Preprint, arXiv:1809.07766

QUADRATIC RESIDUES AND RELATED PERMUTATIONS AND IDENTITIES

Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

Abstract. Let p be an odd prime. In this paper we investigate quadratic residues modulo p and related permutations. For $k=1,\ldots,(p-1)/2$ let $\tau_p(k)$ be the unique integer $k^*\in\{1,\ldots,(p-1)/2$ such that kk^* is congruent to 1 or -1 modulo p. Then τ_p is a permutation on $\{1,\ldots,(p-1)/2\}$ and we show that its sign is $-(\frac{2}{p})$ with $(\frac{\cdot}{p})$ the Legendre symbol. If $a_1<\ldots<a_{(p-1)/2}$ are all the quadratic residues modulo p among $1,\ldots,p-1$, then the list $\{1^2\}_p,\ldots,\{((p-1)/2)^2\}_p$ (with $\{k\}_p$ the least nonnegative residue of k modulo p) is a permutation of $a_1,\ldots,a_{(p-1)/2}$ and we determine its sign in the case $p\equiv 3 \pmod 4$ by evaluating the product $\prod_{1\leqslant j<k\leqslant(p-1)/2}(\cot\pi j^2/p-\cot\pi k^2/p)$ via Dirichlet's class number formula and Galois theory. We also obtain some new identities for the sine and cosine functions; for example, we prove that

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

for any $a\in\mathbb{Z}$ not divisible by p.

1. Introduction

Let p be an odd prime. For any integer a we let $\{a\}_p$ denote the least nonnegative residue of a modulo p. Clearly, if $p\nmid a$ then $\pi_a(k)=\{ak\}_p$ with $1\leqslant k\leqslant p-1$ is a permutation on $\{1,\ldots,p-1\}$. Zolotarev's lemma (cf. [DH] and [Z]) asserts that $\mathrm{sign}(\pi_a)$ (the sign of the permutation π_a) coincides with the Legendre symbol $(\frac{a}{p})$.

Frobenius (cf. [BC]) extended Zolotarev's lemma as follows: If $a\in\mathbb{Z}$ is relatively prime to a positive odd integer n, then the sign of the permutation $\pi_a(k)=\{ak\}_n$ $(0\leqslant k\leqslant n-1)$ on $\{0,\ldots,n-1\}$ equals the Jacobi symbol $(\frac{a}{n})$.

2010 *Mathematics Subject Classification.* Primary 11A15, 11R18; Secondary 05A05, 11A07, 11C20, 11R32, 11T24, 33B10.

Keywords. Congruences modulo primes, permutations, quadratic residues, Galois theory.

Supported by the National Natural Science Foundation of China (grant no. 11571162) and the NSFC-RFBR Cooperation and Exchange Program (grant no. 11811530072).

Let $n>1$ be an odd integer and let a be any integer relatively prime to n. For each $k=1,\ldots,(n-1)/2$ let $\pi_a^*(k)$ be the unique $r\in\{1,\ldots,(n-1)/2\}$ with ak congruent to r or $-r$ modulo n. For the permutation π_a^* on $\{1,\ldots,(n-1)/2\}$, Pan [P06] showed that its sign is given by

$$\operatorname{sign}(\pi_a^*)=\left(\frac{a}{n}\right)^{(n+1)/2}.$$

Let $m>1$ be an odd integer, and let $a_1<\ldots<a_{\varphi(m)}$ be all the numbers among $1,\ldots,m-1$ relatively prime to m. For each $k\in\{1,\ldots,m-1\}$ with $\gcd(k,m)=1$, let $\sigma_m(k)=\bar{k}$ be the inverse of k modulo m, that is, $\bar{k}\in\{1,\ldots,m-1\}$ and $k\bar{k}\equiv 1 \pmod m$. For $k=1,\ldots,(m-1)/2$ with $\gcd(k,m)=1$, let $\tau_m(k)$ be the unique integer $k^*\in\{1,\ldots,(m-1)/2\}$ such that kk^* is congruent to 1 or -1 modulo m. Clearly, σ_m is a permutation of $a_1,\ldots,a_{\varphi(m)}$, and τ_m is the permutation of $a_1,\ldots,a_{\varphi(m)/2}$. Our first theorem determines $\operatorname{sign}(\sigma_m)$ and $\operatorname{sign}(\tau_m)$.

Theorem 1.1. *Suppose that $m=\prod_{s=1}^r p_s^{a_s}$, where $p_1,\ldots,p_r$ are distinct odd primes and $a_1,\ldots,a_r$ are positive integers. Then we have*

$$\operatorname{sign}(\sigma_m)=-1 \iff m \text{ is prime and } m\equiv 1 \pmod 4. \tag{1.1}$$

Also, $\operatorname{sign}(\tau_m)=-1$ *if and only if* $r=1$ & ($p_1\equiv 1$ *or* $4a_1+3 \pmod 8$)*, or* $r=2$ & $p_1+p_2\equiv 0 \pmod 4$. *In particular, when m is an odd prime we have*

$$\operatorname{sign}(\sigma_m)=-\left(\frac{-1}{m}\right) \quad \text{and} \quad \operatorname{sign}(\tau_m)=-\left(\frac{2}{m}\right). \tag{1.2}$$

Let p be an odd prime. By Wilson's theorem,

$$(-1)^{(p-1)/2}\left(\frac{p-1}{2}!\right)^2=\prod_{k=1}^{(p-1)/2}k(p-k)=(p-1)!\equiv -1 \pmod p. \tag{1.3}$$

Write $p=2n+1$ and let $a_1,\ldots,a_n$ be the list of all the n quadratic residues among $1,\ldots,p-1$ in the ascending order. It is well known that the list

$$\{1^2\}_p,\ldots,\{n^2\}_p$$

is a permutation of $a_1,\ldots,a_n$. Clearly, the sign of this permutation is just the sign of the product

$$S_p:=\prod_{1\leqslant i<j\leqslant (p-1)/2}(\{j^2\}_p-\{i^2\}_p). \tag{1.4}$$

It is easy to determine this product modulo p. In fact,

$$\prod_{1\leqslant i<j\leqslant n}(j^2-i^2)\equiv\begin{cases}-n!\pmod p & \text{if } p\equiv 1\pmod 4,\\ 1\pmod p & \text{if } p\equiv 3\pmod 4,\end{cases}\tag{1.5}$$

since

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

and $(n!)^2\equiv(-1)^{n+1}\pmod p$ by (1.3). It is known (cf. Problem N.2 of [Sz, pp. 364-365]) that

$$\prod_{1\leqslant i<j\leqslant (p-1)/2}(i^2+j^2)\equiv(-1)^{\lfloor (p+1)/8\rfloor}\pmod p\tag{1.6}$$

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

Inspired by (1.5) and (1.6), we obtain the following general result.

Theorem 1.2. *Let p be an odd prime.*

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

$$\prod_{\substack{1\leqslant i<j\leqslant (p-1)/2\\ p\nmid i^2+j^2}}(i^2+j^2)\equiv(-1)^{\lfloor (p-5)/8\rfloor}\pmod p.\tag{1.7}$$

(ii) *Let $a,b,c\in\mathbb{Z}$ with $ac(a+b+c)\not\equiv 0\pmod p$, and set $\Delta=b^2-4ac$. Then*

$$\prod_{\substack{1\leqslant i<j\leqslant p-1\\ p\nmid ai^2+bij+cj^2}}(ai^2+bij+cj^2)\equiv\begin{cases}(\frac{a(a+b+c)}{p})\pmod p & \text{if } p\mid\Delta,\\ -(\frac{ac(a+b+c)\Delta}{p})\pmod p & \text{if } p\nmid\Delta.\end{cases}\tag{1.8}$$

If $a+c=0$, then

$$\begin{aligned}&\prod_{\substack{i,j=1\\ p\nmid ai^2+bij+cj^2}}^{(p-1)/2}(ai^2+bij+cj^2)\\ \equiv&\begin{cases}\pm\frac{p-1}{2}!\pmod p & \text{if } (\frac{\Delta}{p})=-1 \text{ or } (p\mid\Delta\ \&\ (\frac{2b}{p})=1),\\ \pm 1\pmod p & \text{if } (\frac{\Delta}{p})=1 \text{ or } (p\mid\Delta\ \&\ (\frac{2b}{p})=-1).\end{cases}\end{aligned}\tag{1.9}$$

To determine the sign of S_p for an arbitrary prime $p\equiv 3\pmod 4$, we need to establish the following theorem via Dirichlet's class number formula and Galois theory.

Theorem 1.3. *Let $p>3$ be a prime and let $\zeta=e^{2\pi i/p}$. Let a be any integer not divisible by p.*

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

$$\prod_{k=1}^{(p-1)/2}(1-\zeta^{ak^2})=\sqrt{p}\,\varepsilon_p^{-(\frac{a}{p})h(p)},\tag{1.10}$$

where ε_p and $h(p)$ are the fundamental unit and the class number of the real quadratic field $\mathbb{Q}(\sqrt{p})$ respectively. If $p\equiv 3\pmod 4$, then

$$\prod_{k=1}^{(p-1)/2}(1-\zeta^{ak^2})=(-1)^{(h(-p)+1)/2}\left(\frac{a}{p}\right)\sqrt{p}\,i.\tag{1.11}$$

(ii) *When $p\equiv 1\pmod 4$, we have*

$$\prod_{1\leqslant j<k\leqslant (p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})^2=(-1)^{(p-1)/4}p^{(p-3)/4}\varepsilon_p^{(\frac{a}{p})h(p)}.\tag{1.12}$$

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

$$\begin{aligned}&\prod_{1\leqslant j<k\leqslant (p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})\\ =&\begin{cases}(-p)^{(p-3)/8} & \text{if } p\equiv 3\pmod 8,\\ (-1)^{(p+1)/8+(h(-p)-1)/2}(\frac{a}{p})p^{(p-3)/8}i & \text{if } p\equiv 7\pmod 8,\end{cases}\end{aligned}\tag{1.13}$$

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

Remark 1.1. For any prime $p\equiv 3\pmod 4$, it is known that $2\nmid h(-p)$; moreover, L. J. Mordell [M61] proved that $\frac{p-1}{2}!\equiv(-1)^{(h(-p)+1)/2}\pmod p$ if $p>3$. Our proof of (1.13) utilizes the congruence (1.5).

Since

$$\sin\pi\theta=\frac{i}{2}e^{-i\pi\theta}(1-e^{2\pi i\theta})\quad\text{and}\quad 2\cos\pi\theta\times\sin\pi\theta=\sin 2\pi\theta,$$

we can easily deduce the following corollary from Theorem 1.3(i).

Corollary 1.1. *Let $p>3$ be a prime and let $a\in\mathbb{Z}$ with $p\nmid a$. Then*

$$\begin{aligned}&2^{(p-1)/2}\prod_{k=1}^{(p-1)/2}\sin\pi\frac{ak^2}{p}\\ =&(-1)^{(a+1)\lfloor (p+1)/4\rfloor}\sqrt{p}\times\begin{cases}\varepsilon_p^{-(\frac{a}{p})h(p)} & \text{if } p\equiv 1\pmod 4,\\ (-1)^{(h(-p)+1)/2}(\frac{a}{p}) & \text{if } p\equiv 3\pmod 4,\end{cases}\end{aligned}\tag{1.14}$$

and

$$2^{(p-1)/2}\prod_{k=1}^{(p-1)/2}\cos\pi\frac{ak^2}{p}=\begin{cases}\varepsilon_p^{(1-(\frac{2}{p}))(\frac{a}{p})h(p)} & \text{if } p\equiv 1 \pmod 4,\\ (-1)^{(p+1)/4} & \text{if } p\equiv 3 \pmod 4.\end{cases}\tag{1.15}$$

For any odd prime p, we define

$$s(p):=\left|\left\{(j,k):\ 1\leqslant j<k\leqslant\frac{p-1}{2}\text{ and }\{j^2\}_p>\{k^2\}_p\right\}\right|\tag{1.16}$$

and

$$t(p):=\left|\left\{(j,k):\ 1\leqslant j<k\leqslant\frac{p-1}{2}\text{ and }\{k^2-j^2\}_p>\frac{p}{2}\right\}\right|.\tag{1.17}$$

For example, $s(11)=t(11)=4$ since $(\{1^2\}_{11},\ldots,\{5^2\}_{11})=(1,4,9,5,3)$,

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

and

$$\left\{(j,k):\ 1\leqslant j<k\leqslant 5\ \&\ \{k^2-j^2\}_{11}>\frac{11}{2}\right\}=\{(1,3),\ (2,5),\ (3,4),\ (4,5)\}.$$

From Theorem 1.3 we deduce the following result.

