Bericht vom
1. Leipziger Seminar am 13. November 2004

Aufgabendiskussion Serie 2

zu Aufgabe 2-5A

Diese Aufgabe war eine Abzählaufgabe. Die Teile a) und b) konnten mittels der Anzahl von Permutationen gelöst werden. Für c) ließ sich das Invarianzprinzip anwenden. Wir haben noch weitere Schachbrettaufgaben gelöst:

Aufgabe 1 Finde (mit Begründung!) für jede der Schachfiguren Dame und Läufer jeweils die maximale Anzahl N, für die man N derartige Figuren auf einem Schachbrett platzieren kann, ohne dass sich gegenseitig bedrohen.

Lösung: Da keine zwei Damen in einer Reihe stehen dürfen, muss die maximal Anzahl kleiner oder gleich 8 sein. Wir vermuten, dass 8 schon die maximale Anzahl ist und müssen jetzt eine Möglichkeit explizit angeben (s. Abb.). Eine solche Verteilung kann man zum Beispiel über *back-tracking* finden, einer Art des systematischen Probierens. Wir verteilen so lange Damen auf dem Schachbrett bis wir keine mehr setzen dürfen.

				D			
						D	
D							
		D					
							D
					D		
			D				
	D						

Sind jetzt noch keine 8 auf dem Schachbrett, nehmen wir die letzte zurück, setzen sie woanders hin und schauen, ob wir noch eine neue Dame setzen können. Wenn nicht, nehmen wir auch diesen Zug wieder zurück und setzen die Dame erneut auf ein neues Feld usw. Haben wir alle möglichen Felder schon ausprobiert, gehen wir in unserer Versuchsreihe noch einen Schritt mehr zurück und nehmen die letzten zwei Damen vom Feld usw. Das *Damenproblem* ist sehr berühmt. Es wird gerne als Aufgabe für Programmierer genommen. Insgesamt gibt es 92 mögliche Anordnungen.

Jetzt zu den Läufern. Läufer bedrohen immer Diagonalen. Es gibt insgesamt 15 Diagonalen von links unten nach rechts oben. Die Maximalanzahl der Läufer ist also kleiner oder gleich 15. Aber zwei dieser Diagonalen bestehen nur aus einem Feld, die obere linke und untere rechte Ecke. Bedroht ein Läufer eine der beiden Ecken, so bedroht er automatisch auch die andere. Es können sich also maximal 14 Läufer nicht gegenseitig

L	L	L	L	L	L	L	
L	L	L	L	L	L	L	

bedrohen. Wie im Bild ersichtlich, können 14 Läufer tatsächlich so aufgestellt werden, dass sie sich nicht bedrohen. □

Bei solchen Aufgaben ist es immer notwendig den Existenzbeweis zu liefern, das heißt eine solche Aufstellung mit 8 *Damen bzw.* 14 *Läufern wirklich anzugeben.*

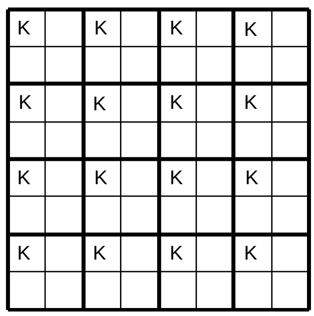
Aufgabe 2 Auf einem Schachbrett sollen w weiße und s schwarze Türme so aufgestellt werden, dass sich Türme verschiedener Farbe nicht schlagen. Wie viele verschiedene Möglichkeiten gibt es jeweils für die in einem Schachspiel relevanten Fälle, d.h. $(w, s) = (1, 1),\ (1, 2),\ (2, 2)$?

zu Aufgabe 2-5B

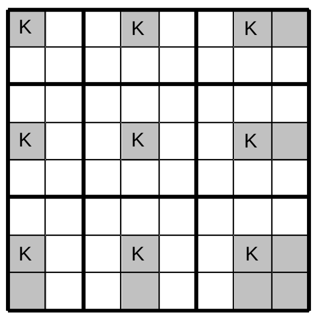
In dieser Aufgabe sollte das Dirichletsche Schubfachprinzip angewendet werden. Das wesentliche Problem bestand darin, die richtigen Schubfächer zu finden. Weiterhin wurde folgende Aufgabe diskutiert:

Aufgabe 3 Wie viele Könige muss man mindestens auf ein Schachbrett stellen, damit sie dieses komplett abdecken, sich aber nicht gegenseitig schlagen? Wie viele Könige kann man unter diesen Bedingungen höchstens aufstellen?

