

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 21 (1975)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: NOTES ON THE CONGRUENCE $y^2 \equiv x^5 - a \pmod{p}$
Autor: Rajwade, A. R.
Kapitel: 6. A RELATION AND AN EXAMPLE
DOI: <https://doi.org/10.5169/seals-47329>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 28.03.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

so that substitution in (5) gives

$$\Delta_a(\pi) = (-a/p)_Z \cdot \begin{cases} \frac{1}{4}(25w - x - 10u - 20v) & \text{if } v \equiv 1 \pmod{5}, \\ \frac{1}{4}(-25w - x - 20u + 10v) & \text{if } v \equiv 2 \pmod{5}, \\ \frac{1}{4}(-25w - x + 20u - 10v) & \text{if } v \equiv 3 \pmod{5}, \\ \frac{1}{4}(25w - x + 10u + 20v) & \text{if } v \equiv 4 \pmod{5}. \end{cases}$$

But letting $(x, u, v, w) \rightarrow (x, -u, -v, w), (x, v, -u, -w), (x, -v, u, -w)$ in the case $v \equiv 1 \pmod{5}$ gives just the cases $v \equiv 2, 3, 4 \pmod{5}$ respectively. This completes the proof of theorem 4.

6. A RELATION AND AN EXAMPLE

THEOREM 5. $(\Delta_g)^2 + (\Delta_{g^2})^2 + (\Delta_{g^3})^2 + (\Delta_{g^4})^2 + (\Delta_{g^5})^2 = 20 \cdot p$

Proof. The left hand side

$$\begin{aligned} &= [f(x, u, v, w)]^2 + [f(x, -u, -v, w)]^2 + \\ &\quad [f(x, v, -u, -w)]^2 + [f(x, -v, u, -w)]^2 + x^2 \\ &= \frac{1}{16} [4 \cdot 625w^2 + 4 \cdot x^2 + 1000(u^2 + v^2)] + x^2 \end{aligned}$$

on simplifying

$$\begin{aligned} &= \frac{5}{4} (125w^2 + x^2 + 50u^2 + 50v^2) = \frac{5}{4} \cdot 16 \cdot p \text{ (by } i \text{ of (4))} \\ &= 20 \cdot p \end{aligned}$$

as required.

An example. Let $p = 11$. The 4 solutions of (4) are

$$(1, 0, 1, 1), (1, 0, -1, 1), (1, 1, 0, -1), (1, -1, 0, -1)$$

and so by theorem 4 the set Δ_a is given by $\pm 1, \pm 4, -9, \pm 11, \pm 1$, so that $1^2 + 4^2 + 9^2 + 11^2 + 1^2 = 220 = 20 \cdot p$.

A direct computation gives the following values

$$\begin{aligned} a &= 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \\ \Delta_a &= 4, -9, -1, -11, -1, 1, 11, 1, 9, -4 \end{aligned}$$

The fifth powers are $4a = 1, 10$ that is $a = 3, 8$ and for these $\Delta_3 = (-3/p)_{\mathbf{Z}} \cdot x = -x = -1$ and $\Delta_8 = (-8/p)_{\mathbf{Z}} \cdot x = x = 1$ as required.

I should like to thank Professor Frohlich sincerely for his suggestion to look at these Δ_a .

APPENDIX

1. For the convenience of the reader we give here the definition of $(\alpha/\beta)_{10}$, the tenth power residue symbol and some of its properties.

First let π be a prime factor of a rational prime $p \equiv 1 \pmod{5}$. The residue classes mod π , in $\mathbf{Z}[\zeta]$, form a field of norm $\pi = p$ elements. The non-zero classes form a cyclic group (multiplicative) $1, \rho, \dots, \rho^{p-2}$ of $p - 1$ elements. This group has in it just 10 elements or order dividing 10 viz. $\rho^{j(p-1)/10}$ ($j = 0, 1, \dots, 9$). These are represented (mod π) by $\pm 1, \pm \zeta, \dots, \pm \zeta^4$, since these are distinct mod π and have order dividing 10. Now let α be any non-zero residue mod π . Then $\alpha^{(p-1)/10}$ has order dividing 10 and so is congruent to one of $\pm 1, \pm \zeta, \dots, \pm \zeta^4 \pmod{\pi}$. We define $(\alpha/\pi)_{10} = \pm 1, \pm \zeta, \dots, \pm \zeta^4$ according as $\alpha^{(p-1)/10}$ is congruent to $\pm 1, \pm \zeta, \dots, \pm \zeta^4 \pmod{\pi}$. It follows that

$$(\alpha/\pi)_{10} \equiv \alpha^{(N\pi-1)/10} \pmod{\pi}.$$

It is immediately verified that $(\alpha\beta/\pi)_{10} = (\alpha/\pi)_{10} \cdot (\beta/\pi)_{10}$, and we define $(\alpha/\pi_1\pi_2)_{10} = (\alpha/\pi_1)_{10} \cdot (\alpha/\pi_2)_{10}$. The following properties may be easily verified directly from the definition.

(i). If $p \equiv 2, 3 \pmod{5}$, so that p stays prime in $\mathbf{Z}[\zeta]$, and if $n \in \mathbf{Z}$, then $(n/p)_{10} = 1$.

(ii). If π is a prime factor of a $p \equiv 4 \pmod{5}$, so that $p = \pi \bar{\pi}$ is the prime decomposition of p in $\mathbf{Z}[\zeta]$, and $n \in \mathbf{Z}$, then

$$(n/\pi)_{10} = 1.$$

(iii). If π is a prime factor of a $p \equiv 1 \pmod{5}$, so that $p = \pi_1 \pi_2 \bar{\pi}_2 \bar{\pi}_1$ is the prime decomposition of p in $\mathbf{Z}[\zeta]$, then

$$(n/\pi)_{10} \cdot (n/\bar{\pi})_{10} = 1.$$