

# ***Diskrete Mathematik***

Sebastian Iwanowski  
FH Wedel

Kap. 4: Zahlentheorie

## **Referenzen zum Nacharbeiten:**

Beutelspacher 5

Lang 7,

Biggs 20, 22, 23 (jeweils teilweise, für Kap. 4.5)

Hachenberger 2 (außer 2.1), 5.1, 5.2, 5.6, 6.1 (zur Vertiefung: 6.2, 6.3)

# 4. Zahlentheorie

In diesem Kapitel repräsentieren die Variablen aller Definitionen und Sätze (Regeln), wenn nicht anders spezifiziert, **ganze** Zahlen (Elemente von  $\mathbb{Z}$ ).

## 4.1 Teilbarkeit

### Definition von Teilbarkeit

Eine ganze Zahl  $m$  **teilt** eine ganze Zahl  $n$ , wenn es eine ganze Zahl  $q$  gibt mit:  $n = q \cdot m$   
( $\forall m, n \in \mathbb{Z}: m \mid n \Leftrightarrow \exists q \in \mathbb{Z}: n = q \cdot m$ )

### Teilbarkeitssätze über Summen, Differenzen und Produkte

$$1) \quad m \mid n_1 \wedge m \mid n_2 \Rightarrow m \mid (n_1 + n_2)$$

$$2) \quad m \mid n_1 \wedge m \mid n_2 \Rightarrow m \mid (n_1 - n_2)$$

$$3) \quad m \mid n_1 \quad \Rightarrow m \mid (n_1 \cdot n_2)$$

# 4. Zahlentheorie

## 4.1 Teilbarkeit

### Größenbeschränkungen für Teiler und Vielfache

- 1) Für jeden echten Teiler  $m \neq 1, n$  von  $n$  gilt:  $m \leq \lfloor n / 2 \rfloor$
- 2) Für zwei Teiler  $p, q$  von  $n$  mit  $p \cdot q = n$  gilt:  $(p \leq \sqrt{n}) \vee (q \leq \sqrt{n})$
- 3) Die einzigen Vielfachen  $n$  von  $m$  mit  $\lfloor n \rfloor \leq \lfloor m \rfloor$  sind  $-m, 0$  und  $m$

# 4. Zahlentheorie

## 4.1 Teilbarkeit

### Zahlendarstellungen mit Hilfe von Zahlenbasen

Dezimale Darstellung

Binäre Darstellung

Definition der Quersumme in Abhängigkeit von der Zahlenbasis

### Quersummenregeln

Eine Zahl ist durch 3 teilbar

⇔ Die dezimale Quersumme der Zahl ist durch 3 teilbar

Eine Zahl ist durch 9 teilbar

⇔ Die dezimale Quersumme der Zahl ist durch 9 teilbar

Für die *binäre* Quersumme gibt es keine entsprechende Quersummenregel

# 4. Zahlentheorie

## 4.1 Teilbarkeit

### Definition von ggT und kgV

$$a = \text{ggT}(m,n) :\Leftrightarrow (a \mid m) \wedge (a \mid n) \wedge [(b \mid m) \wedge (b \mid n) \Rightarrow (b \leq a)]$$

$$a = \text{kgV}(m,n) :\Leftrightarrow (m \mid a) \wedge (n \mid a) \wedge (a > 0) \wedge [(m \mid b) \wedge (n \mid b) \wedge (b \neq 0) \Rightarrow (a \leq |b|)]$$

### Zusammenhang zwischen ggT und kgV

$$\forall m,n \in \mathbb{N} \setminus \{0\}: \quad \text{ggT}(m,n) \cdot \text{kgV}(m,n) = m \cdot n$$

