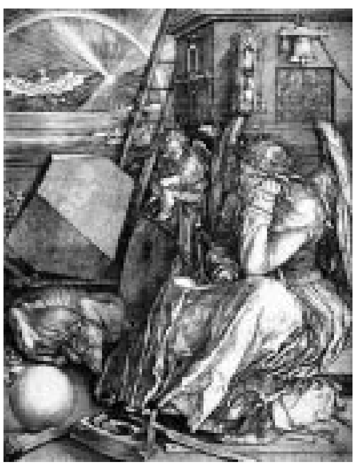
Appendix B: Weihnachtsvorlesung

Magische Quadrate

Ein magisches Quadrat ist eine $n \times n$-Matrix A, deren Einträge die Zahlen von 1 bis n^2 sind und bei der alle Zeilen und Spaltensummen gleich sind. Folgendes magische Quadrat ist als Dürers magisches Quadrat bekannt geworden, da es im Hintergrund des Bildes Melencolia 1 zu sehen ist.



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

Wir wollen heute eine Methode vorstellen, mit der man magische Quadrate konstruieren kann.

Leonhard Eulers Problem mit 36 Offizieren

Leonhard Euler wurde 1707 in Basel geboren und arbeitete ab 1766 in Petersburg zur Zeit von Katherina der Großen. Es wird erzählt, daß Katherina ihm folgende Aufgabe stellte:

> Er solle 36 Offiziere aus 6 Regimentern mit in 6 verschiedenen Of-

> fiziersrängen, von jedem Regiment einer jeden Ranges, so auf einem 6×6-Schachbrett anordnen, daß in jeder Zeile und in jeder Spalte je ein Offizier von jedem Regiment und von jedem Rang vorkomme.

Für ein $n \times n$ Schachbrett können wir die Frage also so verallgemeinern, daß man in einer $n \times n$-Matrix Tupel die Tupel (i, j) mit $i, j = 0, \ldots n-1$ so anordnen soll, daß in jeder Spalte und Zeile in beiden Koordinaten alle Zahlen vorkommen. Da sich an der Eigenschaft durch Permutation der Symbole und Spaltenvertauschungen nichts ändert, können wir annehmen, daß $a_{1j} = (j-1, j-1)$ und $a_{i1} = (i-1, *)$ ist. Wir nennen so eine Matrix ein *orthogonales Paar lateinischer Quadrate.*

n=1,2

Für $n = 1$ ist nichts zu tun. Sei also $a_{11} = (0, 0)$ und $a_{12} = (1, 1)$.Für a_{21} bleibt nun, da die 0en vergeben sind, auch nur $(1, 1)$. Also kann es keine solche Anordnung geben.

n=3,4

Man findet z.B. durch Ausprobieren

00	11	22
12	20	01
21	02	10

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

n=5

Probieren wird langsam etwas mühsam. Hier kommt ein Trick. Und zwar tragen wir in die erste Koordinate "$(i-1)+(j-1)$" ein und in die zweite "$2*(i-1)+j-1$". Wir müssen mit diesen Zahlen nur "richtig" rechnen. Bei Primzahlen ist das leicht, es genügt Modulo-Rechnung also

0+0, 2*0+0	0+1, 2*0+1	0+2, 2*0+2	0+3, 2*0+3	0+4, 2*0+4
1+0, 2*1+0	1+1, 2*1+1	1+2, 2*1+2	1+3, 2*1+3	1+4, 2*1+4
2+0, 2*2+0	2+1, 2*2+1	2+2, 2*2+2	2+3, 2*2+3	2+4, 2*2+4
3+0, 2*3+0	3+1, 2*3+1	3+2, 2*3+2	3+3, 2*3+3	3+4, 2*3+4
4+0, 2*4+0	4+1, 2*4+1	4+2, 2*4+2	4+3, 2*4+3	4+4, 2*4+4

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

.

Vielleicht erkennen Sie die Ähnlichkeit mit dem Fall $n = 3$. Dort haben wir genauso gerechnet. Wie ist im Falle $n = 4$? Der *Körper* mit 4 Elementen hat etwas eigenwillige Rechenregeln.

