Czechoslovak Mathematical Journal

Zhi-Wei Sun

The tangent function and power residues modulo primes

*Czechoslovak Mathematical Journal*, Vol. 73 (2023), No. 3, 971–978

Persistent URL: http://dml.cz/dmlcz/151786

Czechoslovak Mathematical Journal, 73 (148) (2023), 971–978

# THE TANGENT FUNCTION AND POWER RESIDUES MODULO PRIMES

Zhi-Wei Sun, Nanjing

Received September 12, 2022. Published online April 13, 2023.

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

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

In particular, if $p = x^2 + 64y^2$ with $x, y \in \mathbb{Z}$, then

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

*Keywords*: power residues modulo prime; the tangent function; identity

*MSC 2020*: 11A15, 33B10, 05A19

## 1. Introduction

It is well known that the function $\tan\pi x$ has period 1. For any positive odd number $n$ and complex number $x$ with $x - \frac{1}{2} \notin \mathbb{Z}$, Sun, in Lemma 2.1 of [4], proved that

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

The research has been supported by the National Natural Science Foundation of China (grant 11971222).

DOI: 10.21136/CMJ.2023.0395-22 

where $(\frac{\cdot}{n})$ is the Jacobi symbol. In particular, for any odd prime $p$ and integer $a \not\equiv 0 \pmod p$ we have

$$\prod_{k=1}^{p-1}\Big(1+\tan\pi\frac{ak}{p}\Big)=\prod_{r=0}^{p-1}\Big(1+\tan\pi\frac{r}{p}\Big)=\Big(\frac{2}{p}\Big)2^{(p-1)/2}.$$

Let $p$ be an odd prime. Then

$$1^2, 2^2, \ldots, \Big(\frac{p-1}{2}\Big)^2$$

modulo $p$ give all the $\frac{1}{2}(p-1)$ quadratic residues modulo $p$. Sun, in Theorem 1.4 of [4], determined the value of the product $\prod_{k=1}^{(p-1)/2}(1+\tan(\pi ak^2/p))$ for any integer $a$ not divisible by $p$; in particular,

$$\prod_{k=1}^{(p-1)/2}\Big(1+\tan\pi\frac{ak^2}{p}\Big) = \begin{cases} (-1)^{|\{1\leqslant k<p/4:\,(\frac{k}{p})=1\}|}2^{(p-1)/4} & \text{if } p\equiv 1 \pmod 8,\\ (-1)^{|\{1\leqslant k<p/4:\,(\frac{k}{p})=-1\}|}2^{(p-1)/4}\Big(\frac{a}{p}\Big)\varepsilon_p^{-3(\frac{a}{p})h(p)} & \text{if } p\equiv 5 \pmod 8,\end{cases}$$

where $(\frac{\cdot}{p})$ is the Legendre symbol, and $\varepsilon_p$ and $h(p)$ are the fundamental unit and the class number of the real quadratic field $\mathbb{Q}(\sqrt{p})$, respectively.

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

$$R_m(p) = \{k \in \{1,\ldots,p-1\}\colon\ k \text{ is an } m\text{th power residue modulo } p\} \tag{1.1}$$

has cardinality $(p-1)/m$, and $\{k+p\mathbb{Z}\colon\ k\in R_m(p)\}$ is a subgroup of the multiplicative group $\{k+p\mathbb{Z}\colon\ k=1,\ldots,p-1\}$. For an integer $a \not\equiv 0 \pmod p$, the $m$th power residue symbol $(\frac{a}{p})_m$ is a unique $m$th root $\zeta$ of unity such that

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

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

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

Let $p$ be a prime with $p \equiv 1 \pmod{2m}$, where $m \in \mathbb{Z}^+$. Note that $p-1 \in R_m(p)$ since $(-1)^{(p-1)/m} = 1$. If $2 \in R_m(p)$, then $-2 = (-1) \times 2$ is an $m$th power residue modulo $p$, hence

$$\Big(\frac{-2}{p}\Big)_{2m} = \begin{cases} 1 & \text{if } -2 \text{ is a } 2m\text{th power residue modulo } p, \\ -1 & \text{otherwise,} \end{cases}$$

and

$$\Big(\frac{-2}{p}\Big)_{2m}^m = \Big(\frac{-2}{p}\Big) \tag{1.2}$$

since

$$\Big(\frac{-2}{p}\Big)_{2m}^m \equiv ((-2)^{(p-1)/(2m)})^m = (-2)^{(p-1)/2} \equiv \Big(\frac{-2}{p}\Big) \pmod{p}.$$

Now we state our main theorem.

