STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1956-020

Voordracht in de srie
"Actualiteiten"

Griek-Latijnse vierkanten

J. Verhoeff

Rapport ZW 1956-020

Voordracht in de serie

"Actualiteiten"

door

J. Verhoeff

24 November 1956

Grieks-Latijnse vierkanten

§ 0. Inleiding

Wanneer in een vierkant met n x n hokjes in elke rij een permutatie van n symbolen (objecten of officieren) is geplaatst, dusdanig dat in elke kolom ook een permutatie van die symbolen staat, dan noemt men dit een Latijns vierkant (afkorting L-v_n)
Bijvoorbeeld van een L-v_2 $\begin{array}{|c|c|}\hline 1&2\\\hline 2&1\\\hline\end{array}$.

De rijen en de kolommen kunnen wij op één of andere manier nummeren bijvoorbeeld van boven naar beneden, resp. van links naar rechts. Het element uit het hokje gelegen in de i-de rij en de j-de kolom duiden wij aan met a_{ij}. Bij elke (vaste) i vormen dus de symbolen a_{ij} $(j = 1,\ldots,n)$ en permutatie van de n symbolen evenals bij elke (vaste) j de symbolen a_{ij} voor $i = 1,\ldots,n$.

Twee L-v_n's a'_{ij} en a''_{ij} heten orthogonaal als de n^2 paren (a'_{ij},a''_{ij}) $(i,j = 1,\ldots,n)$ alle verschillend zijn. Een k-tal L-v_n's a_{ij}^{l} $(l = 1,\ldots,k)$ heet orthogonaal als elk tweetal dat is.
Bijvoorbeeld voor k = 4 en n = 5.

1	5	4	3	2
2	1	5	4	3
3	2	1	5	4
4	3	2	1	5
5	4	3	2	1

1	5	4	3	2
3	2	1	5	4
5	4	3	2	1
2	1	5	4	3
4	3	2	1	5

1	5	4	3	2
4	3	2	1	5
2	1	5	4	3
5	4	3	2	1
3	2	1	5	4

1	5	4	3	2
5	4	3	2	1
4	3	2	1	5
3	2	1	5	4
2	1	5	4	3

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

Een ander voorbeeld is, beknopt geschreven,

harten aas(!)	schoppen heer (+)	ruiten vrouw(?)	klaveren boer (x)
schoppen boer (?)	harten vrouw(x)	klaveren heer (!)	ruiten aas(+)
ruiten heer (x)	klaveren aas (?)	harten boer (+)	schoppen vrouw(!)
klaveren vrouw(+)	ruiten boer (!)	schoppen aas (x)	harten heer (?)

De kaarten zijn uit vier spellen (!),(?),(x),(+) zodanig gekozen, dat er uit geen enkel spel twee van dezelfde kleur of hetzelfde plaatje zijn genomen.

Wanneer men uit twee orthogonale L-v_n's α_{ij} en a_{ij} een vierkant vormt met op de i,j-de plaats het paar (α_{ij},a_{ij}) dan spreekt men van een Grieks-Latijns vierkant (afkorting G-L-v_n). Euler [1] heeft (voor zover ons bekend) voor het eerst het probleem van de constructie van zulke vierkanten gesteld. Hij vroeg nl. 36 officieren van 6 verschillende regimenten en 6 verschillende rangen, waarbij geen twee officieren uit eenzelfde regiment dezelfde rang hebben, dusdanig in een carré op te stellen, dat in elke rij en in elke kolom zowel elk regiment als elke rang vertegenwoordigd is. Dit staat bekend als het probleem der 36 officieren, ongetwijfeld een van de moeilijkste opgaven waar 36 officieren ooit voor gesteld zijn. Eerst in 1900('01) werd door Tarry [2] de onmogelijkheid aangetoond. Hij deed dit door alle mogelijkheden te proberen (zie ook Fisher and Yates [6] , 1934, en Yamamoto [15] , 1954). Euler had reeds het vermoeden, dat voor $n \equiv 2 \pmod 4$ er geen oplossing zou bestaan. Men noemt een G-L-v_n ook wel een n x n-Euler vierkant.