### Teilbarkeitsregel für teilerfremde Zahlen

**Definition:** Zwei ganze Zahlen  $m,n$  heißen teilerfremd  $:\Leftrightarrow \text{ggT}(m,n) = 1$

**Satz:** Für zwei teilerfremde Zahlen  $m,n$  und eine ganze Zahl  $a$  gilt:  
 $m \mid a \wedge n \mid a \Rightarrow m \cdot n \mid a$

# 4. Zahlentheorie

## 4.2 Teilen mit Rest

### Definition von ganzzahligem Quotienten und Rest

(1) Sei  $n = q \cdot m + r$  für ganze Zahlen  $n, m, q, r$ ,  $0 \leq r < m$

Dann ist  $q$  der ganzzahlige Quotient von  $n$  geteilt durch  $m$  ( $q = n \text{ DIV } m$ )

Dann ist  $r$  der ganzzahlige Rest von  $n$  geteilt durch  $m$  ( $r = n \text{ MOD } m$ )

### Eindeutigkeit und Existenz von ganzzahligem Quotienten und Rest

Für beliebige zwei ganze Zahlen  $n$  und  $m \neq 0$  gibt es die Darstellung (1)

Die Darstellung (1) ist eindeutig,

d.h.  $q$  und  $r$  sind zu gegebenen  $n, m$  eindeutig bestimmt.

# 4. Zahlentheorie

## 4.2 Teilen mit Rest

### Euklidischer Algorithmus zur Bestimmung von ggT und kgV

**Satz:** Sei  $n = q \cdot m + r$  für ganze Zahlen  $n, m, q, r$ ,  $0 \leq r < m$

Dann gilt:  $\text{ggT}(n, m) = \text{ggT}(m, r)$

**Algorithmus:**

- 1) Berechne  $q$  und  $r$  für  $n$  und  $m$
- 2) Falls  $r = 0$ : Setze  $\text{ggT} := m$ , fertig!  
Anderenfalls: Setze  $n := m$  und  $m := r$  und gehe zu 1)

# 4. Zahlentheorie

## 4.3 Primzahlen

*In diesem Abschnitt repräsentieren die Variablen aller Definitionen und Sätze (Regeln), wenn nicht anders spezifiziert, **natürliche** Zahlen (Elemente von  $\mathbb{N}$ ).*

### Definition

Eine natürliche Zahl  $p > 1$  heißt Primzahl, wenn  $p$  und  $1$  die einzigen Teiler von  $p$  sind  
(  $p$  heißt Primzahl  $:\Leftrightarrow (p \in \mathbb{N}) \wedge (p > 1) \wedge ( ((n \in \mathbb{N}) \wedge (n \mid p)) \Rightarrow ((n = 1) \vee (n = p)) )$  )

### Bestimmung von Primzahlen: Sieb des Eratosthenes

- 1) Füge alle Zahlen von 2 bis  $n$  in das Sieb ein.
- 2) Setze  $p := 2$ .
- 3) Solange  $p \leq \sqrt{n}$ , führe folgende Aktionen aus:
  - a) Streiche alle Zahlen durch, die Vielfache von  $p$  sind.
  - b) Setze  $p$  gleich der nächsten nicht durchgestrichenen Zahl.

Behauptung: Am Ende enthält das Sieb alle Primzahlen zwischen 2 und  $n$ .



# 4. Zahlentheorie

## 4.3 Primzahlen

### Anzahl von Primzahlen

- 1) Es gibt unendlich viele Primzahlen.
- 2) Die Primzahlen sind im Durchschnitt fast gleich verteilt:  
Jede  $\ln(n)$  – te Zahl bis  $n$  ist im Durchschnitt eine Primzahl.

# 4. Zahlentheorie

## 4.3 Primzahlen

### **Hauptsatz der elementaren Zahlentheorie: Existenz und Eindeutigkeit der Primzahlzerlegung**

Jede natürliche Zahl  $n > 1$  lässt sich als Produkt von Primzahlpotenzen darstellen:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_s^{e_s}$$

Die Primzahlen dieser Darstellung und die Exponenten (d.h. die Häufigkeit ihres Auftretens) sind eindeutig, d.h. die Darstellung als Produkt von Primzahlpotenzen ist bis auf die Reihenfolge eindeutig.