**Theorem 1.1.** *Let $m \in \mathbb{Z}^+$, and let $p$ be a prime with $p \equiv 1 \pmod{2m}$. Suppose that 2 is an $m$th power residue modulo $p$. For any integer $a$ not divisible by $p$ we have*

$$\prod_{k \in R_m(p)} \Big(1 + \tan \pi \frac{ak}{p}\Big) = \Big(\frac{-2}{p}\Big)_{2m} (-2)^{(p-1)/(2m)} = \Big(\frac{2}{p}\Big)_{2m} 2^{(p-1)/(2m)}. \tag{1.3}$$

To prove Theorem 1.1, we need the following auxiliary result.

**Theorem 1.2.** *Let $m$ be a positive integer, and let $p$ be a prime with $p \equiv 1 \pmod{2m}$. Suppose that 2 is an $m$th power residue modulo $p$. For any integer $a \not\equiv 0 \pmod{p}$ we have*

$$\prod_{k \in R_m(p)} (\mathrm{i} - \mathrm{e}^{2\pi \mathrm{i} ak/p}) = \Big(\frac{-2}{p}\Big)_{2m} \mathrm{i}^{(p-1)/(2m)} \tag{1.4}$$

*and*

$$\prod_{k \in R_m(p)} (\mathrm{i} + \mathrm{e}^{2\pi \mathrm{i} ak/p}) = \Big(\frac{2}{p}\Big)_{2m} \mathrm{i}^{(p-1)/(2m)}. \tag{1.5}$$

Let $p$ be an odd prime with $p \equiv 1 \pmod{m}$, where $m$ is 3 or 4. Then there are unique $x, y \in \mathbb{Z}^+$ such that $p = x^2 + my^2$, cf. [2], pages 7–12. It is well known that $2 \in R_m(p)$ if and only if $p = x^2 + m(my)^2$ for some $x, y \in \mathbb{Z}^+$, cf. Proposition 9.6.2 of [3], page 119, and Exercise 26 of [3], page 64.

Theorem 1.1 with $m = 3$ has the following consequence.

**Corollary 1.1.** *Let $p = x^2 + 27y^2$ be a prime with $x, y \in \mathbb{Z}^+$. For any integer $a \not\equiv 0 \pmod p$ we have*

$$\prod_{k \in R_3(p)} \Big(1 + \tan \pi \frac{ak}{p}\Big) = (-1)^{xy/2}(-2)^{(p-1)/6}. \tag{1.6}$$

From Theorem 1.1 in the case $m = 4$, we can deduce the following result.

**Corollary 1.2.** *Let $p = x^2 + 64y^2$ be a prime with $x, y \in \mathbb{Z}^+$. For any integer $a \not\equiv 0 \pmod p$ we have*

$$\prod_{k \in R_4(p)} \Big(1 + \tan \pi \frac{ak}{p}\Big) = (-1)^{y}(-2)^{(p-1)/8}. \tag{1.7}$$

We will prove Theorems 1.1 and 1.2 in the next section, and deduce Corollaries 1.1 and 1.2 in Section 3.