Slaagt men erin om de n^2 getallen $0,1,\ldots,n^2-1$, in het n-tallig stelsel geschreven, zó in een carré te plaatsen, dat zowel de eerste als de tweede cijfers per rij en per kolom een permutatie van $0,1,\ldots,n$ vormen, dan heeft men een Euler-vierkant, bijvoorbeeld

00	11	22	33
13	02	31	20
21	30	03	12
32	23	10	01

In het 10-tallige stelsel (elk getal bovendien met 1 verhoogd)

is dit

1	6	11	16
12	3	14	9
10	13	4	7
15	12	5	2

Het is een 4 x 4 tovervierkant. Dit geldt algemeen, daar uit $A_{ij} = n\alpha_{ij} + a_{ij} + 1$ (α_{ij} en a_{ij} beide L-v_n's)

volgt $\sum_{i=1}^{n} A_{ij} = n\sum_{i} \alpha_{ij} + n + \sum_{i} a_{ij} = \frac{1}{2}n^2(n-1) + n + \frac{1}{2}n(n-1) = \sum_{j=1}^{n} A_{ij}$. Het "tovervierkant zijn" is een kennelijk zwakkere eis. Er bestaat immers geen G-L-v_6 en wel een 6 x 6 tovervierkant, zoals

23	18	22	15	13	20
26	25	10	9	30	11
35	6	3	4	31	32
2	36	33	34	1	5
8	7	27	28	12	29
17	19	16	21	24	14

.

Bovenstaande beschouwingen laten zich generaliseren voor kubussen en hyperkubussen. Voor $n = p^k$ (p = priem) laten deze zich gemakkelijk (d.w.z. zonder veel denkwerk) construeren.

Er rijzen nu drie vragen.

1e. Hoe contrueert men Grieks-Latijnse vierkanten of zelfs zo groot mogelijke orthogonale stelsels L-v_n's?(§ 1)

2e. Indien 1e niet lukt voor bepaalde n,kan dan bewezen worden, dat er geen G-L-v_n's bestaan voor deze n? (§ 2)

3e. Hoeveel essentieel verschillende G-L-v_n's bestaan er voor vaste n? Met deze vraag zullen wij ons hier niet bezighouden.

§ 1. Constructie [7,9,10,11,14]

Stel de ontbinding van n in priemfactoren is $\prod_{i=1}^{r} p_i^{\alpha_i}$. Wij zullen een stelsel van $\rho = \min_i(p_i^{\alpha_i}-1)$ orthogonale L-v_n's construeren (voor n = 2 + 4m doen wij dus eigenlijk niets) Voor n = 3 vinden wij direct

1	3	2
2	1	3
3	2	1

en

1	2	3
2	3	1
3	1	2

voor n = 4 of 5 voldoen de bovengenoemde voorbeelden.

De gevallen n = 3 en n = 5 suggereren voor n = p(riem) de oplossing $a^k_{ij} = i + kj$ $(k = 1,\ldots,p-1)$; a^k_{ij} is een L-v_p daar kj met j een volledig rest systeem mod p doorloopt. Zij zijn onderling orthogonaal, daar uit $\left\{\begin{matrix} i + kj = r + ks & \text{en} & k \neq l \\ i + lj = r + ls & & 0 < k,\ l < p \end{matrix}\right\}$ volgt $(k-l)(j-s) \equiv 0 \bmod p$, dus $j = s$ en $i = r$.

Men kan de bovenstaande oplossing en die voor n = 4 zó zien: Eén der vierkanten is de Caley tabel van een groep (voor n = p de cyclische groep van de orde p en voor n = 4 de groep van Klein). Het i,j-de element is dan ij^{-1} (vermenigvuldiging in de groep, gemakshalve noemen wij de rijen en kolommen naar elementen van de desbetreffende groep). In de andere vierkanten is $a_{i,j} = (\sigma i)j^{-1}$ waarbij σ een automorfie is, die geen enkel element behalve het eenheidselement op zijn plaats laat. Zelfs is het zo, dat het l-de L-v_n ontstaat door σ^{l-1} toe te passen, waarbij σ^l voor l = 1, 2,...,n-2 automorfieën zijn die alleen de eenheid invariant laten $(\text{en } \sigma^{n-1} = 1)$. Uiteraard zijn dit L-$v_n$'s. Zij zijn ook orthogonaal daar uit $\left\{\begin{matrix} (\sigma^l i)j^{-1} = (\sigma^l r)s^{-1} & l,k = 0,\ldots,n-2 \\ \text{en } (\sigma^k i)j^{-1} = (\sigma^k r)s^{-1} & \end{matrix}\right\}$ volgt

