!}{p}\right)^{n}\prod_{\substack{k=1\\ 2\nmid k}}^{n}\left(\frac{k}{p}\right). \tag{6.4}$$

Case 1. $p\equiv 1\pmod 4$.

In this case, n is even, and hence by (6.4) and [15, (3.5)] we have

$$\prod_{1\leqslant i<j\leqslant n}\left(\frac{j-i}{p}\right)=\left(\frac{(n-1)!!}{p}\right)=(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}.$$

By (3.2) and [14, Lemma 2.3],

$$\prod_{1\leqslant i<j\leqslant n}\left(\frac{j^2-i^2}{p}\right)=\left(\frac{-n!}{p}\right)=\left(\frac{2}{p}\right)=(-1)^{(p-1)/4}.$$

Thus we also have

$$\prod_{1\leqslant i<j\leqslant n}\left(\frac{j+i}{p}\right)=(-1)^{(p-1)/4}(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}=(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}.$$

So (1.21) holds in this case.

Case 2. $p\equiv 3\pmod 4$.

In this case, n is odd and

$$\prod_{1\leqslant i<j\leqslant n}\left(\frac{j^2-i^2}{p}\right)=\left(\frac{1}{p}\right)=1$$

by (3.2). So it suffices to prove (1.21) for $\delta=-1$.

In view of (6.4), we have

$$\prod_{1\leqslant i<j\leqslant n}\left(\frac{j-i}{p}\right)=\left(\frac{n!}{p}\right)\left(\frac{n!!}{p}\right)=\left(\frac{(n-1)!!}{p}\right). \tag{6.5}$$

If $p\equiv 3\pmod 8$, then by [15, (3.6)] we have

$$\left(\frac{(n-1)!!}{p}\right)=(-1)^{\lfloor (p+1)/8\rfloor}=(-1)^{(p-3)/8}$$

and hence (1.21) holds for $\delta=-1$. When $p\equiv 7\pmod 8$, we have

$$\left(\frac{n!}{p}\right)=\left(\frac{(-1)^{(h(-p)+1)/2}}{p}\right)=(-1)^{(h(-p)+1)/2}\ \text{and}\ \left(\frac{n!!}{p}\right)=(-1)^{(p+1)/8}$$

by Mordell [8] and Sun [15, (3.6)] respectively, hence (1.21) with $\delta=-1$ follows from (6.5).

Combining the above, we have finished the proof of (1.21). □

7. Some related conjectures

Motivated by our results in Section 1, here we pose 10 conjectures for further research. We have verified all the following conjectures for primes $p < 13000$.

Conjecture 7.1. *Let $p > 3$ be a prime and let $\delta \in \{\pm 1\}$. Then*

$$\prod_{\substack{1 \leqslant i < j \leqslant (p-1)/2 \\ p \nmid 2i^2 + \delta 5ij + 2j^2}} \left(\frac{2i^2 + \delta 5ij + 2j^2}{p}\right) = \frac{1}{2}\left(\frac{\delta}{p}\right)\left(\left(\frac{-1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{6}{p}\right) - \left(\frac{p}{3}\right)\right). \tag{7.1}$$

Conjecture 7.2. *Let $p > 3$ be a prime. Then*

$$\prod_{\substack{1 \leqslant i < j \leqslant (p-1)/2 \\ p \nmid i^2 - ij + j^2}} \left(\frac{i^2 - ij + j^2}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 5, 7 \pmod{24}, \\ 1 & \text{otherwise.} \end{cases} \tag{7.2}$$

Also,

$$\prod_{\substack{1 \leqslant i < j \leqslant (p-1)/2 \\ p \nmid i^2 + ij + j^2}} \left(\frac{i^2 + ij + j^2}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 5, 11 \pmod{24}, \\ 1 & \text{otherwise.} \end{cases} \tag{7.3}$$

Conjecture 7.3. *Let $p > 3$ be a prime. Then*

$$\prod_{\substack{1 \leqslant i < j \leqslant (p-1)/2 \\ p \nmid i^2 - 3ij + j^2}} \left(\frac{i^2 - 3ij + j^2}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 7, 19 \pmod{20}, \\ 1 & \text{otherwise.} \end{cases} \tag{7.4}$$

Also,

$$\prod_{\substack{1 \leqslant i < j \leqslant (p-1)/2 \\ p \nmid i^2 + 3ij + j^2}} \left(\frac{i^2 + 3ij + j^2}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 19, 23, 27, 31 \pmod{40}, \\ 1 & \text{otherwise.} \end{cases} \tag{7.5}$$

Recall that for any prime $p \equiv 3 \pmod 4$ the class number $h(-p)$ of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ is odd by [8].

