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 $y^2 \equiv x^4 – a(mod \quad p)$

Autor: Singh, Surjit / Rajwade, A. R.

Kapitel: 3. Cyclotomy for p = 1 + 4f.

DOI: https://doi.org/10.5169/seals-46910

3. CYC.OTOMY 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 cyclomic constants (h, k) $(0 \leqslant h, k \leqslant 3)$ are defined to be the number of values of y, $1 \leqslant y \leqslant p - 2$ for which

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

[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 as these cases separately.

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

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

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

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

Consider the numbers $1, 2, \ldots, p - 1$. 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

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

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

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

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

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

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

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

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

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

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

$$(0, 1) + (0, 1) + (0, 2) + (0, 3) = f$$

$$(1, 0) + (1, 1) + (1, 2) + (1, 3) = f$$

$$(2, 0) + (2, 1) + (2, 2) + (2, 3) = f - 1 .$$

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

$$L + M + N + R = f \tag{3.4)'$$

$$R + M + 2S = f \tag{3.5)'$$

$$2N + 2S = f - 1 . \tag{3.6)'$$

4. The Jacobi function

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

$$F(\alpha) = \sum_{k=o}^{p-2} \alpha^k \zeta^{g^k} \text{ where } \zeta^p = 1 \text{ and } \zeta \neq 1 . \tag{4.1}$$