A talk given at *the 6th National Conf. on Combin. Number Theory* (Luoyang, Sept. 20-22, 2019)

Trigonometric identities and quadratic residues

Zhi-Wei Sun

Nanjing University, Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

Sept. 20-22, 2019

Gauss' multiplication formula for the Γ-function

For the classical Γ-function, the Gauss multiplication formula states that for each $n \in \mathbb{Z}^+$ we have

$$\prod_{r=0}^{n-1} \Gamma\left(z + \frac{r}{n}\right) = (2\pi)^{(n-1)/2} n^{1/2-nz} \Gamma(nz)$$

for all $z \in \mathbb{C}$ with $nz \notin \{0, -1, -2, \ldots\}$, where $\mathbb{C}$ denotes the field of complex numbers.

Replacing z by x/n with $x \notin \{0, -1, -2, \ldots\}$, the author rewrote in 1986 the Gauss multiplication formula as

$$\prod_{r=0}^{n-1} f\left(\frac{x+r}{n}, ny\right) = f(x, y)$$

where $f(x, y) = \Gamma(x) y^x / \sqrt{2\pi y}$.

A product formula for the sine function

As $\Gamma(z)\Gamma(1-z)=\pi/(\sin\pi x)$, we obtain from the Gauss multiplication formula the known identity

$$\prod_{r=0}^{n-1}\left(2\sin\pi\frac{x+r}{n}\right)=2\sin\pi x\quad(n\in\mathbb{Z}^+\text{ and }x\in\mathbb{C})$$

By taking logarithmic derivative, one gets the known identity

$$\frac{1}{n}\sum_{r=0}^{n-1}\cot\pi\frac{x+r}{n}=\cot\pi x\ \ (n\in\mathbb{Z}^+\text{ and }x\in\mathbb{C}\setminus\mathbb{Z}).$$

Taking the derivatives, we obtain another well-known formula

$$\frac{1}{n^2}\sum_{r=0}^{n-1}\csc^2\pi\frac{x+r}{n}=\csc^2\pi x\ \ (n\in\mathbb{Z}^+\text{ and }x\in\mathbb{C}\setminus\mathbb{Z}).$$

If n is a positive odd integer, then by taking $x=n/2$ we get the known identity

$$\sum_{r=0}^{n-1}\sec^2\pi\frac{r}{n}=n^2.$$

Known results involving $\zeta = e^{2\pi i/p}$

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

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

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

(ii) (Dirichlet's class number formula) If $p \equiv 1 \pmod 4$, then

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

where ε_p and $h(p)$ are the fundamental unit and the class number of the quadratic field $\mathbb{Q}(\sqrt{p})$ respectively. When $p \equiv 3 \pmod 4$, we have $ph(-p) = -\sum_{k=1}^{p-1} k(\frac{k}{p})$, where $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

On $\prod_{k=1}^{(p-1)/2}(1-\zeta^{ak^2})$

From the above, it is easy to deduce the following result.

Theorem 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

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

(ii) If $p \equiv 3 \pmod 4$, then

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

On $\prod_{k=1}^{(p-1)/2}\sin\pi\frac{ak^2}{p}$ and $\prod_{k=1}^{(p-1)/2}\cos\pi\frac{ak^2}{p}$

Corollary (Z.-W. Sun [Finite Fields Appl. 59(2019), 246-283]).
Let $p>3$ be a prime and let $a\in\mathbb{Z}$ with $p\nmid a$. Then

$$2^{(p-1)/2}\prod_{k=1}^{(p-1)/2}\sin\pi\frac{ak^2}{p}$$
$$=(-1)^{(a+1)\lfloor(p+1)/4\rfloor}\sqrt{p}\times\begin{cases}\varepsilon_p^{-(\frac{a}{p})h(p)} & \text{if } p\equiv1\pmod 4,\\ (-1)^{(h(-p)+1)/2}(\frac{a}{p}) & \text{if } p\equiv3\pmod 4,\end{cases}$$

and

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

New product formulas for tangent and cotangent functions

Theorem 1. (Z.-W. Sun, arXiv:1908.02155) Let n be any positive odd integer. Then

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

for all $x\in\mathbb{C}\setminus\mathbb{Z}$, and

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

for all $x\in\mathbb{C}$ with $x-1/2\notin\mathbb{Z}$, where $(\frac{2}{n})$ is the Jacobi symbol.

