Czechslovak Math. J. 73 (2023), no. 3, 971–978.

THE TANGENT FUNCTION AND POWER RESIDUES MODULO PRIMES

ZHI-WEI SUN

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 mth power residue modulo p, we determine the value of the product $\prod_{k\in R_m(p)}(1+\tan\pi\frac{ak}{p})$, where

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

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

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

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 $x-1/2\notin\mathbb{Z}$, Sun [4, Lemma 2.1] proved that

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

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

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

Let p be an odd prime. Then

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

modulo p give all the $(p-1)/2$ quadratic residues modulo p. Sun [4, Theorem 1.4] determined the value of the product $\prod_{k=1}^{(p-1)/2}(1+\tan\pi\frac{ak^2}{p})$ for any

---

Key words and phrases. Power residues modulo primes, the tangent function, identity.

2020 *Mathematics Subject Classification.* Primary 11A15, 33B10; Secondary 05A19.

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

integer a not divisible by p; in particular,

$$\prod_{k=1}^{(p-1)/2}\left(1+\tan\pi\frac{ak^2}{p}\right)$$
$$=\begin{cases}(-1)^{|\{1\leqslant k<\frac p4:\ (\frac kp)=1\}|}2^{(p-1)/4} & \text{if } p\equiv 1 \pmod 8,\\ (-1)^{|\{1\leqslant k<\frac p4:\ (\frac kp)=-1\}|}2^{(p-1)/4}(\frac ap)\varepsilon_p^{-3(\frac ap)h(p)} & \text{if } p\equiv 5 \pmod 8,\end{cases}$$

where $(\frac{\cdot}{p})$ is the Legendre symbol, and ε_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 mth power residue modulo p. The set

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

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

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

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 mth power residue modulo p, hence

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

and

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

since

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

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 mth power residue modulo p. For any integer a not* *divisible by p, we have*

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

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 mth power residue modulo p. For any integer $a\not\equiv 0 \pmod p$, we have*

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

and

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

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, pp. 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. Prop. 9.6.2 of [3, p. 119] and Exer. 26 of [3, p. 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*

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

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*

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

We will prove Theorems 1.1-1.2 in the next section, and deduce Corollaries 1.1-1.2 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*

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

Proof. Note that -1 is an mth power residue modulo p since $(p-1)/m$ is even. For $k\in\{1,\ldots,p-1\}$, 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. □

Proof of Theorem 1.2. Let

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

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

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

Thus

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

Note that

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

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

$$\prod_{k\in R_m(p)}\left(1-e^{2\pi iak/p}\right)=\prod_{k\in R_m(p)}\left(1-e^{2\pi ia(2k)/p}\right)=\prod_{k\in R_m(p)}\left(1-e^{2\pi ia(4k)/p}\right).$$

Combining the above, we see that

$$c^2=(-1)^{(p-1)/(2m)}\times1\times1=(-1)^{(p-1)/(2m)}.$$

Write $c=\delta i^{(p-1)/(2m)}$ with $\delta\in\{\pm1\}$. In the ring of all algebraic integers, we have

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

$$\equiv \prod_{k\in R_m(p)} (i^p-1) = (i^p-1)^{(p-1)/m}$$
$$= ((i^p-1)^2)^{(p-1)/(2m)} = (-2i^p)^{(p-1)/(2m)} \pmod p.$$

Thus
$$\delta i^{p(p-1)/(2m)} = c^p \equiv (-2)^{(p-1)/(2m)} i^{p(p-1)/(2m)} \pmod p$$
and hence
$$\delta \equiv (-2)^{(p-1)/(2m)} \equiv \left(\frac{-2}{p}\right)_{2m} \pmod p.$$
Therefore $\delta = (\frac{-2}{p})_{2m}$ and hence (1.4) holds.

Taking conjugates of both sides of (1.4), we get
$$\prod_{k\in R_m(p)} (-i-e^{-2\pi iak/p}) = \left(\frac{-2}{p}\right)_{2m} (-i)^{(p-1)/(2m)}$$
and hence
$$(-1)^{(p-1)/m} \prod_{k\in R_m(p)} (i+e^{2\pi ia(p-k)/p}) = \left(\frac{-2}{p}\right)_{2m}\left(\frac{-1}{p}\right)_{2m} i^{(p-1)/(2m)}.$$
This is equivalent to (1.5) since $\{p-k:\ k\in R_m(p)\} = R_m(p)$.

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

Proof of Theorem 1.1. For any $k\in\mathbb{Z}$, we have
$$1+\tan\pi\frac{k}{p} = 1+\frac{\sin\pi k/p}{\cos\pi k/p} = 1+\frac{(e^{i\pi k/p}-e^{-i\pi k/p})/(2i)}{(e^{i\pi k/p}+e^{-i\pi k/p})/2}$$
$$= 1-i\frac{e^{2\pi ik/p}+1-2}{e^{2\pi ik/p}+1} = 1-i+\frac{2i}{e^{2\pi ik/p}+1}$$
$$= (1-i)\left(1+\frac{i-1}{e^{2\pi ik/p}+1}\right) = (1-i)\frac{e^{2\pi ik/p}+i}{e^{2\pi ik/p}-i^2}$$
$$= \frac{i-1}{i-e^{2\pi ik/p}} \times \frac{e^{2\pi i(2k)/p}-i^2}{e^{2\pi ik/p}-i^2}.$$
Therefore
$$\prod_{k\in R_m(p)}\left(1+\tan\pi\frac{ak}{p}\right) = \frac{(i-1)^{|R_m(p)|}}{\prod_{k\in R_m(p)}(i-e^{2\pi iak/p})}. \tag{2.1}$$

Recall (1.4) and note that
$$(i-1)^{|R_m(p)|} = ((i-1)^2)^{(p-1)/(2m)} = (-2i)^{(p-1)/(2m)}.$$
So (2.1) yields that
$$\prod_{k\in R_m(p)}\left(1+\tan\pi\frac{ak}{p}\right) = \frac{(-2i)^{(p-1)/(2m)}}{(\frac{-2}{p})_{2m} i^{(p-1)/(2m)}}$$
$$= \left(\frac{-2}{p}\right)_{2m} (-2)^{(p-1)/(2m)}$$

$$= \left(\frac{2}{p}\right)_{2m} 2^{(p-1)/(2m)}.$$

This concludes our proof of Theorem 1.1. □

3. Proofs of Corollaries 1.1-1.2

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

$$\left(\frac{-2}{p}\right) = (-1)^{xy/2}, \tag{3.1}$$

Proof. 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:

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

Case 1. x is odd and y is even.

In this case,

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

and hence

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

Case 2. x is even and y is odd.

In this case,

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

and hence

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

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

Proof 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

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

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

Proof 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, pp. 227-228], we have

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

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 and K. S. Williams, Gauss and Jacobi Sums, John Wiley & Sons, 1998.

[2] D. A. Cox, Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication, John Wiley & Sons, Inc., New York, 1989.

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

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

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

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