Lösung: Zur Bestimmung der größtmöglichen Anzahl betrachten wir eine Lösung mit 16 Königen (Bild rechts), die man sehr leicht findet. Wir unterteilen das Schachbrett wie eingezeichnet in 16 2×2-Quadrate und benutzen diese als Schubfächer: Wenn es eine Lösung mit mehr als 16 Königen gäbe, so würden sich in einem dieser 16 Quadrate mindestens 2 Könige befinden. Das ist aber nicht möglich, da sich diese sonst schlagen würden. Also ist 16 tatsächlich die maximale Anzahl.



Betrachten wir nun zur Bestimmung der minimalen Anzahl eine Lösung mit 9 Königen, wie sie rechts zu sehen ist. Wir unterteilen das Schachbrett wie eingezeichnet in 9 Rechtecke. Angenommen es gibt eine Lösung mit weniger als 9 Königen, dann muss eines dieser Rechtecke frei bleiben. Allerdings befindet sich in jedem der 9 Rechtecke mindestens ein Feld, dass von einem König, der in einem anderen Rechteck steht, nicht gedeckt werden kann (grau schraffierte Felder). Widerspruch! Also ist die minimale Anzahl 9. □



Wir sehen hier eine interessante „Umkehrung“ des Schubfachprinzips:
Werden k Objekte auf n Schubfächer verteilt und gilt $k < n$, dann gibt es mindestens ein Schubfach, das frei bleibt.

Aufgabe 4 Löse Aufgabe 1 für die Schachfigur des Springers!

Aufgabe 5 In einem rechteckigen Waldstück von 600 m Länge und 500 m Breite wachsen genau 444 Bäume mit einem Stammdurchmesser von 50 cm. In dem Wald sollen 20 rechteckige Grundstücke von 30 m Länge und 20 m Breite, auf denen kein Baum steht, zur Bebauung ausgewählt werden. Ist das bei jeder beliebigen Anordnung der Bäume mit Sicherheit möglich?

Kongruenzen und lineare diophantische Gleichungen

Jeder kennt Division mit Rest, das heißt: Für alle ganzen Zahlen m, n gibt es eindeutig bestimmte ganze Zahlen q (der *Quotient*) und r (der *Rest*) mit

$$m = qn + r \quad \text{und} \quad 0 \leq r < b$$

Zum Beispiel gilt für $m = 7$ und $n = 3$: $7 = 2 \cdot 3 + 1$, also lässt 7 bei Division durch 3 den Rest 1.
Oder für $m = -23$ und $n = 5$ gilt: $-23 = 5 \cdot (-5) + 2$, also lässt -23 bei Division durch 5 den Rest 2.

Wir nennen zwei ganze Zahlen a, b *kongruent modulo* m, wenn sie bei Division durch m den gleichen Rest lassen, und schreiben

$$a \equiv b \mod m \quad \text{oder} \quad a \equiv b \pmod{m} \quad \text{oder einfach} \quad a \equiv b(m)$$

Oben haben wir gesehen: $7 \equiv 1 \pmod 3$ und $-23 \equiv 2 \pmod 5$
Kongruenzen sehen Gleichungen ähnlich. Deshalb fragen wir uns, welche Rechenregeln für Gleichunge auch für Kongruenzen gelten. Einige Regeln seien hier kurz aufgelistet:

(i) $a \equiv b \pmod{m}$ ist dasselbe wie $m|(a-b)$oder $a - b \equiv 0 \pmod{m}$

(ii) Sind $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$, dann gilt:
$a \pm c \equiv b \pm d \pmod{m}$, $ac \equiv bd \pmod{m}$, $a^n \equiv b^n \pmod{m}$ für alle $n \in \mathbb{N}$