Proof of the Theorem

Let $x \in \mathbb{C} \setminus \mathbb{Z}$. For each $r = 0, \dots, n-1$, by Euler's formula $e^{iz} = \cos z + i \sin z$ we have

$$\begin{aligned} 1 + \cot \pi \frac{x+r}{n} =& 1 + \frac{(e^{i\pi(x+r)/n} + e^{-i\pi(x+r)/n})/2}{(e^{i\pi(x+r)/n} - e^{-i\pi(x+r)/n})/(2i)} \\ =& 1 + i \frac{e^{2\pi i(x+r)/n} + 1}{e^{2\pi i(x+r)/n} - 1} = 1 + i \left(1 + \frac{2}{e^{2\pi i(x+r)/n} - 1}\right) \\ =& (1+i) \frac{-i - e^{2\pi i(x+r)/n}}{1 - e^{2\pi i(x+r)/n}}. \end{aligned}$$

Thus

$$\begin{aligned} \prod_{r=0}^{n-1} \left(1 + \cot \pi \frac{x+r}{n}\right) =& (1+i)^n \frac{\prod_{r=0}^{n-1}(y - e^{2\pi i(x+r)/n})\big|_{y=-i}}{\prod_{r=0}^{n-1}(z - e^{2\pi i(x+r)/n})\big|_{z=1}} \\ =& (1+i)\left((1+i)^2\right)^{(n-1)/2} \frac{(y^n - e^{2\pi i x})|_{y=-i}}{(z^n - e^{2\pi i x})|_{z=1}} \\ =& (1+i)(2i)^{(n-1)/2} \frac{e^{2\pi i x} + i(-1)^{(n-1)/2}}{e^{2\pi i x} - 1}. \end{aligned}$$

Proof of the Theorem (continued)

On the other hand,

$$\begin{aligned} 1+\left(\frac{-1}{n}\right)\cot\pi x =& 1+(-1)^{(n-1)/2} i\,\frac{e^{i\pi x}+e^{-i\pi x}}{e^{i\pi x}-e^{-i\pi x}} \\ =& 1+(-1)^{(n-1)/2} i\,\frac{e^{2\pi i x}+1}{e^{2\pi i x}-1} \\ =& (1+(-1)^{(n-1)/2} i)\,\frac{e^{2\pi i x}+i(-1)^{(n-1)/2}}{e^{2\pi i x}-1}. \end{aligned}$$

Therefore

$$\begin{aligned} \prod_{r=0}^{n-1}\left(1+\cot\pi\frac{x+r}{n}\right) =& \frac{(1+i)i^{(n-1)/2}}{1+(-1)^{(n-1)/2} i} 2^{(n-1)/2}\left(1+\left(\frac{-1}{n}\right)\cot\pi x\right) \\ =& \left(\frac{2}{n}\right) 2^{(n-1)/2}\left(1+\left(\frac{-1}{n}\right)\cot\pi x\right). \end{aligned}$$

Proof of the product formula for the tangent function

Now let $x \in \mathbb{C}$ with $x - 1/2 \notin \mathbb{Z}$. Then $x' = n/2 - x \notin \mathbb{Z}$. Applying the product formula for the cotangent function with x replaced by x', we get that

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

i.e.,

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

Theorem 2. (Z.-W. Sun, arXiv:1908.02155) Let n be any positive odd integer. Then

$$\sum_{r=0}^{n-1}\frac{1}{1+\sin 2\pi\frac{x+r}{n}+\cos 2\pi\frac{x+r}{n}}=\frac{(\frac{-1}{n})n}{1+(\frac{-1}{n})\sin 2\pi x+\cos 2\pi x}$$

for any $x\in\mathbb{C}$ with $x+1/2, x+(-1)^{(n-1)/2}/4\notin\mathbb{Z}$, and

$$\sum_{r=0}^{n-1}\frac{1}{1+\sin 2\pi\frac{x+r}{n}-\cos 2\pi\frac{x+r}{n}}=\frac{(\frac{-1}{n})n}{1+(\frac{-1}{n})\sin 2\pi x-\cos 2\pi x}$$

for all $x\in\mathbb{C}$ with $x, x+(-1)^{(n-1)/2}/4\notin\mathbb{Z}$.