Theorem 1.4. *Let p be an odd prime. Then*

$$\operatorname{sign}(S_p)=(-1)^{s(p)}=(-1)^{t(p)}=\begin{cases}1 & \text{if } p\equiv 3 \pmod 8,\\ (-1)^{(h(-p)+1)/2} & \text{if } p\equiv 7 \pmod 8.\end{cases}\tag{1.18}$$

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

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}\csc\pi\frac{a(k^2-j^2)}{p}=\prod_{1\leqslant j<k\leqslant(p-1)/2}\left(\cot\pi\frac{aj^2}{p}-\cot\pi\frac{ak^2}{p}\right)$$
$$=\begin{cases}(2^{p-1}/p)^{(p-3)/8} & \text{if } p\equiv 3 \pmod 8,\\ (-1)^{(h(-p)+1)/2}(\frac{a}{p})(2^{p-1}/p)^{(p-3)/8} & \text{if } p\equiv 7 \pmod 8,\end{cases}\tag{1.19}$$

and in the case $p\equiv 1 \pmod 4$ we have

$$\begin{aligned}&(-1)^{(a-1)(p-1)/4}\prod_{1\leqslant j<k\leqslant(p-1)/2}\csc\pi\frac{a(k^2-j^2)}{p}\\ =&\varepsilon_p^{-(\frac{a}{p})h(p)(p-1)/2}\prod_{1\leqslant j<k\leqslant(p-1)/2}\left(\cot\pi\frac{aj^2}{p}-\cot\pi\frac{ak^2}{p}\right)\\ =&\pm\left(2^{p-1}p^{-1}\right)^{(p-3)/8}\varepsilon_p^{-(\frac{a}{p})h(p)/2}.\end{aligned}\tag{1.20}$$

Remark 1.2. The values of $s(p)$ for the first 2500 odd primes p are available from [S18, A319311]. That $2\mid s(p)$ for any prime $p\equiv 3 \pmod 8$ might have a combinatorial proof.

With the help of Theorem 1.4, we also get the following result.

Theorem 1.5. *Let p be an odd prime and let $\zeta = e^{2\pi i/p}$. Let $a \in \mathbb{Z}$ with $p \nmid a$. Then*

$$\begin{aligned}&(-1)^{a\frac{p+1}{2}\lfloor\frac{p-1}{4}\rfloor}2^{(p-1)(p-3)/8}\prod_{1\leqslant j<k\leqslant(p-1)/2}\cos\pi\frac{a(k^2-j^2)}{p}\\&=\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}+\zeta^{ak^2})=\begin{cases}1 & \text{if } p\equiv 3 \pmod 4,\\ \pm\varepsilon_p^{(\frac{a}{p})h(p)((\frac{2}{p})-1)/2} & \text{if } p\equiv 1 \pmod 4.\end{cases}\end{aligned}\tag{1.21}$$

For a real number x let $\{x\}$ denote its fractional part $x-\lfloor x\rfloor$. If p is an odd prime and $1\leqslant j<k\leqslant(p-1)/2$, then

$$\begin{aligned}\cos 2\pi\frac{k^2-j^2}{p}<0 &\iff \cos 2\pi\left|\left\{\frac{k^2}{p}\right\}-\left\{\frac{j^2}{p}\right\}\right|<0\\&\iff \frac14<\left|\left\{\frac{k^2}{p}\right\}-\left\{\frac{j^2}{p}\right\}\right|<\frac34.\end{aligned}$$

Thus Theorem 1.5 with $a=2$ yields the following corollary.

Corollary 1.2. *For any prime $p\equiv 3 \pmod 4$, we have*

$$\left|\left\{(j,k):\ 1\leqslant j<k\leqslant\frac{p-1}{2}\ \text{and}\ \frac14<\left|\left\{\frac{k^2}{p}\right\}-\left\{\frac{j^2}{p}\right\}\right|<\frac34\right\}\right|\equiv 0 \pmod 2.\tag{1.22}$$

Motivated by the congruences (1.5)-(1.6) and Theorems 1.2-1.5, we establish the following theorem.

Theorem 1.6. *Let p be an odd prime.*

(i) *Let $a\in\mathbb{Z}$ with $p\nmid a$. Then*

$$\begin{aligned}&\prod_{\substack{1\leqslant j<k\leqslant(p-1)/2\\ p\nmid j^2+k^2}}\sin\pi\frac{a(j^2+k^2)}{p}\\&=\left(\frac{p}{2^{p-1}}\right)^{(p-(\frac{-1}{p})-4)/8}\times\begin{cases}\varepsilon_p^{(\frac{a}{p})h(p)(1+(\frac{2}{p}))/2} & \text{if } p\equiv 1 \pmod 4,\\ (-1)^{(p-3)/8} & \text{if } p\equiv 3 \pmod 8,\\ (-1)^{(p+1)/8+(h(-p)+1)/2}(\frac{a}{p}) & \text{if } p\equiv 7 \pmod 8.\end{cases}\end{aligned}\tag{1.23}$$

Also,

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}\cos\pi\frac{a(j^2+k^2)}{p}=(-1)^{a\frac{p+1}{2}\lfloor\frac{p-1}{4}\rfloor}2^{-\frac{p-1}{2}\lfloor\frac{p-3}{4}\rfloor}\tag{1.24}$$

and

$$\prod_{\substack{1\leqslant j<k\leqslant (p-1)/2\\ p\nmid j^2+k^2}}\left(\cot\pi\frac{aj^2}{p}+\cot\pi\frac{ak^2}{p}\right)$$
$$=(2^{p-1}p^{-1})^{(p-(\frac{-1}{p})-4)/8}\times\begin{cases}\varepsilon_p^{(\frac{a}{p})h(p)(p+(\frac{2}{p})-4)/2} & \text{if } p\equiv 1 \pmod 4,\\ (-1)^{(p-3)/8} & \text{if } p\equiv 3 \pmod 8,\\ (-1)^{(p+1)/8+(h(-p)+1)/2}(\frac{a}{p}) & \text{if } p\equiv 7 \pmod 8.\end{cases} \tag{1.25}$$

(ii) *Let $a,b,c\in\mathbb{Z}$ with $ac(a+b+c)\not\equiv 0 \pmod p$. Set $\Delta=b^2-4ac$ and*

$$m=\sum_{\substack{1\leqslant j<k\leqslant p-1\\ p\mid aj^2+bjk+ck^2}}(aj^2+bjk+ck^2). \tag{1.26}$$

Then

$$(-1)^m\left(2^{p-1}p^{-1}\right)^{(p-3-(\frac{\Delta}{p}))/2}\prod_{\substack{1\leqslant j<k\leqslant p-1\\ p\nmid aj^2+bjk+ck^2}}\sin\pi\frac{aj^2+bjk+ck^2}{p}$$
$$=\begin{cases}(-1)^{(b+(\frac{\Delta}{p}))\frac{p-1}{4}}\varepsilon_p^{h(p)((1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))} & \text{if } p\equiv 1 \pmod 4,\\ (-1)^{a+b\frac{p-3}{4}}(\frac{a(a+b+c)}{p}) & \text{if } 4\mid p-3\ \&\ p\mid\Delta,\\ (-1)^{a+(b-1)\frac{p-3}{4}+\frac{h(-p)+1}{2}}(\frac{ac(a+b+c)\Delta}{p}) & \text{if } 4\mid p-3\ \&\ p\nmid\Delta.\end{cases} \tag{1.27}$$

We also have

$$2^{(p-1)(p-3-(\frac{\Delta}{p}))/2}\prod_{1\leqslant j<k\leqslant p-1}\cos\pi\frac{aj^2+bjk+ck^2}{p}$$
$$=\begin{cases}(-1)^{b(p-1)/4}\varepsilon_p^{h(p)((\frac{2}{p})-1)((1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))} & \text{if } p\equiv 1 \pmod 4,\\ (-1)^{a+b(p-3)/4+(\frac{\Delta}{p})(p+1)/4} & \text{if } p\equiv 3 \pmod 4.\end{cases} \tag{1.28}$$

Remark 1.3. Under the notation in Theorem 1.6, as $4a(aj^2+bjk+ck^2)=(2aj+bk)^2-\Delta k^2$ we have $m=0$ in the case $(\frac{\Delta}{p})=-1$. It seems sophisticated to determine the parity of m in the case $(\frac{\Delta}{p})\geqslant 0$.

Let p be any odd prime, For $1\leqslant j<k\leqslant (p-1)/2$, clearly

$$\begin{aligned}\{aj^2\}_p+\{ak^2\}_p>p &\iff \{aj^2\}_p>\{-ak^2\}_p\\ &\iff \cot\pi\frac{aj^2}{p}<\cot\pi\frac{-ak^2}{p}\\ &\iff \cot\pi\frac{aj^2}{p}+\cot\pi\frac{ak^2}{p}<0.\end{aligned}$$

Thus (1.25) yields the following consequence.

Corollary 1.3. *Let p be an odd prime and let $a\in\mathbb{Z}$ with $p\nmid a$. For*

$$N_p:=\left|\left\{(j,k):\ 1\leqslant j<k\leqslant\frac{p-1}{2}:\ \{aj^2\}_p+\{ak^2\}_p>p\right\}\right|,\tag{1.29}$$

we have

$$(-1)^{N_p}=\begin{cases}1 & \text{if } p\equiv 1\pmod 4,\\ (-1)^{(p-3)/8} & \text{if } p\equiv 3\pmod 8,\\ (-1)^{(p+1)/8+(h(-p)+1)/2}(\frac{a}{p}) & \text{if } p\equiv 7\pmod 8.\end{cases}\tag{1.30}$$

Remark 1.4. Let p be an odd prime and let $a\in\mathbb{Z}$ with $p\nmid a$. For $1\leqslant j<k\leqslant(p-1)/2$, by Lucas' theorem (cf. [HS])

$$p\mid\binom{a(j^2+k^2)}{aj^2}\iff\{aj^2+ak^2\}_p<\{aj^2\}_p\iff\{aj^2\}_p+\{ak^2\}_p>p$$

and hence

$$N_p=\left|\left\{(j,k):\ 1\leqslant j<k\leqslant\frac{p-1}{2}\text{ and }p\mid\binom{a(j^2+k^2)}{aj^2}\right\}\right|.$$

We are going to show Theorems 1.1-1.2, Theorem 1.3, Theorems 1.4-1.5 and Theorem 1.6 in Sections 2-5 respectively. In Section 6 we pose some conjectures for further research.

