Multiplication tables in several mods:

mod 3 ×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

mod 4 ×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

mod 5 ×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

mod 6 ×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

mod 7 ×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

no zero has a

no zeroes

mod 8 ×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

mod 9 ×	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	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

not in the 0-row

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

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

multiplicative inverses

$2x = 7$ mod 11

$6 \cdot 2x = 6 \cdot 7$

$1 \cdot x = 9$

multiplicative inverses are useful.

$2 \cdot 3x = 4 \cdot 2 \pmod 5$

$1 \cdot x = 3$

They exist mod p ↑ prime

$3 \cdot 5x = 2 \cdot 3 \pmod 7$

$1 \cdot x = 6$

$2 \cdot 6x = 3 \cdot 2 \pmod{11}$

$1 \cdot x = 6$

(mod 31)

$8^{19} = 8^{16} \cdot 8^2 \cdot 8^1 = 8 \cdot 2 \cdot 8 = 4 \pmod{31}$

Powers by squaring

$8^1 = 8$

$8^2 = 2$

$8^4 = 2^2 = 4$

$8^8 = 4^2 = 16$

$8^{16} = 16^2 = 8$ $\quad 16^2 = 256$ $\quad \frac{256}{31} \sim 8.2\ldots$

$256 = 8 \cdot 31 + \_\_\_\_$

5^{22}

11^{14}

Solve for x

$$\begin{cases} 5x = 9 \pmod{11} \\ 3x = 2 \pmod{7} \\ 8x = 7 \pmod{11} \end{cases}$$

Homework

$7^{23} \pmod{31}$

15^{13}

$12^{24} \pmod{41}$

10^{15}

Find powers by squaring.

See also pg. 115.