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

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

Fassen wir zusammen. Wenn wir auf $\mathbb{F} := \{0, 1, \ldots, n-1\}$ Addition und Multiplikation invertierbar (es gibt Subtraktion und Division) und verträglich miteinander definieren können, so nennen wir $\mathbb{F}$ mit dieser Definition einen Körper. Solche Körper gibt es genau dann, wenn $n = p^m$ eine Primzahlpotenz ist.

Satz 5.5.6 *Sei $\mathbb{F} = \{0, \ldots, n-1\}$ ein Körper mit $n \geq 3$ Elementen und $a \neq b \in \mathbb{F} \setminus \{0\}$. Dann definiert der Eintrag $a_{i,j} := a * (i-1) + (j-1), b * (i-1) + (j-1)$ ein orthogonales Paar lateinischer Quadrate.*

Beweis. Wir zeigen zunächst, daß in jeder Zeile und Spalte in beiden Koordinaten jedes Element c vorkommt. Betrachten wir dazu zunächst die erste Zeile in Koordinate i.

$$\begin{aligned} a * (i-1) + (j-1) &= c \\ \Leftrightarrow (j-1) &= c - a * (i-1). \end{aligned}$$

Bei vorgegebener Spalte j berechnen wir

$$\begin{aligned} a * (i-1) + (j-1) &= c \\ \Leftrightarrow a * (i-1) &= (c - (j-1)) \\ \Leftrightarrow (i-1) &= a^{-1}(c - (j-1)). \end{aligned}$$

Die zweite Koordinate berechnet man analog. Es bleibt zu zeigen, daß jedes Paar genau einmal vorkommt. Betrachten wir also das Paar (c,d), so erhalten wir aus

$$
\begin{aligned}
(a*(i-1)+(j-1), b*(i-1)+(j-1)) &= (c,d) \\
(a-b)(i-1) &= c-d \qquad \text{und} \\
a*(i-1)+ab^{-1}(j-1) &= ab^{-1}d, \qquad \text{also} \\
(1-ab^{-1})(j-1) &= (c-ab^{-1}d).
\end{aligned}
$$

Da $a \neq b$ ist, sind $(a-b)$ und $(1-ab^{-1})$ von Null verschieden und wir können i,j berechnen als

$$
\begin{aligned}
(i-1) &= (a-b)^{-1}(c-d) \qquad \text{und} \\
(j-1) &= (1-ab^{-1})^{-1}(c-ab^{-1}d).
\end{aligned}
$$

□

Haben wir zwei Paare orthogonaler lateinischer Quadrate der Größen n und m, so können wir leicht ein orthogonales Quadrat der Größe nm konstruieren.

Satz 5.5.7 *Sind A und B orthogonale lateinische Quadrate der Ordnungen m bzw. n, so ist $A \times B$ definiert durch*

$$(A \times B)_{in+k,jn+l} := (nA^1_{ij} + B^1_{kl}, nA^2_{ij} + B^2_{kl})$$

ein orthogonales Paar lateinischer Quadrate.

Beispiel 5.5.8 $m = 3, n = 4$

0,0	1,1	2,2	3,3	4,4	5,5	6,6	7,7	8,8	9,9	10,10	11,11
1,2	0,3	3,0	2,1	5,6	4,7	7,4	6,5	9,10	8,11	11,8	10,9
2,3	3,2	0,1	1,0	6,7	7,6	4,5	5,4	10,11	11,10	8,9	9,8
3,1	2,0	1,3	0,2	7,5	6,4	5,7	4,6	11,9	10,8	9,11	8,10
4,8	5,9	6,10	7,11	8,0	9,1	10,2	11,3	0,4	1,5	2,6	3,7
5,10	4,11	7,8	6,9	9,2	4,3	11,0	10,1	1,6	0,7	3, 4	2, 5
6,11	7,10	4,9	5,8	10,3	11,2	8,1	9,0	2,7	3,6	0, 5	1, 4
7,9	6,8	5,11	4,10	3,9	2,8	1,11	0,10	7,1	6,0	5, 3	4, 2
8,4	9,5	10,6	11,7	0,8	1,9	2,10	3,11	4,0	5,1	6,2	7,3
9,6	8,7	11,4	10,5	1,10	0,11	3,8	2,9	5,2	4,3	7, 0	6,1
10,7	11,6	8,5	9,4	2,11	3,10	0,9	1,8	6,3	7,2	0,5	5,0
11,5	10,4	11,3	8,6	3,9	2,8	1,11	0,10	7,1	6,0	5,3	4,2

