Proof. Step 1.

$$\begin{aligned}\Delta_a(\zeta\pi) &= \mathrm{Tr}\big[(-a/p)_Z(4a/\zeta\pi)_5(\zeta\pi)(\zeta\pi)^{\sigma^3}\big]\\ &= \mathrm{Tr}\big[(-a/p)_Z(4a/\pi)_5\,.\,\zeta^4\,.\,\pi\pi^{\sigma^3}\big]\\ &= \mathrm{Tr}\big[(-au/p)_Z(4au/\pi)_5\,.\,\pi\pi^{\sigma^3}\big],\end{aligned}$$

where $(u/p)_Z = 1$, $(u/\pi)_5 = \zeta^4$, and this $= \Delta_{au}(\pi)$. It follows that $\Delta_a(\zeta^i\pi) = \Delta_{au}(\pi)$, where $(u/p)_Z = 1$ and $(u/\pi)_5 = \zeta^{5-i}$ $(i=0, 1, 2, 3, 4)$.

Step 2.

$$\begin{aligned}\Delta_a(\varepsilon\pi) &= \mathrm{Tr}\big[(-a/p)_Z(4a/\varepsilon\pi)_5\,.\,\varepsilon\pi\,.\,(\varepsilon\pi)^{\sigma^3}\big]\\ &= \mathrm{Tr}\big[(-a/p)_Z(4a/\pi)_5\,.\,N_{Q(\sqrt{5})/Q}(\varepsilon)\,.\,\pi\pi^{\sigma^3}\big]\\ &= \Delta_{av}(\pi),\end{aligned}$$

where $(v/p)_Z = N_{Q(\sqrt{5})/Q}(\varepsilon)$, $(v/\pi)_5 = 1$.

Combining steps 1 and 2 we get:

$$\begin{aligned}\Delta_a(\zeta^i\varepsilon\pi) &= \Delta_{au}(\varepsilon\pi) \text{ where } (u/p)_Z = 1,\ (u/\pi)_5 = \zeta^{5-i}\\ &= \Delta_{au.v}(\pi) \text{ where } (v/p)_Z = \text{Norm } \varepsilon,\ (v/\pi)_5 = 1,\\ &= \Delta_{ab}(\pi) \text{ where } b = uv \text{ satisfies the conditions of}\end{aligned}$$

theorem 1. This completes the proof of theorem 1.

We next remove the restriction $(g/\pi)_5 = \zeta$ and see what the Δ_a's mean then.

3. The restriction $(g/\pi)_5 = \zeta$ removed

Here we have to look at $\Delta_a(\pi^\sigma)$ (and similarly $\Delta_a(\pi^{\sigma^2})$ and $\Delta_a(\pi^{\sigma^3})$). We have the following

THEOREM 2. $\Delta_a(\pi^\sigma) = \Delta_a(\pi)$.

Proof. $\Delta_a(\pi^\sigma) = \mathrm{Tr}\,[(-a/p)_Z\,(4a/\pi^\sigma)_5\,.\,\pi^\sigma\,.\,(\pi^\sigma)^{\sigma^3}]$.

Now $(4a/\pi^\sigma)_5 = (4a/\pi_2)_5$, and if $4a \equiv g^\nu \pmod p$ then this $= (g^\nu/\pi_2)_5 = (g/\pi_2)_5^\nu = \zeta^{2\nu} = (g^\nu/\pi_1)_5^2 = (4a/\pi_1)_5^2 = \sigma\,[(4a/\pi)_5]$. Hence

$$\begin{aligned}\Delta_a(\pi^\sigma) &= \mathrm{Tr}\big[(-a/p)_Z\,.\,\sigma(4a/\pi)_5\,.\,\pi\,.\,\pi^{\sigma^3}\big]\\ &= \mathrm{Tr}\big[\sigma\big((-a/p)_Z(4a/\pi)_5\,.\,\pi\pi^{\sigma^3}\big)\big]\\ &= \Delta_a(\pi) \text{ as required.}\end{aligned}$$

A clearer insight is gained into this by looking at the whole thing directly as follows.