### **Anwendungen des Hauptsatzes**

Charakterisierung und Bestimmung vom ggT und kgV

Beweis des Zusammenhangs zwischen ggT und kgV

Charakterisierung von teilerfremden Zahlen

Beweis der Teilbarkeitsregel für teilerfremde Zahlen

# 4. Zahlentheorie

## 4.4 Modulare Arithmetik

### Definition einer Restklasse modulo $n$

Sei  $a \in \mathbb{Z}$ :

Die Menge  $[a]_n := \{b \in \mathbb{Z} : b \bmod n = a \bmod n\}$  heißt *Restklasse* von  $a$  modulo  $n$

### Eigenschaften von Restklassen:

Diese Definition einer Restklasse induziert eine Äquivalenzrelation auf  $\mathbb{Z}$ .

Die Restklassen sind die Äquivalenzklassen bzgl. dieser Äquivalenzrelation.

Mit  $\mathbb{Z}_n$  wird die Menge der Restklassen bezeichnet.

$$\mathbb{Z}_n = \{ [0]_n, [1]_n, \dots, [n-1]_n \} (\mathbb{Z}_n \text{ besteht also aus genau } n \text{ Elementen)}$$

# 4. Zahlentheorie

## 4.4 Modulare Arithmetik

### Rechnen mit Restklassen

**Addition:**  $[a]_n + [b]_n := [a+b]_n$

**Multiplikation:**  $[a]_n \cdot [b]_n := [a \cdot b]_n$

**Satz:** Addition und Multiplikation sind wohldefiniert.

### Definition von neutralen und inversen Elementen bzgl. Verknüpfungen:

Eine *Verknüpfung*  $\circ$  auf einer Menge  $M$  ist eine Funktion  $f: M \times M \rightarrow M$  mit  $f(a,b) = a \circ b$

$e$  heißt *neutrales Element* bzgl. einer Verknüpfung  $\circ$ , wenn  $\forall m \in M: e \circ m = m \circ e = m$

$m^{-1}$  heißt *inverses Element* von  $m$  bzgl. einer Verknüpfung  $\circ$ , wenn  $m^{-1} \circ m = m \circ m^{-1} = e$

Anm.: Bei nichtkommutativen Verknüpfungen unterscheidet man zwischen links- und rechtsneutralen Elementen sowie zwischen links- und rechtsinversen Elementen.

# 4. Zahlentheorie

## 4.4 Modulare Arithmetik

### Neutrale und inverse Elemente von Restklassen

$[0]_n$  ist das neutrale Element der Addition:  $\forall a \in \mathbb{Z}: [0]_n + [a]_n = [a]_n + [0]_n = [a]_n$

$[n-a]_n$  ist das inverse Element von  $[a]_n$  der Addition:  $\forall a \in \mathbb{Z}: [n-a]_n + [a]_n = [a]_n + [n-a]_n = [0]_n$

$[1]_n$  ist das neutrale Element der Multiplikation:  $\forall a \in \mathbb{Z}: [1]_n \cdot [a]_n = [a]_n \cdot [1]_n = [a]_n$

Ein inverses Element von  $[a]_n$  der Multiplikation existiert nicht immer!

**Satz:** Ein inverses Element von  $[a]_n$  der Multiplikation existiert genau dann, wenn  $a$  und  $n$  teilerfremd sind.

**Korollar:** Ein inverses Element von  $[a]_n$  der Multiplikation existiert für alle  $a \neq 0$ , wenn  $n$  eine Primzahl ist.

# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

### Definition der Struktur einer Gruppe:

Sei  $G$  eine nichtleere Menge und  $\oplus$  eine Verknüpfung zwischen den Elementen von  $G$ .  
Dann heißt die Struktur  $(G, \oplus)$  eine **abelsche Gruppe**, wenn folgende Eigenschaften erfüllt sind:

1)  $\forall a, b \in G: a \oplus b \in G$

*innere Verknüpfung*

2)  $\forall a, b, c \in G: (a \oplus b) \oplus c = a \oplus (b \oplus c)$

*Assoziativgesetz*

3)  $\exists e \in G \forall a \in G: e \oplus a = a \oplus e = a$

*Neutrales Element*

4)  $\forall a \in G \exists a^{-1} \in G: a^{-1} \oplus a = a \oplus a^{-1} = e$

*Inverses Element*

5)  $\forall a, b \in G: a \oplus b = b \oplus a$

*Kommutativgesetz*

nur Eigenschaft 1):

Gruppoid

nur Eigenschaft 1), 2):

Halbgruppe

nur Eigenschaft 1), 2), 3), 4):

Gruppe

# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

**Beispiele für unendliche Gruppen bzw. Halbgruppen:**

- 1)  $(\mathbb{N}, +)$
- 2)  $(\mathbb{Z}, +)$
- 3)  $(\mathbb{Z}, \cdot)$
- 4)  $(\mathbb{Q}, +)$
- 5)  $(\mathbb{Q}, \cdot)$
- 6)  $(\mathbb{Q} \setminus \{0\}, \cdot)$
- 7)  $(\mathbb{Q}^+, \cdot)$
- 8)  $(\mathbb{R} \setminus \{0\}, \cdot)$
- 9)  $(\mathbb{R} \setminus \{0\}, +)$
- 10)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}\}, +)$
- 11)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}\}, \cdot)$
- 12)  $(\{f: \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{0\}\}, \cdot)$
- 13)  $(\{f: \mathbb{R}^+ \rightarrow \mathbb{R}^+\}, \cdot)$
- 14)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}\}, \circ)$
- 15)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ bijektiv}\}, \circ)$
- 16)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ differenzierbar}\}, \circ)$
- 17)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ bijektiv und differenzierbar}\}, \circ)$
- 18)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ linear}\}, \circ)$
- 19)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ linear}\}, +)$
- 20)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ Polynomfunktion}\}, +)$

# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

**Beispiele für endliche Gruppen bzw. Halbgruppen:**

- 1)  $(\mathbb{Z}_n, +)$  *(zyklische Gruppe mit additiver Verknüpfung)*
- 2)  $(\mathbb{Z}_n, \cdot)$
- 3)  $(\mathbb{Z}_n \setminus \{[0]_n\}, \cdot)$
- 4)  $(\mathbb{Z}_n^*, \cdot)$  *(multiplikative Gruppe der zu  $n$  teilerfremden Restklassen, prime Restklassengruppe mod  $n$ )*
- 5) Symmetriegruppe eines gleichseitigen Dreiecks
- 6)  $(\{x, \frac{1}{x}, 1-x, \frac{x-1}{x}, \frac{1}{1-x}, \frac{x}{x-1}\}, \circ)$  (Hintereinanderschaltung der Funktionen)
- 7)  $(\mathbb{Z}_n \times \mathbb{Z}_n, +)$  *(2-dimensionale zyklische Gruppe mit koordinatenweise additiver Verknüpfung)*
- 8)  $(\mathbb{Z}_n^r, +)$  *( $r$ -dimensionale zyklische Gruppe mit koordinatenweise additiver Verknüpfung)*



# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

### Wann gelten zwei Gruppen als gleich?

**Definition:** Zwei Gruppen  $(G, \oplus)$  und  $(H, \odot)$  gelten als gleich (isomorph), wenn es zwischen ihnen eine bijektive Abbildung  $I: G \rightarrow H$  gibt, welche die Verknüpfungsstruktur erhält:

$$\forall a, b \in G: I(a \oplus b) = I(a) \odot I(b)$$

$$\forall a, b \in H: I^{-1}(a \odot b) = I^{-1}(a) \oplus I^{-1}(b)$$

$I$  wird *Isomorphismus* genannt.

