## 19. Aufgabe

für alle "a" muss gelten ggT(a,n) = 1
(ggT = größter gemeinsamer Teiler)

Multiplikationstabelle für die Gruppe ( $Z_8^*, \times_8$ ) $\{a \in \mathbb{Z}_n : ggT(a,n) = 1\}$

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

| $\times_8$ | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

## 20. Aufgabe

Primfaktor von n = 9 mit Hilfe von Pollards Rho-Algorithmus finden: $x_1 = 4$ $k = 2$

| 1 | $x_{i-1}^2 - 1$ | $x_i$ | d | y |
|---|---|---|---|---|
| 2 | - | 4 $= x_1$ | - | (4) |
| 3 | $16 - 1 = 15$ | $x_2 = 15 \% 9 = 6$ | $(x_2 - y, n)ggT$ $(6-4, 9) = 1$ | $6 = x_i$ |
| 4 | $6^2 = 36 - 1 = 35$ | $35 \% 9 = 8 = x_3$ | $(x_3 - y, n)ggT$ $(8-6, 9)ggT = 1$ | 6 |
| 5 | $8^2 - 1 = 63$ | $63 \% 9 = 0 = x_4$ | $(0-6, 9)ggT = 3$ | 0 |
| 6 | | | | |

Start i = 1

i = 1 + 1

i = 2 + 1

$i = 2k$ $k = 4$

$i = 8$

Pseudocode (nach berechnung von d):

```
if (d != 1 and d != n):
    return d; #programm beendet

if (i==k):
    y = xi
    k = 2k
```

Der ermittelte Primfaktor: 3