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: 4. Expressions allied to $\Delta_a (\pi)$

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 $(r, p-1) = 1$, $r = i \pmod 5$, $i = 1, 2, 3, 4$. 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 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 $\mathrm{Tr}\,[(-a/p)_Z (4a/\pi)_5 . \pi\, \pi^\sigma]$. We have the following theorem:

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

Proof. We have

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

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