### Charakteristische Elemente endlicher Gruppen:

Ordnung einer Gruppe

Ordnung eines Elements

Erzeugnis eines Elements (einer Menge von Elementen)

**Satz:** Jede endliche Gruppe wird durch endlich viele Elemente erzeugt.

**Bemerkung:** Auch unendliche Gruppen können durch endlich viele Elemente erzeugt werden (aber niemals durch ein einzelnes).

# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

### Definition der Struktur eines Körpers:

Sei  $K$  eine nichtleere Menge und  $\oplus, \odot$  Verknüpfungen zwischen den Elementen von  $G$ . Dann heißt die Struktur  $(K, \oplus, \odot)$  ein **Körper**, wenn folgende Eigenschaften erfüllt sind:

1)  $(K, \oplus)$  ist abelsche Gruppe mit neutralem Element  $e_0$

2)  $(K, \odot)$  ist Halbgruppe

$$\begin{aligned} 3) \forall a, b, c \in K: (a \oplus b) \odot c &= (a \odot c) \oplus (b \odot c) \\ c \odot (a \oplus b) &= (c \odot a) \oplus (c \odot b) \end{aligned}$$

*Distributivgesetze*

$$4) \exists e_1 \in K \forall a \in K: e_1 \odot a = a \odot e_1 = a$$

*Neutrales Element*

$$5) \forall a \in K \setminus \{e_0\} \exists a^{-1} \in K \setminus \{e_0\}: a^{-1} \odot a = a \odot a^{-1} = e_1$$

*Inverses Element*

$$6) \forall a, b \in K: a \odot b = b \odot a$$

*Kommutativgesetz*

nur Eigenschaft 1), 2), 3): Halbring

nur Eigenschaft 1), 2), 3), 4), 6): Ring

nur Eigenschaft 1), 2), 3), 4), 5): Schiefkörper

# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

**Beispiele von unendlichen Körpern, Ringen, etc.:**

1)  $(\mathbb{Z}, +, \cdot)$

2)  $(\mathbb{Q}, +, \cdot)$

3)  $(\mathbb{R} \setminus \{0\}, +, \cdot)$

4)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}\}, +, \cdot)$

5)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ bijektiv}\}, +, \circ)$

6)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ bijektiv}\}, \circ, +)$

7)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ linear}\}, +, \cdot)$

8)  $(\{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ Polynomfunktion}\}, +, \cdot)$

# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

### Endliche Körper:

1)  $(\mathbb{Z}_p, +, \cdot)$  für beliebige Primzahl  $p$

2)  $((\mathbb{Z}_p)^r, +, \cdot)$  für beliebige Primzahl  $p$  und beliebige natürliche Zahl  $r$

### Satz (Galois, 1811-1832): *Das sind alle!*

Endliche Körper gibt es nur mit  $p^r$  Elementen ( $p$  Primzahl,  $r$  natürliche Zahl). Jeder endliche Körper ist bis auf Isomorphie gleich zu den oben genannten. Der Körper mit  $q$  Elementen wird  $GF(q)$  genannt ( $GF = \text{Galoisfeld}$ )

### Wie sieht die multiplikative Verknüpfung für $r > 1$ aus ?

Die multiplikative Gruppe des Körpers  $((\mathbb{Z}_p)^r, +, \cdot)$  ist isomorph zu  $(\mathbb{Z}_{p^r-1}, +)$ .

**In welcher Reihenfolge muss man die Elemente für die multiplikative Verknüpfung anordnen, damit das Distributivgesetz erfüllt ist?**

→ Konstruktionsanleitung mit Hilfe von Polynomen

# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

### Definition Polynom für einen beliebigen Körper K:

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Hierbei steht  $x$  für eine Variable mit Definitionsbereich  $K$ ,  $a_i$  für eine beliebige Konstante aus  $K$  und  $x^i$  bedeutet die  $i$ -fache Hintereinanderschaltung der multiplikativen Verknüpfung angewendet auf das Körperelement  $x$ .