2. Proofs of Theorems 1.1-1.2

Lemma 2.1. *Suppose that $m=\prod_{s=1}^r p_s^{a_s}$, where $p_1,\ldots,p_r$ are distinct odd primes and $a_1,\ldots,a_r$ are positive integers. Then*

$$\left|\left\{1\leqslant k<\frac{m}{2}:\ \gcd(k,m)=1\text{ and }\bar{k}<\frac{m}{2}\right\}\right|\equiv\delta_{r,1}\pmod 2,\tag{2.1}$$

where $\bar{k}$ is inverse of k modulo m (i.e., $1\leqslant k\leqslant m-1$ and $k\bar{k}\equiv 1\pmod m$), and $\delta_{r,1}$ is 1 or 0 according as $r=1$ or not. Also, the number

$$N:=\left|\left\{(i,j):\ 1\leqslant i<j<\frac{m}{2}\text{ and }ij\equiv\pm1\pmod m\right\}\right|\tag{2.2}$$

is odd if and only if $r=1$ & ($p_1\equiv 1$ or $4a_1+3\pmod 8$), or $r=2$ & $p_1+p_2\equiv 0\pmod 4$.

Proof. By Prop. 4.2.3 of [IR, p. 46], for each $\varepsilon\in\{\pm1\}$ and $1\leqslant s\leqslant r$, we have

$$\begin{aligned}&|\{0\leqslant x\leqslant p_s^{a_s}-1:\ x^2\equiv\varepsilon\pmod{p_s^{a_s}}\}|\\=&|\{0\leqslant x\leqslant p_s-1:\ x^2\equiv\varepsilon\pmod{p_s}\}|\\=&\begin{cases}2&\text{if }\varepsilon=1\text{ or }p_s\equiv1\pmod 4,\\0&\text{otherwise.}\end{cases}\end{aligned}$$

Thus, by applying the Chinese Remainder Theorem we see that

$$|\{0\leqslant x\leqslant m-1:\ x^2\equiv1\pmod m\}|=2^r \tag{2.3}$$

and

$$|\{0\leqslant x\leqslant m-1:\ x^2\equiv\pm1\pmod m\}|=2^{(1+\delta)r}, \tag{2.4}$$

where δ is 1 or 0 according as whether $p_s\equiv1\pmod 4$ for all $s=1,\ldots,r$.

Set $n=(m-1)/2$ and

$$S=\{(k,\bar k):\ \gcd(k,m)=1\ \&\ 1\leqslant k,\bar k\leqslant n\}.$$

Clearly, $(k,\bar k)\in S$ if and only if $(\bar k,k)\in S$. Note that

$$k=\bar k\in\{1,\ldots,n\}\iff 1\leqslant k\leqslant n\ \&\ k^2\equiv1\ (\mathrm{mod}\ m).$$

Therefore

$$|S|\equiv\left|\left\{1\leqslant x<\frac m2:\ x^2\equiv1\pmod m\right\}\right|=2^{r-1}\equiv\delta_{r,1}\pmod 2$$

in view of (2.3). This proves (2.1).

In light of (2.4), we have

$$\begin{aligned}2N=&|\{(i,j):\ 1\leqslant i,j\leqslant n\ \&\ ij\equiv\pm1\pmod m\}|\\&-|\{1\leqslant x\leqslant n:\ x^2\equiv\pm1\pmod m\}|\\=&|\{(i,\tau_m(i)):\ 1\leqslant i\leqslant n\ \&\ \gcd(i,m)=1\}|-2^{(1+\delta)r-1}\\=&\frac{\varphi(m)}{2}-2^{(1+\delta)r-1}=\frac12\prod_{s=1}^r p_s^{a_s-1}(p_s-1)-2^{(1+\delta)r-1},\end{aligned}$$

which implies that N is odd if and only if $r=1\ \&\ (p_1\equiv1\text{ or }4a_1+3\pmod 8)$, or $r=2\ \&\ p_1+p_2\equiv0\pmod 4$. This concludes the proof. □

Proof of Theorem 1.1. Set $n=(m-1)/2$. Clearly $\overline{m-k}=m-\bar k$ for all $1\leqslant k\leqslant n$ with $\gcd(k,m)=1$. If $1\leqslant i<j\leqslant m-1$ with $\gcd(i,m)=\gcd(j,m)=1$, then $m-j<m-i$ and

$$(\bar j-\bar i)(\overline{m-i}-\overline{m-j})=(\bar j-\bar i)(m-\bar i-(m-\bar j))=(\bar j-\bar i)^2>0.$$

If $1 \leqslant i < j \leqslant m-1$, $\gcd(i,m) = \gcd(j,m) = 1$ and $(m-j, m-i) = (i,j)$, then $1 \leqslant i \leqslant n$, $j = m-i$ and $\bar{j} - \bar{i} = m - 2\bar{i}$. Thus

$$\mathrm{sign}(\sigma_m) = (-1)^{|\{1\leqslant i\leqslant n:\ \gcd(i,m)=1\ \&\ \bar{i}>n\}|} = (-1)^{\varphi(m)/2-\delta_{r,1}} = (-1)^{\delta_{r,1}(p_1+1)/2}$$

by applying (2.1). This proves (1.1).

Now we turn to show (1.2). For $i, j \in \{1 \leqslant k \leqslant n :\ \gcd(k,n) = 1\}$ with $i < j$, if $i^* < j^*$ then

$$(j^* - i^*)((j^*)^* - (i^*)^*) = (j^* - i^*)(j - i) > 0;$$

If $j^* < i^*$ then

$$(j^* - i^*)((i^*)^* - (j^*)^*) = (j^* - i^*)(i - j) > 0;$$

If $i = i^*$ and $j = j^*$ then $j^* - i^* > 0$; if $(j^*, i^*) = (i, j)$ then $j^* - i^* = i - j < 0$. In view of this, we see that

$$\mathrm{sign}(\tau_m) = (-1)^{|\{1\leqslant i\leqslant n:\ \gcd(i,m)=1\ \&\ i<i^*\}|} = (-1)^N.$$

So the second assertion in Theorem 1.1 holds by Lemma 2.1.

The proof of Theorem 1.1 is now complete. □

Lemma 2.2. *Let p be an odd prime, and let $a, b, c \in \mathbb{Z}$ with a or b not divisible by p. Then*

$$\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right) = \begin{cases} -(\frac{a}{p}) & \text{if } p \nmid b^2-4ac, \\ (p-1)(\frac{a}{p}) & \text{if } p \mid b^2-4ac. \end{cases} \tag{2.5}$$

Remark 2.1. (2.5) in the case $p \mid a$ is trivial. When $p \nmid a$, (2.5) is a known result (see, e.g., [BEW, p. 58]).

Lemma 2.3. *Let p be any odd prime, and define*

$$r(n) := \left|\left\{(j,k):\ 1 \leqslant j < k \leqslant \frac{p-1}{2} \text{ and } j^2 + k^2 \equiv n \pmod{p}\right\}\right|$$

for $n = 0, \ldots, p-1$. Then

$$r(0) = \begin{cases} (p-1)/4 & \text{if } p \equiv 1 \pmod 4, \\ 0 & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{2.6}$$

If $n \in \{1, \ldots, p-1\}$, then

$$r(n) = \left\lfloor\frac{p+1}{8}\right\rfloor - \frac{1+(\frac{2}{p})}{2}\cdot\frac{1+(\frac{n}{p})}{2}. \tag{2.7}$$

Proof. If $p\equiv 3\pmod 4$, then $(\frac{-1}{p})=-1$ and hence $r(0)=0$. When $p\equiv 1\pmod 4$, we have $q^2\equiv -1\pmod p$ for some $q\in\mathbb{Z}$, and hence $r(0)=(p-1)/4$ since

$$j^2+k^2\equiv 0\pmod p\iff j\equiv \pm qk\iff k\equiv \pm qj\pmod p.$$

Below we let $n\in\{1,\ldots,p-1\}$. Observe that

$$\begin{aligned}2r(n)+\frac{1+(\frac{2n}{p})}{2}=&2r(n)+\left|\left\{1\leqslant k\leqslant\frac{p-1}{2}:\ k^2+k^2\equiv n\pmod p\right\}\right|\\ =&\left|\left\{(j,k):\ 1\leqslant j,k\leqslant\frac{p-1}{2}\text{ and }j^2+k^2\equiv n\pmod p\right\}\right|\\ =&\left|\left\{1\leqslant x\leqslant p-1:\ \left(\frac{x}{p}\right)=1\text{ and }\left(\frac{n-x}{p}\right)=1\right\}\right|\\ =&\sum_{x=1}^{p-1}\frac{1+(\frac{x}{p})}{2}\cdot\frac{1+(\frac{n-x}{p})}{2}-\frac{1+(\frac{n}{p})}{2}\cdot\frac{1+(\frac{n-n}{p})}{2}\\ =&\frac{p-1}{4}+\frac14\left(\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)+\sum_{x=0}^{p-1}\left(\frac{n-x}{p}\right)-\left(\frac{n}{p}\right)\right)\\ &+\frac14\left(\frac{-1}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^2-nx}{p}\right)-\frac{1+\left(\frac{n}{p}\right)}{4}\\ =&\frac{p-(\frac{-1}{p})}{4}-\frac{1+(\frac{n}{p})}{2}\end{aligned}$$

with the help of Lemma 2.2. This yields (2.7). □

Lemma 2.4. *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 $\Delta=b^2-4ac$. For each $n=0,1\ldots,p-1$, we have*

$$\begin{aligned}&|\{(j,k):\ 1\leqslant j<k\leqslant p-1\text{ and }aj^2+bjk+ck^2\equiv n\pmod p\}|\\ =&\begin{cases}\frac12(p-3-(\frac{\Delta}{p})-(\frac{n}{p})((1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))) & \text{if } n\neq 0,\\ \frac{p-1}{2}(1+(\frac{\Delta}{p})) & \text{if } n=0.\end{cases}\end{aligned}\tag{2.8}$$

Proof. Let L denote the left-hand side of (2.8). Then

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

and hence

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

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

$$\begin{aligned} N=&\sum_{x=1}^{p-1}\frac{1+(\frac{x}{p})}{2}\left(1+\left(\frac{\Delta x+4an}{p}\right)\right)-\frac{1+(\frac{cn}{p})}{2}-\frac{1+(\frac{(a+b+c)n}{p})}{2}.\\ =&\frac{p-1}{2}+\frac12\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)+\frac12\left(\sum_{x=0}^{p-1}\left(\frac{\Delta x+4an}{p}\right)-\left(\frac{4an}{p}\right)\right)\\ &+\frac12\sum_{x=0}^{p-1}\left(\frac{\Delta x^2+4anx}{p}\right)-1-\frac12\left(\frac{n}{p}\right)\left(\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)\right)\\ =&\frac{p-3}{2}-\frac12\left(\frac{\Delta}{p}\right)-\frac12\left(\frac{n}{p}\right)\left(\left(1-p\delta_{(\frac{\Delta}{p}),0}\right)\left(\frac{a}{p}\right)+\left(\frac{c}{p}\right)+\left(\frac{a+b+c}{p}\right)\right) \end{aligned}$$

with the help of the identity

$$\sum_{x=0}^{p-1}\left(\frac{\Delta x^2+4anx}{p}\right)=-\left(\frac{\Delta}{p}\right)$$

from Lemma 2.2. This proves (2.8). □

Lemma 2.5. *Let p be an odd prime, and let $a,b,c\in\mathbb{Z}$ with $a+c=0$ and $abc\not\equiv 0\pmod p$. Set $\Delta=b^2-4ac$. Then*

$$(-1)^{|\{(i,j):\ 1\leqslant i,j\leqslant (p-1)/2\ \&\ p|ai^2+bij+cj^2\}|}=\begin{cases}1 & \text{if } (\frac{\Delta}{p})=-1,\\ (\frac{2}{p}) & \text{if } (\frac{\Delta}{p})=0,\\ (\frac{-1}{p}) & \text{if } (\frac{\Delta}{p})=1.\end{cases}\qquad(2.9)$$

Proof. Define

$$N=\left|\left\{(i,j):\ 1\leqslant i,j\leqslant\frac{p-1}{2}\ \&\ p\mid ai^2+bij+cj^2\right\}\right|.$$

Case 1. $(\frac{\Delta}{p})=-1$.