## 2. Proofs of Theorems 1.1 and 1.2

**Lemma 2.1.** *Let $m$ be a positive integer, and let $p$ be a prime with $p \equiv 1 \pmod{2m}$. Then we have*

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

P r o o f. Note that $-1$ is an $m$th power residue modulo $p$ since $(p-1)/m$ is even. For $k \in \{1, \dots, p-1\}$, clearly $p - k \in R_m(p)$ if and only if $k \in R_m(p)$. Thus

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

This ends the proof of Lemma 2.1. □

P r o o f of Theorem 1.2. Let

$$c := \prod_{k \in R_m(p)} (\mathrm{i} - \mathrm{e}^{2\pi \mathrm{i} ak/p}).$$

As $k \in \mathbb{Z}$ is an $m$th power residue modulo $p$ if and only if $-k$ is an $m$th power residue modulo $p$, we also have

$$c = \prod_{k \in R_m(p)} (\mathrm{i} - \mathrm{e}^{2\pi \mathrm{i} a(-k)/p}).$$

Thus

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

Note that

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

by Lemma 2.1. As 2 is an $m$th power residue modulo $p$, we also have

$$\prod_{k \in R_m(p)} (1 - \mathrm{e}^{2\pi \mathrm{i} ak/p}) = \prod_{k \in R_m(p)} (1 - \mathrm{e}^{2\pi \mathrm{i} a(2k)/p}) = \prod_{k \in R_m(p)} (1 - \mathrm{e}^{2\pi \mathrm{i} a(4k)/p}).$$

Combining the above, we see that

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

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

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

Thus

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

and hence

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

Therefore $\delta = (\frac{-2}{p})_{2m}$ and hence (1.4) holds.

Taking conjugates of both sides of (1.4), we get

$$\prod_{k\in R_m(p)}(-\mathrm{i}-\mathrm{e}^{-2\pi\mathrm{i}ak/p})=\Big(\frac{-2}{p}\Big)_{2m}(-\mathrm{i})^{(p-1)/(2m)}$$

and hence

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

This is equivalent to (1.5) since $\{p-k\colon\ k\in R_m(p)\}=R_m(p)$.

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

P r o o f of Theorem 1.1. For any $k\in\mathbb{Z}$ we have

$$\begin{aligned}1+\tan\pi\frac{k}{p}&=1+\frac{\sin(\pi k/p)}{\cos(\pi k/p)}=1+\frac{(\mathrm{e}^{\mathrm{i}\pi k/p}-\mathrm{e}^{-\mathrm{i}\pi k/p})/(2\mathrm{i})}{(\mathrm{e}^{\mathrm{i}\pi k/p}+\mathrm{e}^{-\mathrm{i}\pi k/p})/2}=1-\mathrm{i}\frac{\mathrm{e}^{2\pi\mathrm{i}k/p}+1-2}{\mathrm{e}^{2\pi\mathrm{i}k/p}+1}\\&=1-\mathrm{i}+\frac{2\mathrm{i}}{\mathrm{e}^{2\pi\mathrm{i}k/p}+1}=(1-\mathrm{i})\Big(1+\frac{\mathrm{i}-1}{\mathrm{e}^{2\pi\mathrm{i}k/p}+1}\Big)=(1-\mathrm{i})\frac{\mathrm{e}^{2\pi\mathrm{i}k/p}+\mathrm{i}}{\mathrm{e}^{2\pi\mathrm{i}k/p}-\mathrm{i}^2}\\&=\frac{\mathrm{i}-1}{\mathrm{i}-\mathrm{e}^{2\pi\mathrm{i}k/p}}\times\frac{\mathrm{e}^{2\pi\mathrm{i}(2k)/p}-\mathrm{i}^2}{\mathrm{e}^{2\pi\mathrm{i}k/p}-\mathrm{i}^2}.\end{aligned}$$

Therefore

$$\prod_{k\in R_m(p)}\Big(1+\tan\pi\frac{ak}{p}\Big)=\frac{(\mathrm{i}-1)^{|R_m(p)|}}{\prod_{k\in R_m(p)}(\mathrm{i}-\mathrm{e}^{2\pi\mathrm{i}ak/p})}.\tag{2.1}$$

Recall (1.4) and note that

$$(\mathrm{i}-1)^{|R_m(p)|}=((\mathrm{i}-1)^2)^{(p-1)/(2m)}=(-2\mathrm{i})^{(p-1)/(2m)}.$$

