Algebra Speziell für Kryptografie $\mathbb{Z}_n^*$ mit $n = p \cdot q$ Primzahlprodukt

Zahlen-Tafel bis 5 *mal* 7

(%o14)

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35

ZahlenTafel modulo 5

(%o15)

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

ZahlenTafel modulo 7

(%o16)

1	2	3	4	5	6	0
1	2	3	4	5	6	0
1	2	3	4	5	6	0
1	2	3	4	5	6	0
1	2	3	4	5	6	0

Zahlen-Tafel bis 3 *mal* 5

(%o9)

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

ZahlenTafel modulo 3

(%o10)

1	2	0	1	2
0	1	2	0	1
2	0	1	2	0

ZahlenTafel modulo 5

(%o11)

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

$p = 3 \quad q = 5$

Es gibt $n = p \cdot q = 15$ Zahlen in der Tafel, 3 Zeilen, 5 Spalten. Es gibt in jeder Spalte ein Vielfaches von 3, sichtbar an der 0 in der zweiten Tafel, also 5 Vielfache von 3. Es gibt 3 Zeilen, an jedem Zeilenende steht ein Vielfaches von 5, also 3 Nullen in der dritten Tafel. Also gibt es zusammen 5+3-1=7 Nullen, wenn man die Ecke rechts unten nicht doppelt zählt. Bleiben 15-7= 8 Zahlen, die teilefremd zu 15 sind.

Zahlen-Tafel bis 11 *mal* 13

(%o24)

1	2	3	4	5	6	7	8	9	10	11	12	13
14	15	16	17	18	19	20	21	22	23	24	25	26
27	28	29	30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49	50	51	52
53	54	55	56	57	58	59	60	61	62	63	64	65
66	67	68	69	70	71	72	73	74	75	76	77	78
79	80	81	82	83	84	85	86	87	88	89	90	91
92	93	94	95	96	97	98	99	100	101	102	103	104
105	106	107	108	109	110	111	112	113	114	115	116	117
118	119	120	121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140	141	142	143

Allgemein:

$$\varphi(n) = \varphi(p \cdot q) =$$
$$p \cdot q - (q + p - 1) =$$
$$p \cdot q + q - p + 1 =$$
$$(p-1) \cdot (q-1)$$

ZahlenTafel modulo 11

(%o25)

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

$$\varphi(p \cdot q) = (p-1) \cdot (q-1)$$

ZahlenTafel modulo 13

(%o26)

1	2	3	4	5	6	7	8	9	10	11	12	0
1	2	3	4	5	6	7	8	9	10	11	12	0
1	2	3	4	5	6	7	8	9	10	11	12	0
1	2	3	4	5	6	7	8	9	10	11	12	0
1	2	3	4	5	6	7	8	9	10	11	12	0
1	2	3	4	5	6	7	8	9	10	11	12	0
1	2	3	4	5	6	7	8	9	10	11	12	0
1	2	3	4	5	6	7	8	9	10	11	12	0
1	2	3	4	5	6	7	8	9	10	11	12	0
1	2	3	4	5	6	7	8	9	10	11	12	0
1	2	3	4	5	6	7	8	9	10	11	12	0

Wenn die Nullen der modulo-p-Tafel alle in die letzte Zeile sacken und man sie dann in die letzte Zeile der modulo-q-Tafel schreibt, hat man ein Zahlenfeld von $(p-1)(q-1)$ Zahlen ohne Nullen.