In this case,

$$4a(ai^2+bij+cj^2)=(2ai+bj)^2-\Delta j^2\not\equiv 0 \pmod p$$

for all $i,j\in\mathbb{Z}$. Thus $N=0$ and $(-1)^N=1$.

Case 2. $(\frac{\Delta}{p})=0$.

In this case, p divides $\Delta=b^2+4a^2$, hence $(\frac{-1}{p})=1$ and $p\equiv 1 \pmod 4$. As

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

for some $k=0,1$ we have $x:=(-1)^k\frac{p-1}{2}!\equiv -b/(2a) \pmod p$. Thus

$$\begin{aligned}N=&\left|\left\{(i,j):\ 1\leqslant i,j\leqslant\frac{p-1}{2}\ \&\ i\equiv jx \pmod p\right\}\right|\\ =&\frac{p-1}{2}-\left|\left\{1\leqslant j\leqslant\frac{p-1}{2}:\ \{jx\}_p>\frac{p}{2}\right\}\right|\end{aligned}$$

and hence

$$(-1)^N=(-1)^{(p-1)/2}\left(\frac{x}{p}\right)=\left(\frac{((p-1)/2)!}{p}\right)=\left(\frac{2}{p}\right)$$

by using Gauss' Lemma and [S13, Lemma 2.3].

Case 3. $(\frac{\Delta}{p})=1$.

In this case $\delta^2\equiv\Delta$ for some $\delta\in\mathbb{Z}$ with $p\nmid\Delta$. Let x_1 and x_2 be integers with $x_1\equiv(-b+\delta)/(2a) \pmod p$ and $x_2\equiv(-b-\delta)/(2a) \pmod p$. Then $x_1\not\equiv x_2 \pmod p$, $x_1+x_2\equiv -b/a \pmod p$ and $x_1x_2\equiv c/a=-1 \pmod p$. Thus

$$\begin{aligned}N=&\left|\left\{1\leqslant i,j\leqslant\frac{p-1}{2}:\ i\equiv jx_s \pmod p \text{ for some } s=1,2\right\}\right|\\ =&\sum_{s=1}^{2}\left(\frac{p-1}{2}-\left|\left\{1\leqslant j\leqslant\frac{p-1}{2}:\ \{jx_s\}_p>\frac{p}{2}\right\}\right|\right).\end{aligned}$$

Applying Gauss' Lemma we obtain that

$$(-1)^N=(-1)^{p-1}\prod_{s=1}^{2}\left(\frac{x_s}{p}\right)=\left(\frac{x_1x_2}{p}\right)=\left(\frac{-1}{p}\right).$$

In view of the above, we have completed the proof of Lemma 2.5. □

Proof of Theorem 1.2. (i) Let $r(n)$ be as in Lemma 2.3. Then

$$\prod_{\substack{1\leqslant i<j\leqslant (p-1)/2\\ p\nmid i^2+j^2}}(i^2+j^2)\equiv\prod_{n=1}^{p-1}n^{r(n)}=(p-1)!^{\lfloor (p+1)/8\rfloor}\prod_{\substack{n=1\\ (\frac{n}{p})=1}}^{p-1}n^{-(1+(\frac{2}{p}))/2}$$
$$\equiv(-1)^{\lfloor (p+1)/8\rfloor}\prod_{k=1}^{(p-1)/2}(k^2)^{-(1+(\frac{2}{p}))/2}$$
$$\equiv(-1)^{\lfloor (p+1)/8\rfloor}\left((-1)^{(p+1)/2}\right)^{(1+(\frac{2}{p}))/2}\pmod p$$

with the help of (1.3). This yields (1.7) if $p\equiv 1\pmod 4$. It also proves (1.6) in the case $p\equiv 3\pmod 4$.

(ii) If $p\mid\Delta$, then by Lemma 2.4 and Wilson's theorem we have

$$\prod_{\substack{1\leqslant i<j\leqslant (p-1)/2\\ p\nmid ai^2+bij+cj^2}}(ai^2+bij+cj^2)$$
$$\equiv\prod_{n=1}^{p-1}n^{\frac{p-3}{2}+\frac{1-p}{2}(\frac{a}{p})+\frac12((\frac{c}{p})+(\frac{a+b+c}{p}))-\frac12(1+(\frac{n}{p}))((1-p)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))}$$
$$\equiv(-1)^{\frac{p-3}{2}+\frac{1-p}{2}(\frac{a}{p})+\frac12((\frac{c}{p})+(\frac{a+b+c}{p}))}\prod_{k=1}^{(p-1)/2}(k^2)^{(1-p)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))}$$
$$\equiv(-1)^{\frac12((\frac{c}{p})+(\frac{a+b+c}{p}))-1}\left((-1)^{(p+1)/2}\right)^{(1-p)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))}$$
$$=(-1)^{\frac12((\frac{c}{p})+(\frac{a+b+c}{p}))-1}=\left(\frac{c(a+b+c)}{p}\right)=\left(\frac{a(a+b+c)}{p}\right)\pmod p$$

since $4ac\equiv b^2\pmod p$. Similarly, when $p\nmid\Delta$, by Lemma 2.4 and (1.3) we have

$$\prod_{\substack{1\leqslant i<j\leqslant (p-1)/2\\ p\nmid ai^2+bij+cj^2}}(ai^2+bij+cj^2)$$
$$\equiv\prod_{n=1}^{p-1}n^{\frac{p-3}{2}+\frac12((\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p})-(\frac{\Delta}{p}))-\frac12(1+(\frac{n}{p}))((\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))}$$
$$\equiv(-1)^{\frac{p-3}{2}+\frac12((\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p})-(\frac{\Delta}{p}))}\prod_{k=1}^{(p-1)/2}(k^2)^{(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))}$$
$$\equiv(-1)^{\frac{p-3}{2}+\frac12((\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p})-(\frac{\Delta}{p})}\left((-1)^{(p+1)/2}\right)^{(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))}\pmod p$$

and hence

$$\begin{aligned}&\prod_{\substack{1\leqslant i<j\leqslant (p-1)/2\\ p\nmid ai^2+bij+cj^2}}(ai^2+bij+cj^2)\\ &\equiv(-1)^{\frac12((\frac ap)+(\frac cp))}(-1)^{\frac12((\frac{a+b+c}{p})-(\frac{\Delta}{p}))}\\ &=-\left(\frac{ac}{p}\right)\left(\frac{(a+b+c)\Delta}{p}\right)=-\left(\frac{ac(a+b+c)\Delta}{p}\right)\pmod p.\end{aligned}$$

This proves (1.8).

Now assume that $a+c=0$. We deduce (1.9) from (1.8). Observe that

$$\begin{aligned}&\prod_{\substack{1\leqslant i<j\leqslant p-1\\ p\nmid ai^2+bij+cj^2}}(ai^2+bij+cj^2)\\ =&\prod_{\substack{i,j=1\\ p\nmid ai^2-bij+cj^2}}^{(p-1)/2}(ai^2+bi(p-j)+c(p-j)^2)\times\prod_{\substack{1\leqslant i<j\leqslant (p-1)/2\\ p\nmid ai^2+bij+cj^2}}(ai^2+bij+cj^2)\\ &\times\prod_{\substack{1\leqslant j<i\leqslant (p-1)/2\\ p\nmid ai^2+bij+cj^2}}(a(p-i)^2+b(p-i)(p-j)+c(p-j)^2)\\ \equiv&\prod_{\substack{i,j=1\\ p\nmid ai^2-bij+cj^2}}^{(p-1)/2}(ai^2-bij+cj^2)\times\prod_{\substack{i,j=1\\ p\nmid ai^2+bij+cj^2}}^{(p-1)/2}(ai^2+bij+cj^2)\Big/\prod_{i=1}^{(p-1)/2}(ai^2+bi^2+ci^2)\\ \equiv&\frac{(-1)^m}{((p-1)/2)!^2}\left(\frac{a+b+c}{p}\right)\prod_{\substack{i,j=1\\ p\nmid ci^2+bij+aj^2}}^{(p-1)/2}(ci^2+bij+aj^2)\times\prod_{\substack{i,j=1\\ p\nmid ai^2+bij+cj^2}}^{(p-1)/2}(ai^2+bij+cj^2)\\ =&\frac{(-1)^m}{((p-1)/2)!)^2}\left(\frac{a+b+c}{p}\right)\prod_{\substack{i,j=1\\ p\nmid ai^2+bij+cj^2}}^{(p-1)/2}(ai^2+bij+cj^2)^2\pmod p,\end{aligned}$$

where

$$\begin{aligned}m&=\left|\left\{(i,j):\ 1\leqslant i,j\leqslant\frac{p-1}{2}\ \text{and}\ \ p\nmid ai^2-bij+cj^2\right\}\right|\\ &=\left|\left\{(i,j):\ 1\leqslant i,j\leqslant\frac{p-1}{2}\ \text{and}\ \ p\nmid ci^2+bij+aj^2\right\}\right|.\end{aligned}$$

Combining this with (1.8) and noting $ac=-a^2$, we see that

$$\prod_{\substack{i,j=1\\ p\nmid ai^2+bij+cj^2}}^{(p-1)/2}(ai^2+bij+cj^2)^2\equiv(-1)^m\left(\frac{p-1}{2}!\right)^2\times\begin{cases}(\frac ap)\pmod p&\text{if }p\mid\Delta,\\ -(\frac{-\Delta}{p})\pmod p&\text{if }p\nmid\Delta.\end{cases}\tag{2.10}$$

By Lemma 2.5,

$$(-1)^{((p-1)/2)^2-m}=\begin{cases}1&\text{if }(\frac{\Delta}{p})=-1,\\(\frac{2}{p})&\text{if }(\frac{\Delta}{p})=0,\\(\frac{-1}{p})&\text{if }(\frac{\Delta}{p})=1.\end{cases}$$

If p divides $\Delta=b^2+4a^2$, then $(\frac{-1}{p})=1$, $(-1)^m=(\frac{2}{p})$, $(b/(2a))^2\equiv-1\equiv((p-1)/2)!)^2\pmod p$ and

$$\left(\frac{b}{p}\right)=\left(\frac{\pm2((p-1)/2)!}{p}\right)\left(\frac{a}{p}\right)=\left(\frac{a}{p}\right)$$

with the help of [S13, Lemma 2.3]. Thus, in view of (2.10) and (1.3), we have (1.9) if $p\mid\Delta$. When $(\frac{\Delta}{p})=-1$, we have

$$-(-1)^m\left(\frac{-\Delta}{p}\right)=(-1)^m\left(\frac{-1}{p}\right)=1$$

and hence (1.9) holds in view of (2.10). If $(\frac{\Delta}{p})=1$, then

$$-(-1)^m\left(\frac{-\Delta}{p}\right)=-(-1)^m\left(\frac{-1}{p}\right)=-\left(\frac{-1}{p}\right)\equiv\frac{1}{((p-1)/2)!^2}\pmod p$$

and hence (1.9) follows from (2.10).

The proof of Theorem 1.2 is now complete. □

3. Proof of Theorem 1.3

To prove Theorem 1.3, we need some known results.

Lemma 3.1. *Let p be an odd prime, and let $\zeta=e^{2\pi i/p}$.*

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

$$\prod_{n=1}^{p-1}(1-\zeta^{an})=p \tag{3.1}$$

and

$$\sum_{x=0}^{p-1}\zeta^{ax^2}=\left(\frac{a}{p}\right)\sqrt{(-1)^{(p-1)/2}p}. \tag{3.2}$$

(ii) *If $p\equiv1\pmod 4$, then*

$$\prod_{n=1}^{p-1}(1-\zeta^n)^{(\frac{n}{p})}=\varepsilon_p^{-2h(p)}. \tag{3.3}$$

(ii) *When* $p \equiv 3 \pmod 4$, *we have*

$$ph(-p) = -\sum_{k=1}^{p-1} k \left(\frac{k}{p}\right), \tag{3.4}$$

and also

$$\left|\left\{1 \leqslant k \leqslant \frac{p-1}{2} :\ \left(\frac{k}{p}\right) = -1\right\}\right| \equiv \frac{h(-p)+1}{2} \pmod 2 \tag{3.5}$$

provided $p > 3$.

