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: 5. The set {Aa \a = 1, 2, 3,...,/? – 1}

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

Since the choice of g is arbitrary, we change g to another primitive root g^r with $(r, p-1) = 1$, $r = i \,(\text{mod } 5)$, $i = 1, 2, 3, 4$. 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 occuring 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 $(-a/p)_Z (4a/\pi)_5 \,.\, \pi \,.\, \pi^\sigma$ + conjugates, $(-a/p)_Z (4a/\pi)_5 \,.\, \pi^\sigma \,.\, \pi^{\sigma^2}$ + conjugates and $(-a/p)_Z (4a/\pi)_5 \,.\, \pi^{\sigma^2} \,.\, \pi^{\sigma^3}$ + 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 $\text{Tr}\,[(-a/p)_Z (4a/\pi)_5 \,.\, \pi\,\pi^\sigma]$. We have the following theorem:

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

Proof. We have

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

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

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

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

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:*

$$\pm x, \ \pm f(x,u,v,w), \ \pm f(x, -u, -v, w), \ \pm f(x, v, -u, -w),$$
$$\pm f(x, -v, u, -w).$$

Remark. If $4a$ is a quintic residue mod p then $\Delta_a = (-a/p)_Z \, . \, x$.

Proof. In the notation of [2] we have

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

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 $4a \equiv g^\nu \pmod{p}$. We have to look at the five cases $\nu \equiv 0, 1, 2, 3, 4 \pmod{5}$.

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

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

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

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

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

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

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

Proof. The left hand side

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

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

on simplifying

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

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

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