Proof of Theorem 2

Observe that

$$\frac{\frac{d}{dz}(1+\tan z)}{1+\tan z} = \frac{\sec^2 z}{1+\tan z} = \frac{1}{\cos^2 z + \sin z\cos z} = \frac{2}{1+\cos 2z + \sin 2z}.$$

By taking the logarithmic derivative of the identity

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

we obtain the equality

$$\sum_{r=0}^{n-1}\frac{2\pi/n}{1+\cos 2\pi(x+r)/n + \sin 2\pi(x+r)/n} = \frac{(\frac{-1}{n})2\pi}{1+\cos 2\pi x + (\frac{-1}{n})\sin 2\pi x}$$

provided that $x+1/2, x+(-1)^{(n-1)/2}/4 \notin \mathbb{Z}$. (Note that $1+(\frac{-1}{n})\tan\pi x = 0$ if and only if $x+(\frac{-1}{n})\frac{1}{4}\in\mathbb{Z}$.)

Proof of Theorem 2 (continued)

Now let $x \in \mathbb{C}$ with $x \notin \mathbb{Z}$ and $x + (-1)^{(n-1)/2}/4 \notin \mathbb{Z}$. Set $x' = n/2 - x$. Then $x' + 1/2 \notin \mathbb{Z}$ and $x' + (-1)^{(n-1)/2}/4 \notin \mathbb{Z}$. By the last formula with x replaced by x', we have

$$\sum_{r=0}^{n-1} \frac{1}{1 + \sin(\pi - 2\pi(x + n - r)/n) + \cos(\pi - 2\pi(x + n - r)/n)}$$

$$= \frac{(\frac{-1}{n})n}{1 + (\frac{-1}{n})\sin(n\pi - 2\pi x) + \cos(n\pi - 2\pi x)},$$

i.e.,

$$\sum_{r=0}^{n-1} \frac{1}{1 + \sin 2\pi\frac{x+(n-r)}{n} - \cos 2\pi\frac{x+(n-r)}{n}} = \frac{(\frac{-1}{n})n}{1 + (\frac{-1}{n})\sin 2\pi x - \cos 2\pi x}.$$

Therefore

$$\sum_{r=0}^{n-1} \frac{1}{1 + \sin 2\pi\frac{x+r}{n} - \cos 2\pi\frac{x+r}{n}} = \frac{(\frac{-1}{n})n}{1 + (\frac{-1}{n})\sin 2\pi x - \cos 2\pi x}.$$

A corollary

Corollary. Let n be any positive odd integer. Then

$$\frac{1}{n}\sum_{r=0}^{n-1}\csc 2\pi\frac{x+r}{n}=\csc 2\pi x$$

for all $x\in\mathbb{C}$ with $2x\notin\mathbb{Z}$.

Note that

$$\frac{1}{1+\sin 2\pi x+\cos 2\pi x}+\frac{1}{1+\sin 2\pi x-\cos 2\pi x}=\csc 2\pi x.$$

The corollary also implies the identity (with $n\in\mathbb{Z}^+$ odd):

$$\frac{1}{n}\sum_{r=0}^{n-1}\sec 2\pi\frac{x+r}{n}=\left(\frac{-1}{n}\right)\sec 2\pi x.$$

X. Wang and D.-Y. Zheng [JMAA 375(2007)] expressed $\sum_{k=0}^{n-1}(-1)^k\sec^m\pi\frac{x+k}{n}$ in terms of powers of $\sec\pi x$.