(iii) Division ist schwieriger, da das in ganzen Zahlen nicht immer geht. Es gilt:
aus $ac \equiv bc \pmod{m}$ und $\mathrm{ggT}(c, m) = 1$ folgt $a \equiv b \pmod{m}$ und
aus $ac \equiv bc \pmod{mc}$ folgt $a \equiv b \pmod{m}$.
Zusammen ergibt das: $ac \equiv bc \pmod{m} \Longrightarrow a \equiv b \pmod{\frac{m}{ggT(c,m)}}$

(iv) Eine einfache, aber wichtige Eigenschaft ist die Transitivität:
aus $a \equiv b \pmod m$ uns $b \equiv c \pmod m$ folgt $a \equiv c \pmod m$.
Dies erlaubt uns, Zahlen in Kongruenzen durch andere, zu ihr kongruente Zahlen, zu ersetzen.

Aufgabe 6 Zeige: a) $44 | 43^7 - 87^{13}$ und b) $51 | 171^n - 33^{2n}$ für jedes $n \in \mathbb{N}$!

Lösung: a) Wir zeigen: $43^7 - 87^{13} \equiv 0 \pmod{44}$:
$43^7 - 87^{13} \equiv (-1)^7 - (-1)^{13} \equiv (-1) - (-1) \equiv 0 \pmod{44}$
Es ist oft nützlich, negative Reste zu verwenden, da man dann mit kleineren Zahlen arbeiten kann.
b) $171^n - 33^{2n} \equiv 18^n - (-18)^{2n} \equiv 18^n - 18^{2n} \equiv 18^n - (18^2)^n \equiv 18^n - 324^n \equiv 18^n - 18^n \equiv 0 \pmod{51}$ $\square$

Aufgabe 7 Auf welche Ziffer enden: a) 999^{999}, b) 797^{26} und
c) $3826^{12} \cdot 574^8 \cdot 2964^9 \cdot 39^{26}$?

Lösung: Wir wollen das Problem mit Kongruenzen lösen: Endziffer bestimmen ist das Gleiche wie den kleinsten Rest $\pmod{10}$ ermitteln.
a) $999^{999} \equiv (-1)^{999} \equiv -1 \equiv 9 \pmod{10}$. Also endet 999^{999} auf 9.
b) $797^{26} \equiv (-3)^{26} \equiv ((-3)^2)^{13} \equiv 9^{13} \equiv (-1)^{13} \equiv -1 \equiv 9 \pmod{10}$. Also endet diese Zahl auch auf 9.
c) Potenzen einer Zahl, die auf 6 endet, enden wieder auf 6: $3826^{12} \equiv 6 \pmod{10}$.
$574^8 \equiv 4^8 \equiv 16^4 \equiv 6 \pmod{10}$ und analog $2964^9 \equiv 6 \pmod{10}$.
$39^{26} \equiv 1 \pmod{10}$ ist klar. Damit erhalten wir:
$3826^{12} \cdot 574^8 \cdot 2964^9 \cdot 39^{26} \equiv 6 \cdot 6 \cdot 6 \cdot 1 \equiv 8 \pmod{10}$. Also endet die Zahl auf 8.$\square$

Aufgabe 8 Der berühmte französische Mathematiker Serge Lang schrieb das populäre Buch „Faszination Mathematik“. Die ISBN-Nummer des Buches lautet:

$$3 - 322 - 004a5 - 9$$

Wie groß ist die fehlende Ziffer a?

Lösung: Dazu muss man wissen, was die 10 Ziffern einer ISBN-Nummer miteinander zu tun haben: Die letzte Ziffer ist eine Prüfziffer und wenn $a_1 a_2 \dots a_9$ die ersten 9 Ziffern sind, dann ist die letzte genau $1 \cdot a_1 + 2 \cdot a_2 + \dots 9 \cdot a_9 = \sum_{i=1}^{9} i \cdot a_i$ $\pmod{11}$. Überprüfe das bei eigenen Büchern!

Prüfziffern benutzt man, um festzustellen, ob irgendwo ein Fehler (zum Beispiel durch Vertippen) in der Nummer ist. Das benutzt man auch an vielen anderen Stellen, wo solche Codes vorkommen.

