Detlef Laugwitz

Eulerovy čtverce

Pokroky matematiky, fyziky a astronomie, Vol. 25 (1980), No. 2, 69--79

Persistent URL: http://dml.cz/dmlcz/139131

Eulerovy čtverce

Detlef Laugwitz, Darmstadt,) NSR*

Úloha o důstojnících a úloha s vysokými kartami[1])

Proslulé EULEROVĚ úloze je právě 200 let. Tato úloha není zdaleka jen nějakou hříčkou rekreační matematiky, jak by mohl napovědět její původ ve známé „úloze o důstojnících": Seřaďte 36 důstojníků – šesti různých hodností ze šesti různých pluků, přičemž z každého pluku je vybráno právě 6 důstojníků různých hodností – do „Eulerova" čtverce, tj. do čtvercového šiku složeného z 6 řad po 6 důstojnících tak, aby v každé řadě a v každém zástupu byly zastoupeny všechny hodnosti a všechny pluky. Připomeňme si proto slova samotného Eulera z jeho poznámky, kterou předložil petrohradské akademii 17. října 1776:

1. Une question fort curieuse, qui a exercé pendant quelque temps la sagacité de bien du monde, m'a engagé à faire les recherches suivantes, qui semblent ouvrir une nouvelle carrière dans l'Analyse et en particulier dans la doctrine des combinaisons. Cette question rouloit sur une assemblée de 36 officiers, de six différens grades et tirés de six régimes différens, qu'il s'agissoit de ranger dans un quarré de manière que sur chaque ligne, tant horizontale que verticale, il se trouvât six officiers tant de différens caractères que de régimens différens. Or, après toutes les peines qu'on s'est données pour résoudre ce problème, on a été obligé de reconnoitre qu'un tel arrangement est absolument impossible, quoiqu'on ne puisse pas en donner de démonstration rigoureuse.

Jednodušší úloha téhož druhu se objevila už v roce 1723 ve vydání Récréations mathématiques et physiques od OZNAMA: Vyložte 16 vysokých karet – esa A, krále K, dámy D a kluky B jedné karetní hry o čtyřech barvách – do čtverce se 4 řádky a 4 sloupci tak, aby každý řádek a každý sloupec obsahoval všechny barvy a všechny výšky karet (v následujícím řešení je požadavek splněn dokonce i pro úhlopříčky):

Euler předpokládal, že úloha o důstojnících nemá řešení, přestože se nezdá být podstatně odlišná od úlohy s vysokými kartami. Avšak to se podařilo dokázat teprve v r. 1900 G. Tarrymu[2]).

---

[1]) Na straně 215 Notices of the Amer. Math. Soc., 1976, nalezneme tuto zprávu:
"Editor, the Notices,
I should like to register an objection to the Society's total neglect of the bicentennial. I seems to me that an event of major importance is being neglected. Not one special lecture, nor one special seminar celebrates this important anniversary. In 1776, on 17th of October, L. Euler presented a paper to the St. Petersburg Academy in which the Euler conjecture on Latin Squares was first presented. The final settling of this conjecture was not achieved until 1960. Surely a problem which remained unsolved for 184 years deserves recognition on its bicentennial year. E. Mendelsohn"

[2]) G. TARRY: *Le problème des 36 officiers.* C. R. Assoc. Fr. Av. Sci., *1* (1900), 122–123; *2* (1901), 170–203 (pozn. překl.).

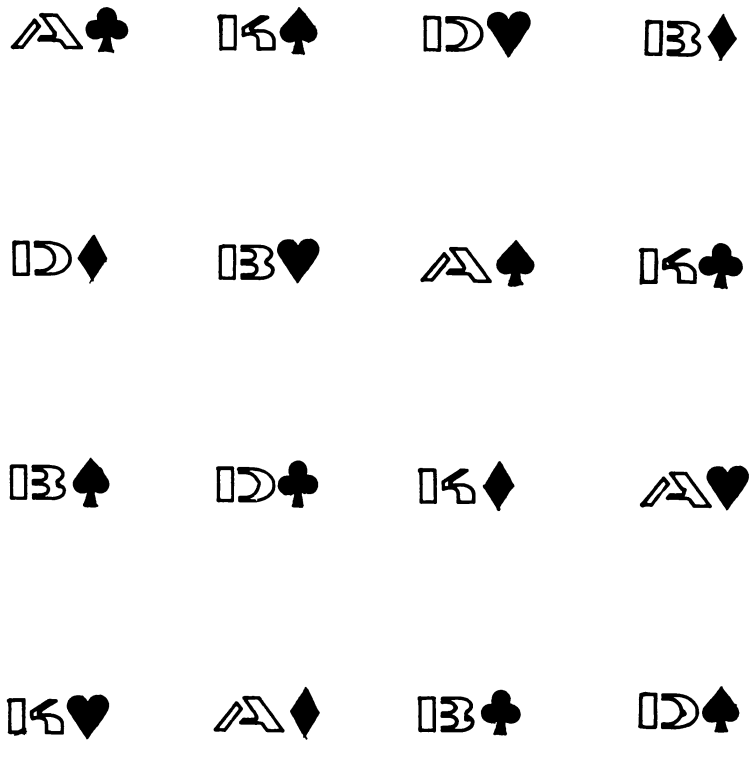
*) DETLEF LAUGWITZ: *Eulersche Quadrate.* Jahrbuch Überblicke Mathematik 1977, s. 174–180.