Another theorem

Theorem 3. (Z.-W. Sun, arXiv:1908.02155) Let n be any positive odd integer. Then

$$\sum_{j,k=0}^{n-1} \frac{1}{\sin 2\pi(x+j)/n + \sin 2\pi(y+k)/n} = \left(\frac{-1}{n}\right) \frac{n^2}{\sin 2\pi x + \sin 2\pi y}$$

for all $x, y \in \mathbb{C}$ with $x + y \notin \mathbb{Z}$ and $x - y - 1/2 \notin \mathbb{Z}$, and

$$\sum_{j,k=0}^{n-1} \frac{1}{\cos 2\pi(x+j)/n + \cos 2\pi(y+k)/n} = \frac{n^2}{\cos 2\pi x + \cos 2\pi y}$$

for all $x, y \in \mathbb{C}$ with $x \pm y - 1/2 \notin \mathbb{Z}$. Also,

$$\sum_{j,k=0}^{n-1} \frac{1}{\sin 2\pi(x+j)/n + \cos 2\pi(y+k)/n} = \frac{n^2}{(\frac{-1}{n}) \sin 2\pi x + \cos 2\pi y}$$

for all $x, y \in \mathbb{C}$ with $x \pm y + (-1)^{(n-1)/2}/4 \notin \mathbb{Z}$.

A special case

The second identity in the special case $x = y = 0$ gives the identity

$$\sum_{j,k=0}^{n-1} \frac{1}{\cos 2\pi j/n + \cos 2\pi k/n} = \frac{n^2}{2} \qquad (*)$$

(where n is a positive odd integer), which was posed by the speaker to `MathOverflow` on August 2, 2019. Both the user Wojowu and Fedor Petrov provided proofs of $(*)$.

The identity $(*)$ implies that for any prime $p \equiv 3 \pmod 4$ we have

$$\sum_{1 \leqslant j < k \leqslant (p-1)/2} \frac{1}{\cos 2\pi j^2/p + \cos 2\pi k^2/p} = -\frac{p+1}{4} \cdot \frac{p-3}{4}.$$

The whole proof of Theorem 3 is complicated. We omit the details here.

A new class number formula

Theorem 4. (Z.-W. Sun, arXiv:1908.02155) Let $p > 3$ be a prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$\sum_{k=1}^{(p-1)/2} \frac{1}{\cot \pi \frac{ak^2}{p} - 1} = \sum_{k=1}^{(p-1)/2} \frac{1}{1 - \tan \pi \frac{ak^2}{p}} - \frac{p-1}{2}$$

$$= \frac{p}{4}\left(\left(\frac{-1}{p}\right) - 1\right) + \left(\frac{-2a}{p}\right)\frac{\sqrt{p}}{2}\sum_{k=1}^{(p-1)/2}(-1)^k\left(\frac{k}{p}\right).$$

For any prime $p \equiv 1 \pmod 4$, $\sum_{k=1}^{(p-1)/2}(\frac{k}{p}) = 0$ and hence

$$\sum_{k=1}^{(p-1)/2}(-1)^k\left(\frac{k}{p}\right) = \sum_{k=1}^{(p-1)/2}(1+(-1)^k)\left(\frac{k}{p}\right) = \left(\frac{2}{p}\right)h(-p)$$

since $\frac{h(-p)}{2} = \sum_{0<k<p/4}(\frac{k}{p})$, therefore we have

$$h(-p) = \frac{2}{\sqrt{p}}\sum_{k=1}^{(p-1)/2}\frac{1}{\cot \pi \frac{k^2}{p} - 1}.$$

Theorem 5

Theorem 5. (Z.-W. Sun, arXiv:1908.02155) Let p be a prime with $p \equiv 1 \pmod 4$ and let $a \in \mathbb{Z}$ with $p \nmid a$.
(i) If $p \equiv 1 \pmod 8$, then

$$\prod_{k=1}^{(p-1)/2}\left(1+\tan\pi\frac{ak^2}{p}\right)=(-1)^{|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}2^{(p-1)/4},$$

$$\prod_{k=1}^{(p-1)/2}\left(1+\cot\pi\frac{ak^2}{p}\right)=(-1)^{|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}\frac{2^{(p-1)/4}}{\sqrt{p}}\varepsilon_p^{(\frac{a}{p})h(p)}.$$