Conjecture 7.4. *Let $\delta \in \{\pm 1\}$.*

(i) *For any prime $p \equiv 1 \pmod{12}$, we have*

$$T_p(1, 4\delta, 1) \equiv -3^{(p-1)/4} \pmod p. \tag{7.6}$$

(ii) *Let $p > 3$ be a prime. Then*

$$\prod_{\substack{1 \leqslant i < j \leqslant (p-1)/2 \\ p \nmid i^2 + \delta 4ij + j^2}} \left(\frac{i^2 + \delta 4ij + j^2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{24}, \\ (-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|} & \text{if } p \equiv 17 \pmod{24}, \\ \delta(-1)^{|\{0<k<\frac{p}{12}:\ (\frac{k}{p})=-1\}|-1} & \text{if } p \equiv 7 \pmod{24}, \\ \delta(-1)^{|\{0<k<\frac{p}{12}:\ (\frac{k}{p})=-1\}|+\frac{h(-p)-1}{2}} & \text{if } p \equiv 19 \pmod{24}. \end{cases} \tag{7.7}$$

Conjecture 7.5. *Let $p > 3$ be a prime. Then*

$$\prod_{\substack{1 \leqslant i \leqslant j \leqslant (p-1)/2 \\ p \nmid 4i^2 + j^2}} \left(\frac{4i^2 + j^2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7, 9, 19 \pmod{20}, \\ -1 & \text{otherwise.} \end{cases}$$

Conjecture 7.6. *Let $p>3$ be a prime. Then*

$$(-1)^{|\{1\leqslant k<p/3:\ (\frac{k}{p})=-1\}|}\prod_{\substack{i,j=1\\ p\nmid 3i+j}}^{(p-1)/2}\left(\frac{3i+j}{p}\right)=\begin{cases}1 & \text{if } p\equiv\pm1 \pmod{12},\\ (-1)^{\lfloor p/12\rfloor} & \text{if } p\equiv\pm5 \pmod{12},\end{cases}$$

and

$$\prod_{\substack{i,j=1\\ p\nmid 3i-j}}^{(p-1)/2}\left(\frac{3i-j}{p}\right)=\begin{cases}(-1)^{|\{1\leqslant k<p/3:\ (\frac{k}{p})=-1\}|+(p-1)/12} & \text{if } p\equiv1 \pmod{12},\\ (-1)^{|\{1\leqslant k<p/3:\ (\frac{k}{p})=-1\}|-1} & \text{if } p\equiv5 \pmod{12},\\ (-1)^{|\{1\leqslant k<p/6:\ (\frac{k}{p})=1\}|+(p+1)/4} & \text{if } p\equiv7 \pmod{12},\\ -1 & \text{if } p\equiv11 \pmod{12}.\end{cases}.$$

Conjecture 7.7. *Let $p>3$ be a prime. Then*

$$\prod_{\substack{i,j=1\\ p\nmid 4i+j}}^{(p-1)/2}\left(\frac{4i+j}{p}\right)=\begin{cases}1 & \text{if } p\equiv1 \pmod{4},\\ (-1)^{(h(-p)-1)/2+\lfloor p/8\rfloor} & \text{if } p\equiv3 \pmod{8},\\ (-1)^{|\{1\leqslant k<p/4:\ (\frac{k}{p})=-1\}|} & \text{if } p\equiv7 \pmod{8},\end{cases}$$

and

$$\prod_{\substack{i,j=1\\ p\nmid 4i-j}}^{(p-1)/2}\left(\frac{4i-j}{p}\right)=\begin{cases}(-1)^{(p-1)/4} & \text{if } p\equiv1 \pmod{4},\\ (-1)^{\lfloor p/8\rfloor} & \text{if } p\equiv3 \pmod{4}.\end{cases}$$

Conjecture 7.8. *Let $p>5$ be a prime. Then*

$$(-1)^{|\{1\leqslant k<p/10:\ (\frac{k}{p})=-1\}|}\prod_{\substack{i,j=1\\ p\nmid 5i+j}}^{(p-1)/2}\left(\frac{5i+j}{p}\right)$$
$$=\begin{cases}(-1)^{\lfloor (p+1)/10\rfloor} & \text{if } p\equiv\pm1,\pm3 \pmod{20},\\ (-1)^{\lfloor p/20\rfloor} & \text{if } p\equiv\pm7 \pmod{20},\\ (-1)^{\lfloor (p+9)/20\rfloor} & \text{if } p\equiv\pm9 \pmod{20},\end{cases}$$

and

$$\prod_{\substack{i,j=1\\ p\nmid 5i-j}}^{(p-1)/2}\left(\frac{5i-j}{p}\right)=\begin{cases}(-1)^{(h(-p)+1)/2} & \text{if } p\equiv3,7 \pmod{20},\\ (-1)^{(p+9)/20} & \text{if } p\equiv-9 \pmod{20},\\ (-1)^{|\{1\leqslant k<p/10:\ (\frac{k}{p})=-1\}|+(h(-p)-1)/2} & \text{if } p\equiv-1 \pmod{20},\\ (-1)^{|\{1\leqslant k<p/10:\ (\frac{k}{p})=-1\}|+\lfloor (p+3)/20\rfloor} & \text{if } p\equiv1,-3 \pmod{20},\\ (-1)^{|\{1\leqslant k<p/10:\ (\frac{k}{p})=-1\}|+\lfloor (p-3)/10\rfloor} & \text{if } p\equiv-7,9 \pmod{20}.\end{cases}$$