Volně přeložili a poznámkami opatřili VĚROSLAV JURÁK a JOSEF KLOUDA.

Přejděme nyní k přirozenému zobecnění předešlé úlohy, k tzv. problému Eulerových čtverců.

Eulerův čtverec obdržíme překrytím dvou vhodných „latinských" čtverců. Latinským čtvercem řádu n rozumíme schéma o n řádcích a n sloupcích, kde v každém řádku a v každém sloupci se každý prvek nějaké množiny M mohutnosti n objevuje právě jednou. V obr. 1. patří výšky karet jednomu latinskému čtverci, barvy zase druhému latinskému čtverci a celek pak znázorňuje překrytí těchto dvou latinských čtverců. Jsou-li tedy dány dva latinské čtverce L a L', jejichž prvky jsou postupně prvky množin M a M' téže mohutnosti n, pak jejich překrytí bude právě tehdy Eulerovým čtvercem, když každá dvojice $(m, m') \in M \times M'$ se v něm objeví právě jednou[3]).

Obr. 1.



Můžeme se snadno přesvědčit, že neexistuje žádný Eulerův čtverec řádu 2. Euler sám našel konstrukci pro všechny řády $n \neq 4k + 2$, kde $k = 0,1,\ldots$ a předpokládal, že pro $n = 6, 10, 14, \ldots$ žádné takové čtverce neexistují. Pro $4k + 2 \geqq 10$ neměl však pravdu:

[3]) Protože Eulerův čtverec zapisujeme ve tvaru matice, přenášíme odtud také pojmy jako je řádek. sloupec a úhlopříčka. Dále, počet řádků, a tedy i počet sloupců Eulerova čtverce, nazveme jeho řádem, Eulerův čtverec řádu 5 je uveden na str. 53 v knize J. Bosák: *Latinské štvorce*, Škola mladých matematiků, *38*, Praha (1976). Tamtéž na str. 60 najdeme podklady k sestrojení Eulerova čtverce řádu 3 (pozn. překl.).

V roce 1959 nalezl E. T. PARKER[4]) první Eulerův čtverec řádu 10 a v témže roce R. C. BOSE a S. S. SHRIKHANDE[5]) provedli konstrukci pro všechny řády $4k + 2 > 10$.

Jednoduché existenční věty

Existenci Eulerových čtverců lichého řádu si můžeme snadno ověřit. Především, jak už bylo řečeno, tyto čtverce obdržíme překrytím dvou vhodných latinských čtverců téhož řádu n. Pro zjednodušení vyberme prvky obou latinských čtverců z téže množiny $M = \{0,1,\ldots,n-1\}$. Jeden takový latinský čtverec je uveden v tabulce I:

Tab. I.

0	1	2	3	...	$n-1$
$n-1$	0	1	2	...	$n-2$
$n-2$	$n-1$	0	1	...	$n-3$
$n-3$	$n-2$	$n-1$	0	...	$n-4$
.....					
1	2	3	4	...	0

Čtverec vytvořený uspořádanými dvojicemi čísel $(q,r) \in M \times M$ bude právě tehdy Eulerovým čtvercem, když q a rovněž r samy o sobě tvoří latinské čtverce a když dále každá dvojice (q,r) se v něm objeví právě jednou. Dva takové latinské čtverce se nazývají „ortogonální". Toto pojmenování snad pochází z toho, že (při lichém n) otočením latinského čtverce z tabulky I kolem jeho středu o 90° (např. ve směru pohybu hodinových ručiček) vznikne nový latinský čtverec, který po překrytí s prvním tvoří Eulerův čtverec. Pro $n = 3$ dostáváme

Tab. II.

01	12	20
22	00	11
10	21	02

Avšak definice ortogonálních latinských čtverců je mnohem obecnější! (Euler použil místo prvních číslic q latinská písmena a místo druhých číslic r řecká písmena[6]); pojmenování latinský čtverec má pak tuto vnější příčinu).