(ii) If $p \equiv 5 \pmod 8$, then

$$\prod_{k=1}^{(p-1)/2}\left(1+\tan\pi\frac{ak^2}{p}\right)=(-1)^{|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}2^{(p-1)/4}\left(\frac{a}{p}\right)\varepsilon_p^{-3(\frac{a}{p})h(p)},$$

$$\prod_{k=1}^{(p-1)/2}\left(1+\cot\pi\frac{ak^2}{p}\right)=(-1)^{|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}\left(\frac{a}{p}\right)\frac{2^{(p-1)/4}}{\sqrt{p}}.$$

On $\prod_{k=1}^{(p-1)/2}(i-e^{2\pi ik^2/p})$

For an odd prime p, we define

$$S_p(x):=\prod_{k=1}^{(p-1)/2}(x-e^{2\pi ik^2/p}).$$

The key step to prove Theorem 5 is to show the following result.

Theorem 6 (Z.-W. Sun, arXiv:1908.02155) Let $p\equiv 1\pmod 4$ be a prime. If $p\equiv 1\pmod 8$, then

$$S_p(i)=(-1)^{\frac{p-1}{8}+|\{1\le k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}.$$

If $p\equiv 5\pmod 8$, then

$$S_p(i)=i(-1)^{\frac{p-5}{8}+|\{1\le k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}\varepsilon_p^{-h(p)}.$$

Proof of Theorem 6

Let $c := S_p(i)$. In the ring of algebraic p-adic integers, we have the congruence

$$c^p \equiv \prod_{k=1}^{(p-1)/2} (i^p - 1) = (i-1)^{(p-1)/2} = (-2i)^{(p-1)/4} \pmod p.$$

As $(\frac{-1}{p}) = 1$, we have

$$c^2 = \prod_{k=1}^{\frac{p-1}{2}} (i - e^{2\pi i k^2/p})(i - e^{-2\pi i k^2/p}) = \prod_{k=1}^{\frac{p-1}{2}} (-ie^{2\pi i k^2/p} - ie^{-2\pi i k^2/p})$$

$$=(2i)^{(p-1)/2} \prod_{k=1}^{(p-1)/2} \cos 2\pi \frac{k^2}{p} = (-1)^{(p-1)/4} \varepsilon_p^{(1-(\frac{2}{p}))(\frac{2}{p})h(p)},$$

and hence

$$c = \delta i^{(p-1)/4} \varepsilon_p^{((\frac{2}{p})-1)h(p)/2}$$

for some $\delta \in \{\pm 1\}$.

Determine δ

Note that $i^p = i$. Thus

$$c^p = \delta i^{(p-1)/4} \varepsilon_p^{((\frac{2}{p})-1)ph(p)/2}$$

and hence

$$(-2)^{(p-1)/4} \equiv \delta \varepsilon_p^{((\frac{2}{p})-1)ph(p)/2} \pmod p.$$

If $p \equiv 1 \pmod 8$, then

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

with the help of a result of K. S. Williams and J. D. Currie [Canad. J. Math. 34(1982)].

The case $p \equiv 5 \pmod 8$

Now assume that $p \equiv 5 \pmod 8$ and write $\varepsilon_p^{h(p)} = a_p + b_p\sqrt{p}$ with $2a_p, 2b_p \in \mathbb{Z}$. Then $a_p \equiv -\frac{p-1}{2}! \pmod p$ by a previous result of the speaker. With the help of Williams-Currie's result on $2^{(p-1)/4} \bmod p$, we get

$$\begin{aligned}(-1)^{|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}\delta\frac{p-1}{2}! &\equiv -\delta 2^{(p-1)/4} \equiv \varepsilon_p^{-ph(p)} = (a_p + b_p\sqrt{p})^{-p} \\ &\equiv \left(a_p^p + b_p^p p^{(p-1)/2}\sqrt{p}\right)^{-1} \\ &\equiv \left(-\frac{p-1}{2}!\right)^{-1} \equiv \frac{p-1}{2}! \pmod p.\end{aligned}$$

(Note that $(\frac{p-1}{2}!)^2 \equiv -1 \pmod p$ by Wilson's theorem.) Therefore

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

On $S_p(\pm\omega)$ with $p \equiv 1 \pmod 4$

Let $\omega := e^{2\pi i/3} = (-1+\sqrt{-3})/2$.