Since the choice of g is arbitrary, we change g to another primitive root g^r with $(r, p-1) = 1$, $r = i \pmod 5$, $i = 1, 2, 3, 4$. This does not alter Δ_a (as Δ_a is independent of g) but replaces π by any desired π_i so that $\Delta_a(\pi) = \Delta_a$ (any other π). Note that such an r exists, for all we want is, for $i = 1, 2, 3, 4$, a λ such that $(i+5\lambda, p-1) = 1$. Now $i + 5\lambda$ takes infinitely many prime values as λ takes positive integer values since $(i, 5) = 1$; so λ may be chosen so that $i + 5\lambda$ is a prime avoiding the primes occuring in $p - 1$.

4. Expressions allied to $\Delta_a(\pi)$

We fix our π now with $(g/\pi)_5 = \zeta$ and normalize it too. It is clear that there are only 3 expressions allied to $\Delta_a(\pi)$ viz $(-a/p)_Z (4a/\pi)_5 \,.\, \pi \,.\, \pi^\sigma$ + conjugates, $(-a/p)_Z (4a/\pi)_5 \,.\, \pi^\sigma \,.\, \pi^{\sigma^2}$ + conjugates and $(-a/p)_Z (4a/\pi)_5 \,.\, \pi^{\sigma^2} \,.\, \pi^{\sigma^3}$ + conjugates. This is so because changing the first term of $\Delta_a(\pi)$ fixes the changes in the other terms (otherwise we will not even get a rational integer!). Let us look at the first of these (the others would be similar), which equals $\mathrm{Tr}\,[(-a/p)_Z (4a/\pi)_5 \,.\, \pi\,\pi^\sigma]$. We have the following theorem:

THEOREM 3. $\mathrm{Tr}\,[(-a/p)_Z (4a/\pi)_5 \,.\, \pi\,\pi^\sigma] = \Delta_{au} - 1\,(\pi)$, *where* $(u/p)_Z = 1$ *and* $(u/\pi)_5 = (4a/\pi)_5$.

Proof. We have

$$\begin{aligned}
\Delta_a(\pi) &= \mathrm{Tr}\,[(-a/p_Z)(4a/\pi)_5 \,.\, \pi \,.\, \pi^{\sigma^3}] \\
&= \mathrm{Tr}\,[(-a/p)_Z (4a/\pi^\sigma)_5 \,.\, \pi^\sigma \,.\, \pi^{\sigma^3}] \text{ by 3 on letting } \pi \to \pi^\sigma, \\
&= \mathrm{Tr}\,[(-a/p)_Z (16a^2/\pi)_5 \,.\, \pi^\sigma \,.\, \pi] \text{ since } (4a/\pi^\sigma)_5 = (g^\nu/\pi_2)_5 \\
&\qquad\qquad = (g^\nu/\pi_1)_5^2 = (4a/\pi)_5^2 = (16a^2/\pi)_5, \\
&= \mathrm{Tr}\,[(-au/p)_Z (4(au)/\pi)_5 \,.\, \pi\,\pi^\sigma], \text{ where } (u/p)_Z = 1 \text{ and } (u/p)_5 \\
&\qquad\qquad = (4a/\pi)_5.
\end{aligned}$$

Now writing a for au we get the theorem.

It follows that the expressions allied to $\Delta_a(\pi)$ also represent the number of solutions of the congruence (1) for a suitable value of a.

5. The set $\{\Delta_a \mid a = 1, 2, 3, \ldots, p-1\}$

Dickson's paper on cyclotomy [1] includes the following Theorem (theorem 8 of [1]). Let $p \equiv 1 \pmod 5$ be a rational prime. Then the Diophantine equations