Die letzten beide Sätze ergeben kombiniert:

Korollar 5.5.9 *Ist $n \not\equiv 2 \, mod \, 4$ so gibt es ein Paar orthogonaler lateinischer Quadrate der Größe n.*

Beweis. Wir führen Induktion über die Anzahl der Primzahlen, die n teilen. Sei also p ein Primzahlen, die n teilt und p^r die höchste Potenz, in der p in n vorkommt. Nach Satz 5.5.6 gibt es ein Paar für p^r. Nun ist $m := \frac{n}{q^r}$ eine natürliche Zahl mit $m \not\equiv 2 \, mod \, 4$ und einem Primteiler weniger als n. Nach Induktionsvoraussetzung gibt es ein Paar für m also nach Satz 5.5.7 auch für n. □

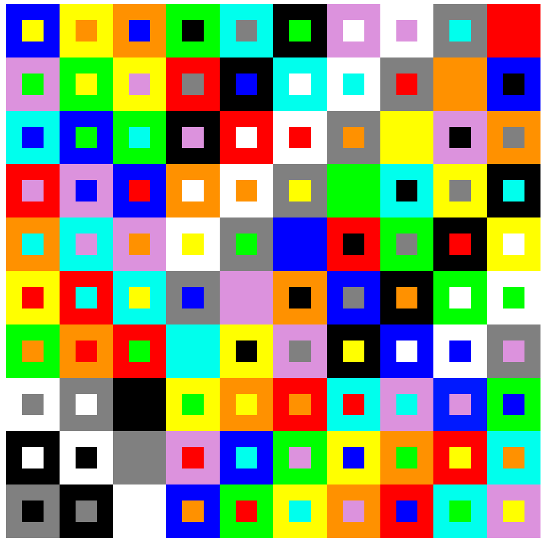
Frage: Wo ist in dem Beweis die Induktionsverankerung geblieben?

Wie steht es mit Eulers Problem, also $n = 6$? Herr Euler vermutete, daß 2 und 6 schon schiefgehen und der Rest relativ einfach ist, daß $n \equiv 2 \, mod \, 4$ nicht geht. Für $n = 6$ zitieren wir:

> Surprisingly there is no such solution. Whether he was asked by Catherine or not, Euler did consider the problem in 1779 and convinced himself that it was impossible. Euler was capable of monumental calculations, but it is not clear that he had really examined all the cases. This was systematically done in 1900 by G. Tarry. Today a computer can do this easily.
>
> *J.H. van Lint & R.M. Wilson "A Course in Combinatorics"*

Zum letzten Satz fällt mir nicht viel ein. Es mag sein, daß die Fallunterscheidungen von einem Computer leicht ausgeixt werden können, der Programmierer aber dennoch etwas Zeit und Intelligenz investieren muß.

Allerdings lag Herr Euler völlig schief. 2 und 6 sind, wie man inzwischen weiß, die einzigen Ausnahmen. Die folgende Grafik zeigt $n = 10$.



Magische Quadrate

Eigentlich sind orthogonale Paare lateinischer Quadrate schon magisch, wenn man die Einträge nur richtig liest, nämlich als zweistellige Ziffern im n-aren System. Offensichtlich hat dann jede Zeile und Spalte genau die Summe

$$(n+1)(\sum_{i=0}^{n-1} i).$$

Die Transformation zu der am Anfang gewünschten Gestalt ist völlig einfach. Der Eintrag (i, j) wird ersetzt durch $ni + j + 1$. Wir erhalten also für $n = 5$ das magische Quadrat

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

Man hat so ein Konstruktionsverfahren, das für alle $n \in \mathbb{N} \setminus \{2, 6\}$ funktioniert. Das heißt aber nicht, daß es keinemagischen Quadrate der Größe 6 gäbe. Schon

Dürers Quadrat hat einen anderen Typ als die hier vorgestellten und auch für $n = 6$ gibt es magische Quadrate.

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

Dieses hat wie auch schon Dürers Beispiel den zusätzlichen Vorteil, daß die magische Summe auch auf der Hauptdiagonalen (bei Dürer auch auf der Nebendiagonalen) angenommen wird, was von manchem Spielverderber schon in der Definition gefordert wird, bei uns im Falle $n = 5$ aber nur zufällig erreicht wurde.