Existenci Eulerových čtverců pro všechna lichá n dokážeme ještě jiným způsobem. Utvořme matici řádu n, jejíž prvky jsou uspořádané dvojice (x, y) zbytkových tříd modulo n, přičemž v i-tém řádku a v j-tém sloupci je napsána dvojice $(\overline{i-1}, \overline{j-1})$. Nyní sestrojíme dvě nové matice řádu n, které budou navzájem ortogonálními latinskými

[4]) E. T. PARKER: *Construction of somesets of mutually orthogonal Latin squares.* Proc. Amer. Math. Soc., *10* (1959), 946—949 (pozn. překl.).

[5]) R. C. BOSE, S. S. SHRIKHANDE: *On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler.* Trans. Amer. Math. Soc., *95* (1960), 191—209 (pozn. překl.).

[6]) Eulerovy čtverce se v literatuře proto často nazývají řecko-latinskými čtverci. Viz str. 53 a další ve výše citované knize Bosákově aj. (pozn. překl.).

čtverci. Pokud je na některém místě v původní matici napsána dvojice (x, y), napíšeme na odpovídající místo v druhé matici zbytkovou třídu c vyhovující kongruenci $x - y \equiv c \pmod{n}$ a v třetí matici zbytkovou třídu d vyhovující kongruenci $x + y \equiv d \pmod{n}$. (Matice s hodnotami c vznikne zřejmě z tabulky I přechodem ke zbytkovým třídám). Aby překrytí obou nových matic dalo Eulerův čtverec, je nutné a stačí, aby ke každé uspořádané dvojici (c, d) existovala právě jedna uspořádaná dvojice (x, y) taková, že $x - y \equiv c \pmod{n}$, $x + y \equiv d \pmod{n}$. Avšak kongruence $2x \equiv c + d \pmod{n}$, $2y \equiv d - c \pmod{n}$ tvoří systém, který je pro liché n jednoznačně řešitelný modulo n, protože 2 a n jsou nesoudělná čísla.

Geometrické hledisko

Celočíselné kongruence modulo n, které jsme výše použili, se dají geometricky interpretovat jako „přímky" v „konečné rovině" s n^2 „body". Pro $n = 3$ dostaneme celkem 9 bodů a 4 svazky rovnoběžek (po třech přímkách v každém svazku). Celkem zde máme 12 přímek, které (uspořádány po jednotlivých svazcích) jsou popsány kongruencemi

$$\begin{aligned} x &\equiv 0, 1, 2 \pmod{3}, \\ y &\equiv 0, 1, 2 \pmod{3}, \\ x + 2y \equiv x - y &\equiv 0, 1, 2 \pmod{3}, \\ x + y &\equiv 0, 1, 2 \pmod{3}.^{7}) \end{aligned}$$

Oba poslední svazky vedou v podstatě k překrytí ortogonálních latinských čtverců, jež je znázorněno v následující tabulce:

Tab. III.

00	11	22
21	02	10
12	20	01

Tento příklad se dá zobecnit na prvočíselné řády $n = p$. Vyjděme z kongruencí

$$ax + by \equiv d \ (\equiv 0, 1, \ldots, p - 1) \pmod{p}, \tag{1}$$

přičemž a, b nejsou současně obě kongruentní s 0. Je-li $a \equiv 0 \pmod{p}$, pak $b \not\equiv 0 \pmod{p}$ a existuje b' takové, že je $b'b \equiv 1 \pmod{p}$. Potom z (1) obdržíme

$$y \equiv c \ (\equiv b'd) \pmod{p}, \tag{2}$$

což je svazek, který má p „vodorovných" přímek.[8]) Když $a \not\equiv 0 \pmod{p}$, násobme

[7]) Zde přímka obsahuje body, jimiž jsou uspořádané dvojice čísel modulo 3 — souřadnic bodu. Například, přímka o rovnici $x + y \equiv 0 \pmod{3}$ obsahuje právě body (0, 0), (1, 2), (2, 1). (Pozn překl.)

[8]) Autor nazval přímky tohoto svazku vodorovnými. Bylo by dobře, aby si čtenář uvědomil, že zde dostáváme svazek přímek, z nichž žádné dvě nemají žádný společný bod — svazek „rovnoběžek". Podobně, je-li $b \equiv 0 \pmod{p}$, pak $a \not\equiv 0 \pmod{p}$ a existuje a' takové, že je $a'a \equiv 1 \pmod{p}$. Potom z (1) obdržíme $x \equiv c' (\equiv a'd) \pmod{p}$, což je zase svazek, který má p „svislých" přímek. (Pozn. překl.)

