

5. The set $\{Aa \mid a = 1, 2, 3, \dots, /? - 1\}$

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **21 (1975)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **23.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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 occurring 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 $(-a/p)_Z (4a/\pi)_5 \cdot \pi \cdot \pi^\sigma +$ conjugates, $(-a/p)_Z (4a/\pi)_5 \cdot \pi^\sigma \cdot \pi^{\sigma^2} +$ conjugates and $(-a/p)_Z (4a/\pi)_5 \cdot \pi^{\sigma^2} \cdot \pi^{\sigma^3} +$ 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 $\text{Tr} [(-a/p)_Z (4a/\pi)_5 \cdot \pi \pi^\sigma]$. We have the following theorem:

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

Proof. We have

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

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

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

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

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 :*

$$\begin{array}{l} \pm x, \pm f(x, u, v, w), \pm f(x, -u, -v, w), \pm f(x, v, -u, -w), \\ \pm f(x, -v, u, -w). \end{array}$$

Remark. If $4a$ is a quintic residue mod p then $\Delta_a = (-a/p)_{\mathbf{Z}} \cdot x$.

Proof. In the notation of [2] we have

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

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

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

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

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

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

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

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

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

Proof. The left hand side

$$\begin{aligned} &= [f(x, u, v, w)]^2 + [f(x, -u, -v, w)]^2 + \\ &\quad [f(x, v, -u, -w)]^2 + [f(x, -v, u, -w)]^2 + x^2 \\ &= \frac{1}{16} [4 \cdot 625w^2 + 4 \cdot x^2 + 1000(u^2 + v^2)] + x^2 \end{aligned}$$

on simplifying

$$\begin{aligned} &= \frac{5}{4} (125w^2 + x^2 + 50u^2 + 50v^2) = \frac{5}{4} \cdot 16 \cdot p \text{ (by } i \text{ of (4))} \\ &= 20 \cdot p \end{aligned}$$

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 $1^2 + 4^2 + 9^2 + 11^2 + 1^2 = 220 = 20 \cdot p$.