Remark 3.1. This lemma is well known. For any $a \in \mathbb{Z}$ with $p \nmid a$, we have (3.1) since

$$\prod_{n=1}^{p-1}(1-\zeta^{an}) = \prod_{k=1}^{p-1}(1-\zeta^k) = \lim_{x\to 1}\frac{x^p-1}{x-1} = p,$$

and we have (3.2) by Gauss' evaluation of quadratic Gauss sums (cf. [IR, pp. 70-75]). Part (ii) and the first assertion in part (iii) are Dirichlet's class number formula. The second assertion in part (iii) was pointed out by Mordell [M61].

Lemma 3.2. *Let* p *be an odd prime and let* $n \in \{1, \ldots, p-1\}$. *Then*

$$\begin{aligned}&\left|\left\{(j,k):\ 1 \leqslant j,k \leqslant \frac{p-1}{2} \text{ and } j^2-k^2 \equiv n \pmod p\right\}\right| \\ &= \left\lfloor \frac{p-1}{4} \right\rfloor - \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ and } (\frac{n}{p}) = 1, \\ 0 & \text{otherwise.}\end{cases}\end{aligned} \tag{3.6}$$

Proof. Let L denote the left-hand side of (3.6). Then

$$\begin{aligned} L =& \left|\left\{1 \leqslant x \leqslant p-1 :\ \left(\frac{x}{p}\right) = 1 \text{ and } \left(\frac{n+x}{p}\right) = 1\right\}\right| \\ =& \sum_{x=1}^{p-1} \frac{(\frac{x}{p})+1}{2} \cdot \frac{(\frac{x+n}{p})+1}{2} - \frac{(\frac{p-n}{p})+1}{2} \cdot \frac{(\frac{p-n+n}{p})+1}{2} \\ =& \frac{p-1}{4} + \frac{1}{4}\sum_{x=0}^{p-1}\left(\frac{x}{p}\right) + \frac{1}{4}\left(\sum_{x=0}^{p-1}\left(\frac{x+n}{p}\right) - \left(\frac{n}{p}\right)\right) \\ &+ \frac{1}{4}\sum_{x=0}^{p-1}\left(\frac{x(x+n)}{p}\right) - \frac{(\frac{-n}{p})+1}{4} \\ =& \frac{p-3-(\frac{n}{p})-(\frac{-n}{p})}{4} \end{aligned}$$

with the help of Lemma 2.2. This yields (3.6). □

Proof of Theorem 1.3. Let φ_a be the element of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with $\varphi_a(\zeta)=\zeta^a$. In view of (3.2),

$$\varphi_a\left(\sqrt{(-1)^{(p-1)/2}p}\right)=\varphi_a\left(\sum_{x=0}^{p-1}\zeta^{x^2}\right)=\sum_{x=0}^{p-1}\zeta^{ax^2}=\left(\frac{a}{p}\right)\sqrt{(-1)^{(p-1)/2}p}. \tag{3.7}$$

(i) We first handle the case $p\equiv 1 \pmod 4$. Combining (3.1) and (3.3), we get

$$\prod_{\substack{n=1\\ (\frac{n}{p})=1}}^{p-1}(1-\zeta^n)^2=\prod_{n=1}^{p-1}(1-\zeta^n)^{1+(\frac{n}{p})}=p\varepsilon_p^{-2h(p)}.$$

Note that

$$\prod_{\substack{n=1\\ (\frac{n}{p})=1}}^{p-1}(1-\zeta^n)=\prod_{\substack{n=1\\ (\frac{n}{p})=1}}^{(p-1)/2}(1-\zeta^n)(1-\zeta^{p-n})=\prod_{\substack{n=1\\ (\frac{n}{p})=1}}^{(p-1)/2}|1-\zeta^n|^2>0.$$

Therefore

$$\prod_{k=1}^{(p-1)/2}(1-\zeta^{k^2})=\prod_{\substack{n=1\\ (\frac{n}{p})=1}}^{p-1}(1-\zeta^n)=\sqrt{p}\,\varepsilon_p^{-h(p)}. \tag{3.8}$$

This proves (1.10) for $a=1$.

Write $\varepsilon_p=u_p+v_p\sqrt{p}$ with $u_p,v_p\in\mathbb{Q}$. In view of (3.7),

$$\varphi_a(\varepsilon_p)=u_p+\left(\frac{a}{p}\right)v_p\sqrt{p}=\frac{N(\varepsilon_p)}{u_p-(\frac{a}{p})v_p}=\begin{cases}\varepsilon_p & \text{if } (\frac{a}{p})=1,\\ N(\varepsilon_p)\varepsilon_p^{-1} & \text{if } (\frac{a}{p})=-1,\end{cases}$$

where $N(\varepsilon_p)$ is the norm of ε_p with respect to the field extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$. Thus, by using (3.8) we obtain

$$\begin{aligned}\prod_{k=1}^{(p-1)/2}(1-\zeta^{ak^2})=&\varphi_a\left(\prod_{k=1}^{(p-1)/2}(1-\zeta^{k^2})\right)=\varphi_a\left(\sqrt{p}\,\varepsilon_p^{-h(p)}\right)\\ =&\begin{cases}\sqrt{p}\,\varepsilon_p^{-h(p)} & \text{if } (\frac{a}{p})=1,\\ -\sqrt{p}\,N(\varepsilon_p)^{-h(p)}\varepsilon_p^{h(p)} & \text{if } (\frac{a}{p})=-1.\end{cases}\end{aligned}$$

This proves (1.10) since $N(\varepsilon_p)^{h(p)}=-1$ (cf. Corollary 1.1 of [S13] and its proof).

Now we consider the case $p\equiv 3 \pmod 4$. In view of (3.4),

$$\begin{aligned}ph(-p)=&-\sum_{r=1}^{(p-1)/2}\left(r\left(\frac{r}{p}\right)+(p-r)\left(\frac{p-r}{p}\right)\right)\\=&-2\sum_{r=1}^{(p-1)/2}r\left(\frac{r}{p}\right)+p\sum_{k=1}^{(p-1)/2}\left(\frac{r}{p}\right)\end{aligned}$$

and hence $p\mid\sum_{r=1}^{(p-1)/2}r(\frac{r}{p})$. Let $N=|\{1\leqslant r\leqslant (p-1)/2:\ (\frac{r}{p})=-1\}|$. Observe that

$$\begin{aligned}\prod_{k=1}^{(p-1)/2}(1-\zeta^{k^2})=&\prod_{k=1}^{(p-1)/2}(1-\zeta^{(2k)^2})\\=&\prod_{\substack{r=1\\(\frac{r}{p})=1}}^{(p-1)/2}(1-\zeta^{4r})\times\prod_{\substack{r=1\\(\frac{r}{p})=-1}}^{(p-1)/2}(1-\zeta^{4(p-r)})\\=&\prod_{\substack{r=1\\(\frac{r}{p})=1}}^{(p-1)/2}(1-\zeta^{4r})\times\prod_{\substack{r=1\\(\frac{r}{p})=-1}}^{(p-1)/2}\frac{\zeta^{4r}-1}{\zeta^{4r}}\\=&(-1)^N\zeta^{-4\sum_{0<r<p/2,\,(\frac{r}{p})=-1}r}\prod_{r=1}^{(p-1)/2}\zeta^{2r}(\zeta^{-2r}-\zeta^{2r})\\=&(-1)^N\zeta^{\sum_{r=1}^{(p-1)/2}2r(\frac{r}{p})}\prod_{r=1}^{(p-1)/2}(\zeta^{-2r}-\zeta^{2r})\\=&(-1)^N\prod_{r=1}^{(p-1)/2}(\zeta^{-2r}-\zeta^{2r})\end{aligned}$$

and hence

$$(-1)^N\prod_{k=1}^{(p-1)/2}(1-\zeta^{k^2})=(-1)^{(p-1)/2}\prod_{r=1}^{(p-1)/2}(\zeta^{2r}-\zeta^{-2r}).\tag{3.9}$$

By Prop. 6.4.3 of [IR, p. 74],

$$\prod_{r=1}^{(p-1)/2}(\zeta^{2r-1}-\zeta^{-(2r-1)})=\sqrt{p}\,i.$$

Thus

$$\sqrt{p}\,i\prod_{r=1}^{(p-1)/2}(\zeta^{2r}-\zeta^{-2r})=\prod_{k=1}^{p-1}(\zeta^k-\zeta^{-k})=\zeta^{\sum_{k=1}^{p-1}(-k)}\prod_{k=1}^{p-1}(1-\zeta^{2k})=p$$

with the help of (3.1). Combining this with (3.9) we obtain

$$(-1)^N\prod_{k=1}^{(p-1)/2}(1-\zeta^{k^2})=\sqrt{p}\,i.$$

Therefore, by using (3.7) we get

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

This yields (1.11) since $N\equiv(h(-p)+1)/2 \pmod 2$ by (3.5).

(ii) Observe that

$$\begin{aligned}&\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})^2\\ =&(-1)^{\binom{(p-1)/2}{2}}\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})(\zeta^{ak^2}-\zeta^{aj^2})\\ =&(-1)^{\binom{(p-1)/2}{2}}\prod_{k=1}^{(p-1)/2}\prod_{\substack{j=1\\ j\neq k}}^{(p-1)/2}(\zeta^{ak^2}-\zeta^{aj^2})\\ =&(-1)^{\binom{(p-1)/2}{2}}\prod_{k=1}^{(p-1)/2}\left((\zeta^{ak^2})^{(p-3)/2}\prod_{\substack{j=1\\ j\neq k}}^{(p-1)/2}(1-\zeta^{a(j^2-k^2)})\right)\\ =&(-1)^{(p-1)(p-3)/8}\zeta^{\frac{p-3}{2}\sum_{k=1}^{(p-1)/2}ak^2}\prod_{\substack{j,k=1\\ j\neq k}}^{(p-1)/2}(1-\zeta^{a(j^2-k^2)}).\end{aligned}$$

Clearly,

$$\sum_{k=1}^{(p-1)/2}k^2=\frac{p^2-1}{24}p\equiv 0 \pmod p. \tag{3.10}$$

So, with the help of Lemma 3.2, from the above we obtain

$$\begin{aligned}\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})^2=&(-1)^{(p-1)(p-3)/8}\prod_{n=1}^{p-1}(1-\zeta^{an})^{\lfloor (p-1)/4\rfloor}\\ &\times\begin{cases}\prod_{0<n<p,\ (\frac{n}{p})=1}(1-\zeta^{an})^{-1} & \text{if } p\equiv 1 \pmod 4,\\ 1 & \text{if } p\equiv 3 \pmod 4.\end{cases}\end{aligned}$$

Noting (1.11) and (3.1) we get

$$\begin{aligned}&\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})^2\\&=(-1)^{(p-1)(p-3)/8}p^{(p-3)/4}\times\begin{cases}\varepsilon_p^{(\frac{a}{p})h(p)} & \text{if } p\equiv 1\pmod 4,\\ 1 & \text{if } p\equiv 3\pmod 4.\end{cases}\end{aligned}\tag{3.11}$$

Thus (1.12) holds when $p\equiv 1 \pmod 4$.