kongruenci (1) číslem a', přičemž opět $a'a \equiv 1 \pmod{p}$, takže dostáváme

$$x + by \equiv d \pmod{p}, \tag{3}$$

kde b probíhá množinu zbytků $0, 1, \ldots, p-1$. Pro každé $b \not\equiv 0 \pmod{p}$ obdržíme latinský čtverec, jestliže na místě označeném (x, a) (tak jako v tabulce I) zapíšeme hodnotu $d \equiv x + by \pmod{p}$. Každé dva z těchto $p-1$ latinských čtverců jsou ortogonální, neboť dvojice kongruencí

$$x + b_1 y \equiv d_1 \pmod{p},$$

$$x + b_2 y \equiv d_2 \pmod{p},$$

má pro $b_1 \not\equiv b_2 \pmod{p}$ právě jedno řešení, takže dvojice (d_1, d_2) se nalézá právě na jednom místě (x, y) překrytí příslušné dvojice ortogonálních latinských čtverců.

Podali jsme tedy, v případě prvočíselného řádu, souvislost ortogonálních latinských čtverců téhož řádu s jistými konečnými afinními rovinami.[9])Uvedená souvislost zůstává v platnosti i v případě, kdy řád latinských čtverců je mocninou prvočísla; viz DEMBOWSKI, str. 47f.

Otázka o počtu latinských čtverců — ještě jedna vyvrácená domněnka

Opravdový kombinatorik se zajímá nejen o existenci, ale i o počet latinských čtverců. Označme l_n počet redukovaných (někdy se říká standardní místo redukovaný) latinských čtverců řádu n, tj. latinských čtverců, které mají v prvním řádku a v prvním sloupci čísla $0, 1, \ldots, n-1$ zapsaná v přirozeném pořádku. Pro jmenovaný počet dostáváme odhad

$$l_n \geqq (n-2)!\,(n-3)! \ldots 1!$$

a pro malá n jsou známy mnohem větší přesné hodnoty

$$l_3 = 1,\ l_4 = 4,\ l_5 = 56,\ l_6 = 9\,408,\ l_7 = 16\,942\,080.^{10})$$

---

[9]) Konečnou afinní rovinou rozumíme konečnou množinu, jejíž prvky nazveme „body", spolu s jistými jejími podmnožinami, jež nazveme „přímky", přičemž platí

(a) každé dva různé body jsou incidentní právě s jednou přímkou,

(b) každý bod, který není incidentní s danou přímkou l, je incidentní právě s jednou přímkou, jež není incidentní s přímkou l,

(c) existují aspoň tři různé body, které nejsou incidentní s jednou přímkou.

Přitom to, že bod je incidentní s přímkou, nebo přímka je incidentní s bodem, znamená, že souřadnice bodu splňují rovnici přímky, atd. Místo toho, můžeme také říci, že bod leží na přímce, atd., jak se v geometrii obvykle hovoří. Pojem řádu se přenáší z latinských čtverců i na příslušnou konečnou afinní rovinu. Takže $n-1$ různých latinských čtverců řádu n po dvou ortogonálních určuje konečnou afinní rovinu řádu n. Čtenář si může ověřit sám, že v našem případě je splněna uvedená definice konečné afinní roviny. (Pozn. překl.)

[10]) Panu B. GANTEROVI vděčím za užitečná upozornění k tomuto článku, mj. za toto sdělení: $l_8 = 535\,281\,401\,856$ (M. B. WELLS, 1967), $l_9 = 377\,597\,570\,964\,258\,816$ (S. E. BAMMEL, J. ROTHSTEIN, 1975).

U ortogonálních latinských čtverců můžeme být bez obav, neboť jejich počet je přehlednější:

Každá množina po dvou ortogonálních latinských čtverců řádu n má nejvýše n − 1 prvků.

(Pro prvočíselné řády jsme tohoto maximálního čísla dosáhli. Stejný výsledek platí pro mocniny prvočísel.) Tato věta je z geometrického hlediska zřejmá a její důkaz je zcela jednoduchý. Bez újmy obecnosti můžeme předpokládat, že první řádek všech po dvou ortogonálních latinských čtverců řádu n je $0, 1, \ldots, n-1$. Toho můžeme dosáhnout přečíslováním. Přitom neporušíme ortogonalitu čtverců. Pro první místo druhého řádku potom přicházejí v úvahu jen čísla $1, 2, \ldots, n-1$ a u různých čtverců nemohou na tomto místě být stejná čísla k, neboť jinak by po překrytí byla dvojice (k, k) na tomto místě a pak ještě v prvním řádku. Tím je důkaz proveden.

