INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus

Mathématique

Qing-Hu Hou, Hao Pan and Zhi-Wei Sun

A new theorem on quadratic residues modulo primes

Volume 360 (2022), p. 1065-1069

https://doi.org/10.5802/crmath.371

Les Comptes Rendus. Mathématique *sont membres du*
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org
e-ISSN : 1778-3569

Comptes Rendus
Mathématique
2022, Vol. 360, p. 1065-1069
https://doi.org/10.5802/crmath.371

Number theory / *Théorie des nombres*

A new theorem on quadratic residues modulo primes

Qing-Hu Hou [a], **Hao Pan** [b] **and Zhi-Wei Sun** [*, c]

[a] School of Mathematics, Tianjin University, Tianjin 300350, People's Republic of China

[b] School of Applied Mathematics, Nanjing University of Finance and Economics, Nanjing 210046, People's Republic of China

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

URL: http://maths.nju.edu.cn/~zwsun

E-mails: qh_hou@tju.edu.cn, haopan79@zoho.com, zwsun@nju.edu.cn

Abstract. Let $p>3$ be a prime, and let $(\frac{\cdot}{p})$ be the Legendre symbol. Let $b\in\mathbb{Z}$ and $\varepsilon\in\{\pm1\}$. We mainly prove that

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

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

2020 Mathematics Subject Classification. 11A15, 11A07, 11R11.

Funding. The first, second and third authors are supported by the National Natural Science Foundation of China (grants 11771330, 12071208 and 11971222, respectively).

Manuscript received 8 March 2022, accepted 26 April 2022.

1. Introduction

The theory of quadratic residues modulo primes plays an important role in fundamental number theory.

Let p be an odd prime and let $a\in\mathbb{Z}$ with $p\nmid a$. By Gauss' Lemma (cf. [4, p. 52]),

$$\left(\frac{a}{p}\right)=(-1)^{|\{1\leqslant k\leqslant\frac{p-1}{2}:\ \{ka\}_p>\frac{p}{2}\}|},$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, and we write $\{x\}_p$ for the least nonnegative residue of an integer x modulo p.

---

[*] Corresponding author.

Let n be any positive odd integer, and let $a \in \mathbb{Z}$ with $\gcd(a(1-a), n) = 1$. In 2020, Z.-W. Sun [6] proved the following new result:

$$(-1)^{|\{1\leqslant k\leqslant \frac{n-1}{2}:\ \{ka\}_n>k\}|} = \left(\frac{2a(1-a)}{n}\right),$$

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

Let p be an odd prime and let $a, b \in \mathbb{Z}$ with $a(1-a) \not\equiv 0 \pmod p$. By [5, Lemma 2.7], we have

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

In 2019 Z.-W. Sun [5] employed Galois theory to prove that

$$(-1)^{|\{1\leqslant i<j\leqslant \frac{p-1}{2}:\ \{i^2\}_p>\{j^2\}_p\}|} = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(h(-p)+1)/2} & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

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

Motivated by the above work, for an odd prime p and integers a and b, we introduce the notation

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

Example 1. We have $N_7(4,0) = 2$ since

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

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

In this paper we establish the following novel theorem which was conjectured by the first and third authors [3] in 2018.

Theorem 2. *Let $p > 3$ be a prime, and let b be any integer. Set*

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

and

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

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

Example 3. Let's adopt the notation in Theorem 2. For $p = 5$, we have $S = \{1\}$ for any $b \in \mathbb{Z}$, and the set T depends on b as illustrated by the following table:

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

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

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

2. Proof of Theorem 2

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

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

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

Remark 5. This is a known result of Dirichlet (cf. [1, Corollary 5.3.13]).

Lemma 6. *For any prime $p\equiv 3 \pmod 4$ with $p>3$, there are $x,y,z\in\{1,\ldots,p-1\}$ such that*

$$\left(\frac{x}{p}\right)=\left(\frac{x+1}{p}\right)=1,\ -\left(\frac{y}{p}\right)=\left(\frac{y+1}{p}\right)=1,\ \textit{and}\ \left(\frac{z}{p}\right)=-\left(\frac{z+1}{p}\right)=1.$$

Proof. By a known result (see, e.g., [2, pp. 64–65]), we have

$$\left|\left\{x\in\{1,\ldots,p-2\}:\ \left(\frac{x}{p}\right)=\left(\frac{x+1}{p}\right)=1\right\}\right|=\frac{p-3}{4}>0.$$

Hence

$$\begin{aligned}\left|\left\{y\in\{1,\ldots,p-2\}:\ -\left(\frac{y}{p}\right)=\left(\frac{y+1}{p}\right)=1\right\}\right|&=\left|\left\{y\in\{1,\ldots,p-2\}:\ \left(\frac{y+1}{p}\right)=1\right\}\right|-\frac{p-3}{4}\\&=\frac{p-1}{2}-1-\frac{p-3}{4}=\frac{p-3}{4}>0\end{aligned}$$

and

$$\begin{aligned}\left|\left\{z\in\{1,\ldots,p-2\}:\ \left(\frac{z}{p}\right)=-\left(\frac{z+1}{p}\right)=1\right\}\right|&=\left|\left\{z\in\{1,\ldots,p-2\}:\ \left(\frac{z}{p}\right)=1\right\}\right|-\frac{p-3}{4}\\&=\frac{p-1}{2}-\frac{p-3}{4}=\frac{p+1}{4}>0.\end{aligned}$$

Now the desired result immediately follows. □

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

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

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

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

Suppose that $(\frac{a}{p})=\varepsilon$ with $\varepsilon\in\{\pm1\}$. Then

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

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

If $\varepsilon = 1$, then

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

does not depend on b.

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

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

thus

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

and

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

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

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

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

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

Thus

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

and hence

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

By Lemma 6, for some $a \in \{2,\dots,p-2\}$ we have $\left(\frac{a-1}{p}\right) = \left(\frac{a}{p}\right) = 1$ and hence $\left(\frac{a(1-a)}{p}\right) = -1$. For $a' = p+1-a$, we have

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

By Lemma 6, for some $a_*, b_* \in \{2,\dots,p-2\}$ we have

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

Note that

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

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

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

The proof of Theorem 2 is now complete. □

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer, 1993.

[2] H. Davenport, *The Higher Arithmetic. An Introduction to the Theory of Numbers*, 8th ed., Cambridge University Press, 2008.

[3] Q.-H. Hou, Z.-W. Sun, "Sequence A320159 at OEIS (On-Line Encyclopedia of Integer Sequences)", 2018, http://oeis.org/A320159.

[4] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer, 1990.

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

[6] ———, "Quadratic residues and quartic residues modulo primes", *Int. J. Number Theory* **16** (2020), no. 8, p. 1833-1858.