Below we suppose $p\equiv 3 \pmod 4$ and want to show (1.13). By (3.11) with $a=1$, for some $\varepsilon\in\{\pm1\}$, we have

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

In view of (3.7), this yields that

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})=\varepsilon\varphi_a(\sqrt{p}\,i)^{(p-3)/4}=\varepsilon\left(\left(\frac{a}{p}\right)\sqrt{p}\,i\right)^{(p-3)/4}.\tag{3.12}$$

As $i^{(p-3)/4}=(-1)^{(p-7)/8}i$ if $p\equiv 7 \pmod 8$, we obtain (1.13) from (3.12) provided that

$$\varepsilon=\begin{cases}1 & \text{if } p\equiv 3\pmod 8,\\ (-1)^{(h(-p)+1)/2} & \text{if } p\equiv 7\pmod 8.\end{cases}\tag{3.13}$$

Now it remains to show (3.13). By (3.12), for any $r=1,\ldots,(p-1)/2$ we have

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

on the other hand,

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

Combining these and noting (3.10) and (1.10), we find that

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

Therefore

$$\varepsilon^{(p-1)/2}=(-1)^{\frac{h(-p)+1}{2}\cdot\frac{(p-1)(p-3)}{8}}\prod_{1\leqslant j<k\leqslant(p-1)/2}\left(\frac{k^2-j^2}{p}\right)=(-1)^{\frac{h(-p)+1}{2}\cdot\frac{p-3}{4}}$$

with the help of (1.5). This proves the desired (3.13) since $\varepsilon=\varepsilon^{(p-1)/2}$.

The proof of Theorem 1.3 is now complete. □

4. Proofs of Theorems 1.4 and 1.5

Lemma 4.1. *Let p be any odd prime. Then*

$$\sum_{1\leqslant j<k\leqslant (p-1)/2}(j^2+k^2)\equiv\begin{cases}p\pmod{2p}&\text{if } p\equiv 5\pmod 8,\\ 0\pmod{2p}&\text{otherwise.}\end{cases}\tag{4.1}$$

Proof. Since

$$\begin{aligned}&2\sum_{1\leqslant j<k\leqslant (p-1)/2}(j^2+k^2)+\sum_{k=1}^{(p-1)/2}(k^2+k^2)\\ =&\sum_{j=1}^{(p-1)/2}\sum_{k=1}^{(p-1)/2}(j^2+k^2)=(p-1)\sum_{k=1}^{(p-1)/2}k^2,\end{aligned}$$

we have

$$\sum_{1\leqslant j<k\leqslant (p-1)/2}(j^2+k^2)=\frac{p-3}{2}\sum_{k=1}^{(p-1)/2}k^2=\frac{p-3}{2}\cdot\frac{p^2-1}{24}p\equiv 0\pmod p.$$

Note that

$$\frac{p-3}{2}\cdot\frac{p^2-1}{24}\equiv\begin{cases}(p-1)/4\pmod 2&\text{if } p\equiv 1\pmod 4,\\ 0\pmod 2&\text{if } p\equiv 3\pmod 4.\end{cases}$$

Therefore (4.1) holds. □

Proof of Theorem 1.3. For $1\leqslant j<k\leqslant (p-1)/2$, clearly

$$\{j^2\}_p>\{k^2\}_p\iff \cot\pi\frac{j^2}{p}-\cot\pi\frac{k^2}{p}<0$$

and

$$\{k^2-j^2\}_p>\frac p2\iff \sin 2\pi\frac{k^2-j^2}{p}<0\iff \csc 2\pi\frac{k^2-j^2}{p}<0.$$

So (1.18) follows from (1.19). As (1.19) holds trivially for $p=3$, below we assume $p>3$.

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

$$\begin{aligned}\sin\pi\frac{a(k^2-j^2)}{p}=&\frac{e^{i\pi a(k^2-j^2)/p}-e^{-i\pi a(k^2-j^2)/p}}{2i}\\ =&\frac i2 e^{-i\pi a(k^2+j^2)/p}(e^{2\pi i a j^2/p}-e^{2\pi i a k^2/p}).\end{aligned}$$

Combining this with Lemma 4.1, we see that

$$\begin{aligned}&\prod_{1\leqslant j<k\leqslant(p-1)/2}\sin\pi\frac{a(k^2-j^2)}{p}\\=&(-1)^{a\frac{p+1}{2}\lfloor\frac{p-1}{4}\rfloor}\left(\frac{i}{2}\right)^{(p-1)(p-3)/8}\prod_{1\leqslant j<k\leqslant(p-1)/2}(e^{2\pi iaj^2/p}-e^{2\pi iak^2/p})\end{aligned}\tag{4.2}$$

For real numbers θ_1 and θ_2, clearly

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

Thus

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

and hence by (1.14) we have

$$\begin{aligned}&\prod_{1\leqslant j<k\leqslant(p-1)/2}\sin\pi\frac{a(k^2-j^2)}{p}\Bigg/\prod_{1\leqslant j<k\leqslant(p-1)/2}\left(\cot\pi\frac{aj^2}{p}-\cot\frac{ak^2}{p}\right)\\=&\left(\frac{p}{2^{p-1}}\right)^{(p-3)/4}\times\begin{cases}(-1)^{(a-1)(p-1)/4}\varepsilon_p^{-(\frac{a}{p})\frac{p-3}{2}h(p)}&\text{if }p\equiv1\pmod 4,\\1&\text{if }p\equiv3\pmod 4.\end{cases}\end{aligned}\tag{4.3}$$

So it suffices to determine $\prod_{1\leqslant j<k\leqslant(p-1)/2}\sin\pi a(k^2-j^2)/p$.

Case 1. $p\equiv3\pmod 4$.

In this case, by combining (4.2) and (1.13) we get

$$\begin{aligned}&\prod_{1\leqslant j<k\leqslant(p-1)/2}\sin\pi\frac{a(k^2-j^2)}{p}\\=&\left(\frac{p}{2^{p-1}}\right)^{(p-3)/8}\times\begin{cases}1&\text{if }p\equiv3\pmod 8,\\(-1)^{(h(-p)+1)/2}(\frac{a}{p})&\text{if }p\equiv7\pmod 8.\end{cases}\end{aligned}$$

Thus (1.19)is valid.

Case 2. $p\equiv1\pmod 4$.

In this case, combining (4.12) with (1.12) we obtain

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}\sin^2\pi\frac{a(k^2-j^2)}{p}=\left(\frac{p}{2^{p-1}}\right)^{(p-3)/4}\varepsilon_p^{(\frac{a}{p})h(p)}\tag{4.4}$$

and hence

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}\csc\pi\frac{a(k^2-j^2)}{p}=\pm(2^{p-1}p^{-1})^{(p-3)/8}\varepsilon_p^{-(\frac{a}{p})h(p)/2}.$$

In view of (4.3), we have

$$\begin{aligned}&\prod_{1\leqslant j<k\leqslant(p-1)/2}\left(\sin\pi\frac{a(k^2-j^2)}{p}\right)\left(\cot\pi\frac{aj^2}{p}-\cot\frac{ak^2}{p}\right)\\ =&(-1)^{(a-1)(p-1)/4}(2^{p-1}p^{-1})^{(p-3)/4}\varepsilon_p^{(\frac{a}{p})\frac{p-3}{2}h(p)}\prod_{1\leqslant j<k\leqslant(p-1)/2}\sin^2\pi\frac{a(k^2-j^2)}{p}.\end{aligned}$$

Combining this with (4.4) we immediately get the first equality in (1.20).

The proof of Theorem 1.4 is now complete. □

Proof of Theorem 1.5. (1.21) is trivial for $p=3$. Below we assume $p>3$. In view of (4.2),

$$\begin{aligned}\prod_{1\leqslant j<k\leqslant(p-1)/2}\left(2\cos\pi\frac{a(k^2-j^2)}{p}\right)=&\prod_{1\leqslant j<k\leqslant(p-1)/2}\frac{\sin\pi(2a)(k^2-j^2)/p}{\sin\pi a(k^2-j^2)/p}\\ =&(-1)^{a\frac{p+1}{2}\lfloor\frac{p-1}{4}\rfloor}\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}+\zeta^{ak^2}).\end{aligned}$$

So we have the first equality in (1.21). On the other hand, by Theorem 1.4 we have

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}\frac{\csc\pi a(k^2-j^2)/p}{\csc\pi(2a)(k^2-j^2)/p}=\begin{cases}1&\text{if }p\equiv3\pmod 4,\\ \pm\varepsilon_p^{(\frac{a}{p})h(p)((\frac{2}{p})-1)/2}&\text{if }p\equiv1\pmod 4.\end{cases}$$

Therefore (1.21) holds.

The proof of Theorem 1.5 is now complete. □

5. Proof of Theorem 1.6

Lemma 5.1. *Let p be an odd prime. Then*

$$\frac{1}{p}\sum_{\substack{1\leqslant j<k\leqslant(p-1)/2\\ p\mid j^2+k^2}}(j^2+k^2)\equiv\begin{cases}1\pmod 2&\text{if }p\equiv5\pmod 8,\\ 0\pmod 2&\text{otherwise.}\end{cases}\tag{5.1}$$

Proof. If $p\equiv3\pmod 4$, then $(\frac{-1}{p})=-1$ and $j^2+k^2\not\equiv0\pmod p$ for any $j,k=1,\dots,(p-1)/2$. So (5.1) is trivial in the case $p\equiv3\pmod 4$.

Now assume that $p \equiv 1 \pmod 4$. Then $q^2 \equiv -1 \pmod p$ for some $q \in \mathbb{Z}$. For each $j = 1, \ldots, (p-1)/2$ let j_* be the unique integer $r \in \{1, \ldots, (p-1)/2\}$ with qj congruent to r or $-r$ modulo p. Clearly, $\{j_* :\ 1 \leqslant j \leqslant (p-1)/2\} = \{1, \ldots, (p-1)/2\}$. Thus

$$\begin{aligned}\sum_{\substack{1\leqslant j<k\leqslant(p-1)/2\\ p\mid j^2+k^2}} (j^2+k^2) =& \frac{1}{2}\sum_{\substack{j,k=1\\ p\mid j^2+k^2}}^{(p-1)/2} (j^2+k^2)\\ =& \frac{1}{2}\sum_{j=1}^{(p-1)/2} (j^2+j_*^2) = \sum_{k=1}^{(p-1)/2} k^2 = \frac{p^2-1}{24}p\end{aligned}$$

and hence

$$\frac{1}{p}\sum_{\substack{1\leqslant j<k\leqslant(p-1)/2\\ p\mid j^2+k^2}} (j^2+k^2) = \frac{p^2-1}{24} \equiv \frac{p^2-1}{8} \equiv \frac{p-1}{4} \pmod 2.$$

Therefore (5.1) holds. $\square$

Proof of Theorem 1.6(i). Let $\zeta = e^{2\pi i/p}$. As

$$\sum_{\substack{1\leqslant j<k\leqslant(p-1)/2\\ p\nmid j^2+k^2}} (j^2+k^2) \equiv 0 \pmod{2p}$$

by Lemmas 4.1 and 5.1, we have

$$\begin{aligned}\prod_{\substack{1\leqslant j<k\leqslant(p-1)/2\\ p\nmid j^2+k^2}} \sin\pi\frac{a(j^2+k^2)}{p} =& \prod_{\substack{1\leqslant j<k\leqslant(p-1)/2\\ p\nmid j^2+k^2}} \frac{-e^{-i\pi a(j^2+k^2)/p}}{2i}(1-\zeta^{a(j^2+k^2)})\\ =& \left(\frac{i}{2}\right)^{|\{(j,k):\ 1\leqslant j<k\leqslant(p-1)/2\ \&\ p\nmid j^2+k^2\}|} f(a)\end{aligned}$$

where

$$f(a) := \prod_{n=1}^{p-1}(1-\zeta^{an})^{r(n)}$$

with $r(n)$ defined as in Lemma 2.3. Note that

$$\begin{aligned}&\left|\left\{(j,k):\ 1\leqslant j<k\leqslant\frac{p-1}{2}\ \&\ p\nmid j^2+k^2\right\}\right|\\ =&\binom{(p-1)/2}{2} - r(0) = \frac{p-1}{2}\left\lfloor\frac{p-3}{4}\right\rfloor\end{aligned} \tag{5.2}$$

with the help of (2.6). So

$$\prod_{\substack{1\leqslant j<k\leqslant (p-1)/2\\ p\nmid j^2+k^2}}\sin\pi\frac{a(j^2+k^2)}{p}=\left(\frac{i}{2}\right)^{\frac{p-1}{2}\lfloor\frac{p-3}{4}\rfloor}f(a).\tag{5.3}$$

By (2.7), (3.1) and Theorem 1.4(i), we have

$$\begin{aligned}f(a)=&p^{\lfloor (p+1)/8\rfloor}\prod_{\substack{n=1\\ (\frac{n}{p})=1}}^{p-1}(1-\zeta^{an})^{-(1+(\frac{2}{p}))/2}\\ =&\begin{cases}p^{\lfloor (p+1)/8\rfloor}&\text{if } p\equiv 3,5\pmod 8,\\ p^{\lfloor (p+1)/8\rfloor-1/2}\varepsilon_p^{(\frac{a}{p})h(p)}&\text{if } p\equiv 1\pmod 8,\\ (-1)^{(h(-p)-1)/2}(\frac{a}{p})p^{\lfloor (p+1)/8\rfloor-1/2}i&\text{if } p\equiv 7\pmod 8.\end{cases}\end{aligned}$$

Combining this with (5.3) we immediately get (1.23).