Theorem 7 (Z.-W. Sun, arXiv:1908.02155) Let $p \equiv 1 \pmod 4$ be a prime. Then

$$(-1)^{|\{1\leqslant k\leqslant\lfloor\frac{p+1}{3}\rfloor:\ (\frac{k}{p})=-1\}|}S_p(\omega) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{12}, \\ \omega\varepsilon_p^{h(p)} & \text{if } p \equiv 5 \pmod{12}; \end{cases}$$

$$S_p(-\omega) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{12}, \\ -\omega\varepsilon_p^{-2h(p)} & \text{if } p \equiv 5 \pmod{24}, \\ \omega & \text{if } p \equiv 17 \pmod{24}. \end{cases}$$

A Key Lemma. Let $p \equiv 1 \pmod 4$ be a prime. Then

$$(-1)^{|\{1\leqslant k<\frac{p}{3}:\ (\frac{k}{p})=-1\}|}(-3)^{(p-1)/4} \equiv \begin{cases} 1 \pmod p & \text{if } 12 \mid p-1, \\ \frac{p-1}{2}! \pmod p & \text{if } 12 \mid p-5, \end{cases}$$

where $h(-3p)$ is the class number of the field $\mathbb{Q}(\sqrt{-3p})$.

On $S_p(i)$ with $p \equiv 3 \pmod 4$

Conjecture 1 (Z.-W. Sun, arXiv:1908.02155). Let $p > 3$ be a prime with $p \equiv 3 \pmod 4$. Write $\varepsilon_p^{h(p)} = a_p + b_p\sqrt{p}$ with a_p and b_p positive integers. Then

$$\left(i - (-1)^{(p+1)/4}\right) S_p(i) = (-1)^{\frac{h(-p)+1}{2}\cdot\frac{p+1}{4}}(s_p - t_p\sqrt{p}),$$

where

$$s_p = \sqrt{a_p + (-1)^{(p+1)/4}} \quad \text{and} \quad t_p = \frac{b_p}{s_p}$$

are positive integers.

For the prime $p = 79$, we have $h(-p) = 5$, $h(p) = 3$ and $\varepsilon_p = 80 + 9\sqrt{p}$. Note that

$$\varepsilon_p^{h(p)} = (80 + 9\sqrt{79})^3 = 2047760 + 230391\sqrt{79},$$

$$s_p = \sqrt{2047760 + 1} = 1431 \quad \text{and} \quad t_p = \frac{230391}{1431} = 161.$$

Thus the conjecture for $p = 79$ states that

$$(i - 1)S_{79}(i) = 1431 - 161\sqrt{79}.$$

On $S_p(\omega)$ with $p \equiv 3 \pmod 4$

Remark. Let $p > 3$ be a prime with $p \equiv 3 \pmod 4$. According to Dickson's book (History of Number Theory, Vol. 2), Dirichlet realized that $(i - (\frac{2}{p}))S_p(i) \in \mathbb{Z}[\sqrt{p}]$ but he did not predict the exact value of $S_p(i)$.

Conjecture 2 (Z.-W. Sun, arXiv:1908.02155). Let $p > 3$ be a prime with $p \equiv 3 \pmod 4$. Then

$$S_p(\omega^{\pm 1}) = (-1)^{(h(-p)+1)/2}\left(\frac{p}{3}\right)\frac{x_p\sqrt{3} \mp y_p\sqrt{p}}{2} \times \begin{cases} i^{\pm 1} & \text{if } p \equiv 7 \pmod{12}, \\ (-1)^{|\{1 \le k < \frac{p}{3}:\ (\frac{k}{p})=1\}|}(i\omega)^{\pm 1} & \text{if } p \equiv 11 \pmod{12}, \end{cases}$$

where (x_p, y_p) is the least positive integer solution to the diophantine equation $3x^2 + 4(\frac{p}{3}) = py^2$.