Zusatzfrage: Auf einigen Büchern steht als letzte „Ziffer“ ein X. Warum? Wofür steht es? (Beispiel: Simon Singhs „Fermats letzter Satz“ hat die ISBN-Nummer $3 - 423 - 33052 - X$)

Nun zur eigentlichen Lösung der Aufgabe: es muss also gelten:

$$1 \cdot 3 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 2 + 5 \cdot 0 + 6 \cdot 0 + 7 \cdot 4 + 8 \cdot a + 9 \cdot 5 \equiv 9 \pmod{11}$$
$$\iff 8a \equiv 1 \pmod{11}$$

Jetzt kann man eine Lösung raten oder aber so vorgehen: $8a \equiv 1 \equiv 12 \equiv 23 \equiv 34 \equiv 45 \equiv 56 \pmod{11}$.
Nun ist 56 durch 8 teilbar und da $\mathrm{ggT}(8, 11) = 1$, folgt: $a \equiv 7 \pmod{11}$
Da wir eine Ziffer suchen, muss a folglich 7 sein. □

Wir haben gerade eine *lineare Kongruenz* gelöst. Allgemein heißt das:
Wir suchen x, so dass für gegebene a, $b \in \mathbb{Z}$, $m \in \mathbb{N}$ gilt:

$$ax \equiv b \pmod{m}.$$

Wie man das macht, haben wir gerade gesehen: Ersetze b durch eine kongruente Zahl, um so schrittweise alle gemeinsamen Faktoren von a und b zu kürzen. Wir müssen dabei die Regeln für die Division beachten!

Aufgabe 9 Löse: $46x \equiv -100 \pmod{12}$

Lösung: Zunächst kürzen wir den Faktor 2: $23x \equiv -50 \pmod{6}$
Daraus folgt $5x \equiv -2 \equiv 10 \pmod{6}$ und schließlich $x \equiv 2 \pmod{6}$.
Wir schreiben dies in eine Gleichung um und erhalten so als Lösungsmenge:
$L = \{x \in \mathbb{Z} : x = 6k + 2, k \in \mathbb{Z}\}$ □

Wenn eine lineare Kongruenz lösbar ist, dann besitzt sie unendlich viele Lösungen, nämlich für jede ganze Zahl eine. Doch: ist eine lineare Kongruenz immer lösbar?
Betrachte als Beispiel: $12x \equiv 7 \pmod{10}$
Mit unserem Verfahren sehen wir: $12x \equiv 7 \equiv 17 \equiv 27 \equiv 37 \equiv 47 \equiv \ldots$
Auf der rechten Seite steht immer eine ungerade Zahl, so dass wir nie den Faktor 2 kürzen können. Das sehen wir leichter, wenn wir die Kongruenz in eine Gleichung umschreiben: $12x = 10k + 7$ bzw. $12x - 10k = 7$. Die linke Seite dieser Gleichung ist durch 2 teilbar, die rechte nicht.
Dies verallgemeinern wir auf eine beliebige Kongruenz $ax \equiv b \pmod{m}$:
Unter Beachtung, dass jeder gemeinsame Teiler von a und m auch ein Teiler des $\mathrm{ggT}(a, m)$ ist, erhalten wir das Lösbarkeitskriterium:

Die Kongruenz $ax \equiv b \pmod{m}$ ist genau dann lösbar, wenn $ggT(a, m) | b$.

Aufgabe 10 Max verschlüsselt Texte mit der folgenden Methode:
Jedem Buchstaben wird die um 1 verkleinerte Nummer seiner Position im Alphabet zugeordnet, also $A \mapsto 0$, $B \mapsto 1$, ..., $Z \mapsto 25$. Um eine Zahlen zu verschlüsseln, multipliziert er diese mit 7, nimmt den kleinsten Rest mod 26 und übersetzt die Zahlen zurück in Buchstaben.
a) Verschlüssele: $MATHEMATIK$
b) Zeige, dass die Verschlüsselung eindeutig ist, d.h. keine zwei Buchstaben werden gleich verschlüsselt.
c) Wie kann man wieder entschlüsseln? Gib eine Entschlüsselungsfunktion an!
d) Entschlüssele: $TAXYCN$