In light of (1.23) and (5.2),

$$\begin{aligned}\prod_{\substack{1\leqslant j<k\leqslant (p-1)/2\\ p\nmid j^2+k^2}}\cos\pi\frac{a(j^2+k^2)}{p}=&\prod_{\substack{1\leqslant j<k\leqslant (p-1)/2\\ p\nmid j^2+k^2}}\frac{\sin\pi(2a)(j^2+k^2)/p}{2\sin\pi a(j^2+k^2)/p}\\ =&2^{-|\{(j,k):\ 1\leqslant j<k\leqslant (p-1)/2\ \&\ p\nmid j^2+k^2\}|}\\ =&2^{-\frac{p-1}{2}\lfloor\frac{p-3}{4}\rfloor}.\end{aligned}$$

Note also that

$$\begin{aligned}&\prod_{\substack{1\leqslant j<k\leqslant (p-1)/2\\ p\mid j^2+k^2}}\cos\pi\frac{a(j^2+k^2)}{p}\\ =&(-1)^{\sum_{1\leqslant j<k\leqslant (p-1)/2\ \&\ p\mid j^2+k^2}a(j^2+k^2)/p}=(-1)^{a\frac{p+1}{2}\lfloor\frac{p-1}{4}\rfloor}\end{aligned}$$

by Lemma 5.1. Therefore (1.24) holds.

Observe that

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

and

$$\prod_{\substack{1\leqslant j<k\leqslant (p-1)/2\\ p\nmid j^2+k^2}}\left(\sin\pi\frac{aj^2}{p}\right)\left(\sin\pi\frac{ak^2}{p}\right)=\prod_{k=1}^{(p-1)/2}\left(\sin\pi\frac{ak^2}{p}\right)^{(p-(\frac{-1}{p})-4)/2}.$$

Combining these with (1.23) and (1.14), we obtain the desired (1.25). This concludes the proof of Theorem 1.6(i). □

Lemma 5.2. *Let p be an odd prime and let $a,b,c\in\mathbb{Z}$ with $p\nmid a$. Then*

$$\sum_{1\leqslant j<k\leqslant p-1}(aj^2+bjk+ck^2)\equiv 0 \pmod p \tag{5.4}$$

and also

$$\frac{1}{p}\sum_{1\leqslant j<k\leqslant p-1}(aj^2+bjk+ck^2)\equiv a\frac{p-1}{2}+b\frac{(p-1)(p-3)}{8} \pmod 2. \tag{5.5}$$

Proof. Let $\Delta=b^2-4ac$. In view of (3.10), we have

$$\begin{aligned}&\sum_{1\leqslant j<k\leqslant p-1}(aj^2+bjk+ck^2)\\ =&\sum_{1\leqslant j<k\leqslant (p-1)/2}(aj^2+bjk+ck^2)\\ &+\sum_{1\leqslant k\leqslant (p-1)/2}\ \sum_{k<j\leqslant p-1}(a(p-j)^2+b(p-j)(p-k)+c(p-k)^2)\\ \equiv&\sum_{k=1}^{(p-1)/2}\left(\sum_{j=0}^{p-1}(aj^2+bjk+ck^2)-ck^2-(a+b+c)k^2\right)\\ \equiv&\sum_{k=1}^{(p-1)/2}\sum_{j=0}^{p-1}\frac{1}{4a}\left((2aj+bk)^2-\Delta k^2\right)\equiv\sum_{k=1}^{(p-1)/2}\frac{1}{4a}\sum_{r=0}^{p-1}r^2\equiv 0 \pmod p.\end{aligned}$$

This proves (5.4).

Observe that

$$\begin{aligned}&\sum_{1\leqslant j<k\leqslant p-1}(aj^2+bjk+ck^2)\\ \equiv&\sum_{1\leqslant j<k\leqslant p-1}(aj+ck)+b\sum_{1\leqslant j<k\leqslant (p-1)/2}(2j-1)(2k-1)\\ \equiv&\sum_{k=1}^{p-1}\left(\sum_{0<j<k}aj+ck(k-1)\right)+b\binom{(p-1)/2}{2}\\ \equiv&\sum_{k=1}^{p-1}\frac{a}{2}(k^2-k)+b\frac{(p-1)(p-3)}{8} \pmod 2\end{aligned}$$

and hence

$$\begin{aligned}&\sum_{1\leqslant j<k\leqslant p-1}(aj^2+bjk+ck^2)-b\frac{(p-1)(p-3)}{8}\\ \equiv&\frac{a}{2}\left(\frac{(p-1)p(2p-1)}{6}-\frac{(p-1)p}{2}\right)=a\frac{p(p-1)(p-2)}{6}\equiv a\frac{p-1}{2} \pmod 2.\end{aligned}$$

Therefore (5.5) also holds. □

Proof of Theorem 1.6(ii). By Lemma 2.4,

$$\begin{aligned}&\left|\{(j,k):\ 1\leqslant j<k\leqslant p-1 \text{ and } p\nmid aj^2+bjk+ck^2\}\right|\\ =&\binom{p-1}{2}-\frac{p-1}{2}\left(1+\left(\frac{\Delta}{p}\right)\right)=\frac{p-1}{2}\left(p-3-\left(\frac{\Delta}{p}\right)\right).\end{aligned}\tag{5.6}$$

Let $\zeta=e^{2\pi i/p}$. Then

$$\begin{aligned}&\prod_{\substack{1\leqslant j<k\leqslant p-1\\ p\nmid aj^2+bjk+ck^2}}\sin\pi\frac{aj^2+bjk+ck^2}{p}\\ =&\prod_{\substack{1\leqslant j<k\leqslant p-1\\ p\nmid aj^2+bjk+ck^2}}\frac{-e^{-i\pi(aj^2+bjk+ck^2)/p}}{2i}(1-\zeta^{aj^2+bjk+ck^2})\\ =&\left(\frac{i}{2}\right)^{\frac{p-1}{2}(p-3-(\frac{\Delta}{p}))}(-1)^{a(p-1)/2+b(p-1)(p-3)/8-m}\\ &\times\prod_{\substack{1\leqslant j<k\leqslant p-1\\ p\nmid aj^2+bjk+ck^2}}(1-\zeta^{aj^2+bjk+ck^2})\end{aligned}$$

with the help of Lemma 5.2. In view of Lemma 2.4, (3.1) and Theorem 1.3(i), we have

$$\begin{aligned}&\prod_{\substack{1\leqslant j<k\leqslant p-1\\ p\nmid aj^2+bjk+ck^2}}(1-\zeta^{aj^2+bjk+ck^2})\\ =&\frac{\prod_{n=1}^{p-1}(1-\zeta^n)^{(p-3-(\frac{\Delta}{p})+(1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))/2}}{\prod_{n=1}^{p-1}(1-\zeta^n)^{((1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))(1+(\frac{n}{p}))/2}}\\ =&\frac{p^{(p-3-(\frac{\Delta}{p})+(1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))/2}}{\prod_{k=1}^{(p-1)/2}(1-\zeta^{k^2})^{(1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p})}}\\ =&p^{(p-3-(\frac{\Delta}{p})/2}\\ &\times\begin{cases}\varepsilon_p^{h(p)((1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))}&\text{if } p\equiv 1\pmod 4,\\ ((-1)^{(h(-p)-1)/2}i)^{(1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p})}&\text{if } p\equiv 3\pmod 4.\end{cases}\end{aligned}$$

Therefore

$$\begin{aligned}&(-1)^m\prod_{\substack{1\leqslant j<k\leqslant p-1\\ p\nmid aj^2+bjk+ck^2}}\sin\pi\frac{aj^2+bjk+ck^2}{p}\\ =&(-1)^{a(p-1)/2+b(p-1)(p-3)/8}i^{\frac{p-1}{2}(p-3-(\frac{\Delta}{p}))}\left(\frac{p}{2^{p-1}}\right)^{(p-3-(\frac{\Delta}{p}))/2}\\ &\times\begin{cases}\varepsilon_p^{h(p)((1-p+p(\frac{\Delta}{p})^2)(\frac{a}{p})+(\frac{c}{p})+(\frac{a+b+c}{p}))}&\text{if } p\equiv 1\pmod 4,\\ (-1)^{(\frac{\Delta}{p})\frac{h(-p)-1}{2}+\frac{1-p}{2}(\frac{a}{p})+\frac{1}{2}((\frac{c}{p})+(\frac{a+b+c}{p}))}i^{p(\frac{\Delta}{p})^2(\frac{a}{p})}&\text{if } p\equiv 3\pmod 4.\end{cases}\end{aligned}$$

It is easy to see that this implies (1.27).

Clearly,

$$\prod_{\substack{1\leqslant j<k\leqslant p-1\\ p\mid aj^2+bjk+ck^2}}\cos\pi\frac{aj^2+bjk+ck^2}{p}=\prod_{\substack{1\leqslant j<k\leqslant p-1\\ p\mid aj^2+bjk+ck^2}}(-1)^{(aj^2+bjk+ck^2)/p}=(-1)^m.$$

On the other hand, by (5.6) we have

$$\begin{aligned}&2^{\frac{p-1}{2}(p-3-(\frac{\Delta}{p}))}\prod_{\substack{1\leqslant j<k\leqslant p-1\\ p\nmid aj^2+bjk+ck^2}}\cos\pi\frac{aj^2+bjk+ck^2}{p}\\ &=\prod_{\substack{1\leqslant j<k\leqslant p-1\\ p\nmid aj^2+bjk+ck^2}}\frac{\sin\pi(2aj^2+2bjk+2ck^2)/p}{\sin\pi(aj^2+bjk+ck^2)/p}.\end{aligned}$$

Combining these with (1.27) we immediately obtain the desired (1.28).

In view of the above, we have completed the proof of Theorem 1.6(ii). □

6. Some conjectures

We are unable to determine the parity of $s(p)$ and $t(p)$ (defined by (1.16) and (1.17)) for a general prime $p\equiv 1 \pmod 4$. However, in contrast with (1.18), we formulate the following conjecture.