Pomocí jistého rozkladu v direktní součin lze dokázat: Existuje-li t latinských čtverců po dvou ortogonálních řádu m, popřípadě n, pak existuje také t takových čtverců řádu mn. Odtud zřejmě plyne: Jestliže $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} (p_1 < p_2 < \ldots < p_n, \alpha_k < 0)$ je prvočíselný rozklad přirozeného čísla N, pak existuje alespoň t latinských čtverců po dvou ortogonálních řádu N, pokud $t = \min \{p_j^{\alpha_j} - 1\} \geqq 2$, $N \not\equiv 2 \pmod 4$.
MacNeish dokázal tuto větu v roce 1922[11]) a připojil domněnku, že $t = \min \{p_j^{\alpha_j} - 1\}$ je také horní hranicí. Také tato domněnka byla vyvrácena: Parker (viz poznámku[4])) našel 4 latinské čtverce řádu 21 po dvou ortogonální a je známo dokonce 5 takových čtverců řádu 12.

Z MacNeishova výsledku nevyplývá existence ortogonálních latinských čtverců pro sudá čísla N, jež nejsou dělitelná 4, tedy pro řády, které postihuje Eulerova doměnka. Pro prvočísla $N = p$ a pro $N = 4$ (podobně postupujeme při $N = 8$) jsme zde řešení našli.

Pojmenování „ortogonální" není zrovna příhodné, protože vyvolává představy, které vždy dobře nevystihují podstatu věci. Tak ze samotné existence „úplného ortogonálního systému" $n - 1$ latinských čtverců řádu n po dvou ortogonálních *neplyne*, že by *každý* latinský čtverec řádu n po doplnění dalšími vedl k úplnému ortogonálnímu systému. Snadno ověříme, že ke čtverci

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

neexistuje žádný s ním ortogonální.

Případ řádu 10

Snad by mohl leckdo namítnout, že by přece jen v době samočinných počítačů nemělo být obtížné rozhodnout o Eulerově úloze o důstojnících. Vždyť je třeba prozkoumat jen

[11]) H. F. MacNeish: *Euler squares.* Ann. of Math. *23* (1922), 221—227. (Pozn. překl.)

konečný počet číselných čtverců. Skutečně, TARRYHO způsob řešení z roku 1900 spočívá v systematickém probrání všech možných případů.[12]) V případě řádu 10 se však ani při nasazení samočinného počítače nedospělo dál než ke dvěma ortogonálním latinským čtvercům. To, že existují dva, se dá dokonce poněkud elegantně dokázat i bez počítače (RYSER 1963).[13])

Výstavba konečné geometrie

Shora uvedené úvahy zahalené do geometrického hávu nás v případě prvočíselného řádu přivedly k maximálnímu počtu latinských čtverců po dvou ortogonálních. Nyní obraťme směr této úvahy: Latinské čtverce nás přivádějí ke konečným rovinám, tj. ke konečným množinám s geometrickou strukturou, jež se dají popsat jednoduchým systémem axiomů — jsou to afinní a projektivní roviny. Vraťme se opět k tabulce III a utvořme z $9 = 3^2$ bodů „afinní rovinu" se 4 svazky po 3 rovnoběžných přímkách: svazek vodorovných přímek, svazek svislých přímek a dva svazky, které dostaneme překrytím $2 = 3 - 1$ ortogonálních latinských čtverců. Zřejmě platí: Každé dva různé body jsou incidentní právě s jednou přímkou; každé dvě různé přímky jsou incidentní nejvýše s jedním bodem (průsečík). Ke každému neincidentnímu páru bod P — přímka g existuje právě jedna přímka incidentní s P a neincidentní s g (přímka, která neprotíná g — axióm rovnoběžnosti). Kromě toho platí ještě údaje o počtech bodů a přímek. Jestliže vyjdeme od latinských čtverců řádu n, dostáváme: V případě afinní roviny řádu n (viz pozn.[9])) leží na každé přímce právě n různých bodů a každým bodem prochází právě $n + 1$ různých přímek. Přidáme-li k tomuto souboru „nekonečně vzdálenou" přímku, tj. takovou, že všechny přímky jednoho svazku rovnoběžek a právě jenom tyto přímky by procházely právě jedním bodem nekonečně vzdálené přímky,[14]) budeme mít k dispozici právě $n(n + 1) + 1$ různých bodů a tentýž počet různých přímek a budou splněny elegantní axiómy projektivní roviny, jejíž model jsme právě našli. Uvedeme pro úplnost abstraktní definici projektivní roviny: Buďte dány dvě neprázdné disjunktní množiny $\mathscr{B}$, $\mathscr{P}$ (bodů, přímek) a relace, tj. část kartézského součinu $\mathscr{I} \subset \mathscr{B} \times \mathscr{P}$, kterou nazveme incidence, přičemž předpokládáme, že

(P1) ke každým dvěma bodům $B_1, B_2 \in \mathscr{B}$, kde $B_1 \neq B_2$, existuje právě jedna přímka $p \in \mathscr{P}$ taková, že $(B_1, p), (B_2, p) \in \mathscr{I}$ (spojnice bodů);

(P2) ke každým dvěma přímkám $p_1, p_2 \in \mathscr{P}$, kde $p_1 \neq p_2$, existuje právě jeden bod $B \in \mathscr{B}$ takový, že $(B, p_1), (B, p_2) \in \mathscr{I}$ (průsečík přímek).