Lösung: Die Verschlüsselungsfunktion ist $f(x) = 7x \pmod{26}$
a) $f(MATHEMATIK) = GADXCGADES$
b) Wir führen den Beweis indirekt: Angenommen es gibt $0 \leq x, y \leq 25$ mit $f(x) = f(y)$, das heißt $7x \equiv 7y \pmod{26}$. Daraus folgt $7(x-y) \equiv 0 \pmod{26}$ und da 7 und 26 teilerfremd sind, muss $x - y$ durch 26 teilbar sein. Wegen $0 \leq x, y \leq 25$, ist dies nur möglich, wenn x und y gleich sind. Also werden alle Buchstaben verschieden verschlüsselt.
c) Die Funktion f bildet x auf $7x$ ab und um zu entschlüsseln brauchen wir eine Funktion g, die $7x$ wieder auf x abbildet (Im Grunde versuchen wir, „Division“ durch 7 anders auszudrücken.). Wir machen den Ansatz $g(y) = a \cdot y \pmod{26}$ und da beim Hintereinanderausführen von Ver- und Entschlüsseln der Ausgangsbuchstabe wieder herauskommen muss, erhalten wir:

$$x = g(f(x)) = a \cdot (7x) = 7ax \pmod{26}$$

Diese Gleichung muss für alle $x = 0, \ldots 25$ gelten, insbesondere für 1. Damit erhalten wir eine einfache Kongruenz

$$7a \equiv 1 \equiv -25 \equiv -51 \equiv -77 \pmod{26} \Longrightarrow a \equiv -11 \equiv 15 \pmod{26}$$

Also ist unsere Entschlüsselungsfunktion $g(y) = 15y \pmod{26}$
Probe: $g(f(x)) = 15 \cdot 7x = 105x \equiv x \pmod{26}$
d) $g(TAXYCN) = ZAHLEN$ □

Zusatzfrage: Mit welchen Zahlen außer 7 kann man noch multiplizieren, um eine vernünftige Verschlüsselung zu erhalten (das heißt b) muss gelten)?

Wer mehr zu Kryptographie wissen will, hier eine Literaturempfehlung:
Simon Singh: „Codes - Die Kunst der Verschlüsselung“

Nun wollen wir uns mit *linearen diophantischen Gleichungen* beschäftigen. Das sind Gleichungen der Form

$$ax + by = c \quad \text{mit } a, b, c \in \mathbb{Z}$$

Wir suchen ganzzahlige Lösungen x und y.

Als Beispiel betrachten wir $4x - 6y = 3$. Diese Gleichung ist nicht lösbar, da die linke Seite der Gleichung durch 2 teilbar ist, die rechte aber nicht. Wie bei linearen Kongruenzen erhalten wir als Lösbarkeitskriterium:

Eine lineare diophantische Gleichung $ax + by = c$ ist genau dann lösbar, wenn $ggT(a, b)|c$.

Es gibt verschiedene Möglichkeiten, eine lineare diophantische Gleichung zu lösen. Hier wird die *Kongruenzmethode* an einem Beispiel vorgestellt:

Beispiel 11 Löse die lineare diophantische Gleichung $5x + 3y = 7$.
Betrachten wir die Gleichung mod 5 oder mod 3, dann fällt eine Variable weg.
(Beachte: *Ist eine Gleichung in $\mathbb{Z}$ wahr, dann ist sie auch* $\pmod{m}$ *wahr*)
Wir betrachten die Gleichung $\pmod 5$:

$$3y \equiv 7 \equiv 12 \pmod 5 \Longrightarrow y \equiv 4 \pmod 5$$

Nun schreiben wir das in eine Gleichung um: $y = 5k + 4$ mit $k \in \mathbb{Z}$.
Diese setzen wir wieder in die Ausgangsgleichung ein:

$$5x + 3(5k + 4) = 7 \Longleftrightarrow x = -3k - 1.$$

Nun können wir die Lösungsmenge aufschreiben:
$L = \{(x, y) : x = -3k - 1, y = 5k + 4, k \in \mathbb{Z}\}$

Allgemeine Beschreibung des Verfahrens:

1. Betrachte eine lineare diophantische Gleichung $ax + by = c$ modulo a (bzw. modulo b), löse die lineare Kongruenz $ax \equiv c \pmod b$ (bzw. $by \equiv c \pmod a$).