Conjecture 7.9. *For any prime $p>3$, we have*

$$\prod_{\substack{i,j=1\\ p\nmid 6i+j}}^{(p-1)/2}\left(\frac{6i+j}{p}\right)=\begin{cases}(-1)^{|\{1\leqslant k<p/12:\ (\frac{k}{p})=-1\}|} & \text{if } p\equiv1 \pmod{24},\\ (-1)^{|\{\frac{p+3}{4}\leqslant k\leqslant\lfloor\frac{p+1}{3}\rfloor:\ (\frac{k}{p})=-1\}|} & \text{if } p\equiv5,-7,-11 \pmod{24},\\ (-1)^{(h(-p)+1)/2+\lfloor (p+1)/24\rfloor} & \text{if } p\equiv-1,-5 \pmod{24},\\ (-1)^{\lfloor p/24\rfloor-1} & \text{if } p\equiv7,11 \pmod{24},\end{cases}$$

and

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

Conjecture 7.10. *Let $p>3$ be a prime. Then*

$$(-1)^{|\{1\leqslant k<p/4:\ (\frac{k}{p})=-1\}|}\prod_{\substack{i,j=1\\ p\nmid 8i+j}}^{(p-1)/2}\left(\frac{8i+j}{p}\right)=\begin{cases}(-1)^{(p+1)/8} & \textit{if } p\equiv -1 \pmod 8,\\ 1 & \textit{otherwise},\end{cases}$$

and

$$\prod_{\substack{i,j=1\\ p\nmid 8i-j}}^{(p-1)/2}\left(\frac{8i-j}{p}\right)=\begin{cases}(-1)^{|\{1\leqslant k<p/4:\ (\frac{k}{p})=1\}|} & \textit{if } p\equiv 1 \pmod 4,\\ (-1)^{(h(-p)+1)/2+(p-3)/8} & \textit{if } p\equiv 3 \pmod 8,\\ -1 & \textit{if } p\equiv 7 \pmod 8.\end{cases}$$

Acknowledgments. The research is supported by the Natural Science Foundation of China (Grant No. 11971222). The author would like to thank the the referee for helpful comments.

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, John Wiley & Sons, 1998.

[2] K. Burde, Eine Verteilungseigenschaft der Legendresymbole, *J. Number Theory* **12** (1980), 273–277.

[3] S. Chowla, B. Dwork and R. J. Evans, On the mod p^2 determination of $\binom{(p-1)/2}{(p-1)/4}$, *J. Number Theory* **24** (1986), 188–196.

[4] L. E. Dickson, *History of the Theory of Numbers*, Vol. III, AMS Chelsea Publ., 1999.

[5] R. H. Hudson and K. S. Williams, Class number formulae of Dirichlet type, *Math. Comp.* **39** (1982), 725–732.

[6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd Edition, Graduate Texts in Math., 84, Springer, New York, 1990.

[7] M. Jenkins, Proof of an Arithmetical Theorem leading, by means of Gauss fourth demonstration of Legendres law of reciprocity, to the extension of that law, *Proc. London Math. Soc.* **2** (1867) 29–32.

[8] L. J. Mordell, The congruence $((p-1)/2)!\equiv\pm1 \pmod{p}$, *Amer. Math. Monthly* **68** (1961) 145–146.

[9] H. Rademacher, *Lectures on Elementary Number Theory*, Blaisdell Publishing Company, New York, 1964.

[10] P. Ribenboim, *The Book of Prime Number Records*, Springer, New York, 1980.

[11] Z.-H. Sun, Values of Lucas sequences modulo primes, *Rocky Mountain J. Math.* **33** (2013) 1123–1145.

[12] Z.-H. Sun and Z.-W. Sun, Fibonacci numbers and Fermat's last theorem, *Acta Arith.* **60** (1992) 371–388.

[13] Z.-W. Sun, Binomial coefficients, Catalan numbers and Lucas quotients, *Sci. China Math.* **53** (2010) 2473–3488.

[14] Z.-W. Sun, On some determinants with Legendre symbol entries, *Finite Fields Appl.* **56** (2019) 285–307.

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

[16] K. S. Williams, On the quadratic residues (mod p) in the interval $(0,p/4)$, *Canad. Math. Bull.* **26** (1983) 123–124.

[17] K. S. Williams and J. D. Currie, Class numbers and biquadratic reciprocity, *Canad. J. Math.* **34** (1982) 969–988.

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: zwsun@nju.edu.cn