---

[12]) Konečně dnes jsou už k dispozici kratší důkazy, jako: R. A. FISHER, F. YATES: *The 6 × 6 latin squares*, Proc. Camb. Phil. Soc. *30* (1934), 492—507, K. YAMAMOTO: *Euler squares and incomplete Euler squares of even degrees*. J. Math. Soc. Japan, *5* (1953), 13—23. (Pozn. překl.)

[13]) Jmenovaný důkaz se najde v Ryserově knize uvedené v závěru tohoto článku. V jejím ruském překladu: H. J. RYSER: *Kombinatornaja matematika*. Mir, Moskva 1966, je na str. 90—93. (Pozn. překl.)

[14]) Autor nazval novou přímku „nekonečně vzdálenou". Čtenář nechť si jen uvědomí, že se přidává další množina $n + 1$ bodů, o nichž prohlásíme, že leží právě na jedné přímce. (Pozn. překl.

Ve formulaci těchto axiómů je skryt princip duality. Znění axiómů zůstane v podstatě zachováno, když zaměníme roli bodů a přímek. Aby naše geometrie nebyla příliš chudá, přidáme ještě další axióm, „axióm hojnosti":

(P3) Existují čtyři různé body, z nichž žádné tři nejsou incidentní s touž přímkou. Odtud snadno plyne duální výrok:

(P4) Existují čtyři různé přímky, z nichž žádné tři nejsou incidentní s týmž bodem.

Nyní lze snadno ukázat: Jestliže množina $\mathscr{B}$ bodů je konečná, leží na každé přímce stejný počet bodů. Je-li to právě $n + 1$ různých bodů, pak každým bodem prochází právě $n + 1$ různých přímek. Počet všech bodů (přímek) je $n^2 + n + 1$. Mluvíme potom o konečné projektivní rovině řádu n. Odstraníme-li jednu přímku a na ní ležící body, zůstane nám konečná afinní rovina téhož řádu n s n^2 různými body a $n(n + 1)$ různými přímkami. Abychom dosáhli uspořádání bodů této afinní roviny do čtverce, můžeme vybrat dva svazky rovnoběžek. Jeden z nich nazveme svazkem vodorovných přímek a druhý svazkem svislých přímek.

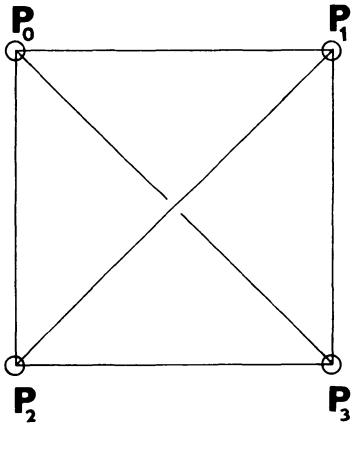
Ke každému ze zbývajících $n - 1$ svazků rovnoběžek náleží jeden latinský čtverec řádu n: Očíslujme všech n přímek jednoho takového svazku a ke každému bodu roviny (jejíž body už máme uspořádány do čtverce) připišme číslo přímky svazku, s níž je tento bod incidentní. Z (P2) plyne, že tyto zápisy dávají $n - 1$ latinských čtverců, jež jsou po dvou ortogonální. Obrácené tvrzení platí také, takže dostáváme:

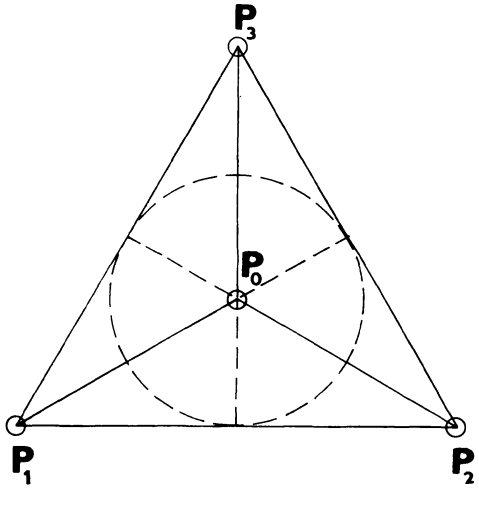
Konečná afinní rovina, a tedy i konečná projektivní rovina řádu $n \geqq 3$ existuje právě tehdy, jestliže existuje $n - 1$ latinských čtverců řádu n po dvou ortogonálních.