2. Schreibe die Lösung der Kongruenz in eine Gleichung um und setze diese in $ax + by = c$ ein.

3. Stelle nach der Variablen x (bzw. y) um und schreibe die Lösungsmenge auf.

Aufgabe 12 Welche Paare (a,b) natürlicher Zahlen a und b erfüllen die Gleichung

$$19a + 99b = 1999 \text{ ?}$$

Lösung: Der Einfachheit halber wählen wir den kleineren Koeffizienten und betrachten die Gleichung (mod 19):

$$99b \equiv 1999 \pmod{19} \Longleftrightarrow 99b \equiv 99 \pmod{19} \Longleftrightarrow b \equiv 1 \pmod{19}$$

Also ist $b = 19k + 1$ mit $k \in \mathbb{Z}$. Einsetzen in die Ausgangsgleichung liefert

$$19a + 99 \cdot 19k + 99 = 1999 \Longleftrightarrow 19a = -99 \cdot 19k + 1900 \Longleftrightarrow a = -99k + 100$$

Die Lösungenge in $\mathbb{Z}$ ist damit: $L = \{(a,b) : a = -99k + 100, b = 19k + 1, k \in \mathbb{Z}\}$
Da a und b natürliche Zahlen sein sollen, muss gelten: $a \geq 0$ und $b \geq 0$. Aus der ersten Ungleichung folgt $k \leq 1$ und aus der zweiten folgt $k \geq 0$. Damit erhalten wir genau zwei Lösungen der obigen Gleichung, nämlich die Paare $(100; 1)$ und $(1; 20)$. $\square$

Aufgabe 13 Am Ende eines Schuljahres sollen 36 Schüler mit je einem Buch ausgezeichnet werden. Es kommen Bücher für 9,50 Euro, 11 Euro und 13,75 Euro in Frage. Insgesamt stehen 400 Euro zur Verfügung, die restlos aufgebraucht werden sollen. Welche Varianten gibt es für den Bücherkauf?

Unterhaltsame Mathematik:

Magische Quadrate

In einem $n \times n$ Quadrat sollen die Zahlen von 1 bis n^2 so angeordnet werden, dass die Summe der Zahlen in jeder Reihe und in den beiden Diagonalen immer gleich ist. Ein solches Quadrat nennt man *magisches Quadrat der Ordnung n.*

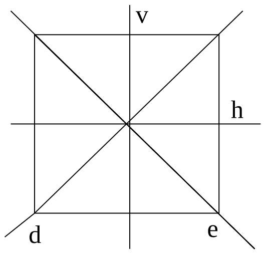
Zuerst suchen wir ein magisches Quadrat der Ordnung 3. Zwei sind in der Abbildung angegeben. Es fällt auf, dass beide durch Spiegelung auseinander hervorgehen, es also bis auf Symmetrie die selben sind.

4	3	8
9	5	1
2	7	6

2	7	6
9	5	1
4	3	8

Aufgabe 14 Wieviele verschiedene magische Quadrate können durch Symmetrie aus einem gegebenen gewonnen werden?

Lösung: Wir können an den vier Symmetriachsen h, v, e und f spiegeln und um den Mittelpunkt des Quadrates um $90°, 180°$ und $270°$ drehen. Aus einem gegebenen magischen Quadrat können wir mindestens sieben neue konstruieren, die bis auf Symmetrie mit dem Ausgangsquadrat identisch sind.



Gibt es noch mehr?
Wir wissen, dass die Hintereinanderausführung zweier Symmetrieoperationen wieder eine Symmetrie ergibt. Drehen wir erst um $90°$ und dann um $270°$, haben wir insgesamt um $360°$, also effektiv gar nicht, gedreht (Diese Symmetrieoperation bezeichnen wir als Identität). Wir erhalten also so kein neues Quadrat. Auch wenn wir erst an v und dann an h spiegeln, haben wir insgesamt um $180°$ gedreht.
Überprüfe, dass jede beliebige Hintereinausführung von einigen der acht (vier Spiegelungen + vier Drehungen (Identität mitgezählt)) Symmetrieoperationen wieder eine dieser Symmetrieoperationen ergibt.

