

# 1. Introduction

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **21 (1975)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **27.04.2024**

## Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

# 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*

$$(1) \quad y^2 \equiv x^5 - a \pmod{p}$$

*is  $p + \Delta_a$ , where  $\Delta_a$  is equal to <sup>1)</sup>*

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

Here  $p = \pi_1 \pi_2 \pi_3 \pi_4 = \pi_1 \cdot \sigma \pi_1 \cdot \sigma^3 \pi_1 \cdot \sigma^2 \pi_1$ , with  $\sigma: \zeta \rightarrow \zeta^2$ , is the decomposition of  $p$  in  $Q(\zeta)$ ,  $\zeta^5 = 1$ ,  $\zeta \neq 1$  and  $\pi_1$  is chosen to satisfy  $(g/\pi_1)_5 = \zeta$ , so that  $(g/\pi_i)_5 = \zeta^i$ , and the  $\pi_j$  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  $\zeta$ ) satisfy

1.  $S(\zeta) \cdot S(\zeta^{-1}) \equiv [S(1)]^2 \pmod{5}$ ,
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  $\Delta_a$  represent? For example the expression

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

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

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  $\pi_i$  in the expression for  $\Delta_a$  and ask what  $\Delta_a$  then represents. The object of this note is to answer these questions and also to determine the set  $\{\Delta_a \mid a = 1, 2, 3, \dots, p-1\}$ .

It is immediate that  $\Delta_a$  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

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

It follows that the distinct values taken by the  $\Delta_a$ , for  $a = 1, 2, \dots, p-1$  are just  $\pm \Delta_g, \pm \Delta_{g2}, \pm \Delta_{g3}, \pm \Delta_{g4}, \pm \Delta_{g5}$ . 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 $\Delta_a$ WITHOUT THE NORMALIZATION RESTRICTIONS ON THE $\pi_j$

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

$$(3) \quad \Delta_a(\pi) = \left( \frac{-a}{p} \right)_Z \cdot \left[ \left( \frac{4a}{\pi_1} \right)_5 \cdot \pi_1 \pi_3 + \left( \frac{4a}{\pi_2} \right)_5 \cdot \pi_1 \pi_2 + \left( \frac{4a}{\pi_3} \right)_5 \cdot \pi_3 \pi_4 + \left( \frac{4a}{\pi_4} \right)_5 \cdot \pi_2 \pi_4 \right].$$

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

Let the condition  $(g/\pi)_5 = \zeta$  be retained first so that we only change  $\pi$  to an associate  $\eta \pi$  where  $\eta = \zeta^i \varepsilon$  ( $0 \leq i \leq 4$ ) with  $\varepsilon$  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.**  $\Delta_a(\zeta^i \varepsilon \cdot \pi) = \Delta_{ab}(\pi)$  where  $(b/\pi)_5 = \zeta^{5-i}$  and  $(b/p)_Z \neq N_{Q(\sqrt{5})/Q}(\varepsilon)$ .