

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.
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: 31.03.2026

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

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 Δ_a is equal to ¹⁾

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

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

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

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

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 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 $\{\Delta_a \mid a = 1, 2, 3, \dots, p - 1\}$.

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 $a = 1, 2, \dots, p - 1$ 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 $p = \pi \cdot \pi^\sigma \cdot \pi^{\sigma^3} \cdot \pi^{\sigma^2}$ (with $(g/\pi)_5 = \zeta) = \pi_1 \pi_2 \pi_3 \pi_4$ say. Since the restrictions on π are going to be removed, we denote Δ_a by $\Delta_a(\pi)$. We write (2) in a more convenient form viz

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

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

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

Proof. Step 1.

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

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.

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

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

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

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

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 occurring 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 $(-a/p)_Z (4a/\pi)_5 \cdot \pi \cdot \pi^\sigma +$ conjugates, $(-a/p)_Z (4a/\pi)_5 \cdot \pi^\sigma \cdot \pi^{\sigma^2} +$ conjugates and $(-a/p)_Z (4a/\pi)_5 \cdot \pi^{\sigma^2} \cdot \pi^{\sigma^3} +$ 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 $\text{Tr} [(-a/p)_Z (4a/\pi)_5 \cdot \pi \pi^\sigma]$. We have the following theorem:

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

Proof. We have

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

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 $\{\Delta_a \mid a = 1, 2, 3, \dots, p-1\}$

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

$$(4) \quad \begin{array}{l} \text{i. } 16p = x^2 + 50u^2 + 50v^2 + 125w^2 \\ \text{ii. } v^2 - 4uv - u^2 = xw \\ \text{iii. } x \equiv 1 \pmod{5} \end{array}$$

have exactly 4 integral simultaneous solutions. If (x, u, v, w) is one solution then the remaining three are $(x, -u, -v, w)$, $(x, v, -u, -w)$, $(x, -v, u, -w)$.

Now let $f(x, u, v, w) = \frac{1}{4}(25w - x - 10u - 20v)$. We have the following

THEOREM 4. *The distinct Δ_a are the following 10 numbers :*

$$\begin{array}{l} \pm x, \pm f(x, u, v, w), \pm f(x, -u, -v, w), \pm f(x, v, -u, -w), \\ \pm f(x, -v, u, -w). \end{array}$$

Remark. If $4a$ is a quintic residue mod p then $\Delta_a = (-a/p)_{\mathbf{Z}} \cdot x$.

Proof. In the notation of [2] we have

$$\Delta_a = (-a/p)_{\mathbf{Z}} \left[\left(\frac{4a}{\pi_1} \right)_5 \cdot T + \left(\frac{4a}{\pi_2} \right)_5 + S \cdot \left(\frac{4a}{\pi_3} \right)_5 \cdot \bar{S} + \left(\frac{4a}{\pi_4} \right)_5 \cdot \bar{T} \right]$$

with $T = s_1 \zeta + s_2 \zeta^2 + s_3 \zeta^3 + s_4 \zeta^4$ and $S = s_3 \zeta + s_1 \zeta^2 + s_4 \zeta^3 + s_2 \zeta^4$. Let $4a \equiv g^v \pmod{p}$. We have to look at the five cases $v \equiv 0, 1, 2, 3, 4 \pmod{5}$.

If $v \equiv 0 \pmod{5}$, so that $(4a/\pi_i)_5 = 1$ for all i , then

$$\begin{aligned} \Delta_a &= (-a/p)_{\mathbf{Z}} (T + \bar{T} + S + \bar{S}) = (-a/p)_{\mathbf{Z}} [(s_1 + s_4)(\zeta + \zeta^4) \\ &+ (s_2 + s_3)(\zeta^2 + \zeta^3) + (s_2 + s_3)(\zeta + \zeta^4) + (s_1 + s_4)(\zeta^2 + \zeta^3)] \\ &= (-a/p)_{\mathbf{Z}} [-(s_1 + s_2 + s_3 + s_4)] = (-a/p)_{\mathbf{Z}} \cdot x \text{ (see equation (62) of [1]).} \end{aligned}$$

If $v \equiv 1, 2, 3, 4 \pmod{5}$, we get respectively, as above

$$(5) \quad \Delta_a(\pi) = (-a/p)_{\mathbf{Z}} \begin{cases} 4s_4 - (s_1 + s_2 + s_3) & \text{if } v \equiv 1 \pmod{5}, \\ 4s_3 - (s_1 + s_2 + s_4) & \text{if } v \equiv 2 \pmod{5}, \\ 4s_2 - (s_1 + s_3 + s_4) & \text{if } v \equiv 3 \pmod{5}, \\ 4s_1 - (s_2 + s_3 + s_4) & \text{if } v \equiv 4 \pmod{5}. \end{cases}$$

Now from equations (62) and (63) of [1] we get, on solving

$$\begin{array}{l} 4s_1 = 5w - x + 2u + 4v, \\ 4s_2 = -5w - x + 4u - 2v, \\ 4s_3 = -5w - x - 4u + 2v, \\ 4s_4 = 5w - x - 2u - 4v. \end{array}$$

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

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

(iv). If π is a complex prime factor of a $p \equiv 1, 4 \pmod{5}$ and σ of a $q \equiv 1, 4 \pmod{5}$, then $\overline{(\pi/\sigma)_{10}} = (\bar{\pi}/\bar{\sigma})_{10}$.

2. The symbol $(\alpha/\beta)_5$ is defined in the same way and has similar properties.

3. The symbol $(a/p)_{\mathbf{Z}}$ is simply the ordinary Legendre symbol, the subscript \mathbf{Z} is used to distinguish it from the symbol $(\alpha/\beta)_2$ which denotes the quadratic character of α modulo β in a given ring, e.g. if $\alpha, \beta \in \mathbf{Z}[i]$

$$\text{then } (\alpha/\beta)_{\mathbf{Z}[i]} = \begin{cases} 1 & \text{if } x^2 \equiv \alpha \pmod{\beta} \text{ is solvable in } \mathbf{Z}[i], \\ -1 & \text{otherwise.} \end{cases}$$

REFERENCES

- [1] DICKSON, L. E. Cyclotomy, higher congruences and Waring's problem. *American Journal of Mathematics*, 57 (1935), pp. 391-424.
- [2] RAJWADE, A. R. On rational primes p congruent to 1 (mod 3 or 5). *Proc. Camb. Phil. Soc.* 66 (1969), pp. 61-70.
- [3] ——— On the congruence $y^2 \equiv x^5 - a \pmod{p}$. *Proc. Camb. Phil. Soc.* (to appear).

(Reçu le 7 janvier 1975)

A. R. Rajwade

Department of Mathematics
Panjab University
Chandigarh, India