Conjecture 6.1. *For any prime $p\equiv 1 \pmod 4$, we have*

$$s(p)+t(p)\equiv\left|\left\{1\leqslant k<\frac{p}{4}:\ \left(\frac{k}{p}\right)=1\right\}\right| \pmod 2. \tag{6.1}$$

For any odd prime p and integer k, we let $R(k,p)$ denote the unique $r\in\{0,\ldots,(p-1)/2\}$ with k congruent to r or $-r$ modulo p. For example,

$$R(1^2,11)=1,\ R(2^2,11)=4,\ R(3^2,11)=2,\ R(4^2,11)=5,\ R(5^2,11)=3.$$

Motivated by Theorem 1.4 and Corollary 1.3, we pose the following conjecture.

Conjecture 6.2. *Let p be an odd prime, and let $a\in\mathbb{Z}$ with $p\nmid a$. Then*

$$\left|\left\{(i,j):\ 1\leqslant i<j\leqslant\frac{p-1}{2}\ \text{and}\ R(ai^2,p)>R(aj^2,p)\right\}\right|\equiv\left\lfloor\frac{p+1}{8}\right\rfloor \pmod 2, \tag{6.2}$$

and

$$\begin{aligned}&(-1)^{|\{1\leqslant i<j\leqslant(p-1)/2:\ R(ai^2,p)+R(aj^2,p)>p/2\}|}\\ &=\begin{cases}(-1)^{|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}(\frac{a}{p})^{(1-(\frac{2}{p}))/2} & \text{if } p\equiv 1 \pmod 4,\\ 1 & \text{if } p\equiv 3 \pmod 4.\end{cases}\end{aligned} \tag{6.3}$$

Remark 6.1. We have verified (6.2) and (6.3) with $a=1$ for all odd primes $p<20000$.

Conjecture 6.3. *Let $p>3$ be a prime. If $p\equiv 3\pmod 4$, then*

$$\begin{aligned}&(-1)^{|\{(j,k):\ 1\leqslant j<k\leqslant (p-1)/2\ \&\ \{j(j+1)/2\}_p>\{k(k+1)/2\}_p\}|}\\&\quad=(-1)^{\frac{h(-p)+1}{2}+|\{1\leqslant k\leqslant\lfloor\frac{p+1}{8}\rfloor:\ (\frac kp)=1\}|}.\end{aligned}\tag{6.4}$$

Also,

$$\begin{aligned}&(-1)^{|\{(j,k):\ 1\leqslant j<k\leqslant (p-1)/2\ \&\ \{j(j+1)/2\}_p+\{k(k+1)/2\}_p>p\}|}\\&=\begin{cases}(-1)^{(p-1)/8}&\text{if } p\equiv 1\pmod 8,\\(-1)^{|\{1\leqslant k<\frac p4:\ (\frac kp)=-1\}|}&\text{if } p\equiv 5\pmod 8,\\(-1)^{\frac{h(-p)+1}{2}+|\{1\leqslant k\leqslant\lfloor\frac{p+1}{8}\rfloor:\ (\frac kp)=-1\}|}&\text{if } p\equiv 3\pmod 4.\end{cases}\end{aligned}\tag{6.5}$$

Conjecture 6.4. *Let p be an odd prime. If $p\equiv 3\pmod 4$, then*

$$(-1)^{|\{(j,k):\ 1\leqslant j<k\leqslant (p-1)/2 \text{ and } \{j(j+1)\}_p>\{k(k+1)\}_p\}|}=(-1)^{\lfloor (p+1)/8\rfloor}.\tag{6.6}$$

Also,

$$\begin{aligned}&(-1)^{|\{(j,k):\ 1\leqslant j<k\leqslant (p-1)/2\ \&\ \{j(j+1)\}_p+\{k(k+1)\}_p>p\}|}\\&=\begin{cases}(-1)^{\lfloor (p-1)/8\rfloor}&\text{if } p\equiv 1\pmod 4,\\(-1)^{(h(-p)+1)/2}&\text{if } p>3\ \&\ p\equiv 3\pmod 8,\\1&\text{if } p\equiv 7\pmod 8.\end{cases}\end{aligned}\tag{6.7}$$

Conjecture 6.5. (i) *For any prime $p\equiv 5\pmod 6$, we have*

$$\left|\left\{1\leqslant k\leqslant\frac{p-1}{2}:\ \{k^3\}_p>\frac p2\right\}\right|-\frac{p+1}{6}\in 2\mathbb N=\{0,2,4,6,\ldots\}\tag{6.8}$$

and

$$|\{(j,k):\ 1\leqslant j<k\leqslant p-1 \text{ and } \{j^3\}_p>\{k^3\}_p\}|\equiv\frac{p+1}{6}\pmod 2.\tag{6.9}$$

(ii) *For any odd prime $p\not\equiv 1\pmod 5$, we have*

$$\left|\left\{1\leqslant k\leqslant\frac{p-1}{2}:\ \{k^5\}_p>\frac p2\right\}\right|\equiv 0\pmod 2.\tag{6.10}$$

(iii) *For any prime $p\equiv 5\pmod{12}$, we have*

$$\left|\left\{1\leqslant k\leqslant\frac{p-1}{2}:\ \{k^6\}_p>\frac p2\right\}\right|-\frac{p-5}{12}\in\{2n+1:\ n\in\mathbb N\}.\tag{6.11}$$

Remark 6.2. Let p be a prime with $p\equiv 5\pmod 6$. The list $\{1^3\}_p,\ldots,\{(p-1)^3\}_p$ is a permutation of $1,\ldots,p-1$, for, if $1\leqslant j<k\leqslant p-1$ then

$$j^3-k^3=(j-k)(j^2+jk+k^2)=\frac{j-k}{4}((2j+k)^2+3k^2)\not\equiv 0\pmod p.$$

See [S18, A320044] for some data related to (6.8). Note that (6.8) implies (6.9) since for any $1\leqslant j<k\leqslant p-1$ we have $1\leqslant p-k<p-j\leqslant p-1$ and

$$(\{j^3\}_p-\{k^3\}_p)(\{(p-k)^3\}_p-\{(p-j)^3\}_p)<0.$$

Conjecture 6.6. *Let p be an odd prime. Then*

$$\begin{aligned}&\left|\left\{(j,k):\ 1\leqslant j<k\leqslant\frac{p-1}{2}\ \text{and}\ \{j^4\}_p>\{k^4\}_p\right\}\right|\\&\equiv\left\lfloor\frac{p+1}{8}\right\rfloor+\begin{cases}(h(-p)+1)/2\pmod 2&\text{if}\ p\equiv 7\pmod 8,\\0\pmod 2&\text{otherwise.}\end{cases}\end{aligned}\tag{6.12}$$

Also,

$$\begin{aligned}&\left|\left\{(j,k):\ 1\leqslant j<k\leqslant\frac{p-1}{2}\ \text{and}\ \{j^8\}_p>\{k^8\}_p\right\}\right|\\&\equiv\begin{cases}|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=1\}|\pmod 2&\text{if}\ p\equiv 1\pmod 8,\\0\pmod 2&\text{if}\ p\equiv 3\pmod 8,\\(p-5)/8\pmod 2&\text{if}\ p\equiv 5\pmod 8,\\(h(-p)+1)/2\pmod 2&\text{if}\ p\equiv 7\pmod 8.\end{cases}\end{aligned}\tag{6.13}$$

Remark 6.3. See [S18, A319882, A319894 and A319903] for related data or similar conjectures.

The following conjecture is motivated by Theorem 1.5.

Conjecture 6.7. *Let p be a prime with $p\equiv 1\pmod 4$, and let $\zeta=e^{2\pi i/p}$. Let a be an integer not divisible by p. Then*

$$\begin{aligned}&(-1)^{|\{1\leqslant k<p/4:\ (\frac{k}{p})=-1\}|}\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}+\zeta^{ak^2})\\&=\begin{cases}1&\text{if}\ p\equiv 1\pmod 8,\\(\frac{a}{p})\varepsilon_p^{-(\frac{a}{p})h(p)}&\text{if}\ p\equiv 5\pmod 8.\end{cases}\end{aligned}\tag{6.14}$$

Remark 6.4. By K. S. Williams and J. D. Currie [WC], for any prime $p\equiv 1\pmod 8$ we have

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

Motivated by (1.19) and (1.20), we pose the following conjecture involving the cotangent function.

Conjecture 6.8. *Let $p>3$ be a prime.*

(i) *Define the matrix T_p by*

$$T_p:=\left[\tan\pi\frac{i^2+j^2}{p}\right]_{0\leqslant i,j\leqslant(p-1)/2}.\tag{6.15}$$

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

$$\det T_p=2^{(p-1)/2}p^{(p+1)/4}. \tag{6.16}$$

(ii) Let T_p^* be the matrix obtaining from T_p via replacing all the entries in the first row by 1. Then

$$\det T_p^*=\begin{cases}(-p)^{(p-1)/4}&\text{if }p\equiv 1\pmod 4,\\ 2^{(p-1)/2}(-p)^{(p-3)/4}\sqrt{p}&\text{if }p\equiv 3\pmod 4.\end{cases} \tag{6.17}$$

Remark 6.5. If $p\equiv 1\pmod 4$ is a prime, then $q^2\equiv -1\pmod p$ for some $q\in\mathbb{Z}$, hence

$$\begin{aligned}-\det T_p&=\det\left[-\tan\pi\frac{i^2+j^2}{p}\right]_{0\leqslant i,j\leqslant (p-1)/2}\\&=\det\left[\tan\pi\frac{(qi)^2+(qj)^2}{p}\right]_{0\leqslant i,j\leqslant (p-1)/2}=\det T_p\end{aligned}$$

and thus $\det T_p=0$.

Conjecture 6.9. *Let p be an odd prime.*

(i) *When* $p\not\equiv 3\pmod 8$, *we have*

$$\det[R(i^2j^2,p)]_{1\leqslant i,j\leqslant (p-1)/2}=0. \tag{6.18}$$

If $p\equiv 1\pmod 4$, *then*

$$\det\left[\left\lfloor\frac{i^2j^2}{p}\right\rfloor\right]_{1\leqslant i,j\leqslant (p-1)/2}=0. \tag{6.19}$$

(ii) *If* $p>7$ *and* $p\equiv 3\pmod 4$, *then*

$$\det\left[\left\lfloor\frac{i^2+j^2}{p}\right\rfloor\right]_{1\leqslant i,j\leqslant (p-1)/2}=\det\left[\left\{\frac{i^2+j^2}{p}\right\}\right]_{1\leqslant i,j\leqslant (p-1)/2}=0. \tag{6.20}$$

References

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

[BC] A. Brunyate and P. L. Clark, *Extending the Zolotarev-Frobenius approach to quadratic reciprocity*, Ramanujan J. **37** (2015), 25–50.

[DH] W. Duke and K. Hopkins, *Quadratic reciprocity in a finite group*, Amer. Math. Monthly **112** (2005), 251–256.

[HS] H. Hu and Z.-W. Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc. **129** (2001), 3471–3478.

[IR] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory (Graduate Texts in Math.; 84), 2nd ed., Springer, New York, 1990.

[M61] L. J. Mordell, *The congruence* $((p-1)/2)! \equiv \pm 1 \pmod p$, Amer. Math. Monthly **68** (1961), 145–146.

[P06] H. Pan, *A remark on Zoloterav's theorem*, preprint, `arXiv:0601026`, 2006.

[S13] Z.-W. Sun, *On some determinants with Legendre symbol entries*, `arXiv:1308.2900`, 2013.

[S18] Z.-W. Sun, Sequences A319311, A319882, A319894, A319903, A320044 in OEIS, `http://oeis.org`.

[Sz] G. J. Szekely (ed.), *Contests in Higher Mathematics*, Springer, New York, 1996.

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

[Z] G. Zolotarev, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Nouvelles Ann. Math. 11(1872), 354–362.