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(mod \quad p)

Autor: Rajwade, A. R.

Kapitel: 6. A RELATION AND AN EXAMPLE

DOI: https://doi.org/10.5169/seals-47329

so that substitution in (5) gives

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

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

6. A RELATION AND AN EXAMPLE

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

Proof. The left hand side

$$= [f(x, u, v, w)]^2 + [f(x, -u, -v, w)]^2 + [f(x, v, -u, -w)]^2 + [f(x, -v, u, -w)]^2 + x^2$$

$$= \frac{1}{16}[4 \,.\, 625 w^2 + 4 \,.\, x^2 + 1000(u^2 + v^2)] + x^2$$

on simplifying

$$= \frac{5}{4}(125 w^2 + x^2 + 50u^2 + 50v^2) = \frac{5}{4} \,.\, 16 \,.\, p \quad (\text{by } i \text{ of } (4))$$

$$= 20 \,.\, p$$

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 $1^2 + 4^2 + 9^2 + 11^2 + 1^2 = 220 = 20 \,.\, \text{p}$.

A direct computation gives the following values

$$a = 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 7, \quad 8, \quad 9, \quad 10$$
$$\Delta_a = 4, \ -9, \ -1, \ -11, \ -1, \ 1, \ 11, \ 1, \ 9, \ -4$$

The fifth powers are $4a = 1, 10$ that is $a = 3, 8$ and for these $\Delta_3 = (-3/p)_Z \cdot x = -x = -1$ and $\Delta_8 = (-8/p)_Z \cdot x = x = 1$ 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) $1, \rho, \ldots, \rho^{p-2}$ of $p-1$ elements. This group has in it just 10 elements or order dividing 10 viz. $\rho^{j(p-1)/10}$ $(j = 0, 1, \ldots, 9)$. These are represented (mod π) by $\pm 1, \pm\zeta, \ldots, \pm \zeta^4$, 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 $\pm 1, \pm \zeta, \ldots, \pm \zeta^4 \pmod \pi$. We define $(\alpha/\pi)_{10} = \pm 1, \pm \zeta, \ldots, \pm \zeta^4$ according as $\alpha^{(p-1)/10}$ is congruent to $\pm 1, \pm \zeta, \ldots, \pm \zeta^4 \pmod \pi$. 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

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