Preprint

A PRODUCT INVOLVING THE TANGENT FUNCTION AND CUBIC RESIDUES

ZHI-WEI SUN

ABSTRACT. For any prime \( p = x^2 + 27y^2 \) with \( x, y \in \mathbb{Z} \), and integer \( a \not\equiv 0 \pmod{p} \), we establish the new identity

\[
\prod_{k \in C(p)} \left( 1 + \tan \frac{\pi ak}{p} \right) = (-1)^{x/p}(2^{(p-1)/6},
\]

where \( C(p) = \{ 0 < k < p : k \text{ is a cubic residue modulo } p \} \).

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 \( x - 1/2 \not\in \mathbb{Z} \), the author [3, Lemma 2.1] proved that

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

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

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 \( p \). The author [3, Theorem 1.4] determined the value of the product \( \prod_{k=1}^{(p-1)/2} (1 + \tan \frac{ak^2}{p}) \) for any integer \( a \) not divisible by \( p \); in particular,

\[
\prod_{k=1}^{(p-1)/2} \left( 1 + \tan \frac{ak^2}{p} \right) =
\begin{cases}
(-1)^{\frac{1}{4}(1 - \left( \frac{a}{p} \right))} 2^{(p-1)/4} & \text{if } p \equiv 1 \pmod{8},
(-1)^{\frac{1}{4}(1 - \left( \frac{a}{p} \right))} 2^{(p-1)/4} \varepsilon_p^{-3\left( \frac{a}{p} \right) h(p)} & \text{if } p \equiv 5 \pmod{8},
\end{cases}
\]

where \( \left( \frac{\cdot}{p} \right) \) 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.

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

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

The work is supported by the National Natural Science Foundation of China (grant 11971222).
Let $p$ be an odd prime with $p \equiv 1 \pmod{3}$. Then there are unique $x, y \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ such that $p = x^2 + 3y^2$ (cf. [1]). Also, the set

$$C(p) = \{ k \in \{1, \ldots, p-1\} : k \text{ is a cubic residue modulo } p \}$$

has cardinality $(p-1)/3$. It is well known that $2 \in C(p)$ if and only if $p = x^2 + 3(3y)^2$ for some $x, y \in \mathbb{Z}^+$ (cf. Prop. 9.6.2 of [2, p. 119]).

In this paper, we obtain the following new result.

**Theorem 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

$$\prod_{k \in C(p)} \left(1 + \tan \pi \frac{ak}{p}\right) = (-1)^{xy/2}(-2)^{(p-1)/6}. \quad (1.2)$$

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

**Theorem 1.2.** Let $p \equiv 1 \pmod{3}$ be a prime, and suppose that $2$ is a cubic residue modulo $p$. For any integer $a \not\equiv 0 \pmod{p}$, we have

$$\prod_{k \in C(p)} \left(i - e^{2\pi iak/p}\right) = \left(-\frac{2}{p}\right)^{i(p-1)/6}. \quad (1.3)$$

and

$$\prod_{k \in C(p)} \left(i + e^{2\pi iak/p}\right) = \left(-2/p\right)^{i(p-1)/6}. \quad (1.4)$$

We will prove Theorems 1.2 and 1.1 in Sections 2 and 3 respectively.

2. **Proof of Theorem 1.2**

**Lemma 2.1.** Let $p \equiv 1 \pmod{3}$ be a prime. Then

$$\sum_{k \in C(p)} k = \frac{p(p-1)}{6}.$$  

**Proof.** Note that $-1$ is a cubic residues modulo $p$. For $k \in \{1, \ldots, p-1\}$, clearly $p-k \in C(p)$ if and only if $k \in C(p)$. Thus

$$\sum_{k \in C(p)} k = \sum_{k=1}^{(p-1)/2} (k + (p-k)) = \frac{|C(p)|}{2} \times p = \frac{p(p-1)}{6}.$$  

This ends the proof. \hfill $\Box$

**Lemma 2.2.** Let $p \equiv 1 \pmod{3}$ be a prime, and suppose that $2$ is a quadratic residue modulo $p$. Then

$$(-2)^{(p-1)/6} \equiv \left(-\frac{2}{p}\right) \pmod{p}.$$
Proof. As $-2 = (-1) \times 2$ is a cubic residue modulo $p$, we have $a^3 \equiv -2 \pmod{p}$ for some integer $a \not\equiv 0 \pmod{p}$. Thus

$$(-2)^{(p-1)/6} \equiv (a^3)^{(p-1)/6} \equiv \left(\frac{a}{p}\right) = \left(\frac{-2}{p}\right) \pmod{p}.$$ 

This concludes the proof. \hfill \Box

Proof of Theorem 1.2. Let

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

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

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

Thus

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

$$= \prod_{k \in C(p)} \left( i^2 + 1 - i \left( e^{2\pi i ak/p} + e^{-2\pi i ak/p} \right) \right)$$

$$= (-i)^{|C(p)|} \prod_{k \in C(p)} \left( e^{2\pi i ak/p} + e^{-2\pi i ak/p} \right)$$

$$= (-i)^{(p-1)/3} \prod_{k \in C(p)} e^{-2\pi i ak/p} \left( 1 + e^{4\pi i ak/p} \right)$$

$$= (-1)^{(p-1)/6} e^{-2\pi i \sum_{k \in C(p)} ak/p} \prod_{k \in C(p)} \frac{1 - e^{2\pi i(4k)/p}}{1 - e^{2\pi i(2k)/p}}.$$

