Definitie Een Latijns Vierkant is een $n \times n$-vierkant met elementen uit $\{0,1,\ldots,n-1\}$ zó dat in geen enkele rij of kolom tweemaal hetzelfde element staat.

Voorbeelden

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

In elke rij en kolom van een Latijns vierkant komen de getallen $0,1,\ldots,n-1$ dus precies éénmaal voor. Door rijen en kolommen te permuteren kunnen we er voor zorgen dat de linkerkolom en bovenrij bestaat uit resp. $0,1,2,\ldots,n-1$. (Zg. genormeerd)

Voorbeeld.

2	3	1	0		0	1	3	2		0	1	2	3
3	0	2	1		1	2	0	3		1	2	3	0
1	2	0	3	$\rightarrow$	2	3	1	0	$\rightarrow$	2	3	0	1
0	1	3	2		3	0	2	1		3	0	1	2

In feite is het aantal Latijnse vierkanten van orde n gigantisch groot. Voor kleine n wordt het aantal genormeerde Latijnse vierkanten van orde n gegeven door

n	1	2	3	4	5	6	7
#	1	1	1	4	56	9408	16942080

Definitie. Twee $n \times n$-vierkanten $[a_{ij}]$ en $[b_{ij}]$ met elementen uit $\{0,1,\ldots,n-1\}$ heten orthogonaal als alle paren $(a_{ij}, b_{ij})_{i,j=0}^{n-1}$ verschillend zijn. Een aantal $n \times n$ vierkanten heet orthogonaal als elk tweetal van die vierkanten orthogonaal is

Voorbeeld. De volgende drie vierkanten zijn orthogonaal (zg. O.L.V.)

0	1	2	3		0	1	2	3		0	1	2	3
1	0	3	2		3	2	1	0		2	3	0	1
2	3	0	1		1	0	3	2		3	2	1	0
3	2	1	0		2	3	0	1		1	0	3	2

en ook

0	1	2			0	1	2
1	2	0	en		2	0	1
2	0	1			1	2	0

Het officierenprobleem van Euler vraagt in wezen of er twee O.L.V. van orde 6 zijn. Het algemenere probleem genoemd in de inleiding vraagt voor welke n er twee O.L.V. van orde n zijn.

Stelling 4.1. Een stelsel O.L.V. van orde n omvat ten hoogste n−1 vierkanten.

Bewijs. De orthogonaliteit wordt niet aangetast als in een van de vierkanten de getallen $0,1,\ldots,n-1$ op consequente wijze gepermuteerd worden. Door dit voor alle vierkanten op geschikte wijze te doen, kunnen we er voor zorgen dat de eerste rij van elk vierkant er uit ziet als $0\ 1\ \ldots\ n-1$. Voor het eerste element op de tweede rij komt 0 niet in aanmerking. Dus resten $1,2,\ldots,n-1$. Het is niet toegestaan dat in twee vierkanten op die plaats hetzelfde element staat. Dus het aantal O.L.V. is ten hoogste $n-1$.

Definitie. Een stel van $n-1$ O.L.V. van orde n heet volledig

We hebben al gezien dat er voor $n=2,3,4$ volledige stelsels O.L.V. bestaan. Een zeer belangrijke vraag is voor welke andere waarden van n zo'n stelsel bestaat.

Stelling 4.2. Als $n=p^k$ met p priem, $k\in\mathbb{N}$, dan bestaat een volledig stel O.L.V. van orde n.

Bewijs. Uit hoofdstuk 3 weten we dat er een eindig lichaam is met $n=p^k$ elementen. Laat $a_0=0, a_1=1, a_2, \ldots, a_{n-1}$ de elementen van F_n zijn. We definiëren het vierkant

$$A_e = [\,a_{ij}^{(e)}\,] \qquad \begin{matrix} e = 1,\ldots,n-1 \\ i,j = 0,1,\ldots,n-1 \end{matrix}$$

door

$$a_{ij}^{(e)} = a_e a_i + a_j$$

Nu komt op een rij van $A^{(e)}$ nooit tweemaal hetzelfde element voor, want

$$a_e a_i + a_j = a_e a_{i'} + a_j \Rightarrow a_j = a_{j'} \Rightarrow j = j'.$$

Ook komt in $A^{(e)}$ in een kolom nooit hetzelfde element tweemaal voor, want

$$a_e a_i + a_j = a_e a_{i'} + a_j \Rightarrow a_e a_i = a_e a_{i'} \overset{a_e \neq 0}{\Longrightarrow} a_i = a_{i'} \Rightarrow i = i'.$$

Dus op elke rij en elke kolom van elk vierkant komt elk element van het lichaam precies éénmaal voor.

We tonen nu aan dat de n^2 paren $(1 \leq e < f < n)$

$$(a_e a_i + a_j \,,\; a_f a_i + a_j) \qquad i = 0,1,\ldots,n-1 \;;\; j = 0,1,\ldots,n-1$$

alle verschillend zijn. Immers

$$(a_e a_i + a_j \,,\; a_f a_i + a_j) = (a_e a_{i'} + a_{j'} \,,\; a_f a_{i'} + a_{j'})$$

impliceert

(1) $\quad a_e a_i + a_j = a_e a_{i'} + a_{j'}$ èn $a_f a_i + a_j = a_f a_{i'} + a_{j'}$,

dus, door aftrekking,

$$(a_e - a_f) a_i = (a_e - a_f) a_{i'}$$

Omdat $a_e - a_f \neq 0$, volgt hieruit dat $a_i = a_{i'}$, ofwel $i = i'$.