Nyní tedy víme: Existují konečné projektivní roviny řádu 3, 4, 5, 7, 8, 9, 11, ..., obecně řádu, který je mocninou prvočísla. Jistě neexistuje žádná konečná projektivní rovina řádu 6. Dále, není doposud známo, zda existuje konečná projektivní rovina řádu 10.

Konečná projektivní rovina řádu 2 není touto větou popsána. K jejímu sestrojení není třeba dvojice ortogonálních čtverců. Vystačíme s jediným latinským čtvercem $\begin{smallmatrix} 01 \\ 10 \end{smallmatrix}$. Konečnou afinní rovinu řádu 2 a k ní příslušnou konečnou projektivní rovinu máme znázorněnu na obr. 2. Nekonečně vzdálená přímka je zde znázorněna jako kružnice vepsaná trojúhelníku.

Obr. 2.





BRUCK a RYSER (1949)[15]) dokázali, že konečné projektivní roviny neexistují i pro některé další řády. Buď $n \equiv 1$, nebo 2 (mod 4) a nechť kvadratický zbytek n obsahuje aspoň jeden prvočíselný činitel $p \equiv 3$ (mod 4), potom neexistuje žádná konečná projektivní rovina řádu n, a tedy neexistuje žádných $n - 1$ latinských čtverců řádu n po dvou ortogonálních. Tato věta znovu postihuje řád 6, dále řády 14, 21 a další, avšak nikoliv řád 10.[16])

Magické čtverce

S Eulerovými čtverci souvisí jedna metoda konstrukce magických čtverců,[17]), která byla autorsky řešena v letech 1687–88 francouzským vyslancem v Siamu (S. DE LA LOUBÈRE, *Du Royaume de Siam*). Pro dané liché n postupujeme podle tohoto způsobu takto: Nakreslíme si čtvercovou mřížku, která bude mít $n \times n$ políček. Doprostřed prvního řádku zapíšeme 1 a pak zapíšeme postupně další přirozená čísla 2, 3, ..., n^2 takto: Následující číslo zapíšeme hned vpravo, ale o řádek výš, až na následující výjimky. Jestliže by zápis následujícího čísla překročil horní okraj mřížky, zapíšeme jej sice zase vpravo, ale do posledního řádku. Když by zápis následujícího čísla překročil pravý okraj mřížky, zapíšeme jej o řádek výš, než je zapsán předchůdce, avšak do prvního sloupce. Konečně, když zapíšeme číslo dělitelné n, pak jeho následovník bude zapsán v témže sloupci o řádek níž.[18]) Pro $n = 5$ dostáváme tuto tabulku:[19])

Tab. IV.

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

Abychom snadněji poznali, že tento čtverec je magický, zapišme všechna jeho čísla v soustavě se základem n,[20]) přičemž předtím ode všech čísel odečteme jedničku. Byl-li

[15]) R. H. BRUCK, H. J. RYSER: *The non-existence of certain finite projective planes.* Canad. J. Math., *1* (1949), 88–93. (Pozn. překl.)

[16]) Někdy bývá tvrzení Bruckovo-Ryserovo vysloveno takto: Je-li $n \equiv 1$ nebo 2 (mod 4), pak neexistuje žádná konečná projektivní rovina řádu n, vyjma ta n, jež se dají napsat ve tvaru součtu dvou čtverců, tj. $n = a^2 + b^2$. (Pozn. překl.)

[17]) Magickým čtvercem řádu n rozumíme sestavu n^2 nezáporných celých čísel (obvykle, ale nikoliv nutně po sobě jdoucích a obvykle, ale nikoliv nutně různých) do čtverce $n \times n$ tak, že součet čísel v každém řádku, v každém sloupci a v každé úhlopříčce je týž. (Pozn. překl.)

[18]) Čtenář snadno porozumí způsobu zápisu, když si mřížku vystřihne a stočí ji do tvaru pláště válce. Jednou tak, aby horní okraj splynul s dolním okrajem, po druhé zase tak, aby levý okraj splynul s pravým okrajem. Dále si pak snadno odvodí eventuální změny v postupu. Odtud už pak pochopí, že dostane magický čtverec. (Pozn. překl.)

[19]) Zde součet čísel v každém řádku, v každém sloupci a v každé z úhlopříček je roven 65. (Pozn. překl.)

[20]) Pro nezáporné celé číslo $a < n^2$ dostáváme $a/n = \alpha + \beta/n$, takže $a = \alpha n^1 + \beta n^0$, kde $\alpha, \beta = \equiv 0, 1, \ldots, n - 1$. V soustavě se základem n je pak stručně zapisujeme ve tvaru $\alpha\beta$.

původní čtverec magický, bude magický i potom. Pro $n = 5$ dostáváme tuto tabulku:

Tab. V.