Wir vermuten, dass für ein Quadrat nur acht Symmetrieoperationen existieren. Wie beweisen wir das?
Bei jeder Symmetrie muss eine Ecke in eine Ecke überführt werden. Wir nummerieren die Ecken von 1 bis 4 durch. Wir sehen, die 1 kann auf vier Ecken abgebildet werden. Dann gibt es für die 2 nur noch zwei Möglichkeiten, da sie direkt neben der 1 stehen muss, und danach ist es der Platz der 3 und der 4 eindeutig bestimmt. Insgesamt gibt es damit nur $4 \cdot 2 = 8$ Symmetrien für das Quadrat. □

Mit diesen Überlegungen haben wir gezeigt, dass es immer 8 magische Quadrate gibt, die bis auf Symmetrie identisch sind. Doch gibt es noch magische Quadrate der Ordnung 3, die nicht identisch zu dem gefundenen sind?

An dem zuerst gefundenen magischen Quadrat können wir ablesen, dass die Summe in einer Reihe (oder Spalte oder Diagonale) immer 15 ist. Diese Zahl heißt *magische Konstante.*
Die Tripel $(9, 5, 1)$ und $(9, 4, 2)$ sind die einzigen Möglichkeiten, die magische Konstante als Summe zweier Zahlen und der 9 auszudrücken. Da die Ecken und auch die Mitte jeweils Teil von mehr als zwei Tripeln (Reihe, Spalte oder Diagonale) ist, kann die 9 nur in einem der vier restlichen Felder stehen. Es gibt somit für die 9 nur eine Möglichkeit (bis auf Symmetrie). 5 ist die einzige Möglichkeit für die Mitte (warum?). Daraus ergibt sich als einzige Möglichkeit das schon oben gefundene magische Quadrat.

Aufgabe 15 Bestimme die magische Konstante M_n für ein magisches Quadrat der Ordnung n.

Lösung: Die Summe in jeder der n Reihen ist M_n. Addieren wir alle Zahlen, haben wir die Summe aller Zahlen von 1 bis n^2 gebildet. Damit haben wir aber auch die Summe aller n Reihen berechnet und es folgt:

$$M_n = \frac{1}{n}\sum_{i=1}^{n^2} i = \frac{1}{n}\frac{n^2(n^2+1)}{2} = \frac{1}{2}n(n^2+1) \in \mathbb{N}$$

Wir haben für diese Lösung die Methode des *doppelten Abzählens* verwendet! □

So sind z.B. $M_3 = 15,\ M_4 = 34$ und $M_5 = 65$.

Jetzt wollen wir einige magische Quadrate der Ordnung 4 finden. Eines ist wieder in der Abbildung angegeben. Dies ist, wie wir bald sehen werden, ein besonderes magisches Quadrat der Ordnung 4. Wir werden mit Hilfe dieses Quadrates leicht neue konstruieren können. Dazu ziehen wir von jeder Zahl eins ab und schreiben sie im Zahlensystem zur Basis 4 (Die Zahl 14 ist z.B. zur Basis 4 gleich 32, denn $14 = \underline{3} \cdot 4^1 + \underline{2} \cdot 4^0$). Es fällt auf, dass in jeder Reihe, jeder Spalte und jeder Diagonale die Zahlen von 0 bis 3 sowohl in der ersten Ziffer als auch in der zweiten genau einmal vorkommen. D.h. sowohl die Vierer- als auch die Einerstellen bilden ein perfektes lateinisches Quadrat (s. Abb.). Ein $n \times n$ Quadrat heißt *lateinisch*, wenn die Zahlen von 0 bis $n-1$ in jeder Spalte und in jeder Zeile genau einmal vorkommen. Gilt dies zusätzlich auch für die beiden Diagonalen, nennen wir das lateinische Quadrat *perfekt*. Nicht alle magischen Quadrate der Ordnung 4 haben diese Eigenschaft, dass sie zu zwei perfekten lateinischen Quadraten führen.

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

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

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

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

Aufgabe 16 Finde ein magisches Quadrat der Ordnung 4, das nicht aus zwei perfekten lateinischen Quadraten entsteht!

