

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 20 (1974)
Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE NUMBER OF SOLUTIONS OF THE CONGRUENCE $y^2 \equiv x^4 - a \pmod{p}$
Autor: Singh, Surjit / Rajwade, A. R.
Kapitel: 3. Cyclotomy for $p = 1 + 4f$.
DOI: <https://doi.org/10.5169/seals-46910>

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: 18.04.2026

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

3. CYCLOTOMY FOR $p = 1 + 4f$.

Let g be a primitive root mod p which we have already fixed in § 2. Divide the non-zero residues mod p into four classes A_0, A_1, A_2, A_3 by putting $m \equiv g^v$ in A_i if $v \equiv i \pmod{4}$. The cyclotomic constants (h, k) ($0 \leq h, k \leq 3$) are defined to be the number of values of $y, 1 \leq y \leq p - 2$ for which

$$(3.1) \quad y \equiv g^{4t+h} \pmod{p}, \quad 1 + y \equiv g^{4s+k} \pmod{p}$$

[i.e. for which $y \in A_h, 1 + y \in A_k$].

As results differ in the two cases $p \equiv 1 \pmod{8}$ and $p \equiv 5 \pmod{8}$ we look at these cases separately.

Case 1: $p \equiv 1 \pmod{8}$. In this case $p = 1 + 4f$ where f is even. We know [3] that

$$(3.2) \quad \begin{cases} (h, k) = (k, h) \\ (h, k) = (-h, k-h) \end{cases}$$

Thus $(1, 2) = (2, 3) = (1, 3); (1, 1) = (0, 3); (2, 2) = (0, 2); (3, 3) = (0, 1)$. Therefore of the 16 cyclotomic constants which may be written as a (4×4) matrix, only five are different and we have

$$(3.3) \quad \begin{bmatrix} (0, 0) & (1, 0) & (2, 0) & (3, 0) \\ (0, 1) & (1, 1) & (2, 1) & (3, 1) \\ (0, 2) & (1, 2) & (2, 2) & (3, 2) \\ (0, 3) & (1, 3) & (2, 3) & (3, 3) \end{bmatrix} = \begin{bmatrix} A & D & C & B \\ D & B & E & E \\ C & E & C & E \\ B & E & E & D \end{bmatrix}$$

Consider the numbers $1, 2, \dots, p - 1$. Each $y \in A_0$ (there are f such y 's) except the last (i.e. $p - 1$ which is in A_0 in this case) is followed by $y + 1$ which may belong to A_0, A_1, A_2 or A_3 .

Similarly each $y \in A_1$ without exception is followed by $y + 1$ which may belong to A_0, A_1, A_2 or A_3 and so on. Hence we get

$$(3.4) \quad A + D + C + B = f - 1$$

$$(3.5) \quad D + B + 2E = f$$

$$(3.6) \quad 2C + 2E = f.$$

Case 2: $p \equiv 5 \pmod{8}$. In this case $p = 4f + 1$ where f is odd. Now look at the congruence

$$(3.1)' \quad 1 + g^{4t+h} + g^{4s+k} \equiv 0 \pmod{p}.$$

Denote the number of solutions of (3.1)' by $\{h, k\}$. Then clearly $\{h, k\} = \{k, h\}$ and the following relations are known [3]

$$(3.2)' \quad \begin{cases} \{-h, k-h\} = \{h, k\} \text{ for any } f \text{ even or odd} \\ \{h, k\} = (h, k+2) \text{ for } f \text{ odd.} \end{cases}$$

Thus $\{1, 0\} = \{3, 3\}$; $\{3, 0\} = \{1, 1\}$; $\{2, 0\} = \{2, 2\}$ and $\{3, 1\} = \{1, 2\} = \{3, 2\}$.

Therefore the matrix of the cyclotomic constants $\{h, k\}$ can be written as

$$(3.3)' \quad \begin{bmatrix} \{0, 0\} & \{1, 0\} & \{2, 0\} & \{3, 0\} \\ \{0, 1\} & \{1, 1\} & \{2, 1\} & \{3, 1\} \\ \{0, 2\} & \{1, 2\} & \{2, 2\} & \{3, 2\} \\ \{0, 3\} & \{1, 3\} & \{2, 3\} & \{3, 3\} \end{bmatrix} = \begin{bmatrix} L & M & N & R \\ M & R & S & S \\ N & S & N & S \\ R & S & S & M \end{bmatrix}$$

Since f is odd, $p - 1$ belongs to A_2 hence in this case as before

$$\begin{aligned} (0, 1) + (0, 1) + (0, 2) + (0, 3) &= f \\ (1, 0) + (1, 1) + (1, 2) + (1, 3) &= f \\ (2, 0) + (2, 1) + (2, 2) + (2, 3) &= f - 1. \end{aligned}$$

Now using (3.2)' and (3.3)' we get

$$(3.4)' \quad L + M + N + R = f$$

$$(3.5)' \quad R + M + 2S = f$$

$$(3.6)' \quad 2N + 2S = f - 1.$$

4. THE JACOBI FUNCTION

Let α be any root ($\neq 1$) of $\alpha^{p-1} = 1$. Write

$$(4.1) \quad F(\alpha) = \sum_{k=0}^{p-2} \alpha^k \zeta^{qk} \text{ where } \zeta^p = 1 \text{ and } \zeta \neq 1.$$