Zeitschrift: 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)

Kapitel: 1. Introduction

Autor: Rajwade, A. R.

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

NOTES ON THE CONGRUENCE $y^2 \equiv x^5 - a \pmod p$

by A. R. Rajwade

1. Introduction

In a previous paper [3] we proved the following

Theorem. *Let* $p \equiv 1 \pmod 5$ *be a rational prime and* g *a fixed primitive root* mod p. *Then the number of solutions of the congruence*

$$y^2 \equiv x^5 - a \pmod p \tag{1}$$

is $p + \Delta_a$, *where* Δ_a *is equal to* [1])

$$\left(\frac{-4a}{\pi_1}\right)_{10} . \pi_3 \pi_4 + \left(\frac{-4a}{\pi_2}\right)_{10} . \pi_1 \pi_3 + \left(\frac{-4a}{\pi_3}\right)_{10} . \pi_2 \pi_4 + \left(\frac{-4a}{\pi_4}\right)_{10} . \pi_1 \pi_2 . \tag{2}$$

Here $p = \pi_1 \pi_2 \pi_3 \pi_4 = \pi_1 . \sigma\pi_1 . \sigma^3 \pi_1 . \sigma^2 \pi_1$, with $\sigma : \zeta \to \zeta^2$, is the decomposition of p in $Q(\zeta)$, $\zeta^5 = 1$, $\zeta \neq 1$ and π_1 is chosen to satisfy $(g/\pi_1)_5 = \zeta$, so that $(g/\pi_i)_5 = \zeta^i$, and the π_j are normalized so that the products $S = \pi_1 \pi_2$, $\bar{S} = \pi_3 \pi_4$, $T = \pi_1 \pi_3$, $\bar{T} = \pi_2 \pi_4$ (all polynomials in ζ) satisfy

1. $S(\zeta) . S(\zeta^{-1}) \equiv [S(1)]^2 \pmod 5$,
2. $S(\zeta) \equiv S(1) \pmod{(1-\zeta)^2}$,
3. $S(1) \equiv 4 \pmod 5$.

(and similarly for $\bar{S}$, T, $\bar{T}$).

In (2) the 4 products $\pi_i \pi_j$ are those 4 out of the 6 combinations $\pi_1 \pi_2$, $\pi_1 \pi_3$, $\pi_1 \pi_4$, $\pi_2 \pi_3$, $\pi_2 \pi_4$, $\pi_3 \pi_4$ for which $\bar{\pi}_i \neq \pi_j$. But there is no symmetrical way of coupling the residue symbol $\left(\frac{-4a}{\pi_i}\right)_{10}$ with $\pi_j \pi_k$. We ask: What do other expressions similar to Δ_a represent? For example the expression

[1]) See Appendix for the definitions of $(\alpha/\beta)_{10}$, $(\alpha/\beta)_5$, $(a/p)_Z$.

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

being the trace of $(-4a/\pi_1)_{10} \cdot \pi_1 \pi_2$, 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 $\{\Delta_a \mid a = 1, 2, 3, ..., p-1\}$.

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

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

It follows that the distinct values taken by the Δ_a, for $a = 1, 2, ..., p-1$ 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) $$\Delta_a(\pi) =$$

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

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

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 $(b/p)_{\mathbf{Z}} \neq N_{Q(\sqrt{5})/Q}(\varepsilon)$.*