Note that

$$e^{-2\pi i \sum_{k \in C(p)} ak/p} = e^{-2\pi i (p-1)/6} = 1$$

by Lemma 2.1. As 2 is a cubic residue modulo $p$, we also have

$$\prod_{k \in C(p)} \left( 1 - e^{2\pi i ak/p} \right) = \prod_{k \in C(p)} \left( 1 - e^{2\pi i (2k)/p} \right) = \prod_{k \in C(p)} \left( 1 - e^{2\pi i (4k)/p} \right).$$

Combining the above, we see that

$$c^2 = (-1)^{(p-1)/6} \times 1 \times 1 = (-1)^{(p-1)/6}.$$

Write $c = \delta (p-1)/6$ with $\delta \in \{\pm 1\}$. In the ring of all algebraic integers, we have

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

$$\equiv \prod_{k \in C(p)} (i^p - 1) = (i^p - 1)^{(p-1)/3}.$$
\[ ((i^p - 1)^2)^{(p-1)/6} = (-2i^p)^{(p-1)/6} \pmod{p}. \]

Thus
\[ \delta i^{p(p-1)/6} = c^p \equiv (-2)^{(p-1)/6} p^{(p-1)/6} \pmod{p} \]
and hence
\[ \delta \equiv (-2)^{(p-1)/6} \equiv \left( \frac{-2}{p} \right) \pmod{p} \]
with the aid of Lemma 2.2. Therefore \( \delta = \left( \frac{-2}{p} \right) \) and hence (1.3) holds.

Taking conjugates of both sides of (1.3), we get
\[ \prod_{k \in C(p)} (-i - e^{-2\pi i a k/p}) = \left( \frac{-2}{p} \right) (-i)^{(p-1)/6} \]
and hence
\[ (-1)^{(p-1)/3} \prod_{k \in C(p)} (i + e^{2\pi i a (p-k)/p}) = \left( \frac{-2}{p} \right) (-1)^{(p-1)/2} i^{(p-1)/6}. \]

This is equivalent to (1.4) since \( \{ p - k : k \in C(p) \} = C(p) \).

In view of the above, we have completed the proof of Theorem 1.2. \( \square \)

3. Proof of Theorem 1.1

Lemma 3.1. For any prime \( p = x^2 + 27y^2 \) with \( x, y \in \mathbb{Z}^+ \), we have
\[ \left( \frac{-2}{p} \right) = (-1)^{xy/2}, \] (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
\[ 4 \mid xy \iff p \equiv 1, 3 \pmod{8}. \] (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 Theorem 1.1. As \( p = x^2 + 27y^2 \), we see that \( p \equiv 1 \pmod{6} \) and \( 2 \) is a cubic residue modulo \( p \).

For any \( k \in \mathbb{Z} \), we have

\[
1 + \tan \frac{\pi k}{p} = 1 + \frac{\sin \frac{\pi k}{p}}{\cos \frac{\pi k}{p}} = 1 + \frac{(e^{i\pi k/p} - e^{-i\pi k/p})/(2i)}{(e^{i\pi k/p} + e^{-i\pi k/p})/2} = 1 - i \frac{e^{2\pi ik/p} + 1}{e^{2\pi ik/p} + 1} = 1 - i \frac{2i}{e^{2\pi ik/p} + 1}
\]

\[
= (1 - i) \left( 1 + \frac{i - 1}{e^{2\pi ik/p} + 1} \right) = (1 - i) \frac{e^{2\pi ik/p} + i}{e^{2\pi ik/p} - i^2}
\]

\[
= \frac{1 - i}{e^{2\pi ik/p} - i} = \frac{i - 1}{i - e^{2\pi ik/p}}
\]

Therefore

\[
\prod_{k \in C(p)} \left( 1 + \tan \frac{\pi ak}{p} \right) = \frac{(i - 1)^{|C(p)|}}{\prod_{k \in C(p)} (i - e^{2\pi ik/p})}. \tag{3.3}
\]

Note that

\[
(i - 1)^{|C(p)|} = ((i - 1)^2)^{(p-1)/6} = (-2i)^{(p-1)/6}
\]

and

\[
\prod_{k \in C(p)} (i - e^{2\pi ik/p}) = (-1)^{xy/2i(p-1)/6}
\]

by (1.3) and Lemma 3.1. So (3.3) yields that

\[
\prod_{k \in C(p)} \left( 1 + \tan \frac{\pi ak}{p} \right) = \frac{(-2i)^{(p-1)/6}}{(-1)^{xy/2i(p-1)/6}} = \frac{(-1)^{xy/2}(-2)^{(p-1)/6}}{(-1)^{xy/2i(p-1)/6}}.
\]

This concludes our proof of Theorem 1.1. □

References

[1] 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.

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

[3] Z.-W. Sun, Trigonometric identities and quadratic residues, Publ. Math. Debrecen, in press.

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

Email address: zwsun@nju.edu.cn