$$(\sigma^k i)(\sigma^l i)^{-1} = (\sigma^k r)(\sigma^l r)^{-1} = (\sigma^k i)\,\sigma^k(i^{-1}r)(\sigma^l r)^{-1} \quad \text{of wel}$$

$$(\sigma^l r)^{-1}(\sigma^l r) = \sigma^k(i^{-1}r)$$

$$i^{-1}r = \sigma^{k-l}(i^{-1}r) \quad \text{dus } i = r \text{ en } j = s\ .$$

Nu het algemene geval $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Als groep nemen wij het directe product (som) van cyclische groepen van priemorde

$$G = (\underbrace{p_1,p_1,\ldots,p_1}_{\alpha_1 \text{ keer}}, \underbrace{p_2,\ldots,p_2}_{\alpha_2 \text{ keer}}, \ldots, \underbrace{p_r,\ldots,p_r}_{\alpha_r \text{ keer}})$$

Voor de groepen $G_i = (\underbrace{p_i,\ldots,p_i}_{\alpha_i \text{ keer}})$ $i = 1,\ldots,r$ is gemakkelijk een automorfie σ aan te geven, zodat σ^k voor $k = 1,\ldots,p_i^{\alpha_i}-2$ de eenheid invariant laat, en dat $\sigma^k = 1$ voor $k = p_i^{\alpha_i} - 1$. Hiertoe gebruiken wij de volgende stellingen uit de theorie der eindige lichamen.

1e. Het aantal elementen van een eindig lichaam K is een macht van een priemgetal en bij elke p en elke k hoort een eindig lichaam met p^k elementen.

2e. De additieve groep K^+ van een eindig lichaam met p^k elementen is isomorf met de directe som van k cyclische groepen van de orde p

3^e. De elementen $\neq 0$ uit K vormen t.o.v. de vermenigvuldiging een cyclische groep K^x van de orde $p^k - 1$.
4^e. De vermenigvuldiging met een element uit K^x werkt op K^+ als een automorfie, die alleen de nul invariant laat.
Krachtens 3^e bestaat er dus een automorfie σ zodat σ^l voor $l = 1,\ldots,p^k-2$ alleen de nul invariant laat en zodat σ^l voor $l = p^k-1$ de identiteit is. Dit geeft dus voor elk der groepen G_i $p_i^{\alpha_i} - 1$ automorfieën (machten van σ_i). Voor $G = (G_1,G_2,\ldots,G_r)$ kiezen wij nu de automorfieën σ^l: $\sigma^l(x_1,x_2,\ldots,x_r) = (\sigma_1^l x_1, \sigma_2^l x_2,\ldots,\sigma_r^l x_r)$; $x_i \in G_i$ en $l = (0,1,\ldots,\rho)$ $\rho = \min_i(p_i^{\alpha_i}-1)$. Deze geven ρ orthogonale L-v_n's, zoals beloofd was.

Opmerking

Men kan ook laten zien, dat uit een gegeven Grieks-Latijnse vierkanten voor $n = a$ en $n = b$ er één voor $n = ab$ geconstrueerd kan worden.

Bovenstaande oplossingen ontstaan dus door in een groepstabel bijvoorbeeld de kolommen "volgens een automorfie" te permuteren. Deze permutaties behoeven echter geen automorfieën te zijn, zoals het volgende voorbeeld laat zien: $n = 12$, $G = (2,2,3)$. De basiselementen zijn P,Q en R met de relaties $P^2 = R^2 = Q^3 = 1$.
De permutatie van de kolommen is:

$$\begin{pmatrix} 1, & P, & R & PR, & Q, & PQ, & RQ, & PRQ, & Q^2, & PQ^2, & RQ^2, & PRQ^2 \\ 1, & RQ, & PQ^2, & RQ^2, & Q^2, & PR, & PQ, & RQ, & Q, & PRQ^2, & P, & R \end{pmatrix}$$

en dit is geen automorfie. Dergelijke oplossingen heten gebaseerd op een groep.