Door dit in (1) in te vullen vinden we

$$a_e a_i + a_j = a_e a_i + a_{j'} \quad \text{en dit geeft } a_j = a_{j'}, \text{ ofwel } j = j'.$$

Door nu $0, 1, a_2, \ldots, a_{n-1}$ te vervangen door $0, 1, \ldots, n-1$, respectievelijk, krijgen we $n-1$ O.L.V. van orde n. □

Voorbeelden.

$n = 5$. De getallen $0, 1, 2, \ldots, 4$ met optelling en vermenigvuldiging mod. 5 vormen een eindig lichaam. Zo vinden we $(a_{ij}^{(e)} = ei + j)$

A_1	A_2	A_3	A_4
0 1 2 3 4	0 1 2 3 4	0 1 2 3 4	0 1 2 3 4
1 2 3 4 0	2 3 4 0 1	3 4 0 1 2	4 0 1 2 3
2 3 4 0 1	4 0 1 2 3	1 2 3 4 0	3 4 0 1 2
3 4 0 1 2	1 2 3 4 0	4 0 1 2 3	2 3 4 0 1
4 0 1 2 3	3 4 0 1 2	2 3 4 0 1	1 2 3 4 0

$n = 4$. De getallen $0, 1, a, a+1$ met optelling mod. 2 en vermenigvuldiging $a^2 = a+1$ vormen een lichaam van vier elementen. Zo vinden we

A_1	A_2	A_3
0 1 a a+1	0 1 a a+1	0 1 a a+1
1 0 a+1 a	a a+1 0 1	a+1 a 1 0
a a+1 0 1	a+1 a 1 0	1 0 a+1 a
a+1 a 1 0	1 0 a+1 a	a a+1 a 1

Door nu a door 2 en $a+1$ door 3 te vervangen krijgen we het stelsel onderaan p. 21. Merk op dat het helemaal misgaat als we $a_{ij}^{(e)} \equiv ei+j \pmod 4$ nemen, ~~want~~ want dit geeft

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

0	1	2	3
2	3	0	1
0	1	2	3
2	3	0	1

0	1	2	3
3	0	1	2
2	3	0	1
1	2	3	0

Het middelste vierkant is niet Latijns, en de eerste en derde staan niet orthogonaal op elkaar.

Andere waarden voor n dan priemmachten zó dat een volledig stel O.L.V. van orde n bestaat, zijn niet bekend. Het is zeer wel mogelijk dat voor elke andere n het maximale aantal O.L.V. van orde n kleiner is dan n-1. Voor een zekere verzameling getallen, nl. die die niet te schrijven zijn als som van twee kwadraten en $\equiv 1$ of $\equiv 2$ zijn, volgt dit uit een stelling die later bewezen zal worden. Dankzij de getaltheorie kunnen we dit gevolg zó formuleren:

Stelling 4.3. (Bruck – Ryser, 1949)
Zij $n \equiv 1 \pmod 4$ of $n \equiv 2 \pmod 4$. Stel er is een priemgetal p met $p \equiv 3 \pmod 4$ zódat n een oneven aantal factoren p bevat. Dan is er geen volledig stelsel O.L.V. van orde n.

Er is dus bijv. geen volledig stel O.L.V. van orde n als
$n = 6 = 2 \times 3$, $14 = 2 \times 7$, $21 = 3 \times 7$, $22 = 2 \times 11$, $30 = 2 \times 3 \times 5$.

De stand van zaken ziet er voor $n \leq 30$ dus als volgt uit:

(+ = wel, – = niet, ? = onbekend)

	k: 1	2	3	4	5	6	7	8	9	10
n =	k	+	+	+	+	–	+	+	+	– (zie p. 26)
n = 10 + k:	+	?	+	–	?	+	+	?	+	?
n = 20 + k:	–	–	+	?	+	?	+	?	+	–

Zie Beth, Jungnickel & Lenz
p. 280, 4.5
p. 277, 4.3.e)

We keren nu terug naar de vraag voor welke waarden van n er twee O.L.V. van orde n bestaan. Daarvoor bewijzen we eerst:

Stelling 4.4. Als er t O.L.V. van orde m en t O.L.V. van orde n bestaan, dan is er ook een t tal O.L.V. van orde mn.

Bewijs. Stel $A_e = [a_{ij}^{(e)}]_{i,j=0}^{m-1}$ en $B_e = [b_{ij}^{(e)}]_{i,j=0}^{n-1}$ zijn voor $e=1,2,\ldots,t$ stelsels O.L.V. van orde m resp. n. We construeren eerst t L.V. van orde mn en laten dan zien dat ze paarsgewijs orthogonaal zijn.

