Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 21 (1975)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: NOTES ON THE CONGRUENCE $y^2 \equiv x^5 -a(mod \quad p)

Autor: Rajwade, A. R.

Kapitel: 2. Determination of Δ_a WITHOUT THE NORMALIZATION RESTRICTIONS ON THE π_j

DOI: https://doi.org/10.5169/seals-47329

$$\left(\frac{-4a}{\pi_1}\right)_{10} . \pi_1 \pi_2 + \left(\frac{-4a}{\pi_2}\right)_{10} . \pi_2 \pi_4 + \left(\frac{-4a}{\pi_3}\right)_{10} . \pi_1 \pi_3 + \left(\frac{-4a}{\pi_4}\right)_{10} . \pi_3 \pi_4$$

being the trace of $(-4a/\pi_1)_{10} . \pi_1 \pi_2$, is a rational integer. What does it represent?

One could also remove the various restrictions on the π_i in the expression for Δ_a and ask what Δ_a then represents. The object of this note is to answer these questions and also to determine the set $\{\Delta_a \mid a = 1, 2, 3, \ldots, p-1\}$.

It is immediate that Δ_a can take only 10 distinct values. This follows by looking at (2) or directly from the congruence (1) as follows: Let $(e, p) = 1$, then we have

$$\Delta_a = \sum \left(\frac{x^5 - a}{p}\right) \text{ and so } \Delta_{ae^5} = (e/p)_Z . \Delta_a .$$

It follows that the distinct values taken by the Δ_a, for $a = 1, 2, \ldots, p-1$ are just $\pm \Delta_g$, $\pm \Delta_{g^2}$, $\pm \Delta_{g^3}$, $\pm \Delta_{g^4}$, $\pm \Delta_{g^5}$. We shall determine these 10 values as a set. Which value is associated with which a will not be clear except when $4a$ is a quintic residue mod p.

2. Determination of Δ_a without the normalization restrictions on the π_j

Write $p = \pi . \pi^\sigma . \pi^{\sigma^3} . \pi^{\sigma^2}$ (with $(g/\pi)_5 = \zeta) = \pi_1 \pi_2 \pi_3 \pi_4$ say. Since the restrictions on π are going to be removed, we denote Δ_a by $\Delta_a(\pi)$. We write (2) in a more convenient form viz

(3) $$\Delta_a(\pi) =$$

$$\left(\frac{-a}{p}\right)_Z . \left[\left(\frac{4a}{\pi_1}\right)_5 . \pi_1 \pi_3 + \left(\frac{4a}{\pi_2}\right)_5 . \pi_1 \pi_2 + \left(\frac{4a}{\pi_3}\right)_5 . \pi_3 \pi_4 + \left(\frac{4a}{\pi_4}\right)_5 . \pi_2 \pi_4\right].$$

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

Let the condition $(g/\pi)_5 = \zeta$ be retained first so that we only change π to an associate $\eta \pi$ where $\eta = \zeta^i \varepsilon \, (0 \leqslant i \leqslant 4)$ with ε a real fundamental unit, say $\pm \left(\frac{1+\sqrt{5}}{2}\right)^j$, $j \in \mathbf{Z}$, of $Q(\sqrt{5})$. We have the following

Theorem 1. *$\Delta_a(\zeta^i \varepsilon . \pi) = \Delta_{ab}(\pi)$ where $(b/\pi)_5 = \zeta^{5-i}$ and $(b/p)_Z \neq N_{Q(\sqrt{5})/Q}(\varepsilon)$.*

Proof. Step 1.

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

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.

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

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. $\Delta_a(\pi^\sigma) = \mathrm{Tr}\left[(-a/p)_Z(4a/\pi^\sigma)_5 \,.\, \pi^\sigma \,.\, (\pi^\sigma)^{\sigma^3}\right]$.
Now $(4a/\pi^\sigma)_5 = (4a/\pi_2)_5$, and if $4a \equiv g^\nu \pmod p$ then this $= (g^\nu/\pi_2)_5 = (g/\pi_2)_5^\nu = \zeta^{2\nu} = (g^\nu/\pi_1)_5^2 = (4a/\pi_1)_5^2 = \sigma\left[(4a/\pi)_5\right]$. Hence

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

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