H.B. Mann [11,12] bewees, dat, als $n = 4m + 2$ er geen Grieks-Latijnse vierkanten bestaan, die op een groep gebaseerd zijn. Hij bewees verder, dat voor $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ er met de "automorfie-methode" niet meer dan $\rho = \min_i(p_i^{\alpha_i}-1)$ orthogonale L-vierkanten geconstrueerd kunnen worden.

§2. Non-existentie bewijzen

Euler vermoedde: voor $n \equiv 2 \pmod 4$ bestaan er geen G-L-v_n. Wernicke [3], 1910 gaf een "bewijs" van dit vermoeden in de verscherpte vorm. Voor $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ bestaan er hoogstens $\rho = \min_i(p_i^{\alpha_i}-1)$ orthogonale L-v_n. Tot in 1921 Mc Neish [4] (en in 1938 Witt [8]) dit "bewijs" ontzenuwde, waande men dit probleem van de baan. In 1921 gaf Mc Neish [5] zelf een ander "bewijs", dat echter ook niet juis bleek. Voor zover ons bekend, staat het probleem dus thans weer open.

Zoals reeds boven vermeld, heeft Tarry [1] in het geval n = 6 probererenderwijs de onmogelijkheid aangetoond (zie ook Yamamoto [15]). De resultaten van Mann [11, 12] zijn reeds in de vorige § ter sprake gekomen.

Er bestaat een zeker verband tussen eindige projectieve meetkunden en systemen voor orthogonale Latijnse vierkanten. Een eindige projectieve meetkunde is een projectieve meetkunde met eindig veel punten (Axioma's: I, Door twee punten gaat één en slechts één lijn. II,Twee lijnen bezitten juist één gemeenschappelijk punt. III, Er zijn (minstens) vier punten waarvan er geen drie op één lijn liggen.). Bekend is, dat elke lijn evenveel (stel n+1) punten bevat en dat door elk punt dan n + 1 lijnen gaan. Het totaal aantal punten is dan $n^2 + n + 1$. Als er zo'n meetkunde gegeven is ($n \geq 3$), dan kunnen wij n - 1 orthogonale L-v_n's aangeven. Kies nl. een punt O en noem de n + 1 lijnen erdoor resp. a, b, $l_1, l_2, \ldots, l_{n-1}$. Nummer de van O verschillende punten op één of andere wijze, op elk der n + 1 lijnen. Wij vormen nu n - 1 L-v_n's L_k als volgt: In het i,j-de hokje van L_k plaatsen wij het nummer van het snijpunt van l_k met de lijn, die het punt i van a met het punt j van b verbindt.
Al deze vierkanten zijn Latijns, daar bij vaste i (resp j) het snijpunt op l_k met j (resp. i) alle punten doorloopt.
Twee van deze vierkanten L_λ en L_μ zijn orthogonaal, daar de combinatie r,s slechts één keer voorkomt. Verbindt het r-de punt van l_λ met het s-de punt van l_μ. Deze lijn snijdt a en b in punten i' en j' waaruit men ziet, dat de combinatie r,s slechts voorkomt op de i',j'-de plaats.

Het kan bewezen worden, dat omgekeerd een orthogonaal stelsel van (n-1) L-v_n's een projectieve meetkunde bepaalt met n + 1 punten op elke lijn (zie bijvoorbeeld [16]). Men kan zo ook bewijzen, dat er in ieder geval nooit meer dan (n-1) orthogonale L-v_n's kunnen bestaan ([16] , p. 291).