Was nützt uns diese Beobachtung zur Konstruktion neuer magischer Quadrate? Wenn wir die Zahlen innerhalb eines solchen perfekten lateinischen Quadrates permutieren, bleibt dies natürlich ein perfektes lateinisches Quadrat.

Ein Beispiel ist in der nebenstehenden Abbildung gegeben. Dort wurde nur im zweiten lateinischen Quadrat permutiert.

Führen wir jetzt die beiden wieder zu einem lateinischen Quadrat zusammen, übersetzen die Zahlen ins Dezimalsystem und addieren wieder jeweils eins, erhalten wir ein neues magisches Quadrat.

Dies ist bei jeder Permutation der Fall. Warum?

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

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

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

Bei der Addition ist es egal, in welcher Reihenfolge wir addieren. Berechnen wir also die Summe zur Basis 4, in dem wir Einer- und Viererstellen erst einzeln addieren:

$$(0 + 1 + 2 + 3) \cdot 10 + (0 + 1 + 2 + 3) = 12 \cdot 10 + 12 = 120 + 12 = 132.$$

Sie ist konstant unter Permutationen. Damit ist auch die Summe im Dezimalsystem konstant und wir erhalten auf diese Weise immer ein magisches Quadrat.

Wie viele magische Quadrate erhalten wir mit unseren beiden perfekten lateinischen Quadraten?

Für ein perfektes lateinisches Quadrat haben wir $4! = 24$ Permutationsmöglichkeiten, Permutationen der Zahlen von 0 bis 3. Dies gilt für beide perfekten lateinischen Quadrate. Wir bezeichnen das perfekte lateinische Quadrat, welches aus den Viererstellen gebildet wird mit A, und das, welches aus den Einerstellen gebildet wird mit B. Aus einem perfekten lateinischen Quadrat A', welches durch Permutation aus A erzeugt wird, und einem Quadrat B', durch Permutation aus B gebildet, können wir, wie oben gesehen, ein magisches Quadrat bilden und haben dafür insgesamt dann $4! \cdot 4! = 24^2 = 576$ Möglichkeiten. Je zwei dieser Möglichkeiten ergeben verschiedene magische Quadrate (unabhängig von der Symmetrie). Können zwei der dadurch erstandenen magischen Quadrate durch Symmetrie auseinander hervorgehen? Dann müsste auch schon jedes der beiden perfekten lateinischen Quadrate A' und B' durch Symmetrie aus A bzw. B entstehen.

Aufgabe 17 Betrachte das perfekte lateinische Quadrat A und alle Quadrate die durch Symmetrie aus diesem entstehen (insgesamt 8). Zeige, dass 4 dieser 8 Quadrate auch durch Permutation aus A gewonnen werden können?

Somit haben wir schon $576/4 = 144$ echt verschiedene (das heißt, sie sind auch noch nach Anwenden von Symmetrieoperationen voneinander verschieden) magische Quadrate der Ordnung 4 gefunden und das nur mit den beiden perfekten lateinischen Quadraten vom Anfang.

Aufgabe 18 Wie viele perfekte lateinische Quadrate der Ordnung 4 gibt es, wie viele bis auf Symmetrie und Permutation?

Können wir aus je zwei perfekten lateinischen Quadraten immer ein magisches Quadrat bauen? Nein, nehmen wir z.B. zwei identische lateinische Quadrate, können wir nicht gewährleisten, dass jede Zahl von 1 bis 16 genau einmal vorkommt. Welche Kombinationen von perfekten lateinischen Quadraten sind möglich?

Wie sieht das Ganze für andere Ordnungen aus? Probiere selbst aus!

Aufgabe 19 Finde alle lateinischen Quadrate der Ordnung 3. Wie viele von ihnen sind perfekt?

Anworten auf alle Fragen und Lösungen zu den Aufgaben, die offen geblieben sind, könnt ihr uns gern zuschicken. Am besten an

Alexander Unger
Schirmerstraße 21
04318 Leipzig

oder per E-Mail an

`nadgr@gmx.de` oder `alex.unger@gmx.de`

Natürlich nehmen wir auch eure Fragen, Ideen und Anregungen zu diesen oder anderen Themen gern entgegen.

Nadine Große und Alexander Unger