Example. For the primes $p = 79, 227$, Conjecture 2 predicts that

$$S_{79}(\omega) = i\frac{\sqrt{79} - 5\sqrt{3}}{2} \text{ and } S_{227}(\omega) = i\omega(1338106\sqrt{3} - 153829\sqrt{227}).$$

On $S_p(\omega)$ with $p \equiv 3 \pmod 4$

Conjecture 3 (Z.-W. Sun, arXiv:1908.02155). Let $p > 3$ be a prime.

(i) If $p \equiv 13 \pmod{24}$, then

$$S_p(e^{\pm 2\pi i/12}) = i(-1)^{\frac{p-5}{8}+|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=\mp 1\}|}(x_p\sqrt{3} - y_p\sqrt{p})$$

and

$$S_p(e^{\pm 2\pi i\frac{5}{12}}) = i(-1)^{\frac{p-5}{8}+|\{1\leqslant k<\frac{p}{4}:\ (\frac{k}{p})=\pm 1\}|}(x_p\sqrt{3} + y_p\sqrt{p}),$$

where (x_p, y_p) is the least positive integer solution to the equation $3x^2 + 1 = py^2$.

(ii) When $p \equiv 19 \pmod{24}$, we may write $p = (4x)^2 + 3y^2$ with $x, y \in \mathbb{Z}$, and we have

$$S_p(e^{\pm 2\pi i/12}) = (-1)^{(p-19)/24+x}(1 \pm i)\frac{1+\sqrt{3}}{2}$$

and

$$S_p(e^{\pm 2\pi i\frac{5}{12}}) = (-1)^{(p-19)/24+x}(1 \pm i)\frac{1-\sqrt{3}}{2}.$$

On $S_p(\zeta)$ with $\zeta^{10} = 1$

Remark. The speaker posted to `MathOverflow` his conjecture that the equation $3x^2 + 1 = py^2$ has integer solutions for each prime $p \equiv 13 \pmod{24}$, and this was confirmed by the user `GH from MO` via the theory of binary quadratic forms. For any odd prime p, it is known that $h(-p)$ is even or odd according as p is congruent to 1 or 3 modulo 4.

Conjecture 4 (Z.-W. Sun, arXiv:1908.02155). Let ζ be any primitive tenth root of unity. Then

$$\prod_{k=1}^{(p-1)/2} (\zeta - e^{2\pi i k^2/p}) = (-1)^{|\{1 \le k \le \frac{p+9}{10}:\ (\frac{k}{p})=-1\}|}$$

for each prime $p \equiv 21 \pmod{40}$, and

$$\prod_{k=1}^{(p-1)/2} (\zeta - e^{2\pi i k^2/p}) = (-1)^{|\{1 \le k \le \frac{p+1}{10}:\ (\frac{k}{p})=-1\}|} \zeta^2$$

for any prime $p \equiv 29 \pmod{40}$.

On $S_p(\zeta)$ with $\zeta^{2^n} = 1$

Conjecture 5 (Z.-W. Sun, arXiv:1908.02155). Let $p > 3$ be a prime and let $n > 2$ be an integer. Let a be any positive odd integer smaller than 2^n.

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

$$(-1)^{|\{1\leqslant k<\frac{ap}{2^n}:\ (\frac{k}{p})=1\}|}S_p(e^{2\pi ia/2^n})e^{-2\pi ia(p-1)/2^{n+2}} > 0.$$

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

$$(-1)^{\frac{h(-p)+1}{2}+|\{1\leqslant k<\frac{ap}{2^n}:\ (\frac{k}{p})=1\}|}S_p(e^{2\pi ia/2^n})e^{-2\pi i(a(p-1)+2^n)/2^{n+2}} > 0.$$

Main references:

1. Z.-W. Sun, *Quadratic residues and related permutations and identities*, Finite Fields Appl. **59** (2019), 246-283.

2. Z.-W. Sun, *Trigonometric identities and quadratic residues*, arXiv:1908.02155, `http://arxiv.org/abs/1908.02155`

Thank you!