Zij C_e het vierkant van orde mn dat verkregen wordt door in B_e het element $b_{kl}^{(e)}$ te vervangen door het $m \times m$-vierkant $A_e + m\, b_{kl}^{(e)}$. Dit geeft een $mn \times mn$ vierkant met als elementen de gehele getallen c met $0 \leq c \leq m-1 + m(n-1) = mn-1$.

1) C_e is een Latijns vierkant:
$a_{ij}^{(e)} + m\, b_{kl}^{(e)} = a_{ij'}^{(e)} + m\, b_{kl'}^{(e)} \Rightarrow a_{ij}^{(e)} = a_{ij'}^{(e)} \wedge b_{kl}^{(e)} = b_{kl'}^{(e)} \Rightarrow j=j' \wedge l=l'$.
Dus de elementen op een rij van C_e zijn verschillend.
Analoog kan men bewijzen dat de elementen op een kolom van C_e verschillend zijn.

2) Zij $1 \leq e < f \leq t$. Dan zijn C_e en C_f orthogonaal:
Stel $\left(a_{ij}^{(e)} + m b_{kl}^{(e)},\ a_{ij}^{(f)} + m\, b_{kl}^{(f)}\right) = \left(a_{i'j'}^{(e)} + m\, b_{k'l'}^{(e)},\ a_{i'j'}^{(f)} + m\, b_{k'l'}^{(f)}\right)$
Dan volgt
$$a_{ij}^{(e)} + m\, b_{kl}^{(e)} = a_{i'j'}^{(e)} + m\, b_{k'l'}^{(e)} \wedge a_{ij}^{(f)} + m\, b_{kl}^{(f)} = a_{i'j'}^{(f)} + m\, b_{k'l'}^{(f)},$$
dus, door mod. m en veelvoud van m te onderscheiden,
$$a_{ij}^{(e)} = a_{i'j'}^{(e)} \wedge b_{kl}^{(e)} = b_{k'l'}^{(e)} \wedge a_{ij}^{(f)} = a_{i'j'}^{(f)} \wedge b_{kl}^{(f)} = b_{k'l'}^{(f)}.$$

Omdat A_e en A_f orthogonaal zijn, volgt $i=i'$, $j=j'$.
Omdat B_e en B_f orthogonaal zijn, volgt $k=k'$, $l=l'$.
Dus geen twee paren zijn gelijk. □

Stelling 4.5. Als $n \not\equiv 2 \pmod 4$, $n \geq 3$, dan zijn er twee O.L.V. van orde n.

Bewijs. Zij $n = 2^k p_1^{k_1} \cdots p_r^{k_r}$ met $2 < p_1 < \cdots < p_r$ priem en $k_1, \ldots, k_r > 0$.
Dan is $k \neq 1$. Volgens Stelling 4.2 zijn er twee O.L.V. van orde

2^k (als $k>1$), $p_1^{k_1}$, $p_2^{k_2}$, ..., $p_r^{k_r}$. Door Stelling 4.4 toe te passen op 2^k en $p_1^{k_1}$, dan op $2^k p_1^{k_1}$ en $p_2^{k_2}$, dan op $2^k p_1^{k_1} p_2^{k_2}$ en $p_3^{k_3}$, enz., vinden we uiteindelijk twee O.L.V. van orde n. □

Euler sprak het vermoeden uit dat er geen twee O.L.V. van orde n bestaan als $n \equiv 2 \pmod 4$. Voor $n=2$ is het triviaal. Voor $n=6$ werd dit in 1900 door Tarry bewezen. (Dus Euler's officierenprobleem is niet op te lossen.) In 1959 bewezen Bose, Shrikhande en Parker dat voor $n \geq 7$ er wel twee O.L.V. van orde n bestaan. Hun constructie werkt voor elke $n \equiv 2 \pmod 4$ met $n \geq 10$. Het resultaat voor $n=10$ staat hieronder. Er zijn nu zelfs een drietal O.L.V. van orde 10 bekend.

Twee O.L.V. van orde 10.

0	6	5	4	9	8	7	1	2	3
7	1	0	6	5	9	8	2	3	4
8	7	2	1	0	6	9	3	4	5
9	8	7	3	2	1	0	4	5	6
1	9	8	7	4	3	2	5	6	0
3	2	9	8	7	5	4	6	0	1
5	4	3	9	8	7	6	0	1	2
2	3	4	5	6	0	1	7	8	9
4	5	6	0	1	2	3	8	9	7
6	0	1	2	3	4	5	9	7	8

0	7	8	9	1	3	5	2	4	6
6	1	7	8	9	2	4	3	5	0
5	0	2	7	8	9	3	4	6	1
4	6	1	3	7	8	9	5	0	2
9	5	0	2	4	7	8	6	1	3
8	9	6	1	3	5	7	0	2	4
7	8	9	0	2	4	6	1	3	5
1	2	3	4	5	6	0	7	8	9
2	3	4	5	6	0	1	9	7	8
3	4	5	6	0	1	2	8	9	7

In 1991 bewees C.W.H. Lam, Amer. Math. Monthly 98 (1991), 305–318 dat er geen volledig stel O.L.V. van orde 10 bestaat.