Ein Polynom ist durch die Angabe des Tupels  $(a_n, a_{n-1}, \dots, a_1, a_0)$  eindeutig charakterisiert.

Das größte  $n$  mit  $a_n \neq 0$  wird als *Grad des Polynoms* bezeichnet.

Die Menge der Polynome über einem Körper  $K$  wird mit  $K[x]$  bezeichnet.

### Satz:

$(K[x], +, \cdot)$  bildet einen Ring.

# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

### Polynomdivision mit Rest:

Seien  $f[x]$ ,  $g[x]$  Polynome.

Dann gibt es Polynome  $q[x]$ ,  $r[x]$  mit  $\text{Grad}(r[x]) < \text{Grad}(g[x])$ :

$$f[x] = q[x] \cdot g[x] + r[x]$$

Die Polynome  $q[x]$ ,  $r[x]$  werden analog zum schriftlichen Divisionsverfahren von Zahlen gebildet. (Euklidischer Algorithmus).

Analog zur Definition bei Zahlen wird das Restpolynom  $r[x]$  auch  $f[x] \bmod g[x]$  genannt.

### Definitionen:

Eine **Nullstelle** zu einem gegebenen Polynom ist ein Wert des Körpers  $K$ , dessen Einsetzung in das Polynom den Wert 0 ergibt.

Ein **Polynom**  $f[x]$  über einem Körper  $K$  heißt **reduzibel**, wenn es zwei Polynome  $g[x]$ ,  $h[x]$  in  $K[x]$  gibt mit  $f[x] = g[x] \cdot h[x]$  (übliche Polynommultiplikation). Wenn es keine solche Zerlegungsmöglichkeit gibt, heißt  $f[x]$  **irreduzibel**.

**Satz:**  $f[x]$  ist irreduzibel  $\Rightarrow$   $f[x]$  hat keine Nullstelle

Für Polynome  $f[x]$  mit  $\text{Grad} \leq 3$  gilt sogar:  $f[x]$  ist irreduzibel  $\Leftrightarrow$   $f[x]$  hat keine Nullstelle.

# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

**Konstruktionsanleitung** für GF (q) mit  $q = p^r$  (p Primzahl, r natürliche Zahl):

- 1) Bestimme die Additions- und Multiplikationstabellen von GF (p):  
Dieser *Primkörper* ist isomorph zum Restklassenkörper  $(\mathbb{Z}_p, +, \cdot)$ .
- 2) Identifiziere die Elemente aus GF (q) mit den  $p^r$  verschiedenen Polynomen über  $(\mathbb{Z}_p, +, \cdot)$  mit Grad  $< r$
- 3) Bilde die Additionstabelle wie bei Polynomen üblich.  
(Anmerkung: Die entstehende Gruppe ist isomorph zu  $((\mathbb{Z}_p)^r, +)$ )
- 4) Wähle ein irreduzibles Polynom  $g[x]$  über GF (p) mit Grad = r.  
Bilde die Multiplikationstabelle wie bei Polynomen üblich,  
aber *rechne modulo  $g[x]$* , um jeweils Polynome mit Grad  $< r$  zu erzeugen.  
(Anmerkung: Die entstehende Gruppe ist isomorph zu  $(\mathbb{Z}_{q-1}, +)$ )

# 4. Zahlentheorie

## 4.5 Algebraische Strukturen

**Beispiel:** GF (9)      $9 = 3^2$  ( $p = 3, r = 2$ )

Der Primkörper ist also GF(3)

Elemente:  $\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$

Alle Polynome mit Grad  $< 2$

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

Irreduzibles Polynom:  $x^2+1$

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

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