Gauss Sum

Tristan Shin

29 Sep 2018

Let p be an odd prime. If $\zeta = e^{i\cdot\frac{2\pi}{p}}$, then

$$\sum_{n=0}^{p-1}\left(\frac{n}{p}\right)\zeta^n = \begin{cases}\sqrt{p} & \text{if } p\equiv 1 \pmod 4\\ i\sqrt{p} & \text{if } p\equiv 3 \pmod 4\end{cases}$$

Let $g_p = \sum_{n=0}^{p-1}\left(\frac{n}{p}\right)\zeta^n$.

The first step is to prove that $g_p^2 = (-1)^{\frac{p-1}{2}}p$. To do this, observe that

$$\begin{aligned}
g_p\overline{g_p} &= \sum_{n=0}^{p-1}\sum_{m=0}^{p-1}\left(\frac{nm}{p}\right)\zeta^{n-m}\\
&= \sum_{d=0}^{p-1}\zeta^d\sum_{n=0}^{p-1}\left(\frac{n(n-d)}{p}\right)\\
&= p-1+\sum_{d=1}^{p-1}\zeta^d\sum_{n=1}^{p-1}\left(\frac{n(n-d)}{p}\right)\\
&= p-1+\sum_{d=1}^{p-1}\zeta^d\sum_{n=1}^{p-1}\left(\frac{1-\frac{d}{n}}{p}\right)\\
&= p-1+\sum_{d=1}^{p-1}\zeta^d\sum_{\substack{0\le e\le p-1\\ e\ne 1}}\left(\frac{e}{p}\right)\\
&= p-1+\sum_{d=1}^{p-1}(-\zeta^d)\\
&= p.
\end{aligned}$$

But

$$\overline{g_p} = \sum_{m=0}^{p-1}\left(\frac{m}{p}\right)\zeta^{-m} = \sum_{m=0}^{p-1}\left(\frac{-m}{p}\right)\zeta^{m} = (-1)^{\frac{p-1}{2}}g_p$$

so $g_p^2 = (-1)^{\frac{p-1}{2}}p$ as desired.

Now, define polynomials

$$\begin{aligned}
G(X) &= \sum_{n=0}^{p-1}\left(\frac{n}{p}\right)X^n\\
H(X) &= \prod_{k=1}^{\frac{p-1}{2}}\left(X^{-k/2}-X^{k/2}\right)
\end{aligned}$$

where the exponents in h are taken mod p.

We know that $G(\zeta)^2 = p^*$. Observe that

$$\begin{aligned}
H(\zeta)^2 &= \prod_{k=1}^{\frac{p-1}{2}} \left(\zeta^{-k/2} - \zeta^{k/2}\right)^2 = \prod_{k=1}^{\frac{p-1}{2}} \left(\zeta^{-k} - 1\right)\left(1 - \zeta^k\right) \\
&= (-1)^{\frac{p-1}{2}} \prod_{k=1}^{p-1} \left(1 - \zeta^k\right) = (-1)^{\frac{p-1}{2}} \Phi_p(1) = (-1)^{\frac{p-1}{2}} p
\end{aligned}$$

so $G(\zeta)^2 = H(\zeta)^2$. It follows that $G(\zeta) = \epsilon H(\zeta)$ for some $\epsilon \in \{\pm 1\}$ and thus ζ is a root of the polynomial $G - \epsilon H$. Thus Φ_p divides $G - \epsilon H$.

Now, we work in $\mathbb{F}_p$. First note that

$$\begin{aligned}
G(1+Y) &= \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)(1+Y)^n \\
&= \sum_{n=0}^{p-1}\sum_{m=0}^{n} \left(\frac{n}{p}\right)\binom{n}{m} Y^m \\
&= \sum_{m=0}^{p-1}\left(\sum_{n=m}^{p-1} \binom{n}{m}\left(\frac{n}{p}\right)\right) Y^m.
\end{aligned}$$

Suppose that $m < \frac{p-1}{2}$ and consider the inside sum. Let $\binom{X}{m} = \frac{1}{m!}\sum_{j=0}^{m} a_{m,j} X^j$ be the binomial coefficient polynomial. Then

$$\sum_{n=m}^{p-1} \binom{n}{m}\left(\frac{n}{p}\right) = \sum_{n=0}^{p-1} \binom{n}{m}\left(\frac{n}{p}\right) = \sum_{n=0}^{p-1}\sum_{j=0}^{m} \frac{a_{m,j}}{m!} n^{j+\frac{p-1}{2}} = \sum_{j=0}^{m} \frac{a_{m,j}}{m!} \sum_{n=0}^{p-1} n^{j+\frac{p-1}{2}}.$$

Take a generator g. Then

$$\sum_{n=0}^{p-1} n^{j+\frac{p-1}{2}} = \sum_{n=0}^{p-1} (gn)^{j+\frac{p-1}{2}} = g^{j+\frac{p-1}{2}} \sum_{n=0}^{p-1} n^{j+\frac{p-1}{2}}$$

so $\sum_{n=0}^{p-1} n^{j+\frac{p-1}{2}} = 0$ because $0 < j + \frac{p-1}{2} < p-1$. Thus $\sum_{n=m}^{p-1} \binom{n}{m}\left(\frac{n}{p}\right) = 0$. But if $m = \frac{p-1}{2}$, then

$$\sum_{n=m}^{p-1} \binom{n}{m}\left(\frac{n}{p}\right) = \sum_{j=0}^{m} \frac{a_{m,j}}{m!} \sum_{n=0}^{p-1} n^{j+\frac{p-1}{2}} = \frac{a_{m,m}}{m!}(p-1) = -\frac{1}{\left(\frac{p-1}{2}\right)!}$$

so

$$G(1+Y) \equiv -\frac{1}{\left(\frac{p-1}{2}\right)!} Y^{\frac{p-1}{2}} \pmod{Y^{\frac{p+1}{2}}}.$$

Now we expand $H(1+Y)$. Note that $(1+Y)^{-k/2} - (1+Y)^{k/2} \equiv -kY \pmod{Y^2}$ so

$$H(1+Y) \equiv (-1)(-2)\cdots\left(-\frac{p-1}{2}\right) Y^{p-1} 2 \equiv \frac{(p-1)!}{\left(\frac{p-1}{2}\right)!} Y^{\frac{p-1}{2}} \pmod{Y^{\frac{p+1}{2}}}.$$

But $G(1+Y) \equiv \epsilon H(1+Y) \pmod{\Phi}_p(1+Y)$ and $\Phi_p(1+Y) = Y^{p-1}$, so $G(1+Y) \equiv \epsilon H(1+Y) \pmod{Y}^{\frac{p+1}{2}}$. It follows that

$$-1 \equiv \epsilon(p-1)! \pmod{Y}$$

so by Wilson's Theorem, $\epsilon = 1$.

Revert to $\mathbb{C}$. We have $G(\zeta) = H(\zeta)$. Check that $\zeta^{-k/2} - \zeta^{k/2} = -2i \sin \frac{2\pi(k/2)}{p}$ (where $k/2$ is taken mod p). This is a positive multiple of i when k is odd and a negative multiple of i when k is even. Thus every odd-even consecutive pair is a positive real number times $i \cdot (-i) = 1$. It follows that $H(\zeta)$ is either along the positive real axis or positive imaginary axis. Since $g_p = G(\zeta) = H(\zeta)$ and $|g_p| = \sqrt{p}$, the result follows. ■