31	43	00	12	24
42	04	11	23	30
03	10	22	34	41
14	21	33	40	02
20	32	44	01	13

To je zřejně Eulerův čtverec. Bezprostředně totiž vidíme, že v každém řádku, v každém sloupci a v každé úhlopříčce dostáváme týž součet, a to

$$(0 + 1 + \ldots + (n - 1))\, n + 0 + 1 + \ldots + (n - 1) = n(n - 1)\,(n + 1)/2.^{21})$$

Tato metoda selhává pro sudá n, ale poznámka, že Eulerův čtverec vede k magickému čtverci, platí, jestliže pokládáme zápisy za čísla napsaná v soustavě o základu n. Z Eulerova čtverce z úlohy o vysokých kartách (obr. 1.) například obdržíme:

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

nebo v desítkové soustavě a po přičtení 1:

1	6	11	16
12	15	2	5
14	9	8	3
7	4	13	10

Zde je součet čísel v každém řádku, v každém sloupci a v každé z úhlopříček roven 34. Proslulý DÜRERŮV čtverec[22])

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

je sice magický, ale nepřísluší žádnému Eulerovu čtverci. Zatímco neexistuje žádný Eulerův čtverec řádu 6, zkonstruoval už CORNELIUS AGRIPPA (1486–1535) magické čtverce všech řádů od řádu 3 až po řád 9 a dal je do souvislosti se sedmi astrologickými planetami.[23]) Magický čtverec řádu 3, který je vytvořen podle siamského pravidla,

[21]) Tabulce tedy odpovídají součty rovné 60 (nezapomeňme, že jsme v tabulce IV nejdříve každé číslo zmenšili o 1). (Pozn. překl.)

[22]) Vyobrazený na mědirytině MELENCOLIAεI z roku 1514. (Pozn. překl.)

$$\begin{matrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{matrix}$$

a vede k Eulerovu čtverci

$$\begin{matrix} 21 & 00 & 12 \\ 02 & 11 & 20 \\ 10 & 22 & 01 \end{matrix}$$

je připisován čínskému císaři Yu (který žil kolem roku 2200 před n. l.)[24])

To je také až na symetrie a otáčení jediný magický čtverec řádu 3. Existuje 880 podstatně různých magických čtverců řádu 4. Počet magických čtverců řádu 5 podstatně různých není znám, ale odhaduje se, že je jistě vyjádřen sedmimistným číslem.

Co tomu říká algebra?

Ukázali jsme, jak souvisí naše kombinatorické otázky s geometrií a s elementární teorií čísel. Jak je tomu s algebrou? S tou jsme se už setkali při konstrukci latinského čtverce pomocí kongruence $x + a \equiv d \pmod{n}$. Tento čtverec není nic jiného než multiplikativní tabulka (bez záhlaví) aditivní grupy zbytkových tříd modulo n a je zřejmé, že každá konečná grupa $(G, \circ)$, $G = \{e = a_0, a_1, \ldots, a_{n-1}\}$ má za svou multiplikativní tabulku latinský čtverec. Obrácené tvrzení neplatí: latinský čtverec není obecně multiplikativní tabulkou grupy, ale pouze kvazigrupy.[25])

Literatura

EULER, L.: *Recherches sur une nouvelle espèce de quarrés magiques.* (Eneström-Index Nr. 530). *De quadratis magicis* (Eneström-Index Nr. 795). (Vytištěno v *Opera omnia*, Ser. I. Vol. VII.)

Knihy o kombinatorice

DEMBOWSKI, P.: *Kombinatorik.* BI-Hochschulskriptum 741a, Mannheim 1970.
RYSER, H. J.: *Combinatorial mathematics.* Math. Assoc. of America 1963 (se seznamem literatury, odkaz v článku se týká str. 94-95).
DÉNES J. and A. D. KEEDWELL: *Latin squares and their applications.* New York 1974, 574 stran.

---

[23]) CORNELIUS AGRIPPA je autorem slavného spisku *Laus Asini*. Znamenitý čínský matematik YANG HUI (2. pol. 13. stol.) uvádí ve své učebnici 13 magických čtverců od řádu 3 počínaje do řádu 10 včetně. (Pozn. př.)

[24]) Podle legendy jej spatřil na štítě Nebeské Želvy. (Pozn. překl.)

[25]) Buď G neprázdná množina a $(x, y) \mapsto x \,.\, y$ binární operace na G. Množina G s touto binární operací se nazývá kvazigrupa, jestliže ke každým dvěma prvkům $a, b \in G$ existuje právě jedno $x \in G$ a právě jedno $y \in G$ tak, že $a \,.\, x = b = y \,.\, a$. Odtud a z definice latinského čtverce už plyne, že jej můžeme pokládat za multiplikativní tabulku kvazigrupy. (Pozn. překl.)