Men kan gemakkelijk een eindige projectieve meetkunde bouwen met n + 1 punten op een rechte, mits $n = p^k$. De meetkunde is dan de analytische meetkunde over het eindige lichaam met p^k elementen. Er zijn óók eindige projectieve meetkunden bekend, die niet opgevat kunnen worden als analytische meetkunden over een eindig lichaam. n is in die gevallen echter wel een macht van een priemgetal, zodat al deze meetkunden aanleiding geven tot $p^k - 1$ orthogonale L-v_{p^k}'s. Reeds lang bestaat het vermoeden, dat een

projectieve meetkunde slechts kan bestaan voor $n = p^k$.

Bruck and Ryser [13] hebben bewezen, dat als $n \equiv 1$ of $2 \pmod 4$ en als bovendien het kwadraatvrije deel van n deelbaar is door een priemfactor $p \equiv 3 \pmod 4$, er geen projectieve meetkunde bestaat met $n + 1$ punten op elke rechte.

Hun methode is ruw geschetst als volgt:

Nummer de lijnen en de punten op een of andere manier van 1 t/m $n^2 + n + 1$. De matrix $(a_{ij}) = A$ met

$$\begin{cases} a_{ij} = 1, \text{ als het i-de punt op de j-de lijn ligt} \\ a_{ij} = 0, \text{ als dit niet zo is} \end{cases}$$

heet de incidentie matrix. Er geldt dan $AA^T = A^TA = B_n = (\beta_{ij})$ met $\beta_{ij} = 1 + \delta_{ij}n$. De kwadratische vorm is blijkbaar rationaal equivalent met de eenheidsmatrix E_n. Door berekening van de invarianten t.o.v. de rationale equivalentie van B_n en E_n volgt hun stelling, daar voor bovengenoemde waarden van n deze invarianten niet overeenstemmen. Hieruit volgt dus tevens, dat voor deze waarden van n er geen $(n-1)$ orthogonale L_n's bestaan. Uiteraard is het probleem van deze $\S$ hiermee nog lang niet opgelost.

Bibliografie

1. 1782 L. Euler, Recherches sur une nouvelle espèce de Quarrés magiques, Verh. Zeeuws Genootschap v. Wetenschap 9. Vlissingen, p. 85-239.

2. 1901 G. Tarry, Le problème de 36 officiers. Compte Rendu de l'Association francaise pour l'Avancement de Science Naturel, 1. p. 122-123, 2. p. 170-203.

3. 1910 P. Wernicke, Das Problem der 36 Offiziere, Jahresber. der D.M.V., vol. 19, p. 264-267.

4. 1921 H.F. Mac Neish, Das Problem der 36 Offiziere, Jahresber. der D.M.V. 30, p. 151-153.

5. 1921/22 H.F. Mac Neish, Euler Squares, Ann. of Math. 23, p. 221-227.

6. 1934 R.A. Fisher and F. Yates, The 6 x 6 latin squares, Proc. Cambridge Phil. Soc. 30, p. 492-507.

7. 1938 R.C. Bose, On the application of the properties of Galois fields to the problem of construction of hyper-latin squares, Sankhyá 3, p. 323-338.

8. 1938 E. Witt, Zum Problem der 36 Offiziere, Jahresber. der D.M.V. 48, p. 66-67 (cursief)

9. 1939 W.L. Stevens, The completely orthogonalized latin-square, Annals of Engenics, 9, p.82-93.

10. 1942 R.C. Bose and K.R. Nair, On complete sets of latin-squares, Sankhyá 5, p. 361-382.

11. 1942 H.B. Mann, The construction of orthogonal latin-squares, Ann. of Math. Statistics 13, p. 418-423.

12. 1942 H.B. Mann, On orthogonal latin-squares, Bull. Am. Math. Soc. 50, p. 249-257.

13. 1949 R.H. Bruck and H.J. Ryser, The non-existence of certain finite projective planes, Canadian Journal of Math. 1, p. 88-93.

14. 1951 R.H. Bruck, Finite Nets, I. Numerical invariants. Canadian Journal of Math. 3.

15. 1954 K. Yamamoto, Euler squares and squares of even Fac. of Science Kynsyn Univ., series A, vol. 8, p. 161-180.

16. 1955 S. Pickert, Projektive Ebenen, Grundl. der Math. Wiss. Bd. 80, Springer Verlag.