So (2.1) yields that

$$\begin{aligned}\prod_{k\in R_m(p)}\Big(1+\tan\pi\frac{ak}{p}\Big)&=\frac{(-2\mathrm{i})^{(p-1)/(2m)}}{(\frac{-2}{p})_{2m}\mathrm{i}^{(p-1)/(2m)}}=\Big(\frac{-2}{p}\Big)_{2m}(-2)^{(p-1)/(2m)}\\&=\Big(\frac{2}{p}\Big)_{2m}2^{(p-1)/(2m)}.\end{aligned}$$

This concludes our proof of Theorem 1.1. □

## 3. Proofs of Corollaries 1.1 and 1.2

**Lemma 3.1.** *For any prime $p = x^2 + 27y^2$ with $x, y \in \mathbb{Z}^+$, we have*

$$\Big(\frac{-2}{p}\Big) = (-1)^{xy/2}. \tag{3.1}$$

P r o o f. Clearly $p \equiv 1 \pmod 6$ and $x \not\equiv y \pmod 2$ since $p = x^2 + 27y^2$. Note that (3.1) has the equivalent form:

$$4 \mid xy \Leftrightarrow p \equiv 1, 3 \pmod 8. \tag{3.2}$$

*Case 1*: $x$ is odd and $y$ is even. In this case,

$$p = x^2 + 27y^2 \equiv 1 + 3y^2 = 1 + 12\Big(\frac{y}{2}\Big)^2 \equiv 1 + 4\Big(\frac{y}{2}\Big)^2 \pmod 8$$

and hence

$$p \equiv 1, 3 \pmod 8 \Leftrightarrow p \equiv 1 \pmod 8 \Leftrightarrow 2 \mid \frac{y}{2} \Leftrightarrow 4 \mid y \Leftrightarrow 4 \mid xy.$$

*Case 2*: $x$ is even and $y$ is odd. In this case,

$$p = x^2 + 27y^2 \equiv x^2 + 3y^2 = 4\Big(\frac{x}{2}\Big)^2 + 3 \pmod 8$$

and hence

$$p \equiv 1, 3 \pmod 8 \Leftrightarrow p \equiv 3 \pmod 8 \Leftrightarrow 2 \mid \frac{x}{2} \Leftrightarrow 4 \mid x \Leftrightarrow 4 \mid xy.$$

In view of the above, we have completed the proof of Lemma 3.1. □

P r o o f of Corollary 1.1. As $p = x^2 + 27y^2$, we see that $p \equiv 1 \pmod 6$ and 2 is a cubic residue modulo $p$. By Lemma 3.1 and (1.2) with $m = 3$, we have

$$\Big(\frac{-2}{p}\Big)_6 = \Big(\frac{-2}{p}\Big) = (-1)^{xy/2}.$$

Combining this with Theorem 1.1 in the case $m = 3$, we immediately obtain the desired (1.6). □

P r o o f of Corollary 1.2. As $p = x^2 + 64y^2$, we see that $p \equiv 1 \pmod 8$ and 2 is a quartic residue modulo $p$. By Theorem 7.5.7 or Corollary 7.5.8 of [1], pages 227–228, we have

$$\Big(\frac{-2}{p}\Big)_8 = (-1)^y.$$

Combining this with Theorem 1.1 in the case $m = 4$, we immediately obtain the desired (1.7). □

**Acknowledgment.** The author would like to thank the referee for helpful comments.

*References*

[1] *B. C. Berndt, R. J. Evans, K. S. Williams*: Gauss and Jacobi Sums. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, New York, 1998. zbl MR

[2] *D. A. Cox*: Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. Pure and Applied Mathematics. A Wiley-Interscience Series of Texts, Monographs and Tracts. John Wiley & Sons, New York, 1989. zbl MR doi

[3] *K. Ireland, M. Rosen*: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics 84. Springer, New York, 1990. zbl MR doi

[4] *Z.-W. Sun*: Trigonometric identities and quadratic residues. Publ. Math. Debr. *102* (2023), 111–138. zbl doi

*Author's address*: Zhi-Wei Sun, Department of Mathematics, Nanjing University, West Building, Gulou Campus, No. 22 Hankou Road, Nanjing 210093, P. R. China, e-mail: zwsun@nju.edu.cn.